(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6134880号
(P6134880)

(45)発行日　平成29年5月31日(2017.5.31)　(24)登録日　平成29年5月12日(2017.5.12)

(51)Int.Cl.		F I		
G06F 21/32	(2013.01)	G06F	21/32	
H04W 12/06	(2009.01)	H04W	12/06	
H04M 3/42	(2006.01)	H04M	3/42	E

請求項の数 17　(全 13 頁)

(21)出願番号	特願2014-539022(P2014-539022)
(86)(22)出願日	平成24年10月25日(2012.10.25)
(65)公表番号	特表2015-504195(P2015-504195A)
(43)公表日	平成27年2月5日(2015.2.5)
(86)国際出願番号	PCT/US2012/061999
(87)国際公開番号	WO2013/063326
(87)国際公開日	平成25年5月2日(2013.5.2)
審査請求日	平成27年10月26日(2015.10.26)
(31)優先権主張番号	61/609,824
(32)優先日	平成24年3月12日(2012.3.12)
(33)優先権主張国	米国(US)
(31)優先権主張番号	61/693,690
(32)優先日	平成24年8月27日(2012.8.27)
(33)優先権主張国	米国(US)

(73)特許権者　510319351
セールスフォース・ドットコム　インコーポレーテッド
アメリカ合衆国　カリフォルニア州　９４１０５，サンフランシスコ，ザ　ランドマーク　アット　ワン　マーケット　ストリート，スイート　３００
(74)代理人　100109634
弁理士　舛谷　威志
(74)代理人　100129263
弁理士　中尾　洋之
(74)代理人　100163991
弁理士　加藤　慎司
(74)代理人　100146374
弁理士　有馬　百子

最終頁に続く

(54)【発明の名称】２要素認証システムおよび方法

(57)【特許請求の範囲】

【請求項１】

認証サーバが、ユーザと関連付けられたモバイルデバイスへ第１許可リクエストを送る工程であって、前記第１許可リクエストはアクションを実行するためのものであり、前記モバイルデバイスは、少なくとも１つの自動化基準が満たされた場合には前記アクションと同じアクションの将来の許可リクエストに対する応答を自動化するか否かの選択をユーザに可能にするメッセージを前記モバイルデバイスに表示させることができる命令を保存するメモリを備えている、第１許可リクエストを送る工程と、

前記認証サーバが、前記第１許可リクエストを送る工程の後に、前記同じアクションを実行するために前記モバイルデバイスへ第２許可リクエストを送る工程と、

前記認証サーバが、前記メッセージに対して前記モバイルデバイスで受信されたユーザ入力に基づいて前記モバイルデバイスによって自動生成された前記第２許可リクエストへの応答を受信する工程と、

を含む、方法。

【請求項２】

前記少なくとも１つの自動化基準は、前記モバイルデバイスの地理的位置に基づく、請求項１に記載の方法。

【請求項３】

前記少なくとも１つの自動化基準は、前記ユーザの生体情報に基づく、請求項１に記載の方法。

【請求項４】
前記少なくとも１つの自動化基準は、前記ユーザの指紋に基づく、請求項１に記載の方法。
【請求項５】
前記少なくとも１つの自動化基準は、前記ユーザの声に基づく、請求項１に記載の方法。
【請求項６】
前記少なくとも１つの自動化基準は、地理的位置、生体情報、および／または前記ユーザの声、の組み合わせに基づく、請求項１に記載の方法。
【請求項７】
前記少なくとも１つの自動化基準が満たされるか否かを判別する情報は、前記モバイルデバイス上に保存される、請求項１に記載の方法。
【請求項８】
モバイルデバイスであって、
１または複数のプロセッサと、
１または複数のメモリと、を備え、
前記１または複数のメモリは、前記モバイルデバイスに工程を実行させるようになっているプログラム命令を保存しており、前記工程は、
認証サーバから、アクションを実行するための許可リクエストを受信する工程と、
少なくとも１つの自動化基準に基づいて、前記アクションと同じアクションの将来の許可リクエストに対する自動応答を選択するための選択肢を表示する工程と、
自動応答を選択するユーザの入力を受信する工程と、
前記ユーザのためのアクションを実行するための後続の許可リクエストを受信する工程と、
前記後続の許可リクエストが前記少なくとも１つの自動化基準を満たすか否かを判断する工程と、
前記判断する工程における判断に応じて、前記後続の許可リクエストへの許諾または拒否を示すユーザの入力を受信することなく、前記後続の許可リクエストに自動で応答する工程と、
を含む、モバイルデバイス。
【請求項９】
前記許可リクエストは認証サービスから受信され、前記モバイルデバイスは前記認証サービスとペアリングされる、
請求項８に記載のモバイルデバイス。
【請求項１０】
前記少なくとも１つの自動化基準は、前記ユーザの生体情報または前記ユーザの指紋に関連付けられた基準を含む、
請求項８に記載のモバイルデバイス。
【請求項１１】
前記少なくとも１つの自動化基準が満たされるか否かを判別する情報は、前記モバイルデバイス上に保存される、請求項８に記載のモバイルデバイス。
【請求項１２】
プログラム命令が保存されたコンピュータ可読媒体であって、
前記プログラム命令は、モバイルデバイスに工程を実行させるものであって、前記工程は、
認証サーバからアクションを実行するための第１許可リクエストを受信する工程と、
少なくとも１つの自動化基準が満たされた場合には前記アクションと同じアクションの将来の許可リクエストに対する応答を自動化するか否かの選択をユーザに可能にするメッセージを表示させる工程と、
前記メッセージに対する第１ユーザ入力を受信する工程と、

前記第１ユーザ入力を受信した後に、前記アクションと同じアクションを実行するために前記認証サーバから第２許可リクエストを受信する工程と、
前記第２許可リクエストが前記少なくとも１つの自動化基準を満たすか否かを判断する工程と、
前記判断する工程における判断に応じて、前記第２許可リクエストへの許諾または拒否を示すユーザの入力を追加で要求することなく、前記第１ユーザ入力に基づいて前記第２許可リクエストに自動で応答する工程と、
を含む、コンピュータ可読媒体。
【請求項１３】
前記少なくとも１つの自動化基準は、前記ユーザが自動応答を選択した地理的領域内に前記モバイルデバイスが物理的に位置しているという基準を含む、
請求項１２に記載のコンピュータ可読媒体。
【請求項１４】
前記アクションは、前記モバイルデバイスとは異なるコンピュータデバイスを介して要求される、
請求項１２に記載のコンピュータ可読媒体。
【請求項１５】
前記工程は、
前記少なくとも１つの自動化基準が変更された場合、前記第１および第２許可リクエストに関連するデバイスに事前シード自動応答を送信する工程をさらに含む、
請求項１２に記載のコンピュータ可読媒体。
【請求項１６】
前記アクションは、認証アクションである、
請求項１２に記載のコンピュータ可読媒体。
【請求項１７】
前記少なくとも１つの自動化基準が満たされるか否かを判別する情報は、前記モバイルデバイス上に保存される、請求項１２に記載のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、米国仮出願第６１／５５１，３７０号（出願日：２０１１年１０月２５日）、米国仮出願第６１／６０９，８２４号（出願日：２０１２年３月１２日）および米国仮出願第６１／６９３，６９０号（出願日：２０１２年８月２７日）の優先権の利益を主張する。
【０００２】
本発明の実施形態は、認証システムおよび方法に関し、より具体的には、モバイルデバイス内の地理位置情報ツールを用いた、そのようなシステムおよび方法に関する。
【背景技術】
【０００３】
セキュリティコミュニティにおいて、ユーザ認証手段として、パスワードを補完し、補強するための実行可能な第２の要素が長い間求められてきた。従来の試みにおける解決法は、高コストおよび煩雑過ぎるため、主流の解決方法として採用されるには至っておらず、そのため、従来の試みは行き詰っている。
【０００４】
セキュリティコミュニティとって残念なことに、パスワードは、未だに大部分のユーザアカウントに対する唯一の認証メカニズムとしての地位を強固に保っている。その主な理由は、パスワードによるアカウントホルダの提供が単純かつ容易であるという点にある。しかしながら、パスワードのみが単一の認証要素として用いられた場合、多くの問題が連鎖的に発生することとなる。すなわち、パスワードは記憶しておくことが困難であるかまたは推測することが容易であることが多く、ユーザは、多数のアカウントに対して同じパ

スワードを使い回すことが多く、パスワードはクライアントおよびサーバ双方において非セキュアに保存される場合が多い等々、その他様々な問題が発生する。そのため、この厄介な第１の要素を補完および補強することが可能な追加的なメカニズムについての切迫したニーズが、長年存在している。長年にわたり、多数の解決法が提案されているが、どの解決法も、この極めて必要とされている第２の要素を提供するものの、多様な理由に起因して、比較的少数のニッチユーザを除いては、いずれも広範な採用には至っていない。そのため、主流の大多数のユーザは保護されておらず、既存の認証ルーチンに対して大きく影響を与えない解決法があれば、主流の大多数のユーザーは、大きな恩恵を受けることができるであろう。

【０００５】

近年、いくつかの２要素認証（ＴＦＡ：Two-Factor Authentication）メカニズムが用いられている。しかしながら、これらの既知の解決法は、いずれも理想的ではない。すなわち、現在用いられている多くのＴＦＡメカニズムは、セキュリティトークンを中心として使用している。このスキームにおいては、ユーザに対し、トークンが発行される。トークンは、定期的に変化し、一見乱数のようにみえる数字を表示する画面を備える小型ハードウェアデバイスを用いて発行されることが多い。トークンをネットワークリソースとペアリングしたユーザは、画面上に現在表示されている数字を、任意の所与の瞬間におけるログイン手順の一部として、（第１の認証要素である静的パスワードに加えて）入力しなければならない。提供されたコードが、所与のインスタンス用のトークンアウェアバックエンド（token-aware backend）での期待値と整合した場合、システムは認証リクエストを承諾する。つまり、システムは、（何らかの既知の）パスワードおよびトークン画面からの（何らかの所有された）有効コードを提供するリクエストが、正当なリクエストである可能性が合理的に高いとみなす。ハードウェアトークンを用いるセキュリティスキームは、２要素認証機構として比較的成功を収めている。しかしながら、これらのスキームは、使用が必須である（例えば、企業ＶＰＮへのログイン用等）環境にしか使用されていない。これらの使用が必須である環境を除いて広範に採用されていない理由として、採用を阻む以下の２つの主な障壁がある。すなわち、１つ目の障壁は、このようなシステムの実施には、多大なインフラストラクチャ（例えば、複雑なバックエンドサーバ、ハードウェアコスト等）が要求されることにあり、２つ目の障壁は、ログインが要求される度に、トークンを読み出し、コードを入力しなければならないというユーザにとっての利便性の欠如にある。

【０００６】

より最近の解決法は、困難なインフラストラクチャ要求のうちいくつかを軽減できている（例えば、ＦａｃｅｂｏｏｋおよびＧｏｏｇｌｅのような企業によって展開されているＴＦＡメカニズム）。これらの種類のメカニズムは、多数のユーザが既に個人的に所持しているモバイルデバイス上に常駐するソフトウェアベースのトークンを提供している。しかしながら、これらのシステムは、ユーザが自身のモバイルデバイスを取り出し、必要なアプリケーションを起動し、モバイルデバイス画面上に現在表示されているコードを入力することを依然として要求している。多くのユーザにとって、この解決法は煩雑であり、苛立ちの元である。

【０００７】

いくつかの他の最近の解決法は、より大規模な認証プロセスの一部として、モバイルデバイスの位置認識を用いている。しかしながら、これらのアプローチは、ユーザ位置または他の識別情報の中央サーバへの送信を必要としている。そのため、データ保存がセキュアに行われていないサードパーティサーバ上に大量の個人データ（例えば、日常的な旅行習慣）が保存されるという、ユーザにとってプライバシー上の懸念が発生する。

他の位置ベースのアプローチは、認証を試みている端末デバイスに対する演繹的またはオンデマンドの位置認識を必要としている。

よって、複雑なインフラストラクチャ実装の必要を無くしつつ、ユーザへの過大な負担無くＴＦＡを達成するシステムに対するニーズが存在している。

【発明の概要】
【発明が解決しようとする課題】
【０００８】
認証方法の一実施形態は、以下の工程を含む。ユーザの代わりにアクションを実行するために、認証サービスから認証リクエストが受信される。アクションを実行する許可を承諾または拒否するために、許可リクエストが、ユーザと関連付けられたモバイルデバイスへと送られる。許可応答が、認証サービスへ送られる。許可応答を自動化するための任意選択肢がユーザへ提供される。ここで、将来の許可リクエストは、少なくとも１つの自動化基準を満たす。
【０００９】
認証システムの一実施形態は、以下の要素を含む。少なくとも１つのプロセッサと、少なくとも１つのプロセッサを制御して以下を含む工程を実行させるための命令が保存されている少なくとも１つのメモリ要素とを含む。ユーザの代わりにアクションを実行するために、認証サービスから、認証リクエストが受信される。アクションを承諾または拒否するための許可リクエストが、ユーザと関連付けられたモバイルデバイスへと送られる。許可応答が、認証サービスへ送られる。許可応答を自動化するための任意選択肢がユーザへ提供される。ここで、将来の許可リクエストは、少なくとも１つの自動化基準を満たす。ユーザが自動化するよう任意選択肢を選択した場合、将来の許可リクエストを承諾または拒否するようユーザに指示を促すことなく将来の許可リクエストを自動的に生成するよう、許可応答が自動化される。
【００１０】
非一時的コンピュータ可読媒体の実施形態は、１つ以上の命令シーケンスを含む。これらの命令が１つ以上のプロセッサによって実行されると、１つ以上のプロセッサは、以下を含む工程を実行する。ユーザの代わりにアクションを実行するために、認証サービスから、認証リクエストが受信される。アクションの実行を承諾または拒否するために、許可リクエストが、ユーザと関連付けられたモバイルデバイスへ送られる。許可応答が、認証サービスへ送られる。許可応答を自動化するための任意選択肢がユーザへ提供される。ここで、将来の許可リクエストは、少なくとも１つの自動化基準を満たす。ユーザが自動化するよう任意選択肢を選択した場合、将来の許可リクエストを承諾または拒否するようユーザに指示を促すことなく、将来の許可リクエストに対する許可応答が自動化される。
【００１１】
認証サービスからの許可リクエストを認証するためのモバイルデバイスの一実施形態において、モバイルデバイスは、プロセッサを含み、以下を含む動作を実行することができる。許可リクエストが、認証サービス端末から受信される。該許可リクエストに関連する情報が提示される。許可応答を判別するために、ユーザからの感覚入力が受信される。許可応答が認証サービス端末へ送られる。少なくとも１つの自動化基準が満たされる場合に、将来の許可リクエストに対する許可応答を自動化するか否かを選択するユーザからの感覚入力が受信される。これにより、将来の許可応答は、ユーザからの感覚入力を必要としなくなる。少なくとも１つの自動化基準が満たされるか否かを判別するために必要な情報が、モバイルデバイス上に保存される。
【図面の簡単な説明】
【００１２】
【図１】は、認証方法のフローチャートである。
【図２】は、認証システムを示す図である。
【図３】は、例示的なモバイル認証デバイスからの一連のスクリーンショットを示す。
【図４】は、例示的なモバイル認証デバイスからの一連のスクリーンショットを示す。
【図５】は、モバイル認証デバイスからのスクリーンショットを示す。
【図６】は、許可リクエストを認証するために、モバイルデバイスによって実行され得る動作のフローチャートを示す。
【発明を実施するための形態】

【００１３】
本発明の実施形態は、多数の様態で実行することができる（例えば、方法、プロセス、装置、システム、組成物、コンピュータ可読媒体（例えば、コンピュータ可読記憶媒体または、プログラム命令が光学リンクまたは通信リンクを介して送られるコンピュータネットワーク）。タスクを実行するよう構成されたコンポーネント（例えば、プロセッサまたはメモリ）は、タスクを所与の時期に実行するよう一時的に構成された汎用コンポーネントおよび／またはタスクを実行するよう製造された特定のコンポーネントの双方の一般的なコンポーネントを含む。一般的に、開示の方法またはプロセスの工程の順序は、本発明の範囲内において変更することが可能である。
【００１４】
本発明の１つ以上の実施形態の詳細な説明を、添付図面と共に以下に示す。添付図面は、動作の原理を示す。本発明の実施形態について詳細に説明するが、本発明は任意の実施形態に限定されない。本発明の範囲は、特許請求の範囲のみによって限定され、本発明は、多数の改変例、変更例および均等例を包含する。以下の記載において、本発明の深い理解を提供するために、多数の特定の詳細について説明する。これらの詳細は、例示のためのものであり、本発明は、特許請求の範囲に従って（特定の詳細のうち一部または全てを必要とすることなく）実行することが可能である。明瞭性のため、本発明に関連する技術分野において公知である技術的事項については、本発明を不必要に不明瞭にしないために詳述を控える。
【００１５】
ここで、多様な様態について、コンピュータシステムの要素によって実行可能なアクションシーケンスとの文脈から記述される特定の様態を含む、例示的な実施形態に関連して説明を行う。例えば、実施形態それぞれにおいて、多様なアクションは、特殊な回路、回路構成（例えば、特殊機能を行うように相互接続された個別のおよび／または集積された論理ゲート）、１つ以上のプロセッサによって実行されるプログラム命令、または任意の組み合わせによって実行可能であることは理解されるであろう。よって、多様な様態は、多数の異なる形態において実装することができ、このような形態は全て、記述される事項の範囲内である。ユーザアクションを認証するためのコンピュータプログラムの命令は、命令実行システム、装置またはデバイスによって用いられるか、命令実行システム、装置またはデバイスと併せて用いられる任意のコンピュータ可読媒体内に実装することができる（例えば、コンピュータ可読媒体、装置またはデバイスから命令をフェッチし、当該命令を実行することが可能なコンピュータベースのシステム、プロセッサを含むシステム、または他のシステム）。
【００１６】
本明細書中において用いられる「コンピュータ可読媒体」という用語は、命令実行システム、装置またはデバイスによって用いられるか、命令実行システム、装置またはデバイスに併せて用いられるプログラムを含むか、保存するか、通信するか、伝達させるか、転送し得る任意の手段であり得る。コンピュータ可読媒体の例を非限定的に挙げると、電気、磁気、光学、電磁気、赤外線または半導体システム、装置、デバイスまたは伝播媒体を挙げることができる。コンピュータ可読媒体のより詳細な例を以下に挙げる：１つ以上のワイヤを有する電気接続、ポータブルコンピュータディスケットまたはコンパクトディスクリードオンリーメモリ（ＣＤ－ＲＯＭ）、ランダムアクセスメモリ（ＲＡＭ）、リードオンリーメモリ（ＲＯＭ）、消去可能プログラマブルリードオンリーメモリ（ＥＰＲＯＭまたはフラッシュメモリ）および光ファイバ。他の種類のコンピュータ可読媒体もこれに企図される。
【００１７】
本発明の実施形態により、規定されたユーザアクションの認証を提供するシステムおよび方法が提供される。これは、現代のモバイルデバイス（例えば、スマートフォン、タブレットコンピュータ等）のネットワーク接続性および位置認識を利用することにより行われ、これにより、自動化されかつ目立たない要素認証が提供される。このような要素認証

は、典型的には、第１の要素（例えば、ユーザ名／パスワードログインの組み合わせ）と併せて用いられる認証の第２の要素である。

【００１８】

図１は、本発明の実施形態に係る認証方法のフローチャートである。認証サービスは、ユーザの代わりにアクションを実行するために、認証サービスから認証リクエストを受信する。その後、認証サービスは、ユーザに関連付けられたモバイルデバイスへ許可リクエストを送り、アクションを実行することを望むか否かについてユーザに尋ねる。ユーザは、許可応答をモバイルデバイスを介して認証サービスへ送り、アクションを承諾または拒否する。ユーザに対し、（少なくとも１つの自動化基準（例えば、モバイルデバイスの物理的位置）が満たされる限り）将来の類似の応答を自動化するための任意選択肢が提供され、これにより、将来の許可リクエストに対し手動で応答する必要が無くなる。自動化基準が満たされているか否かを判別するために必要な情報は、モバイルデバイス上にローカルに保存される。

【００１９】

認証サービス（例えば、ログインを要求するウェブサイトまたは車両セキュリティコンピュータ）がユーザアクションを認証する必要がある場合、認証リクエストが認証サービスへ送られる。認証リクエストが認証サービスから送られているのであれば、表面上は第１の認証要素は既に提供されている。ウェブサイトの場合、第１の要素は、通常、ユーザ名／パスワードの組み合わせである。車両セキュリティシステムの例において、第１の認証要素は、鍵からの信号であり得る。図１に示す認証方法により、第１の要素によって提供されるセキュリティを増強する第２の要素を提供するための能率化されたプロセスが得られる。上記した認証サービスは例示である。実際、本明細書中全体において、例示的なウェブサービスへログインするアクションについて言及している。しかしながら、これは、あくまで、本明細書中により詳細に記載するような本発明の実施形態を用いて認証可能な１つのアクションにすぎないことは理解されるだろう。

【００２０】

プロセスを能率化する１つの方法は、ユーザによる繰り返しの承諾／拒否許可応答の必要性を無くすことにある。本発明の実施形態は、ほとんどの現代のモバイルデバイスに既に備えられている位置認識技術を用いることにより、これを達成する。位置認識により、認証プロセスをさらに自動化し、繰り返しの承諾／拒否アクションの必要性を無くす１つの方法が得られ、これにより、例えばユーザのモバイルデバイスをポケット、パース内にまたはユーザの近隣のドッキングステーション上に収容したままにしておくことが可能になる。

【００２１】

これは、アクション（例えば、サービスへのログオン）と、当該アクションが開始された物理的位置との間の直観的ペアリングにより可能とされる。例えば、ユーザは、典型的には、所与のデバイスを用いて位置のうちのごく一部（例えば、自宅、仕事場、地域の喫茶店）から電子メールを確認する。ユーザがこれらの位置のうちの１つに居るときに既知のデバイスからログインを試みた場合、これが正当なリクエストである可能性は有意に増加する。よって、自動化すべきリクエストの種類をモバイルデバイスに「教示する」認証アプリケーションを用いることにより、慣れ親しんだ位置からのこれらの許可応答を自動化することができる。換言すれば、ユーザのモバイルデバイスは、自動化すべき認証リクエストを「学習」し、これにより、ユーザは、許可応答を送るための承諾／拒否アクションを繰り返し実行する必要が無くなる。

【００２２】

この学習プロセスは、いくつかの方法によって実施することができる。例えば、学習プロセスは、所与の認証リクエストを自動化すべきかについてユーザに尋ねるだけのようなシンプルなものであってもよいし、あるいは、ユーザ経験を能率化するためのいくつかの追加的な自動化メカニズムを含んでいてもよい。例えば、モバイルデバイスは、受信した認証リクエストを自動的に承諾し、認証リクエストが受信された位置を受信し、保存する

学習モードに入ることができる。この学習プロセスは、他の多数の方法で実施することも可能である。認証サービス、位置およびモバイルデバイスが関連付けられ（すなわち、学習され）ると、システムは、類似のリクエストが将来提示された場合、ユーザに任意の追加的なアクションを促すことなく、自動的に応答することができる。本方法／システムにより、ロバストかつ目立たない第２の認証要素の自動化のための迅速かつ容易な方法が提供される。

【００２３】

図２は、本発明の実施形態に係るコンポーネントを含む認証システム２００を示す図である。ユーザは、いくつかの認証端末２０２（例えば、自宅のコンピュータ、仕事用コンピュータ、喫茶店におけるラップトップ等）を用いて、認証サービス２０４（例えば、サードパーティウェブサイト）へアクセスする。ここで、第１の認証要素（例えば、パスワード）を認証端末２０２から認証サービス２０４へと通信する。認証サービス２０４は、認証サービス２０６と通信を実行し、ユーザアクションを確認する。これは、ユーザと関連付けられたモバイル認証デバイス２０８へ許可リクエストを送ることにより実行される。ユーザは、モバイルデバイス２０８を用いて、許可応答を認証サービス２０６へ送る。この許可応答は、認証サービス２０４にも送られ、認証の第２の要素が提供される。将来の許可応答は、モバイルデバイス２０８を介して自動化される。認証端末２０２、認証サービス２０４およびモバイルデバイス２０８それぞれに対し、ユニバーサルユニーク識別子（ＵＵＩＤ）が割り当てられる。ユニバーサルユニーク識別子（ＵＵＩＤ）は、認証サービス２０６内における識別のために用いられる。

方法およびシステムの実施形態において、２つの主要なアクション（すなわち、ペアリングおよび認証）が用いられる。

【００２４】

ペアリング

モバイル認証デバイス２０８が認証サービス２０４を認証するためには、両者をペアリングする必要がある。ペアリングプロセスは、後続の認証リクエストを成功させるために必要な任意の情報の通信を含む。例えば、認証サービス２０４が、認証リクエストを有効化するためにワンタイムパスワード（ＯＴＰ）を用いることを要求する場合、ペアリングプロセスにより、モバイル認証デバイス２０８と認証サービス２０４との間に（暗号鍵と同様の）共有秘密が確立される。後続の認証リクエストが出された場合、モバイル認証デバイス２０８は、この共有秘密を用いてＯＴＰを生成し、認証において共有秘密を用いて、ＯＴＰが正しいものであることを確認する。ペアリングプロセスは、追加的な情報（例えば、暗号鍵、デジタル署名情報）を要求してもよい。また、ペアリングプロセスは、ペアリング用のユニーク識別子を確立する。この識別子は、将来の認証リクエスト中に含められる。モバイルデバイス２０８は、既知の有効なペアリング識別子を含まない認証リクエストを放棄するように構成されていてもよい。

【００２５】

図３ａ～図３ｃは、認証サービス２０６のアプリケーションおよびアンドロイドオペレーティングシステムを実行する例示的なモバイル認証デバイス２０８からの一連のスクリーンショット３００、３１０および３２０を示す。図３ａにおいて、スクリーンショット３００は、モバイルデバイス２０８によって生成されたペアリングフレーズ３０２を示している。その後、このペアリングフレーズは、認証端末２０２においてユーザによって入力される。その後、認証サービス２０６は、図３ｂ中のスクリーンショット３１０に示すように、ペアリングリクエストをモバイルデバイス２０８へプッシュする。ペアリングリクエストは、ユーザ名３１２および認証サービス名３１４を含み、これにより、ユーザは、ペアリングを承諾する前に、ペアリングを確認するために必要な情報を得ることができる。図３ｃ中のスクリーンショット３２０は、モバイルデバイス２０８と、認証サービス２０４とのペアリングが成功した様子を示す。そして、認証サービス名３１４が、ペアリングされたサービスリスト中に表示される。

【００２６】

図４ａ～図４ｃに示す類似の１組のスクリーンショット４１０、４１２および４１４は、ｉＯＳプラットフォーム上の認証サービス２０６のアプリケーションを実行するモバイルデバイス２０８上で処理されるペアリングプロセスを例示する。図４ｃは、ペアリングされたサービスリストを示す。このリストから、認証サービス名４３２が選択される。ポップアップ対話ボックス４３４により、ユーザは、「ペアリング解除」ボタン４３６を用いてモバイルデバイス２０８を認証サービス２０４からペアリング解除するか、または、「位置消去」ボタン４３８を用いてペアリングリスト全体を消去することができる。

【００２７】

認証

本明細書中に開示される方法およびシステムの主な目的は、認証である。モバイルデバイス２０８が認証サービス２０６とペアリングされた後、ユーザによって実行されるべきアクションを認証サービス２０６が確認することを望む度に、実際の認証が発生する。この認証においては、典型的には、アクションを実行するための認証リクエストが受信される。認証リクエストが受信されると、認証サービス２０６は、リクエストの真正性を確認しなければならない。その後、アクションを行うことが許可されている旨を認証サービス２０４へ通信する。１つの可能な実施例として、ユーザは、自身のラップトップを用いて、ウェブベースの電子メールサービスへのログインを試みる。ここで、ラップトップは認証端末２０２であり、ウェブベースの電子メールサービスは、認証サービス２０４である。認証サービス２０４は（必ずしも必要ではないが）適切には、何らかの種類の第１の要素認証情報（例えば、パスワード）の提示をユーザに要求する。本明細書中に開示される方法およびシステムの実施形態を用いて、認証サービス２０４は、認証のための追加的な第２の要素をユーザに提供した後、認証リクエストを認証サービス２０６を通じて開始し、認証を試みているユーザ用に適切なペアリング識別子を提供する。認証サービス２０６は、許可リクエストを適切なモバイル認証デバイス２０８へと送る。適切なモバイル認証デバイス２０８は、本明細書中に概要を述べるような許可応答と共に応答を実行する。

上述したように、許可応答は、自動的に生成することもできるし、あるいは手動で生成することもできる。

【００２８】

自動化応答モードにおいて、モバイル認証デバイス２０８は、内部データベースを確認し、認証リクエストが少なくとも１つの自動化基準と整合するかを判別する。自動化用の基準を選択するための任意選択肢が多数存在し、メカニズムにより、認証サービス２０４が、自動化方針を柔軟に指定することが可能になる。１つの例示的な実施形態において、認証サービス２０４は、モバイル認証デバイスが保存されている位置の特定の近傍範囲内に存在する場合、ユーザが、特定の種類の許可リクエストが、承諾／拒否許可応答が自動生成されるように、指定することができる。認証リクエストが受信され、当該位置を保存するために当初用いられた同一端末の識別子から来たことが示される。これは、認証リクエストが生成されたときに、認証サービス２０４にログインするために用いられた端末２０２と、モバイル認証デバイス２０８の位置との間の直観的ペアリングを示す。自動化が可能である場合、命令（承諾または拒否）は、許可応答内にカプセル化された状態で認証サービス２０６へ送られる。この応答は、モバイルデバイス２０８をさらに確認するための現在有効なＯＴＰと、従来の暗号化およびデジタル署名メカニズムとを任意選択的に含み得る。

【００２９】

加えて、リクエスト自動化待ち時間が重要である場合、認証サービスが（オンデマンドでのモバイルデバイスとの接触を必ずしも必要とすることなく）適切に応答することが可能となるように自動化基準の状態が変化したとき、モバイル認証デバイス２０８は、許可応答を事前シード処理することができる。例えば、許可応答が自動化されている地理的領域にモバイルデバイスが進入または退出したとき、基準自動化状態が変化し得る。この特性の種類の事前シード処理方法は、「ジオフェンシング（geo-fencing）」として公知である。他の多数の方法を用いて、自動化された許可応答を事前シード処理することができ

る。

【００３０】

許可リクエストが既知の自動化データベース入力に整合しない場合、許可応答はデフォルトで拒否となるか、または、モバイルデバイス２０８は、シンプルに、許可応答を手入力するようユーザに促し得る。

【００３１】

自動化を達成することができない場合（例えば、位置信号の不良）または他の望ましくない場合、許可応答の手動生成を用いることができる。この場合、許可応答をユーザを促す。許可応答のリクエストに加えて、本発明の実施形態は、ユーザーが許可応答を促された際に、上記したような同じ認証決定を受けるべき類似の将来のリクエストをユーザに示す能力も含む。

【００３２】

図５ａおよび図５ｂに示すモバイルデバイス２０８のスクリーンショット５００および５２０は、手動の許可応答を要求する許可リクエストを提示している。スクリーンショット５００は、アンドロイドオペレーティングシステムを実行しているモバイルデバイス２０８上に表示された許可リクエストを示す。この実施形態において、許可リクエストは、認証サービス５０２の指示子、アクション記述５０４、ユーザ名５０６および端末記述５０８を含む。認証決定を通知するための関連情報が提示されると、ユーザは、対応するボタン５１０および５１２を用いて許可リクエストを承諾または拒否することができる。類似の将来の許可リクエストに対する許可応答の自動生成を（ユーザによる承諾または拒否を促すことなく）実行することをユーザが望む場合、自動化応答ボタン５１４が選択されることとなる。自動化がアクティブ化されると、自動化データベースは、将来の許可応答の生成に利用される許可リクエスト時におけるモバイル認証デバイス２０８の位置によって更新される。。

【００３３】

図６は、本発明の実施形態に係る許可リクエストを認証するために、モバイルデバイス２０８によって実行可能な動作のフローチャートである。モバイルデバイスは、認証サービス２０６から許可リクエストを受信する。許可リクエストに関連する情報が、ユーザに提示される。この情報は、画面上に視覚的に提示してもよいし、テキスト音声変換アプリケーションによって可聴形式で提示してもよいし、あるいは他の方法によって提示してもよい。モバイルデバイス２０８は、許可応答を判別するために、ユーザから感覚入力を受信するように構成されている。感覚入力は、触覚入力（例えば、ボタン押圧）、言語入力、または一定種類の入力を含む。その後、モバイルデバイス２０８は、許可応答を認証サービス２０６へ送る。また、モバイルデバイス２０８は、本明細書中に記載のように、許可応答を自動化するために、ユーザから感覚入力を受信するようにも構成されている。

【００３４】

上述したように、本明細書中に記載の例示的な方法およびシステムは、ウェブサイトへのログインアクションに焦点を当てたものである。しかしながら、記載の認証方法およびシステムは、コンピュータネットワークを介してアクセスまたはアクションを認証する必要がある任意の状況に適用可能である。例えば、実施形態の１つの方法は、車両自身の位置認識を利用し、さらに、車両位置認識を認証リクエストにおけるコンポーネントとして含ませることによって、車両セキュリティを向上させることができる。モバイルデバイスは、モバイルデバイスと車両とが相互に近接していない限り、許可リクエストを承諾しない。別の実施形態は、トランザクション確認を含み得る（例えば、クレジットカードプロセッサがクレジットカードトランザクション全体またはその一部を確認するための手段の提供）。

【００３５】

さらに、ペアリングされたモバイルデバイスがエントリーされた地点の近傍にある場合のみ、アクセスを許可することにより、物理的アクセス制御を増強することができる。この方法を認証手段として用いることにより、このようなアクセス制御をさらに向上させる

ことができる。この場合、１つ以上の追加的なペアリングされたデバイスが、承諾されるべきエントリーリクエストを承認する必要がある。例えば、メンテナンス作業者が工場のフロアーへの立ち入りを試みる際、メンテナンス作業者は、作業オーダーと共に立ち入りをリクエストすることができ、このリクエストは、工場管理者のモバイルデバイスへ送信され、明示的承認を受けた後、アクセスが承諾される。

【００３６】

また、本明細書中に記載の認証方法およびシステムは、他のよりセキュアな認証要素と共に用いることも可能である。例えば、より高いセキュリティが要求される用途（例えば、軍事現場における操作）の場合、モバイルデバイスからの許可応答と共に、生体認証要素（例えば、網膜スキャン、指紋、声プロファイル等）を要求してもよい。認証層を追加する毎に、セキュリティは飛躍的に高まる。

【００３７】

本明細書中に記載される本発明の実施形態は、バックエンドコンポーネント（例えば、データサーバ）を含むコンピューティングシステム、ミドルウェアコンポーネント（例えば、アプリケーションサーバ）を含むコンピューティングシステム、フロントエンドコンポーネント（例えば、（本明細書中に記載の本発明の実施形態とユーザとの相互通信を媒介する）グラフィカルユーザインターフェースまたはウェブブラウザを有するクライアントコンピュータ）を含むコンピューティングシステム、または１つ以上のこのようなバックエンド、ミドルウェアまたはフロントエンドコンポーネントの任意の組み合わせを含むコンピューティングシステムにおいて、実施することができる。本システムのコンポーネントは、任意のデジタルデータ通信（例えば、通信ネットワーク）の形態または媒体によって相互接続され得る。通信ネットワークの例として、ローカルエリアネットワーク（「ＬＡＮ」）および広域ネットワーク（「ＷＡＮ」）（例えば、インターネット）が挙げられる。

【００３８】

コンピューティングシステムは、クライアントおよびサーバを含み得る。クライアントおよびサーバは、相互に離隔位置にある場合が多いため、通信ネットワークを介して相互通信する場合が多い。クライアントおよびサーバの関係は、各コンピュータ上において実行しかつ相互にクライアントーサーバ関係を有するコンピュータプログラムによって得られる。

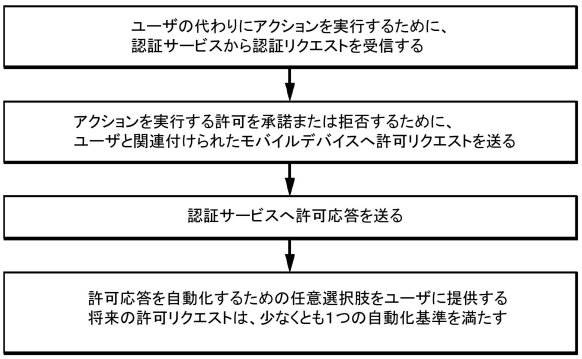
【００３９】

本明細書中、多数の特定の実施形態の詳細について述べたが、これらの詳細は、任意の発明の範囲の限定または特許請求の範囲の限定として解釈されるべきではなく、特定の発明の特定の実施形態に特有の特徴の記述として解釈されるべきである。本明細書中において別個の実施形態の文脈において述べた特定の特徴を、単一の実施形態において組み合わせて実行することが可能である。逆に、単一の実施形態の文脈において述べた多様な特徴を複数の実施形態において別個にまたは任意の適切なさらなる組み合わせで実行することも可能である。さらに、上記した特徴は、特定の組み合わせおよびさらには最初に特許請求の範囲中に述べたように機能し得るが、場合によっては、１つの請求項に記載される組み合わせからの１つ以上の特徴を当該組み合わせから削除し、当該請求項に記載の組み合わせをさらなる組み合わせまたはその変更例と共に用いることも可能である。

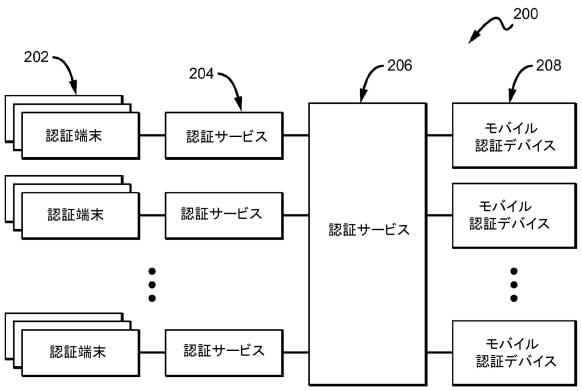
【００４０】

さらに、図面中に示すフローチャートは、所望の結果を達成するための図示の特定の順序または連続的順序に限定されない。また、他の工程を設けてもよいし、あるいは工程を記載のフローから削除してもよいし、記載のシステムに他のコンポーネントを追加してもよいし、あるいは記載のシステムから他のコンポーネントを除去してもよい。よって、他の実施形態も、以下の特許請求の範囲内である。

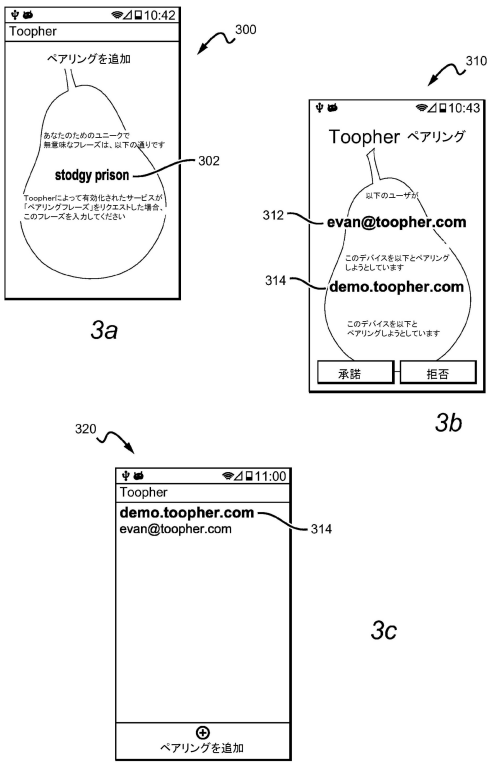
【図１】



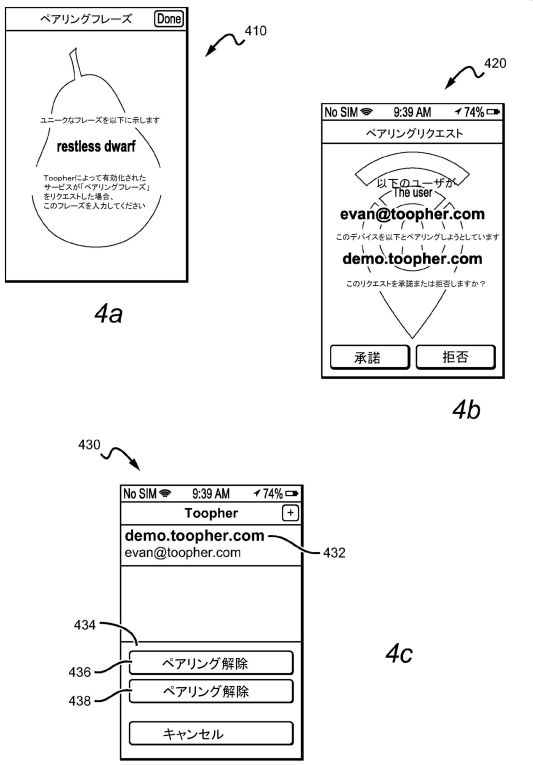
【図２】



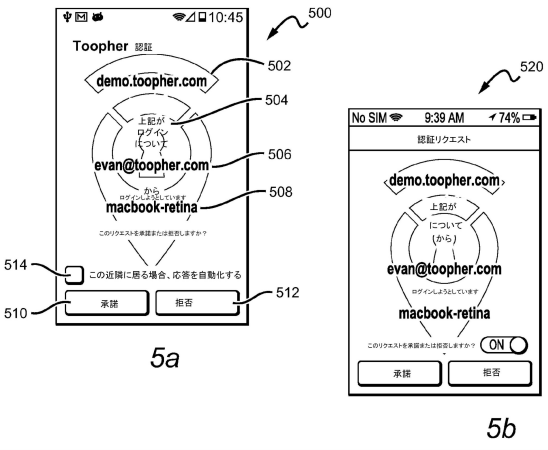
【図３】



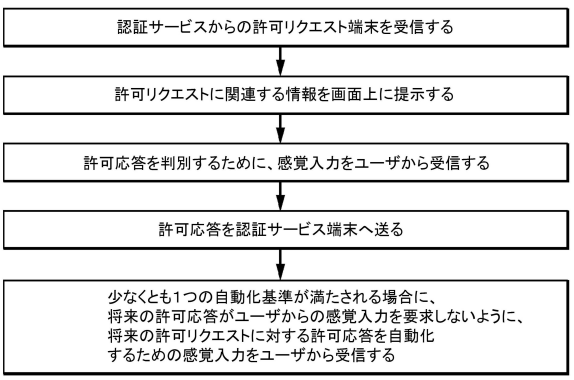
【図４】



【図５】



【図６】



フロントページの続き

(31)優先権主張番号　61/551,370
(32)優先日　平成23年10月25日(2011.10.25)
(33)優先権主張国　米国(US)

早期審査対象出願

(74)代理人　100153947
弁理士　家成　隆彦
(72)発明者　エヴァン、タイラー、グリム
アメリカ合衆国　テキサス州７８７０１，　オースティン，１７１７　ウェスト　第６　ストリート，スイート４６０

審査官　青木　重徳

(56)参考文献　国際公開第２００９／１４０３３３（WO，Ａ１）
特開２００９－１５１７９０（ＪＰ，Ａ）
特開２００７－０４２１０３（ＪＰ，Ａ）
米国特許出願公開第２０１０／０２１７８８０（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０２９３５９８（ＵＳ，Ａ１）
田中　俊昭　他，ＩＴＳにおけるエージェント認証・認可方式の検討，第６１回（平成１２年後期）全国大会講演論文集（３），日本，社団法人情報処理学会，２０００年１０月　３日，３Ｆ－７，ｐ．３－２４３～３－２４４

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２
Ｈ０４Ｍ　３／４２
Ｈ０４Ｗ　１２／０６