

(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2017-538180

(P2017-538180A)

(43) 公表日 平成29年12月21日 (2017. 12. 21)

|                             |            |             |
|-----------------------------|------------|-------------|
| (51) Int. Cl.               | F I        | テーマコード (参考) |
| <b>G06F 21/31 (2013.01)</b> | G06F 21/31 | 5 K 1 2 7   |
| <b>H04M 1/00 (2006.01)</b>  | H04M 1/00  | R           |
| <b>H04M 1/67 (2006.01)</b>  | H04M 1/67  |             |

審査請求 未請求 予備審査請求 有 (全 25 頁)

|               |                              |          |                     |
|---------------|------------------------------|----------|---------------------|
| (21) 出願番号     | 特願2017-515104 (P2017-515104) | (71) 出願人 | 507364838           |
| (86) (22) 出願日 | 平成27年8月28日 (2015. 8. 28)     |          | クアルコム, インコーポレイテッド   |
| (85) 翻訳文提出日   | 平成29年3月17日 (2017. 3. 17)     |          | アメリカ合衆国 カリフォルニア 921 |
| (86) 国際出願番号   | PCT/US2015/047578            |          | 21 サン ディエゴ モアハウス ドラ |
| (87) 国際公開番号   | W02016/048583                |          | イブ 5775             |
| (87) 国際公開日    | 平成28年3月31日 (2016. 3. 31)     | (74) 代理人 | 100108453           |
| (31) 優先権主張番号  | 14/494, 543                  |          | 弁理士 村山 靖彦           |
| (32) 優先日      | 平成26年9月23日 (2014. 9. 23)     | (74) 代理人 | 100163522           |
| (33) 優先権主張国   | 米国 (US)                      |          | 弁理士 黒田 晋平           |
|               |                              | (72) 発明者 | ロバート・ターツ            |
|               |                              |          | アメリカ合衆国・カリフォルニア・921 |
|               |                              |          | 21-1714・サン・ディエゴ・モアハ |
|               |                              |          | ウス・ドライブ・5775        |

最終頁に続く

(54) 【発明の名称】 センサー入力に基づくスケーラブル認証プロセス選択

## (57) 【要約】

センサー入力およびモバイルデバイス機能に基づいて認証プロセスを選択するモバイルデバイスが開示される。モバイルデバイスは、複数のセンサーと、プロセッサとを含み得る。プロセッサは、アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定し、複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択し、認証プロセスを実行するように構成され得る。

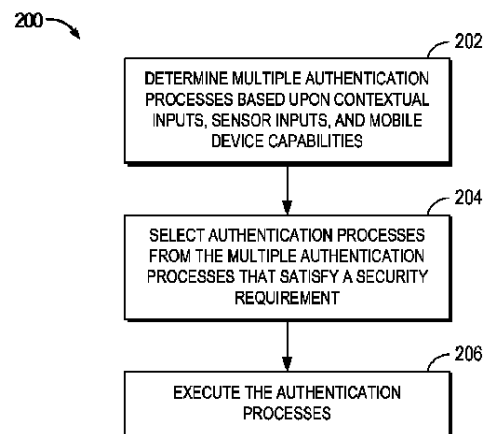


FIG. 2

**【特許請求の範囲】****【請求項 1】**

複数のセンサーと、  
プロセッサと

を備えるモバイルデバイスであって、前記プロセッサが、

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定し、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択し、  
前記認証プロセスを実行するように構成される、モバイルデバイス。

10

**【請求項 2】**

前記プロセッサが、コンテキスト入力に基づいてリスクインデックスを決定するようにさらに構成される、請求項1に記載のモバイルデバイス。

**【請求項 3】**

前記プロセッサが、前記センサー入力に基づいて信用インデックスを決定するようにさらに構成される、請求項2に記載のモバイルデバイス。

**【請求項 4】**

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件を満たされる、請求項3に記載のモバイルデバイス。

**【請求項 5】**

認証プロセスがユーザ定義される、請求項1に記載のモバイルデバイス。

20

**【請求項 6】**

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定するステップと、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択するステップと、

前記認証プロセスを実行するステップと

を含む方法。

**【請求項 7】**

コンテキスト入力に基づいてリスクインデックスを決定するステップをさらに含む、請求項6に記載の方法。

30

**【請求項 8】**

前記センサー入力に基づいて信用インデックスを決定するステップをさらに含む、請求項7に記載の方法。

**【請求項 9】**

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件を満たされる、請求項8に記載の方法。

**【請求項 10】**

認証プロセスがユーザ定義される、請求項6に記載の方法。

40

**【請求項 11】**

プロセッサによって実行されたとき、前記プロセッサに、

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定させ、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択させ、  
前記認証プロセスを実行させる

コードを含む非一時的コンピュータ可読媒体。

**【請求項 12】**

コンテキスト入力に基づいてリスクインデックスを決定するためのコードをさらに含む

50

請求項11に記載のコンピュータ可読媒体。

【請求項 13】

前記センサー入力に基づいて信用インデックスを決定するためのコードをさらに含む請求項12に記載のコンピュータ可読媒体。

【請求項 14】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされる、請求項13に記載のコンピュータ可読媒体。

【請求項 15】

ユーザ定義された認証プロセスを可能にするためのコードをさらに含む請求項11に記載のコンピュータ可読媒体。

【請求項 16】

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定するための手段と、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択するための手段と、

前記認証プロセスを実行するための手段と

を備えるモバイルデバイス。

【請求項 17】

コンテキスト入力に基づいてリスクインデックスを決定するための手段をさらに備える請求項16に記載のモバイルデバイス。

【請求項 18】

前記センサー入力に基づいて信用インデックスを決定するための手段をさらに備える請求項17に記載のモバイルデバイス。

【請求項 19】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされると決定するための手段をさらに備える請求項18に記載のモバイルデバイス。

【請求項 20】

ユーザ定義された認証プロセスを可能にするための手段をさらに備える請求項16に記載のモバイルデバイス。

【発明の詳細な説明】

【技術分野】

【0001】

関連出願の相互参照

本出願は、参照により本明細書に組み込まれる2014年9月23日に出願された「SCALABLE AUTHENTICATION PROCESS SELECTION BASED UPON SENSOR INPUTS」という名称の米国特許出願第14/494,543号からの優先権の利益を主張する。

【0002】

本発明は、センサー入力に基づいて認証プロセスを選択するモバイルデバイスに関する。

【背景技術】

【0003】

ユーザ認証は、通常、サービスプロバイダ、ウェブサイト、ネットワーク、アプリケーション、デバイスなどにアクセスするときに必要とされる。一般に開発されている認証方法はパスワードを使用することであるが、様々なバイオメトリック認証方法がより普及しつつある。失うまたは覚えるべきものがないのでバイオメトリック認証方法は便利であるが、それらが高度にセキュアであるためにはユーザの労力の増加を必要とし、認証の試み中の多くの誤った拒絶がよく起こる。バイオメトリック方法を使用して首尾よく認証するために、ユーザの労力が増加するということは、認証行動への注意(たとえば、虹彩走査

10

20

30

40

50

の場合 - 正しい時間にわたって、正しい照明の中で、頭の姿勢を適切にして、目の位置を適切にして、デバイスを正しい方向、正しい距離に保つこと)が増加するということであり、かつ/または首尾よく認証するために複数回の認証の試みが求められる。

#### 【 0 0 0 4 】

しかしながら、多くの事例では、ユーザはセキュリティに少ししか関心がない可能性があり(たとえば、ゲーミング統計(Gaming Stats)にアクセスすること、または写真を見ること)、他の事例では、セキュリティはもっと重要であり(たとえば、オンラインで何かを購入すること、または電子メールにアクセスすること)、いくつかの事例では、セキュリティは不可欠である(たとえば、銀行預金口座にアクセスすること、または家屋/自動車へのアクセス制御)。現在、これらのシナリオの各々は、しばしば、ユーザの過度の注意および労力を必要とする同じバイオメトリック方法を使用して認証することをユーザに求め、そのことは、セキュリティがそれほど重要でないシナリオでは(たとえば、最初の事例では)煩わしさをもたらすことがあり、一方、もっと重要なセキュリティの不可欠なシナリオでは(たとえば、最後の事例では)、同じバイオメトリック方法は十分に足りてはいない。

10

#### 【 発明の概要 】

#### 【 課題を解決するための手段 】

#### 【 0 0 0 5 】

本発明の態様は、センサー入力に基づいて認証プロセスを選択するモバイルデバイスに関する。モバイルデバイスは、複数のセンサーと、プロセッサとを含み得る。プロセッサは、センサー入力、およびアプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能に基づいて、複数の認証プロセスを決定し、複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択し、認証プロセスを実行するように構成され得る。

20

#### 【 図面の簡単な説明 】

#### 【 0 0 0 6 】

【 図 1 】 本発明の態様が実践され得るデバイスの図である。

【 図 2 】 認証プロセスを選択するためのプロセスを示すフロー図である。

【 図 3 】 リスクインデックスを示す表である。

【 図 4 】 信用インデックスを示す表である。

30

【 図 5 】 認証プロセスを選択するためのプロセスを示す図である。

#### 【 発明を実施するための形態 】

#### 【 0 0 0 7 】

「例示的」または「例」という語は、本明細書では、「例、実例、または例示としての役割を果たすこと」を意味するために使用される。「例示的」または「例」として本明細書に記載される任意の態様または実施形態は、必ずしも、他の態様または実施形態に比べて好ましいか、または有利であると解釈されるべきではない。

#### 【 0 0 0 8 】

本明細書で使用するとき、「モバイルデバイス」という用語は、限定はしないが、ラップトップコンピュータ、タブレット、スマートフォン、テレビジョン、デスクトップコンピュータ、家庭電気製品、セルラー電話、パーソナルテレビジョンデバイス、携帯情報端末(PDA)、パームトップコンピュータ、ワイヤレス電子メールレシーバ、マルチメディアインターネット対応セルラー電話、グローバルポジショニングシステム(GPS)レシーバ、ワイヤレスゲームコントローラ、車両(たとえば、自動車)内のレシーバ、対話型ゲームデバイス、ノートブック、スマートブック、ネットブック、モバイルテレビジョンデバイス、または任意のコンピューティングデバイスもしくはデータ処理装置を含む、任意の形態のプログラマブルコンピュータデバイスを指す。

40

#### 【 0 0 0 9 】

図1は、本発明の実施形態が実践され得る例示的なデバイスを示すブロック図である。システムは、1つまたは複数のプロセッサ101、メモリ105、I/Oコントローラ125、および

50

ネットワークインターフェース110を含み得るコンピューティングデバイス(たとえば、モバイルデバイス100)であり得る。モバイルデバイス100はまた、プロセッサ101にさらに結合された1つまたは複数のバスまたは信号線に結合されたいくつかのセンサーを含み得る。モバイルデバイス100がまた、ディスプレイ120(たとえば、タッチスクリーンディスプレイ)、ユーザインターフェース119(たとえば、キーボード、タッチスクリーン、または類似のデバイス)、電力デバイス121(たとえば、バッテリー)、ならびに一般に電子デバイスに関連する他の構成要素を含み得ることを諒解されたい。いくつかの実施形態では、モバイルデバイス100は移送可能なデバイスであり得るが、デバイス100が、モバイルまたは非モバイル(たとえば、特定のロケーションにおいて固定される)である任意のタイプのコンピューティングデバイスであり得ることを諒解されたい。

10

**【0010】**

モバイルデバイス100は、クロック130、周辺光センサー(ALS:ambient light sensor)135、心拍数センサー137、加速度計140、ジャイロスコープ145、磁力計150、方位センサー151、指紋センサー152、気象センサー155(たとえば、温度、風、湿度、気圧など)、グローバルポジショニングセンサー(GPS)160、赤外線(IR)センサー153、近接センサー167、および近距離場通信(NFC:near field communication)センサー169などの、センサーを含み得る。さらに、センサー/デバイスは、マイクロフォン(たとえば、音声センサー)165およびカメラ170を含み得る。通信構成要素は、同様にデバイスの環境(たとえば、位置)を分析するために使用されるセンサーと見なされ得る、ワイヤレスサブシステム115(Bluetooth(登録商標)166、Wi-Fi111、セルラー161)を含み得る。いくつかの実施形態では、複数のカメラがデバイスに組み込まれるか、またはデバイスにアクセス可能である。たとえば、モバイルデバイスは、少なくとも前面および背面取付け式カメラを有し得る。いくつかの実施形態では、他のセンサーも複数の設置またはバージョンを有し得る。

20

**【0011】**

プロセッサ101による実行のための命令を記憶するために、メモリ105がプロセッサ101に結合され得る。いくつかの実施形態では、メモリ105は非一時的である。メモリ105はまた、プロセッサ101によって実施される以下で説明する実施形態を実施するために、1つまたは複数のモデル、モジュール、エンジンを記憶し得る。メモリ105はまた、一体型センサーまたは外部センサーからのデータを記憶し得る。

**【0012】**

モバイルデバイス100は、1つまたは複数のアンテナ123およびトランシーバ122を含み得る。トランシーバ122は、アンテナおよび/または1つもしくは複数の有線リンクもしくはワイヤレスリンクを介し、ネットワークインターフェース110およびワイヤレスサブシステム115と協働して、1つまたは複数のネットワークと双方向に通信するように構成され得る。ネットワークインターフェース110は、ワイヤレスリンクを通じてデータストリームをワイヤレスネットワークに送信するとともにワイヤレスネットワークから受信するための、いくつかのワイヤレスサブシステム115(たとえば、Bluetooth(登録商標)166、Wi-Fi111、セルラー161、または他のネットワーク)に結合され得るか、またはネットワーク(たとえば、インターネット、イーサネット(登録商標)、または他のワイヤレスシステム)に直接接続するための有線インターフェースであり得る。モバイルデバイス100は、1つまたは複数のアンテナに接続された1つまたは複数のローカルエリアネットワークトランシーバを含み得る。ローカルエリアネットワークトランシーバは、WAPと通信し、かつ/またはWAPへの/からの信号を検出し、かつ/またはネットワーク内の他のワイヤレスデバイスと直接通信するのに適したデバイス、ハードウェア、および/またはソフトウェアを備える。一態様では、ローカルエリアネットワークトランシーバは、1つまたは複数のワイヤレスアクセスポイントと通信するのに適したWi-Fi(802.11x)通信システムを備え得る。

30

40

**【0013】**

モバイルデバイス100はまた、1つまたは複数のアンテナに接続され得る1つまたは複数のワイドエリアネットワークトランシーバを含み得る。ワイドエリアネットワークトランシーバは、ネットワーク内の他のワイヤレスデバイスと通信し、かつ/またはネットワー

50

ク内の他のワイヤレスデバイスへの/からの信号を検出するのに適したデバイス、ハードウェア、および/またはソフトウェアを備える。一態様では、ワイドエリアネットワークトランシーバは、ワイヤレス基地局のCDMAネットワークと通信するのに適したCDMA通信システムを備え得るが、他の態様では、ワイヤレス通信システムは、たとえば、TDMA、LTE、アドバンスドLTE、WCDMA(登録商標)、UMTS、4G、またはGSM(登録商標)などの、別のタイプのセルラー電話ネットワークまたはフェムトセルを備え得る。さらに、たとえば、WiMax(802.16)、ウルトラワイドバンド、ZigBee、ワイヤレスUSBなどの任意の他のタイプのワイヤレスネットワーキング技術が使用され得る。従来のデジタルセルラーネットワークでは、位置ロケーション機能が、様々な時間および/または位相測定技法によって提供され得る。たとえば、CDMAネットワークでは、使用される1つの位置決定手法は、アドバンスドフォワードリンクトリラテレーション(AFLT:Advanced Forward Link Trilateration)である。

10

#### 【0014】

したがって、デバイス100は、モバイルデバイス、ワイヤレスデバイス、セルラーフォン、携帯情報端末、モバイルコンピュータ、ウェアラブルデバイス(たとえば、ヘッドマウントディスプレイ、腕時計、バーチャルリアリティグラスなど)、自動車、ホームモニタリングデバイス、インターネット機器、ゲームコンソール、デジタルビデオレコーダ、電子リーダー、ロボットナビゲーションシステム、タブレット、パーソナルコンピュータ、ラップトップコンピュータ、または処理機能を有する任意のタイプのデバイスであり得る。本明細書で使用する時、モバイルデバイスは、1つまたは複数のワイヤレス通信デバイスまたはネットワークから送信されたワイヤレス信号を取り込み、1つまたは複数のワイヤレス通信デバイスまたはネットワークにワイヤレス信号を送信するように構成可能である、可搬型の、または移動可能な任意のデバイスまたは機械であり得る。したがって、限定ではなく例として、モバイルデバイス100は、無線デバイス、セルラー電話デバイス、コンピューティングデバイス、パーソナル通信システムデバイス、または他の同様の移動可能なワイヤレス通信機能搭載デバイス、機器、もしくは機械を含み得る。「モバイルデバイス」という用語はまた、衛星信号受信、支援データ受信、および/または位置関連処理がデバイス100において行われるのかどうかにかかわらず、短距離のワイヤレス接続、赤外線接続、ワイヤ線接続、または他の接続などによってパーソナルナビゲーションデバイスと通信するデバイスを含むことが意図される。また、「モバイルデバイス」は、衛星信号受信、支援データ受信、および/または位置関連処理が、そのデバイスにおいて行われるのか、サーバにおいて行われるのか、それともネットワークに関連する別のデバイスにおいて行われるのかにかかわらず、インターネット、Wi-Fi、または他のネットワークなどを介してサーバと通信することができる、ワイヤレス通信デバイス、コンピュータ、ラップトップなどを含むすべてのデバイスを含むことが意図される。上記の任意の動作可能な組合せも、「モバイルデバイス」と見なされる。

20

30

#### 【0015】

以下で説明するような本発明の実施形態が、モバイルデバイス100のプロセッサ101、ならびに/またはデバイスおよび/もしくは他のデバイスの他の回路によって、たとえば、メモリ105または他の要素に記憶されるような命令の実行を通じて実施され得ることを諒解されたい。詳細には、限定はしないがプロセッサ101を含むデバイスの回路は、プログラム、ルーチン、または本発明の実施形態による方法もしくはプロセスを実行するための命令の実行の制御下で動作し得る。たとえば、そのようなプログラムは、(たとえば、メモリ105および/または他のロケーションに記憶された)ファームウェアまたはソフトウェアに実装されてよく、プロセッサ101などのプロセッサ、および/またはデバイスの他の回路によって実装されてよい。さらに、プロセッサ、マイクロプロセッサ、回路、コントローラなどの用語が、論理、コマンド、命令、ソフトウェア、ファームウェア、機能などを実行することができる任意のタイプの論理または回路を指し得ることを諒解されたい。モバイルデバイス100内の各ユニットまたはモジュールの機能はまた、1つまたは複数の汎用プロセッサまたは特定用途向けプロセッサによって実行されるようにフォーマットされた、

40

50

メモリの中で具現化される命令を用いて、全体的または部分的に実装されてもよい。

【0016】

本発明の実施形態は、様々なセンサー入力、およびサービスプロバイダ、アプリケーション、またはデバイスの動的なセキュリティ要件を満たすためのデバイス機能に基づいて、様々なコンテキスト入力を使用して複数の認証プロセスを動的に選択およびスケリングするための装置および方法に関係し得る。詳細には、以下で説明するように、モバイルデバイス100は、プロセッサ101の制御下で、サービスプロバイダ、アプリケーション、またはデバイスの動的なセキュリティ要件を満たす認証プロセスを、様々なコンテキスト入力を使用して多数の異なる認証プロセスの中から選択し得る。

【0017】

本発明の態様の理解を助けるために、様々な用語が説明される。センサー入力は、前に説明したセンサー、たとえば、クロック130、周辺光センサー(ALS)135、心拍数センサー137、加速度計140、ジャイロスコープ145、磁力計150、方位センサー151、指紋センサー152、気象センサー155(たとえば、温度、風、湿度、気圧など)、グローバルポジショニングセンサー(GPS)160、赤外線(IR)センサー153、マイクロフォン165(たとえば、音声入力用の)、近接センサー167、近距離場通信(NFC)センサー169、カメラ170のいずれかからの任意の入力を指し得る。詳細には、センサー入力のうちのいくつかは、心拍数センサー137、指紋センサー152(たとえば、指紋入力)、タッチスクリーン120(たとえば、ハンドジオメトリ)、圧力センサー(ハンドジオメトリ)、マイクロフォン165(たとえば、音声走査)、カメラ170(顔面走査)、カメラ170(虹彩または強膜走査)などを含み得るバイオメトリックセンサーからのバイオメトリックセンサー入力と呼ばれることがある。これらがバイオメトリックセンサー入力およびバイオメトリックセンサーの例にすぎず、多種多様な追加のセンサー入力を利用され得ることを諒解されたい。

【0018】

さらに、コンテキスト情報またはコンテキスト入力は、モバイルデバイス100が現在その中にある、現在の環境を指し得る。したがって、コンテキストセンサーは、光、加速度、速度、気象、方位、ロケーション、近接度、音などのコンテキスト感知情報に関係し得る、モバイルデバイスの現在のコンテキスト状況に関係する任意のタイプのセンサーであるものと見なされ得る。したがって、コンテキストセンサーの例は、周辺光センサー135、加速度計140、気象センサー155、方位センサー151、GPS160、近接センサー167、マイクロフォン165などを含み得る。これらは、コンテキスト入力およびコンテキストセンサーの例にすぎない。同様に、コンテキスト入力はまた、以下でより詳細に説明するように、購入中の取引額、ユーザ支出データ、クラウドソースデータ、人口統計学的データ、訪れたウェブサイト、電子メール、行われた通話、オープンされたファイル、使用されたネットワーク、使用されたアプリケーションなどの、エンドユーザについて集められたデータとして特徴付けられ得る。

【0019】

一実施形態では、モバイルデバイス100は、センサー入力、コンテキスト入力、およびモバイルデバイス機能に基づいて、複数の異なる認証プロセスの中から認証プロセスを選択する。詳細には、モバイルデバイス100は、複数のセンサー(前に説明したような)およびプロセッサ101を含み得る。プロセッサ101は、コンテキスト入力、センサー入力、およびサービスプロバイダ190またはアプリケーション192またはデバイスのうちの少なくとも1つとの認証のためのモバイルデバイス100の機能に基づいて、複数の認証プロセスを決定するように構成され得る。さらに、プロセッサ101は、複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択し、認証プロセスを実行するように構成され得る。アプリケーション192を動作させるサービスプロバイダ190が、ウェブサイト(たとえば、銀行ウェブサイト、医療ウェブサイト、店舗ウェブサイト、ソーシャルメディアウェブサイトなど)、プライベートネットワーク/公衆ネットワーク、またはリンクを介して接続され得るデータ/サービスを提供する任意のタイプのコンピューティングデバイスであり得ることを諒解されたい。たとえば、モバイルデバイス100は、ワイヤレスリンク(たと

えば、セルラー、Wi-Fi、または他のネットワークなど)または有線リンクを介して、サービスプロバイダ190に接続し得る。また、アプリケーション192がモバイルデバイス100自体にあってよいことを諒解されたい。さらに、モバイルデバイス機能は、ワイヤレスデバイス100が、クロック130、周辺光センサー(ALS)135、心拍数センサー137、加速度計140、ジャイロスコープ145、磁力計150、方位センサー151、指紋センサー152、気象センサー155、グローバルポジショニングセンサー(GPS)160、赤外線(IR)センサー153、マイクロフォン165、近接センサー167、近距離場通信(NFC)センサー169、カメラ170などの特定のセンサーを含むか否かにかかわらず、ワイヤレスデバイス100自体のそのような機能を指し得ることを諒解されたい。モバイルデバイス機能はまた、プロセッサのタイプ、メモリ、速度、およびセンサー自体の精度を含み得る。

10

#### 【0020】

一実施形態では、コンテキスト入力、コンテキストセンサーからの入力であり得、かつ/または現在のユーザ入力データ、前のユーザ入力データ、ロケーション、時間、または人口統計学的データのうちの少なくとも1つを含み得る。前に説明したように、コンテキストセンサーは、光、加速度、気象、方位、ロケーション、近接度、音などの感知情報に関係し得る、モバイルデバイスの現在のコンテキスト状況に関係する任意のタイプのセンサーであるものと見なされ得る。したがって、コンテキストセンサーの例は、周辺光センサー135、加速度計140、気象センサー155、方位センサー151、GPS160、近接センサー167、マイクロフォン165などを含み得る。さらに、センサー入力は、バイオメトリックセンサーからのバイオメトリックセンサー入力を含む。たとえば、前に説明したように、バイオメトリックセンサー入力用のバイオメトリックセンサーは、心拍数センサー137、指紋センサー152(たとえば、指紋入力)、タッチスクリーン120(たとえば、ハンドジオメトリ)、圧力センサー(ハンドジオメトリ)、マイクロフォン165(たとえば、音声走査)、カメラ170(顔面走査)、カメラ170(虹彩または強膜走査)などを含み得る。多種多様な異なるタイプのセンサーが利用されてよく、これらが例にすぎないことを諒解されたい。また、ハンドジオメトリ用の静電容量式タッチスクリーンなどの、特定のタイプのセンサーが利用されてよい。しかしながら、やはり、これらは例にすぎない。

20

#### 【0021】

さらに、以下でより詳細に説明するように、プロセッサ101は、コンテキスト入力に基づいてリスクインデックスを決定し、センサー入力に基づいて信用インデックスを決定するようにさらに構成され得る。信用インデックスがリスクインデックスよりも大きい場合、セキュリティ要件は満たされていると決定され得る。このようにして、複数の認証プロセスのうちの複数の中からセキュリティ要件を満たす認証プロセスが選択され、認証プロセスが実行されて、モバイルデバイス101がサービスプロバイダ190および/またはアプリケーション192および/またはデバイスに認証されることを可能にする。さらに簡潔に図2を参照すると、モバイルデバイス100は、コンテキスト入力、センサー入力、およびサービスプロバイダ190またはアプリケーション192のうちの少なくとも1つとの認証のためのモバイルデバイス100の機能に基づいて、複数の認証プロセスを決定し(ブロック202)、複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択し(ブロック204)、認証プロセスを実行する(ブロック206)ためのプロセス200を実施し得る。

30

40

#### 【0022】

一例として、プロセッサ101の制御下でのモバイルデバイス100は、購入トランザクションを履行すること(たとえば、サービスプロバイダ190が店舗ウェブサイトである)、または振替すること(たとえば、サービスプロバイダ190が銀行ウェブサイトである)などの機能を実行するために、サービスプロバイダ190に接続し得る。さらに、プロセッサ101の制御下でのモバイルデバイス101は、アプリケーション192またはデバイスにログインしようと試み得る。これらのシナリオのいずれかにおいて、認証プロセスが必要とされてよく、認証プロセスで使用するためにリスクレベルが計算され得る。

#### 【0023】

銀行取引を利用すると(たとえば、サービスプロバイダ190が銀行ウェブサイトである)

50



、例として、振替額、ユーザのロケーション、および他のコンテキスト入力、事前に割り当てられたリスクレベルを使用してリスクインデックスを計算するために使用され得る。リスクインデックス300の一例が、図3を参照しながら見られ得る。この例では、サービス302は、高リスクレーティング302を有する。また、例として、取引額304(たとえば、>\$1000.00)およびロケーション310(たとえば、遠方)は、高リスクを示し得る。信用インデックスは、モバイルデバイス100とともに記録された、バイオメトリック認証方式の各々に関連付けられた信用のレベルに基づいて計算され得る。信用インデックス400の一例が、図4を参照しながら見られ得る。サービスプロバイダ190とのトランザクションを首尾よく認証および履行するためにセキュリティ要件が満たされるように、モバイルデバイス100のプロセッサ101は、信用インデックスが高く、かつリスクインデックスよりも大きくなるようなバイオメトリック認証プロセス(たとえば、指紋センサー)406を選択し得る。セキュリティ要件を満たすためのこの計算に基づいて、このバイオメトリック認証プロセス(たとえば、指紋センサー)406が複数の他の認証プロセスから選択され、この認証プロセスは、モバイルデバイス101をサービスプロバイダ190に認証するために実行され得る。

10

20

30

40

50

#### 【0024】

このようにして、ユーザへの利便性は、認証するときに動的に最大化される。さらに、現在のサービスプロバイダ190/アプリケーション192/デバイスのセキュリティ要求を満たすように認証プロセスを選択およびスケールすることは、首尾よく認証するために必要な最小量のセキュリティしか必要とせず、それによって、ユーザの労力の増加を最小限に抑える。銀行取引(たとえば、モバイル支払い、モバイル購入、振替)、ログイン情報、およびアクセスなどの、多数の可能な利用場面があることを諒解されたい。アクセスの例は、デバイス(たとえば、電話)、アプリケーション、オンラインサービス、オンラインネットワーク、ソーシャルネットワーク、電子メール、モバイルクラウドストレージ、モバイルバンキングサービスなどへのアクセスを含む。任意のタイプのサーバ、ウェブサイト、アプリケーション、デバイスなどにモバイルデバイスを認証するために、このプロセスが利用され得ることを諒解されたい。

#### 【0025】

一例として、機能がモバイルデバイス100によって実行されるべきであり(たとえば、サービスプロバイダ190を通じた金融取引、アプリケーション192のログイン、デバイスのログイン)、認証プロセスが実行される必要があるとき、モバイルデバイス100は、コンテキスト入力およびセンサー入力に基づいて複数の認証プロセスを決定し得る。詳細には、リスクインデックスの表300を示す図3をさらに参照すると、セキュリティ要件を生成するためにコンテキスト入力を利用されて、以下のコンテキスト入力パラメータ、すなわち、アプリケーション/サービスプロバイダ/デバイスのログイン302(これは低(たとえば、ゲーム)、中(たとえば、ソーシャルネットワーク)、高(たとえば、銀行取引)を含む)、取引ドル額304(たとえば、\$100.00よりも少ない低、\$1000.00よりも少ない中、または\$1000.00よりも多い高)、(GPS、WiFi決定の)ロケーション310(これは低(たとえば、自宅/職場の近く)、中(たとえば、町/地域の中)、高(たとえば、遠方)を含む)、学習された支出行動パターンからのユーザ支出行動偏差312(低(たとえば、過去のデータと一致する)、中(たとえば、過去のデータとほとんど一致する)、高(たとえば、過去のデータと矛盾する))、イベントの間に集められたクラウドソースデータ314(低(たとえば、多くの確認済みデータ)、中(たとえば、いくつかの確認済みデータ)、高(たとえば、確認済みデータなし))、人口統計学的プロファイル316(低リスク、中リスク、高リスク)の各々に関連付けられたリスクのレベルを使用してリスクインデックスを計算し得る。

#### 【0026】

例として、アプリケーション/サービスプロバイダ/デバイスのログイン302の場合、ユーザは、認証を必要とするアプリケーション、サービスプロバイダ、またはデバイスにアクセス(にログイン)しようと試みている場合がある。たとえば、ゲームアプリケーションは、もっと低いセキュリティ要件(低リスクインデックス)を有し得、バンキングサービスは、もっと高いセキュリティ要件(高リスクインデックス)を有し得る。セキュリティ要件

を發展させることも、この方法を使用してサポートされ得る(たとえば、新たなポリシーに起因して写真共有サービスに対するセキュリティ要件が高まる)。別の例として、その各々が特定のリスク、たとえば、取引ドル額304(たとえば、\$100.00よりも少ない低リスク、\$1000.00よりも少ない中リスク、\$1000.00よりも多い高リスク)を有し得るいくつかのドル額のオンライン取引を、ユーザが履行しようとして試みている場合がある。セキュリティ要件を満たす際に使用するためのコンテキスト入力の別の例として、ロケーションセンサーによって決定されたロケーションがリスクインデックスとして利用され得る。リスクインデックスは、自宅、職場、もしくは親類の家などの普通の毎日のロケーションにおいて、またはその近くで、サービスまたは取引にアクセスするユーザにとって低であり得るが、特に普通のロケーションから遠い場合(たとえば、別の都市または国)、公共の設定には高リスクが関連付けられ得る。全般的な地域または地域内の特定のロケーションは、「高リスク」としてタグ付けされ得る(たとえば、既知の不正な活動が過去に報告されている場所)。同様に、他の地域または特定のロケーションは、「低リスク」としてタグ付けされ得る(たとえば、既知の不正な活動が報告されていない場合)。セキュリティ要件を満たす際に使用するためのコンテキスト入力のまた別の例として、ユーザ支出行動偏差312が利用され得る。これは、時間およびロケーションベースのインデックスである。たとえば、ユーザが隔週の金曜日に、より自由な支出に関与する場合(支払い小切手を受け取ることに起因して)、この支出行動は全体的な支出パターンの一部であることになり、したがって、全体的なリスクインデックスを知らせ得る。別のパターンは、休日の間、別の都市にいながら(たとえば、休日の間、親類を訪問する)、より頻繁に支出することであり得る。両方の事例において支出行動パターンが確立されるので、これらの例の両方は低リスクに帰着することになる。

10

20

30

40

50

#### 【0027】

さらなる例として、イベントの間に集められたクラウドソースデータ314が、セキュリティ要件を決定する際のコンテキスト入力として利用され得る。たとえば、イベントが特定の時間および場所において開催されており(たとえば、カウンティフェア)、多くの人々が特定の購入先において支出している場合(たとえば、入場料)、このデータは全体的なリスクインデックスを知らせ得る。この例では、あるロケーションにおいてイベント中に行われている多くの取引が、より低リスクレベルに帰着することになる。別の例として、人口統計学的プロファイルデータ316が、セキュリティ要件を決定する際のコンテキスト入力として利用され得る。人口統計学的プロファイル(たとえば、性別、年齢、民族性、所得、クレジットスコア、なりすまし犯罪履歴など)のいくつかの特徴が、個人にとってのリスクインデックスの包括的な乗数として使用され得る。たとえば、個人が極めて若くまたは年配である場合、彼らは不正行為の事例に対して無防備であり得る。そのような場合、計算されたリスクインデックスに乗数が包括的に適用され得る(たとえば、リスクインデックス\*1.2)。過去に識別情報を盗まれた個人はまた、リスクインデックスをわずかに引き上げることで恩恵を受け得る。他のグループは、主にリスクインデックススコアをわずかな量だけ包括的に低くすることから最大の恩恵を引き出し得る(たとえば、中程度の所得レベルを有し年齢25~55歳の間の人、リスクインデックス\*.80)。

#### 【0028】

したがって、リスクインデックスは、図3の表300を参照しながら前に説明したコンテキスト入力パラメータを使用することによって計算され得る。一例として、全体的なリスクインデックスは1~10にわたってよく、ここで、1~3は低リスクであり得、4~7は中リスクであり得、8~10は高リスクであり得る。リスクインデックスを計算するために、利用可能な各コンテキスト入力を使用され得る。他の実装形態では、ユーザは、選択されたアプリケーションまたはサービスごとにリスクインデックスを直接設定してよい。この実装形態では、いくつかのアプリケーションまたはサービスが、上記のコンテキスト入力に依存する動的な(計算された)リスクインデックスを使用することを可能にすること、および他のアプリケーションまたはサービスが、毎回適用される静的設定のリスクインデックスを使用することが可能であることになる。

## 【 0 0 2 9 】

説明されたように、リスクインデックスはコンテキスト入力に基づいて決定され得、信用インデックスはセンサー入力に基づいて決定され得る。信用インデックスがリスクインデックスよりも大きい場合(信用インデックス>リスクインデックス)、セキュリティ要件は満たされていると決定され得る。このようにして、複数の認証プロセスのうちの複数の中からセキュリティ要件を満たす認証プロセスが選択され、認証プロセスが実行されて、モバイルデバイス101がサービスプロバイダおよび/またはアプリケーションおよび/またはデバイスに認証されることを可能にする。

## 【 0 0 3 0 】

リスクインデックス表300の例を利用する、コンテキスト入力に基づいてリスクインデックスを計算することの特定の例が示される。たとえば、以下のコンテキスト変数が、リスクインデックスを重み付けするために使用され得る。すなわち、取引額が中程度(たとえば、\$150)である場合(リスクインデックス=中(4))、ロケーションが公共である場合(リスクインデックスは中(5)に高められる)、ユーザ支出行動偏差が過去の行動と矛盾する場合(リスクインデックスは中~高(7)に高められる)、クラウドソースデータがユーザのロケーションにおいて高リスクを報告する場合(リスクインデックスは高(8)に高められる)、ユーザ人口統計学がいくらか高リスクであった場合、インデックスは重み付けられ得る(たとえば、 $\times 1.1$ )。この例では、全体的なリスクインデックスは、次いで、 $\text{リスクインデックス} = 8 \times 1.1 = 8.8$ になる。したがって、この例では、全体的なリスクインデックスは8.8であると決定される。この例では、セキュリティ要件(信用インデックス>リスクインデックス)を満たす認証プロセスは、複数の認証プロセスのうちの複数の中から選択され、高信用インデックスを有する認証プロセス(たとえば、虹彩走査、または指紋走査および音声走査など)を必要とする。

## 【 0 0 3 1 】

認証プロセスの例が以下で説明される。認証方式は、虹彩スキャナ(誤った受諾が極めて低い)などの、極めて高いセキュリティ方法から、指紋走査やハンドジオメトリ走査などの、セキュリティはより低いがもっと便利で社会的に受け入れられる方法までわたる。したがって、登録された所与のデータベースサイズに対する基本的な誤った受諾および誤った拒絶に基づいて、信用レベルが各認証方法に関連付けられ得る。バイオメトリック認証方法の技術上の実装形態は異なる場合があるが、特定のバイオメトリック特徴の一意性および適合性の、人間の生理学的な限界は、集団の中で全体として変化しない(いくつかの特徴は、(人々の間で)より固有であるとともに(個人の中で)他の特徴よりも不変であり、したがって、より強力なセキュリティの能力がある)。たとえば、虹彩は非常に固有であるので、誤った受諾率(FAR:false accept rate)が120万回の試行において恐らく1であるが、指紋は、一般に、4桁PINと同様に10,000回の試行において誤った受諾が1回という結果になることが知られている。ハンドジオメトリは、対照的に、標準的なカメラおよび方法を使用して抽出されるときにFARが1:1000であるが、タッチスクリーンからのハンドジオメトリ特徴の抽出は、同様の数の試行およびデータベースサイズを仮定すれば、ずっと小さいFARしか得られない。セキュリティがより低いバイオメトリクスは、対照的に、さほど侵襲的でないが、セキュリティがより高いバイオメトリック方法よりも社会的に受け入れられ、使用するのに便利であるという傾向がある。

## 【 0 0 3 2 】

前に説明したように、いくつかの実施形態では、センサー入力は、信用インデックスを作り出すために利用されるバイオメトリックセンサーからのバイオメトリックセンサー入力を含む。たとえば、前に説明したように、バイオメトリックセンサー入力用のバイオメトリックセンサーは、心拍数センサー137、指紋センサー152(たとえば、指紋入力)、タッチスクリーン120(たとえば、ハンドジオメトリ)、圧力センサー(ハンドジオメトリ)、マイクロフォン165(たとえば、音声走査)、カメラ170(顔面走査)などを含み得る。

## 【 0 0 3 3 】

さらに図4を参照すると、信用インデックス400が、例示的な信用レベルを提供する以下

10

20

30

40

50

の認証方法を使用して生成され得る。図4に示すように、低信用レベル(1~3)は、低いバイオメトリック認証プロセス402、すなわち、ソフトバイオメトリクス(たとえば、髪の色)、指紋/ハンドジオメトリ、ECG走査などしか必要とし得ない。中信用レベル(4~7)は、中間のバイオメトリック認証プロセス404、すなわち、音声走査、顔面走査、パスワードなどを必要とし得る。一方、高信用レベル(8~10)は、高いバイオメトリック認証プロセス406、すなわち、指紋走査、虹彩走査などを必要とし得る。

#### 【0034】

前に説明したように、リスクインデックスはコンテキスト入力に基づいて決定され得、信用インデックスはセンサー入力、詳細には、バイオメトリックセンサー入力に基づいて決定され得る。信用インデックスがリスクインデックスよりも大きい場合(信用インデックス>リスクインデックス)、セキュリティ要件は満たされていると決定され得る。このようにして、複数の認証プロセスのうちの複数の中からセキュリティ要件を満たす認証プロセスが選択され、認証プロセスが実行されて、モバイルデバイス101がサービスプロバイダおよび/またはアプリケーションおよび/またはデバイスに認証されることを可能にする。一例として、特に高いリスクの銀行取引(たとえば、高リスクインデックス)の場合、リスクインデックスよりも大きくないとしても、少なくともリスクインデックスに等しい信用インデックスを与えるように高い信用レベルに関連付けられている認証方法が選択される。たとえば、高リスク銀行取引(8~10)の場合、求められるセキュリティレベルは、信用インデックスレベルがリスクインデックスレベルを上回るような、高信用インデックスレベル(8~10)を有する指紋走査プロセスを必要とし得る。代替として、モバイルデバイスが指紋走査の能力がない場合、求められる信用インデックスレベルを満たすために、顔走査+音声走査などが利用され得る。

#### 【0035】

いくつかの実施形態では、認証が求められるとき、音、光、および動きの周辺レベルが、それぞれ、マイクロフォン165、光センサー135、および加速度計140からサンプリングされて、最も信頼できるデータを与える最適なバイオメトリック方法を選択およびスケールリングする助けとなり得る。たとえば、背景雑音が音声バイオメトリックデータを収集するのにあまりに大きいと決定される場合、他の認証方法が選択され得る(たとえば、顔面走査、虹彩走査、指紋走査、ECGモニタリングなど)。さらに、音声走査がマイクロフォン165によって収集される場合、それに関連付けられた信用レベルは、それに応じて重み付けられ得る(たとえば、音声走査の信用レベルは背景雑音レベルに比例して下がる)。同様に、周辺光が、(周辺光センサー135を介して測定されるような)顔面バイオメトリックデータを適切に測定するのにあまりに薄暗いか、または虹彩バイオメトリックデータを測定するのにあまりに明るい(反射を引き起こす)場合、他の認証方法が選択され得る(たとえば、音声走査、指紋走査、ハンドジオメトリ、手の脈管、ECGモニタリングなど)。さらに、顔面走査が収集される場合、それに関連付けられた信用レベルは、それに応じて重み付けられ得る(たとえば、顔面走査の信用レベルは周辺輝度に比例して下がる)。いくつかの実施形態では、指紋、指/ハンドジオメトリ、指/手の脈管パターン、またはECGバイオメトリックデータを収集するのにあまりに多くの動きがある場合、他の認証方法(たとえば、音声走査、顔面走査、虹彩走査)が収集され得る。さらに、指紋が、たとえば、収集される場合、それに関連付けられた信用レベルは、それに応じて重み付けられ得る(たとえば、指紋の信用レベルは動きに比例して下がる)。

#### 【0036】

さらに、主要な人口統計学的コンテキスト入力(たとえば、年齢)が推定され得るか、または知られている場合(たとえば、年齢)、バイオメトリック特徴の信頼性を最適にする認証プロセスが選択され得る。たとえば、声をかすれさせ、または声を変える確率がより高くなり得るので、十代の少年向けのバイオメトリック認証プロセスは、声紋認証を差し控えてよく、または使用される場合、ユーザのこのグループ向けの信用インデックスにおいて、より低く重み付けられ得る。別の例は、年配のユーザ(たとえば、>年齢75歳)向けの指紋プロファイルがいくらか信頼できないことがあり、そのため、これらのユーザ向けの指紋走査は、選択

され得ないか、または使用されるなら、このグループ向けの信用インデックスにおいて潜在的により低く重み付けられ得ることである。

【 0 0 3 7 】

さらに図5を参照すると、認証プロセス500の一実施形態が説明される。ステップ502において、ユーザは、認証を求めるサービスプロバイダ、アプリケーション、またはデバイスにアクセスする(ブロック502)。たとえば、前に説明したように、ユーザは、振替を追跡するために銀行ウェブサイトアクセスする。ブロック504において、リスクインデックスが計算される。たとえば、リスクインデックスは、登録されている各コンテキスト入力に関連付けられたリスクレベルに基づいて、ブロック504のリスクインデックス式に従って計算され得る。コンテキスト入力510の例は、取引額、ロケーションデータ(GPS、Wi-Fiなど)、ユーザ支出行動偏差、クラウドソースデータ、人口統計学的プロファイルを含む。コンテキスト入力に基づくリスクインデックスの決定は、前に図3を参照しながら詳細に説明されている。したがって、認証の時間において、前に説明した利用可能なコンテキスト入力の各々に関連付けられたリスクのレベルに基づいて、リスクインデックスが計算される。いくつかのコンテキスト入力/変数がモバイルデバイスに記憶されてよく、異なる時間においてアクセスされてよいことを諒解されたい。

【 0 0 3 8 】

さらに、ブロック530において、信用インデックスが計算される。たとえば、信用インデックスは、選択された認証プロセスの各々に関連付けられた信用レベルに基づいて、ブロック530の信用インデックス式に従って計算され得る。認証プロセスまたは方法532の例は、ハンドジオメトリ、音声走査、顔面走査、パスワード、指紋走査、虹彩走査などを含む。認証プロセス、詳細には、バイオメトリック認証プロセスに基づく信用インデックスの決定は、前に図4を参照しながら詳細に説明されている。したがって、選択された認証プロセスの各々に関連付けられた信用のレベルに基づいて、信用インデックスが計算される。

【 0 0 3 9 】

詳細には、ブロック535に示すように、セキュリティ要件、すなわち、信用インデックス>リスクインデックスが満たされるように、利用可能な認証方法/プロセスが選択され、重み付けられる。詳細には、モバイルデバイス上で利用可能な認証プロセスの各々に関連付けられた信用のレベルに基づいて、信用インデックスが計算される。信用インデックス>リスクインデックスであるこれらのタイプ選択の例は、前に詳細に説明されている(たとえば、音声走査+指走査が、7としてのリスクインデックスよりも大きい高信用インデックス(9)に等しい)。さらに、前に説明したように、信用インデックスの選択および重み付けにおいて、周辺動きレベル、周辺光レベル、および周辺音レベルが利用され得る。ブロック540を参照すると、認証プロセスが選択されると、認証プロセスにとって必要なハードウェア構成要素をセキュアにするために、セキュアな実行環境(たとえば、トラストゾーン)がモバイルデバイス100のプロセッサ101によって実施され得る(ブロック542)。これらのタイプのセキュアなハードウェア構成要素550の例は、虹彩走査用のIRセンサー153/カメラ170、指紋走査用の指紋センサー152、パスワード用またはPIN用のユーザインターフェース/キーボード116、顔面走査用のカメラ170、音声走査用のマイクロフォン165、ハンドジオメトリ走査用のタッチスクリーンディスプレイ120などを含む。いくつかの実施形態では、高信用レベル(たとえば、高信用レベル406、図4)を有する高いセキュリティ方法が最初に求められてよく、規定の時間期間の後、および/またはコンテキスト入力に基づくリスクインデックスがしきい値に影響を及ぼすほど(たとえば、信用インデックス>リスクインデックス)著しく変化しなかった場合、ユーザは、状況(たとえば、コンテキスト)が変化するまで、より低い信用レベル(たとえば、低信用レベル402、図4)を有する低いセキュリティ方法を利用することを許容され得ることを諒解されたい。

【 0 0 4 0 】

ブロック560において、選択された複数の認証プロセスの各々が、連続的にまたは並行してユーザに表示され得る。とはいえ、1つの認証プロセスだけが必要とされ得る。しか

しながら、ユーザによるいかなる手動入力も求めず、したがって最もじゃまにならない「受動的」認証プロセスが有益であり得ることを諒解されたい。したがって、リスクインデックスよりも大きい信用インデックスがモバイルデバイスによって(受動的認証プロセスに基づいて)選択可能である場合、受動的認証プロセス(たとえば、タッチスクリーンからのハンドジオメトリ)が選択され、ユーザによる手動入力は求められず、認証プロセスが表示される必要がない。ブロック562において、選択された認証プロセスから特徴(たとえば、センサー入力)が抽出される。ブロック565において、取り込まれた特徴が、記憶されているテンプレートからの登録されている特徴と整合する場合、サービス/アプリケーション/デバイスが認証され(ブロック572)、そうでない場合、サービス/アプリケーション/デバイスは認証されない(ブロック570)。

10

#### 【0041】

また、いくつかの実施形態では、認証プロセス500は、2人以上の人々が、サービス/アプリケーション/デバイスが認証されるような認証プロセス500を実行するように求められる実施形態を含み得る。別の特定の例示的な実施形態として、未成年者の代わりに親が認証プロセス500を実行するように求められてもよい。

#### 【0042】

したがって、一例では、モバイルデバイス100は、コンテキスト入力(たとえば、取引額、ロケーションデータ、ユーザ支出行動データ、クラウドソースデータ、人口統計学的プロフィールなど)、およびバイオメトリックセンサー入力(たとえば、ハンドジオメトリ、音声走査、顔面走査、指紋走査、虹彩走査など)に基づいて、複数の認証方法を使用する認証プロセスを選択し得る。詳細には、モバイルデバイス100のプロセッサ101は、コンテキスト入力、バイオメトリックセンサー入力、およびサービスプロバイダ/アプリケーション/デバイスなどのうちの少なくとも1つとの認証のためのモバイルデバイス100の機能に基づいて、複数の認証プロセスを決定するように構成され得る。さらに、プロセッサ101は、前に詳細に説明したように、複数の認証方法の中から、信用インデックスがリスクインデックスよりも大きいものとしてセキュリティ要件が定義され得るセキュリティ要件を満たす認証プロセスを選択するように構成され得る。

20

#### 【0043】

いくつかの実施形態では、認証方法はユーザ定義されてよい。たとえば、ユーザは、モバイルデバイスが利用できる複数の認証方法(たとえば、パスワード、顔面走査、音声走査、ハンドジオメトリ、ECG、指紋走査、虹彩走査など)を登録および使用してよく、他の認証方法を登録しないことを選んでよい。また、いくつかの実施形態では、特定のバイオメトリックセンサーが、雑音に起因する部分的なデータ(たとえば、よごれまたは動きに起因する部分的なデータ)、またはシャドーイングに起因する部分的な顔面走査、または背景雑音に起因する部分的な音声走査、または反射、斜視、もしくは目の動きに起因する部分的な虹彩走査しか抽出することができない場合、抽出され得る限定された特徴のみに基づいて信用インデックスが計算されてよい。部分的な走査は、たとえば、低セキュリティのアプリケーション(たとえば、写真を見る)を認証するためのセキュリティ要件(信用インデックス>リスクインデックス)を満たし得る。しかしながら、部分的な走査しか抽出しないことは、より高いセキュリティのアプリケーションのセキュリティ要求を満たせないことがあり(すなわち、信用インデックス<リスクインデックス)、追加の認証が求められてよい。PINまたはパスワード認証は、オンライン金融サービスまたはモバイルサービスにとっての要件であり得るが、これは求められる最小レベルのセキュリティとして働き得る。コンテキスト入力は、それがオンラインPINまたはパスワードに関連付けられた信用レベルを上回るように、計算されたリスクインデックスをつり上げてよく、リスクインデックススコアを満たすための追加のバイオメトリック認証方法を必要とする。

30

40

#### 【0044】

前に説明した本発明の態様が、前に説明したようにデバイスのプロセッサによる命令の実行に関連して実施され得ることを諒解されたい。詳細には、限定はしないが、プロセッサを含むデバイスの回路は、プログラム、ルーチン、または本発明の実施形態による方法

50

もしくはプロセスを実行するための命令の実行の制御下で動作し得る。たとえば、そのようなプログラムは、(たとえば、メモリおよび/または他のロケーションに記憶された)ファームウェアまたはソフトウェアに実装されてよく、プロセッサ、および/またはデバイスの他の回路によって実装されてよい。さらに、プロセッサ、マイクロプロセッサ、回路、コントローラなどの用語が、論理、コマンド、命令、ソフトウェア、ファームウェア、機能などを実行することができる任意のタイプの論理または回路を指すことを諒解されたい。

#### 【0045】

デバイスがモバイルデバイスまたはワイヤレスデバイスであるとき、デバイスは、任意の適切なワイヤレス通信技術に基づくか、またはそうしたワイヤレス通信技術を別の方法でサポートするワイヤレスネットワークを通じて、1つまたは複数のワイヤレス通信リンクを介して通信し得ることを諒解されたい。たとえば、いくつかの態様では、ワイヤレスデバイスおよび他のデバイスは、ワイヤレスネットワークを含むネットワークと関連し得る。いくつかの態様では、ネットワークは、ボディエリアネットワークまたはパーソナルエリアネットワーク(たとえばウルトラワイドバンドネットワーク)を備え得る。いくつかの態様では、ネットワークは、ローカルエリアネットワークまたはワイドエリアネットワークを備え得る。ワイヤレスデバイスは、様々なワイヤレス通信技術、プロトコル、または、たとえば、3G、LTE、アドバンスドLTE、4G、CDMA、TDMA、OFDM、OFDMA、WiMAX、およびWiFiなどの規格のうちの1つまたは複数をサポートし得るか、あるいは別の方法で使用し得る。同様に、ワイヤレスデバイスは、様々な対応する変調方式または多重化方式のうちの1つまたは複数をサポートし得るか、あるいは別の方法で使用し得る。ワイヤレスデバイスは、上記または他のワイヤレス通信技術を使用して、1つまたは複数のワイヤレス通信リンクを確立し、そうした通信リンクを介して通信するのに適した構成要素(たとえば、エアインターフェース)をそのように含み得る。たとえば、デバイスは、ワイヤレス媒体を介した通信を容易にする様々な構成要素(たとえば、信号発生器および信号プロセッサ)を含み得る、関連する送信機構成要素および受信機構成要素(たとえば、送信機および受信機)を有するワイヤレストランシーバを備え得る。よく知られているように、モバイルワイヤレスデバイスは、したがって、他のモバイルデバイス、セルフォン、他の有線コンピュータおよびワイヤレスコンピュータ、インターネットウェブサイトなどと、ワイヤレス通信し得る。

#### 【0046】

本明細書の教示は、様々な装置(たとえば、デバイス)に組み込まれ(たとえば、その中に実装され、またはそれによって実行され)得る。たとえば、本明細書において教示される1つまたは複数の態様は、電話(たとえば、セルラー電話)、携帯情報端末(「PDA」)、タブレット、モバイルコンピュータ、ラップトップコンピュータ、エンターテインメントデバイス(たとえば、音楽デバイスまたはビデオデバイス)、ヘッドセット(たとえば、ヘッドフォン、イヤピースなど)、医療デバイス(たとえば、心拍数モニタ、歩数計、心電図デバイスなど)、ユーザI/Oデバイス、コンピュータ、有線コンピュータ、固定コンピュータ、デスクトップコンピュータ、サーバ、ポイントオブセールデバイス、セットトップボックス、または任意の他の適切なデバイスに組み込まれ得る。これらのデバイスは、異なる電力要件およびデータ要件を有し得る。

#### 【0047】

様々な異なる技術および技法のいずれかを使用して情報および信号が表され得ることは、当業者であれば理解されよう。たとえば、上記の説明全体にわたって参照され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

#### 【0048】

本明細書で開示する実施形態に関連して説明した様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップが、電子ハードウェア、コンピュータソフトウ

10

20

30

40

50

ェア、または両方の組合せとして実装され得ることは、当業者であればさらに諒解されよう。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップが、概してそれらの機能に関して上記で説明された。そのような機能がハードウェアとして実現されるのか、それともソフトウェアとして実現されるのかは、特定の適用例および全体的なシステムに課された設計制約によって決まる。当業者は説明した機能を特定の適用例ごとに様々な方法で実装し得るが、そのような実装決定は、本発明の範囲からの逸脱を引き起こすと解釈されるべきではない。

#### 【0049】

本明細書で開示する実施形態に関連して説明した様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明する機能を実行するように設計されたそれらの任意の組合せを用いて、実施され得るか、または実行され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、またはステートマシンであってもよい。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装され得る。

#### 【0050】

本明細書で開示する実施形態に関連して説明した方法またはアルゴリズムのステップは、ハードウェアとして直接、プロセッサによって実行されるソフトウェアモジュールにおいて、または2つの組合せで具現化され得る。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野において知られている任意の他の形態の記憶媒体の中に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、また記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体は、プロセッサに一体化されてもよい。プロセッサおよび記憶媒体は、ASICの中に存在してよい。ASICは、ユーザ端末の中に存在してよい。代替として、プロセッサおよび記憶媒体は、個別構成要素としてユーザ端末の中に存在してもよい。

#### 【0051】

1つまたは複数の例示的な実施形態では、説明した機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せで実装され得る。コンピュータプログラム製品としてソフトウェアで実装される場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶され得るか、またはコンピュータ可読媒体を介して送信され得る。コンピュータ可読媒体は、コンピュータ記憶媒体と、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む通信媒体の両方を含む。記憶媒体は、コンピュータによりアクセスされ得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または命令もしくはデータ構造の形態の所望のプログラムコードを搬送もしくは記憶するために使用され得、コンピュータによってアクセスされ得る任意の他の媒体を備えることができる。また、任意の接続も厳密にはコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するとき、ディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザーデ



ディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピーディスク(disk)、およびBlu-ray(登録商標)ディスク(disc)を含み、ディスク(disk)は、通常、データを磁氣的に再生し、ディスク(disc)は、レーザーを用いてデータを光学的に再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれるべきである。

#### 【 0 0 5 2 】

開示した実施形態の前述の説明は、当業者が本発明を作成または使用することを可能にするために与えられる。これらの実施形態への様々な修正が当業者には容易に明らかとなり、本明細書で定義される一般原理は、本発明の趣旨または範囲から逸脱することなく他の実施形態に適用され得る。したがって、本発明は、本明細書に示す実施形態に限定されることは意図されておらず、本明細書で開示する原理および新規の特徴に一致する最も広い範囲を与えられるべきである。

10

#### 【 符号の説明 】

#### 【 0 0 5 3 】

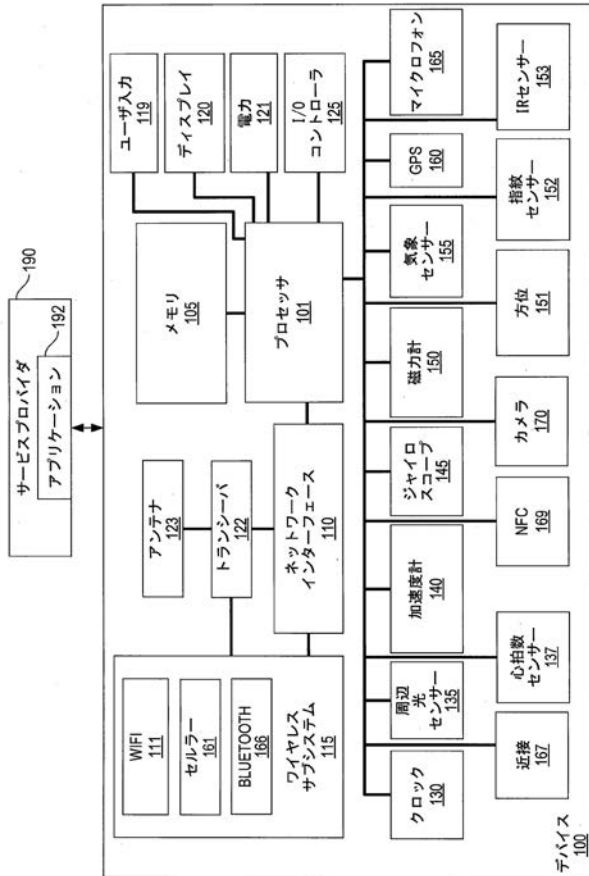
- 100 モバイルデバイス
- 101 プロセッサ
- 105 メモリ
- 110 ネットワークインターフェース
- 111 Wi-Fi
- 115 ワイヤレスサブシステム
- 119 ユーザインターフェース
- 120 ディスプレイ
- 121 電力デバイス
- 122 トランシーバ
- 123 アンテナ
- 125 I/Oコントローラ
- 130 クロック
- 135 周辺光センサー
- 137 心拍数センサー
- 140 加速度計
- 145 ジャイロスコープ
- 150 磁力計
- 151 方位センサー
- 152 指紋センサー
- 153 赤外線センサー
- 155 気象センサー
- 160 グローバルポジショニングセンサー
- 161 セルラー
- 165 マイクロフォン
- 166 Bluetooth(登録商標)
- 167 近接センサー
- 169 近距離場通信センサー
- 170 カメラ
- 190 サービスプロバイダ
- 192 アプリケーション

20

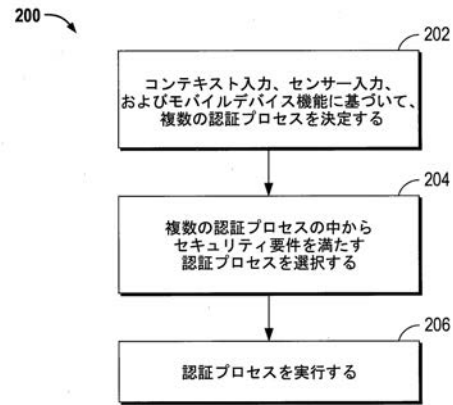
30

40

【図 1】



【図 2】



【図 3】

リスクインデックス

| 300                     | 302                   | 304                               | 310             | 312              | 314          | 316 |
|-------------------------|-----------------------|-----------------------------------|-----------------|------------------|--------------|-----|
| アプリケーション/サービス/デバイスのログイン | 取引ドル額                 | ロケーション (GPS、WiFi)                 | ユーザ支出行動履歴       | クラウドソースデータ       | 人口統計学的プロフィール |     |
| 低 (たとえば、写真、ゲーム)         | 低 (たとえば、\$100)        | 自宅/職場の近く (5マイル)、または低リスクとタグ付けされた地域 | 過去のデータと一致する     | 多くの確認済みデータ (低)   | 低リスク         |     |
| 中 (たとえば、ソーシャルネットワーク)    | 中 (たとえば、\$100~\$1000) | 町の中 (5~100マイル)、または中リスクとタグ付けされた地域  | 過去のデータとほとんど一致する | いくつかの確認済みデータ (中) | 中リスク         |     |
| 高 (たとえば、銀行、セキュリティ設定)    | 高 (たとえば、>\$1000)      | 遠方 (>100マイル)、または高リスクとタグ付けされた地域    | 過去のデータと矛盾する     | 確認済みデータなし (高)    | 高リスク         |     |

【図 4】

信用インデックス

| 400 | 402               | 404                                     | 406             | 信用レベル    |
|-----|-------------------|---|-----------------|----------|
|     | 認証プロセス (バイオメトリクス) | ソフトバイオメトリクス (たとえば、髪の色) 指/ハンドジオメトリ ECG走査 | 音声走査 顔面走査 パスワード | 低 (1~3)  |
|     |                   | 指紋走査 虹彩走査                               |                 | 中 (4~7)  |
|     |                   |   |                 | 高 (8~10) |

[illegible]

前記プロセッサが、前記センサー入力に基づいて信用インデックスを決定するようにさ

らに構成される、請求項2に記載のモバイルデバイス。

【請求項4】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされる、請求項3に記載のモバイルデバイス。

【請求項5】

認証プロセスがユーザ定義される、請求項1に記載のモバイルデバイス。

【請求項6】

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定するステップと、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択するステップであって、前記認証プロセスに関連付けられた信用レベルが、音、光、または動きの周辺レベルのうちの少なくとも1つに基づいて調整される、ステップと、

前記認証プロセスを実行するステップと

を含む方法。

【請求項7】

コンテキスト入力に基づいてリスクインデックスを決定するステップをさらに含む、請求項6に記載の方法。

【請求項8】

前記センサー入力に基づいて信用インデックスを決定するステップをさらに含む、請求項7に記載の方法。

【請求項9】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされる、請求項8に記載の方法。

【請求項10】

認証プロセスがユーザ定義される、請求項6に記載の方法。

【請求項11】

プロセッサによって実行されたとき、前記プロセッサに、

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のためのモバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定すること、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択することであって、前記認証プロセスに関連付けられた信用レベルが、音、光、または動きの周辺レベルのうちの少なくとも1つに基づいて調整されること、および

前記認証プロセスを実行すること

を行わせるコードを含む非一時的コンピュータ可読記録媒体。

【請求項12】

コンテキスト入力に基づいてリスクインデックスを決定するためのコードをさらに含む請求項11に記載のコンピュータ可読記録媒体。

【請求項13】

前記センサー入力に基づいて信用インデックスを決定するためのコードをさらに含む請求項12に記載のコンピュータ可読記録媒体。

【請求項14】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされる、請求項13に記載のコンピュータ可読記録媒体。

【請求項15】

ユーザ定義された認証プロセスを可能にするためのコードをさらに含む請求項11に記載のコンピュータ可読記録媒体。

【請求項16】

アプリケーションまたはサービスプロバイダのうちの少なくとも1つとの認証のための

モバイルデバイス機能、およびセンサー入力に基づいて、複数の認証プロセスを決定するための手段と、

前記複数の認証プロセスの中からセキュリティ要件を満たす認証プロセスを選択するための手段であって、前記認証プロセスに関連付けられた信用レベルが、音、光、または動きの周辺レベルのうちの少なくとも1つに基づいて調整される、手段と、

前記認証プロセスを実行するための手段と  
を備えるモバイルデバイス。

【請求項 17】

コンテキスト入力に基づいてリスクインデックスを決定するための手段をさらに備える請求項16に記載のモバイルデバイス。

【請求項 18】

前記センサー入力に基づいて信用インデックスを決定するための手段をさらに備える請求項17に記載のモバイルデバイス。

【請求項 19】

前記信用インデックスが前記リスクインデックスよりも大きい場合、前記セキュリティ要件が満たされると決定するための手段をさらに備える請求項18に記載のモバイルデバイス。

【請求項 20】

ユーザ定義された認証プロセスを可能にするための手段をさらに備える請求項16に記載のモバイルデバイス。

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No

PCT/US2015/047578

## A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/06

ADD. H04L29/06

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)

G06K H04L H04W G06Q

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

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

EPO-Internal, COMPENDEX, INSPEC, WPI Data

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|-----------|--|-----------------------|
| X         | EP 2 743 873 A1 (ACCENTURE GLOBAL SERVICES LTD [IE]) 18 June 2014 (2014-06-18)<br>paragraphs [0027] - [0066]<br>figures 1-10<br>-----                  | 1-20                  |
| X         | US 2014/157401 A1 (ALAMEH RACHID M [US] ET AL) 5 June 2014 (2014-06-05)<br>paragraphs [0013] - [0035]<br>figures 1-4<br>-----                          | 1-20                  |
| X         | US 2014/208419 A1 (CHANG MATTHEW-LOUIS CHEN WEN [GB] ET AL)<br>24 July 2014 (2014-07-24)<br>paragraphs [0038] - [0059]<br>figures 1-5<br>-----<br>-/-- | 1-20                  |

☒ 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 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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

6 November 2015

Date of mailing of the international search report

16/11/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel: (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

Ghomrasseni, Z

**INTERNATIONAL SEARCH REPORT**

International application No

PCT/US2015/047578

| C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |  |                       |
|--|--|-----------------------|
| Category*  | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| X  | US 2013/267204 A1 (SCHULTZ PAUL T [US] ET AL) 10 October 2013 (2013-10-10)<br>paragraphs [0018] - [0058]<br>figures 1-6<br>----- | 1-20                  |

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No

PCT/US2015/047578

| Patent document<br>cited in search report |    | Publication<br>date | Patent family<br>member(s)   | Publication<br>date  |
|---|----|---------------------|--|--|
| EP 2743873                                | A1 | 18-06-2014          | AU 2013270621 A1<br>CA 2836717 A1<br>EP 2743873 A1<br>US 2014172707 A1                                       | 03-07-2014<br>14-06-2014<br>18-06-2014<br>19-06-2014                             |
| US 2014157401                             | A1 | 05-06-2014          | US 2014157401 A1<br>WO 2014085658 A2   | 05-06-2014<br>05-06-2014   |
| US 2014208419                             | A1 | 24-07-2014          | CN 104937909 A<br>DE 112013006496 T5<br>GB 2510120 A<br>GB 2525361 A<br>US 2014208419 A1<br>WO 2014114998 A1 | 23-09-2015<br>05-11-2015<br>30-07-2014<br>21-10-2015<br>24-07-2014<br>31-07-2014 |
| US 2013267204                             | A1 | 10-10-2013          | NONE   |  |



## 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, ST, 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, 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 . Z I G B E E

(72)発明者 クアツィ・バシール

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ジョナサン・キース

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 スザーナ・アレラーノ

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

(72)発明者 ヴァージニア・キーティング

アメリカ合衆国・カリフォルニア・9 2 1 2 1 - 1 7 1 4・サン・ディエゴ・モアハウス・ドライブ・5 7 7 5

Fターム(参考) 5K127 AA21 BA03 GE02 HA08 HA11 JA07 JA21 JA25 JA41 JA48  
JA49 KA20