

(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2016-533580

(P2016-533580A)

(43) 公表日 平成28年10月27日 (2016. 10. 27)

(51) Int. Cl.	F I	テーマコード (参考)
G06F 21/31 (2013.01)	G06F 21/31	Z E C
H04L 9/32 (2006.01)	H04L 9/00	5 J 1 0 4
G06F 21/62 (2013.01)	G06F 21/62	6 7 3 D

審査請求 有 予備審査請求 未請求 (全 16 頁)

(21) 出願番号	特願2016-533503 (P2016-533503)	(71) 出願人	506291542
(86) (22) 出願日	平成26年8月14日 (2014. 8. 14)		ペイパル インコーポレイテッド
(85) 翻訳文提出日	平成28年2月4日 (2016. 2. 4)		アメリカ合衆国 カリフォルニア州 95
(86) 国際出願番号	PCT/US2014/051051		131 サンノゼ ノース ファースト
(87) 国際公開番号	W02015/026622		ストリート 2211
(87) 国際公開日	平成27年2月26日 (2015. 2. 26)	(74) 代理人	100074099
(31) 優先権主張番号	13/971, 717		弁理士 大菅 義之
(32) 優先日	平成25年8月20日 (2013. 8. 20)	(74) 代理人	110000132
(33) 優先権主張国	米国 (US)		大菅内外国特許事務所特許業務法人
		(72) 発明者	ライマン, ネイト リー
			アメリカ合衆国, カリフォルニア州 95
			125, サンノゼ, ハミルトン アベニュー
			2145

最終頁に続く

(54) 【発明の名称】 位置ベースデバイスセキュリティのためのシステムおよび方法

(57) 【要約】

デバイスはデバイス周囲の環境情報を収集してもよい。収集された環境情報に基づいて、デバイスは、セキュリティリスクがより低い、潜在的に安全な位置を自動的に識別してもよい。潜在的に安全な位置が識別されると、デバイスは、安全な位置に対してセキュリティ要件を低減するセキュリティプロファイルの設定をユーザに促してもよい。デバイスは、セキュリティプロファイルを記憶し、安全な位置とセキュリティプロファイルを関連付けてもよい。デバイスは、デバイスが安全な位置内にあるとき、セキュリティ要件を低減するセキュリティプロファイルをアクティブ化してもよい。さらに、セキュリティプロファイルは、デバイスが安全な位置にあるとき、デバイスのある機能の無効化を要求してもよい。

【選択図】 図3

300

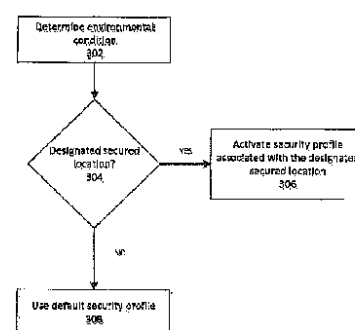


FIG. 3

【特許請求の範囲】**【請求項 1】**

デバイスのセキュリティ設定を管理するためのシステムであって、
安全な位置に対応する情報を記憶するメモリと、
前記メモリと通信する一つ以上のプロセッサであって、
前記デバイスで検出された環境情報を受信し、
前記環境情報に基づいて、前記デバイスが前記安全な位置内にあるか否かを判定し、
前記デバイスが前記安全な位置内にあるとき、前記デバイスまたは前記デバイスを使用
するサービスにアクセスするために低減した認証要件をアクティブ化する、
ように適応された一つ以上のプロセッサと、
を含む、
ことを特徴とするシステム。

10

【請求項 2】

前記一つ以上のプロセッサは、
前記低減した認証要件に基づいて低減した認証要求を作成し、
前記低減した認証要求を前記デバイスに通信し、
低減した認証応答を前記デバイスで受信し、
前記低減した認証応答を認証し、
前記低減した認証応答が認証されると、前記デバイスまたは前記デバイスを使用するサ
ービスに対するアクセスを承諾する
ようにさらに適応される、
ことを特徴とする請求項 1 に記載のシステム。

20

【請求項 3】

前記低減した認証要件は、前記デバイスが前記安全な位置内にないときよりも少ないユ
ーザ入力を要求する、
ことを特徴とする請求項 1 に記載のシステム。

【請求項 4】

前記低減した認証要件は、パスワードなしで、前記デバイスまたは前記デバイスを使用
するサービスに対する自動アクセスを許可する、
ことを特徴とする請求項 1 に記載のシステム。

30

【請求項 5】

前記安全な位置は、地理的位置に関連付けられる、
ことを特徴とする請求項 1 に記載のシステム。

【請求項 6】

前記安全な位置は、特定の通信ネットワークを前記デバイスが検出する環境条件と関連
付けられる、
ことを特徴とする請求項 1 に記載のシステム。

【請求項 7】

前記安全な位置は、前記デバイスがビーコンデバイスから送信されたビーコン信号を検
出する環境条件と関連付けられる、
ことを特徴とする請求項 1 に記載のシステム。

40

【請求項 8】

前記安全な位置は、前記デバイスが別のデバイスの近接範囲を検出する環境条件と関連
付けられる、
ことを特徴とする請求項 1 に記載のシステム。

【請求項 9】

前記一つ以上のプロセッサは、
前記環境情報に基づいて、潜在的に安全な位置を判定し、
前記潜在的に安全な位置とみなす環境条件を含む、前記潜在的に安全な位置を示す通知
を作成し、

50

前記安全な位置として、前記潜在的に安全な位置を指定するためにユーザ入力を受信する、

ようにさらに適応される、

ことを特徴とする請求項 1 に記載のシステム。

【請求項 10】

前記一つ以上のプロセッサは、

前記環境情報に基づいて安全ではない位置を判定し、

前記デバイスが前記安全ではない位置内にあるとき、前記デバイスまたは前記デバイスを使用するサービスにアクセスするための高い認証要件をアクティブ化する、

ようにさらに適応される、

ことを特徴とする請求項 1 に記載のシステム。

10

【請求項 11】

デバイスのセキュリティ設定を管理するための方法であって、

前記デバイスで検出された環境情報を受信することと、

前記環境情報に基づいて、前記デバイスが安全な位置内にあるか否かを判定することと

、

前記デバイスが前記安全な位置内にあるとき、前記デバイスまたは前記デバイスを使用するサービスにアクセスするために低減した認証要件をアクティブ化することと、

を含む、

ことを特徴とする方法。

20

【請求項 12】

前記方法は、

前記低減した認証要件に基づいて低減した認証要求を作成することと、

前記低減した認証要求を前記デバイスに通信することと、

低減した認証応答を前記デバイスで受信することと、

前記低減した認証応答を認証することと、

前記低減した認証応答が認証されると、前記デバイスまたは前記デバイスを使用するサービスに対するアクセスを承諾することと、

をさらに含む、

ことを特徴とする請求項 11 に記載の方法。

30

【請求項 13】

前記低減した認証要件は、前記デバイスが前記安全な位置内にないときよりも少ないユーザ入力を要求する、

ことを特徴とする請求項 11 に記載の方法。

【請求項 14】

前記低減した認証要件は、パスワードなしで前記デバイスまたは前記デバイスを使用するサービスに対する自動アクセスを許可する、

ことを特徴とする請求項 11 に記載の方法。

【請求項 15】

前記安全な位置は、地理的位置に関連付けられる、

ことを特徴とする請求項 11 に記載の方法。

40

【請求項 16】

前記安全な位置は、前記デバイスが特定の通信ネットワークを検出する環境条件と関連付けられる、

ことを特徴とする請求項 11 に記載の方法。

【請求項 17】

前記安全な位置は、前記デバイスがビーコンデバイスから送信されたビーコン信号を検出する環境条件と関連付けられる、

ことを特徴とする請求項 11 に記載の方法。

【請求項 18】

50

前記安全な位置は、前記デバイスが別のデバイスの近接範囲を検出する環境条件と関連付けられる、
ことを特徴とする請求項 11 に記載の方法。

【請求項 19】

前記環境情報に基づいて潜在的に安全な位置を判定することと、
前記潜在的に安全な位置とみなす環境条件を含む、前記潜在的に安全な位置を示す通知を作成することと、
前記安全な位置として、前記潜在的に安全な位置を指定するためのユーザ入力を受信することと、
をさらに含む、
ことを特徴とする請求項 11 に記載の方法。

10

【請求項 20】

前記環境情報に基づいて安全ではない位置を判定することと、
前記デバイスが前記安全ではない位置内にあるとき、前記デバイスまたは前記デバイスを使用するサービスに対するアクセスに対して、高い認証要件をアクティブ化することと、
をさらに含む、
ことを特徴とする請求項 11 に記載の方法。

【発明の詳細な説明】

20

【技術分野】

【0001】

[関連出願に対する相互参照]

本出願は、2013年8月20日に出願された米国特許出願整理番号13/971,717に対する優先権の利益を享受する権利を主張し、その全開示は、全ての目的のためにその全体において参照によって本明細書に組み入れられる。

【0002】

本発明は、概してデバイス用の位置ベース (location-based) セキュリティを実現するためのシステムおよび方法に関する。

【背景技術】

30

【0003】

インターネット上の商行為 (コマース) の拡大とともに、オンラインセキュリティは、多くのインターネットユーザに対して主要な懸念事項になりつつある。従来のユーザログイン名およびパスワードは、セキュリティを提供するために、もはや十分なものではないになっている。多くのオンラインサービスは、いまや、セキュリティ質問、追加のパスフレーズ、画像などさらなるセキュリティ機能を必要とする。さらに、さらなるセキュリティは、コンピュータおよびモバイルデバイスに対しても追加される。なぜなら、ユーザは、オンラインビジネストラランザクションを実施するためにこれらのデバイスをますます使用するようになってきているからである。さらなるセキュリティが必要となる結果、オンラインサービスまたはオンラインサービス用に使用されるデバイスにアクセスするときにより厳しい認証要求を生じる。例えば、ユーザは、デバイスまたはオンラインサービスに対するアクセスを承諾されるために、複数のパスワードまたはパスフレーズを入力することを要求されることがある。このように、ユーザがデバイスまたはオンラインサービスに対するアクセスを得ることは、ますます冗漫なことになっている。したがって、過度のセキュリティ要件が必要とされないような安全な位置 (secured location) にユーザがいるときには、デバイスまたはオンラインサービスに対するアクセスを容易に得ることを可能にするシステムまたは方法に対する必要性が存在する。

40

【図面の簡単な説明】

【0004】

【図1】一実施形態による位置ベースデバイスセキュリティ用のプロセスを実現するのに

50

好適なネットワークシステムのブロック図である。

【図 2】一実施形態により、安全な位置を指定するためのプロセスを示すフローチャートである。

【図 3】一実施形態により、セキュリティプロファイルをアクティブ化するためのプロセスを示すフローチャートである。

【図 4】一実施形態により、図 1 の一つ以上のコンポーネントを実現するために好適なコンピュータシステムのブロック図である。

【0005】

本開示の実施形態およびその利点は、以下の詳細な説明を参照することによって最良に理解される。類似の参照番号は、一つ以上の図面に図示される類似の構成要素を識別するために使用されるものであり、その図示は、本開示の実施形態を例示することを目的とするものであって、それを限定する目的のためのものではないことを理解されたい。

【発明を実施するための形態】

【0006】

一実施形態により、デバイスがよりセキュリティリスクの低い環境に入ると、デバイスは、この環境を安全な位置とするよう指定するように、ユーザに促してもよい。例えば、安全な位置は、家または職場などの高頻度に使用される位置であってもよい。ユーザが、安全な位置として環境を指定する場合、デバイスは、安全な位置とセキュリティ要件の少ないセキュリティプロファイルを関連付けてもよい。例えば、少ないセキュリティ要件は、デバイスに対するアクセス認証中に、ほとんどまたは全くパスワードを要求しないことがある。デバイスは、デバイスが安全な領域にあるときに、セキュリティ要件が少ないセキュリティプロファイルをアクティブ化してもよい。

【0007】

一実施形態により、セキュリティプロファイルは、デバイスが安全な位置にあるとき、デバイスのある機能を無効化するように要求してもよい。例えば、携帯電話のテキストメッセージ機能は、携帯電話が移動中の車内にあるときには無効化されてもよい。このように、移動中の自動車は、携帯電話によってテキストメッセージが送受信されない安全な位置であり得る。

【0008】

図 1 は、本発明の一実施形態により、位置ベースデバイスセキュリティ用のプロセスを実現するように構成されたネットワークシステム 100 のブロック図である。ネットワークシステム 100 は、種々の支払トランザクションまたはプロセスを実施するように動作する複数のサーバおよび／またはソフトウェアコンポーネントを含むか、または実装してもよい。例示的サーバは、例えば、MICROSOFT（登録商標）OS、UNIX（登録商標）OS、LINUX（登録商標）OS、または他の好適なサーバベース OS などのサーバ OS を作動するスタンドアロンおよび企業クラスサーバを含んでもよい。図 1 に示されたサーバは、他の方法で展開されてもよく、このようなサーバによって実施される動作および／または提供されるサービスは与えられた実装に対して組み合わせられてもよいし、分離されてもよく、より多数または少数のサーバによって実施されてもよいことを理解されたい。一つ以上のサーバは、同一または異なるエンティティによって作動されるか、および／または保持されてもよい。

【0009】

システム 100 は、ネットワーク 160 を介して通信するユーザデバイス 110 およびサービスプロバイダサーバ 170 を含んでもよい。サービスプロバイダサーバ 170 は、San Jose, CA の PayPal, Inc. などのオンラインサービスプロバイダによって維持されてもよい。送信者または消費者などのユーザ 105 は、サービスプロバイダサーバ 170 を使用して、業務を実施するためにユーザデバイス 110 を使用する。例えば、ユーザ 105 は、支払トランザクションを開始する、トランザクション承認要求を受信する、または要求に回答するためにユーザデバイス 110 を使用してもよい。本明細書で用いられるトランザクションとは、支払、情報の伝送、情報の表示などを含む、ユ

ーザデバイスを使用して実施される任意の好適な動作のことを称することに留意されたい。

【0010】

ユーザデバイス110およびサービスプロバイダサーバ170は、一つ以上のプロセッサ、メモリおよび本明細書で記述された種々のアプリケーション、データおよびステップを実現するために、一つ以上のコンピュータ可読媒体に記憶されたプログラムコードおよび／またはデータなどの命令を実行するための他の好適なコンポーネントを各々含んでもよい。例えば、このような命令は、メモリまたはシステム100の種々のコンポーネントの内部および／または外部および／またはネットワーク160を介してアクセス可能なデータ記憶デバイスなどの一つ以上のコンピュータ可読媒体に記憶されてもよい。

10

【0011】

ネットワーク160は、単一のネットワークとして、または複数のネットワークの組み合わせとして実装されてもよい。例えば、種々の実施形態においては、ネットワーク160は、インターネットまたは一つ以上のイントラネット、固定電話回線ネットワーク、無線ネットワークおよび／または他の好適な種類のネットワークを含んでもよい。

【0012】

ユーザデバイス110は、ネットワーク160を介して有線および／または無線通信するように構成された任意の好適なハードウェアおよびソフトウェアを使用して実現されてもよい。例えば、一実施形態においては、ユーザデバイスは、パーソナルコンピュータ（PC）、スマートフォン、パーソナルデジタルアシスタント（PDA）、ラップトップコンピュータおよび／またはApple（商標）のiPad（商標）など、データの送受信が可能な他の種類のコンピューティングデバイスとして実現されてもよい。

20

【0013】

ユーザデバイス110は、例えば、ユーザ105がネットワーク160を介して使用可能な情報を閲覧することを許可するために、簡便なインターフェイスを提供するために使用され得る一つ以上のブラウザアプリケーション115を含んでもよい。例えば、一実施形態においては、ブラウザアプリケーション115は、贈物を閲覧および購入するための贈物リストおよび／または商人（マーチャント）サイトを設定するためのユーザアカウントなど、インターネットを介して使用可能な情報を閲覧するように構成されたウェブブラウザとして実装されてもよい。ユーザデバイス110は、例えば、ユーザ105によって選択される動作に応じて、所望のタスクを実施するためのクライアント側処理を提供するために使用され得る一つ以上のツールバーアプリケーション120も含んでもよい。一実施形態においては、ツールバーアプリケーション120は、ブラウザアプリケーション115と接続して、ユーザインターフェイスを表示してもよい。

30

【0014】

ユーザデバイス110は、ユーザデバイスに所望の機能を提供するために、特定の実施形態で望まれ得るように、他のアプリケーション125をさらに含んでもよい。例えば他のアプリケーション125は、クライアント側セキュリティ機能を実装するためのセキュリティアプリケーション、ネットワーク160を介して好適なアプリケーションプログラミングインターフェイス（API）とインターフェイス接続するためのプログラマチッククライアントアプリケーションまたは他の種類のアプリケーションを含んでもよい。

40

【0015】

アプリケーション125は、ユーザが通信し、情報を伝送し、支払することを可能にし、且つ、さもなければ上述されたような支払プロバイダを通じてスマートウォレットを使用することを可能にするアプリケーションと同様に、ネットワーク160を介して電子メール、通話およびテキストをユーザ105が送受信することを可能とする電子メール、テキストメッセージおよびIMアプリケーションも含んでもよい。ユーザデバイス110は、例えば、オペレーティングシステムレジストリエントリとして、ブラウザアプリケーション115と関連付けられるクッキーとして、ユーザデバイス110のハードウェアと関連付けられる識別子として、または支払／ユーザ／デバイス認証用に使用される他の好適な識

50

別子として、実装され得る一つ以上のユーザ識別子 130 を含む。一実施形態においては、ユーザ識別子 130 は、支払プロバイダによって保持される特定のアカウントとユーザ 105 を関連付けるために、支払サービスプロバイダによって使用されてもよい。関連するインターフェイスを有する通信アプリケーション 122 は、ユーザデバイス 110 がシステム 100 内で通信することを可能とする。

【0016】

ユーザデバイス 110 は、グローバルポジショニングシステム (GPS) を介した測位データ、温度データ、高度データ、湿度データ、デバイスの動きに関するデータ、周囲音データ、カメラを介した画像データなどの環境データを収集するためのアプリケーションも含んでもよい。さらに、ジオフェンシング技術は、位置を定義するための境界を設定するために使用されてもよい。ユーザデバイス 110 は、ジオフェンシング技術を実現するデバイスから信号を検出してもよい。これらの環境データは、ユーザデバイス 110 が位置する位置または環境を決定するために使用されてもよい。

【0017】

サービスプロバイダサーバ 170 は、例えば、オンラインサービスをユーザ 105 に提供するオンラインサービスプロバイダによって維持されてもよい。この点において、サービスプロバイダサーバ 170 は、ユーザデバイス 110 でサービスを容易にするため、および情報を通信／表示するために、ネットワーク 160 を介してユーザデバイス 110 と相互作用するように構成され得る一つ以上のサービスアプリケーション 175 を含む。例えば、サービスプロバイダサーバ 170 は、支払トランザクション、銀行業務、買い物などのサービスを提供してもよい。

【0018】

サービスプロバイダサーバ 170 は、複数のユーザアカウント 180 も保持し、その各々はユーザに関連付けられたアカウント情報 185 を含んでもよい。例えば、アカウント情報 185 は、アカウント番号、パスワード、デバイス識別子、ユーザ名、電話番号、クレジットカード情報、銀行情報またはユーザ 105 によるオンライントランザクションを容易にするために使用され得る他の金融情報などの、デバイスのユーザの個人金融情報を含んでもよい。アカウント情報 185 は、ユーザまたはユーザデバイスに対するセキュリティプロファイルも含んでもよい。

【0019】

サービスアプリケーション 175 の一部または個別のセキュリティアプリケーション 190 は、サービスデータベース 195 内の処理および記憶用に、ユーザデバイスからセキュリティ情報を受信するように構成されてもよい。セキュリティアプリケーション 190 は、ユーザ 105 からのセキュリティ情報を処理して管理するための一つ以上のアプリケーションを含んでもよい。このように、セキュリティアプリケーション 190 は、ユーザまたはユーザデバイスからのセキュリティプロファイルの詳細、関連する安全な位置などを記憶してもよい。サービスアプリケーション 175 は、ユーザアカウントの設定および管理など、必要に応じて新規のアカウントを作成するのと同様、ユーザ 105 に対する存在を判定し、アカウントを管理するようにさらに構成されてもよい。

【0020】

図 2 は、一実施形態により、安全な位置を指定するためのプロセス 200 を示すフローチャートである。ステップ 202 において、ユーザデバイス 110 は、環境データを検出してもよい。例えば、ユーザデバイス 110 は、Wi-Fi 信号、Bluetooth 信号、利用可能なネットワーク、グローバルポジショニングシステム (GPS) を介した地理的位置、携帯電話信号、近接場通信 (NFC) 信号などを検出してもよい。さらに、ユーザデバイス 110 は、日付および時刻、デバイスの動き、周囲音／雑音、温度、湿度、環境光などを検出してもよい。ユーザデバイス 110 は、ユーザデバイス 110 の環境条件または位置を判定するためにこれらの環境データを検出して収集してもよい。ユーザデバイス 110 は、履歴ログに環境データを保存してもよい。このように、履歴環境データは、ユーザデバイス 110 に記憶されてもよい。一実施形態においては、ユーザデバイス 1

10

20

30

40

50

110は、サービスプロバイダサーバ170で記憶される環境データをサービスプロバイダサーバ170に送信してもよい。

【0021】

ステップ204において、ユーザデバイス110は、ユーザデバイス110が検出された環境データを使用して潜在的に安全な位置にあるか否かを判定してもよい。一実施形態においては、ユーザデバイス110は、サービスプロバイダサーバ170に検出された環境データを送信してもよい。サービスプロバイダサーバ170は、ユーザデバイス110から環境データを受信し、環境データに基づいてユーザデバイス110が潜在的に安全な位置にあるか否かを判定してもよい。家または職場など、以前にユーザデバイス110が複数回アクセスされた日常的な位置が、潜在的に安全な位置であってもよい。例えば、ユーザデバイス110は、家または職場で無線または有線ネットワークを検出し、履歴環境データに基づいて、ユーザデバイス110が無線または有線ネットワークの領域内で以前複数回アクセスされたか否かを判定してもよい。このように、ユーザデバイス110は、同一の無線または有線ネットワークが検出される家または職場などの位置が潜在的に安全な位置であると判定してもよい。サービスプロバイダが、ユーザデバイスの位置がユーザの指定した位置内にあるか否かを判定するように、ユーザは、家または職場の住所を安全な位置として指定してもよい。

【0022】

一実施形態においては、潜在的に安全な位置は、他のデバイスの近接範囲に基づいて判定されてもよい。例えば、ユーザデバイス110は、時計、プリンタ、ラップトップ、タブレットコンピュータ、眼鏡、他のウェアラブルデバイスなどのユーザの他の周辺デバイスから発されたNFC信号またはBluetoothなどの信号を検出してもよい。履歴環境データに基づいて、ユーザデバイス110は、ユーザデバイス110がこれらの周辺デバイスの近接範囲内に以前複数回アクセスしたことを判定してもよい。このように、ユーザデバイス110は、これらの周辺デバイスの近接範囲が潜在的に安全な位置を構成することを判定してもよい。一実施形態においては、ユーザデバイス110の近接範囲内にあるユーザの他のデバイスの数が増加するにつれて、ユーザデバイス110にアクセスするためのセキュリティ要件が低減することがある。

【0023】

一実施形態においては、法人サーバの管理者は、ユーザデバイス110に対する特定の安全な位置を指定してもよい。例えば、会社ビルおよび従業員の居住の地理的位置が、安全な位置として指定されてもよい。GPSセンサによって検出された地理的位置に基づいて、ユーザデバイス110は、これらの指定された安全な位置でのセキュリティ要件を減らして、アクセスを許可してもよい。さらに、関連するホテルチェーンのホテル位置などの他の位置が、会社によって安全な位置として指定されてもよい。このように、ユーザデバイス110は、会社の従業員が職務旅行でこれらのホテルに滞在するときに、関連するホテルチェーンのホテル位置でセキュリティ要件を減らしてアクセスを許可してもよい。

【0024】

一実施形態においては、映画館、病院、裁判所、航空機、礼拝所などの公共空間は、公共空間用のセキュリティプロファイルを示すWi-FiまたはBluetooth信号などの信号をブロードキャストするビーコンデバイスを有してもよい。例えば、映画館でのビーコンデバイスは、モバイルデバイスに対する通話を制限するか、または電話呼出音をバイブレートに切り替えるセキュリティプロファイル用の信号をブロードキャストしてもよい。このように、ビーコンデバイスは、この公共空間で安全な位置を示してもよい。ユーザデバイス110は、ビーコン信号を検出して、ユーザデバイス110が潜在的に安全な位置にあることを判定してもよい。

【0025】

ユーザデバイス110は、潜在的に安全な位置を判定するために、動き、音、環境光、温度などの種々のセンサによって収集された環境データを使用してもよい。例えば、ユーザデバイス110が高速で、例えば、毎時150マイル(mph)を超えた速度で移動し

10

20

30

40

50

ていることをユーザデバイス110が検出した場合、ユーザデバイス110が航空機内で離陸中であり、ユーザデバイス110が通話またはテキストングを制限するセキュリティプロファイルに関連付けられた航空機モードに変更すべきであることを、ユーザデバイス110が判定してもよい。ユーザデバイス110は、航空機モードにユーザデバイス110を切り替えることをユーザに示唆してもよい。

【0026】

ステップ204において、ユーザデバイス110またはサービスプロバイダサーバ170によって、潜在的に安全な位置が判定された後、ステップ206で、潜在的に安全な位置が検出されたことをユーザに通知するために通知が作成されてもよい。通知は、潜在的に安全な位置とみなすために使用される環境条件の記述を含んでもよい。例えば、通知は、同一ユーザに属する二つの他の周辺デバイスが潜在的に安全な位置としてみなす環境条件として、ユーザデバイスの近接範囲内にあることを示してもよい。

10

【0027】

ステップ208において、その位置を安全な位置として指定するための要求が作成されて、ユーザに対して表示されてもよい。例えば、潜在的に安全な位置は、ユーザデバイス110が、購入を行うために複数回使用された商店であってもよい。通知は、複数の購入がユーザデバイス110を使用してその商店で行われたこと、次の購入に対して使用され得るセキュリティ要件を減らすように、その商店を安全な位置としてユーザが指定したいか否か、をユーザに知らせてもよい。

【0028】

別の例においては、ユーザデバイス110は、ユーザデバイス110が映画館に入ると、映画館モードを示すビーコン信号を検出してもよい。ユーザにユーザデバイス110が映画館に現れたことをユーザに知らせて、通話を制限し、パイブレードのみのモードに切り替えるか、または電話呼出音をオフするためにユーザデバイス110に対して映画館モードを使用したいか否かを要求するために、通知が作成されて、ユーザデバイス110に表示されてもよい。

20

【0029】

ステップ210において、ユーザデバイス110は、ユーザ応答を受信し、ユーザの応答に基づいて、潜在的に安全な位置に対するセキュリティプロファイルを設定するか否かを判定してもよい。ステップ210において、潜在的に安全な位置に対するセキュリティプロファイルを設定すべきではないことをユーザ応答が示す場合、ユーザデバイス110は、ステップ216において、潜在的に安全な位置を検索し続けてもよい。例えば、プロセスは、ステップ202に戻り、環境データの収集を継続してもよい。ユーザデバイス110は、他の潜在的に安全な位置を識別するために、環境データを監視し、分析し続けてもよい。このプロセスによって、ユーザの環境、活動または習慣を探知し続け、ユーザに適切な潜在的に安全な位置をシステムまたはユーザデバイス110が示唆することを可能とする。

30

【0030】

一実施形態においては、潜在的に安全な位置が最初に安全な位置として指定されない場合、セキュリティプロファイルを設定するための通知または要求が、ユーザデバイス110が同一の潜在的に安全な位置に入る次の時間まで作成されないように、潜在的に安全な位置は、記憶されるか、フラグを付されてもよい。このように、ユーザが最初に、ある潜在的に安全な位置の指定を拒否した後、ユーザは、ユーザデバイス110が将来、その潜在的に安全な位置に入るときに、再度通知されない。

40

【0031】

ユーザ応答がステップ210において、潜在的に安全な位置として設定すべきことを示す場合、ユーザデバイス110は、ステップ212において、セキュリティプロファイルを設定するためにユーザ入力を受信してもよい。パスコードの減少、認証なしでの自動アクセス、電話使用制限などの種々のセキュリティオプションがユーザの選択のために提示されてもよい。例えば、会社のビルは、会社の発行したラップトップに対する安全な位置

50

であってもよい。会社の発行したラップトップのユーザは、会社の発行したラップトップが認証プロセスなしで、例えば、パスワードまたはID入力なしで、会社のVPNネットワークに自動的に接続されるように、会社のビルに対するセキュリティプロファイルを設定してもよい。別の例においては、ユーザは、テキストングまたは通話が移動中の自動車内で制限されるように、セキュリティプロファイルを設定してもよい。

【0032】

さらに他の例においては、平日午前7時から午前9時までのコーヒー店の位置は、安全な位置および時刻として指定されてもよい。なぜなら、ユーザは、一杯のコーヒーを購入するために、毎日平日の朝コーヒー店を訪れるからである。平日午前7時から午前9時の間のコーヒー店でユーザデバイス110を使用する支払トランザクションが、認証を必要としないように、ユーザは、この位置および時刻に対してセキュリティプロファイルを設定してもよい。

10

【0033】

ステップ214において、ユーザデバイス110は、ユーザによって設定されたセキュリティプロファイルを有する指定された安全な位置（および時刻）を記憶してもよい。一実施形態においては、サービスプロバイダサーバ170は、指定された安全な位置を記憶し、セキュリティプロファイルと関連付けてもよい。このように、ユーザデバイス110が将来指定された安全な位置を訪れたとき、適切なセキュリティプロファイルは、ユーザの簡便のために自動的にアクティブ化されてもよい。例えば、頻繁に訪れる商店において、ユーザは、ユーザデバイス110を使用して購入を行うために、例えば、部分的パスワードなど認証要件を低減してもよい。

20

【0034】

上記のプロセスを使用することによって、潜在的に安全な位置は、自動的に識別されて、ユーザに示唆されてもよい。ユーザは、安全な位置を指定し、安全な位置に対するセキュリティプロファイルを設定することが可能となる。このように、適切なセキュリティ要件または制限は、ユーザデバイス110の時刻および位置に基づいて、ユーザデバイス110に対して実現されてもよい。

【0035】

図3は、一実施形態により、セキュリティプロファイルをアクティブ化するためのプロセスを示すフローチャートである。ステップ302において、ユーザデバイス110は、環境データを監視して収集してもよい。例えば、ユーザデバイス110は、Wi-Fi信号、Bluetooth信号、NFC信号、GPS位置、デバイスの動き、温度、周囲雑音、環境光などを検出するための種々の通信デバイスまたはセンサを使用してもよい。

30

【0036】

ステップ304において、ユーザデバイス110またはサービスプロバイダサーバ170は、ユーザデバイス110が指定された安全な位置にあるか否かを判定してもよい。例えば、指定された安全な位置のプロファイルは、ユーザデバイス110またはサービスプロバイダサーバ170内に記憶されてもよい。指定された安全な位置の各プロファイルは、他のデバイスの近接範囲、地理的位置、ある信号の検出など指定された安全な位置を識別する環境条件を含んでもよい。

40

【0037】

現在の環境条件が指定された安全な位置の環境条件と一致するとき、ユーザデバイス110またはサービスプロバイダサーバ170は、ユーザデバイス110がステップ304において指定された安全な位置にあるかを判定してもよい。ステップ306において、ユーザデバイス110は、指定された安全な位置と関連付けられたセキュリティプロファイルをアクティブ化してもよい。例えば、指定された安全な位置用の環境条件である家の無線通信ネットワークが検出されると、指定された安全な位置と関連付けられたセキュリティプロファイルがアクティブ化されてもよい。家用のセキュリティプロファイルは、認証なしで全ての機密および個人的データに自動的にフルアクセスを有するためのものであってもよい。このように、ユーザは、家でユーザデバイス110を使用するときには、冗漫

50

な認証プロセスをスキップしてもよい。

【0038】

一実施形態においては、サービスプロバイダサーバ170は、ユーザデバイス110に与えられたサービス用に、指定された安全な位置と関連付けられたセキュリティプロファイルをアクティブ化してもよい。例えば、ユーザがサービスプロバイダサーバ170でユーザアカウントにアクセスを試みる場合、サービスプロバイダサーバ170は、ユーザデバイス110からユーザデバイス110で検出された環境データおよびユーザアカウントに対する識別情報を受信してもよい。サービスプロバイダサーバ170は、受信された環境データおよびユーザアカウントに関連付けられた指定された安全な位置に基づいて、ユーザデバイス110がユーザに指定された安全な位置にあるか否かを判定してもよい。その場合、サービスプロバイダサーバ170は、ユーザデバイス110用の指定された安全な位置と関連付けられたセキュリティプロファイルをアクティブ化してもよい。サービスプロバイダサーバ170は、その後、アクティブ化されたセキュリティプロファイルに基づいて、認証要件を低減して、認証要求を作成してもよい。例えば、サービスプロバイダサーバ170は、完全なパスワードの代わりに、例えば、パスワードの最初の三文字など、部分的なパスワードの入力をユーザに促す認証要求を作成してもよい。サービスプロバイダサーバ170は、認証要求に応じてユーザの応答を受信し、サービスプロバイダサーバ170でユーザアカウントと記憶されたパスワードが一致するか否かを判定してもよい。このように、認証要件を低減することによって、サービスプロバイダサーバ170にアクセスするために必要なユーザの入力を低減することができる。

10

20

【0039】

サービスプロバイダサーバ170が支払サービスプロバイダであり、安全ではない位置でユーザデバイス110を介して購入を行うために使用されるとき、サービスプロバイダサーバ170は、完全なユーザIDおよびパスワード入力をユーザに促す認証要求を作成してもよい。さらに、サービスプロバイダサーバ170は、支払トランザクション用の標準的詐欺分析を実施してもよい。一方、購入が指定された安全な位置で行われると、サービスプロバイダサーバ170は、パスワードをほとんどまたは全く必要としないで認証要求を作成してもよい。さらに、サービスプロバイダサーバ170は、指定された安全な位置内で行われる支払トランザクションに対してより軽い詐欺分析を実施してもよい。

【0040】

認証要求の少ない例は、オンラインサービスまたは、仮想プライベートネットワーク（VPN）に対する自動アクセスを含んでもよい。別の例においては、認証用のユーザIDおよびパスワードは、指定された安全な位置でユーザに対して自動的に入力されてもよい。

30

【0041】

検出された環境条件がステップ304で指定された安全な位置と関連付けられた環境位置のうちのいずれとも一致しない場合、ユーザデバイス110は、ステップ308でデフォルトセキュリティプロファイルを使用してもよい。例えば、ユーザデバイス110が新規の地理的位置にあるとき、ユーザデバイス110は、ユーザデバイス110またはユーザデバイス110を介してサービスプロバイダサーバ170に提供される他のオンラインサービスにアクセスするために、標準的認証プロセスを必要とするデフォルトのセキュリティプロファイルを使用してもよい。

40

【0042】

一実施形態においては、ユーザデバイス110が訪れたことない新規位置にあることをユーザデバイス110が検出すると、ユーザデバイス110が高いセキュリティのセキュリティプロファイルを使用してもよい。例えば、ユーザが新しい州または郡に旅行し、ユーザデバイス110を介してサービスプロバイダサーバ170を使用して銀行業務を実施することを望む場合、ユーザデバイス110は、ユーザデバイス110が新規位置を訪れたことを検出し、サービスプロバイダサーバ170は、ユーザの銀行口座に対するユーザログイン中にさらなるセキュリティ質問などの高いセキュリティ要件でセキュリティプロ

50

ファイルを使用してもよい。

【0043】

上記のプロセスを使用することによって、潜在的に安全な位置が識別され、ユーザに通知されてもよい。ユーザは、安全な位置を指定し、指定された安全な位置に対するセキュリティプロファイルを設定することが可能となってもよい。セキュリティプロファイルは、デバイスが指定された安全な位置に入ると自動的にアクティブ化されてもよい。セキュリティおよび他の設定は、デバイスが存在する位置および環境に基づいて調整されてもよい。このように、適切なセキュリティ設定は、ユーザの経験を改善するためにデバイスに対して自動的に使用されてもよい。

【0044】

図4は、本開示の一つ以上の実施形態を実現するために好適なコンピュータシステム400のブロック図である。種々の実装においては、ユーザデバイスは、ネットワークで通信することが可能なパーソナルコンピューティングデバイス（例えば、スマートフォン、コンピューティングタブレット、パーソナルコンピュータ、ラップトップ、PDA、Bluetoothデバイス、キーFOB、バッジなど）を含んでもよい。商人および／または支払プロバイダは、ネットワークで通信することが可能なネットワークコンピューティングデバイス（例えば、ネットワークサーバ）を使用してもよい。ユーザ、商人、支払プロバイダによって使用される各デバイスは、以下の方法でコンピュータシステム400として実現されてもよいことを理解されたい。

【0045】

コンピュータシステム400は、バス402またはコンピュータシステム400の種々のコンポーネント間で情報データ、信号、情報を通信するための他の通信機構を含む。コンポーネントは、キーパッド／キーボードからキーを選択すること、一つ以上のボタンまたはリンクを選択することなどのユーザ動作を処理し、バス402に対応する信号を送信する入力／出力（I/O）コンポーネント404を含む。I/Oコンポーネント404は、ディスプレイ411およびカーソル制御413（キーボード、キーパッド、マウスなど）などの出力コンポーネントも含んでもよい。任意の音声入力／出力コンポーネント405も、音声信号を変換することによってユーザが入力情報用に音声を使用することを可能とするために、含まれてもよい。音声I/Oコンポーネント405は、音声をユーザが聞くことを可能にしてもよい。送受信機またはネットワークインターフェイス406は、コンピュータシステム400と別のユーザデバイス、商人サーバまたは支払プロバイダサーバなどの他のデバイスとの間で、ネットワーク360を介して信号を送受信する。一実施形態においては、伝送は無線であるが、他の伝送媒体および方法もまた好適なことがある。マイクロコントローラ、デジタル信号プロセッサ（DSP）または他の処理コンポーネントである可能性があるプロセッサ412は、コンピュータシステム400上の表示または通信リンク418を介した他のデバイスへの伝送などの、これらの種々の信号を処理する。プロセッサ412も、クッキーまたはIPアドレスなどの情報の他のデバイスへの伝送を制御してもよい。

【0046】

コンピュータシステム400のコンポーネントは、システムメモリコンポーネント414（例えば、RAM）、スタティック記憶コンポーネント416（例えば、ROM）および／またはディスクドライブ417も含む。コンピュータシステム400は、システムメモリコンポーネント414内に含まれる一つ以上の命令シーケンスを実行することによって、プロセッサ412および他のコンポーネントによって特定の動作を実施する。論理は、コンピュータ可読媒体内にエンコードされ、コンピュータ可読媒体は、実行用のプロセッサ412に対する命令の提供に関与する任意の媒体のことを称する。このような媒体は、多くの形式をとることがあり、不揮発性媒体、揮発性媒体、伝送媒体を含むがそのいずれにも限定はされない。種々の実装においては、不揮発性媒体は、光学または磁気ディスクを含み、揮発性媒体はシステムメモリコンポーネント414などのダイナミックメモリを含み、伝送媒体は、バス402から成る有線を含む同軸ケーブル、銅線および光ファイ

10

20

30

40

50

パを含む。一実施形態においては、論理は、非一時的コンピュータ可読媒体にエンコードされる。一例においては、伝送媒体は、ラジオ波、光および赤外線データ通信中に作成されるような音波または光波の形態をとってもよい。

【0047】

コンピュータ可読媒体の幾つかの一般的形式は、例えば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープ、任意の他の磁気媒体、CD-ROM、任意の他の光学媒体、パンチカード、紙テープ、穴のパターンを有する任意の他の物理的媒体、RAM、PROM、EEPROM、FLASH-EEPROM、任意の他のメモリチップもしくはカートリッジまたはコンピュータが読み出すように適応された任意の他の媒体を含む。

10

【0048】

本開示の種々の実施形態においては、本開示を実現するための命令シーケンスの実行は、コンピュータシステム400によって実施されてもよい。本開示の種々の他の実施形態においては、通信リンク418（例えば、LAN、WLAN、PTSNおよび／または遠距離通信、モバイルおよび携帯電話ネットワークを含む種々の他の有線もしくは無線ネットワーク、）によってネットワークに結合された複数のコンピュータシステム400は、互いに協働して本開示を実現するために命令シーケンスを実行してもよい。

【0049】

適用可能な場合、本開示によって提供された種々の実施形態は、ハードウェア、ソフトウェア、またはハードウェアおよびソフトウェアの組み合わせを使用して実現されてもよい。また、適用可能な場合には、本明細書で説明された種々のハードウェアコンポーネントおよび／またはソフトウェアコンポーネントは、本開示の趣旨から逸脱することなく、ソフトウェア、ハードウェアおよび／またはその双方を含む合成コンポーネントに組み合わせられてもよい。適用可能な場合、本明細書で説明された種々のハードウェアコンポーネントおよび／またはソフトウェアコンポーネントは、本開示の範囲から逸脱することなく、ソフトウェア、ハードウェアまたはその双方を含むサブコンポーネントに分離されてもよい。さらに、適用可能な場合、ソフトウェアコンポーネントは、ハードウェアコンポーネントとして実装されてもよく、その逆でもよいと考えられる。

20

【0050】

プログラムコードおよび／またはデータなどの、本開示に従うソフトウェアは、一つ以上のコンピュータ可読媒体上に記憶されてもよい。本明細書で識別されるソフトウェアは、一つ以上の汎用または専用コンピュータおよび／またはコンピュータシステム、ネットワークおよび／またはその他を使用して実現されてもよいことを考慮されたい。適用可能な場合、本明細書で記述される種々のステップの順序は、本明細書で記述された特徴を提供するために、変更されてもよいし、合成ステップに組み合わせられてもよいし、および／またはサブステップに分離されてもよい。

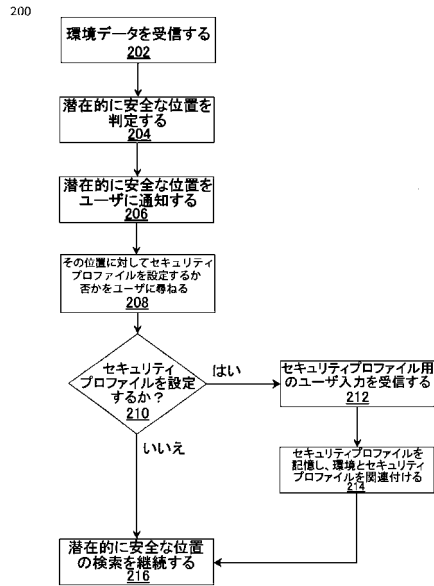
30

【0051】

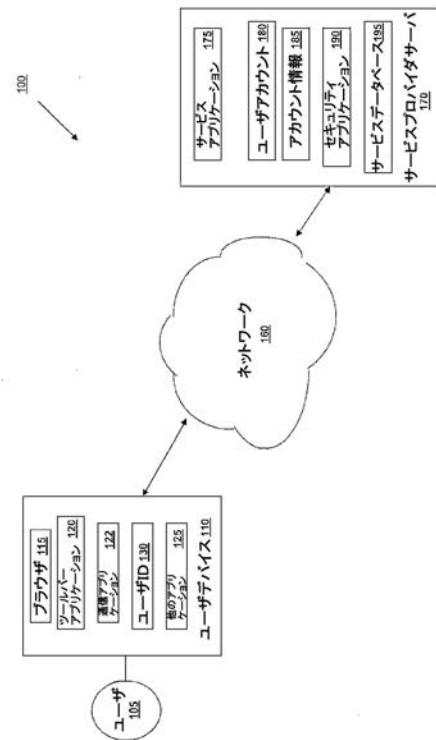
前述の開示は、開示された詳細な形態または特定の利用分野に本開示を限定することを意図するものではない。このように、本開示に対する種々の代替的实施形態および／または改変は、本明細書で明白に記述されるかまたは暗示されるかに関わらず、本開示に照らして可能であると考えられる。本開示の実施形態をこのように記述すると、本開示の範囲から逸脱することなく、形態および詳細に対して変更が行われてもよいことを当業者は理解するであろう。したがって、本開示は請求項によってのみ限定される。

40

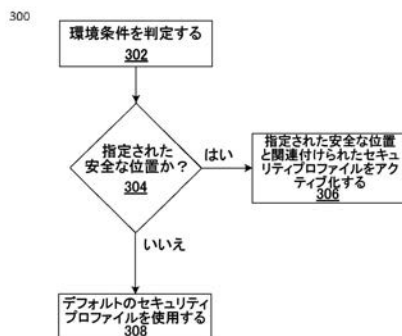
【図 2】



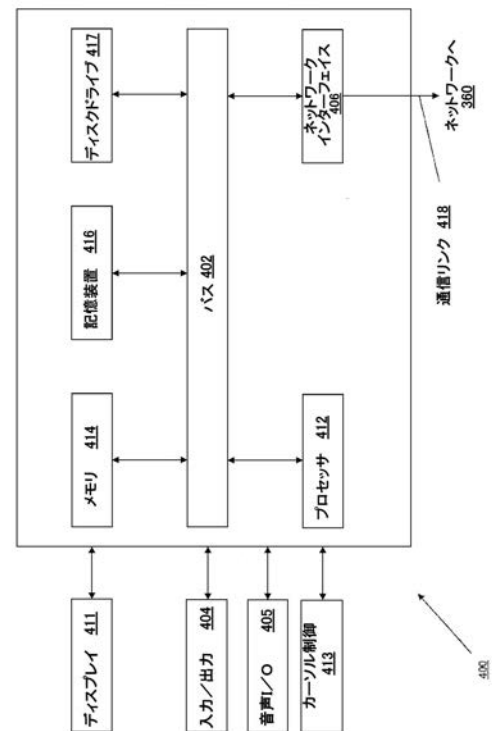
【図 1】



【図 3】



【図 4】



【国際調査報告】

INTERNATIONAL SEARCH REPORT		International application no. PCT/US 14/51051												
A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F 17/00 (2014.01) CPC - H04L 63/20 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(8): G06F 17/00 (2014.01) CPC: H04L 63/20 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched USPC: 455/456.1 or 455/456.3 or 726/1 or 726/2 or 726/3 IPC(8): G06F 17/00 (2014.01) CPC: H04L 63/20 or H04L 63/102 or G06F 21/8218 or G06F 21/604 or H04L 63/027 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Patbase; Google Scholar; Google Patents; secure, restricted, location, area, environment, sound, noise, audio, GPS, authentication, authorization, validation, device, phone, reduce, lower														
C. DOCUMENTS CONSIDERED TO BE RELEVANT <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>US 8,302,152 B1 (Hewinson) 30 October 2012 (30.10.2012) entire document (especially col. 4, ln 15-27; col. 5, ln 15-50; col. 5, ln 58 to col. 6, ln 3; col. 6, ln 10-14)</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>US 2012/0304310 A1 (Blaisdell) 29 November 2012 (29.11.2012) (para [0028], [0044])</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>US 8,229,463 B2 (Feren et al.) 24 July 2012 (24.07.2012) (col. 2, ln 10-21)</td> <td>7, 17</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	Y	US 8,302,152 B1 (Hewinson) 30 October 2012 (30.10.2012) entire document (especially col. 4, ln 15-27; col. 5, ln 15-50; col. 5, ln 58 to col. 6, ln 3; col. 6, ln 10-14)	1-20	Y	US 2012/0304310 A1 (Blaisdell) 29 November 2012 (29.11.2012) (para [0028], [0044])	1-20	Y	US 8,229,463 B2 (Feren et al.) 24 July 2012 (24.07.2012) (col. 2, ln 10-21)	7, 17
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.												
Y	US 8,302,152 B1 (Hewinson) 30 October 2012 (30.10.2012) entire document (especially col. 4, ln 15-27; col. 5, ln 15-50; col. 5, ln 58 to col. 6, ln 3; col. 6, ln 10-14)	1-20												
Y	US 2012/0304310 A1 (Blaisdell) 29 November 2012 (29.11.2012) (para [0028], [0044])	1-20												
Y	US 8,229,463 B2 (Feren et al.) 24 July 2012 (24.07.2012) (col. 2, ln 10-21)	7, 17												
☐ Further documents are listed in the continuation of Box C. ☐														
* 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 another 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 13 November 2014 (13.11.2014)		Date of mailing of the international search report 08 DEC 2014												
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774												

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, 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, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(特許庁注：以下のものは登録商標)

1. BLUETOOTH

(72)発明者 キャンプ, ロイ レオン
アメリカ合衆国, カリフォルニア州 9 5 1 2 5, サンノゼ, ハミルトン アベニュー 2 1 4 5
(72)発明者 ファラーロ, エリック ジョン
アメリカ合衆国, カリフォルニア州 9 5 1 2 5, サンノゼ, ハミルトン アベニュー 2 1 4 5
(72)発明者 タップレイ, ジョン リチャード
アメリカ合衆国, カリフォルニア州 9 5 1 2 5, サンノゼ, ハミルトン アベニュー 2 1 4 5
Fターム(参考) 5J104 AA07 KA01 KA20