(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2014-503909
(P2014-503909A)
(43)公表日　平成26年2月13日(2014.2.13)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/62 (2013.01)	G06F 21/24 163G	
	G06F 21/24 163D	

審査請求 未請求　予備審査請求 未請求　（全 17 頁）

(21)出願番号	特願2013-546268 (P2013-546268)
(86)(22)出願日	平成23年12月19日 (2011.12.19)
(85)翻訳文提出日	平成25年8月14日 (2013.8.14)
(86)国際出願番号	PCT/US2011/065707
(87)国際公開番号	WO2012/087853
(87)国際公開日	平成24年6月28日 (2012.6.28)
(31)優先権主張番号	12/972,534
(32)優先日	平成22年12月20日 (2010.12.20)
(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】改ざん防止ロケーションサービス

(57)【要約】
アクセス決定を行うためのロケーションベースのサービスおよびハードウェアを利用するセキュアロケーションシステムを、本明細書で説明する。多くのモバイルコンピューターは、ＧＰＳなどのロケーションデバイスを有する。多くのモバイルコンピューターはまた、信頼されたプラットフォームモジュール（ＴＰＭ）または他のセキュリティデバイスを有する。現在、ＧＰＳのロケーションデータは、単一のプロトコルを使用して信頼されないアプリケーションコードに直接アクセス可能となる。セキュアロケーションシステムは、特定の時間におけるコンピューターのＧＰＳのロケーションが、オペレーティングシステムのカーネルおよびＴＰＭにより認証されることが可能なセキュアなメカニズムを提供する。セキュアロケーションシステムは、行為の時間におけるコンピューティングデバイスの地理的ロケーションを示すラベルとともに、ユーザーの行為のログを記録する。セキュアロケーションシステムは、改ざんが困難でかつタイムスタンプ付きのロケーションを、カーネルモードのＧＰＳアクセスとＴＰＭセキュリティハードウェアの組み

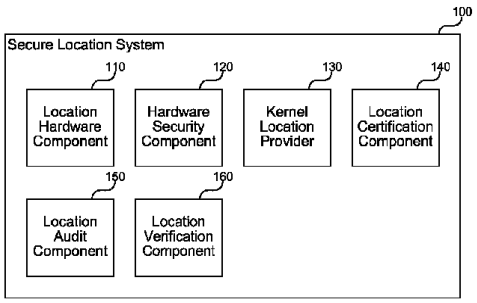


FIG. 1

【特許請求の範囲】
【請求項１】
ロケーション情報に基づいてリソースに関するアクセス権限を設定するコンピューターにより実行される方法であって、
ロケーションベースの権限情報を含むように、識別されたリソースに対する権限を更新する権限更新リクエストを受信するステップと、
前記識別されたリソースを配置するステップと、
前記識別されたリソースに関連付けられたアクセスコントロール情報を配置するステップと、
前記リクエストを伴う前記ロケーションベースの権限情報から１つまたは複数の許可された行為を判定するステップと、
前記許可されたロケーションベースの行為を含むように前記配置されたアクセスコントロール情報を更新するステップと、
前記識別されたリソースに関連付けられた、前記更新されたアクセスコントロール情報を格納することによって、前記識別されたリソースにアクセスする後続の試みが、特定のロケーションベースのアクセス情報の影響を受けることになるステップと、を備え、
前記ステップが少なくとも１つのプロセッサーにより実行されることを特徴とする方法。
【請求項２】
前記識別されたリソースは、少なくとも１つのアクセスコントロールリスト（ＡＣＬ）またはアクセスコントロールエントリー（ＡＣＥ）を含む、関連付けられたセキュリティ情報を含むオペレーティングシステムにより管理されたオブジェクトであることを特徴とする請求項１に記載の方法。
【請求項３】
前記権限更新リクエストを受信するステップは、オペレーティングシステム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）を通じてアプリケーションから前記リクエストを受信することを含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記権限更新リクエストを受信するステップは、少なくとも１つのアクセス基準として地理的ロケーションを含む、アクセスコントロール情報を受信するパスによって、前記リソースを識別する情報を受信することを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記識別されたリソースを配置するステップは、構成データベース内または構成ディレクトリー内のディスク上の前記リソースにアクセスすることと、前記リソースに関連付けられた関連するアクセスコントロールメタデータにアクセスすることとを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記アクセスコントロール情報を配置するステップは、ロケーションベースの情報を含むアクセスコントロール情報をナビゲートし、および／または修正する、オペレーティングシステム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）を呼び出すことを含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記１つまたは複数の許可された行為を判定するステップは、前記リソースが格納されたコンピューティングデバイスの地理的ロケーションに基づいて、前記リソースを読み取ることができるか、書き込むことができるか、またはリストに含めることができるかを判定することを含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記１つまたは複数の許可された行為を判定するステップは、地理的領域の１つまたは複数の特定の境界線に基づいて、前記地理的領域を判定することを含むことを特徴とする請求項１に記載の方法。

【請求項９】
前記アクセスコントロール情報を更新するステップは、前記識別されたリソースに関連した特定の行為が許可される地理的領域を示す、階層的なアクセスコントロールエントリー（ＡＣＥ）を追加することを含むことを特徴とする請求項１に記載の方法。
【請求項１０】
前記アクセスコントロール情報を更新するステップは、ロケーションベースのアクセスコントロール情報と、非ロケーションベースのアクセスコントロール情報とを組み合わせて、前記識別されたリソースにアクセスする１つまたは複数の基準を示すことを含むことを特徴とする請求項１に記載の方法。
【請求項１１】
ソフトウェアアプリケーションに対し、改ざん防止ロケーションサービスを提供するコンピューターシステムであって、
前記システムの現在の地理的ロケーションを示すハードウェア信号を提供するロケーションハードウェアコンポーネントと、
前記システム上で稼動するソフトウェアコードに対する信頼できるコンピューターの保証を提供するハードウェアセキュリティコンポーネントと、
下記のコンポーネント内で具現化されるソフトウェア命令を実行するように構成されたプロセッサーおよびメモリーと、
オペレーティングシステムのカーネルからロケーション情報を使用するユーザモードのサービスおよびアプリケーションまでのインターフェースを提供するカーネルロケーションプロバイダーと、
前記ロケーションハードウェアコンポーネントおよびハードウェアセキュリティコンポーネントからの情報によって、前記コンピューターシステムの現在のロケーションを示す認証を取り出す、ロケーション認証コンポーネントと、
前記コンピューターシステムに関連付けられたセキュアロケーションシステムの監査証跡を格納するロケーション監査コンポーネントと、
前記カーネルロケーションプロバイダーからのロケーション情報を要求し、および受信されたロケーション情報に基づいて１つまたは複数の行為を実行するロケーション照合コンポーネントと、
を備えることを特徴とするシステム。
【請求項１２】
前記ロケーションハードウェアコンポーネントは、グローバルポジショニングシステム（ＧＰＳ）信号を受信し、および前記システムのロケーション情報を判定するＧＰＳハードウェアデバイスを含むことを特徴とする請求項１１に記載のシステム。
【請求項１３】
前記ハードウェアセキュリティコンポーネントは、コンピューティングデバイスのセキュリティに関連した暗号によって照合可能な承認情報を提供する、信頼されたプラットフォームモジュール（ＴＰＭ）を含むことを特徴とする請求項１１に記載のシステム。
【請求項１４】
前記ハードウェアセキュリティコンポーネントおよび前記ロケーションハードウェアコンポーネントは、通信用のセキュアチャネルを介して接続されることを特徴とする請求項１１に記載のシステム。
【請求項１５】
前記ハードウェアセキュリティコンポーネントは、前記ロケーションハードウェアコンポーネントから前記オペレーティングシステムまでの信頼のセキュアな連鎖を生成するために、前記ロケーションハードウェアコンポーネントに関連付けられたソフトウェアドライバーに対する承認情報を照合することを特徴とする請求項１１に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は改ざん防止ロケーションサービスに関する。

【背景技術】

【０００２】

ロケーションサービスは、一般的なコンピューティングデバイスのより一般的な部分になっている。グローバルポジショニングシステム（ＧＰＳ）チップは、最初は、方位を提供する専用デバイスにおいて一般的になったが、携帯電話、携帯ゲーム機およびラップトップコンピューターにおいてより一般的になっている。コンピューターソフトウェアは、デバイスの現在のロケーションを使用して、地域の情報一覧（例えば、レストラン又は他のサービスに関する）、方位、および気象情報などの様々なサービスを提供することを始めている。一部のオペレーティングシステムを更新して、ソフトウェアアプリケーションが一貫した方法で（例えば、異なるハードウェアタイプに対する修正をすることなしに）ロケーション情報を得るように呼び出すことができるロケーションサービスアプリケーションプログラムインターフェース（ＡＰＩ）を含むようにしてきた。

【０００３】

地理的ロケーションは、単に、ユーザーが発見することに関心のある、ある種の小売店に影響を及ぼすだけではない。例えば、多くの国は、それらの国におけるデバイスに含めることができる暗号化のタイプを制限する輸出法を有する。他の国は著作権により保護されたコンテンツの輸送を制限する。したがって、ユーザーのロケーションは、どのようにユーザーを、コンピューティングデバイスを使用することを許可することに影響を及ぼす法的枠組みを変える可能性がある。

【０００４】

オペレーティングシステムは、通常、データおよびサービスへのアクセスコントロールを実施することを担当し、および、時には、どのユーザーがどの動作を実行したかを示す監査証跡を提供することが期待される。現在、アクセスコントロールの決定は、主として、ユーザー識別子（例えば、ユーザー名およびパスワード）によって大概は識別される、セキュリティプリンシパル（security principal）の考え方に基づくものであり、それ以外に基づくことはほとんどない。モバイルコンピューティングデバイスによって、データおよびサービスを、多様な地理的ロケーションにおいてアクセスすることができる。オペレーティングシステムは、現在、決定を行うのに、ロケーション情報を活用していない。特定の動作が実行されたときに、コンピューターがあるロケーションにいたことを証明することができることが望ましいという状況もあるが、今日、ロケーションサービスを、そのような例では使用しない。

【発明の概要】

【０００５】

本明細書では、アクセス決定を行うためにロケーションベースのサービスおよびハードウェアを利用するセキュアロケーションシステムを説明する。多くのモバイルコンピューターは、ＧＰＳなどのロケーションデバイスを有する。それらはまた、信頼されたプラットフォームモジュール（ＴＰＭ：trusted platform module）または他のセキュリティデバイスを有する。現在、ＧＰＳのロケーションデータは、単一のプロトコルを使用して、信頼されていないアプリケーションコードに直接アクセスが可能である。セキュアロケーションシステムは、特定の時間におけるコンピューターのＧＰＳのロケーションを、オペレーティングシステムのカーネルおよびＴＰＭにより認証することができるセキュアなメカニズムを提供する。一部の実施形態では、セキュアロケーションシステムは、動作の時間において、コンピューティングデバイスの地理的ロケーションを示すラベルとともに、ユーザーの活動を記録する。セキュアロケーションシステムは、改ざんが困難で（すなわち改ざん防止）、かつタイムスタンプ付きのロケーションを、カーネルモードのＧＰＳのアクセスとＴＰＭセキュリティハードウェアとの組み合わせを通じて提供することができる。

【０００６】

一部の実施形態では、システムは、特定の行動が特定のロケーションで発生したことを

照合するのに使用することができるセキュアな監査証跡を提供する。当該システムはまた、地理的ロケーションおよび／または時間に基づいて、アクセスコントロールの決定に対するオペレーティングシステムのサービスまたは利用を制限することができる。セキュアロケーションシステムは、ＧＰＳのハードウェアをカーネルのみによりアクセス可能にすることによって、これらの動作を実行する。ＴＰＭは、オペレーティングシステムおよびブートローダーコードが、信頼されたソースに基づくことを保証する。オペレーティングシステムは、セキュアなＧＰＳのロケーションを読み出し、およびユーザー空間プロセスに対して、認証されたＧＰＳデータ／時間データを提供する。システムは、ブートプロセスの初期から、アプリケーションによってどのようにＧＰＳ情報を提供し、および使用するかをモニタリングおよび制御するユーザプロセスの実行までの信頼の連鎖を生成する。したがって、セキュアロケーションシステムは、セキュアなロケーション情報を、承認および他のオペレーティングシステムの決定に組み込む。

【０００７】

この「発明の概要」を、下記の「発明を実施するための形態」においてさらに詳細に説明する概念の選択を簡易な形式で紹介するために提供する。この「発明の概要」は、特許請求の範囲の主要な特徴または本質的な特徴を特定することを意図するものではなく、特許請求の範囲を制限するのに使用することを意図するものでもない。

【図面の簡単な説明】

【０００８】

【図１】一実施形態における、セキュアロケーションシステムのコンポーネントを示すブロック図である。

【図２】一実施形態における、ロケーション情報に基づいてリソース権限を設定するセキュアロケーションシステムの処理を示すフローチャートである。

【図３】一実施形態における、ロケーション情報ベースのアクセス権限によりリソースにアクセスするセキュアロケーションシステムの処理を示すフローチャートである。

【発明を実施するための形態】

【０００９】

本明細書では、アクセス決定を行うためにロケーションベースのサービスおよびハードウェアを利用するセキュアロケーションシステムを説明する。例えば、オペレーティングシステムが、コンピューターの物理的なロケーションに基づいてファイルおよびサービスの異なるサブセットへのアクセスを許可すべきと考えられ、例えば、あるファイルが様々な国にあるとき、またはオフィスの外にあるときにおいて、当該ファイルに対してはアクセスを許可しない。多くのモバイルコンピューターは、ＧＰＳなどのロケーションデバイスを有する。それらはまた、信頼されたプラットフォームモジュール（ＴＰＭ：trusted platoform module）または他のセキュリティデバイスを有する。現在、ＧＰＳのロケーションデータは、単一のプロトコル（例えばＲＳ２３２またはＵＳＢ）を使用して、信頼されていないアプリケーションコードに直接アクセスが可能である。セキュアロケーションシステムは、セキュアメカニズムを提供し、当該メカニズムにより、特定の時間におけるコンピューターのＧＰＳのロケーションを、オペレーティングシステムのカーネルおよびＴＰＭにより認証してもよい。一部の実施形態では、セキュアロケーションシステムは、動作時間においてコンピューティングデバイスの地理的ロケーションを示すラベルとともにユーザーの活動を記録する。

【００１０】

セキュアロケーションシステムは、改ざんが困難で（すなわち改ざん防止）かつタイムスタンプ付きのロケーションを、カーネルモードのＧＰＳのアクセスとＴＰＭ（または同様の）セキュリティハードウェアとの組み合わせを通じて提供することができる。一部の実施形態では、システムは、特定の行動が特定のロケーションで発生したことを照合するのに使用することができるセキュアな監査証跡を提供する。当該システムはまた、地理的ロケーションおよび／または時間に基づいて（ファイルの）アクセスコントロールの決定に対するオペレーティングシステムのサービスまたは利用を制限することができる。例え

ば、会社は、コンピューターが会社の内部にあるときは、ラップトップコンピューター上のファイルの１セットへのアクセスを提供してもよいが、コンピューターを他の場所に持って行くときには、ファイルのより小さなサブセットに対するアクセスに限定してもよい。別の例として、セキュアロケーションシステムは、コンピューティングデバイスが５６ビットの暗号化の制限を許可する国にあるときに、あるタイプの暗号化（例えばセキュアなウェブページへのアクセスに対する）を使用してもよく、およびより高度なレベルの暗号化を許可する国においては、別のタイプの暗号化を使用してもよい。この例では、オペレーティングシステムのベンダーは、たとえバイナリモジュールの共有セットが各々の場所に運ばれたとしても、オペレーティングシステムがその国の法律を守ることを、各々の場所に対して承認することができる。

【００１１】

セキュアロケーションシステムは、カーネルによってのみＧＰＳハードウェアに対するアクセスを可能にすることによって、可能であれば個別の暗号化チャネルによって、これらの動作を実行する。ＴＰＭは、オペレーティングシステムおよびブートローダーコードが、信頼されたソースに基づいていることを保証する。オペレーティングシステムは、セキュアなＧＰＳのロケーションを読み出し、および認証されたＧＰＳデータ／時間データをユーザー空間のプロセスに提供する。システムは、ブートプロセスの初期から、アプリケーションによってどのようにＧＰＳの情報を提供し、および使用するかをモニタリングおよび制御するユーザプロセスの実行までの信頼の連鎖を形成する。システムは、地理的領域が埋め込まれたアクセスコントロールリストを含むように、修正されたファイル、ディレクトリー、および他のリソースのメタデータを含んでもよい。例えば、管理者は、誰が、だけではなく、どこで、（そして、いつ、さえも）ファイルがアクセス可能であるかを特定することができる。ファイルおよびディレクトリーのタイムスタンプ（ａｔｉｍｅ、ｃｔｉｍｅ、ｍｔｉｍｅ）を、地理的ロケーションを含むように増補することができる。オペレーティングシステムは、セキュアなＧＰＳのロケーションデータにより、ユーザー動作のログ（例えばＭｉｃｒｏｓｏｆｔ（登録商標） ＴＭ ＷＩＮＤＯＷＳ（登録商標）ＴＭ セキュリティイベントログ）を増補する。アプリケーションは、ロケーションの認証を読み出しおよび取得することができる。アプリケーションがファイルを読み出すときに、アプリケーションが返すデータを、ロケーションに基づいて、オペレーティングシステムにおいて、またはより高いセキュアレベルにおいて選択することができる。一部の実施形態では、セキュアロケーションシステムは、コンピューターが現在どの国／地域にあるかに基づいて、ユーザーのレベルにおいて、ファイルシステム全体の見え方を交換することができる（例えば、ステガノグラフィーファイルシステムを使用して）。したがって、セキュアロケーションシステムは、セキュアなロケーション情報を、承認および他のオペレーティングシステムの決定に組み込む。

【００１２】

図１は、一実施形態におけるセキュアロケーションシステムのコンポーネントを示すブロック図である。システム１００は、ロケーションハードウェアコンポーネント１１０と、ハードウェアセキュリティコンポーネント１２０と、カーネルロケーションプロバイダー１３０と、ロケーション認証コンポーネント１４０と、ロケーション監査コンポーネント１５０と、ロケーション照合コンポーネント１６０と、を含む。それらのコンポーネントの各々を、本明細書においてさらに詳細に説明する。

【００１３】

ロケーションハードウェアコンポーネント１１０は、システムの現在の地理的ロケーションを示すハードウェア信号を提供する。例えば、当該コンポーネント１１０は、ＧＰＳチップ、Ｗｉ－Ｆｉチップ、またはセルラーチップを含んでもよく、それらのチップは緯度座標および経度座標、緯度及び経度を導出することができる三角測量情報、または他のロケーション情報を提供する。モバイルデバイスは、ハードウェア情報と他の情報（例えば、振り当てられたインターネットプロトコル（ＩＰ）アドレス）との組み合わせを使用して、コンピューティングデバイスのおおよそのロケーションまたは正確なロケーション

を判定することができる。ロケーションハードウェアコンポーネント１１０は、ルート（root）情報を提供し、当該ルート情報からシステムのロケーションを判定する。

【００１４】

ハードウェアセキュリティコンポーネント１２０は、システム上で稼動するソフトウェアコードに対する信頼できるコンピューターの保証を提供する。当該コンポーネント１２０は、ＴＰＭ、プロセッサーのシリアル番号、信頼の暗号の連鎖、またはコンピューティングデバイスのセキュリティに関する承認情報を提供するように設計された他のハードウェアおよびソフトウェアコンポーネントを含んでいてもよい。一部のケースでは、システムは、ＴＰＭ内の鍵により暗号化及び復号化されて格納されるブートローダーコードを含んでもよい。このことにより、ＴＰＭが、ブートローダーコードが安全であり、かつ信頼できるソースに基づいていることを照合することが可能になる。一部のケースでは、鍵は、公開鍵／秘密鍵のペアの公開された部分であり、および公開鍵により復号できることは、当該コードが秘密鍵の所有者により署名されたことを示す。ブートローダーコードを復号化した後、ハードウェアセキュリティコンポーネント１２０は、同様の方法で、オペレーティングシステムのロードを継続し、実行されているコードのソースを照合してもよい。同様に、システムは、ロケーションハードウェアコンポーネント１１０に対するドライバーを照合して、それによりロケーションハードウェアからオペレーティングシステムまでの信頼のセキュアな連鎖を生成するようにしてもよい。

【００１５】

カーネルロケーションプロバイダー１３０は、オペレーティングシステムのカーネルから、ユーザーモードサービスおよびロケーション情報を使用するアプリケーションまでのインターフェースを提供する。当該インターフェースは、アプリケーションまたはオペレーティングシステムのサービスが、セキュアなロケーション情報を受信し、およびコンピューティングデバイスの現在ロケーションに基づく決定を行うように使用することができる、１つまたは複数のＡＰＩを含んでもよい。カーネルロケーションプロバイダー１３０は、共通の方法でセキュアなロケーション情報をアプリケーションおよびサービスに開示するために、ドライバー、または様々なロケーションハードウェアデバイスおよびセキュリティハードウェアデバイスと対話するほかのソフトウェアを提供するプラグ着脱可能モデルを含んでもよい。

【００１６】

ロケーション認証コンポーネント１４０は、ロケーションハードウェアコンポーネント１１０およびハードウェアセキュリティコンポーネント１２０からの現在のロケーションを示す認証を取り出す。当該認証は、コンピューティングデバイスのロケーション、および認証が生成された時間の署名されたインジケーションを含んでもよい。ハードウェアセキュリティコンポーネント１２０は、ロケーション情報のソースの署名として認証が生成されたコンピューティングデバイスに固有の鍵または他の暗号化識別子によって、認証を署名してもよい。アプリケーションは、照合可能なロケーション情報に基づいて、動作が実行されたことの証明として、認証を格納してもよい。

【００１７】

ロケーション監査コンポーネント１５０は、コンピューティングデバイスに関連付けられたセキュアなロケーション情報の監査証跡を格納する。当該コンポーネントは、様々な時刻におけるデバイスの１つまたは複数のロケーションを示す、１つまたは複数のファイル、データベースエントリー、または他の構造化データを格納してもよい。一部の実施形態では、ロケーション監査コンポーネント１５０は、アプリケーションまたはサービスがロケーション認証コンポーネント１４０にロケーション認証を要求するたびに、当該デバイスのロケーションのインジケーションを格納する。システム１００はまた、定期的にロケーション監査コンポーネント１５０に対し、ロケーションハードウェアコンポーネント１１０からのロケーション情報の取得し、および受信した情報とともに監査証跡を格納するように指示してもよい。このことにより、管理者または他のユーザーが、コンピューティングデバイスがどこに移動していたか、および、場合によっては各々のロケーションで

何の動作を実行していたかを後に照合することが可能になる。一部の実施形態では、管理者は、中央リポジトリーに監査証跡を定期的にアップロードするソフトウェアをコンピューティングデバイス上にインストールしてもよく、それによって、組織が当該組織に関連付けられたデバイスをどこで使用しており、およびどのように使用しているかを追跡することができる。システム１００はまた、例えばデバイスが定義された許容範囲のロケーション境界の外側に持ち出された場合に、ＩＴ担当者に警告または通知を提供してもよい。例えば、会社は、リリース前のコンピューティングデバイスが、試験機関または会社のビルから出ることを防止するようにしてもよい。

【００１８】

ロケーション照合コンポーネント１６０は、カーネルロケーションプロバイダー１３０に対してロケーション情報を要求し、および受信したロケーション情報に基づいて１つまたは複数の動作を実行する。コンピューティングデバイスは、当該デバイスの現在のロケーションに基づいて決定をするロケーション照合コンポーネント１６０を含む、多数のアプリケーションおよびサービスを有してもよい。例えば、ファイルシステムフィルターは、デバイスの現在のロケーションに基づいて、どのファイルにアプリケーションがアクセスすることができるかを判定してもよい。マッピングロケーションは、デバイスの現在のロケーションに基づいて、マッピングおよび他の情報を表示してもよい。オペレーティングシステムは、地域の法律に基づいて機能を有効にし、もしくは無効にしてもよく、またはデバイスのロケーションに基づいて他の制限を有効にし、もしくは無効にしてもよい。デバイスの最先のブートから、カーネル層まで実施された信頼の連鎖により、アプリケーションおよびサービスが、オペレーティングシステムから受信されたロケーション情報を信頼することが可能になる。

【００１９】

セキュアロケーションシステムが実装されたコンピューティングデバイスは、中央処理装置、メモリー、入力デバイス（例えば、キーボードおよびポインティングデバイス）、出力デバイス（例えば、ディスプレイデバイス）、ならびに記憶装置（例えば、ディスクドライブ、またはその他の不揮発性記憶媒体）を含んでもよい。メモリーおよび記憶装置は、システムを実行または有効にするコンピューター実行可能命令（例えばソフトウェア）により符号化することができるコンピューター可読記憶媒体である。加えて、データ構造およびメッセージ構造を格納してもよく、または通信リンク上の信号などのデータ伝送媒体を介して伝送してもよい。インターネット、ローカルエリアネットワーク、ワイドエリアネットワーク、ポイントツーポイントダイヤルアップ接続、および携帯電話ネットワークなどの様々な通信リンクを使用してもよい。

【００２０】

システムの実施形態を、パーソナルコンピューター、サーバーコンピューター、ハンドヘルドデバイスもしくはラップトップデバイス、マルチプロセッサーシステム、マイクロプロセッサーベースのシステム、プログラミング可能な家庭用電化製品、デジタルカメラ、ネットワークＰＣ、ミニコンピューター、メインフレームコンピューター、上述したデバイスもしくはシステムのいずれかを含む分散コンピューティング環境、セットトップボックス、およびシステムオンチップ（ＳＯＣ）などを含む、様々なオペレーティング環境において実装してもよい。当該コンピューターシステムは、携帯電話、携帯情報端末、スマートフォン、パーソナルコンピューター、プログラミング可能な家庭用電化製品、およびデジタルカメラなどであってもよい。

【００２１】

システムを、１つもしくは複数のコンピューターまたは他のデバイスによって実行されるプログラムモジュールなどのコンピューター実行可能命令の一般的なコンテキストにおいて説明してもよい。一般的には、プログラムモジュールは、特定のタスクを実行し、または特定の抽象データタイプを実装するルーチン、プログラム、オブジェクト、コンポーネント、およびデータ構造などを含む。主として、当該プログラムモジュールの機能を、様々な実施形態で求められるように、組み合わせ、または分散してもよい。

【００２２】
図２は、一実施形態における、ロケーション情報に基づいてリソース権限を設定するセキュアロケーションシステムの処理を示すフローチャートである。リソースは、ファイル、ディレクトリー、プリンター、設定項目、ユーザーアカウント、またはアクセスコントロールリスト（ＡＣＬ）もしくはアクセスコントロールエントリー（ＡＣＥ）などのセキュリティ情報を一般的に含むオペレーティングシステム内の任意の他のオブジェクトを含んでもよい。セキュアロケーションシステムは、リソースにアクセスするための権限の基準としてロケーション情報を含むようにこれらのデータ構造を拡張する。
【００２３】
ブロック２１０において開始し、システムは、権限更新リクエストを受信して、ロケーションベースの権限情報を含むように識別されたリソースに対する権限を更新する。例えば、アプリケーションは、オペレーティングシステムＡＰＩを通じてリクエストを送信してもよく、またはユーザーは、シェルプログラムもしくは他のツールに当該リクエストを投入させてもよい。当該リクエストは、パスまたは他の識別子によりリソースを識別し、ならびに少なくとも１つのアクセス基準として地理的ロケーションを含むＡＣＬおよび／またはＡＣＥなどのアクセスコントロール情報を含む。例えば、当該リクエストは、米国からのみアクセスすることができるファイルに対する権限を示してもよい。
【００２４】
続いてブロック２２０において、システムは、識別したリソースを配置する。当該リソースを、ディスク上（例えば、ファイルまたはフォルダー）、構成データベース内（例えば、レジストリーエントリ）、ディレクトリー内（例えば、アクティブディレクトリーリソース）などに格納してもよい。システムは、リソースを配置して、エントリーに関連付けられた任意の関係するアクセスコントロールメタデータを取り出す。例えば、当該リソースは、当該リソースに隣接して格納され、または当該リソースに関連付けられて格納されたレコードを含んでもよく、当該レコードは、アクセスコントロール情報を特定する。
【００２５】
続いてブロック２３０において、システムは、識別したリソースに関連付けられたアクセスコントロールリストを配置する。一部の実施形態では、システムは、既存のオペレーティングシステムＡＰＩを修正して、地理的アクセス制限に対するアクセスコントロール情報を設定しおよび取り出す。オペレーティングシステムは、一般的に、様々なタイプのリソースに関連付けられたアクセスコントロール情報をナビゲートし、および修正するために、セキュリティＡＰＩの強固なセットを含む。
【００２６】
続いてブロック２４０において、システムは、リクエストを伴うロケーションベースの権限情報から、１つまたは複数の許可された行為を判定する。当該行為は、リソースを読み取ることができるか、書き込むことができるか、およびリストに含めることができるかなどを含んでもよい。ロケーションベースの権限情報は、座標によって定義された角を有する長方形などの、境界のある地理的領域、または他の適切な領域を特定してもよい。例えば、システムは、行為が許可される地理的領域、または行為が許可されない地理的領域かを識別する中心点および当該中心点の周りの半径を受信してもよい。権限は、本質的に肯定と否定の両方であることができ、識別されたリソースに関連して許可される何らかのもの、または許可されない何らかのもののいずれかを示す。
【００２７】
続いてブロック２５０において、システムは、許可されたロケーションベースの行為を含むように、配置したアクセスコントロールリストを更新する。アクセスコントロールリストは、どのユーザーがどの行為を実行することができるかに関する権限データの階層を含むことが多く、およびシステムは、どこで行為を実行することができるかを含むようにこれらのリストを修正する。ロケーションベースのアクセスコントロール情報を、例えば、管理者が任意のロケーションでファイルを読み取ることができるが、より限定されたユーザーが特定の地理的領域内でのみファイルを読み取ることができるように、他のアクセ

スコントロール情報と組み合わせてもよい。

【００２８】

続いてブロック２６０において、システムは、識別したリソースに関連付けられた、更新したアクセスコントロールリストを格納することにより、当該識別したリソースにアクセスする後続の試みは、特定のロケーションベースのアクセス情報の影響を受ける。例えば、当該アクセスコントロールリストが、行為を実行することができる特定の領域を示す場合、システムは、アクセスを許可する前にアクセスリクエストが当該領域で発生しているかをテストする。このプロセスを、図３を参照してさらに説明する。ブロック２６０の後に、これらのステップは完了する。

【００２９】

図３は、一実施形態における、ロケーションベースのアクセス権限によってリソースへアクセスするセキュアロケーションシステムの処理を示すフローチャートである。コンピューティングシステム内のリソースは、リソースへのアクセスのための複数の基準の１つとしてのロケーション情報を含んでもよい。例えば、ファイルは、ユーザーおよびロケーションの制限を含んでもよく、それにより、特定のユーザーが特定のロケーションからのみファイルへアクセスすることができる。

【００３０】

ブロック３１０において開始し、システムは、識別したリソースにアクセスするリクエストを受信する。当該識別したリソースは、ロケーションベースのアクセス情報を含む。例えば、リソースは、ファイル、ディレクトリー、プリンター、コンピューター周辺機器、構成データベースエントリー、またはオペレーティングシステムがアクセスコントロールを定義し、および実施する他のリソースを含んでもよい。リクエストは、ファイルまたは他のリソースへアクセスするための、オペレーティングシステムのＡＰＩを呼び出すアプリケーションに基づいてもよい。リクエストは、当該リクエストに関連付けられたセキュリティプリンシパルを識別するセキュリティトークンを含む。

【００３１】

続いてブロック３２０において、システムは、ロケーション情報のセキュアソースにアクセスする。例えば、システムは、照合可能で且つ監査可能なロケーション情報インジケーションを提供する、ＧＰＳおよび／またはＴＰＭハードウェアからロケーション情報の認証をリクエストする、オペレーティングシステムのＡＰＩを起動してもよい。当該ロケーション情報インジケーションは、緯度座標および経度座標、もしくは他のロケーション情報の詳細、並びにタイムスタンプ、および当該ロケーション情報が現在のものであり、改ざんされてないことを確認する他の識別情報を含んでもよい。コンピューティングデバイスは、信頼の連鎖を生成するセキュアブートプロセスを含んでもよい。当該信頼の連鎖は、オペレーティングシステムがロケーション情報ハードウェアの制御を有すること、およびオペレーティングシステムから受信したロケーション情報に関連した出力が信頼できることを保証する。

【００３２】

続いてブロック３３０において、システムは、リクエストを受信したコンピューティングデバイスの現在の地理的ロケーションを示すロケーション情報のセキュアソースから、ロケーションの認証を受信する。当該認証は、署名、またはロケーション情報のソースの他の暗号によって照合可能なインジケーションを含んでもよい。受信側は、ＴＰＭまたは他のセキュリティハードウェアに問い合わせをして、認証において提供されたロケーション情報に改ざんが為されてないことを保証するために署名を照合してもよい。システムはまた、発行されたロケーション認証のログを生成してもよい。当該ログは、特定のロケーションにおいて実行された行為のいかなる事後調査のための監査証跡を形成する。

【００３３】

続いてブロック３４０において、システムは、受信したロケーションの認証により提供されたロケーションベースの情報を、識別したリソースに関連付けられたアクセスコントロールリストの少なくとも１つのロケーションベースの制限と比較する。例えば、アクセ

スコントロールリストは、米国外ではリソースを読み取ることができず、または書き込むことができず、ならびに米国内ではどこでも、読み取ることができ、および特定の都市内でのみ書き込むことができる、ことを規定してもよい。このことは単なる一例であり、当業者は、アクセスコントロールリストがアクセス制限の様々な組み合わせを許可して、任意の特定目的のためにリソースのアクセスを調整することを理解するであろう。

【００３４】

続いて判定ブロック３５０において、当該比較が、リソースの要求したアクセスが、現在のロケーションにおいて許可されてないことを示す場合、システムはブロック３６０に進み、そうでない場合は、システムはブロック３７０に進む。続いてブロック３６０において、システムはアクセスリクエストを拒否する。システムは、エラーメッセージまたはリクエストが拒否されたことを示す他のインジケーションを提供してもよい。一部の実施形態では、システムはリソースが存在しないかのように動作してもよく、ロケーションまたは他の制限を満たさないことに起因してアクセスが許可されないときには、リソースを事実上隠してもよい。一部の実施形態では、システムは、どの条件下でリソースをアクセスすることができるかを示すエラーメッセージを提供してもよく、それにより、例えば、ユーザーは、許可されたロケーションに前記デバイスを移動することができる。

【００３５】

続いてブロック３７０において、システムは、アクセスリクエストを許可し、およびリソースへの要求したアクセスを提供する。例えば、リソースがファイルである場合、システムは、ファイルの内容を開き、および参照するリクエストを許可してもよい。一部の実施形態では、システムは、アクセスリクエストを許可するが、デバイスの判定したロケーションに基づいてファイルデータを置き換えてもよい。例えば、システムは、デバイスがあるロケーションにあるときには、関心のないデータで満たされたファイルシステムを返してもよいが、デバイスが他のロケーションにあるときには、秘密の情報を返してもよい。ブロック３７０の後、前記ステップは完了する。

【００３６】

一部の実施形態では、セキュアロケーションシステムは、ステガノグラフィーファイルシステムの実装を容易にする。ステガノグラフィーファイルシステムは、記憶装置上のデータに対するアクセスのレイヤーを提供する。例えば、ベースレイヤーは、鍵が無くてもアクセス可能であってもよく、またはいかなるロケーションからアクセス可能であってもよく、および特にセキュリティセンシティブではないビナイン（benign）データを含んでもよい。ＴＰＭまたは他のセキュアハードウェアは、デバイスの現在のロケーションに基づいて、アクセスリクエストに応答して暗号鍵を提供してもよい。より上位レイヤーになるにしたがって、適切な鍵を持つものに対しては、センシティブなデータに対するより多くのアクセスを提供してもよい。このように、コンピューターは、あるロケーションではベナインなデータで満たされているように見え、しかし別のロケーションではセキュリティにセンシティブな情報を有してもよい。このことは、コンピューターユーザーに対し、コンピューティングデバイスが盗難にあった場合、悪意のあるユーザーが、センシティブなユーザー情報にアクセスさせないことの保証を提供することができる。

【００３７】

一部の実施形態では、セキュアロケーションシステムは、オペレーティングシステムが、システム上で稼動しているコンピューティングデバイスのロケーションに基づいて、異なる特徴を提供することを可能にする。例えば、セキュアロケーションシステムは、コンピューティングデバイスがクッキーの使用を制限している国にある場合、ウェブブラウザの中にあるクッキーをオフにしてもよい。別の例として、オペレーティングシステムは、セキュアソケットレイヤー（ＳＳＬ）に使用される暗号化のレベル、またはデバイスが使用されている場所の地域の法律に基づく他の暗号化された通信のために使用される暗号化のレベルを変更してもよい。オペレーティングシステムのベンダーは現在、特定の国において各々出荷されるオペレーティングシステムの多数の最小在庫単位（ＳＫＵ：Stock-Keeping Units）を管理する。そのようなＳＫＵの管理が困難であるだけでなく、特定の国

において特定のＳＫＵを販売しても、ある人物が非正規なＳＫＵを国の中に持ち込まないという保証はない。セキュアロケーションシステムを使用して、オペレーティングシステムのベンダーは、ＳＫＵが使用されているロケーションのセキュアな知識に基づいて、その振る舞いを自動的に修正する単一のＳＫＵを出荷することができ、複数のＳＫＵに対する必要性を削減しまたは取り除き、および管理コストを削減することができる。

【００３８】

一部の実施形態では、セキュアロケーションシステムを、ロケーションベースの決定を容易にするために組み込みデバイスに使用する。例えば、レンタカー会社は、どこで全車両における１台を運転することが許可されるかに関する地理的制限を実施するため、その全レンタル車両に当該システムを実装するデバイスを含めることができる。一部のレンタカー会社では、車に対し、ある特定の国または州を離れることを望まなくてもよく、およびこのタイプの制限を実施するために当該システムを使用することができる。他の実装形態では、会社は、他の地理的地域における使用を許可してもよいが、車両が使用された各地域に対して、異なる料金をレンタルに関して課せるように情報を記録してもよい。

【００３９】

一部の実施形態では、セキュアロケーションシステムは、様々なロケーションベースのハードウェアによって動作する。デバイスのＧＰＳチップは、今日、多くの異なるベンダーからの一般的なものであり、およびシステムを修正して、これらの各々と動作することができる。加えて、システムは、ロケーション認証の一部として捕捉することができるＧＰＳチップ毎の実質上一意な識別子を含む、ＧＰＳハードウェアを採用してもよく、ロケーション情報を提供する特定のロケーションの権限を識別する。プロセッサーおよびＴＰＭは、暗号化及び識別の目的で一意なシリアル番号を使用してきたので、それらが危険にさらされる場合、および他の理由の場合に、特定のインスタンスを禁止することができる。類似する技術を、ＧＰＳハードウェアに適用して、各ＧＰＳユニットを一意に識別し、および信頼できないインスタンスへのアクセスを拒否することができる。

【００４０】

一部の実施形態では、セキュアロケーションシステムは、ＧＰＳモジュールおよびＴＰＭなどのロケーション情報ハードウェアとセキュリティハードウェアとの間でセキュアなデータ通信チャネルを使用する。当該チャネルにより、ＴＰＭがＧＰＳチップの出力を認証すること、およびＧＰＳハードウェアとオペレーティングシステムまたはアプリケーションとの間で改ざんを防止する信頼の連鎖を保証することが可能になる、暗号化された通信を含んでもよい。一部の実施形態では、リソースへのアクセスを、ＴＰＭまたは他のセキュリティハードウェアにより管理された暗号鍵によって保護してもよく、およびＴＰＭは、ロケーション情報ハードウェアから得られたデバイスの現在のロケーションに基づいて、期限付きの鍵を配布してもよい。

【００４１】

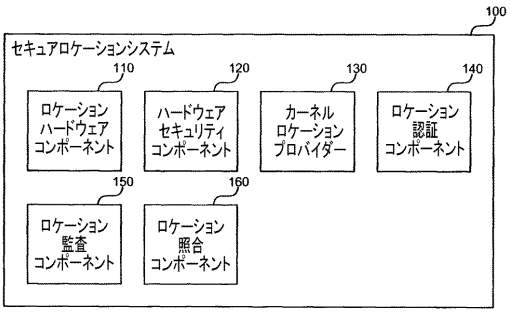
一部の実施形態では、セキュアロケーションシステムは、ロケーション情報を使用して、モバイルコンピューティングデバイス上のネットワークセキュリティポリシーを実施する。例えば、システムは、デバイスが企業のネットワークにアクセスすることができる前に、ウィルススキャンを完了すべきことを判定するために、ラップトップが最近海外にあったという情報を使用してもよい。これを行うには、ネットワークインフラストラクチャーは、最新のセキュリティチェックがもしあれば、当該セキュリティチェックが為されてからデバイスがどこにあったかという監査証跡を提供する、コンピューティングデバイス上に格納されたロケーション情報の履歴にアクセスする。システムは、入来するネットワークトラフィック、出来するネットワークトラフィックまたはその両方を制限してもよい。これらのおよび他のポリシーを、セキュアロケーションシステムにより実施することができる。

【００４２】

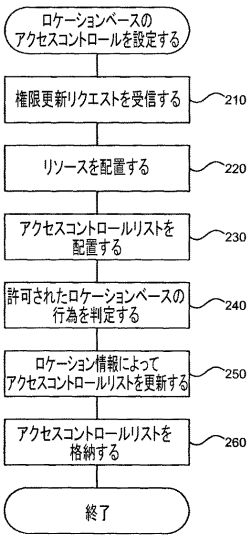
上記説明から、セキュアロケーションシステムの特定の実施形態を、本明細書において例示の目的で説明していることが理解されるであろうが、本発明の精神及び範囲から逸脱

することなしに、様々な修正を行ってもよいことが理解されるであろう。したがって、本発明は、添付の特許請求の範囲以外のものによって制限されることはない。

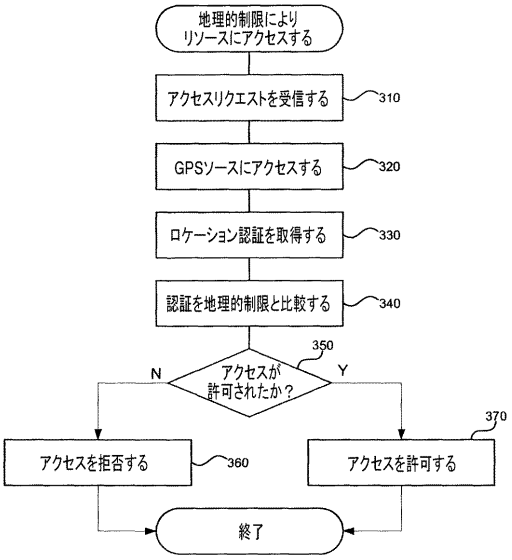
【図１】



【図２】



【図３】


地理的制限により
リソースにアクセスする
アクセスリクエストを受信する
310
GPSソースにアクセスする
320
ロケーション認証を取得する
330
認証を地理的制限と比較する
340
350
アクセスが
許可されたか？
N
Y
370
アクセスを拒否する
360
アクセスを許可する
終了

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065707

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/20(2006.01)i, H04L 9/32(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)
IPC: G06F; H04L

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: secure location system, GPS, TPM, location-based service

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7624424 B2 (YOICHIRO MORITA et al.) 24 November 2009 See col.2 lines 25-28, 36-38, col.3 lines 3-29, col.39 lines 36-42, col.43 lines 39-51, col.44 lines 10-24, 32-48, col.45 lines 15-17, 38-41, 56-59, col.58 lines 58-64 and figures 14, 15, 29, 55.	1-15
A	US 2006-0236369 A1 (MICHAEL J. COVINGTON et al.) 19 October 2006 See abstract and figures 4, 5.	1-15
A	US 7853786 B1 (DAVID FULTZ et al.) 14 December 2010 See abstract; claim 1 and figure 1.	1-15
A	US 2006-0277187 A1 (JOHN J. ROESE et al.) 07 December 2006 See abstract; claim 1 and figure 4.	1-15

☐ 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
13 SEPTEMBER 2012 (13.09.2012)	**14 SEPTEMBER 2012 (14.09.2012)**
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 Park Jin A Telephone No. 82-42-481-8536

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/065707

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7624424 B2	24.11.2009	JP 2006-012117 A	12.01.2006
		JP 4706262 B2	22.06.2011
		US 2005-0262132 A1	24.11.2005
US 2006-0236369 A1	19.10.2006	US 2006-0218621 A1	28.09.2006
US 7853786 B1	14.12.2010	None	
US 2006-0277187 A1	07.12.2006	US 2003-0217151 A1	20.11.2003
		US 7092943 B2	15.08.2006

Form PCT/ISA/210 (patent family annex) (July 2009)

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 ポール バーラム
アメリカ合衆国 ９８０５２ 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 ジョセフ エヌ．フィゲロア
アメリカ合衆国 ９８０５２ 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

【要約の続き】
合わせを介して提供することができる。このようにして、セキュアロケーションシステムは、セキュアなロケーション情報を、承認決定及び他のオペレーティングシステムの決定に組み込む。