(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6147731号
(P6147731)
(45)発行日　平成29年6月14日(2017.6.14)　(24)登録日　平成29年5月26日(2017.5.26)

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

請求項の数 10 (全 20 頁)

(21)出願番号	特願2014-509279(P2014-509279)
(86)(22)出願日	平成23年10月10日(2011.10.10)
(65)公表番号	特表2014-517383(P2014-517383A)
(43)公表日	平成26年7月17日(2014.7.17)
(86)国際出願番号	PCT/US2011/055629
(87)国際公開番号	WO2012/150955
(87)国際公開日	平成24年11月8日(2012.11.8)
審査請求日	平成26年9月25日(2014.9.25)
審判番号	不服2016-8827(P2016-8827/J1)
審判請求日	平成28年6月14日(2016.6.14)
(31)優先権主張番号	13/099,260
(32)優先日	平成23年5月2日(2011.5.2)
(33)優先権主張国	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　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】デバイス機能へのアプリケーションの結び付け

(57)【特許請求の範囲】
【請求項１】
コンピュータデバイスのオペレーティングシステムにおける方法であって、
前記コンピュータデバイスにインストールされているハードウェアデバイスの複数の機能のうちの第１の機能にアクセスするリクエストをアプリケーションから受け取るステップと、
前記オペレーティングシステムによって、前記アプリケーションが前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されているとデバイス許可記録において特定されるかどうかを確認するステップと、
前記アプリケーションが前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されていると前記デバイス許可記録が示す場合は、前記アプリケーションが前記ハードウェアデバイスの前記第１の機能にアクセスすることを可能にし、前記アプリケーションが前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されていると前記デバイス許可記録が示さない場合は、前記リクエストを拒絶するステップと
を有し、
前記デバイス許可記録は、前記オペレーティングシステムの一部分として含まれており、前記複数の機能の夫々について機能識別子を保持し、異なる承諾タイプが異なる機能識別子と関連付けられ、夫々の機能識別子は、前記ハードウェアデバイスの機能群に対応し、夫々の機能識別子について、当該機能識別子と関連付けられている承諾タイプは、もしあれば、前記アプリケーションが前記機能群にアクセスするために必要とされる承諾のタ

イプを示す、方法。
【請求項２】
前記確認するステップは、前記アプリケーションの識別子を取得し、該アプリケーションの識別子が前記ハードウェアデバイスの前記第１の機能に関連付けられるように前記デバイス許可記録において含まれるかどうかを確認する、
請求項１に記載の方法。
【請求項３】
前記リクエストは、前記ハードウェアデバイスの前記第１の機能を特定するデバイスインターフェースクラスにアクセスするリクエストを有する、
請求項１に記載の方法。
【請求項４】
前記リクエストは、特定のベンダーからハードウェアデバイスにアクセスするリクエストを有し、前記アクセスすることを可能にするステップは、前記アプリケーションが前記特定のベンダーから前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されていることを前記デバイス許可記録が示す場合にのみ、前記アプリケーションが前記ハードウェアデバイスの前記第１の機能にアクセスすることを可能にする、
請求項１に記載の方法。
【請求項５】
前記デバイス許可記録は、夫々の機能識別子について、前記機能群にアクセスすることを許可されている１又はそれ以上のアプリケーション識別子の関連リストを含み、
当該方法は、新しいハードウェアデバイスの前記コンピュータデバイスにおけるインストールの間、追加の機能識別子と、該追加の機能識別子に関連付けられる１又はそれ以上のアプリケーション識別子の追加のリストとを加えるステップを更に有する、
請求項１に記載の方法。
【請求項６】
プロセッサと、複数の命令を記憶したコンピュータ可読媒体とを有し、
前記複数の命令は、前記プロセッサによって実行される場合に、該プロセッサに、オペレーティングシステムにおいて、
ハードウェアデバイスに関連するインストールデータを取得する動作と、
前記インストールデータから、前記ハードウェアデバイスの複数の機能のうちの第１の機能にアクセスすることを許可されるアプリケーションの識別子と、前記複数の機能の夫々についての許可情報とを特定する動作と、
前記オペレーティングシステムの一部分として含まれているデバイス許可記録において、更なるユーザ承認なしで前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されるものとして前記アプリケーションの識別子を格納するとともに、前記許可情報を格納する動作と
を実行させ、
前記デバイス許可記録は、前記複数の機能の夫々について機能識別子を保持し、異なる承諾タイプが異なる機能識別子と関連付けられ、夫々の機能識別子は、前記ハードウェアデバイスの機能群に対応し、夫々の機能識別子について、当該機能識別子と関連付けられている承諾タイプは、もしあれば、前記アプリケーションが前記機能群にアクセスするために必要とされる承諾のタイプを示し、前記許可情報は、前記デバイス許可記録に対してなされるべき変更を特定する、コンピュータデバイス。
【請求項７】
前記複数の命令は、更に、前記プロセッサに、前記コンピュータデバイスにおける前記ハードウェアデバイスのインストールの間に前記特定する動作及び前記格納する動作を実行させる、
請求項６に記載のコンピュータデバイス。
【請求項８】
前記複数の命令は、更に、前記プロセッサに、前記オペレーティングシステムにおいて

、
前記ハードウェアデバイスに関連する更新データを取得する動作と、
前記更新データから、前記ハードウェアデバイスに前記第１の機能にアクセスすることを許可される追加のアプリケーションの識別子を特定する動作と、
前記ハードウェアデバイスの前記第１の機能にアクセスすることを許可されるように前記デバイス許可記録において前記追加のアプリケーションの識別子を格納する動作と
を実行させる、請求項６に記載のコンピュータデバイス。
【請求項９】
前記デバイス許可記録は、夫々の機能識別子の夫々について、前記機能群にアクセスすることを許可される１又はそれ以上のアプリケーション識別子の関連リストを含み、
前記アプリケーションの識別子を格納する動作は、前記ハードウェアデバイスの前記第１の機能に関連付けられるアプリケーション識別子を前記１又はそれ以上のアプリケーション識別子のリストに加えることを含む、
請求項６に記載のコンピュータデバイス。
【請求項１０】
前記ハードウェアデバイスの前記第１の機能にアクセスすることを示す承諾タイプに関連付けられる前記ハードウェアデバイスの前記第１の機能は、アプリケーション識別子のリストにおいて特定される特権を持ったアプリケーションにのみ許可され、前記ハードウェアデバイスの第２の機能にアクセスすることを示す承諾タイプに関連付けられる前記ハードウェアデバイスの前記第２の機能は、どのアプリケーションが前記ハードウェアデバイスの前記第２の機能へのアクセスをリクエストしているのかにかかわらず許可される、
請求項６に記載のコンピュータデバイス。
【発明の詳細な説明】
【背景技術】
【０００１】
コンピュータは、通常、プログラムが、記憶デバイス、カメラ、マイクロホン、プリンタ等のような様々なハードウェアデバイスにアクセスすることを可能にする。利用可能なそのようなハードウェアデバイスを有することは、ユーザが望む機能性をプログラムが提供することを可能にする一方、異なるプログラムによるそのようなハードウェアデバイスへのアクセスを制御することは問題がある。そのような問題の１つは、ユーザは、プログラムがハードウェアデバイスにアクセスするために彼らの承認を求められるが、そのようなプロンプトはユーザに説明するのが難しい点である。例えば、ユーザに承認を求める場合に、特定のハードウェアデバイスへのアクセスがどのようなものであるのか及び、アクセスを許可する意味合いがどのようなものであるのかを正確にユーザに説明することは困難でありうる。これは、ユーザ経験を混乱させて、コンピュータの使いやすさを減じる結果をもたらしうる。
【０００２】
更に、ユーザは、サポートされる場合に、自身の既存のコンピュータ設定に新しいハードウェアデバイスを追加することがある。そのような新しいハードウェアデバイスの追加は、既知の可能なハードウェアデバイス及びそれらの機能のリストが常に利用可能であるとしばしば推測されるので、プログラムがハードウェアデバイスにアクセスすることを可能にする従来アプローチを複雑にする。
【発明の概要】
【課題を解決するための手段】
【０００３】
この項目は、詳細な説明において以下で更に記載される簡略化された形において概念の選択を導入するよう設けられている。この項目は、請求対象の重要な特徴又は必須の特徴を特定するよう意図されず、且つ、請求対象の適用範囲を制限するために使用されるよう意図されない。
【０００４】

１又はそれ以上の態様に従って、コンピュータデバイスにインストールされているハードウェアデバイスの機能にアクセスするリクエストがアプリケーションから受信される。コンピュータデバイスによって、アプリケーションがハードウェアデバイスの機能にアクセスすることを許可されているとデバイス許可記録において特定されるかどうかに関して、確認がなされる。アプリケーションがハードウェアデバイスの機能にアクセスすることを許可されているとデバイス許可記録が示す場合は、アプリケーションはハードウェアデバイスの機能にアクセスすることを可能にされ、そうでない場合は、アプリケーションからのリクエストは拒絶される。

【０００５】

１又はそれ以上の態様に従って、ハードウェアデバイスに関連するインストールデータが取得される。ハードウェアデバイスの機能にアクセスすることを許可されるアプリケーションの識別子は、インストールデータから特定される。アプリケーションの識別子は、更なるユーザ承諾なしでハードウェアデバイスの機能にアクセスすることを許可されるようにデバイス許可記録に格納される。

【図面の簡単な説明】

【０００６】

【図１】１又はそれ以上の実施形態に従ってデバイス機能へのアプリケーションの結び付けを実施するコンピュータデバイスの例を表すブロック図である。

【図２】１又はそれ以上の実施形態に従ってデバイス機能へのアプリケーションの結び付けを実施するシステムの例を表すブロック図である。

【図３】１又はそれ以上の実施形態に従ってデバイス許可記録を変更する処理の例を表すフローチャートである。

【図４】１又はそれ以上の実施形態に従ってハードウェアデバイスの機能にアクセスするリクエストに応答する処理の例を表すフローチャートである。

【図５】１又はそれ以上の実施形態に従ってデバイス機能へのアプリケーションの結び付けを実施するよう構成され得るコンピュータデバイスの例を表す。

【発明を実施するための形態】

【０００７】

同じ参照符号は、図面の全体を通して、同じ特徴を参照するために用いられる。

【０００８】

デバイス機能へのアプリケーションの結び付けがここで論じられる。コンピュータデバイスは、種々のハードウェアを自身にインストールされ得、それら種々のハードウェアデバイスは、様々な機能を有することができる。デバイス許可記録が保持され、これは、どのアプリケーションがコンピュータデバイスのどのハードウェアデバイスのどの機能にアクセスすることを許可されるのかを示す。このデバイス許可記録は動的であり、どのアプリケーションがコンピュータデバイスのどのハードウェアデバイスのどの機能にアクセスすることを許可されるのかを示す様々なユーザ入力に応答して時間にわたって変化する。幾つかの実施形態は、固定された組のデバイス許可記録を有し、一方、他の実施形態は、新しい、これまで知られていなかったハードウェアデバイスがコンピュータデバイスに加えられる場合に新しい記録が作られることを可能にする拡張可能な組のデバイス許可記録をサポートする。コンピュータデバイスで実行されるアプリケーションは、そのコンピュータデバイスにインストールされるハードウェアデバイスの特定の機能へのアクセスをリクエストすることができる。そのようなリクエストに応答して、デバイスブローカーは、アプリケーションが特定のハードウェアデバイスの特定の機能にアクセスすることを許可されるかどうかを決定するよう、デバイス許可記録を確認する。アプリケーションは、アプリケーションがその特定のハードウェアデバイスのその特定の機能にアクセスすることを許可されることをデバイス許可記録が示す場合に、そうすることを可能にされ、そうでない場合は、アプリケーションは、そのハードウェアデバイスにアクセスすることを認められない。

【０００９】

ここでは、対称キー暗号化、公衆キー暗号化、及び公衆／プライベートキー対が参照される。たとえそのようなキー暗号化が当業者によく知られているとしても、そのような暗号化の概要は読者の助けとなるようここに含まれる。公衆キー暗号化において、エンティティ（例えば、ユーザ、ハードウェア又はソフトウェアコンポーネント、デバイス、ドメイン、等）は、それと公衆／プライベートキー対を関連付けている。公衆キーは、公に利用可能にされ得るが、エンティティは、プライベートキーを秘密にしたままとする。プライベートキーによらないと、公衆キーを用いて暗号化されているデータを解読することは、計算上非常に困難である。故に、データは、公衆キーを有する何らかのエンティティによって暗号化され、対応するプライベートキーを有するエンティティによってのみ解読され得る。更に、データのためのデジタル署名は、データ及びプライベートキーを用いることによって生成され得る。プライベートキーによらないと、公衆キーを用いて照合され得る署名を生成することは、計算上非常に困難である。公衆キーを有する如何なるエンティティも、公衆キー、署名、及びに署名されたデータに関して適切なデジタル署名照合を実行することによってデジタル署名を照合するために公衆キーを用いることができる。

【００１０】

対称キー暗号化において、他方で、共有キー（対象キーとも呼ばれる。）は２つのエンティティによって知られ、それらによって秘密にされる。共有キーを有する如何なるエンティティも、通常、その共有キーにより暗号化されたデータを解読することができる。共有キーによらないと、共有キーにより暗号化されているデータを解読することは、計算上非常に困難である。故に、２つのエンティティが両方とも共有キーを知っている場合に、夫々は、他方によって解読可能なデータを暗号化することができるが、他方のエンティティが共有キーを知らない場合は、その他方のエンティティはデータを解読することができない。同様に、共有キーを有するエンティティは、同じエンティティによって解読可能なデータを暗号化することができるが、他のエンティティは、その他のエンティティが共有キーを知らない場合は、データを解読することができない。更に、デジタル署名は、例えばキーハッシュメッセージ認証コードメカニズムを用いるような対称キー暗号化に基づき、生成され得る。共有キーを有する如何なるエンティティも、デジタル署名を生成して照合することができる。例えば、信頼される第三機関は、特定のエンティティの識別に基づき対称キーを生成することができ、次いで、その特定のエンティティのために（例えば、対称キーを用いてデータを暗号化又は解読することによって）デジタル署名の生成及び照合の両方を行うことができる。

【００１１】

図１は、１又はそれ以上の実施形態に従って、デバイス機能へのアプリケーションの結び付けを実施するコンピュータデバイス１００の例を表すブロック図である。コンピュータデバイス１００は、様々な異なるタイプのデバイスであってよい。例えば、コンピュータデバイス１００は、デスクトップコンピュータ、ネットブック若しくはラップトップコンピュータ、ノートパッド若しくはタブレットコンピュータ、モバイル局、エンターテイメント機器、表示デバイスへ通信上結合されるセットトップボックス、テレビ受像機若しくは他の表示デバイス、携帯電話若しくは他の無線電話、ゲーム機、自動車コンピュータ、等であってよい。

【００１２】

コンピュータデバイス１００は、オペレーティングシステム１０２と、１又はそれ以上（ｍ）のアプリケーション１０４（１），・・・，１０４（ｍ）と、１又はそれ以上（ｎ）のハードウェアデバイス１０６（１），・・・，１０６（ｎ）とを有する。アプリケーション１０４は夫々、ゲーム若しくは他のエンターテイメントアプリケーション、ユーティリティアプリケーション、プロダクティビティアプリケーション（例えば、ワード処理又は表計算アプリケーション）、リファレンスアプリケーション、通信アプリケーション、等のような、様々な異なるタイプのアプリケーションのいずれかであってもよい。アプリケーション１０４は、コンピュータデバイス１００によって、ローカルソースから取得され（例えば、ローカルディスク又はフラッシュメモリデバイスからインストールされ）

、且つ／あるいは、リモートソースから取得され（例えば、インターネット、セルラー又は他の無線ネットワークのようなネットワークを介して他のデバイスから取得され）得る。

【００１３】

ハードウェアデバイス１０６は夫々、オペレーティングシステム１０２にアクセス可能な様々な異なるタイプのデバイス又はコンポーネントのいずれかであってよい。例えば、ハードウェアデバイス１０６は、カメラ、マイクロホン、プリンタ、記憶デバイス（例えば、フラッシュメモリ、加入者識別モジュール（ＳＩＭ）カード、等）、モバイルブロードバンドチップセット又はカード、等であってよい。ハードウェアデバイス１０６は、コンピュータデバイス１００の部分として含まれて（例えば、コンピュータデバイス１００のプロセッサ及びメモリと同じ筐体に含まれて）、且つ／あるいは、（例えば、有線又は無線接続を介して）コンピュータデバイス１００へ結合される別個のデバイスであってよい。ハードウェアデバイス１０６は、新しいハードウェアデバイスをコンピュータデバイス１００と同じ物理的筐体に物理的に加えることによって、又は新しいハードウェアデバイスをコンピュータデバイス１００へ（例えば、有線及び／又は無線接続を用いて）別なふうに結合して、コンピュータデバイス１００に（それまでインストールされていない場合に）インストールされる関連するソフトウェア及び／又はファームウェアを有することによって、コンピュータデバイス１００にインストールされる。その関連するソフトウェア及び／又はファームウェアは、デバイスドライバとも呼ばれ、関連するハードウェアデバイスと如何にして通信すべきかを理解し、コンピュータデバイス１００における他のアプリケーション、コンポーネント、又はモジュールがその関連するハードウェアデバイスにアクセスすることを可能にする。デバイスドライバによって提供される正確な機能性は、コンピュータデバイス１００が作られた時にオペレーティングシステム１０２に知られても又は知られていなくてもよい。

【００１４】

オペレーティングシステム１０２は、コンピュータデバイス１００で実行されるアプリケーション１０４を管理するとともに、アプリケーション１０４によるハードウェアデバイス１０６へのアクセスを管理する。オペレーティングシステム１０２は、デバイスブローカー１１２と、デバイス許可記録１１４とを有する。ハードウェアデバイス１０６にアクセスするために、アプリケーション１０４は、オペレーティングシステム１０２からそのハードウェアデバイス１０６へのアクセスをリクエストする。デバイスブローカー１１２は、リクエスト元のアプリケーション１０４がそのハードウェアデバイス１０６にアクセスすることを許可されているかどうかを決定するよう、デバイス許可記録１１４を確認する。リクエスト元のアプリケーション１０４がそのハードウェアデバイス１０６にアクセスすることを許可されていることをデバイス許可記録１１４が示す場合は、デバイスブローカー１１２は、リクエスト元のアプリケーション１０４がそのハードウェアデバイス１０６にアクセスすることを可能にする。しかし、リクエスト元のアプリケーション１０４がそのハードウェアデバイス１０６にアクセスすることを許可されていないとデバイス許可記録１１４が示す場合は、デバイスブローカー１１２は、リクエスト元のアプリケーション１０４がそのハードウェアデバイス１０６にアクセスすることを妨げる（又は別なふうに認めない）。

【００１５】

図２は、１又はそれ以上の実施形態に従ってデバイス機能へのアプリケーションの結び付けを実施するシステム２００の例を表すブロック図である。システム２００は、図１のコンピュータデバイス１００のようなコンピュータデバイスにおいて実施される。システム２００は、図１のアプリケーション１０４であってよいアプリケーション２０２を有する。アプリケーション２０２は、システム２００のデバイス及び／又は他のリソース（例えば、メモリ、他のアプリケーション、等）にアクセスするアプリケーション２０２の能力が制限される形で実行され得る。コンピュータデバイスのオペレーティングシステム（又は代替的に他のソフトウェア若しくはファームウェア）は、アプリケーション２０２が

、アプリケーション２０２に割り当てられた又は別なふうに利用可能にされたコンピュータデバイスのメモリにアクセスすることを可能にするが、アプリケーション２０２がコンピュータデバイスの他のメモリ及び／又はコンピュータデバイスで実行される他のアプリケーションにアクセスすることを妨げる。これは、コンピュータデバイスで実行される他のアプリケーションがアプリケーション２０２によって干渉されないようにする同時に、アプリケーション２０２がコンピュータデバイスで実行される他のアプリケーションによって干渉されないようにする。１又はそれ以上の実施形態において、アプリケーション２０２は、サンドボックス（サンドボックス２０４として破線により示される。）においてアプリケーション２０２を実行することによって、制限された形で実行される。単一のアプリケーション２０２がシステム２００にインストールされているが、複数のアプリケーションが同時にシステム２００において実行され得る点に留意されたい（夫々のアプリケーションは、通常、それ自身のサンドボックスにおいて実行される。）。

【００１６】

コンピュータデバイスにより実施されるシステム２００にインストールされるハードウェアデバイスは、様々な機能を有することができ、その中の１又はそれ以上は、一群又は分類の機能にまとめられ得る。ハードウェアデバイスの機能は、ハードウェアデバイスによって提供される又は別なふうにサポート若しくは許可される機能性及び／又は動作をいう。ハードウェアデバイスの特定の機能及びそれらがまとめられる方法は、ハードウェアデバイスの設計者若しくはベンダーによって、又は代替的に他のコンポーネント若しくはエンティティによって（例えば、コンピュータデバイスにおけるオペレーティングシステムの設計者若しくはベンダーによって）、定義され得る。例えば、プリンタデバイスは、（アプリケーションが印刷のためにプリンタへデータを送信することを可能にする）印刷機能、及び（アプリケーションがプリントヘッドを再校正すること、インク又はトナーのレベルを取得すること、印刷に関する統計値を取得すること、等を可能にする）管理機能を有してよい。他の例として、モバイルブロードバンドデバイスは、（アプリケーションがテキストメッセージ、マルチメディアメッセージ、ウェブページ、等のようなデータをモバイルブロードバンド接続を介して送信及び／又は受信することを可能にする）通信機能、（アプリケーションが特定のネットワークにおける使用のためにモバイルブロードバンドデバイスを提供又はセットアップすることを可能にする）プロビショニング機能、及び（アプリケーションが特定のネットワークによる使用のためにコンフィグレーション設定を調整すること、特定のネットワーク上での使用に関する情報（例えば、送信及び／又は受信されるデータの量）を取得すること、等を可能にする）管理機能、等を有してよい。コンピュータデバイスにより実施されるシステム２００へ結合されるハードウェアデバイスの機能性は、アプリケーション２０２以外のシステムのオペレーティングシステム又は他のコンポーネントに知られる必要はない（なお、代替的に、知られていてもよい）。

【００１７】

ハードウェアデバイスの機能の特定の分類にアクセスするために、アプリケーション２０２は、所望の機能にアクセスするようデバイスブローカー２０６へリクエストを発する。

デバイスブローカー２０６は、例えば、図１のデバイスブローカー１１２であってよい。アプリケーション２０２は、様々な異なる方法においてデバイスブローカー２０６へリクエストを発する。１又はそれ以上の実施形態において、アプリケーション２０２は、アプリケーション２０２がその場合に所望の機能にアクセスするために使用することができるハードウェアデバイスの所望の機能へのハンドル（又はそれらの他の識別子）を公開又は作成するリクエストを発する。リクエストは、例えば、デバイスインターフェースクラスへのハンドルを公開するリクエストであってよい。リクエストに応答して、デバイスブローカー２０６は、アプリケーション２０２がリクエストされる機能にアクセスすることを許可されているかどうかを決定するよう、デバイス許可記録２０８（図１のデバイス許可記録１１４であってよい。）を確認する。デバイスブローカー２０６は、アプリケーション２０２がリクエストされる機能にアクセスすることを許可されているとデバイス許可記

録２０８が示す場合にのみ、リクエストされる機能へのリクエストされるハンドル（又は他の識別子）を返す。リクエストされる機能へのこのハンドル（又は他の識別子）は、ハードウェアデバイスに関連する１又はそれ以上のデバイスドライバ（例えば、ソフトウェア又はファームウェア）の識別、ハードウェアデバイスに関連する１又はそれ以上のデバイスドライバの１又はそれ以上のアプリケーションプログラミングインターフェース（ＡＰＩ）の識別、等のように、様々な形を取ることができる。１又はそれ以上の実施形態において、デバイスブローカー２０６（又は、少なくとも、デバイス許可記録２０８を確認するデバイスブローカー２０６の部分）は、アプリケーション２０２がデバイス許可記録２０８を確認するデバイスブローカー２０６に干渉することを妨げるよう、システム２００の信頼されるコンポーネント（例えば、オペレーティングシステムの信頼されるコアの部分又は他の信頼される部分）として実施される。

【００１８】

デバイス許可記録２０８は、機能識別子２１４と、関連する承諾タイプ２１６とを含む。コンピュータデバイスにより実施されるシステム２００にインストールされるハードウェアデバイスの機能の各群又は分類は、対応する機能識別子２１４を有する。各機能識別子２１４は、必要に応じて、アプリケーションがその機能識別子２１４によって特定される分類の機能にアクセスするために、どのような承諾が必要とされるかを示す関連する承諾タイプ２１６を有する。よって、同じハードウェアデバイスのための異なる分類の機能は、アプリケーションがそれらの異なる分類の機能にアクセスするために必要とされる異なるタイプの承諾を示す異なる関連する承諾タイプを有することができる。アプリケーションが機能識別子２１４によって特定される分類の機能にアクセスするために必要とされる承諾のタイプに依存して、機能識別子はまた、関連するアプリケーション識別子（ＩＤ）リスト２１８を有してよい。各アプリケーションＩＤリスト２１８は、関連する機能識別子２１４によって特定される機能にアクセスすることを許可される１又はそれ以上のアプリケーション識別子のリストである。

【００１９】

１又はそれ以上の実施形態において、各機能識別子２１４は、特定のタイプのハードウェアデバイスの特定の分類又は群の機能を特定するデバイスインターフェースクラスである。例えば、機能識別子２１４は、カメラタイプのデバイスの画像捕捉機能の識別子、カメラタイプのデバイスのカメラ設定機能の識別子、モバイルブロードバンドタイプのデバイスの通信機能の識別子、モバイルブロードバンドタイプのデバイスのプロビショニング機能の識別子、等であってよい。同じタイプの複数の異なるハードウェアデバイス（例えば、複数の異なるカメラ）は、同じデバイスインターフェースクラスの部分として含まれ得る。デバイスインターフェースクラスは、オペレーティングシステム（例えば、図１のオペレーティングシステム１０２）によって若しくはその部分として、及び／又は他のエンティティ（例えば、ハードウェアデバイス設計者若しくはベンダー）によって、定義され得る。

【００２０】

システム２００の動作の間、コンピュータデバイスにインストールされる特定のハードウェアデバイスに関連するデバイスドライバは、その特定のハードウェアデバイスのためのデバイスインターフェースクラスのインスタンスを、コンピュータデバイスのオペレーティングシステムに登録する。オペレーティングシステムは、デバイスインターフェースクラスのそのインスタンスを特定のハードウェアデバイスに関連付け、如何にしてアプリケーション（例えば、アプリケーション２０２）がそのインスタンスの機能にアクセスすることができるかのインジケーションを保持する。１又はそれ以上の実施形態において、このインジケーションは、デバイスのインスタンスのためのハンドルである。代替的に、このインジケーションは、機能のポインタ、リンク、又は他の識別子のような他の形で実施され得る。ハンドルがここでは論じられているが、如何にしてアプリケーションがインスタンスの機能にアクセスすることができるのかの他のインジケーションがハンドルと同じように使用され得る点に留意されたい。その特定のハードウェアデバイスの機能にアク

セスするために、アプリケーション２０２は、デバイスブローカー２０６から、そのインスタンスのためのハンドルをリクエストする。デバイスブローカー２０６は、アプリケーション２０２が特定のデバイスインターフェースクラスにアクセスすることを許可されることをデバイス許可記録２０８が示す場合にのみ、その特定のデバイスインターフェースクラスのインスタンスのためのハンドルを返す。

【００２１】

代替的に、デバイスインターフェースクラスよりむしろ、機能識別子２１４は、他の方法においてハードウェアデバイス又はハードウェアデバイスのタイプを特定することができる。１又はそれ以上の実施形態において、デバイスインターフェースクラスよりむしろ、ハードウェアデバイスの他のカテゴリ又はグルーピングが保持され、そのようなカテゴリ又はグルーピングは夫々、承諾タイプと関連付けられる。それらのカテゴリ又はグルーピングは、同じ分配者によって提供される又は同じベンダーによって製造されるデバイスの集まり、特定の会社、グループ若しくは他のエンティティによって評価又は承認されたデバイスの集まり、等のように、種々の方法において定義され得る。他の実施形態において、デバイスインターフェースクラスよりむしろ、個々のハードウェアデバイスが夫々、承諾タイプ２１６と関連付けられ得る。個々のハードウェアデバイスは、例えば、ハードウェアデバイスの分配者又はベンダーによって割り当てられるモデル番号又は他の識別子によって、ハードウェアデバイスに関連するデバイスドライバの識別子によって、等、種々の方法において特定され得る。

【００２２】

よって、一例として、機能識別子２１４は、特定のハードウェアデバイスの特定のデバイスインターフェースのインスタンスを特定するハードウェアインスタンスＩＤであってよい。他の例として、機能識別子２１４は、特定のハードウェアデバイスのモデルＩＤであってよく、このモデルＩＤは、特定のハードウェアデイバスの様々な機能を特定する（例えば、ベンダーの製造識別子、分類識別子、改訂識別子、それらの組み合わせ、等）。

【００２３】

各承諾タイプ２１６は、必要に応じて、アプリケーションが関連する機能識別子２１４によって特定される分類の機能にアクセスするために、どのような承諾が必要とされるのかを示す。様々な異なるタイプの承諾が承諾タイプ２１６において特定され得る。１又はそれ以上の実施形態において、各承諾タイプ２１６は、許可、拒絶、プロンプト、又は特権付与の中の１以上である。許可承諾タイプは、関連する機能へのアクセスが（ハードウェアデバイスへのアクセスするリクエストするアプリケーションと無関係に）許可されることを示す。拒絶承諾タイプは、関連する機能へのアクセスが（ハードウェアデバイスへのアクセスするリクエストするアプリケーションと無関係に）許可されないことを示す。プロンプト承諾タイプは、コンピュータデバイスにより実施されるシステム２００のユーザが、アプリケーションが関連する機能にアクセスするための承認を促されることを示す。特権付与承諾タイプは、関連する機能へのアクセスが特権を持ったアプリケーションにのみ許可されることを示す。

【００２４】

特定の機能識別子２１４において示される承諾タイプ２１６が特権付与承諾タイプである場合に、デバイス許可記録２０８はまた、機能識別子２１４に関連付けられたアプリケーションＩＤリスト２１８を含む。特定の機能識別子２１４において示される承諾タイプ２１６が特権付与承諾タイプ以外である（例えば、許可、拒絶、又はプロンプト承諾タイプである）場合は、その特定の機能識別２１４に関連付けられたアプリケーションＩＤリスト２１８はデバイス許可記録２０８に含まれる必要がない。各アプリケーションＩＤリスト２１８は、関連する機能識別子２１４によって特定される機能にアクセスすることを許可又は承認される１又はそれ以上のアプリケーション識別子（例えば、特権を持ったアプリケーション）のリストである。機能のための承諾タイプが特権付与承諾タイプであり、且つ、アプリケーション２０２が、それがアクセスをリクエストするハードウェアデバイスの機能の機能識別子２１４と関連付けられたアプリケーションＩＤリストに含まれな

い場合は、アプリケーション２０２は、ハードウェアデバイスのそれらの機能へのアクセスを拒絶される。代替的に、機能のための承諾タイプが特権付与である場合は、特権付与承諾タイプのインジケーションは、機能識別子２１４と関連付けられる承諾タイプ２１６として含まれる必要はない。むしろ、機能識別子２１４と関連付けられるアプリケーションＩＤリスト２１８の存在により、機能識別子２１４と関連付けられる承諾タイプは特権付与承諾タイプであることが暗に示され得る。

【００２５】

ハードウェアデバイス機能（又はハードウェアのタイプ）と、それらの機能にアクセスすることを許可されるアプリケーション識別子との関連付けは、ハードウェアデバイスへのアプリケーションの結び付けとも呼ばれる。アプリケーション２０２の識別子が、機能識別子２１４と関連付けられるアプリケーションＩＤリストに含まれる場合は、アプリケーション２０２は、関連する機能識別子２１４によって特定される機能と結び付けられる。なお、アプリケーション２０２の識別子が機能識別子２１４と関連付けられるアプリケーションＩＤリストに含まれない場合は、アプリケーション２０２は、関連する機能識別子２１４によって特定される機能と結び付けられない。

【００２６】

アプリケーション２０２のためのアプリケーション識別子は、様々な異なる方法において生成され得る。１又はそれ以上の実施形態において、アプリケーション２０２のためのアプリケーション識別子は、暗号化ハッシュ機能をアプリケーション２０２及び／又はアプリケーション２０２のメタデータに適用してハッシュ値を生成することによって、生成される。様々な異なる暗号化ハッシュ関数のいずれかが用いられ得る。例えば、ＳＨＡ－１（Secure Hash Algorithm 1）又はＳＨＡ－２、ワールプール（Whirlpool）、タイガー（Tiger）、ＦＳＢ（First Syndrome-based hash functions）、等がある。デバイスブローカー２０６、又はデバイスブローカー２０６によって信頼される他のコンポーネント若しくはモジュールは、アプリケーション２０２のためのハッシュ値を生成することができる。アプリケーション２０２のためのハッシュ値は、種々の時点で生成されてよく、例えば、アプリケーション２０２のためのハッシュ値は、前もって生成され、デバイスブローカー２０６へ供給される（例えば、アプリケーション２０２がコンピュータデバイスにより実施されるシステム２００にインストールされる時、アプリケーション２０２が実行を開始する時、等に、生成される。）。アプリケーション２０２のためのハッシュ値が前もって生成される状況において、ハッシュ値が生成された後に変更されないように（あるいは、ハッシュ値の変更が検出可能であるように）注意が払われる。例えば、ハッシュ値は、デバイスブローカー２０６によって信頼されるエンティティによってデジタル署名され得る。代替的に、アプリケーション２０２のためのハッシュ値は、他の時点で、例えば、所望のハードウェアデバイスにアクセスするためのアプリケーション２０２からのリクエストに応答して、生成され得る。

【００２７】

代替的に、アプリケーション２０２のためのアプリケーション識別子は、他の方法において生成され得る。例えば、識別子は、（例えば、アプリケーション２０２の開発者又は分配者によって）アプリケーション２０２へ割り当てられ、信頼されるエンティティ（デバイスブローカー２０６によって信頼されるコンポーネント、モジュール、デバイス、又の他のエンティティ）によってデジタル署名され得る。デバイスブローカー２０６、又はデバイスブローカー２０６によって信頼される他のコンポーネント若しくはモジュールは、アプリケーション２０２のアプリケーション識別子がデバイスブローカー２０６によって信頼され得ることを確かめるよう、アプリケーション２０２のためのデジタル署名を照合することができる。デジタル署名は、所望のハードウェアデバイスにアクセスするためのアプリケーション２０２からのリクエストに応答して、又は上述されたようなアプリケーション２０２のためのハッシュ値の生成と同じ他の時点で、照合され得る。

【００２８】

デバイス許可記録２０８は、様々な時点で生成され、変更され得る。１又はそれ以上の

実施形態において、デバイスブローカー２０６を含むオペレーティングシステム（例えば、図１のオペレーティングシステム１０２）は、初期デバイス許可記録２０８を有する。追加のデバイスインターフェースクラス及び関連する許可エントリは、新しいハードウェアがコンピュータデバイスにより実施されるシステム２００にインストールされる場合に、デバイス許可記録２０８に加えられ得る。デバイスインターフェースクラス及び関連する許可エントリは、システム２００の更新の間にも追加、除去、及び／又は変更され得る。よって、特定のハードウェアデバイス及び／又はハードウェアデバイスの特定の機能（並びにそれらの識別子）は、コンピュータデバイスが作成又は構築される場合に、コンピュータデバイスにより実施されるシステム２００のオペレーティングシステムに知られる必要はなく、むしろ、最後の時点でコンピュータデバイスに加えられ得る。更に、ハードウェアデバイスの特定の機能及びそれらの識別子は、コンピュータデバイスにより実施されるシステム２００のオペレーティングシステムに定義されるか、又はそのオペレーティングシステムによって知られるそれらの機能性である必要はない。むしろ、特定の機能と関連付けられる機能識別子がデバイス許可記録２０８に加えられ、アプリケーション２０２に知られる機能であってよい。アプリケーション２０２は、それらの機能がどのようなものであるかを知るオペレーティングシステム（及びシステム２００の他のコンポーネント）がない場合に、（デバイス許可記録２０８に基づき）それらの機能にアクセスすることを可能にされ得る。

【００２９】

１又はそれ以上の実施形態において、システム２００は、デバイスインストールファイル及びデータ２３２を受信し又は別なふうに取得するインストールマネージャ２３０を有する。デバイスインストールファイル及びデータ２３２は、コンピュータデバイスにより実施されるシステム２００においてハードウェアデバイスのためのデバイスドライバとしてインストールされる１又はそれ以上のファイル及び／又はデータを含む。デバイスインストールファイル及びデータ２３２は、新しいハードウェアデバイスがコンピュータデバイスにより実施されるシステム２００にインストールされる場合に、インストールマネージャ２３０によって取得される。例えば、デバイスインストールファイル及びデータ２３２は、新しいハードウェアデバイスがコンピュータデバイスにより実施されるシステム２００にインストールされる場合に、リモートサービスから自動的にダウンロードされ得る。デバイスインストールファイル及びデータ２３２は、デバイスドライバ、セットアップ情報ファイル（例えば、ＩＮＦファイル）、デバイスドライバに関連するメタデータ、マニフェスト、等のように、様々な異なる形を取ることができる。

【００３０】

インストールマネージャ２３０は、デバイスインストールファイル及びデータ２３２において許可情報を特定し、その許可情報をデバイス許可記録２０８に加える。この許可情報は、デバイス許可記録２０８に対してなされるべき変更を特定する。例えば、この許可情報は、特定のデバイスインターフェースクラスのためのアプリケーションＩＤリストに加えられる（又はそれから除かれる）１以上の新しいアプリケーション識別子を含むことができる。他の例として、この許可情報は、記録２０８に加える１以上の新しいデバイスインターフェースクラス及び関連する許可エントリを含むことができる。更なる他の例として、この許可情報は、許可のタイプの変更を含むことができる（例えば、プロンプト承諾タイプから特権付与承諾タイプへの又はその逆の、特定のデバイスインターフェースクラスと関連付けられる承諾タイプ２１６の変更）。上述されたようなアプリケーション２０２のためのハッシュ値と同様に、生成された後に、デバイスインストールファイル及びデータ２３２が変更されないように（又は許可情報の変更が検出可能であるように）注意が払われる。例えば、許可情報は、インストールマネージャ２３０によって信頼されるエンティティによってデジタル署名され得る。

【００３１】

同様に、インストールマネージャ２３０はまた、デバイス更新ファイル及びデータ２３４を受信し又は別なふうに取得することができる。デバイス更新ファイル及びデータ２３

４は、デバイスインストールファイル及びデータ２３２と同様であり、デバイス許可記録２０８に対してなされるべき変更を特定する。しかし、デバイス更新ファイル及びデータ２３４は、コンピュータデバイスにより実施されるシステム２００に既にインストールされているハードウェアデバイスのためのデバイスドライバ及び／又は他のデータを更新するようインストールマネージャ２３０によって取得される。デバイス更新ファイル及びデータ２３４は、デバイスドライバ、セットアップ情報ファイル（例えば、ＩＮＦファイル）、デバイスドライバに関連するメタデータ、マニフェスト、等のように、様々な異なる形を取ることができる。デバイス更新ファイル及びデータ２３４は、インストールマネージャ２３０が、デバイスインストールファイル及びデータ２３２に含まれる許可情報と同様に、デバイス許可記録２０８に加える様々な許可情報を特定することができる。上述されたようなデバイスインストールファイル及びデータ２３２における許可情報と同様に、生成された後に、デバイス更新ファイル及びデータ２３４が変更されないように（又は許可情報の変更が検出可能であるように）注意が払われる。例えば、許可情報は、インストールマネージャ２３０によって信頼されるエンティティによってデジタル署名によってデジタル署名され得る。

【００３２】

デバイスインストールファイル及びデータ２３２（及び／又はデバイス更新ファイル及びデータ２３４）は、同じデバイスの異なる機能に加えられる異なるアプリケーションＩＤを有することができる点に留意されたい。アプリケーションは、ハードウェアデバイスの全ての機能へのアクセスを与えられる必要はない。例えば、インストール及び／又は更新データは、モバイルブロードバンドデバイスのプロビショニング機能を特定する機能識別子２１４に加えられる１つのアプリケーションＩＤと、モバイルブロードバンドデバイスの管理機能を特定する機能識別子２１４に加えられる他のアプリケーションＩＤとを特定することができる。

【００３３】

１又はそれ以上の実施形態において、コンピュータデバイスにより実施されるシステム２００にインストールされるハードウェアデバイスは、拡張マークアップ言語（ＸＭＬ）ファイルである関連するメタデータファイルと、ＩＮＦファイルである関連するセットアップ情報ファイルとを有する。同様に、１又はそれ以上の実施形態において、コンピュータデバイスにより実施されるシステム２００に既にインストールされており更新されるハードウェアデバイスは、関連するメタデータＸＭＬファイル及び／又はＩＮＦファイルを有することができる。ＩＮＦファイルは、インストールする特定のファイル及び、それらのファイルがコンピュータデバイスにおいてどこにインストールされるべきか、（例えば、オペレーティングシステムレジストリのようなオペレーティングシステム記憶において）必要とされる設定、等をインストールマネージャ２３０に示す。ＩＮＦファイルはまた、デバイスの機能にアクセスするための特定のデバイスインターフェースクラスを（例えば、デバイスインターフェースクラスが互いに区別されることを可能にするグローバル一意識別子（ＧＵＩＤ）又は他の識別子を用いて）特定するとともに、それらのデバイスインターフェースクラスの夫々と関連付けられる承諾タイプを特定する。メタデータＸＭＬファイルは、特許付与の承諾タイプを有するＩＮＦファイルにおいて特定される各デバイスインターフェースクラスについて、そのデバイスインターフェースクラスの機能にアクセスすることを許可される１又はそれ以上のアプリケーションＩＤを含む。なお、機能識別子、承諾タイプ、及び／又はアプリケーションＩＤリストは、メタデータＸＭＬ及びＩＮＦファイルよりむしろ、他の方法においてデバイスインストールファイル及びデータ２３２及び／又はデバイス更新ファイル及びデータ２３４に含まれ得る点に留意されたい。

【００３４】

また、デバイス許可記録２０８は、他の時点で、及び／又は他のイベントに応答して、変更され得る点に留意されたい。例えば、システム２００のユーザ又は管理者は、デバイス許可記録２０８に行う特定の変更を示す入力（例えば、特定の機能識別子と関連付けられる特定の承諾タイプを特定する入力、特定の機能識別子と関連付けられるアプリケーシ

ョンＩＤリストに加えられる特定のアプリケーションＩＤを特定する入力、等）を提供してよい。そのような入力は、システム２００の設定ユーザインターフェースにアクセスするシステム２００のユーザ又は管理者によって、アプリケーションが関連する機能にアクセスするための承認を促される場合に“許可”選択肢を選択するシステム２００のユーザによって（例えば、“許可”選択肢のユーザ選択に応答して、アプリケーションの識別子は、特定の機能識別子と関連付けられるアプリケーションＩＤリストに加えられ得る。）、等により、提供され得る。

【００３５】

１又はそれ以上の実施形態において、デバイス許可記録２０８は、どのコンポーネント又はモジュールが記録２０８を更新することを認められるかを制限する安全な方法で記憶される。例えば、デバイス許可記録２０８は、特定のコンポーネント又はモジュール（インストールマネージャ２３０の１又はそれ以上のモジュール、又デバイスブローカー２０６を含むオペレーティングシステムのモジュールのみ）によってのみ、例えば、様々な従来の信頼されるブート又は安全なブート技術を用いるような、任意に特定の時点で（例えば、コンピュータデバイスにより実施されるシステム２００をブーティングする処理の間）、変更され得る保護されたメモリに記憶され得る。他の例として、デバイス許可記録２０８は、（例えば、インストールマネージャ２３０、又はデバイスブローカー２０６によって信頼される他のエンティティによって）デジタル署名され、記録２０８におけるデジタル署名が照合される場合にのみデバイスブローカー２０６によって使用され得る。

【００３６】

デバイス許可記録２０８は、複数の機能識別子並びに関連する承諾タイプ及び／又はアプリケーションＩＤリストを含むテーブルとして、図２では表されている。テーブルとして表されているが、デバイス許可記録２０８は、様々な異なるデータ構造又は記憶技術を用いて実施され得る点に留意されたい。また、デバイス許可記録２０８は、複数の記憶又はテーブルに分けられ得る点にも留意されたい。例えば、デバイス許可記録２０８は２つの記憶を有してよく、１つの記憶は機能識別子２１４及び関連する承諾タイプ２１６を含み、他の記憶は機能識別子２１４及び関連するアプリケーションＩＤリスト２１８を含む。

【００３７】

更に、コンピュータデバイスにより実施されるシステム２００に知られるハードウェアデバイスのリストは静的である必要はない（が代替的に静的であってもよい）点に留意されたい。ハードウェアデバイスがコンピュータデバイスにより実施されるシステム２００に加えられる場合に、デバイス許可記録２０８は、アプリケーション２０２によるアクセスのためのその後の要求時に、どのようなタイプの承諾がコンピュータデバイスにより実施されるシステム２００に加えられるハードウェアデバイスの新しいインスタンスに加えられるべきかを適切に反映するよう管理される。ハードウェアデバイスの新しいインスタンスは、機能識別子２１４がデバイス許可記録２０８に既に含まれている機能を有するハードウェアデバイスをいう。例えば、１つの特定のカメラ（カメラの１つのインスタンス）は予め、コンピュータデバイスにより実施されるシステム２００へ結合されてよく、第２のカメラ（カメラの新しいインスタンス）は、コンピュータデバイスにインストールされてよい。カメラの機能のための機能識別子２１４は、この第２のカメラがコンピュータデバイスにインストールされる新しいカメラであるとしても、デバイス許可記録２０８に既に含まれ得る。

【００３８】

１又はそれ以上の実施形態において、デバイスブローカー２０６は、コンピュータデバイスにより実施されるシステム２００にインストールされるハードウェアデバイスの新しいインスタンスのための様々なポリシー又はルールの１又はそれ以上を適用する。例えば、デバイスブローカー２０６は、デバイス許可記録２０８において特定の機能識別子２１４によって特定される承諾のタイプが、いつハードウェアデバイスがインストールされたのかにかかわらず、その特定の機能識別子２１４によって特定される分類の機能にアクセ

スするようリクエストする全てのアプリケーションに適用可能であると決定することができる。他の例として、デバイスブローカー２０６は、ハードウェアデバイスの新しいインスタンスのために特定の機能識別子２１４によって特定される分類の機能へのアクセスが、適切な承諾がユーザから得られる（例えば、ユーザが、ハードウェアデバイスの新しいインスタンスがアクセスされるための承認を促されるか、又はハードウェアデバイスの新しいインスタンスが、コンピュータデバイスに既にインストールされているハードウェアデバイスの他のインスタンスと同じように扱われるための承諾を促される）まで拒絶されると決定することができる。代替的に、如何にして承諾がハードウェアデバイスの新しいインスタンスに適用されるべきかのより精細な決定が（例えば、特定の機能識別子２１４、又はアクセスがリクエストされている機能識別子２１４と関連付けられる特定の承諾タイプ２１６に基づき）なされてよい。

【００３９】

更に、１又はそれ以上の実施形態において、特定のアプリケーションは、特定のハードウェアデバイスの機能へのアクセスに制限される。そのような制限は、例えば、特定のベンダー（例えば、製造者、分配者、等）が、どのアプリケーションがそのベンダーのハードウェアデバイスの機能にアクセスすることができるのかを（他のベンダーからの他のハードウェアデバイスが同じ機能をサポートするかどうかにかかわらず）制限することを可能にする。そのような制限は、種々の方法において実施され得る。例えば、異なる機能識別子２１４が、（それらの異なる機能識別子によって特定される機能が同じであるとしても）異なるハードウェアデバイスについて使用され得る。他の例として、ハードウェアデバイスに関連するデータ（例えば、最初にオペレーティングシステムに含まれるデータ、デバイスインストールファイル及びデータ２３２におけるデータ、デバイス更新ファイル及びデータ２３４におけるデータ、等）は、特定のアプリケーションＩＤリストを有するアプリケーションによってアクセスされ得る（例えば、ハードウェアデバイスベンダー、ハードウェアデバイスモデル、等によって特定される）特定のハードウェアデバイスのインジケーションを含むことができる。それらのハードウェアデバイスのインジケーションは、例えば、それらのハードウェアデバイスのインジケーションをデバイス許可記録２０８において特定のアプリケーションＩＤと関連付けることによって、保持され得る。この例に従い、デバイスブローカー２０６は、アプリケーション２０２のアプリケーションＩＤが特定のハードウェアデバイスの機能の分類と関連付けられるアプリケーションＩＤリスト２１８に含まれる場合且つその特定のハードウェアデバイスがその機能の分類についてアプリケーションＩＤリスト２１８におけるアプリケーション２０２のアプリケーション２０２と関連付けられる場合にのみ、アプリケーション２０２がその機能の分類にアクセスすることを可能にすることができる。

【００４０】

図３は、１又はそれ以上の実施形態に従ってデバイス許可記録を変更する処理３００の例を表すフローチャートである。処理３００は、コンピュータデバイス、例えば、図１のコンピュータデバイス１００によって、実行され、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組み合わせにおいて実施され得る。処理３００は、動作の組として示され、様々な動作の操作を実行するために示された順序に制限されない。処理３００は、デバイス許可記録を変更する処理の例であり、デバイス許可記録の変更に関する更なる議論は、異なる図を参照してここに含まれる。

【００４１】

処理３００において、ハードウェアデバイスに関連するインストール又は更新データが取得される（動作３０２）。このデータは、コンピュータデバイスでのハードウェアデバイスのインストールの間、且つ／あるいは、コンピュータデバイスに予めインストールされているハードウェアデバイスのためのデバイスドライバ及び／又は他のデータの更新の間、使用される。データは、例えば、図２のデバイスインストールファイル及びデータ２３２並びに／又はデバイス更新ファイル及びデータ２３４からであってよい。

【００４２】

インストール又は更新データが新しい又は更新される承諾タイプを含むかどうかに関して、確認がなされる（動作３０４）。新しい承諾タイプは、コンピュータデバイスにインストールされる新しいハードウェアデバイスの機能のための承諾タイプと、コンピュータデバイスに予めインストールされているハードウェアデバイスの新しい機能のための承諾タイプとに言及する。更新される承諾タイプは、コンピュータデバイスに予めインストールされているハードウェアデバイスの機能のための承諾タイプにおける変更に言及する。

【００４３】

インストール又は更新データが新しい又は更新される承諾タイプを含む場合は、デバイス許可記録は、取得されたインストール又は更新データに基づき更新される（動作３０６）。デバイス許可記録のこの更新は、デバイス許可記録への新しい承諾タイプの追加、コンピュータデバイスに予めインストールされているハードウェアデバイスの機能のための承諾タイプの変更、等といった、デバイス許可記録に対する様々な変更を含む。

【００４４】

更に、インストール又は更新データがアプリケーションＩＤリストに対する変更を含むかどうかに関しても、確認がなされる（動作３０８）。アプリケーションＩＤリストに対する変更は、コンピュータデバイスにインストールされる又は既にインストールされているハードウェアデバイスの機能にアクセスすることを許可されるべき１又はそれ以上のアプリケーションの識別子に対する変更（例えば、追加、除外、等）に言及する。アプリケーションＩＤリストに対する変更は、上述されたように、特権付与承諾タイプと関連付けられる機能についてインストール又は更新データにおいて含まれ得る。

【００４５】

なされるべきでデバイス許可記録のアプリケーションＩＤリストに対する変更は、インストール又は更新データから特定される（動作３１０）。この特定は、ハードウェアデバイスの特定の機能にアクセスすることを許可されるアプリケーションの識別子を特定すること、又はハードウェアデバイスの特定の機能にアクセスすることを許可されないアプリケーションの識別子を特定することであってよい。

【００４６】

デバイス許可記録のアプリケーションＩＤリストは、取得されたインストール又は更新データに基づき更新される（動作３１２）。動作３１２におけるこの更新は、更なるユーザ承諾なしでハードウェアデバイスの特定の機能にアクセスすることを許可されるようにデバイス許可記録においてアプリケーションの識別子を格納にすること（例えば、特定の機能と関連付けられるアプリケーションＩＤリストに識別子を加えること）、アプリケーションがハードウェアデバイスの特定の機能にアクセスすることを許可されないようにデバイス許可記録からアプリケーションの識別子を除くこと（例えば、特定の機能と関連付けられるアプリケーションＩＤリストから識別子を除くこと）、等を含むことができる。

【００４７】

デバイス許可記録がインストール又は更新データに基づきあらゆる新しい又は更新される承諾タイプを反映するよう更新され、且つ／あるいは、アプリケーションの識別子に対するあらゆる変更を反映するよう更新された後、動作３０２において取得されたデータに基づくインストール又は更新は終了される（動作３１４）。更なるインストール又は更新データが後の時点で取得されてよく、処理３００は繰り返されて、その更なるインストール又は更新データに基づきなされるデバイス許可記録に対する更なる変更をもたらす。

【００４８】

代替的に、動作３０２で取得されるインストール又は更新データがハードウェアデバイスの新しいインスタンスのためのインストールデータである状況では、動作３０４乃至３１４は、適切な承諾がユーザから受け取られた後にのみ、実行され得る。よって、デバイス許可記録の承諾タイプに対する変更及びデバイス許可記録のアプリケーションＩＤリストに対する変更は、そのような変更がユーザによって承諾されるまでは、ハードウェアデバイスの新しいインスタンスのためのインストールデータに基づき行われない。

【００４９】

図４は、１又はそれ以上の実施形態に従ってハードウェアデバイスの機能にアクセスするリクエストに応答する処理４００の例を表すフローチャートである。処理４００は、コンピュータデバイス、例えば、図１のコンピュータデバイス１００によって、実行され、ソフトウェア、ファームウェア、又はそれらの組み合わせにおいて実施され得る。処理４００は、動作の組として示され、様々な動作の操作を実行するために示された順序に制限されない。処理４００は、ハードウェアデバイスの機能にアクセスするリクエストに応答する処理の例であり、ハードウェアデバイスの機能にアクセスするリクエストに対する応答に関する更なる議論は、異なる図を参照してここに含まれる。

【００５０】

処理４００において、ハードウェアデバイスの機能にアクセスするリクエストが受信される（動作４０２）。このリクエストは、上述されたように、デバイスブローカーで受信される。

【００５１】

アプリケーションが機能にアクセスすることを許可されていることをデバイス許可記録が示すかどうかに関して、確認がなされる（動作４０４）。この確認は、例えば、機能と関連付けられる承諾タイプが特権付与承諾タイプであるかどうかを確認し、そうである場合は、アプリケーションの識別子がハードウェアデバイスの機能と関連付けられるアプリケーションＩＤリストに含まれるかどうかを確認することによって、行われる。この確認は、通常、上述されたように、アプリケーションが確認を不正に変更し又は別なふうに干渉することを防ぐよう、コンピュータデバイスにより実施される処理４００のオペレーティングシステムの信頼される部分において行われる。

【００５２】

動作４０４における確認に基づき、アプリケーションが機能にアクセスすることを許可されると決定される場合は、リクエストは許可され、アプリケーションは機能にアクセスすることを可能にされる（動作４０６）。この許可は、例えば、上述されたように、リクエストされている機能へのハンドル又は他の識別子をアプリケーションへ返すことであってよい。なお、動作４０４における確認に基づき、アプリケーションが機能にアクセスすることを許可されないと決定される場合は、リクエストは拒絶され、アプリケーションは機能にアクセスすることを認められない（動作４０８）。この拒絶は、例えば、上述されたように、機能へのハンドル又は他の識別子をアプリケーションへ返すことを拒むことであってよい。

【００５３】

よって、ここで論じられるデバイス機能へのアプリケーションの結び付けの技術は、ハードウェアデバイスの種々の機能が特定のアプリケーションにのみアクセス可能であることを可能にする。例えば、プリンタのベンダーは、彼らが流通させるプリンタを管理するアプリケーションを分配することができ、それにより、全てのアプリケーションがそのプリンタを用いてデータを印刷することを可能にしながら、彼らが開発又は別なふうに承認する（任意に、他のプリンタベンダーが開発又は別なふうに承認する）プリンタ管理のためのアプリケーションのみがプリンタを管理することを可能にする。他の例として、ベンダーは、新しいハードウェアデバイスと、そのハードウェアデバイスを使用するアプリケーションを開発し、ベンダーが開発するアプリケーションおみがそのハードウェアデバイスを使用することを可能にすることができる。

【００５４】

更に、ここで論じられるデバイス機能へのアプリケーションの結び付けの技術を用いるシステムは拡張可能である。どのアプリケーションがハードウェアにアクセスすることを許可されるのかは、時間にわたって変化しうる。更に、（例えば。１又はそれ以上の新しいハードウェアデバイスインターフェースクラスを有する）新しいハードウェアデバイスは、ハードウェアデバイスの開発者又はベンダーがハードウェアデバイスにアクセスすることができると望むアプリケーションのみがハードウェアデバイスにアクセスすることができるように、システムにインストールされ得る。

【００５５】
図５は、１又はそれ以上の実施形態に従ってデバイス機能へのアプリケーションの結び付けを実施するよう構成され得るコンピュータデバイス５００の例を表す。コンピュータデバイス５００は、例えば、図１のコンピュータデバイス１００であってよく、且つ／あるいは、図２のシステム２００を実施してよい。
【００５６】
コンピュータデバイス５００は、１又はそれ以上のプロセッサ又はプロセッシングユニット５０２と、１又はそれ以上のメモリ及び／又は記憶コンポーネント５０６を有することができる１又はそれ以上のコンピュータ可読媒体５０４と、１又はそれ以上の入出力（Ｉ／Ｏ）デバイス５０８と、様々なコンポーネント及びデバイスが互いと通信することを可能にするバス５１０とを有する。コンピュータ可読媒体５０４及び／又は１又はそれ以上のＩ／Ｏデバイス５０８は、コンピュータデバイス５００の一部として含まれてよく、あるいは、代替的に、コンピュータデバイス５００へ結合されてよい。バス５１０は、様々な異なるバスアーキテクチャを用いるメモリバス又はメモリコントローラ、ペリフェラルバス、アクセラレイティッド・グラフィクス・ポート、プロセッサ又はローカルバス、等を含む様々なタイプのバス構造の中の１又はそれ以上を表す。バス５１０は、有線及び／又は無線バスを有することができる。
【００５７】
メモリ／記憶コンポーネント５０６は、１又はそれ以上のコンピュータ記憶媒体を表す。コンポーネント５０６は、揮発性媒体（例えば、ランダムアクセスメモリ（ＲＡＭ））及び／又は不揮発性媒体（例えば、読出専用メモリ（ＲＯＭ）、フラッシュメモリ、光ディスク、磁気ディスク、等）を有することができる。コンポーネント５０６は、固定式媒体（例えば、ＲＡＭ、ＲＯＭ、固定式ハードドライブ、等）及び取り外し可能な媒体（例えば、フラッシュメモリドライブ、リムーバブル・ハードドライブ、光ディスク、等）を有することができる。
【００５８】
ここで論じられる技術は、１又はそれ以上のプロセッシングユニット５０２によって実行される命令を有するソフトウェアにおいて実施可能である。当然に、種々の命令がコンピュータデバイス５００の種々のコンポーネントにおいて、例えば、プロセッシングユニット５０２において、プロセッシングユニット５０２の様々なキャッシュメモリにおいて、デバイス５００の他のキャッシュメモリにおいて（図示せず。）、他のコンピュータ可読媒体において、等で、記憶され得る。更に、当然に、命令がコンピュータデバイス５００において記憶される場所は、時間にわたって変化しうる。
【００５９】
１又はそれ以上の入出力デバイス５０８は、ユーザがコマンド及び情報をコンピュータデバイス５００に入力することを可能にし、更に、情報がユーザ及び／又は他のコンポーネント若しくはデバイスに提示されることを可能にする。入力デバイスの例には、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、スキャナ等があり、出力デバイスの例には、表示デバイス（例えば、モニタ又はプロジェクタ）、スピーカ、プリンタ、ネットワークカード等がある。
【００６０】
様々な技術が、ソフトウェア又はプログラムモジュールの一般的な脈略においてここで記載される。一般的に、ソフトウェアは、特定のタスクを実行し又は特定の抽象データ型を実施するルーチン、プログラム、アプリケーション、オブジェクト、コンポーネント、データ構造、等を含む。それらのモジュール及び技術の実施は、何らかの形のコンピュータ可読媒体において記憶され、又はそれにわたって伝送されてよい。コンピュータ可読媒体は、コンピュータデバイスによってアクセス可能な如何なる利用可能な媒体であってもよい。限定されない例として、コンピュータ可読媒体は、“コンピュータ記憶媒体”及び“通信媒体”を有してよい。
【００６１】

“コンピュータ記憶媒体”は、コンピュータ可読命令、データ構造、プログラムモジュール、又は他のデータ等の情報の記憶のためのあらゆる方法又は技術において実施される揮発性及び不揮発性、リムーバブル及び非リムーバブル媒体を含む。コンピュータ記憶媒体は、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ若しくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）若しくは他の光記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置若しくは他の磁気記憶装置、又は所望の情報を記憶するために使用可能であり且つコンピュータによってアクセス可能なあらゆる他の媒体を含むが、これらに限られない。

【００６２】

“通信媒体”は、通常、コンピュータ可読命令、データ構造、プログラムモジュール、又は他のデータを、搬送波又は他の伝送メカニズムのような変調データ信号において具現する。通信媒体はまた、あらゆる情報送達媒体を含む。語“変調データ信号”は、信号において情報を符号化するようにその特性の１又はそれ以上を設定又は変更された信号を意味する。限定されない例として、通信媒体は、有線ネットワーク及び直接有線接続のような有線媒体、並びに音響、ＲＦ、赤外線、及び他の無線媒体のような無線媒体を含む。上記のいずれかの組み合わせも、コンピュータ可読媒体の適用範囲内に含まれる。

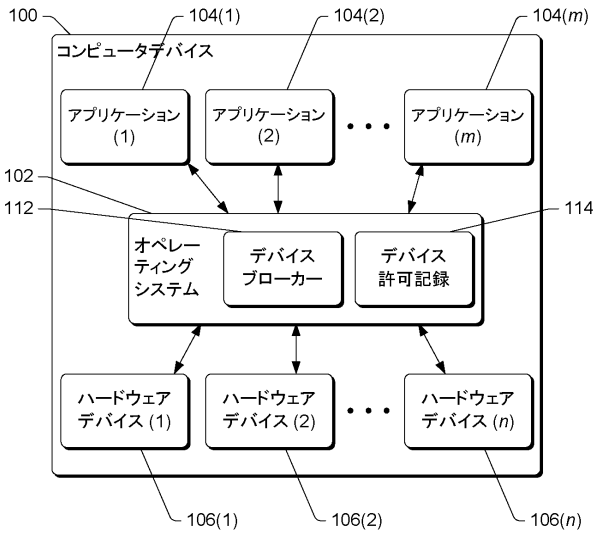
【００６３】

一般に、ここで記載される機能又は技術のいずれも、ソフトウェア、ファームウェア、ハードウェア（例えば、固定ロジック回路）、手動プロセッシング、又はそれらの実施の組み合わせを用いて実施され得る。ここで使用される語“モジュール”及び“コンポーネント”は、一般に、ソフトウェア、ファームウェア、ハードウェア、又はそれらの組み合わせを表す。ソフトウェア実施の場合に、モジュール又はコンポーネントは、プロセッサ（例えば、１又は複数のＣＰＵ）で実行される場合に、指定されるタスクを実行するプログラムコードを表す。プログラムコードは、１又はそれ以上のコンピュータ可読メモリデバイスにおいて記憶され得る。これに関する更なる記載は、図５を参照して見つけられてよい。ここで記載されるデバイス機能へのアプリケーションの結び付けの技術の特徴は、プラットフォーム非依存であり、当該技術が、様々なプロセッサを有する様々な市販のコンピュータプラットフォームで実施され得ることを意味する。

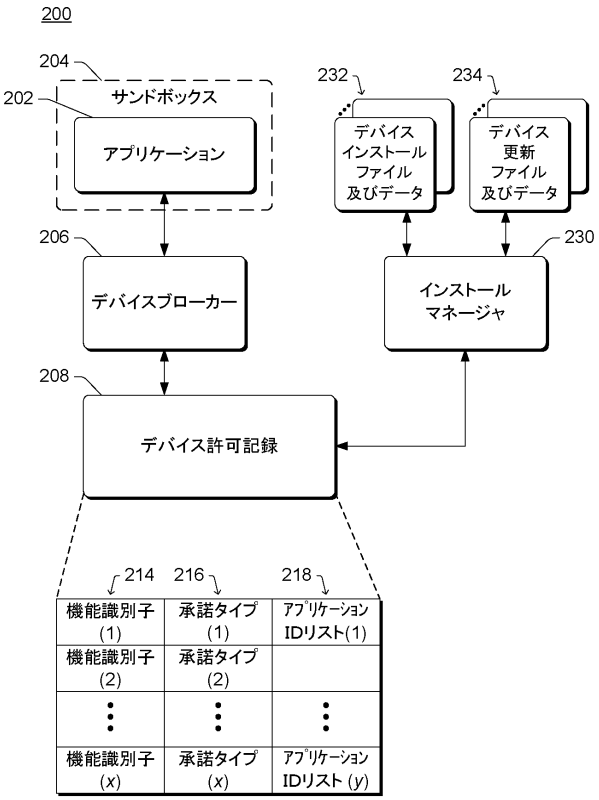
【００６４】

対象について、構造上の特徴及び／又は方法上の動作に特有の言語において記載してきたが、添付の特許請求の範囲において定義される対象は、必ずしも、上記の具体的な特徴又は動作に限定されないことが理解されるべきである。むしろ、上記の具体的な特徴及び動作は、特許請求の範囲を実施する例となる形態として開示される。

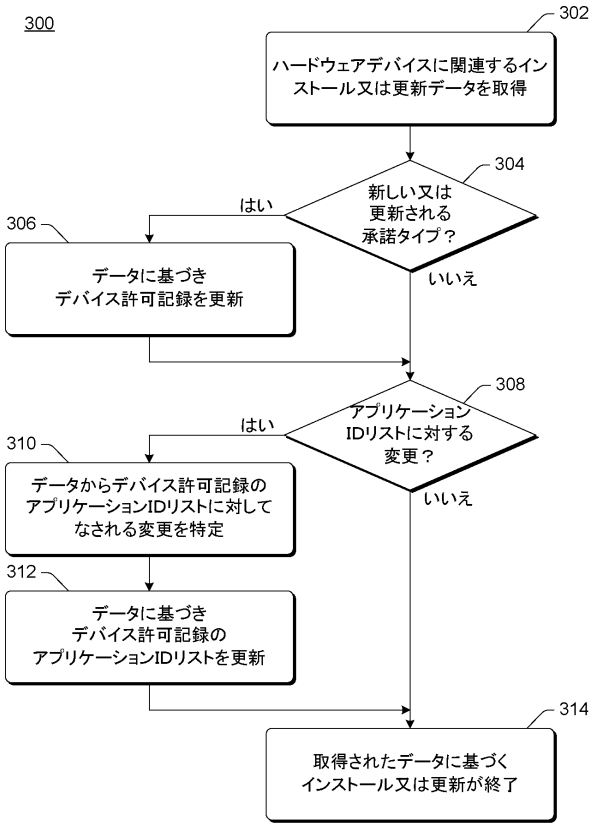
【図１】


100
104(1)
104(2)
104(m)
コンピュータデバイス
アプリケーション (1)
アプリケーション (2)
アプリケーション (m)
102
112
114
オペレーティングシステム
デバイスブローカー
デバイス許可記録
ハードウェアデバイス (1)
ハードウェアデバイス (2)
ハードウェアデバイス (n)
106(1)
106(2)
106(n)

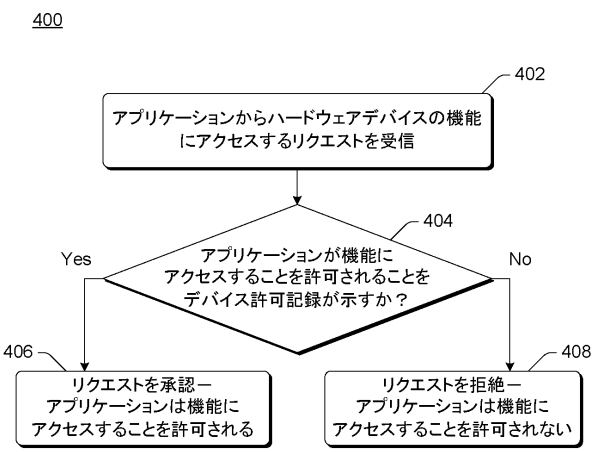
【図２】


200
204
202
サンドボックス
アプリケーション
232
234
デバイスインストールファイル及びデータ
デバイス更新ファイル及びデータ
206
デバイスブローカー
230
インストールマネージャ
208
デバイス許可記録
214
216
218
機能識別子 (1)
承諾タイプ (1)
アプリケーションIDリスト(1)
機能識別子 (2)
承諾タイプ (2)
機能識別子 (x)
承諾タイプ (x)
アプリケーションIDリスト (y)

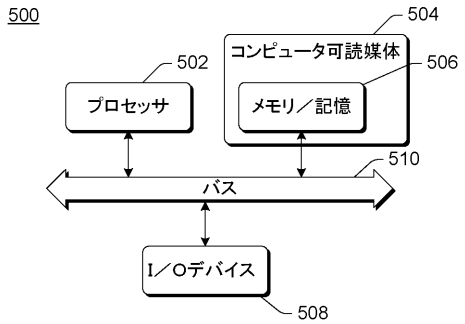
【図３】


300
302
ハードウェアデバイスに関連するインストール又は更新データを取得
304
新しい又は更新される承諾タイプ？
はい
いいえ
306
データに基づきデバイス許可記録を更新
308
アプリケーションIDリストに対する変更？
はい
いいえ
310
データからデバイス許可記録のアプリケーションIDリストに対してなされる変更を特定
312
データに基づきデバイス許可記録のアプリケーションIDリストを更新
314
取得されたデータに基づくインストール又は更新が終了

【図４】


400
402
アプリケーションからハードウェアデバイスの機能にアクセスするリクエストを受信
404
アプリケーションが機能にアクセスすることを許可されることをデバイス許可記録が示すか？
Yes
No
406
リクエストを承認－アプリケーションは機能にアクセスすることを許可される
408
リクエストを拒絶－アプリケーションは機能にアクセスすることを許可されない

【図５】


500
504
コンピュータ可読媒体
502
506
プロセッサ
メモリ／記憶
510
バス
I／Oデバイス
508

フロントページの続き

(72)発明者 ガナパティ，ナラヤナン
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 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 エルシーエー－インターナショナル パテンツ 内
(72)発明者 モリス，マックス ジー.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 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 エルシーエー－インターナショナル パテンツ 内
(72)発明者 スリヴォヴィッツ，ポール
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 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 エルシーエー－インターナショナル パテンツ 内
(72)発明者 デイヴィス，ダレン アール.
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 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 エルシーエー－インターナショナル パテンツ 内
(72)発明者 ルソス，ジョージ エヴァンゲロス
アメリカ合衆国 ９８０５２－６３９９ ワシントン州 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 エルシーエー－インターナショナル パテンツ 内

合議体
審判長 高木 進
審判官 辻本 泰隆
審判官 須田 勝巳

(56)参考文献 特開２００８－３０５３３６（ＪＰ，Ａ）
特開２００４－１９２１００（ＪＰ，Ａ）
特表２００５－５０２１２８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/00-21/88