(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2014-526734
(P2014-526734A)
(43)公表日　平成26年10月6日(2014.10.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/12	(2013.01)	G06F	21/22	112B	5B376
G06F 9/445	(2006.01)	G06F	9/06	610A	

審査請求 未請求　予備審査請求 未請求　（全 23 頁）

(21)出願番号　特願2014-529689 (P2014-529689)
(86)(22)出願日　平成23年10月11日 (2011.10.11)
(85)翻訳文提出日　平成26年4月24日 (2014.4.24)
(86)国際出願番号　PCT/US2011/055795
(87)国際公開番号　WO2013/039530
(87)国際公開日　平成25年3月21日 (2013.3.21)
(31)優先権主張番号　13/230,611
(32)優先日　平成23年9月12日 (2011.9.12)
(33)優先権主張国　米国 (US)

(71)出願人　500046438
マイクロソフト　コーポレーション
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
(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】宣言及び承諾に基づくアクセス調停

(57)【要約】
実施形態は、デバイス機能のような機能へのアプリケーションアクセスを調停する処理、システム及びデバイスを含む。アクセスブローカーは、機能にアクセスするためのアプリケーションからの要求を受け取る。アクセスブローカーは、アプリケーションマニフェストがその機能を宣言しているかどうかに少なくとも部分的に基づき、アクセスを許可すべきかどうかを決定する。アクセスブローカーはまた、アクセス要求へのユーザ承諾を求めるようユーザインターフェース要素を表示させてよい。また、アプリケーション内ユーザインターフェース要素が提供され、特定のアプリケーションのための機能アクセス設定を表示する。アプリケーション内ユーザインターフェース要素は、それらの設定を変更するための選択可能なオプションを含む。ユーザインターフェースを介したそれらの設定の変更は、アクセスブローカーにおける設定を更新する。

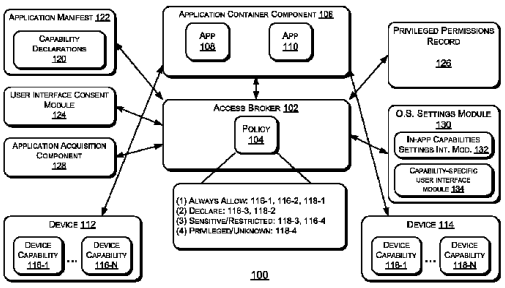


FIG. 1

【特許請求の範囲】
【請求項１】
コンピュータシステムのアクセスブローカーによって、前記コンピュータシステムのアプリケーションから、前記コンピュータシステムの利用可能な機能性の機能へのアクセスのための要求を受け取るステップと、
前記アクセスブローカーによって、前記要求に応答して、前記アプリケーションのアプリケーションマニフェストに関連する機能宣言にアクセスするステップと、
前記アクセスブローカーによって、前記アプリケーションが前記機能にアクセスするよう構成されるファンクションを含むことを示す宣言を前記機能宣言が含むとの決定に少なくとも部分的に基づき、前記要求を許可するステップと
を有する方法。
【請求項２】
前記アクセスブローカーによって、前記機能へのアクセスの許可がユーザ承諾を必要とするとのインジケーションを前記アクセスブローカーのポリシーが含むと決定するステップと、
前記アクセスブローカーによって、前記インジケーションを含むとの決定に応答して、前記要求を承諾するための選択可能なオプションを有する、前記コンピュータシステムのオペレーティングシステムのユーザインターフェース要素の表示を引き起こすステップと
を更に有し、
前記許可は更に、前記要求に対するユーザ承諾を示す入力の受信に少なくとも部分的に基づく、
請求項１に記載の方法。
【請求項３】
前記アクセスブローカーによって、前記機能へのアクセスの許可がユーザ承諾を必要とするとのインジケーションを前記アクセスブローカーのポリシーが含むと決定するステップ
を更に有し、
前記要求の許可は更に、前記機能へのアクセスのためのユーザ承諾を示す入力がオペレーティングシステム設定モジュールを介して受け取られたとの決定に少なくとも部分的に基づく、
請求項１に記載の方法。
【請求項４】
１又はそれ以上のプロセッサと、
コンピュータシステムにインストールされるハードウェアデバイスと、
前記１又はそれ以上のプロセッサによって実行可能であり且つユーザインターフェース要素を表示するよう構成されるユーザ承諾コンポーネントと、
前記１又はそれ以上のプロセッサによって実行可能であるアクセスブローカーと
を有し、
前記アクセスブローカーは、前記ハードウェアデバイスのデバイス機能にアクセスするための前記コンピュータシステムのアプリケーションからの要求の受信に応答して、前記ユーザ承諾コンポーネントに、前記ハードウェアの前記デバイス機能へのアクセスがユーザ承諾を必要とするとのインジケーションを前記コンピュータシステムのブローカーポリシーが含むとの当該アクセスブローカーによる決定の上に、前記要求を承諾するための選択可能なオプションを有するユーザインターフェース要素を表示させるよう構成される、
コンピュータシステム。
【請求項５】
前記アクセスブローカーは更に、前記要求に対するユーザ承諾を示す入力の受信に少なくとも部分的に基づき前記デバイス機能にアクセスするのに使用可能なインターフェースハンドルを前記アプリケーションへ提供するよう構成される、
請求項４に記載のコンピュータシステム。

【請求項６】
前記アクセスブローカーは、前記ハードウェアデバイスの前記デバイス機能にアクセスするための以前の要求に対するユーザ承諾を示す入力が前記要求の受信の前に受け取られたとの決定の上に前記要求を許可するよう構成される、
請求項４に記載のコンピュータシステム。
【請求項７】
当該コンピュータシステムのメモリに記憶される前記アプリケーションのアプリケーションマニフェストを更に有し、
前記アクセスブローカーは、前記要求に対するユーザ承諾を示す入力の受信と、前記アプリケーションが前記デバイス機能にアクセスするためのファンクションを含むことを示す宣言を前記アプリケーションマニフェストが含むとの決定とに基づき、インターフェースハンドルを前記アプリケーションへ返すよう構成される、
請求項４に記載のコンピュータシステム。
【請求項８】
前記１又はそれ以上のプロセッサによって実行可能であり且つ前記アプリケーションを取得するための選択可能なオプションを有するアプリケーション取得インターフェースを表示するよう構成されるアプリケーション取得モジュールを更に有し、
前記アプリケーション取得インターフェースは、前記アプリケーションが前記デバイス機能にアクセスするためのファンクションを含むことを示す前記宣言を含む前記アプリケーションマニフェストから１又はそれ以上の宣言を表示する、
請求項７に記載のコンピュータシステム。
【請求項９】
特定の機能にアクセスするための要求が前記アクセスブローカーによって調停されることを条件とするセキュア実行モードにおいて前記１又はそれ以上のプロセッサによる前記アプリケーションの実行を強いるよう構成されるアプリケーションコンテナを更に有する
請求項４に記載のコンピュータシステム。
【請求項１０】
アプリケーションの実行中に、ユーザ入力装置からの入力に応答して、前記アプリケーションの機能アクセス設定を変更するための選択可能なオプションを含むアプリケーション特有オペレーティングシステムユーザインターフェース要素を表示するステップと、
前記選択可能なオプションが選択されることを示すユーザ入力装置からの入力の受信に応答して、前記アプリケーションの前記機能アクセス設定を変更するようアクセスブローカーを更新するステップと
を有する方法を実行するようコンピュータシステムの１又はそれ以上のプロセッサによって実行可能な複数のプログラミング命令を有するコンピュータ可読媒体。

【発明の詳細な説明】
【背景技術】
【０００１】
コンピュータシステムに設置されるハードウェアデバイスは、印刷、デバイス管理、位置特定サービス、メッセージング、ビデオキャプチャ、等のような様々な機能を提供する。インストールされるアプリケーションは、機能性をコンピュータシステムに提供するようそれら及び他の機能にアクセスする。しかし、ユーザの承諾又は認識なしでアプリケーションが潜在的に危険な機能にアクセスすることがあり得る。例えば、位置特定サービス、メッセージングサービス、及び他を標的とする既存のエクスプロイトが存在する。それらのエクスプロイトは、ユーザのプライバシーを危うくし、又はユーザがユーザの認識又は承諾なしで彼らのネットワークプロバイダによって課金される事態を引き起こし得る。
【０００２】
アプリケーション開発者に利するように不正な意図がない場合でさえ、潜在的に危険な機能へのアプリケーションアクセスは、コンピュータシステムの安全性又はユーザのプラ

イバシーを意図せず危うくし得る。そして、ユーザがアプリケーションによる機能アクセスを承諾することを認められる場合でさえ、どのような状況においてアプリケーションが機能にアクセスするのかをユーザが理解することは困難であり得る。すなわち、そのようなことをユーザに説明することは困難であり得る。ユーザは、アプリケーションが特定の機能にアクセスすることを可能にする悪影響を認識できないことがある。従って、ユーザは、機能へのアプリケーションアクセスを十分に認めないか又は過度に認めるかの何れかである場合があり、それにより潜在的にユーザ経験を弱体化させるか又はユーザのプライバシー及び安全性を危うくする。

【発明の概要】

【課題を解決するための手段】

【０００３】

本概要は、詳細な説明において以下で更に説明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る。本概要は、請求される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、更に、請求される対象の適用範囲を制限するよう用いられるよう意図されない。

【０００４】

アクセスブローカーは、ハードウェアデバイス機能のようなコンピュータシステム機能へのアプリケーションアクセスを制御する。アクセスブローカーは、機能へのアクセスのためのアプリケーションからの要求を受け取り、アクセスを許可すべきかどうかを決定するようポリシーを適用する。ポリシーは、アプリケーションが機能へのアクセスを許可されるためにアプリケーションがそれらの機能を宣言するアプリケーションマニフェストを有することを求めてよい。また、ポリシーは、アプリケーションが機能へのアクセスを許可されるためにユーザが要求を承諾することを求めてよい。

【０００５】

ユーザインターフェースコンポーネントは、アプリケーション特有の機能設定とともに、それらの設定を変更するための選択可能なオプションを含むユーザインターフェースを提供する。それらのユーザインターフェースは、アプリケーションとのユーザインタラクションの間立ち上げられて、ユーザに、特定のアプリケーションのための機能設定を見且つ設定するようシングルロケーションを提供する。それらのユーザインターフェースはオペレーティングシステムユーザインターフェースであるから、ユーザは、オペレーティングシステムが潜在的に危険な機能へのアプリケーションアクセスを制御しているとのより確かな信頼を提供される。

【図面の簡単な説明】

【０００６】

【図１】アクセスブローカーサービスを提供するのに使用可能なシステムの例の概略図である。

【図２】実施形態に従ってアクセスブローカーサービスを提供するのに使用可能なコンピュータ装置の例のブロック図である。

【図３】アプリケーション宣言及びユーザ承諾に基づき機能アクセスを調停する処理の例を示すフロー図である。

【図４】アプリケーション内機能インターフェース設定構成を提供する処理の例を示すフロー図である。

【図５】機能に特有の設定を見且つ設定するための処理の例を示すフロー図である。

【図６】細心の注意を払うべき機能のためのアプリケーション要求へのユーザ承諾を得るユーザインターフェース表示を例示する。

【図７】機能の表示を含むアプリケーション取得ユーザインターフェース表示を例示する。

【図８】アプリケーション内機能設定情報を表示するユーザインターフェース表示を例示する。

【図９】機能に特有の設定情報を表示するユーザインターフェース表示を例示する。

【発明を実施するための形態】
【０００７】
詳細な説明は、添付の図を参照して記載される。図中、参照符号の左端の数字は、その参照符号が最初に現れる図を特定する。異なる図における同じ参照符号は、類似する又は同じ事項を示す。
【０００８】
［概要］
上述されたように、アプリケーションは、機能性をユーザに提供するために様々な機能にアクセスする。デバイス位置特定、メッセージング、ビデオキャプチャ、インターネットアクセス、及び他のような、それらの機能の幾つかは潜在的に危険であり、ユーザはそれらへのアクセスを制御又は禁止したいと望むことがある。また、ユーザは、ユーザがアプリケーションを取得又は実行すべきか否かを決定することができるように、アプリケーションがどの機能にアクセスするよう構成されるかを決定することができる必要がある。
【０００９】
実施形態において、アクセスブローカーは、デバイス機能のような機能へのアプリケーションアクセスを制御する。保護されたアプリケーションコンテナ内で実行されるアプリケーションは、アクセスブローカーを通じて機能へのアクセスを要求する。要求される機能へ適用するポリシーのタイプに基づき、アクセスブローカーは、アプリケーション毎にポリシーを実施する方策を講じる。例えば、アクセスブローカーのポリシーは、アプリケーションが機能へのアクセスを許可されるためにユーザ承諾が取得されるべきことを示してよい。ポリシーは、アプリケーションが機能へのアクセスを許可されるために、機能がアプリケーションにそのアプリケーションマニフェストにおいて当該機能を宣言するよう求めることを示してよい。ポリシーは、アプリケーションが特定の機能へのアクセスを許可されるために、アプリケーションがその特定の機能にアクセスすることを許可されると特権的許可記録において具体的に特定されていることを求めてよい（２０１１年５月２日付けでＧａｎａｐｈａｔｈｙ等によって出願された、特権的許可記録を用いてアクセス調停に関する詳細のための“BINDING APPLICATIONS TO DEVICE CAPABILITIES”と題された米国特許出願第１３／０９９２６０を参照のこと。）。
【００１０】
よって、特定の機能へ適用するポリシータイプに依存して、アクセスブローカーは、ユーザインターフェース要素が機能を承諾するための選択可能なオプションを有して表示されるようにしてよい。このユーザインターフェース要素は、アプリケーションとのユーザのインタラクションとの関連でオペレーティングシステムによって表示される。これは、ユーザが、いつアプリケーションがなぜ機能にアクセスするのかを理解することを容易にする。
【００１１】
実施形態において、ユーザは、アプリケーションと相互作用するという状況で、オペレーティングシステムユーザインターフェース要素を呼び出すオプションを与えられる。オペレーティングシステムユーザインターフェース要素は、アプリケーションがアクセスすることができる機能を示す。ユーザインターフェース要素は、ユーザが様々な機能へのアクセスを有効又は無効にすることを可能にする。このアプリケーション特有のビューは、アプリケーションがどの機能へアクセスすることができるのかを決定するために複数の設定ページを開く必要なしに、アプリケーションがアクセスすることができる全ての、デバイス機能のような機能を見るためのシングルプレイスをユーザに与える。
【００１２】
実施形態において、オペレーティングシステム設定モジュールは、特定の機能にアクセスすることができる全てのアプリケーションのビューをユーザに提供する。この機能に特有のビューは、ユーザがアプリケーション毎に又は全体としてアクセスを制御することを可能にし、それにより更にユーザ経験を高める。それらの特徴、すなわち、ユーザ承諾、アプリケーションマニフェストにおける機能宣言、アプリケーション特有の機能設定、及

び機能特有のコンフィグレーション設定の組み合わせは、潜在的に危険な機能へのアプリケーションアクセスが適切に制御されるとの確かな信頼をユーザに提供する。

【００１３】

この詳細な説明の全体を通して、語「構成される（configured）」は、アプリケーションの機能ファンクションを記述するために使用される場合に、アプリケーションが、ハードウェアデバイスのデバイス機能のような特定の機能へアクセスする機能性を有してプログラミングされることを意味する。この詳細な説明の全体を通して、語「有効にされる（enabled）」は、アプリケーションの機能ファンクションを記述するために使用される場合に、アプリケーションが機能にアクセスすることを可能に又は許可されることを意味する。従って、アプリケーションは、特定の機能にアクセスするよう“構成される”と同時に、同じ機能にアクセスすることを“有効にされ”ないことがある。

【００１４】

本願で記載される処理、システム及び装置は、多くの方法において実施されてよい。実施例は、添付の図面を参照して以下で与えられる。

【００１５】

［アクセスブローカーサービスを提供する環境の例］

図１は、アクセスブローカーサービスを提供するのに使用可能なシステム１００の例の概略図である。システム１００は、アクセスブローカーサービスを実施することができる様々な適切なコンピュータ装置タイプで実施されてよい。適切なコンピュータ装置は、１以上のパーソナルコンピュータ、サーバ、サーバファーム、データセンター、特別目的のコンピュータ、タブレットコンピュータ、ゲーム機、スマートフォン、それらの組み合わせ、又はデバイスブローカーサービスの全て若しくは一部を記憶及び実行することができる何らかの他のコンピュータ装置を含むか又はその一部であってよい。

【００１６】

図１の実例では、システム１００はアクセスブローカー１０２を有する。アクセスブローカー１０２は、様々なアクセスレベルの下にある機能のリストを含むポリシー１０４を有する。アクセスレベルの例には、“常に許可する（always allow）”、“宣言する（declare）”、“細心の注意を払うべき／制限される（sensitive/restricted）”、及び“特別許可された／未知（privileged/unknown）”がある。それらのレベルの例は、本願では説明のために使用され、限定の意味でとられるべきではない。様々な実施形態において、アクセスレベルは、他のアクセスレベルのサブレベルであってよい。１つの制限されない例において、機能は、“宣言する”及び“細心の注意を払うべき／制限される”の両方に該当することがある。他の制限されない例において、機能は、“細心の注意を払うべき／制限される”及び“特別許可された”の両方に該当することがある。

【００１７】

アプリケーションコンテナコンポーネント１０６は、メモリ、アプリケーション、アプリケーションプログラミングインターフェース（ＡＰＩ）、又はデバイスのような様々なシステムリソースへのアプリケーションアクセスを制御するセキュア実行モードにおいてアプリケーションの実行を強制するための機能を提供する。アプリケーション（Ａｐｐ）１０８及び１１０は、アプリケーションコンテナコンポーネント１０６によって実施されるセキュアモードにおいて実行されるよう構成される。それらのアプリケーションは、デバイス１１２及びデバイス１１４のようなシステム１００の様々なデバイスと相互作用するよう構成される様々なファンクションを含む。デバイス１１２は、デバイス機能１１６－１乃至１１６－Ｎのような様々な機能を提供することができる。そして、デバイス１１４は、デバイス機能１１８－１乃至１１８－Ｎのような様々な機能を提供することができる。デバイス機能の制限されない例には、位置特定サービス（例えば、グローバルポジショニングシステム（ＧＰＳ）サービス）、メッセージングサービス（例えば、ショートメッセージサービス（ＳＭＳ））、ビデオキャプチャサービス、及び他がある。

【００１８】

ポリシー１０４は、様々なアクセスレベルの下でデバイス１１２及び１１４の様々な機

能をリストアップする。例えば、デバイス機能１１６－１、１１６－２及び１１８－１は“常に許可する”の下でリストアップされ、デバイス機能１１６－３及び１１８－２は“宣言する”の下でリストアップされ、デバイス機能１１８－３及び１１６－４は“細心の注意を払うべき／制限される”の下でリストアップされ、デバイス機能１１８－４は“特別許可された”の下でリストアップされる。

【００１９】

アクセスブローカー１０２は、デバイス１１２及び１１４の様々な機能にアクセスするためのアプリケーション１０８及び１１０からの要求を受け取るよう構成される。第１の例では、アプリケーション１１０は、デバイス１１２のデバイス機能１１６－１へのアクセスを要求する。アクセスブローカー１０２は、ポリシー１０４に対してルックアップ動作を実行し、デバイス機能１１６－１が“常に許可する”レベルに該当すると決定する。結果として、アクセスブローカー１０２は、デバイス機能１１６－１へアクセスするようアプリケーション１１０へデバイスハンドルを提供する。次いで、アプリケーション１１０はハンドルを利用して、データ及びコマンドを送信及び受信することを含め、デバイス機能１１６－１と相互作用することができる。“常に許可する”レベルに該当する機能は、最も危険性がないと考えられる。１つの制限されない例において、印刷サービスは“常に許可する”又は同等のアクセスレベルの下でリストアップされてよい。

【００２０】

第２の例では、アクセスブローカー１０２は、デバイス１１４のデバイス機能１１８－２のような機能にアクセスするためのアプリケーション１０８からの要求を受け取る。アクセスブローカー１０２は、ポリシー１０４に対してルックアップ動作を実行し、デバイス機能１１８－２が“宣言する”アクセスレベルに該当すると決定する。従って、アクセスブローカー１０２は、アプリケーション１０８に関連するアプリケーションマニフェスト１２２内のデバイス宣言１２０が、アプリケーション１０８がデバイス１１４のデバイス機能１１８－２にアクセスすることを可能にされるとの宣言を含むかどうかを決定する。デバイス宣言１２０は、“ＳＭＳメッセージング”又は“ビデオキャプチャ”のような機能のための“扱いやすい”名称とともに、グローバル一意識別子（ＧＵＩＤ）のような機能のための一意の識別子を含んでよい。宣言がアプリケーションマニフェスト１２２に存在すると決定されると、アクセスブローカー１０２は、デバイス１１４のデバイス機能１１８－２にアクセスするのに使用可能なデバイスハンドルをアプリケーション１０８に提供する。宣言がアプリケーションマニフェスト１２２に存在しないと決定されると、アクセスブローカー１０２は、アプリケーション１０８へ例外ハンドル（又はその他のエラーメッセージ若しくはコード）を返してアクセス要求を拒否する。アプリケーションが自身が特定の機能にアクセスすることを可能にするためにそのマニフェストにそれらの機能を含めることを条件とすることは、アプリケーションがそれらの機能にアクセスするよう構成されるという事実について正直であることを必要とする。これはつまり、ユーザが、アプリケーションがアクセスするよう構成されるデバイス機能を含む機能を知った上でアプリケーションをアクセスし、取得し、ダウンロードし、インストールし、及び／又は実行すべきかどうかを決定することを可能にする。

【００２１】

第３の例では、アプリケーション１０８は、デバイス１１２のデバイス機能１１６－４のような機能へのアクセスを要求する。アクセスブローカー１０２は、ポリシー１０４に対してルックアップ動作を実行し、デバイス機能１１６－４が“細心の注意を払うべき／制限される”レベルに該当すると決定する。結果として、アクセスブローカー１０２は、ユーザインターフェース承諾モジュール１２４に、アクセス要求を承諾するための選択可能なオプションを有するユーザインターフェースを表示させる。要求へのユーザ承諾を示す入力の受信時に（又はユーザ承諾が以前に与えられたとの決定の上に）、アクセスブローカー１０２は、デバイス機能１１６－４のインスタンスと相互作用するのに使用可能なデバイスハンドルをアプリケーション１０８に提供する。実施形態において、ポリシー１０４は、“細心の注意を払うべき／制限される”レベルに該当する機能が、それらの機能

へのアクセスを提供するために（ユーザ承諾に加えて）アプリケーションマニフェストにおいても宣言されることを条件としてよい。

【００２２】

第４の例では、アプリケーション１１０は、デバイス１１４のデバイス機能１１８－４のような機能へのアクセスを要求する。アクセスブローカー１０２は、ポリシー１０４に対してルックアップ動作を実行し、デバイス機能１１８－４が“特別許可された”レベルに該当すると決定する。結果として、アクセスブローカー１０２は、特権的許可記録１２６に対するルックアップを実行して、アプリケーション１１０がその中でデバイス機能１１８－４にアクセスすることを許可されていると具体的にリストアップされているかどうかを決定する（２０１１年５月２日付けでＧａｎａｐｈａｔｈｙ等によって出願された、特権的許可記録を用いてアクセス調停に関する詳細のための“BINDING APPLICATIONS TO DEVICE CAPABILITIES”と題された米国特許出願第１３／０９９２６０を参照のこと。）。

【００２３】

上記の例では、機能にアクセスするための要求は、特定のデバイスの特定の機能に係る。実施形態において、アプリケーションは汎用的な機能へのアクセスを要求することがあり、アクセスブローカー１０２は、もしあれば、どのデバイスが汎用的な機能を提供するのかを決定してよい。例えば、ユーザのコンピュータ装置に設置された１よりも多いウェブカメラが存在してよく、アクセスブローカー１０２は、ウェブカメラにアクセスするためのアプリケーションからの要求を受け取った後、１のウェブカメラへのアクセス又は他（おそらく、ユーザに１つを選択するよう促すこと。）を調停する。アクセスブローカー１０２はまた、一連の動作の前に、コンピュータシステムがウェブカメラを備えることを確かめるよう確認する。

【００２４】

システム１００は、アプリケーション１０８及びアプリケーション１１０のようなアプリケーションを取得するようオンライン又はオフラインストアへのインターフェースを提供するアプリケーション取得コンポーネント１２８を有する。アプリケーション１０８を取得するためのオプションを提示する場合に、例えば、アプリケーション取得コンポーネント１２８は、アプリケーション１０８に関連するアプリケーションマニフェスト１２２内の機能宣言１２０の表示を引き起こすよう構成される。よって、ユーザは、アプリケーション１０８がアクセスするよう構成されるそれらの機能に部分的に基づき、アプリケーションを取得すべきかどうかを決定することができる。

【００２５】

システム１００は、アプリケーション内機能設定インターフェースモジュール１３２及び機能特有ユーザインターフェースモジュール１３４を有するオペレーティングシステム設定モジュール１３０を有する。オペレーティングシステム設定モジュール１３０は、アプリケーションとのユーザインタラクションとの関連でアプリケーション内機能設定インターフェースモジュール１３２を表示するためのユーザ入力を受け取るよう構成される。アプリケーション内機能設定インターフェースモジュール１３２は、設定可能な機能アクセス設定のリストを提供する。アプリケーション内機能設定インターフェースモジュール１３２は、アプリケーションがアクセスするよう構成される機能と、それらの機能が現在そのアプリケーションに使用可能であるかどうかと、それらの機能をアプリケーションに使用可能又は不可能とするための選択可能なオプションとをリストアップする。

【００２６】

例えば、アプリケーション１０８と相互作用するという状況で、ユーザは、アプリケーション内機能設定インターフェースモジュール１３２の表示を要求してよい。アプリケーション内機能設定インターフェースモジュール１３２はその後、デバイス１１４のデバイス機能１１８－３へのアプリケーション１０８のアクセスを無効にするユーザ入力を受け取ってよい。よって、たとえユーザが以前に、アプリケーション１０８がデバイス１１４のデバイス機能１１８－３にアクセスすることを可能にすると承諾していたとしても、ア

クセスブローカー１０２は、現在のアクセスを破棄し、デバイス機能１１８－３に対するアプリケーション１０８からの更なる要求を拒否するか、又は代替的に、ユーザがデバイス機能１１８－３にアクセスするためのアプリケーション１０８からの将来の要求を承諾するよう求めてよい。

【００２７】

オペレーティングシステム設定モジュール１３０は、機能特有ユーザインターフェースモジュール１３４を表示させるよう構成される。機能特有ユーザインターフェースモジュール１３４は、特定の機能にアクセスするよう構成されるアプリケーションをリストアップするユーザインターフェース要素の表示を引き起こす。ユーザインターフェース要素はまた、その機能にアクセスするよう構成される全て又は何れかのアプリケーションについて機能を使用不可能又は可能にするための選択可能なオプションを含む。

【００２８】

実施形態において、１以上の機能は、その実施の時点でオペレーティングシステムに知られていることがある。実施形態において、オペレーティングシステムは、１以上の宣言処理を介して、サポートされる機能の組の拡張を可能にしてよい。幾つかの場合に、機能の組を増やす機能は、オペレーティングシステムに制限されてよく、一方、他の場合に、オペレーティングシステムは、第三者デバイスのような第三者プロバイダが新しい機能を宣言することを可能にしてよい（２０１１年５月２日付けでＧａｎａｐｈａｔｈｙ等によって出願された、特権的許可記録を用いてアクセス調停に関する詳細のための“BINDING APPLICATIONS TO DEVICE CAPABILITIES”と題された米国特許出願第１３／０９９２６０を参照のこと。）。

【００２９】

様々な実施形態において、デバイス機能は、総称的に、それらが実施されるデバイスに関して表される。そのような実施形態は、アプリケーションによって使用されることを認められるデバイスをユーザが選択することを可能にする。そうすることによって、ユーザは、アプリケーションがデバイスの全ての機能を使用することを承諾する。例えば、ユーザのコンピュータに接続された多機能デバイスは、ＳＭＳ機能、Ｇｅｏｌｏｃａｔｉｏｎ機能、及び携帯電話機の製造業者によって定義されるカスタム機能をサポートする携帯電話機であってよい。デバイスベースのモデルでは、ユーザは、アプリケーションがデバイスの全ての機能にアクセスすることを可能にする機会を与えられる。代替の実施形態は、ユーザがデバイスの全ての機能よりむしろデバイスの個々の機能を使用可能にすることを可能にされるように、特定の機能に関連するユーザ経験メタデータを加えるモデルを提供してよい。よって、一例において、ユーザは、アプリケーションがＧｅｏｌｏｃａｔｉｏｎ機能を除くＳＭＳ機能及びカスタム機能（例えば、製造業者がカスタム機能を記述するユーザインターフェース要素を提供していた場合）にアクセスすることを可能にするよう選択してよい。

【００３０】

アクセス調停に係る制限されない例において、ユーザは、メディアプレーヤアプリケーションを取得し、アプリケーション取得コンポーネント１２８は、オーディオ及びビデオキャプチャ、ＳＭＳ、並びに他のような、メディアプレーヤがアクセスするよう構成される機能の表示を引き起こす。それらの機能は、メディアプレーヤアプリケーションに関連するアプリケーションマニフェスト（例えば、アプリケーションマニフェスト１２２）においてリストアップされる。従って、アプリケーション取得コンポーネント１２８によって提示されるインターフェースは、ユーザが、メディアプレーヤがアクセスするよう構成される機能に少なくとも部分的に基づき、メディアプレーヤアプリケーションを取得すべきかどうかを選択することを可能にする。それらの機能は、ウェブカメラ、マイクロホン、及び／又は携帯電話機のような様々なデバイスによって提供されてよい。代替的に、それらの機能の１以上は、ユーザのコンピュータ装置で実行されるソフトウェアモジュールによって、又はウェブベースのサービスによって提供されてよい。

【００３１】

引き続き同じ、制限されない例において、ユーザは後に、ＳＭＳメッセージを介して他のユーザへプレイリストを送信するよう構成されるメディアプレーヤアプリケーションのファンクションを選択してよい。ＳＭＳメッセージング機能はユーザ承諾を必要とするとポリシー１０４が定める場合（例えば、ＳＭＳメッセージングが“細心の注意を払うべき／制限される”レベルに該当するため）は、アクセスブローカー１０２は、ユーザインターフェース承諾モジュール１２４に、メディアプレーヤアプリケーションがＳＭＳ機能にアクセスすることを可能にすると承諾するための選択可能なオプションを表示させる。承諾するための選択可能なオプションの表示はＳＭＳを介してプレイリストを送信する状況の間生じるので、ユーザは、いつメディアプレーヤがなぜＳＭＳ機能にアクセスするのかをより良く理解することができる。対照的に、アプリケーションが立ち上げられる時点で又はアプリケーションがインストールされる場合にメディアプレーヤがＳＭＳ機能にアクセスすることを可能にするようユーザがプロンプトされるか、あるいは、全くそうされない場合は、ユーザは、いつメディアプレーヤがなぜＳＭＳにアクセスするのかに関して当惑することとなる。ユーザインターフェース承諾モジュール１２４は（メディアプレーヤアプリケーションの要素よりむしろ）オペレーティングシステム要素であるから、ユーザは、メディアプレーヤアプリケーションが、ユーザの承諾、認識及び制御なしで、ＳＭＳのような潜在的に危険な機能にアクセスしないとの更なる信頼を有することができる。

【００３２】

アクセスブローカー１２０がＳＭＳ機能にアクセスするための別のアプリケーションからのその後の要求を受け取るべき場合は、メディアプレーヤアプリケーションがＳＭＳ機能にアクセスするためのユーザの以前の承諾は適用されず、アクセスブローカー１０２は、ユーザに、ＳＭＳ機能への他のアプリケーションのアクセスを承諾するようプロンプトする。メディアプレーヤアプリケーションが例えば位置特定サービスのような別の機能へのアクセスを要求すべき場合は、メディアプレーヤアプリケーションがＳＭＳ機能にアクセスすることを可能にするユーザの以前の承諾は適用されず、アクセスブローカー１０２は、ユーザに、位置特定サービスへアクセスするためのメディアプレーヤの要求を承諾するようプロンプトする。

【００３３】

更に引き続き同じ、制限されない例において、アプリケーション内機能設定モジュール１３２は、メディアプレーヤアプリケーションと相互作用する状況において、アプリケーション特有の機能設定の表示を引き起こす。ユーザは、このアプリケーション特有のビューを用いてメディアプレーヤのＳＭＳ機能アクセスを制御することができる。機能特有ユーザインターフェースモジュール１３４は、単一のリストにおいてＳＭＳ機能にアクセスすることができるメディアプレーヤアプリケーションのようなアプリケーションを見て、ユーザが望む何れか及び全てのアプリケーションに対してＳＭＳ機能アクセスをオン又はオフするオプションをユーザに提供する。よって、この詳細な説明の実施形態は、ユーザのコンピュータシステムがデバイス機能のような機能へのメディアプレーヤアプリケーションのアクセスを適切に制御しているとの更なる信頼をユーザに提供する。

【００３４】

［コンピュータ装置の例］

図２は、実施形態に従ってアクセスブローカーサービスを提供するのに使用可能なコンピュータシステムの例のブロック図である。コンピュータシステム２００は、アクセスブローカーサービスを実施することができる如何なる適切なコンピュータ装置としても構成されてよい。様々な制限されない例に従って、適切なコンピュータ装置は、パーソナルコンピュータ（ＰＣ）、サーバ、サーバファーム、データセンター、特別目的のコンピュータ、タブレットコンピュータ、ゲーム機、スマートフォン、それらの組み合わせ、又はブローカーサービスの全て又は一部を記憶及び実行することができる何らかの他のコンピュータ装置を有してよい。

【００３５】

一例の構成において、コンピュータシステム２００は１以上のプロセッサ２０２及びメ

モリ２０４を有する。コンピュータシステム２００は、様々な他のシステムとの通信を可能にする通信接続２０６を更に有してよい。コンピュータシステム２００は、プロセッサ２０２及びメモリ２０４と通信上結合されている、キーボード、マウス、ペン、音声入力装置、タッチ入力装置等のような１以上の入力装置２０８と、ディスプレイ、スピーカ、プリンタ等のような１以上の出力装置２１０とを更に有してよい。

【００３６】

メモリ２０４は、プロセッサ２０２でロード可能且つ実行可能であるプログラム命令と、それらのプログラムの実行中に生成され及び／又はそれらのプログラムとともに使用されるデータとを記憶してよい。表されている例では、メモリ２０４はオペレーティングシステム２１２を記憶する。オペレーティングシステム２１２は、コンピュータシステム２００の基本システム機能性を提供し、特に、コンピュータシステム２００の他のプログラム及びモジュールの動作を提供する。

【００３７】

メモリ２０４は、図１のアクセスブローカー１０２と同じか又は類似するアクセスブローカー２１４を有する。アクセスブローカー２１４は、図１のデバイス１１２及び１１４の一方又は両方と同じか又は類似するデバイス２１６へのアプリケーションアクセスを調停するよう構成される。

【００３８】

メモリ２０４は、図１のアプリケーションコンテナコンポーネント１０６と同じか又は類似であるアプリケーションコンテナコンポーネント２１８を有する。アプリケーションコンテナコンポーネント２１８は、デバイス１１２のようなシステムリソースへのアプリケーションアクセスを制御するセキュア実行モードを実施するよう構成される。

【００３９】

メモリ２０４は、図１のアプリケーションマニフェスト１２０と同じか又は類似であるアプリケーションマニフェスト２２０を有する。メモリ２０４は、図１のユーザインターフェース承諾モジュール１２４及びオペレーティングシステム設定モジュール１３０と夫々同じか又は類似であるユーザインターフェース承諾モジュール２２２及びオペレーティングシステム設定モジュール２２４を更に有する。ユーザインターフェース承諾モジュール２２２及びオペレーティングシステム設定モジュール２２４は、オペレーティングシステム２１２内の構成要素であってよいが、説明のために図２では別々に示されている。

【００４０】

メモリ２０４は、図１の特権的許可記録１２６と同じか又は類似である特権的許可記録２２６を有する。メモリ２０４は、図１のアプリケーション取得コンポーネント１２８と同じか又は類似であるアプリケーション取得コンポーネント２２８を更に有する。

【００４１】

［機能アクセスを調停する動作の例］

図３は、アプリケーション宣言及びユーザ承諾に基づき機能アクセスを調停する処理３００の例を示すフロー図である。コンピュータシステムのアクセスブローカーは、ブロック３０２で、コンピュータシステムに設置されているハードウェアデバイスのデバイス機能のような機能にアクセスするためのアプリケーションからの要求を受け取る。アプリケーションは、メモリ、他のアプリケーション、及び設置されているハードウェアデバイスのようなシステムリソースへのアクセスを制御するセキュア実行モードにおいて実行中であってよい。

【００４２】

アクセスブローカーは、ブロック３０４で、要求されている機能のアクセスレベルを決定するようポリシーに対するルックアップ動作を実行する。要求されている機能が“特別許可された”機能であるか又は機能が未知の機能であるとポリシーが示すとブロック３０６で決定されると、アクセスブローカーはブロック３０８で、許可記録に対するルックアップ動作を実行する。許可記録は、特別許可された機能にアクセスすることを認められるとしてデバイスドライバによって登録されているアプリケーションを含んでよい。

【００４３】
アプリケーションが要求されている機能にアクセスすることを認められるとして許可記録においてリストアップされているとブロック３１０で決定されると、アクセスブローカーはブロック３１２で、要求されている機能と相互作用するのに使用可能なハンドルをアプリケーションに提供する。アプリケーションが要求されている機能にアクセスすることを認められるとして許可記録においてリストアップされていないと決定されると、アクセスブローカーはブロック３１４で、エラーコードをアプリケーションへ返し、それによってアプリケーションの要求を拒否する（２０１１年５月２日付けでＧａｎａｐｈａｔｈｙ等によって出願された、特権的許可記録を用いてアクセス調停に関する詳細のための“BINDING APPLICATIONS TO DEVICE CAPABILITIES”と題された米国特許出願第１３／０９９２６０を参照のこと。）。
【００４４】
アクセスブローカーはブロック３１６で、要求されている機能が“宣言される”機能に該当するかどうかを決定する。宣言される機能は、機能アクセス要求がアプリケーションに対して許可されるためにその機能がアプリケーションのマニフェストに含まれることを条件とする。
【００４５】
要求されている機能が“宣言される”機能レベルに該当すると決定されると、アクセスブローカーはブロック３１８で、アプリケーションのアプリケーションマニフェストが要求されている機能の宣言を含むかどうかを決定する。その決定は、アプリケーションマニフェストに対するルックアップを含んでよく、あるいは、アプリケーションマニフェストは、アプリケーションが立ち上げられる場合又はその他の時点でアクセスブローカーポリシー（又はその他の場所）にロードされてよい。アプリケーションマニフェストが要求されている機能を宣言していると決定されると、アクセスブローカーはブロック３１２で、アプリケーションへハンドルを提供する。
【００４６】
要求されている機能が“細心の注意を払うべき／制限される”アクセスレベルに該当するとブロック３２０で決定されると、アクセスブローカーはブロック３２２で、要求されている機能にアクセスするためのアプリケーションによる以前の要求に対してユーザによる以前の承諾が存在するかどうかを決定する。実施形態において、アクセスブローカーは更に、その以前の要求がアプリケーションの同じインスタンスによって受け取られたかどうかを決定する。それがアプリケーションの新しいインスタンスである場合は、以前の承諾は無効であると見なされてよい。代替の実施形態において、アクセスブローカーポリシーは、ユーザが、以前の承諾に係るアプリケーションのインスタンスの異同にかかわらず、承諾を求めるアプリケーションの各インスタンスを承諾することを条件としてよい。以前の承諾があったと決定されると、アクセスブローカーはブロック３１２で、アプリケーションにハンドルを提供する。
【００４７】
以前の承諾がなかったと決定されると、アクセスブローカーはブロック３２４で、機能アクセス要求を承諾するための選択可能なオプションを有するオペレーティングシステムのユーザインターフェース要素の表示を引き起こす。ユーザインターフェース要素は、要求されている機能に関する情報を含む。ユーザインターフェース要素は、ユーザがアプリケーションと相互作用する状況で現れるので、ユーザは、いつアプリケーションがなぜ機能にアクセスするのかをより良く理解することができる。ブロック３２６でユーザ承諾を示す入力が受信されると、アクセスブローカーは、ブロック３１２でハンドルを提供する前に、ブロック３１８で、アプリケーションマニフェストが要求されている機能を宣言するかどうかを決定する。代替の実施形態において、アクセスブローカーは、アプリケーションマニフェストが要求されている機能を宣言するかどうかを最初に決定することなく、ハンドルを返す。更なる他の実施形態において、アクセスブローカーは、承諾ユーザインターフェースを表示させることに代えて、又はそれに加えて、アクセスが許可されるべき

かどうかを決定するための他のオペレーティングシステム要素を呼び出すよう構成されてよい。

【００４８】

要求されている機能が“常に許可”アクセスレベルに該当するとブロック３２８で決定されると、アクセスブローカーはブロック３１２で、アプリケーションにハンドルを提供する。

【００４９】

実施形態において、ポリシーは、１以上の機能が複数のアクセスレベルに該当することを示してよい。１つの制限されない例において、特定の機能は、“特別許可された”及び“宣言する”の両アクセスレベルに該当するとポリシーにおいて示されてよい。そのような場合に、アクセスブローカーは、機能にアクセスするためにアプリケーションへハンドルを提供する前に、ブロック３０８及びブロック３１８に関連するファンクションを実行してよい。図３で示される動作の厳密な順序及び流れは、本詳細な説明において又は特許請求の範囲において別なふうに示されない限り、限定であると解されるべきではない。

【００５０】

［アプリケーション内機能設定を提供する動作の例］

図４は、アプリケーション内機能インターフェース設定構成を提供する処理４００の例を示すフロー図である。アプリケーションはブロック４０２で、セキュア実行モード（例えば、アプリケーションコンテナコンポーネントによって提供される。）において実行されている。セキュア実行モードは、システムリソースへのアプリケーションのアクセスに対する制御を提供する。

【００５１】

アクセスブローカーは、アプリケーションの実行中に、ブロック４０４で、アプリケーションの機能アクセス設定を変更するための選択可能なオプションを含むアプリケーション特有のオペレーティングシステムユーザインターフェース要素を表示するコマンドを示すユーザ入力装置からの入力を受け取る。ユーザインターフェース要素はオペレーティングシステム要素であるから、ユーザは、オペレーティングシステムがデバイス機能のような機能へのアプリケーションアクセスを適切に制御しているとの確かさ及び信頼を大いに有する。

【００５２】

アプリケーション内ユーザインターフェースモジュールはブロック４０６で、アプリケーションのための機能アクセス設定を変更するコマンドを示すユーザ入力を受け取る。コマンドは、機能へのアプリケーションのアクセスを無効又は有効にするものであってよい。機能設定を変更するコマンドの受信は、アプリケーションが機能にアクセスすることを可能にするようユーザが与えていた如何なる以前の承諾も覆す。従って、アプリケーションのための機能アクセス設定のステータスはブロック４０８で、変更を反映するために、アクセスブローカーにおいて、更に機能特有オペレーティングシステム設定モジュールにおいて、更新される。幾らかの後に、アプリケーションはその特定の機能へのアクセスを要求する場合に、アクセスブローカーは、この詳細な説明内の他の場所で記載されるように、要求を拒否するか、又はユーザに承諾をプロンプトしてよい。

【００５３】

［機能に特有の設定構成を提供する動作の例］

図５は、デバイス機能に特有の設定のような、機能に特有の設定を見且つ設定するための処理５００を示すフロー図である。コンピュータシステムはブロック５０２で、オペレーティングシステム設定モジュールを立ち上げる。これは、デバイス機能設定を含む機能アクセス設定のような様々なシステム設定へのアクセスを提供する“制御パネル”タイプのインターフェースを提供してよい。

【００５４】

オペレーティングシステム設定モジュールはブロック５０４で、機能アクセス設定を見るためのユーザ入力を受け取る。これに応答して、オペレーティングシステム設定モジュ

ールはブロック５０６で、機能のリストを表示する。特定の機能はデフォルトで選択されてよい。

【００５５】

オペレーティングシステム設定モジュールはブロック５０８で、特定の機能を選択するユーザコマンドを示す入力を受け取る。この入力に応答して、オペレーティングシステム設定モジュールはブロック５１０で、選択された機能にアクセスよう構成されるアプリケーションのリストを表示する。

【００５６】

オペレーティングシステム設定モジュールはまたブロック５１２で、アプリケーションが現在機能にアクセスすることを可能にされているかどうかを示すよう、アプリケーションの隣にインジケータを表示する。アプリケーションは、以前のユーザ承諾により、アプリケーション宣言により、アプリケーションが特権的許可記録においてリストアップされているために、又はその他の理由により、機能にアクセスすることを可能にされてよい。

【００５７】

オペレーティングシステム設定モジュールはブロック５１４で、特定のアプリケーションについて機能を有効又は無効にするコマンドを示す入力を受け取る。この入力は、オペレーティングシステム設定モジュールの表示と相互作用するユーザ入力装置を介して、受信されてよい。例えば、入力は、アプリケーションが現在機能にアクセスすることを可能にされているかどうかを示すよう表示されるインジケータとのインタラクションの間に受信されてよい。インジケータの制限されない例には、２ボタンインジケータ（有効／無効、オン／オフ、又は他）、スライド制御、ノブ、又はその他の対話型インジケータがある。

【００５８】

機能アクセス設定の変更に応答して、オペレーティングシステム設定モジュールはブロック５１６で、コンピュータシステムのアクセスブローカーの更新を引き起こす。ユーザ入力がその特定のアプリケーションについて機能の無効化を示す場合は、アクセスブローカーは、この詳細な説明内の他の場所で記載されるように、その機能へのアクセスのためのアプリケーションによる更なる要求を拒否するか、又はユーザの承諾をプロンプトする。

【００５９】

図３乃至５は、様々な実施形態に従う処理の例を示すフロー図を表す。それらの処理の動作は、個々のブロックにおいて表され、それらのブロックを参照して要約される。処理は論理フロー図として表され、その夫々の動作は、ハードウェア、ソフトウェア、又はそれらの組み合わせにおいて実施され得る動作の組を表してよい。ソフトウェアとの関連で、動作は、１以上のプロセッサによって実行される場合に該１以上のプロセッサが挙げられている動作を実行することを可能にする、１以上のコンピュータ記憶媒体に記憶されたコンピュータ実行可能命令に相当する。概して、コンピュータ実行可能命令は、特定の機能を実行するか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、モジュール、コンポーネント、データ構造、等を含む。動作が記載される順序は、限定として解釈されるよう意図されず、如何なる数の記載される動作も、処理を実施するために、如何なる順序においても結合され、従属する動作に分離され、及び／又は並行して実行され得る。様々な実施形態に従う処理は、論理フロー図において表される動作の一部又は全てを含んでよい。

【００６０】

［ユーザインターフェースの例］

図６は、細心の注意を払うべきデバイス機能のような、慎重を期する機能についてのアプリケーション要求に対するユーザ承諾を取得するユーザインターフェース表示を例示する。アプリケーションインターフェース６００は、コンピュータシステムのユーザインターフェース内で実行され得る如何なるアプリケーションも表す（この場合、アプリケーション“ FooApp ”）。そのポリシーにおいて“ 細心の注意を払うべき ”として挙げられてい

る機能にアクセスするためのアプリケーションからの要求が受け取られると、アクセスブローカーは、承諾ユーザインターフェース要素６０２の表示を引き起こす。承諾ユーザインターフェース要素６０２は、アプリケーションが要求している機能の記述６０４と、要求を承諾するための選択可能なオプション（“許可”ボタン６０６）とを含む。図６で示される例では、アプリケーション“FooApp”は、位置特定機能へのアクセスを要求している。様々な実施形態において、位置特定機能は、ＧＰＳデバイスのようなコンピュータシステムのハードウェアデバイスによって提供されてよい。他の実施形態においては、位置特定機能は、コンピュータシステムのデバイス以外のウェブサービス又はその他のサービスによって提供されてよい。

【００６１】

図６で示される例では、ユーザは、要求を承諾又は拒否するよう“許可”ボタン６０６又は“拒否”ボタン６０８を選択してよい。承諾ユーザインターフェース要素６０２は、“細心の注意を払うべき”機能（本例では、位置特定サービス）にアクセスするためのアプリケーションからの要求の受信の上に且つアプリケーションとのユーザインタラクションとの関連で表示されるので、ユーザは、いつアプリケーションがなぜ位置特定サービスを使用するのかをより良く判断することができる。これは、例えば、アプリケーションに位置特定サービス機能へのハンドルを要求させたアプリケーションの何らかの機能性をユーザが起動したためであってよい。そして、ユーザは、従って、ファンクションの自身の起動を、自身が位置特定サービスのアプリケーションのアクセスを承諾するよう求められることとより良く結びつけることができる。例えば、アプリケーションは、ユーザがある位置で“チェックイン”することを可能にしてよく、それにより、ユーザの位置はソーシャルネットワーキングサイトで利用可能となる。よって、ユーザがアプリケーションの“チェックイン”ファンクションを選択する場合に、ユーザは、アプリケーションがそのアプリケーションの“チェックイン”機能性を進めるよう位置特定サービスへのアクセスを要求していると、より良く理解することができる。

【００６２】

図７は、デバイス機能を含む機能の表示を含むアプリケーション取得ユーザインターフェース表示を例示する。ユーザインターフェース表示７００は、アプリケーションを取得し、ダウンロードし、及び／又はインストールするオプションをユーザに提供するよう有効にされるアプリケーション取得サービスによって表示される。ユーザインターフェース表示７００は、アプリケーション名７０２、アプリケーションアイコングラフィック７０４、及びアプリケーションをダウンロード又は購入するための選択可能なオプション７０６のような１以上のフィーチャーを含む。ユーザインターフェース表示７００は、アプリケーションがアクセスすることを可能にされている１以上の機能を表示する機能リスト７０８を含む。機能リスト７０８は、デバイス機能と、ユーザの写真ライブラリにアクセスするファンクションのような他の非デバイス機能とを含むアプリケーションファンクションを表示してよい。機能リスト７０８は機能のサブセットしか有さなくてよい。従って、機能リスト７０８は、全ての機能のリスト７１２を見るための選択可能なオプション７１０を含む。

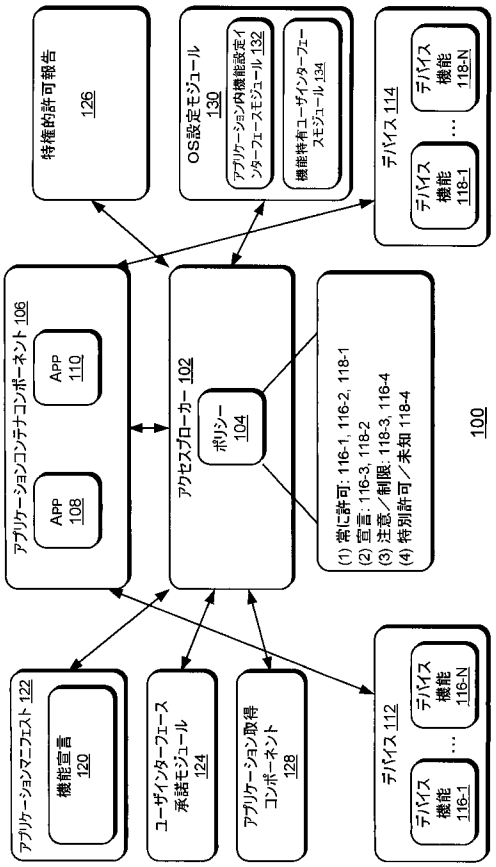
【００６３】

ユーザインターフェース表示７００は、ユーザがアプリケーションを購入し、ダウンロードし、インストールし、及び／又は実行する前に、どの機能をアプリケーションが実行することを可能にされているかをユーザがより良く判断することを可能にする。全ての機能のリスト７１２は、アプリケーションのマニフェスト（図示せず。）において宣言されており、ユーザインターフェース表示７００は、アプリケーションのマニフェストからリスト７１２を得る。幾らか後に、ユーザがアプリケーションを取得し実行した後、アプリケーションは機能へのアクセスを要求してよい。この要求はアクセスブローカーによって受信される。この詳細な説明内の他の場所で記載されるように、アクセスブローカーは、機能がアプリケーションマニフェストにおいて宣言されない限り、アプリケーションがその機能にアクセスすることを認めなくてよい。

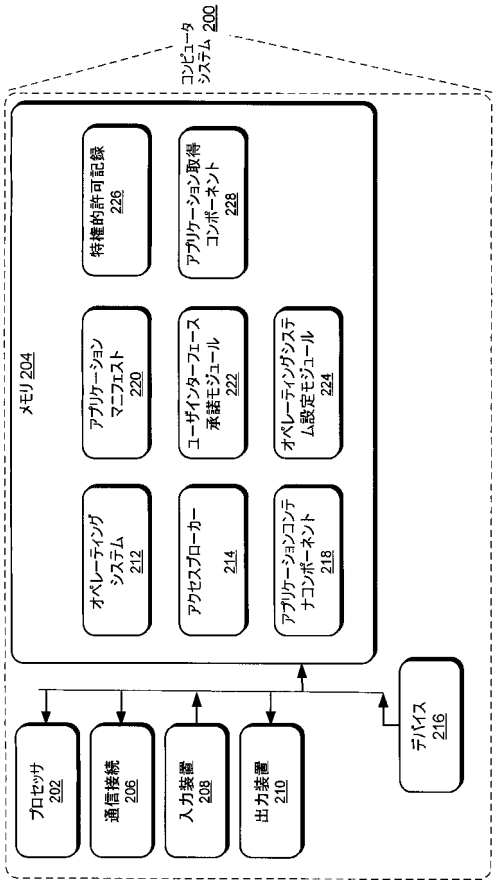
【００６４】
アプリケーションが取得される時点でアプリケーションマニフェストからデバイス機能宣言を含む機能宣言を提示し、アプリケーションがその機能へのアクセスを得るためにアプリケーションにそのマニフェストにおいて機能を宣言することを求めるポリシーを実施することは、ユーザに開示される機能と、アプリケーションが使用することを認められる機能との間の連続性を保つ。このように、アプリケーションは、ユーザから機能にアクセスするファンクションを隠すことができない。
【００６５】
図８は、アプリケーション内機能設定情報を表示するユーザインターフェース表示を例示する。アプリケーションインターフェース８００は、アプリケーション内機能設定表示ウィンドウ８０２によって部分的にオーバレイされている。アプリケーション内機能設定表示ウィンドウ８０２はオペレーティングシステムユーザインターフェースである。アプリケーション内機能設定表示ウィンドウ８０２は、機能８０４（それらの一部又は全てはデバイス機能であってよい。）を、それらの機能８０４を有効又は無効にするための選択可能な制御８０６とともにリストアップする。アプリケーション内機能設定表示ウィンドウ８０２はまた、様々なデバイス機能を含む、アプリケーションが使用又はアクセスするよう構成される様々な機能のリスト８０８を表示する。リスト８０８はアプリケーションマニフェストから取得される。
【００６６】
アプリケーション内機能設定表示ウィンドウ８０２は、アプリケーションがアクセスするよう構成される全ての機能をユーザがシングルロケーションにおいて見ることを可能にする。このように、ユーザは、この情報を見るために複数のコンフィグレーション設定ウィンドウを開く必要がない。また、アプリケーション内機能設定表示ウィンドウ８０２はアプリケーションとのインタラクションの間アクセスされ得るので、ユーザはより容易に、機能へのアプリケーションのアクセスを制御することができる。アプリケーションの設定がアプリケーション内機能設定表示ウィンドウ８０２を介して変更されると、アクセスブローカーは、その機能へのアプリケーションのアクセスの現在の状態を反映するよう更新される。
【００６７】
図９は、機能に特有の設定情報を表示するユーザインターフェース表示を例示する。オペレーティングシステム設定表示９００は、例えば、“プライバシー／デバイス承諾”設定ウィンドウ９０４において見ることができる様々な設定の選択可能なリスト９０２を含む。“プライバシー／デバイス承諾”設定ウィンドウ９０４は、機能の選択可能なリスト９０６（破線円で示される。）を含む。図９で示される例では、“ＳＭＳ”機能が現在選択されており、それにより、“ＳＭＳ”ファンクションにアクセスするよう構成される全てのアプリケーションのリスト９０８を引き起こす。例えば、“位置特定”機能が選択されるならば、異なるリストが提示され、位置特定サービスにアクセスするよう構成される全てのアプリケーションを示す（リスト９０８と同じアプリケーションを含んでも含まなくてもよい。）。リスト９０６における機能のリストは、デバイスによって、又はデバイス以外のサービスによって提供される機能を含んでよい。
【００６８】
リスト９０８におけるアプリケーションは、機能への特定のアプリケーションのアクセスを無効又は有効にするための選択可能な制御９１０の隣に提示される。“プライバシー／デバイス承諾”設定ウィンドウ９０４はまた、全てのアプリケーションについて選択された機能を有効又は無効にするよう選択可能である大域的オプション（GLOBAL）９１２（破線において示される。）を有してよい。従って、“プライバシー／デバイス承諾”設定ウィンドウ９０４は、ユーザが特定のアプリケーションについて特定の機能へのアクセスを制御するか、又は代替的に、全てのアプリケーションについてその機能をオン若しくはオフすることを可能にしてよい。アプリケーションの設定がオペレーティングシステム設定表示９００を介して変更されると、アクセスブローカーは、その機能へのアプリケーシ

ョンのアクセスの現在の状態を反映するよう更新される。
【００６９】
図６乃至９は様々なユーザインターフェースを表す。それらのユーザインターフェースは、説明のために提示され、それらの厳密なレイアウト及び内容は限定として解釈されるべきではない。代替のレイアウト及び内容が、この詳細な説明の適用範囲から逸脱することなしに使用され得る。
【００７０】
［コンピュータ可読媒体］
使用されるコンピュータ装置の構成及びタイプに依存して、図２におけるコンピュータシステム２００のメモリ２０４は、揮発性メモリ（例えば、ランダムアクセスメモリ（ＲＡＭ））及び／又は不揮発性メモリ（例えば、読み出し専用メモリ（ＲＯＭ）、フラッシュメモリ、等）を有してよい。メモリ２０４はまた、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュール及びコンピュータシステム２００のための他のデータの不揮発性ストレージを提供することができるフラッシュメモリ、磁気ストレージ、光学ストレージ、及び／又はテープストレージを含むがそれらに限られない追加のリムーバブルストレージ及び／又は非リムーバブルストレージを有してよい。
【００７１】
メモリ２０４はコンピュータ可読媒体の例である。コンピュータ可読媒体は、少なくとも２つのタイプのコンピュータ可読媒体、すなわち、コンピュータ記憶媒体及び通信媒体を含む。
【００７２】
コンピュータ記憶媒体は、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュール、及び他のデータのような情報の記憶のためのあらゆる処理又は技術においても実施される揮発性及び不揮発性の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、相変化メモリ（ＰＲＡＭ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、動的ランダムアクセスメモリ（ＤＲＡＭ）、他のタイプのランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、電気的消去可能なプログラム可能読み出し専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリ若しくは他のメモリ技術、コンパクトディスク読み出し専用メモリ（ＣＤ－ＲＯＭ）、デジタルバーサタイルディスク（ＤＶＤ）若しくは他の光学ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージ若しくは他の磁気ストレージデバイス、又はコンピュータ装置によるアクセスのために情報を記憶するのに使用され得る何らかの他の非伝送媒体を含むがそれらに限られない。
【００７３】
対照的に、通信媒体は、コンピュータにより読み出し可能な命令、データ構造、プログラムモジュール、又は他のデータを、搬送波のような変調データ信号又は他の伝送メカニズムにおいて具現してよい。本願で定義されるように、コンピュータ記憶媒体は通信媒体を含まない。
【００７４】
［結び］
本開示は、構造的な特徴及び／又は方法論的な動作に特有の言語において記載されてきたが、本発明は、必ずしも、記載される具体的な特徴又は動作に制限されないことが理解されるべきである。むしろ、具体的な特徴及び動作は、本発明を実施する例となる形態として開示される。

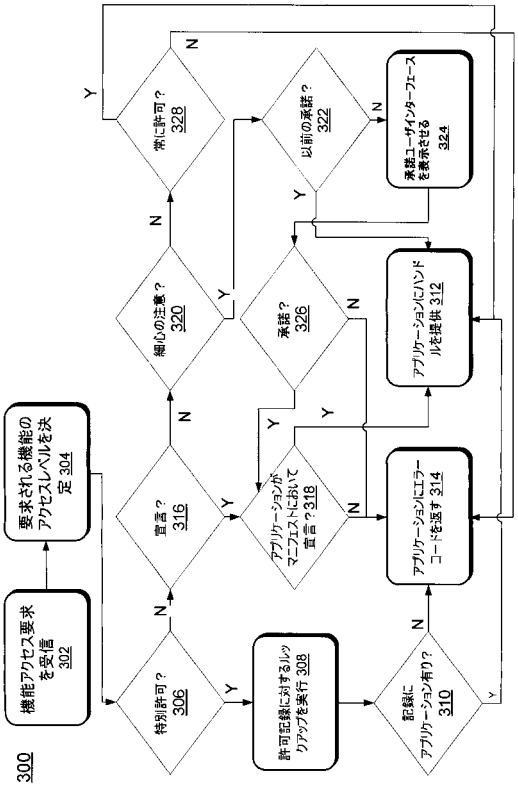
【図１】


特権的許可報告 126
OS設定モジュール 130
アプリケーション内機能設定インターフェースモジュール 132
機能特有ユーザインターフェースモジュール 134
デバイス 114
デバイス機能 118-1
デバイス機能 118-N
アプリケーションコンテナコンポーネント 106
APP 108
APP 110
アクセスブローカー 102
ポリシー 104
(1) 常に許可: 116-1, 116-2, 118-1
(2) 宣言: 116-3, 118-2
(3) 注意／制限: 118-3, 116-4
(4) 特別許可／未知 118-4
100
アプリケーションマニフェスト 122
機能宣言 120
ユーザインターフェース承諾モジュール 124
アプリケーション取得コンポーネント 128
デバイス 112
デバイス機能 116-1
デバイス機能 116-N

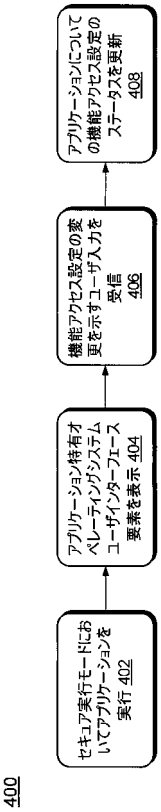
【図２】


コンピュータシステム 200
メモリ 204
オペレーティングシステム 212
アプリケーションマニフェスト 220
特権的許可記録 226
アプリケーション取得コンポーネント 228
アクセスブローカー 214
ユーザインターフェース承諾モジュール 222
オペレーティングシステム設定モジュール 224
アプリケーションコンテナコンポーネント 218
プロセッサ 202
通信接続 206
入力装置 208
出力装置 210
デバイス 216

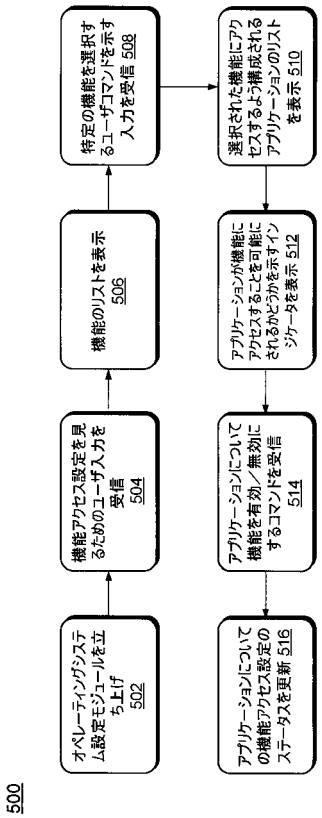
【図３】


300
機能アクセス要求を受信 302
要求される機能のアクセスレベルを決定 304
特別許可？ 306
許可記録に対するルックアップを実行 308
記録にアプリケーション有り？ 310
アプリケーションにエラーコードを返す 314
宣言？ 316
アプリケーションがマニフェストにおいて宣言？ 318
アプリケーションにハンドルを提供 312
細心の注意？ 320
承諾？ 326
以前の承諾？ 322
承諾ユーザインターフェースを表示させる 324
常に許可？ 328
Y
N

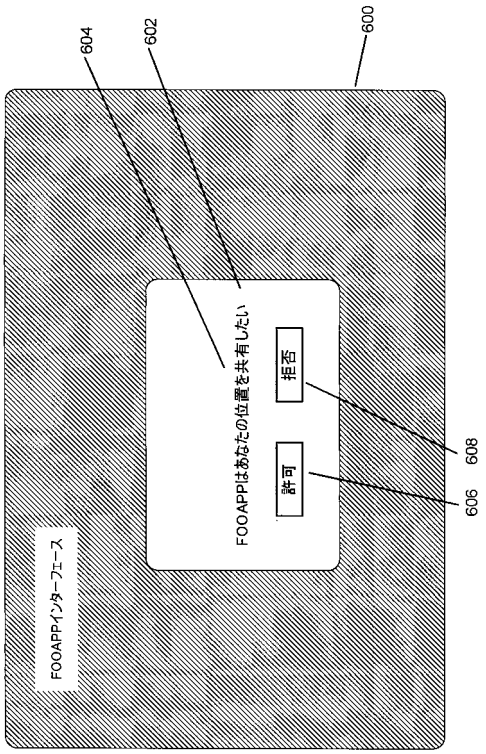
【図４】


400
セキュア実行モードにおいてアプリケーションを実行 402
アプリケーション特有オペレーティングシステムユーザインターフェース要素を表示 404
機能アクセス設定の変更を示すユーザ入力を受信 406
アプリケーションについての機能アクセス設定のステータスを更新 408

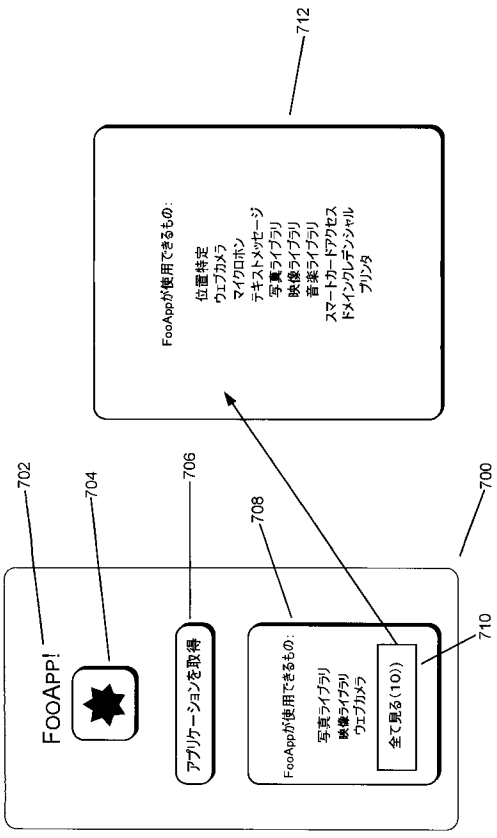
【図５】


オペレーティングシステム設定モジュールを立ち上げ 502
機能アクセス設定を見るためのユーザ入力を受信 504
機能のリストを表示 506
特定の機能を選択するユーザコマンドを示す入力を受信 508
アプリケーションについての機能アクセス設定のステータスを更新 516
アプリケーションについて機能を有効／無効にするコマンドを受信 514
アプリケーションが機能にアクセスすることを可能にされるかどうかを示すインジケータを表示 512
選択された機能にアクセスするよう構成されるアプリケーションのリストを表示 510
500

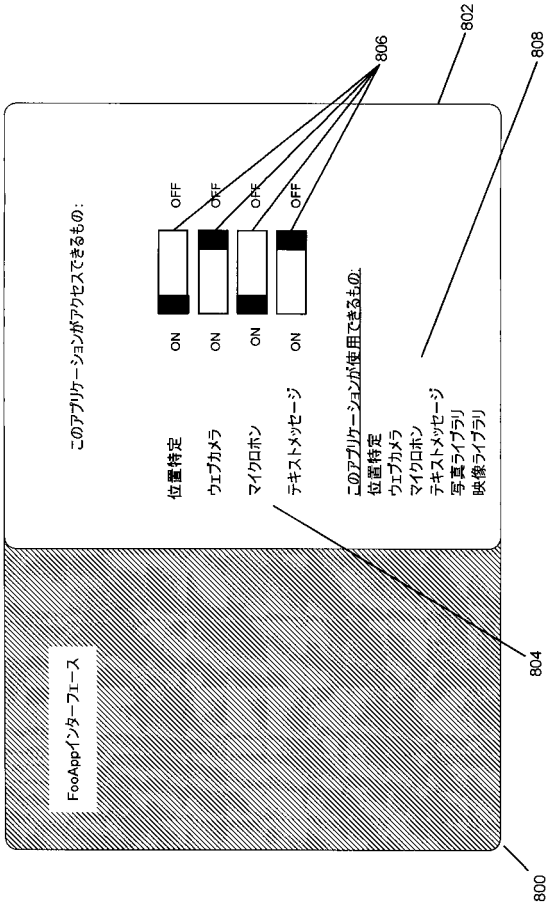
【図６】


604
602
600
FOOAPPインターフェース
FOOAPPはあなたの位置を共有したい
許可
拒否
606
608

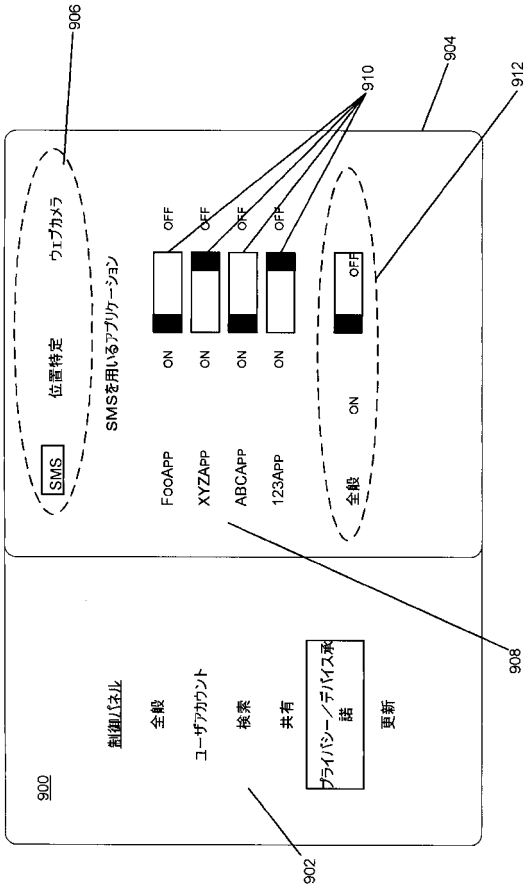
【図７】


712
FooAppが使用できるもの:
位置特定
ウェブカメラ
マイクロホン
テキストメッセージ
写真ライブラリ
映像ライブラリ
音楽ライブラリ
スマートカードアクセス
ドメインレジデンシャルプリンタ
702
704
706
708
700
710
FOOAPP!
アプリケーションを取得
FooAppが使用できるもの:
写真ライブラリ
映像ライブラリ
ウェブカメラ
全て見る(10)

【図８】


806
802
808
このアプリケーションがアクセスできるもの:
位置特定
ウェブカメラ
マイクロホン
テキストメッセージ
ON
OFF
このアプリケーションが使用できるもの:
位置特定
ウェブカメラ
マイクロホン
テキストメッセージ
写真ライブラリ
映像ライブラリ
FooAppインターフェース
804
800

【図９】


906
904
910
912
908
902
900
制御パネル
全般
ユーザアカウント
検索
共有
プライバシー／デバイス承諾
更新
SMSを用いるアプリケーション
SMS
位置特定
ウェブカメラ
FooApp
XYZApp
ABCApp
123App
全般
ON
OFF

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/055795

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/22(2006.01)i, G06F 21/20(2006.01)i, G06F 9/44(2006.01)i, G06F 3/048(2006.01)i, G06F 3/14(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/22; G06F 15/16; G06F 15/173; G06F 19/00; G06F 17/00; G06Q 30/00; G06F 17/30; H04M 1/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: access, broker, declaration, consent, application, capability, functionality, manifest, policy, display, user, interface, grant

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003-0105864 A1 (MICHAEL MULLIGAN et al.) 05 June 2003 See abstract; paragraphs [60] - [67]; figures 1-5.	1-10
A	US 2010-0325018 A1 (BORELLI STEVEN J. et al.) 23 December 2010 See abstract; paragraphs [37] - [40]; figures 1-2.	1-10
A	US 2006-0026042 A1 (CHRISTIAN AWARAJI et al.) 02 February 2006 See abstract; paragraphs [36] - [50]; figures 1-4.	1-10
A	US 2010-0112983 A1 (WALKER DAVID et al.) 06 May 2010 See abstract; paragraphs [53] - [95]; figures 2-5.	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 SEPTEMBER 2012 (20.09.2012)	**21 SEPTEMBER 2012 (21.09.2012)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Shin Sang Gil Telephone No. 82-42-481-8480

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/055795

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003-0105864 A1	05.06.2003	AU 2002-347415 A1	10.06.2003
		AU 2002-347415 A8	10.06.2003
		CN 1669014 A	14.09.2005
		CN 1669014 C0	14.09.2005
		EP 1454209 A2	08.09.2004
		EP 2397950 A1	21.12.2011
		KR 10-0561217 B1	15.03.2006
		US 2003-0095540 A1	22.05.2003
		US 2008-0140789 A1	12.06.2008
		US 7254614 B2	07.08.2007
		US 7673007 B2	02.03.2010
		WO 03-044615 A2	30.05.2003
		WO 03-044615 A3	30.05.2003
US 2010-0325018 A1	23.12.2010	AU 2002-336701 A8	12.05.2003
		US 2006-0020525 A1	26.01.2006
		US 7917394 B2	29.03.2011
		WO 03-038562 A2	08.05.2003
		WO 03-038562 A3	08.05.2003
US 2006-0026042 A1	02.02.2006	AU 2005-266922 A1	02.02.2006
		CA 2574885 A1	02.02.2006
		WO 2006-012589 A2	02.02.2006
		WO 2006-012589 A3	02.02.2006
US 2010-0112983 A1	06.05.2010	EP 1866789 A2	19.12.2007
		EP 2345205 A1	20.07.2011
		US 2006-0224742 A1	05.10.2006
		US 2010-0115581 A1	06.05.2010
		US 2010-0115582 A1	06.05.2010
		US 2011-0167470 A1	07.07.2011
		WO 2006-093917 A2	08.09.2006
		WO 2006-093917 A3	08.09.2006
		WO 2010-054258 A1	14.05.2010

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN

(72)発明者 モリス，マックス グレン
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 ガナパティー，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 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 ゴル，デイヴィッド エー
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 スリオヴィチ，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 ルーソス，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
(72)発明者 メンドンサ，ルエラ ジェイ
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

Ｆターム(参考) 5B376 AA11 AA17 FA13