(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6584500号
(P6584500)
(45)発行日　令和1年10月2日(2019.10.2)　(24)登録日　令和1年9月13日(2019.9.13)

(51)Int.Cl.　　F I
G06F 21/12 (2013.01)　　G06F 21/12 310
G06F 21/62 (2013.01)　　G06F 21/62 318

請求項の数 13　(全 21 頁)

(21)出願番号　特願2017-516669(P2017-516669)
(86)(22)出願日　平成27年9月23日(2015.9.23)
(65)公表番号　特表2017-530471(P2017-530471A)
(43)公表日　平成29年10月12日(2017.10.12)
(86)国際出願番号　PCT/US2015/051683
(87)国際公開番号　WO2016/049157
(87)国際公開日　平成28年3月31日(2016.3.31)
審査請求日　平成30年8月17日(2018.8.17)
(31)優先権主張番号　14/497,221
(32)優先日　平成26年9月25日(2014.9.25)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　314015767
マイクロソフト　テクノロジー　ライセンシング，エルエルシー
アメリカ合衆国　ワシントン州　９８０５２　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100106208
弁理士　宮前　徹
(74)代理人　100120112
弁理士　中西　基晴

最終頁に続く

(54)【発明の名称】トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストの表現

(57)【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伝えら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連する識別情報ベースの情報を表す、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、
要求コンテキストに基づいて再作成された認可プリンシパル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、

前記再作成された認可プリンシパル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、

前記再作成された認可プリンシパル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】

前記動作が、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伝えら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連する識別情報ベースの情報を表す、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、要求コンテキストに基づいて再作成された認可プリンシパル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】
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。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストの表現に関する。
【背景技術】
【０００２】
[0001]コンピューターがますます一般的になってきたことから、コンピューター上に記憶されるデータ量が増加している。このことは、比較的小スペース内に大量のデータを記憶する能力を含む、多くの利便性をユーザーにもたらす。ただし、このデータのいくらかは、多くの場合、秘密に保たれる、又は特定の個人に対してのみ明かされることが意図される。このデータは、パスワード又は個人識別番号を使用するなど、異なる方法で保護され得る。このような保護は有用であり得るが、コンピューターは、パスワード又は個人識別番号を推測するためのおびただしい数の試みがなされる辞書攻撃又はブルートフォース攻撃などの攻撃に対しては脆弱である恐れがある。これらの脆弱性は、ユーザーを彼らのコンピューターへの信頼を低下させるように導き、積極的なユーザーエクスペリエンスを損ねる可能性がある。
【発明の概要】

【発明が解決しようとする課題】
【０００３】
本発明は上記の課題を解決しようとするものである。
【課題を解決するための手段】
【０００４】
[0002]この発明の概要は、発明を実施するための形態でさらに後述される一揃いの概念を簡略化した形式で紹介するために提供される。この発明の概要は、クレームされた事項の主要な特徴又は本質的特徴を識別することを意図するものではなく、クレームされた事項の範囲を判断する際の補助として用いられることを意図するものでもない。
【０００５】
[0003]トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストを表現するための技術が説明される。少なくともいくつかの実施形態では、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が、トラステッドプラットフォームモジュール内で導出される。認可プリンシパルは、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へのアクセスのための認可ポリシーを定義するために使用され得る。
【０００６】
[0004]発明を実施するための形態は、添付図面を参照して説明される。図面では、参照番号の最上位桁は、その参照番号が最初に現れる図面を識別する。説明及び図面の中で異なるインスタンスに同一の参照番号を使用することは、類似の又は同一の物を示す可能性がある。
【図面の簡単な説明】
【０００７】
【図１】[0005]１つ又は複数の実施形態に従って本明細書で論じられる技術を用いて動作可能となる実装例での環境の図である。
【図２】[0006]１つ又は複数の実施形態による認可プリンシパルの実装の例を示す。
【図３】[0007]１つ又は複数の実施形態による認可ポリシーの実装の例を示す。
【図４】[0008]１つ又は複数の実施形態に従って認可プリンシパルを導出するための方法におけるステップを説明するフロー図である。
【図５】[0009]１つ又は複数の実施形態に従って認可ポリシーをセキュリティ資産に結び付けるための方法におけるステップを説明するフロー図である。
【図６】[0010]１つ又は複数の実施形態に従って認可ポリシーをセキュリティ資産に結び付けさせるための方法におけるステップを説明するフロー図である。
【図７】[0011]本明細書で説明する技術の実施形態を実装するように構成される、図１を参照して説明するシステム及びコンピューティングデバイスの例を示す。
【発明を実施するための形態】
【０００８】
概要
[0012]トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストを表現するための技術が説明される。概して、トラステッドプラットフォームモジュールは、保護されたハードウェア及び／又はファームウェア環境等の、一般的なシステムアクセスから保護される機能を指す。例えば、トラステッドプラットフォームモジュールは、コードが安全に実行され得る耐タンパ環境を表す。
【０００９】
[0013]様々な実装によれば、オペレーティングシステムコンテキストは、トラステッドプラットフォームモジュールを介して実装される認可プリンシパルを介して表現される。概して、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可能性のある異なった識別情報に基づく状態条件を表す。オペレーティングシステムコンテキスト属性の例は、ユーザー識別子、アプリケーション及びプロセス識別子、（例えば、ユーザーグループのための）グループ識別子、（例えば、異なるアクセス及び

セキュリティ特権レベルのための）特権識別子などを含む。

【００１０】

[0014]様々な実装によれば、認可プリンシパルは、オペレーティングシステムコンテキストに基づき定義される。例えば、オペレーティングシステムコンテキスト属性は、トラステッドプラットフォームモジュール（ＴＰＭ）アクセスモジュールによって処理されて、対応する認可プリンシパルを生成する。認可プリンシパルは、セキュリティキー（例えば、秘密キー）、セキュリティ証明書、保護されたデータなどの、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バインドされることができる。例えば、認可ポリシーは、認可プリンシパルで構成されて、バインドされたセキュリティ資産へのアクセスを制御することができる。

【００１１】

[0015]様々な実装によれば、本明細書で論じられる技術は、オペレーティングシステムコンテキストがトラステッドプラットフォームモジュールにおいて表現されることを可能にし、これにより、それまでのオペレーティングシステムの実装を超えてシステムセキュリティを高める。さらに、本明細書で論じられる技術は、トラステッドプラットフォームモジュールにおいて特徴付けられ、表現される多種多様なオペレーティングシステム関連の属性を提供し、それによって、既存のトラステッドプラットフォームモジュールの能力を高めて、異なるオペレーティングシステムコンテキストに関連したセキュリティ資産を保護する。

【００１２】

[0016]以下の説明では、最初に、本明細書に記載された技術を用いて動作可能である環境の例が説明される。次に、「手続きの例」と題するセクションは、１つ又は複数の実施形態に従ったトラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストを表現するためのいくつかの方法の例を説明する。最後に、「システム及びデバイスの例」と題するセクションは、１つ又は複数の実施形態に従って本明細書で論じる技術を用いて動作可能であるシステム及びデバイスの例を説明する。

環境の例

[0017]図１は、本明細書で論じるトラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストの技術表現を用いて動作可能な実装例における環境１００の図である。環境１００は、限定ではなく例として、スマートフォン、タブレットコンピューター、ポータブルコンピューター（例えば、ラップトップ）、デスクトップコンピューター、ウェアラブルデバイスなどの、任意の適切なデバイスとして具現化され得るコンピューティングデバイス１０２を含む。コンピューティングデバイス１０２の様々な異なる例の１つが示され、図７において後述される。

【００１３】

[0018]概して、コンピューティングデバイス１０２は、様々なユーザー１０４からアクセス可能であり、このユーザー１０４は様々なタスクを実行するためにコンピューティングデバイス１０２を活用することができる個人を表す。例えば、ユーザー１０４は、コンピューティングデバイス１０２を生産性業務（例えば、ワードプロセッシング、データ操作など）のために、通信（例えば、電子メール、ソーシャルネットワーキングなど）のために、コンテンツ消費（例えば、オーディオコンテンツ、ビデオコンテンツなど）のために、及び様々なその他の業務のために利用することができる。ユーザー１０４は、ユーザー識別子（ＩＤ）１０６に関連付けられ、ユーザー識別子は、個々のユーザー１０４を識別し、かつ個々のユーザー１０４を相互に区別するために活用され得るデータを表す。

【００１４】

[0019]様々な実装によれば、ユーザー１０４は、異なる基準に基づき異なるグループ１０８に集約され得る。個々のグループ１０８は、例えば、共通のセキュリティ及び／又はアクセス特権を共有するユーザー１０４の集合を表す。グループ１０８は、あるグループ１０８を別のグループ１０８から区別するために使用され得るグループ名を表す、グループ識別子（ＩＤ）１１０を介して互いに区別される。

【００１５】
[0020]コンピューティングデバイス１０２は、様々な活動及び業務を、例えばユーザー１０４によって実行されることを可能にする様々な異なる機能を含む。例えば、コンピューティングデバイス１０２は、オペレーティングシステム１１２及びアプリケーション１１４を含む。概して、オペレーティングシステム１１２は、ハードウェア、カーネルレベルモジュール及びサービス等のコンピューティングデバイス１０２の様々なシステムコンポーネントを統合するための機能を表す。例えば、オペレーティングシステム１１２は、コンピューティングデバイス１０２の様々な構成要素をアプリケーション１１４に統合して、コンポーネントとアプリケーション１１４間の対話を可能にすることができる。
【００１６】
[0021]アプリケーション１１４は、コンピューティングデバイス１０２を介して、ワードプロセッシング、ウェブブラウジング、電子メール、ソーシャルメディア、企業業務などの、様々な業務及び活動が実行されることを可能にする機能を表す。アプリケーション１１４は、コンピューティングデバイス１０２上にローカルにインストールされて、ローカルなランタイム環境を介して実行され得、かつ／又は、クラウドベースサービス、ウェブアプリなどの遠隔機能へのポータルを表すことができる。したがって、アプリケーション１１４は、ローカルに実行されるコード、遠隔のホストサービスへのポータルなどの、様々な形態をとることができる。
【００１７】
[0022]コンピューティングデバイス１０２は、さらに、トラステッドプラットフォームモジュール（ＴＰＭ）１１６を含み、ＴＰＭ１１６は、コンピューティングデバイス１０２の大部分又は全ての他の機能による一般的なアクセスから保護されるコンピューティングデバイス１０２の一部を表す。ＴＰＭ１１６は、別個の、専用ハードウェア環境（例えば専用チップ）、既存のハードウェア環境の細分化された部分（例えば、中央処理装置（ＣＰＵ）の副部分）、保護されたファームウェア環境などの、様々な方法で実装され得る。１つ又は複数の実装では、ＴＰＭ１１６は、Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｉｎｇ Ｇｒｏｕｐ（ＴＣＧ）から利用可能であるトラステッドプラットフォームモジュール（ＴＰＭ）仕様に従ったモジュールである。しかしながら、このことは限定することを意図するものではなく、ＴＰＭ１１６は、様々な他の方法で実装されてもよい。
【００１８】
[0023]様々な実装によれば、ＴＰＭ１１６との対話は、ＴＰＭアクセスモジュール１１８により仲介される。概して、ＴＰＭアクセスモジュール１１８は、オペレーティングシステム１１２のコンポーネント、アプリケーション１１４、ユーザー１０４などの、コンピューティングデバイス１０２の様々なコンポーネントがＴＰＭ１１６と対話することを可能にする機能を表す。少なくともいくつかの実装では、ＴＰＭアクセスモジュール１１８は、ＴＰＭ１１６に対する唯一のインターフェイスとして機能する。ＴＰＭアクセスモジュール１１８は、例えば、ＴＰＭ１１６のためのデバイスドライバーを表す。ＴＰＭアクセスモジュール１１８は、オペレーティングシステム１１２のコンポーネント、コンピューティングデバイス１０２の別個のシステムコンポーネント（例えば、カーネルレベルのコンポーネント）、これらの組合せなどの、様々な方法で実装されてもよい。
【００１９】
[0024]ＴＰＭ１１６は、ＴＰＭプロセッサ１２０及びＴＰＭ記憶装置１２２を含む。様々な実装によれば、ＴＰＭプロセッサ１２０は、ＴＰＭ１１６により活用されて、様々な処理タスクを実行することができる専用ハードウェア処理ユニットを表す。ＴＰＭ記憶装置１２２は、ＴＰＭ１１６のためのデータ記憶容量を表し、これは、ＴＰＭ１１６の外部のエンティティによるアクセスから保護される。
【００２０】
[0025]ＴＰＭ記憶装置１２２に、セキュリティ資産１２４、認可ポリシー１２６及び認可プリンシパル１２８が記憶される。概して、セキュリティ資産１２４は、特定のエンティティの識別情報、様々な種類のデータの認証及び／又は信頼される状態などを検証する

ために活用され得る異なる種類のセキュリティ関連情報を表す。セキュリティ資産１２４の例は、セキュリティキー（例えば、暗号化キー）、セキュリティ証明書、暗号化及び復号化アルゴリズム、保護されたデータなどを含む。認可プリンシパル１２８は、ＴＰＭ１１６の他の機能とは別個に例示されるが、少なくともいくつかの実装では、認可プリンシパル１２８は、ＴＰＭ内の既存のオブジェクト（例えば、セキュリティ資産１２４）によって表現され得る。セキュリティ資産１２４が構成され、活用され得る方法に関する詳細は、以下で論じられる。

【００２１】

[0026]認可ポリシー１２６は、セキュリティ資産１２４へのアクセスを制御するための異なる条件、規則、パラメータ及び命令を表す。例えば、個々の認可ポリシー１２６は、個々のセキュリティ資産１２４へのアクセスがそれぞれの認可ポリシー１２６を介して制御され得るように、個々のセキュリティ資産１２４にバインドされ得る。

【００２２】

[0027]様々な実装によれば、認可プリンシパル１２８は、オペレーティングシステム（ＯＳ）コンテキストが、例えば、認可ポリシー１２６を構成して、セキュリティ資産１２４へのアクセスを制御するために、ＴＰＭ１１６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す。概して、ＯＳコンテキストは、コンピューティングデバイス１０２に対する異なる実行シナリオに関連して発生する異なるオペレーティングシステム属性及びパラメータを指す。認可プリンシパル１２８を介して表されることができる異なるＯＳコンテキスト属性の例は、ユーザーＩＤ１０６、グループＩＤ１１０、アプリケーション１１４のためのアプリケーション識別子（ＩＤ）１３０などを含む。さらに詳細に以下で説明するように、認可ポリシー１２６は、認可プリンシパル１２８の１つ又は複数で構成されて、個々のセキュリティ資産１２４を特定の認可ポリシー１２６に結び付けることができる。

【００２３】

[0028]少なくともいくつかの実装では、認可プリンシパル１２８は、それぞれのプリンシパル識別子（ＩＤ）１３２を介して個別に識別可能であり、プリンシパルＩＤ１３２は、それぞれ、認可プリンシパル１２８の異なるインスタンスを参照する。様々な実装によれば、個々のプリンシパルＩＤ１３２は、対応する認可プリンシパル１２８が作成されるそれぞれのＯＳコンテキストに基づき生成される。例えば、特定の認可プリンシパル１２８を識別するプリンシパルＩＤ１３２は、それぞれのＯＳコンテキストに対する識別子をハッシュすることにより生成されて、ユーザーＩＤ１０６のダイジェスト、グループＩＤ１１０のダイジェスト、アプリケーションＩＤ１３０のダイジェスト、それらの組合せなどの、ＯＳコンテキストのダイジェストを生成することができる。

【００２４】

[0029]プリンシパルＩＤ１３２は、認可プリンシパル１２８とは別個に実装されるように例示されているが、これは限定することを意図するものではない。例えば、少なくともいくつかの実装では、プリンシパルＩＤ１３２は、認可プリンシパル１２８内に埋め込まれ、かつ／又は認可プリンシパル１２８の一部として実装され得る。例えば、少なくともいくつかの実装では、プリンシパルＩＤ１３２は、異なる認可プリンシパル１２８を識別し、区別するために参照可能である認可プリンシパル１２８の部分を表すことができる。

【００２５】

[0030]プリンシパルＩＤ１３２を利用するための付加的な又は代替の実装として、ＴＰＭアクセスモジュール１１８は、認可プリンシパルマッピング１３４を活用して、ＯＳコンテキストの対応する認可プリンシパル１２８への対応付を維持することができ、認可プリンシパルマッピング１２４に基づき、認可プリンシパル１２８を利用してＴＰＭ１１６内の対応する認可プリンシパル１２８にバインドされたセキュリティ資産１２４にアクセスすることができる。

【００２６】

[0031]ＴＰＭ１１６はさらに、プラットフォーム機能１３６及びプラットフォームレジ

スタ１３８を含む。プラットフォーム機能１３６は、認証機能、キー生成機能、暗号化及び復号化機能、コンテキスト関連機能などの、情報のセキュアな記憶装置を提供するために使用される様々な機能を表す。様々な実装によれば、ＴＰＭアクセスモジュール１１８は、プラットフォーム機能１３６と対話して、認可プリンシパル１２８、認可ポリシー１２６などを生成し、かつ／又は構成することができる。

【００２７】

[0032]プラットフォームレジスタ１３８は、コンピューティングデバイス１０２についてのシステム状態及びコンテキスト情報を記憶するための記憶場所を表す。例えば、プラットフォームレジスタ１３８は、システムブート時に収集されるオペレーティングシステム１１２のモジュールの測定値などの、様々なシステムコンポーネントの「測定値」を記憶するために活用されることができる。少なくともいくつかの実装では、プラットフォームレジスタは、ＴＰＭ１１６のプラットフォーム構成レジスタ（ＰＣＲ）を表す。

【００２８】

[0033]概して、「測定値」は、コンピューティングデバイス１０２のコードモジュール、コンピューティングデバイス１０２の構成データなどの、様々なデバイス関連データを識別及び／又は特徴付ける方法を指す。本明細書で使用されるように、用語「コードモジュール」は、概して、アプリケーション１１４の部分、サービス、オペレーティングシステム１１２のモジュール、プロセス、様々なバイナリ及び／又は実行可能ファイルなどの、実行可能なコードの部分を指す。測定値の例は、デバイス関連データ、データ署名、デバイス関連データの暗号化バージョン及び／又はデバイス関連データの部分などから生成されたハッシュ値を含む。測定値は、例えば、セキュアハッシュアルゴリズム（ＳＨＡ）、例えば、ＳＨＡ－１、ＳＨＡ－２など、をデバイス関連データに適用することにより生成されることができる。

【００２９】

[0034]様々な実装によれば、デバイス関連データの測定値は、システムのブート時に生成され、プラットフォームレジスタ１３８に記憶されることができる。概して、プラットフォームレジスタ１３８は、コンピューティングデバイス１０２のデバイス関連データに対する一連の測定値を記憶しており、新たな測定値を既存のレジスタ値に付加して連結値のハッシュを計算することにより特定のプラットフォームレジスタ１３８の新しい値が計算される。このプロセスは、デバイス関連データの複数の異なるインスタンス、例えば複数のコードモジュールに対して繰り返されることができる。様々な実装によれば、特定のデバイス関連データ（例えば、コードモジュール）がロードされたか否かに関するその後の決定は、プラットフォームレジスタ１３８に対する現在の値を計算するために使用されるプロセスに基づきデバイス関連データのハッシュを計算することにより実行され得る。次いで、計算されたハッシュは、プラットフォームレジスタ１３８に記憶された値と比較して、ハッシュが値と合致するか否かを確認する。ハッシュがこの値に合致する場合、このことは、コードモジュールがロードされていること、及びコードモジュールの現在のバージョンがプラットフォームレジスタ１３８で測定されたバージョンと合致することを示す。

【００３０】

[0035]例えば、特定のコードモジュールが、保護されたリソース（例えば、セキュリティ資産１２４）へのアクセスを要求する場合、プラットフォームレジスタ１３８内の現在の測定値が、このセキュリティ資産１２４のための認可ポリシー１２６に記憶された値と比較されることができる。値が合致する場合、システムが、認可ポリシー１２６が構成されたときのシステムの元の状態から変更されておらず、したがって、安全であり、保護されたリソースへのアクセスを可能にされ得ると判断され得る。測定値が合致しない場合、コンピューティングデバイスの状態は安全ではなく、したがって、保護されたリソースへのアクセスが拒否されてもよいと判断され得る。概して、コードモジュールの測定値を比較するプロセスは「安全性検証（ａｔｔｅｓｔａｔｉｏｎ）」と呼ばれる。

【００３１】

[0036]環境１００はまた、ネットワーク１４２を介してコンピューティングデバイス１０２に通信可能にアクセス可能であり得る様々な種類のリソースを表す、リモートリソース１４０を含む。リモートリソース１４０の例は、ウェブサイト、コンテンツストア、ネットワーク－ホスト型アプリケーション（例えば、ウェブアプリ）、ネットワーク－ホスト型サービス、ソーシャルメディアプラットフォームなどを含む。概して、リモートリソース１４０は、コンピューティングデバイス１０２が、コンテンツ、サービスなどにアクセスするといった、対話をすることができる任意の種類のリソースを表す。リモートリソース１４０は、コンピューティングデバイスの様々な種類及び／又は組合せを介して実装されることができて、これらの例は、図７において後述される。

【００３２】

[0037]１つ又は複数のネットワーク１４２は、環境１００の様々なエンティティが通信することができるネットワークを表す。ネットワーク１４２は、ローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、インターネット等の、様々な異なる構成をとることができる。少なくともいくつかの実装では、環境１００を参照して論じられる機能及び／又は本明細書での説明の他の部分は、図７を参照してより詳細に説明されるように、分散された環境（例えば、「クラウド上」）に実装されることができる。

【００３３】

[0038]図２は、１つ又は複数の実装に従った認可プリンシパル１２８の実装例を示す。上述したように、認可プリンシパル１２８は、オペレーティングシステム１１２と対話する異なるエンティティに対する識別子などの、コンピューティングデバイス１０２上に存在する可能性のある異なるＯＳコンテキストに基づいて導出される。

【００３４】

[0039]図２には、認可プリンシパル１２８を導出するために使用され得る、異なるＯＳ関連の識別子及び属性を表す一組のＯＳコンテキスト２００が含まれる。さらに、ＯＳコンテキスト２００に基づき導出される一組の認可プリンシパル２０２が示される。様々な実装によれば、認可プリンシパル２０２は、様々な異なる方法で導出されることができる。例えば、ＴＰＭ１１６は、ＴＰＭ１１６に対する内部的なキー（例えば、保証キー）を持つＯＳコンテキスト２０２の値に署名して、認可プリンシパル２０２を生成することができる。

【００３５】

[0040]認可プリンシパル２０２は、（ｎ個の）認可プリンシパル２０４（１）、・・・２０４（ｎ）を含む。認可プリンシパル２０４（１）、２０４（２）は、上述のユーザーＩＤ１０６などの、異なるユーザーを互いに区別するために使用されることができるユーザー識別子から導出される。認可プリンシパル２０４（３）、２０４（４）、２０４（５）は、上述のグループＩＤ１１０などの、グループを互いに区別するために使用されることができるグループ識別子から導出される。

【００３６】

[0041]認可プリンシパル２０４（６）、２０４（７）は、上述のアプリケーションＩＤ１３０などの、アプリケーションを互いに区別するために使用されることができるアプリケーション識別子から導出される。認可プリンシパル２０４（８）、２０４（９）は、アクセス特権、セキュリティ特権、操作特権などの、異なる特権レベルを互いに区別するために使用されることができる、特権識別子から導出される。これらの認可プリンシパルの例は、例示の目的のみのために提示されており、幅広く様々な他の種類及びインスタンスの認可プリンシパルが、開示された実装の趣旨及び範囲内で用いられ得ることを理解されたい。

【００３７】

[0042]様々な実装によれば、個々の認可プリンシパル２０２は、異なる方法で組み合わされて、様々な実行シナリオにおいて存在する可能性のあるＯＳコンテキストの異なる組合せを特徴付けることができる。

【００３８】

[0043]図３は、１つ又は複数の実装に従った認可ポリシー１２６の実装例を示す。認可ポリシー１２６は、セキュリティ資産３０２にバインドされた認可ポリシー３００を含む。様々な実装によれば、セキュリティ資産３０２は、上述のセキュリティ資産１２４のインスタンスを表す。認可ポリシー３００は、セキュリティ資産３０２へのアクセスを可能にするために満足されるべき様々な条件を指定する、ポリシー条件３０４を含む。この特定の例では、ポリシー条件３０４は、セキュリティ資産３０２に対するアクセスが許可される以前に適用されるべき一組の認可プリンシパルを指定する。

【００３９】

[0044]例えば、ポリシー条件３０４は、プリンシパル（アプリＩＤ＿Ｅ）及びプリンシパル（グループ＿Ｂ）の認可プリンシパルを指定する。したがって、要求側パーティが、プリンシパル（アプリＩＤ＿Ｅ）及びプリンシパル（グループ＿Ｂ）両者へのアクセス権を有していると検証済みである（例えば、安全性検証されている（ａｔｔｅｓｔｅｄ））場合、当該パーティは、セキュリティ資産３０２へのアクセスが可能になる。一方、要求側パーティが、プリンシパル（アプリＩＤ＿Ｅ）及びプリンシパル（グループ＿Ｂ）のプリンシパルの１つ又は複数へのアクセス権を有していない場合、要求側パーティは、セキュリティ資産３０２へのアクセスを拒否されることになる。

【００４０】

[0045]認可ポリシー１２６はさらに、セキュリティ資産３０８にバインドされる認可ポリシー３０６を含む。様々な実装によれば、セキュリティ資産３０８は、上述のセキュリティ資産１２４のインスタンスを表す。認可ポリシー３０２は、セキュリティ資産３０８へのアクセスを可能にするために満足されるべき様々な条件を指定する、ポリシー条件３１０を含む。この特定の例では、ポリシー条件３１０は、セキュリティ資産３０８に対するアクセスが許可される以前に適用されるべき一組の認可プリンシパルを指定する。

【００４１】

[0046]例えば、ポリシー条件３１０は、プリンシパル（ユーザー＿Ａ）、プリンシパル（アプリＩＤ＿Ｊ）及びプリンシパル（グループ＿｛Ｂ，Ｃ｝）の認可プリンシパルを指定する。したがって、要求側パーティが、プリンシパル（ユーザー＿Ａ）及びプリンシパル（アプリＩＤ＿Ｊ）プリンシパル両者、ならびにプリンシパル（グループ＿｛Ｂ，Ｃ｝）プリンシパルの少なくとも１つへのアクセス権を有していると検証済みである場合、当該パーティは、セキュリティ資産３０８へのアクセスが可能になる。一方、要求側パーティが、プリンシパル（ユーザー＿Ａ）及びプリンシパル（アプリＩＤ＿Ｊ）の１つ又は複数、ならびにプリンシパル（グループ＿｛Ｂ，Ｃ｝）プリンシパルの少なくとも１つへのアクセス権を有していない場合、要求側パーティは、セキュリティ資産３０８へのアクセスを拒否されることになる。

【００４２】

[0047]これらの認可ポリシー構成は、例の目的としてのみ提示されており、認可ポリシーが、様々な異なる方法で構成されて異なる認可プリンシパル構成及び組合せの多様な配列を反映することができることを理解されたい。

【００４３】

[0048]本明細書に記載された技術が動作することのできる環境の例を説明してきたが、ここで、１つ又は複数の実施形態に従ったいくつかの手続きの例の議論について考える。

手続きの例

[0049]以下のセクションでは、１つ又は複数の実施形態に従ったトラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストを表現するためのいくつかの手続きの例を説明する。手続きの例は、図１の環境１００、図７のシステム００、及び／又は任意の他の適切な環境において用いられ得る。例えば、本手順は、コンピューティングデバイス１０２により、例えばＴＰＭアクセスモジュール１１８を介して実行され得る。少なくともいくつかの実施形態では、様々な手続きについて説明するステップは、自動的に実装され、ユーザーの操作に依存しない。

【００４４】

[0050]図４は、１つ又は複数の実施形態による方法におけるステップを説明する、フロー図である。例えば、本方法は、１つ又は複数の実施形態に従った認可プリンシパルを導出するための手続きの例を説明する。

【００４５】

[0051]ステップ４００は、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において導出させる。概して、オペレーティングシステム（ＯＳ）コンテキストは、オペレーティングシステムに関して存在する可能性のある異なる識別情報ベースの状態条件を表す。例えば、ＴＰＭアクセスモジュール１１８は、プロセスから（例えば、アプリケーション１１４、システムプロセスなどから）要求を受信して、認可プリンシパルを生成する。概して、プロセスは、アプリケーションプロセス、システムプロセスなどの、ＴＰＭ１１６の外部のコンピューティングデバイス上で実行することができる任意のプロセスを表す。

【００４６】

[0052]例えば、認可プリンシパルは、プロセスに関連付けられたオペレーティングシステムコンテキストに基づく。したがって、ＴＰＭアクセスモジュール１１８は、認可プリンシパルをＴＰＭ１１６内に導出させる。例えば、ＯＳコンテキストデータ（例えば、ユーザーＩＤ、アプリケーションＩＤなど）は、トラステッドプラットフォームモジュールに対して安全であるキー（例えば、主キー、ルートキーなど）を使用してＴＰＭ１１６により処理されて、認可プリンシパルを導出する。したがって、個々の認可プリンシパル１２８は、様々な異なるＯＳコンテキストに対して作成され得る。

【００４７】

[0053]ステップ４０２は、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、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記憶されたセキュリティ資産とバインドさせる。例えば、ＴＰＭアクセスモジュール１１８は、セキュリティ資産へのアクセスが、認可ポリシー１２６を満足することを条件とするように、認可ポリシー１２６を認可プリンシパルで構成させる。

【００４８】

[0054]ステップ４０４は、認可プリンシパルへのアクセスの要求を受信する。例えば、プロセスは、認可プリンシパルにバインドされたセキュリティ資産へのアクセスを可能にするために、認可プリンシパルへのアクセス権を要求する。

【００４９】

[0055]ステップ４０６は、要求についての要求コンテキストが認可プリンシパルに合致するか否かを確認する。例えば、要求コンテキストは、認可プリンシパルへのアクセス権を要求するプロセスのためのＯＳコンテキストに対応する。ＯＳコンテキストの例は、プロセスに関連付けられたユーザー識別子、プロセスに関連付けられたアプリケーション識別子、プロセスに関連付けられたグループ識別子、プロセスに関連付けられた特権レベルなどを含む。

【００５０】

[0056]様々な実装によれば、要求コンテキストが認可プリンシパルと合致するか否かを確認するステップは、要求コンテキスト、例えば、提供されたＯＳコンテキストに基づいて認可プリンシパルを再作成することにより認可プリンシパルへのアクセス権を証明するステップを含む。例えば、認可プリンシパルを生成するために使用されるキー（主及び／又はルートキー）が、要求コンテキストを処理するために適用される。次いで、処理された要求コンテキストは、認可プリンシパルと比較されて、処理された要求コンテキストが認可プリンシパルに合致するか否かが確認される。要求コンテキスト（例えば、現在のＯＳコンテキスト）に基づき認可プリンシパルを再作成することによって、関連付けられた認可ポリシーが、認可プリンシパルへのアクセスが許可されているか否かを確認するために利用され得る。

【００５１】

[0057]要求についての要求コンテキストが認可プリンシパルに合致する場合（「はい」

）、ステップ４０８は、要求コンテキストが認可プリンシパルに合致することに応答して、認可プリンシパルへのアクセスを可能にする。少なくともいくつかの実装では、認可プリンシパルへのアクセス権は、認可プリンシパルにバインドされたセキュリティ資産へのアクセスを可能にする。例えば、認可プリンシパルへのアクセスの要求は、ＴＰＭ１１６に転送されることができ、ＴＰＭ１１６は、要求コンテキストがセキュリティ資産の認可ポリシーを満足することに応答して、セキュリティ資産へのアクセスを可能にすることができる。

【００５２】

[0058]上述のように、要求コンテキストを認可プリンシパルに合致させるステップは、認可プリンシパルを生成するために使用されるキーを要求コンテキストに適用することによって認可プリンシパルを再作成しようと試みるステップを含むことができる。したがって、認可プリンシパルが、要求コンテキストを使用して成功裡に再作成された場合、認可プリンシパルへのアクセスが許可される。

【００５３】

[0059]要求についての要求コンテキストが認可プリンシパルに合致しない場合（「いいえ」）、ステップ４１０は、要求コンテキストが認可プリンシパルに合致しないことに応答して、認可プリンシパルへのアクセスを拒否する。例えば、ＴＰＭアクセスモジュール１１８は、認可プリンシパルへのアクセスの要求がＴＰＭ１１６に転送されることを防止する。

【００５４】

[0060]上述のように、要求コンテキストを認可プリンシパルに合致させるステップは、認可プリンシパルを生成するために使用されるキーを要求コンテキストに適用することによって認可プリンシパルを再作成しようと試みるステップを含むことができる。したがって、認可プリンシパルが、要求コンテキストを使用して成功裡に再作成されなかった場合、認可プリンシパルへのアクセスは許可されない。

【００５５】

[0061]図５は、１つ又は複数の実施形態に従った方法のステップを説明するフロー図である。例えば、本方法は、１つ又は複数の実施形態に従って認可ポリシーをセキュリティ資産にバインドするための手続きの例を説明する。

【００５６】

[0062]ステップ５００は、要求を受信して、トラステッドプラットフォームモジュール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。例えば、要求は、アプリケーション、及び／又は、コンピューティングデバイス１０２上にローカルに存在する他のプロセスから受信される。あるいは要求は、リモートリソース１４０などの遠隔のエンティティから受信されてもよい。様々な実装によれば、この要求は、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する。少なくともいくつかの実装では、セキュリティ資産は、上述のセキュリティ資産１２４の実装を表す。

【００５７】

[0063]ステップ５０２は、認可ポリシーをトラステッドプラットフォームモジュール内で１つ又は複数の認可プリンシパルで構成させる。例えば、ＴＰＭアクセスモジュール１１８は、１つ又は複数の認可プリンシパルをＴＰＭ１１６に伝達し、ＴＰＭ１１６は認可ポリシー１２６に１つ又は複数の認可プリンシパルを設定する。

【００５８】

[0064]ステップ５０４は、認可ポリシーを、トラステッドプラットフォームモジュールに記憶されたセキュリティ資産にバインドさせる。例えば、ＴＰＭアクセスモジュール１１８は、認証ポリシーがセキュリティ資産にバインドされるべきであることをＴＰＭ１１６に指示する。様々な実装によれば、セキュリティ資産へのアクセスの要求を可能にするステップは、要求コンテキストが認可ポリシーの１つ又は複数の認可プリンシパルに合致することが条件とされる。

【００５９】
[0065]ステップ５０６は、セキュリティ資産へのアクセスの要求を受信する。例えば、コンピューティングデバイス１０２上で走行するプロセスは、セキュリティ資産へのアクセスを要求する。
【００６０】
[0066]ステップ５０８は、要求についての要求コンテキストが認可ポリシーを満足するか否かを確認する。例えば、要求コンテキストが、認可ポリシーにより指定された１つ又は複数の認可プリンシパルに合致するか否かが判断される。上述のように、要求は、例えば、アプリケーション１１４に関連付けられる、コンピューティングデバイス１０２上で走行するプロセスによって始動されることができる。したがって、要求コンテキストは、プロセスに関連付けられた１つ又は複数のＯＳコンテキストを含むことができ、この例が詳細に上述されている。
【００６１】
[0067]様々な実装によれば、要求コンテキストが認可ポリシーを満足するか否かを確認するステップは、要求コンテキスト、認可ポリシーにバインドされた１つ又は複数の認可プリンシパルを再作成しようと試みるステップを含む。例えば、１つ又は複数の認可プリンシパルを生成するために使用されるキーが、要求コンテキストに適用される。したがって、１つ又は複数の認可プリンシパルへのアクセス権は、１つ又は複数の認可プリンシパルが要求コンテキストを使用して成功裡に再作成されたか否かに基づく。
【００６２】
[0068]要求についての要求コンテキストが認可ポリシーを満足する場合（「はい」）、ステップ５１０は、要求についての要求コンテキストが認可ポリシーを満足することに応答して要求を可能にする。例えば、認可ポリシーにバインドされた１つ又は複数の認可プリンシパルが、要求コンテキストを使用して成功裡に再作成される場合、セキュリティ資産へのアクセスの要求が許可される。様々な実装によれば、要求を許可するステップは、要求側エンティティがセキュリティ資産にアクセスすることを可能とする。
【００６３】
[0069]要求についての要求コンテキストが認可ポリシーを満足しない場合（「いいえ」）、ステップ５１２は、要求についての要求コンテキストが認可ポリシーを満足しないことに応答して要求を拒否する。例えば、認可ポリシーにバインドされた１つ又は複数の認可プリンシパルが、要求コンテキストを使用して成功裡に再作成されない場合には、セキュリティ資産へのアクセスの要求は拒否される。例えば、要求側エンティティは、セキュリティ資産へのアクセスを拒否される。
【００６４】
[0070]図６は、１つ又は複数の実施形態に従った方法のステップを説明するフロー図である。例えば、本方法は、認可ポリシーを１つ又は複数の実施形態に従ってセキュリティ資産にバインドさせるための手続きの例を説明する。
【００６５】
[0071]ステップ６００は、コンピューティングデバイスのプロセスのための認可プリンシパルを、コンピューティングデバイスのトラステッドプラットフォームモジュールのレジスタに拡張する。例えば、ＴＰＭアクセスモジュール１１８は、プロセスの１つ又は複数の認可プリンシパルをレジスタに拡張させる特定のプラットフォームレジスタ１３８上の拡張動作を実行する。例えば、レジスタは、トラステッドプラットフォームモジュールのプラットフォーム構成レジスタ（ＰＣＲ）に対応する。
【００６６】
[0072]ステップ６０２は、トラステッドプラットフォームモジュールのレジスタからのデータについての要求側エンティティからの要求を受信する。様々な実装によれば、要求側エンティティは、アプリケーション１１４、リモートリソース１４０などのようなトラステッドプラットフォームモジュールの外部にある。
【００６７】

[0073]ステップ６０４は、レジスタからのデータを要求側エンティティに返し、返されたデータは、プロセスのための認可プリンシパルに基づいて生成された識別子を含む。例えば、識別子は、プロセスのオペレーティングシステムコンテキストに対応した認可プリンシパルに少なくとも部分的には基づき生成される。例えば、上述のように、識別子は、認可プリンシパル１２８のために生成されるプリンシパルＩＤ１３２に対応することができる。さらに上述のように、プリンシパルＩＤ１３２は、関連する認可プリンシパル１２８とは別個に、あるいは、関連する認可プリンシパル１３２内に埋め込まれかつ／又はその一部として実装される識別子として実装されることができる。

【００６８】

[0074]ステップ６０６は、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が認可プリンシパルで構成された認可ポリシーにバインドされるべきとの要求側エンティティからの指示を受信する。例えば、ＴＰＭアクセスモジュール１１８は、要求側エンティティから要求を受信する。

【００６９】

[0075]ステップ６０８は、認可プリンシパルがセキュリティ資産へのアクセスのための条件を表すように、認可ポリシーをトラステッドプラットフォームモジュール内のセキュリティ資産にバインドさせる。例えば、ＴＰＭアクセスモジュール１１８は、ＴＰＭ１１６と対話して、セキュリティ資産に対する認可ポリシーを構成する。概して、認可ポリシーは、セキュリティ資産へのアクセスのための様々な条件を指定する。例えば、認可ポリシーがセキュリティ資産へのアクセスを指定することは、要求側エンティティが認可ポリシー内で指定された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。少なくともいくつかの実装では、認可ポリシーは、セキュリティ資産へのアクセスのための条件を表す複数の認可プリンシパルを指定する。

【００７０】

[0076]トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストの表現のためのいくつかの手続きの例を論じてきたが、ここで、１つ又は複数の実施形態に従ったシステム及びデバイスの例についての議論を考える。

システム及びデバイスの例

[0077]図７は、コンピューティングデバイスの例７０２を含む、システムの例を全体的に７００で示し、コンピューティングデバイスの例７０２は、本明細書で説明される様々な技術を実装し得る１つ又は複数のコンピューティングシステム及び／又はデバイスを表す。例えば、図１を参照して上記で論じたコンピューティングデバイス１０２は、コンピューティングデバイス７０２として具現化されることができる。コンピューティングデバイス７０２は、例えば、サービスプロバイダーのサーバー、クライアントに関連付けられるデバイス（例えば、クライアントデバイス）、オンチップシステム、及び／又はいかなる他の適切なコンピューティングデバイスもしくはコンピューティングシステムであってもよい。

【００７１】

[0078]図示するコンピューティングデバイスの例７０２は、互いに通信可能に連結される、処理システム７０４、１つ又は複数のコンピューター可読メディア７０６、及び１つ又は複数の入力／出力（Ｉ／Ｏ：Ｉｎｐｕｔ／Ｏｕｔｐｕｔ）インターフェイス７０８を含む。図示していないが、コンピューティングデバイス７０２は、様々なコンポーネントを互いに連結する、システムバス、又は他のデータ及びコマンド転送システムをさらに含んでもよい。システムバスは、様々なバスアーキテクチャのいずれかを利用する、メモリバスもしくはメモリコントローラ、周辺バス、ユニバーサルシリアルバス、及び／又はプロセッサバスもしくはローカルバスなどの、様々なバス構造のうちのいずれか１つ又はその組合せを含むことができる。様々な他の例も、制御ライン及びデータラインとして検討される。

【００７２】

[0079]処理システム７０４は、１つ又は複数の動作を、ハードウェアを使用して実行す

る機能を表す。したがって、処理システム７０４は、プロセッサ、機能ブロックなどとして構成され得るハードウェア要素７１０を含むものとして示される。これは、特定用途向け集積回路、又は１つもしくは複数の半導体を使用して形成される他の論理デバイスとしてのハードウェアでの実装を含んでもよい。ハードウェア要素７１０は、それらが形成される物質、又はそこで採用される処理機構によって限定されない。例えば、プロセッサは、半導体及び／又はトランジスタ（例えば、電子集積回路（ＩＣ：ｉｎｔｅｇｒａｔｅｄ　ｃｉｒｃｕｉｔ））からなるものでもよい。このような文脈において、プロセッサが実行可能な命令は、電子的に実行可能な命令であってもよい。

【００７３】

[0080]コンピューター可読メディア７０６は、メモリ／記憶装置７１２を含むものとして示される。メモリ／記憶装置７１２は、１つ又は複数のコンピューター可読メディアに関連付けられるメモリ／記憶装置の容量を表す。メモリ／記憶装置７１２は、揮発性メディア（ランダムアクセスメモリ（ＲＡＭ：ｒａｎｄｏｍ　ａｃｃｅｓｓ　ｍｅｍｏｒｙ）など）及び／又は不揮発性メディア（読み出し専用メモリ（ＲＯＭ：ｒｅａｄ　ｏｎｌｙ　ｍｅｍｏｒｙ）、フラッシュメモリ、光ディスク、磁気ディスクなど）を含んでもよい。メモリ／記憶装置７１２は、固定メディア（例えば、ＲＡＭ、ＲＯＭ、固定ハードドライブなど）及びリムーバブルメディア（例えば、フラッシュメモリ、リムーバブルハードドライブ、光ディスクなど）を含んでもよい。コンピューター可読メディア７０６は、以下でさらに説明される、様々な他の方法で構成されてもよい。

【００７４】

[0081]入力／出力インターフェイス７０８は、ユーザーがコンピューティングデバイス７０２にコマンド及び情報を入力することを可能にし、かつ、情報が様々な入力／出力デバイスを用いてユーザー及び／又は他のコンポーネントもしくはデバイスに提示されることをも可能にする、機能を表す。入力デバイスの例は、キーボード、カーソル制御デバイス（例えば、マウス）、マイクロホン（例えば、音声認識用及び／又は音声入力用）、スキャナー、タッチ機能（例えば、物理的接触を検出するように構成される、容量性センサー又は他のセンサー）、カメラ（例えば、接触をジェスチャとして含まない、動きを検出するために赤外振動数などの可視又は不可視波長を採用し得るカメラ）などを含む。出力デバイスの例は、ディスプレイデバイス（例えば、モニター又はプロジェクター）、スピーカー、プリンター、ネットワークカード、触覚レスポンスデバイスなどを含む。したがって、コンピューティングデバイス７０２は、以下さらに説明するような様々な方法で、ユーザーの操作をサポートするように構成され得る。

【００７５】

[0082]ソフトウェア、ハードウェア要素、又はプログラムモジュールの一般的な文脈において、様々な技術が本明細書で説明され得る。概して、このようなモジュールは、特定のタスクを実行し、又は特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、要素、コンポーネント、データ構造などを含む。本明細書で用いる「モジュール」、「機能」、「エンティティ」及び「コンポーネント」という用語は、概して、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組合せを表す。本明細書で説明する技術の特徴は、プラットフォームに依存しないことであり、これは、様々なプロセッサを有する、様々な商用コンピューティングプラットフォーム上で、技術が実装され得ることを意味する。

【００７６】

[0083]説明したモジュール及び技術の実装は、何らかの形式のコンピューター可読メディア上に記憶され、又は何らかの形式のコンピューター可読メディアを介して送信されてもよい。コンピューター可読メディアは、コンピューティングデバイス７０２によってアクセスされ得る、様々なメディアを含んでもよい。限定ではなく例として、コンピューター可読メディアは、「コンピューター可読記憶メディア」及び「コンピューター可読信号メディア」を含むことができる。

【００７７】

[0084]「コンピューター可読記憶メディア」は、単なる信号伝送、搬送波、又は信号自体とは対照的に、情報の永続的記憶を可能にするメディア及び／又はデバイスを指すことができる。コンピューター可読記憶メディアは、信号自体を含まない。コンピューター可読記憶メディアは、コンピューター可読命令、データ構造、プログラムモジュール、論理素子／回路、又は他のデータなどの情報の記憶に適切な方法又は技術で実装される、揮発性の及び不揮発性の、リムーバブル及び非リムーバブルメディアならびに／又は記憶デバイスなどのハードウェアを含む。コンピューター可読記憶メディアの例は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、もしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ：ｄｉｇｉｔａｌ　ｖｅｒｓａｔｉｌｅ　ｄｉｓｋｓ）もしくは他の光学式記憶装置、ハードディスク、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、又は他の記憶デバイス、有形メディア、もしくは所望の情報を記憶するのに適切で、コンピューターによりアクセスされ得る製品を含むことができるが、限定はされない。

【００７８】

[0085]「コンピューター可読信号メディア」は、ネットワークを介するなどして命令をコンピューティングデバイス７０２のハードウェアに送信するように構成される信号担持メディアを指すことができる。信号メディアは、典型的には、コンピューター可読命令、データ構造、プログラムモジュール、又は、搬送波、データ信号、もしくは他の伝送機構などの変調データ信号中の他のデータを具現化することができる。信号メディアは、いかなる情報配信メディアをも含む。「変調データ信号」という用語は、信号内の情報を符号化するように設定され、又は変更される信号の特性のうち１つ又は複数の特性を有する信号を意味する。限定ではなく例として、通信メディアは、有線ネットワーク又は直接有線接続などの有線メディア、ならびに音波、無線周波数（ＲＦ：ｒａｄｉｏ　ｆｒｅｑｕｅｎｃｙ）、赤外線、及び他の無線メディアなどの無線メディアを含む。

【００７９】

[0086]前述したように、ハードウェア要素７１０及びコンピューター可読メディア７０６は、本明細書で説明する技術の少なくともいくつかの態様を実装するために、いくつかの実施形態で採用され得る命令、モジュール、プログラム可能なデバイスロジック及び／又はハードウェア形式で実装される固定デバイスロジックを表す。ハードウェア要素は、集積回路又はオンチップシステムのコンポーネント、特定用途向け集積回路（ＡＳＩＣ：ａｐｐｌｉｃａｔｉｏｎ－ｓｐｅｃｉｆｉｃ　ｉｎｔｅｇｒａｔｅｄ　ｃｉｒｃｕｉｔ）、フィールドプログラマブルゲートアレイ（ＦＰＧＡ：ｆｉｅｌｄ－ｐｒｏｇｒａｍｍａｂｌｅ　ｇａｔｅ　ａｒｒａｙ）、結合プログラム可能論理回路（ＣＰＬＤ：ｃｏｍｐｌｅｘ　ｐｒｏｇｒａｍｍａｂｌｅ　ｌｏｇｉｃ　ｄｅｖｉｃｅ）、及びシリコン又は他のハードウェアデバイスでの他の実装を含んでもよい。この文脈では、ハードウェア要素は、処理デバイスとして動作してもよく、処理デバイスは、実行する命令を記憶するために利用されるハードウェア要素及びハードウェアデバイス、例えば、前述のコンピューター可読記憶メディアにより具現化される命令、モジュール、及び／又はロジックにより定義されるプログラムタスクを実行する。

【００８０】

[0087]前述したものを組み合わせたものが、また、本明細書で説明した様々な技術及びモジュールを実装するために採用されることができる。したがって、ソフトウェア、ハードウェア、又はプログラムモジュール、及び他のプログラムモジュールは、ある形式のコンピューター可読記憶メディア上で、及び／又は１つ又は複数のハードウェア要素７１０によって具現化される、１つ又は複数の命令及び／又はロジックとして実装されることができる。コンピューティングデバイス７０２は、ソフトウェアモジュール及び／又はハードウェアモジュールに対応する特定の命令及び／又は関数を実装するように構成されてもよい。したがって、コンピューティングデバイス７０２によってソフトウェアとして実行可能なモジュールの実装は、例えば、処理システムのコンピューター可読記憶メディア及び／又はハードウェア要素７１０の使用を通じて、ハードウェア内で少なくとも部分的に

実現されることができる。命令及び／又は関数は、１つ又は複数の製品（例えば、１つ又は複数のコンピューティングデバイス７０２及び／又は処理システム７０４）によって、本明細書で説明される技術、モジュール、及び例を実装するように実行可能／動作可能であってもよい。

【００８１】

[0088]図７でさらに示すように、システムの例７００は、パーソナルコンピューター（ＰＣ：ｐｅｒｓｏｎａｌ　ｃｏｍｐｕｔｅｒ）、テレビジョンデバイス、及び／又はモバイルデバイス上でのアプリケーション実行時における、シームレスなユーザーエクスペリエンスのためのユビキタス環境を可能にする。アプリケーションを利用する、ビデオゲームをする、ビデオを見るなどの間に、１つのデバイスから次のデバイスへと移行する際の共通のユーザーエクスペリエンスについて、サービス及びアプリケーションは、３つの環境全てにおいて実質的に同様に実行される。

【００８２】

[0089]システムの例７００では、複数のデバイスは、中央コンピューティングデバイスを通じて相互接続される。中央コンピューティングデバイスは、複数のデバイスに対しローカル接続されてもよく、又は、複数のデバイスから遠隔設置されてもよい。１つの実施形態では、中央コンピューティングデバイスは、ネットワーク、インターネット、又は他のデータ通信リンクを通じて複数のデバイスに接続される１つ又は複数のサーバーコンピューターのクラウドであってもよい。

【００８３】

[0090]１つの実施形態では、この相互接続アーキテクチャによって、複数のデバイスを横断して配信される機能が、複数のデバイスのユーザーに共通の、かつシームレスなエクスペリエンスを提供することが可能となる。複数のデバイスのそれぞれは、異なる物理的要件及び能力を有する可能性があり、中央コンピューティングデバイスは、プラットフォームを使用して、デバイスに適合し、かつ全てのデバイスに共通するエクスペリエンスがデバイスに配信されることを可能にする。１つの実施形態では、ターゲットデバイスのクラスが生成され、エクスペリエンスは、デバイスのジェネリッククラスに適合する。デバイスのクラスは、デバイスの物理的特徴、使用形態、又は他の共通の特性によって定義されることができる。

【００８４】

[0091]様々な実装では、コンピューティングデバイス７０２は、コンピューター７１４、モバイル７１６、及びテレビジョン７１８の使用のためなどの、様々な異なる構成を想定してもよい。これらの構成のそれぞれは、概して異なる構成及び能力を有する可能性があるデバイスを含み、したがって、コンピューティングデバイス７０２は、異なるデバイスクラスのうちの１つ又は複数のデバイスクラスに従って構成され得る。例えば、コンピューティングデバイス７０２は、パーソナルコンピューター、デスクトップコンピューター、マルチ画面コンピューター、ラップトップコンピューター、ネットブックなどを含む、コンピューター７１４クラスのデバイスとして実装されてもよい。

【００８５】

[0092]コンピューティングデバイス７０２はまた、携帯電話、携帯型音楽プレーヤー、携帯ゲームデバイス、タブレットコンピューター、ウェアラブルデバイス、マルチ画面用コンピューターなどのモバイルデバイスを含むモバイル７１６クラスのデバイスとしても実装され得る。コンピューティングデバイス７０２は、また、普段の視聴環境において、通常大型画面を有し、又は通常大型画面に接続されるデバイスを含む、テレビジョン７１８クラスのデバイスとして実装されてもよい。これらのデバイスは、テレビジョン、セットトップボックス、ゲームコンソールなどを含む。

【００８６】

[0093]本明細書で説明した技術は、コンピューティングデバイス７０２のこれら様々な構成によってサポートされ得るが、本明細書で説明した技術の特定の例に限定されない。例えば、コンピューティングデバイス１０２及び／又はＴＰＭアクセスモジュール１１８

に関して論じた機能は、以下で説明されるように「クラウド」７２０上でプラットフォーム７２２を介するなどして、分散システムの使用を通じて全体又は一部が実装され得る。

【００８７】

[0094]クラウド７２０は、リソース７２４のためのプラットフォーム７２２を含み、かつ／又は表す。プラットフォーム７２２は、クラウド７２０のハードウェア（例えば、サーバー）及びソフトウェアリソースの基盤となる機能を抽象化する。リソース７２４は、コンピューティングデバイス７０２から離れたサーバー上でコンピューター処理が実行される間に利用できるアプリケーション及び／又はデータを含んでもよい。リソース７２４は、インターネット上で、及び／又はセルラーネットワークもしくはＷｉ－Ｆｉネットワークなどのサブスクライバーネットワークを通じて提供されるサービスを含むこともできる。

【００８８】

[0095]プラットフォーム７２２は、コンピューティングデバイス７０２を他のコンピューティングデバイスと接続するためのリソース及び関数を抽象化することができる。プラットフォーム７２２は、また、プラットフォーム７２２を介して実装されるリソース７２４について直面する要求に対して、対応するレベルのスケールを提供するためのリソースのスケーリングを抽象化する役割をする。したがって、相互接続したデバイスの実施形態では、本明細書で説明する機能の実装は、システム７００の至る所に分散されることができる。例えば、機能は、コンピューティングデバイス７０２上で部分的に実装されることができ、同様に、クラウド７２０の機能を抽象化するプラットフォーム７２２を介して実装されることができる。

【００８９】

[0096]本明細書で論じるのは、本明細書で論じる技術を実行するように実装され得る多数の方法である。方法の態様は、ハードウェア、ファームウェアもしくはソフトウェア、又はこれらの組合せで実装されることができる。方法は、１つ又は複数のデバイスによって実行される動作を指定するステップの集合として示され、動作の実行についてそれぞれのブロックによって示される順序に必ずしも限定されない。さらに、特定の方法に関して示す動作は、１つ又は複数の実装に従って、別の方法の動作と組み合わされてもよく、かつ／又は交換されてもよい。方法の態様は、環境１００に関して上記で論じた様々なエンティティ間の相互作用を介して実装されることができる。

結論

[0097]トラステッドプラットフォームモジュールにおけるオペレーティングシステムコンテキストの表現のための技術が説明される。構造的特徴及び／又は方法論的な動作に固有の言葉で、実施形態が説明されているが、添付の請求項で定義される実施形態は、説明した特定の特徴又は動作に必ずしも限定されないと理解されるべきである。むしろ、特定の特徴及び動作は、クレームされる実施形態を実装する形式の例として開示される。

【図１】

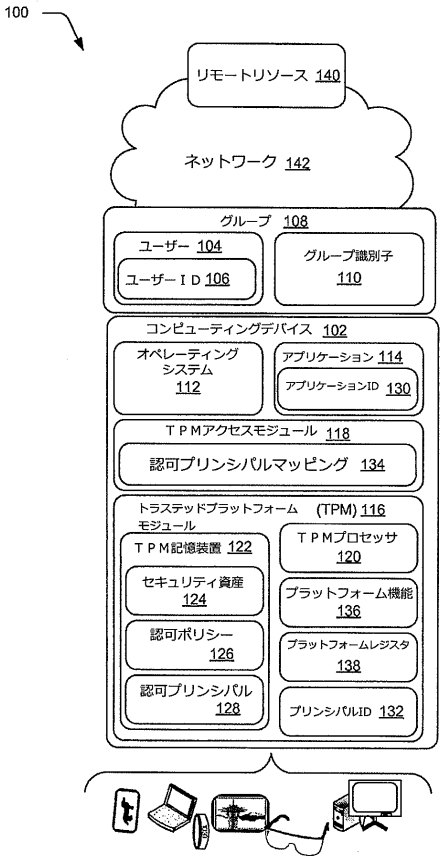

FIG. 1

【図２】

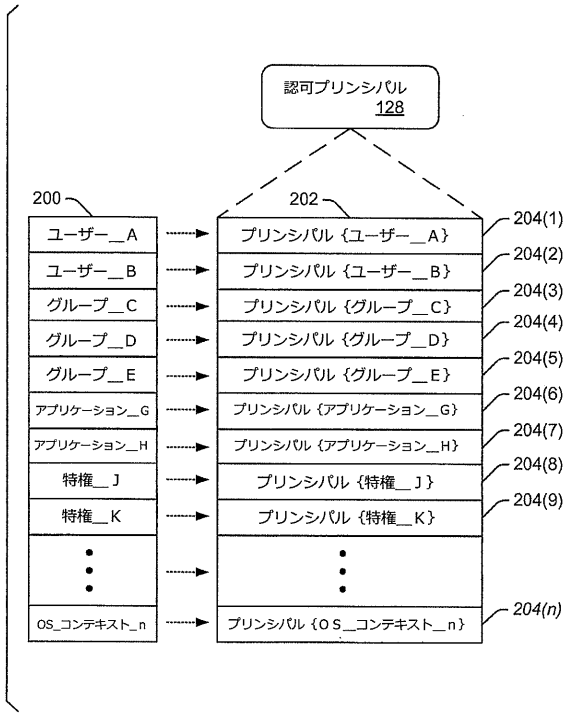

FIG. 2

【図３】

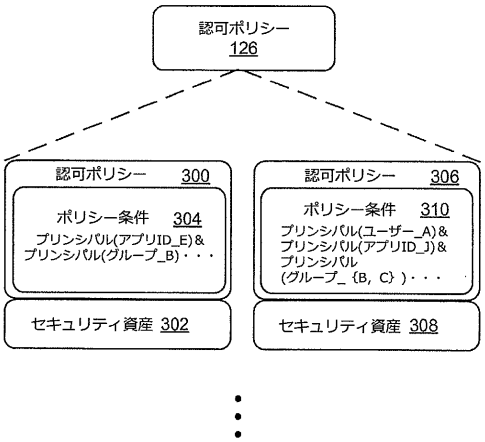

FIG. 3

【図４】

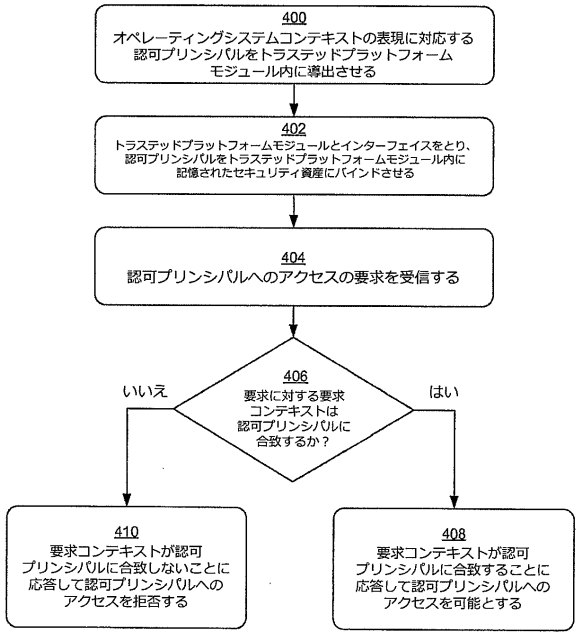

FIG. 4

【図５】

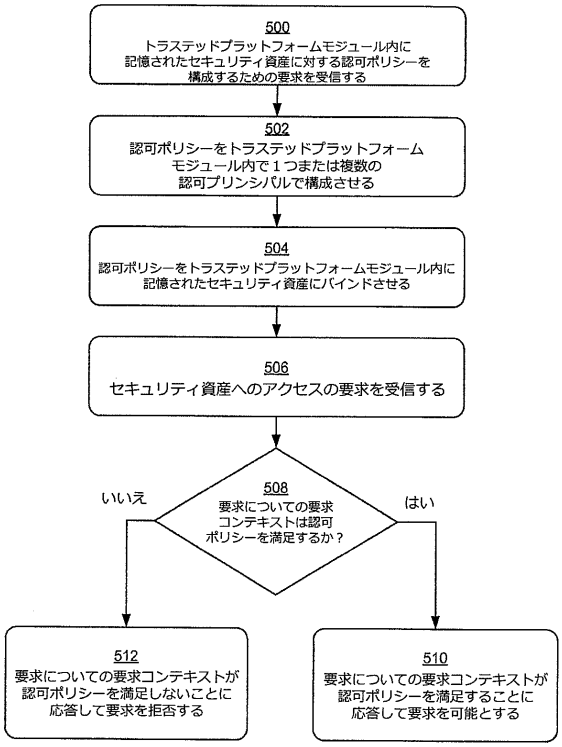

FIG. 5

【図６】

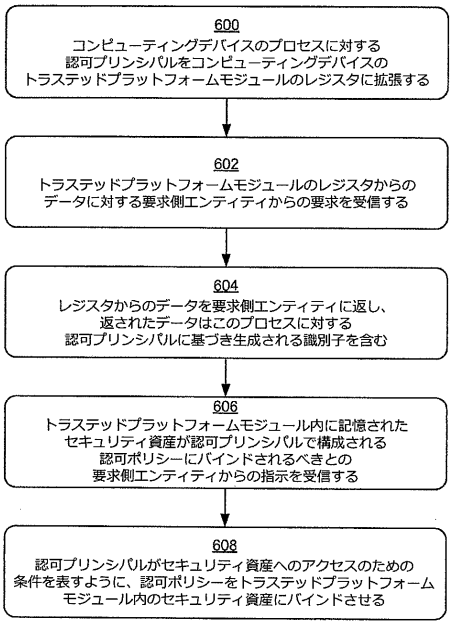

FIG. 6

【図７】

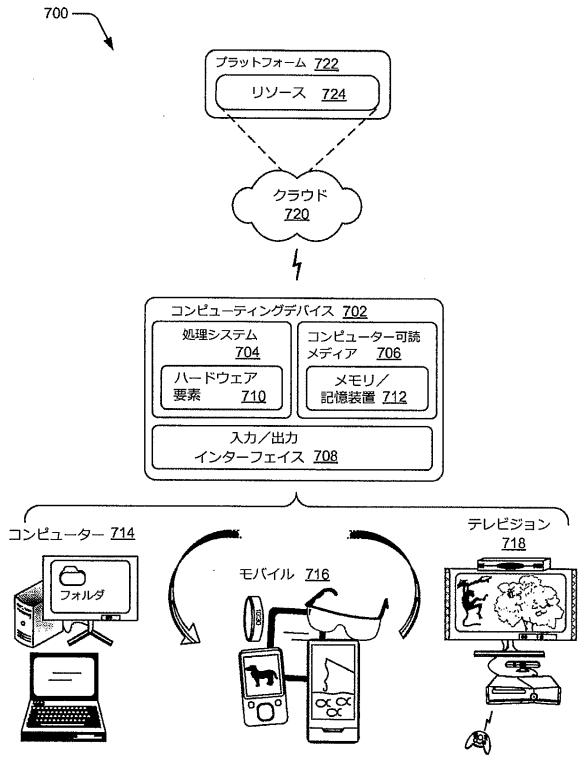

FIG. 7

フロントページの続き

(74)代理人 100147991
弁理士 鳥居 健一
(72)発明者 トム, ステファン
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ
(72)発明者 アイグナー, ロナルド
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ
(72)発明者 パイ, ナヴィン
アメリカ合衆国 ワシントン州 ９８０５２－６３９９ レッドモンド ワン マイクロソフト ウェイ, マイクロソフト コーポレーション, エルシーエイ－インターナショナル・パテンツ

審査官 金沢 史明

(56)参考文献 特表２０１４－５０３９０９（ＪＰ, Ａ）
特表２０１２－５２０５０１（ＪＰ, Ａ）
特開平１１－１７５４０２（ＪＰ, Ａ）
米国特許出願公開第２０１２／０２９７４５５（ＵＳ, Ａ１）
Stan Reimer, 他, Microsoft Windows Server 2008 リソースキット Active Directory編, 日経BPソフトプレス, ２００８年 9月２９日, 初版, pp. 283-290

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１／１２
Ｇ０６Ｆ ２１／６２