(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2017-520033
(P2017-520033A)
(43)公表日　平成29年7月20日(2017.7.20)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/35	(2013.01)	G06F	21/35		4C017
H04L 9/32	(2006.01)	H04L	9/00	673D	4C038
G06F 3/01	(2006.01)	G06F	3/01	514	5E555
A61B 5/11	(2006.01)	A61B	5/10	310A	5J104
A61B 5/117	(2016.01)	A61B	5/10	310G	

審査請求 未請求　予備審査請求 有　（全 53 頁）　最終頁に続く

(21)出願番号　特願2016-558389 (P2016-558389)
(86)(22)出願日　平成27年3月31日 (2015.3.31)
(85)翻訳文提出日　平成28年9月21日 (2016.9.21)
(86)国際出願番号　PCT/US2015/023719
(87)国際公開番号　WO2015/153688
(87)国際公開日　平成27年10月8日 (2015.10.8)
(31)優先権主張番号　61/975,684
(32)優先日　平成26年4月4日 (2014.4.4)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　14/444,620
(32)優先日　平成26年7月28日 (2014.7.28)
(33)優先権主張国　米国 (US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ビョルン・マーカス・ジェイコブソン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

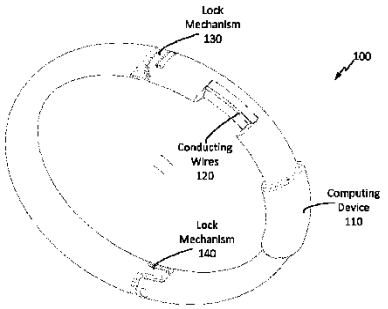
Fターム(参考)　4C017 AA10 AB02 AB03 DD14 FF17
4C038 VA04 VA07 VB11 VC20

最終頁に続く

(54)【発明の名称】ウェアラブルアイデンティティマネージャを容易にする方法および装置

(57)【要約】
ウェアラブルアイデンティティマネージャシステムに向けられた様々な態様が開示される。第1の態様では、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態は、ウェアラブルアイデンティティマネージャデバイスがユーザによって装着されているかどうかに基づいて確認され、ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータが監視される。動きデータを含む認証データは、次いで、関連付け状態に基づいて送信される。別の態様では、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態は、再び、ウェアラブルアイデンティティマネージャデバイスがユーザによって装着されているかどうかに基づいて決定される。ここでは、しかしながら、ウェアラブルアイデンティティマネージャデバイスは、ペアリングデバイスとペアリングされ、認証データは、ペアリングデバイスを介するユーザ認証を容易にするために、関連付け状態に基づいてペアリングデバイスに送信される。

FIG. 1



【特許請求の範囲】
【請求項１】
ウェアラブルアイデンティティマネージャデバイスであって、
メモリと、
前記メモリに通信可能に結合されたプロセッサと
を備え、前記プロセッサが、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づいて、ユーザと前記ウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定することと、
ユーザ認証を決定することを容易にすることと、
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視することと、
前記関連付け状態に基づいて認証データを送信することであって、前記認証データが前記動きデータを含む、ことと
を行うように構成された、ウェアラブルアイデンティティマネージャデバイス。
【請求項２】
前記プロセッサが、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングさせることと、
前記関連付け状態に基づいて、前記認証データを前記ペアリングデバイスに送信することと
を行うようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項３】
前記プロセッサが、関連付け手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けるように構成され、前記関連付け状態が前記関連付け手順の結果に基づく、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項４】
前記動きデータが、前記ウェアラブルアイデンティティマネージャデバイスによって横断された経路を含む、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項５】
前記プロセッサが、ジャイロ、全地球測位システム(GPS)デバイス、タッチ感知センサ、またはマイクロホンのうちの少なくとも1つからセンサデータを取得するようにさらに構成され、前記認証データが前記センサデータをさらに備える、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項６】
前記プロセッサが、留め金センサ、圧力センサ、温度センサ、脈拍センサ、動きセンサ、または伸縮センサのうちの少なくとも1つから取得されたデータに基づいて、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを推論するようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項７】
前記プロセッサが、
認証要求を受信することと、
信用証明書を提供することと、
前記認証要求に基づいて前記信用証明書を送信することと
を行うようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。

【請求項８】
前記プロセッサが、
認証要求を受信することと、
前記認証要求に関連付けられたセキュリティレベルを確認することと、
前記セキュリティレベルに基づいて前記認証データを送信することと
を行うようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項９】
1つまたは複数の命令が記憶されている非一時的機械可読記憶媒体であって、前記1つまたは複数の命令が、少なくとも1つのプロセッサによって実行されると、前記少なくとも1つのプロセッサに、
ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を確認することであって、前記関連付け状態が、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づいて確認される、ことと、
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視することと、
前記関連付け状態に基づいて認証データを送信することであって、前記認証データが前記動きデータを含む、ことと
を行わせる、非一時的機械可読記憶媒体。
【請求項１０】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングさせることと、
前記関連付け状態基づいて、前記ペアリングデバイスに前記認証データを送信させることであって、前記認証データが、前記ペアリングデバイスを介するユーザ認証を容易にする、ことと
を行わせる命令をさらに備える、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１１】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、認証手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けさせる命令をさらに備え、前記関連付け状態が前記認証手順の結果に基づく、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１２】
前記関連付け手順が、ローカルに記憶されたパスワードを、関連付けデバイスから受信されたパスワードと一致させることを含む、請求項11に記載の非一時的機械可読記憶媒体。
【請求項１３】
前記関連付け手順が、前記ウェアラブルアイデンティティマネージャデバイスの関連付け運動を、関連付けデバイスの運動に対応する受信されたデータと一致させること含む、請求項11に記載の非一時的機械可読記憶媒体。
【請求項１４】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
認証要求を受信することと、
ユーザアクション、または前記認証要求から推定された実行コンテキストのうちの少なくとも1つに基づいて、信用証明書を提供することと
を行わせる命令をさらに備える、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１５】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
認証要求を受信することと、
前記認証要求に関連付けられたセキュリティレベルを確認することと、

前記セキュリティレベルに基づいて前記認証データを提供することと
を行わせる命令をさらに備える、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１６】
前記セキュリティレベルが、ユーザの好みの設定、実行コンテキスト、または1つもしくは過去の実行コンテキストのうちの少なくとも1つに従って確認される、請求項15に記載の非一時的機械可読記憶媒体。
【請求項１７】
ワイヤレス通信を容易にする方法であって、
ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するステップであって、前記決定するステップが、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを決定するステップを含む、ステップと、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするステップと、
前記関連付け状態に基づいて、前記ペアリングデバイスに認証データを送信するステップであって、前記認証データが、前記ペアリングデバイスを介するユーザ認証を容易にする、ステップと
を含む方法。
【請求項１８】
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視するステップをさらに含み、前記認証データが前記動きデータを含む、請求項17に記載の方法。
【請求項１９】
関連付け手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けるステップをさらに含み、前記関連付け状態が、前記関連付け手順の結果に基づく、請求項17に記載の方法。
【請求項２０】
前記関連付け手順が、ローカルに保存されたパスワードを、関連付けデバイスから受信されたパスワードと一致させるステップを含む、請求項19に記載の方法。
【請求項２１】
前記関連付け手順が、前記ウェアラブルアイデンティティマネージャデバイスの関連付け運動を、関連付けデバイスの運動に対応する受信されたデータと一致させるステップを含む、請求項19に記載の方法。
【請求項２２】
前記ユーザに関連付けられた信用証明書を記憶するステップと、
認証要求に応じて前記ペアリングデバイスに前記信用証明書を提供するステップと
をさらに含む、請求項17に記載の方法。
【請求項２３】
前記認証要求に関連付けられたセキュリティレベルを確認するステップと、
前記セキュリティレベルに基づいて、前記ペアリングデバイスに送信される信用証明書の量を制限するステップと
をさらに含む、請求項22に記載の方法。
【請求項２４】
ウェアラブルアイデンティティマネージャデバイスであって、
ユーザと前記ウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するための手段であって、前記関連付け状態が、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づく、手段と、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするための手段と、
前記関連付け状態に基づいて前記ペアリングデバイスに認証データを送信するための手段であって、前記認証データが、前記ペアリングデバイスを介してユーザ認証を容易にす

る、手段と
を備えるウェアラブルアイデンティティマネージャデバイス。
【請求項２５】
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視する手段をさらに備え、前記認証データが前記動きデータを含む、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２６】
前記動きデータが、前記ウェアラブルアイデンティティマネージャデバイスによって横断された経路を含む、請求項25に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２７】
前記監視するための手段が、ジャイロ、タッチ感知センサ、またはマイクロホンのうちの少なくとも1つからセンサデータを受信するための手段をさらに備え、前記認証データが、前記センサデータをさらに含む、請求項25に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２８】
前記決定するための手段が、留め金センサ、圧力センサ、温度センサ、または伸縮センサのうちの少なくとも1つから受信されたデータに基づいて、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを推論するための手段をさらに備える、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２９】
認証要求を受信するための手段と、
前記認証要求に関連付けられたセキュリティレベルを確認するための手段と
をさらに備え、前記送信するための手段が、前記セキュリティレベルに基づいて前記ペアリングデバイスに前記認証データを送信するための手段を備える、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項３０】
前記確認するための手段が、複数の可能なセキュリティレベルから前記セキュリティレベルを選択するための手段を備える、請求項29に記載のウェアラブルアイデンティティマネージャデバイス。
【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、その内容全体が参照により本明細書に組み込まれている、2014年7月28日に出願した米国特許出願第14/444,620号、および2014年4月4日に出願した米国仮特許出願第61/975,684号の優先権および利益を主張するものである。
【０００２】
本開示の態様は、全体的には、ワイヤレス通信システムに関し、より具体的には、ユーザを認証することを容易にするウェアラブルアイデンティティマネージャシステムに関する。
【背景技術】
【０００３】
ユーザ認証は、不満および不正リスクの増加する源である。典型的な消費者は、複数のサービスに同じまたは非常に類似したパスワードを使用し、これは、違反が引き起こす不正への露出を増加させる。多くのユーザは、パスワードを入力することの困難さのため、モバイルデバイス上でパスワードを要求するサービスを使用することに抵抗する。パスワードマネージャが使用され得るが、それらは、友好的不正(すなわち、デバイス所有者に近いユーザによって開始される悪用の取引(abusive transactions))への露出を増加させ、デバイスの紛失に関連するリスクを増加させる。同様に、個人識別番号(PIN(personal

identification number))および他の形態の記憶ベースの認証は、同様の問題を引き起こす。

【発明の概要】

【課題を解決するための手段】

【０００４】

以下は、本開示の1つまたは複数の態様の基本的な理解を提供するために、そのような態様の簡略化された概要を提示する。この概要は、本開示のすべての企図される特徴の広範囲にわたる概観ではなく、本開示のすべての態様の主要なまたは重要な要素を特定することも、本開示の任意のまたはすべての態様の範囲を叙述することも意図していない。その唯一の目的は、後で提示されるより詳細な説明の前置きとして、簡略化した形態で本開示の1つまたは複数の態様のいくつかの概念を提示することである。

【０００５】

本開示の態様は、ユーザを認証することを容易にするウェアラブルアイデンティティマネージャシステムに向けられた方法、装置、コンピュータプログラム製品、および処理システムを提供する。一態様では、本開示は、ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態(association status)を決定するステップを含む、取引を容易にするための方法を提供する。方法は、ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするステップと、ペアリングデバイスを介するユーザ認証を容易にするために、関連付け状態に基づいて、ペアリングデバイスに認証データを送信するステップとをさらに含む。

【０００６】

別の態様では、取引を容易にするように構成されたウェアラブルアイデンティティマネージャデバイスが開示される。ウェアラブルアイデンティティマネージャは、検出器構成要素と、決定構成要素と、送信構成要素とを備える。ここで、検出器構成要素は、ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するように構成され、決定構成要素は、ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視するように構成されたセンサ構成要素を介してユーザ認証を決定することを容易にするように構成される。送信構成要素は、次いで、認証データが動きデータを含むように、関連付け状態に基づいて認証データを送信するように構成される。

【０００７】

さらなる態様では、取引を容易にするように構成された別のウェアラブルアイデンティティマネージャデバイスが開示される。ここで、デバイスは、ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するための手段と、ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするための手段とを備える。ウェアラブルアイデンティティマネージャデバイスは、認証データがペアリングデバイスを介するユーザ認証を容易にするように、関連付け状態に基づいてペアリングデバイスに認証データを送信するための手段をさらに備える。

【０００８】

さらに別の態様では、その上に記憶された1つまたは複数の命令を介して取引を容易にするように構成された非一時的機械可読記憶媒体が開示される。ここで、少なくとも1つのプロセッサによって実行されると、1つまたは複数の命令は、少なくとも1つのプロセッサに様々な動作を実行させる。動作は、ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を確認することと、ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視することとを含む。動作は、認証データが動きデータを含むように、関連付け状態に基づいて認証データを送信するこ

とをさらに含む。

【０００９】

これらの開示する態様および他の開示する態様は、以下の詳細な説明を検討すれば、より十分に理解されるであろう。添付図面とともに本発明の特定の例示的な態様の以下の説明を検討すれば、本発明の他の態様、特徴、および態様が当業者に明らかになろう。本発明の特徴は、以下のいくつかの態様および図面に関連して説明され得るが、本発明のすべての態様は、本明細書で説明される有利な特徴のうちの1つまたは複数を含み得る。言い換えれば、1つまたは複数の態様は、いくつかの有利な特徴を有するものとして説明され得るが、そのような特徴のうちの1つまたは複数はまた、本明細書で説明される本発明の様々な態様に従って使用され得る。同様に、例示的な態様は、デバイスの態様、システムの態様、または方法の態様として以下で説明され得るが、そのような例示的な態様は様々なデバイス、システム、および方法において実施され得ることを理解されたい。

【図面の簡単な説明】

【００１０】

【図１】本開示の一態様による、例示的なウェアラブルアイデンティティマネージャデバイスの概略図である。

【図２】ロックおよびアンロック構成における例示的なウェアラブルアイデンティティマネージャデバイスの概略図である。

【図３】本明細書の一態様による、ウェアラブルアイデンティティマネージャデバイスを介してユーザを認証することを容易にする例示的な環境を示す図である。

【図４】本開示のいくつかの態様による、ウェアラブルアイデンティティマネージャデバイスを利用することを容易にする例示的なプロセスを示すフローチャートである。

【図５】本開示の一態様による、ペアリングデバイスとペアリングされた例示的なウェアラブルアイデンティティマネージャデバイスの概略図である。

【図６】本開示のいくつかの態様による、処理システムを用いるウェアラブルアイデンティティマネージャデバイスの一例を示すブロック図である。

【図７】本開示の一態様による、例示的な検出器構成要素を示すブロック図である。

【図８】本開示のいくつかの態様による、ウェアラブルアイデンティティマネージャデバイスにユーザを関連付けることを容易にする例示的なプロセスを示すフローチャートである。

【図９】本開示のいくつかの態様による、ウェアラブルアイデンティティマネージャデバイスからユーザを分離することを容易にする例示的なプロセスを示すフローチャートである。

【図１０】本開示の一態様による、例示的な決定構成要素を示すブロック図である。

【図１１】本開示のいくつかの態様による、ユーザ認証を容易にするためにセンサデータが利用される例示的なプロセスを示すフローチャートである。

【図１２】本開示のいくつかの態様による、ユーザ認証を容易にするためにペアリングデバイスが利用される例示的なプロセスを示すフローチャートである。

【図１３】本開示のいくつかの態様による、ユーザ認証を容易にするために、確認されたセキュリティレベルに応じて信用証明書が送信される例示的なプロセスを示すフローチャートである。

【図１４】本開示の一態様による、アイデンティティマネージャと局との間の例示的な近接性検証(proximity verification)を示す概略図である。

【図１５】本開示の一態様による、アイデンティティマネージャと局との間の例示的な暗黙の保証および明示的な確認のプロトコルを示す概略図である。

【図１６】本開示の一態様による、販売時点端末における例示的なユーザ認証を示す第1の概略図である。

【図１７】本開示の一態様による、販売時点端末における例示的なユーザ認証を示す第2の概略図である。

【図１８】本明細書に記載の様々な実施形態が実装され得る例示的で非限定的なネットワ

ーク環境を表すブロック図である。
【図１９】本明細書に記載の様々な実施形態の1つまたは複数の態様が実装され得る例示的で非限定的なコンピューティングシステムまたは動作環境を表すブロック図である。
【発明を実施するための形態】
【００１１】
概要
背景で説明したように、従来のユーザ認証メカニズムの様々な制限のため、ユーザは、しばしば、潜在的な不正から自分自身を保護するために、ワイヤレスベースの認証取引を不必要に控える。本明細書に開示された態様は、ユーザがウェアラブルアイデンティティマネージャデバイスを装着しているかどうかに基づいてユーザを認証する認証インフラストラクチャを提供することによって、そのような制限を克服することに向けられている。すなわち、ユーザが自分自身をウェアラブルアイデンティティマネージャデバイスと関連付けることを可能にする態様が開示され、ウェアラブルアイデンティティマネージャデバイスは、ウェアラブルアイデンティティマネージャデバイスがユーザによって連続的に装着されている限り、別のデバイスへのユーザのワイヤレス認証を容易にするように構成される。
【００１２】
例示的なウェアラブルアイデンティティマネージャデバイス
次に図1を参照すると、例示的なウェアラブルアイデンティティマネージャデバイスが、本開示の一態様に従って提供されている。図示のように、ウェアラブルアイデンティティマネージャデバイス100は、第1のロック機構130と第2のロック機構140とを備える装着可能なブレスレットとして構成される。ウェアラブルアイデンティティマネージャ100はまた、コンピューティングデバイス110と導線120とを備え、コンピューティングデバイス110は、導線120間の接続が切断されているかどうかを検出するように構成される。すなわち、図2に示すように、ウェアラブルアイデンティティマネージャデバイス100は、ロック機構130を介してユーザに取付可能であることが企図され、ロック構成200は、導線120間の閉回路を作成し、アンロック構成205は、導線120間の回路を遮断する。さらに、コンピューティングデバイス110は、導線120間の接続が遮断されている(すなわち、アンロック構成205)か、または閉じられている(すなわち、ロック構成200)かに応じて、ウェアラブルアイデンティティマネージャデバイス100がユーザによって装着されているかどうかを検出することになることが企図される。
【００１３】
以下でより詳細に説明するように、ウェアラブルアイデンティティマネージャデバイス100が他のデバイスへユーザの認証を容易にすることを可能にすることは、最初に、ウェアラブルアイデンティティマネージャデバイス100とユーザとの間の関連付けを必要とする。たとえば、ユーザの手首にウェアラブルアイデンティティマネージャデバイス100を取り付ける際に、ユーザは、ウェアラブルアイデンティティマネージャデバイス100にユーザのアイデンティティを確認するために、(たとえば、コンピューティングデバイス110上のユーザインターフェースを介して、またはウェアラブルアイデンティティマネージャデバイス100とペアリングされた別のデバイスを介して)パスワードを入力することを要求されてもよい。ユーザのアイデンティティを確認すると、ウェアラブルアイデンティティマネージャデバイス100は、次いで、ロック機構130がロック構成のままである限り、認証データを他のエンティティ(たとえば、販売時点デバイス、料金所、金融機関ウェブサイト、など)にワイヤレス送信することによって、これらのエンティティによるその後のユーザ認証を容易にすることができることが企図される。そうでなければ、コンピューティングデバイス110が、ロック機構130がアンロックになったことを検出した場合、コンピューティングデバイス110は、ユーザがもはやウェアラブルアイデンティティマネージャデバイス100を装着していないと推論し、したがって、ユーザがウェアラブルアイデンティティマネージャデバイス100と再関連付けするまで、認証データを送信しないことになる。

【００１４】
代替実施態様では、ロッキング機構を使用するのではなく、様々な他のデバイスのいずれかは、ウェアラブルアイデンティティマネージャデバイス100がユーザによって装着されているかどうかを検出するために使用されてもよい。たとえば、ウェアラブルアイデンティティマネージャデバイスは、脈拍センサをさらに備えてもよい。ここで、脈拍センサが所定の時間(たとえば、30秒)の間、信号を検出していない場合、ウェアラブルアイデンティティマネージャデバイス100は、ユーザがもはやデバイスを装着していないと推論してもよい。脈拍が再び検出されるとすぐに、ウェアラブルアイデンティティマネージャデバイス100は、ウェアラブルアイデンティティマネージャデバイス100が装着されている可能性があると推論してもよく、それにより、ウェアラブルアイデンティティマネージャデバイス100はアイデンティティ取得モードに再び入る。アイデンティティ取得モードが開始された後、1分などのある時間部分の間に検出された通信がない場合、デバイスは、関連付け解除モードに戻ってもよく、またはアイデンティティ取得モードにおいてプロキシ(proxy)として使用されるデバイスを起動させるために信号を送ってもよい。

【００１５】
加速度計センサはまた、ウェアラブルアイデンティティマネージャデバイス100が装着されているかどうかを決定するために使用され得る。そのような実施態様内では、少なくともしきい値時間(たとえば、5分)の間、信号が加速度計によって検出されない場合、またはデバイスが装着されていることを示さない動きのみが検出された場合、ウェアラブルアイデンティティマネージャデバイス100は、関連付け解除されるようになり、これは、それが以前に表していたユーザをもはや表さないことを意味する。十分に強い加速度計信号が再び検出されたとき、ウェアラブルアイデンティティマネージャデバイス100は、いくらかの時間の間、またはアイデンティティが取得されるまで、それ自体をアイデンティティ取得モードに置くことになる。ジャイロなどの、他の機能的に関連するセンサはまた、加速度計と組み合わせて、またはその代替として使用され得る。

【００１６】
ウェアラブルアイデンティティマネージャデバイス100が装着されているかどうかを決定するために使用され得るさらに別のセンサは、圧力またはタッチセンサである。そのようなセンサは、ウェアラブルアイデンティティマネージャデバイス100を自分の身体にしっかりと装着するユーザに特に望ましい可能性がある(たとえば、ぴったりフィットするブレスレット、リングなど)。ある時間の間、圧力/タッチが検出されなかった場合、ウェアラブルアイデンティティマネージャデバイス100は、それが以前に表していたアイデンティティからそれ自体の関連付けを解除する。圧力/タッチが再び検出されたとき、ウェアラブルアイデンティティマネージャデバイス100は、アイデンティティ取得モードに戻る。

【００１７】
伸縮センサの実施態様も企図される。たとえば、ウェアラブルアイデンティティマネージャデバイス100が伸縮性ブレスレットとして構成されている場合、ウェアラブルアイデンティティマネージャデバイス100は、ユーザからの除去時に引き伸ばされることが企図される。したがって、ウェアラブルアイデンティティマネージャデバイス100は、ウェアラブルアイデンティティマネージャデバイス100がしきい値伸縮メトリックを越えて引き伸ばされたかどうかを検出するように構成された伸縮センサを備えてもよい。そのような実施態様内では、ウェアラブルアイデンティティマネージャデバイス100は、次いで、伸縮センサから受信したデータに基づいて、関連付け/関連付け解除プロセスをトリガするように構成されてもよい。

【００１８】
センサはまた、関連付け/関連付け解除に対するユーザの希望を示す明示的なユーザアクションを検出するために含められてもよい。ここで、関連付け解除するための明示的なアクションは、不注意な関連付け解除から保護するために、関連付けるための明示的なアクションよりも意図的であってもよい。たとえば、関連付け解除を引き起こす、ウェアラ

ブルアイデンティティマネージャデバイス100を装着している間にユーザが典型的には関わることができない種類の迅速な回転を検出するために、ジャイロセンサが含められてもよい。同じまたは別の運動は、関連付ける必要性を識別するために使用され得る。

【００１９】

ウェアラブルアイデンティティマネージャデバイス100はまた、状態を変更する希望を合図するように構成されたボタンを含んでもよい。たとえば、そのようなボタンを10秒間押下することによって、ウェアラブルアイデンティティマネージャデバイス100は、関連付け解除するように構成されてもよく、同じボタンを3回連続して押下することは、ウェアラブルアイデンティティマネージャデバイス100にアイデンティティを取得することを試みさせてもよい。

【００２０】

また、明示的なユーザアクションは、暗黙のユーザアクションと組み合わされ得ることが企図される。たとえば、(たとえば、加速度計データを介して)ウェアラブルアイデンティティマネージャデバイス100が少なくとも1分の間静止しているとみなされながら、ボタンが10秒間押下された場合、関連付け解除は、実行されてもよい。アイデンティティの取得は、次いで、脈拍センサが心拍を検出しながら、ウェアラブルアイデンティティマネージャデバイス100が回されるか速く振り回された場合、開始されてもよい。

【００２１】

この特定の例について、ウェアラブルアイデンティティマネージャデバイス100は、ブレスレットとして構成されているが、様々な装着可能な構成のいずれかが企図されることが理解されるべきである。たとえば、ネックレス状の構成も企図され、そのような構成は、2つの部分、ストリング構成要素およびロック構成要素を有する。ここで、ユーザは、ユーザがネックレスを付け、ロックを閉じたとき、アイデンティティが選択され、他のエンティティとの連続した認証セッションのために利用可能にされる関連付けモードに入ることができることを知る。同様に、ユーザは、ユーザがロックを開いたとき、最初に別の認証セッションを経ることなしに、認証のためにネックレスを使用することがもはやできないことを知る。

【００２２】

さらなる例では、ウェアラブルアイデンティティマネージャデバイス100は、ベルトとして構成される。ユーザがバックルを閉じた場合、ウェアラブルアイデンティティマネージャデバイス100は、アイデンティティ取得モードに設定される。さらに、ベルトに関連付けられた加速度計が1分間動きを検出しなかった場合、ウェアラブルアイデンティティマネージャデバイス100は、アイデンティティ関連付け解除モードに入る。本開示の特定の態様では、ウェアラブルアイデンティティマネージャデバイス100は、スレーブデバイスと組み合わせてマスタデバイスとして動作するように企図される。たとえば、ウェアラブルアイデンティティマネージャデバイス100は、ベルトが装着されているかどうかを決定するように構成され、さらに、ベルトが装着され続ける限り、アイデンティティを維持するように構成されたベルトデバイスであってもよい。スレーブデバイス(たとえば、リング、スマートウォッチ、ブレスレット、など)は、次いで、意図を決定するために利用されてもよく、スレーブデバイスは、様々な通信プロトコル(たとえば、Bluetooth（登録商標） LE)のいずれかを介してマスタデバイスと通信してもよい。ここで、そのような意図は、マスタデバイスが装着されながら、スレーブデバイス上で明示的なアクションを実行するようにユーザに要求することによって有効にされてもよく、したがって、ユーザに関連付けられてもよい。たとえば、意図は、マスタデバイスが装着されている間に、スレーブデバイス上のボタンを押下することによって有効にされてもよい。ボタン有効化が実際に実行されたことの指示をスレーブデバイスから受信すると、マスタデバイスは、次いで、様々な要因のいずれかに基づいて取引をさらに認証してもよい。たとえば、スレーブデバイスから受信され、ボタン有効化と関連付けられるメタデータ(たとえば、ボタンが押下されたときの、スレーブデバイスの位置データ、スレーブデバイスの動きデータ、など)は、ユーザを認証するために、マスタデバイスデータ(たとえば、マスタデバイスの位

置データ、マスタデバイスの動きデータ、など)と同期化、または他の方法で比較され得る。

【００２３】

一般に、したがって、ウェアラブルアイデンティティマネージャデバイス100は、電子回路を含む、ブレスレット、スマートウォッチ、リング、タトゥー、ベルト、衣類、などの、様々な独立型の装着可能なアイテムのいずれかとして構成され得ることが理解されるべきである。ウェアラブルアイデンティティマネージャデバイス100はまた、たとえば、ボタンサイズの電池として構成され得、従来の電池の代わりに使用され得る。ウェアラブルアイデンティティマネージャデバイス100はまた、印刷可能なステッカーとして構成され得、腕時計の裏、ネックレスのチャーム、などの、様々な装着可能なアイテムのいずれかの上に配置され得る。ステッカーまたはパッチに関して、アイデンティティ取得は、裏材が除去されたときに開始してもよく、関連付け解除は、ステッカーまたはパッチがちぎれて回路が破損したら開始してもよい。

【００２４】

本開示の一態様では、潜在的な泥棒に対する様々な保護は、容易に実現され得る。たとえば、開示された技術が広く知られるようになると、泥棒志望者は、彼らが電話または他の携帯デバイスを含む人のバッグを盗み、この人が認証のためのウェアラブルアイデンティティマネージャデバイスを使用している場合、デバイスがロックされることを知ることになる。これは、取り外されたウェアラブルアイデンティティマネージャデバイスを借りる、または盗むことができる人によるウェアラブルアイデンティティマネージャデバイスの望ましくない使用から保護する。

【００２５】

別の例示的なシナリオでは、ネックレスが引きちぎられると回路が破壊されることになるので、被害者の首からネックレス状のウェアラブルアイデンティティマネージャデバイスを引きちぎることは、ウェアラブルアイデンティティマネージャをユーザおよびユーザのアカウントから自動的に関連付け解除することになることを泥棒志望者が知ることが望ましい。これは、ネックレスを取り外すのと同じ効果を持つことになる。先に述べたように、これは、ロックを含むネックレス全体に導電性ワイヤを埋め込むことによって達成されてもよい。代替的には、しかしながら、プロセッサからロックに、次いで背面に、次いでロックの他の部分に、そして背面に延びる第2の回路がネックレス内に埋め込まれる。この第2の回路が破壊された場合、それは、ネックレスが取り外されたことを示すのではなく、引きちぎられたことを示し、それは、警報信号を開始するために使用され得る。警報信号は、警備会社または警察に送信されてもよく、ウェアラブルアイデンティティマネージャデバイスに関連付けられた任意のモバイルデバイスにロックダウン指令を通信するために使用されてもよく、それによってリソースを暗号化し、サービスプロバイダに警告する。リソースは、次いで、以下でより詳細に説明するように、暗号鍵のバックアップが取得された後、より後でのみアクセス可能であってもよい。

【００２６】

さらに別の態様では、誘拐のシナリオが企図される。そのようなシナリオ内では、十分に動機づけられた人が、ウェアラブルアイデンティティマネージャデバイスをユーザから関連付け解除することなく、ウェアラブルアイデンティティマネージャデバイスを物理的に除去することができるようにウェアラブルアイデンティティマネージャデバイスを構成することが望ましいであろう。実際、そのような構成は、除去する際にウェアラブルアイデンティティマネージャデバイスを関連付け解除することを回避するために誘拐犯が被害者を傷つけることを考える可能性があるシナリオのために特に望ましい可能性がある。図1に戻って参照すると、この問題に対する可能な解決策は、本明細書に開示されている。すなわち、デュアル回路設計が企図され、導線120間の一次接続は、ロッキング機構130をアンロックすることによって切断可能であり、導線120間の二次接続は、ロッキング機構140をアンロックすることによって切断可能である。ここで、ロッキング機構140を開くことによって、ユーザは、導線120間の一次接続を切断することなく、ウェアラブルアイデ

ンティティマネージャデバイス100を除去することができ、これは、ウェアラブルアイデンティティマネージャデバイス100とユーザとの間の関連付けを維持する(それによって、残忍な攻撃に対するセキュリティを提供する)。本開示の一態様では、ロッキング機構140は、ロッキング機構130よりも開くことが著しくより困難である。代替的には、ロッキング機構140は、アンロックを可能にするがその後のロックを可能にしないように設計され得る。さらに、ロッキング機構140の個々の構成要素は、それらが1つの同じ物理的なロック内で常時接触するように、互いに隣に取り付けられてもよい。このように、回路全体は、従来式に見えるネックレス、ブレスレット、または腕時計バンド内に含まれ得、2つの別々のストランド、または2つの異なるロックを回避する。

【００２７】

例示的なウェアラブルアイデンティティマネージャシステム

ここで図3に向かうと、ウェアラブルアイデンティティマネージャデバイスを介してユーザを認証することを容易にする例示的な環境が、本開示の一態様に従って提供されている。図示のように、環境300は、ネットワーク310(たとえば、インターネット、ピアツーピアネットワーク、など)を介してペアリングデバイス330および外部デバイス340に結合され得るウェアラブルアイデンティティマネージャデバイス320を含む。ここで、ウェアラブルアイデンティティマネージャデバイス320は、無線対応デバイスとして構成されてもよく、ウェアラブルアイデンティティマネージャデバイス320は、本明細書で開示されたウェアラブルアイデンティティマネージャデバイスのいずれかと全体的に類似していることが企図される。この特定の例について、ウェアラブルアイデンティティマネージャデバイス320がユーザによって適切に関連付けられ、ユーザに取り付けられていると仮定すると、ウェアラブルアイデンティティマネージャデバイス320は、外部デバイス340に認証データをワイヤレス送信することによって、様々なタイプのエンティティ(たとえば、販売時点デバイス、料金所、金融機関のウェブサイト、など)のいずれかに対応する外部デバイス340に対してユーザを認証することを容易にすることができる。代替的には、外部デバイス340に直接認証データを送信するのではなく、ウェアラブルアイデンティティマネージャデバイス320は、ペアリングデバイス330(たとえば、スマートフォン、パーソナルコンピュータ、など)を介してそのような認証データを送信するように構成されてもよく、そのようなデータは、以下でより詳細に説明するように、ウェアラブルアイデンティティマネージャデバイス320および/またはペアリングデバイス330内に存在してもよい。

【００２８】

例示的なウェアラブルアイデンティティ認証プロセス

次に図4を参照すると、本開示の一態様による、ウェアラブルアイデンティティマネージャデバイスを利用することを容易にする例示的な方法を示すフローチャートが提供されている。図示のように、プロセス400は、本明細書の一態様による、様々なタイプのコンピューティングデバイス(たとえば、ウェアラブルアイデンティティマネージャデバイス320、ペアリングデバイス330、および/または外部エンティティ340)のいずれかの中で実行され得る一連の行為を含む。たとえば、プロセス400は、プロセッサを採用して、コンピュータ可読記憶媒体上に記憶されたコンピュータ実行可能命令を実行して、一連の行為を実施することによって実施され得る。別の態様では、プロセス400の行為を少なくとも1つのコンピュータに実施させるコードを備えるコンピュータ可読媒体が企図される。

【００２９】

図示のように、プロセス400は、ウェアラブルアイデンティティマネージャデバイスにユーザのアイデンティティを確認するために、ユーザがウェアラブルアイデンティティ管理デバイスと関連付けられる行為410で開始する。そのような関連付けプロセスは、ウェアラブルアイデンティティ管理デバイスがユーザの手首の周りに配置されたとき、ユーザの首の周りに配置されたとき、または他の方法でユーザに装着もしくは物理的に関連付けられたとき、開始されてもよい。さらに、ウェアラブルアイデンティティマネージャデバイスは、たとえば、閉じられている留め金、ロック、またはバックルによって、ユーザによって潜在的に装着されている状況を検出する。逆に、関連付け解除プロセスは、(たと

えば、留め金、ロック、またはバックスを開くことによって、ユーザの手首または首からウェアラブルアイデンティティマネージャデバイスを除去して)ウェアラブルアイデンティティマネージャデバイスが取り外されたとき、開始する。

【００３０】

先に述べたように、ウェアラブルアイデンティティマネージャデバイスは、閉じられたときに一定の電気接点を提供する(すなわち、ウェアラブルアイデンティティマネージャデバイスがロック構成にある間、導線の内部回路が閉じられる)ロッキング機構を備えてもよい。さらに、ロックが開かれるとすぐ、回路は、切断される。これは、ウェアラブルアイデンティティマネージャデバイスが潜在的にユーザによって着用させるようになっているとき、すなわち、留め金が閉じられたときと、ユーザから除去されているとき、すなわち留め金が開かれているときとを検出するために使用される。一時的にロックを開き、次いでそれを閉じている間、ウェアラブルアイデンティティマネージャを装着し続けることができるのと同様に、ウェアラブルアイデンティティマネージャを装着することなく、留め金を閉じることができるが、ロックは、それにもかかわらず、ウェアラブルアイデンティティマネージャデバイスが潜在的に装着されている状態と装着されていない見込みがある状態との間で状態を変更しているときを決定することを容易にすることができる。閉じられたときの接触を改善するために磁気構成要素を有するロック、または、代替的には、ねじ込むことによって開閉されるねじ付きロックを使用することも可能であり、ねじ部は、電気を伝導する材料で作られる。

【００３１】

代替の実施態様では、留め金は、磁石と、留め金が開かれたときに生じる磁界の変化を検出する回路とを備える。当業者は、ロックまたは留め金が開かれているもしくは開かれるようになっている、および/または閉じられているもしくは閉じられているようになっていることを検出する、さらに他の変形が予測されることを理解するであろう。他の代替的な手法は、ウェアラブルアイデンティティマネージャデバイスがユーザと物理的に関連付けられているおよび/または関連付け解除されているときを決定するように構成されたセンサを備える。可能な実施態様は、圧力センサと、温度センサと、心拍センサと、人へのありそうな近接を決定するために使用され得る同様のタイプのセンサとを使用することを含む。

【００３２】

ウェアラブルアイデンティティマネージャデバイスをユーザの手首に取り付ける際に、ユーザは、様々な方法のいずれかにおける関連付け処理を完了してもよい。たとえば、ユーザは、ウェアラブルアイデンティティマネージャデバイス上のユーザインターフェースを介してパスワードを入力することを要求されてもよい。しかしながら、ウェアラブルアイデンティティマネージャデバイスがユーザインターフェースを持たない場合、関連付けは、行為420において、ユーザインターフェースを有するペアリングデバイスにウェアラブルアイデンティティマネージャデバイスをペアリングすることによって完了されてもよい。そのようなペアリングプロセスは、ウェアラブルアイデンティティマネージャデバイスを、たとえば、モバイルデバイス、パーソナルコンピュータ、スクリーン付き眼鏡、または、スクリーン、キーボード、ポインタ、ボタン、マイクロホン、スピーカ、販売時点デバイス、もしくはドアロックを制御するコンピュータ、もしくはそのようなユーザI/O構成要素などのユーザ入力/出力(I/O)機構を有する他のデバイスを含む、様々なタイプのデバイスのいずれかと関連付けてもよい。簡単にするために、そのようなデバイスは、しばしば、「ペアリングデバイス」および/または「関連付けデバイス」と呼ばれる。

【００３３】

プロセス400は、ユーザが取引のために認証される行為430で終了する。本開示の特定の態様では、そのような認証プロセスは、ユーザアクションによって容易にされることが企図される。たとえば、認証プロセスが開始されたとき、ウェアラブルアイデンティティマネージャデバイスは、内蔵の無線送信機を使用して、関連付けられたペアリングデバイスと通信してもよい。ウェアラブルアイデンティティマネージャデバイスが複数のデバイス

とペアリングされている場合、たとえば、近接度、または意図のユーザ指示に基づいて、1つが選択される。たとえば、図5に示すように、そのような意図は、ウェアラブルアイデンティティマネージャデバイス500とペアリングデバイス510の両方を同期して移動することを含んでもよい。他の企図される指示は、ウェアラブルアイデンティティマネージャデバイス500およびペアリングデバイス510を一緒に叩くこと、それらを非常に近くに置くこと、などを含んでもよい。ペアリングデバイスが選択されると、ペアリングの確認は、触覚フィードバック、画像の表示、または音の放出などの、ペアリングデバイスによって放射される信号を介してユーザに伝達されてもよい。

【００３４】

本開示の別の態様では、パスワードマネージャの関わり合いが企図され、そのような関わり合いは、上記で説明したように、ウェアラブルアイデンティティマネージャデバイスがペアリングデバイスを選択した後、実行されてもよい。一実施態様では、ペアリングデバイスは、パスワードマネージャを備え、ペアリングデバイスの選択は、ウェアラブルアイデンティティマネージャデバイスからペアリングデバイスに送られるべきアンロック信号を発生し、その後、パスワードマネージャは、認証のコンテキストを決定し、ユーザアイデンティティ、および、該当する場合、コンテキストに関連付けられた信用証明書の探索を実行する。たとえば、コンテキストは、関連するドメインを含む、金融サービスプロバイダへのログイン画面を含んでもよい。パスワードマネージャは、少なくとも1つのユーザプロファイルを含み、ユーザプロファイルは、1人のユーザまたは1人の人物(自宅のユーザ、職場のユーザ、など)に関連付けられる。ウェアラブルアイデンティティマネージャデバイスに関連付けられたアイデンティティに基づいて、1つまたは複数のユーザプロファイルが選択され、地理的位置、ユーザ入力、ネットワーク識別子、などのコンテキスト情報に基づいて、1つまたは複数の選択されたユーザプロファイル間のさらなる選択が実行される。パスワードマネージャは、次いで、ログイン画面のドメインなどのコンテキストに基づいて、どのようなアカウントが選択されるべきなのかを決定する。代替的には、ユーザは、ペアリングデバイスに関連付けられたユーザインターフェースを使用してこれを選択する。

【００３５】

アカウントが選択されたとき、関連するユーザ名および信用証明書は、ログインおよび他の認証取引を実行するために使用される。信用証明書の一例は、パスワードであり、別の例は、個人識別番号(PIN)であり、別の例は、暗号鍵であり、さらに別の例は、チャレンジ質問および関連する回答の集合である。例示的な実施態様では、ログインセッションが完了した後、セッションは、デスクトップコンピュータ、ドアロック、または販売時点デバイスなどの、別の計算エンティティに転送され、そこで、ユーザは、セッションを完了し、ログアウトを開始する。別の実施態様では、セッションは、転送されることなく、ペアリングデバイス上で完了される。

【００３６】

代替的には、ウェアラブルアイデンティティマネージャデバイスは、パスワードマネージャを備え、上記で説明したようにログインを実行する。その後、セッションは、オプションで、別の計算デバイスに転送され、または、いくつかの事例では、信用証明書またはアンロック信号は、ウェアラブルアイデンティティマネージャデバイスからペアリングデバイスに通信される。

【００３７】

さらに別の態様では、ウェアラブルアイデンティティマネージャデバイスは、ペアリングデバイスの代わりに、ドアロックまたは販売時点レジスタなどの、登録された局と通信する。そのような実施態様内では、登録された局は、ウェアラブルアイデンティティマネージャデバイスとペアリングされている計算デバイスと関連付けられる。アンロック信号は、反射攻撃を阻止するために、擬似ランダムシーケンス発生器、またはそのような関数の近似などの、信号の発生器によって発生されたビットのシーケンスを含んでもよい。同じシーケンス、またはその選択された部分は、ウェアラブルアイデンティティマネージャ

デバイス、および登録された局に関連付けられた検証機によって生成されてもよい。認証トークンおよび検証機を同期させる方法は、当該技術分野において周知であり、これらの技術は、ウェアラブルアイデンティティマネージャデバイス、および登録された局に関連付けられた検証機を同期させるために使用され得る。

【００３８】

異なるタイプの承認を合図するための異なるユーザの関与の使用も企図される。たとえば、第1のタイプのユーザ関与は、まったくの無関与である。これの第1の例は、ユーザが企業の建物の中に許可される前に、ユーザのアイデンティティが決定される企業のシナリオである。第2の例は、ユーザがユーザの車を有料道路上で運転するときの通行料のためである。そこで、料金所は、ユーザが近づいたとき、ユーザの電話との連絡を確立しており、ユーザの電話は、ユーザのアイデンティティを確認するために、ユーザのウェアラブルアイデンティティマネージャデバイスと対話する。同じプロセスは、次いで、ユーザがアクセスするために請求されるべき道路の正確な長さを決定するために、ユーザが有料道路を出るときに実行されてもよい。ユーザがウェアラブルアイデンティティマネージャデバイス、電話、その他を持っていない場合、プロトコルは、正常に完了しない。そのとき、料金は、適切なユーザに請求するために、たとえば、ナンバープレートを撮影した写真を使用することによって、代替的な方法で請求されてもよい。

【００３９】

第2のタイプのユーザ関与は、ログインを合図するものである。たとえば、図5に示すように、ペアリングされたデバイスおよびウェアラブルアイデンティティマネージャデバイスを同期して監視することが使用されてもよい。ここで、ユーザは、十分に強い動きがペアリングデバイスとウェアラブルアイデンティティマネージャデバイスの両方について登録され、これらの2つの動きが互いに強く相関することが決定されるまで、動きを行い続ける必要があってもよい。ログインに関連付けられた例示的な動きは、水平方向のスワイプであり、いくつかの電話が現在アンロックされている方法を模倣する。

【００４０】

第3のタイプのユーザ関与は、購入の承認を合図するものである。一例は、手で予め定義された上方、下方、上方に振り、続いて、ペアリングデバイス上の承認ボタンを押下することである。ユーザに異なる種類のアクションの曖昧さをなくすのを助けるため、有用な場合、確認を作成するのを助けるため、および、明示的な確認を記録することよりも重要である場合、ユーザ体験を簡略化するのを助けるための、異なるユーザ関与タイプの使用を含む、追加のタイプのユーザ関与が追加されてもよい。支払に関連付けられた別の例示的な動きは、クレジットカードのスワイプを模倣する、垂直方向のスワイプである。

【００４１】

本開示のさらなる態様では、ウェアラブルアイデンティティマネージャデバイスは、リソースを復号するために使用される鍵を提供してもよい。たとえば、ユーザは、デバイスが静止している、または、異常な加速を経験しているデバイスなどの、突然なイベントが行われたとき、自動的に暗号化されたユーザのデバイスのメモリ階層全体を有するように選択してもよい。別のユーザは、デバイスがオフにされたとき、または、それがしきい値時間を超える期間中に使用されていないときにのみ、自動的に暗号化された、メールホルダおよびアドレス帳などの、選択された部分のみを有するように選択してもよい。暗号化されているメモリ領域にアクセスする唯一の方法は、ウェアラブルアイデンティティマネージャデバイスによって保持され、制御された状況下でのみ解除される鍵を用いてそれらを復号することであってもよい。たとえば、アンロックされるべきデバイスが存在するもとで、ユーザがデバイスをアンロックすることに特定の振る動作を実行する場合にのみ、鍵が開放されるのみである規則が実施されてもよい。これは、盗難および不要な使用に対してペアリングデバイスを保護する。

【００４２】

また、ウェアラブルアイデンティティマネージャデバイスは、それが使用される1回目に、長期アクセス信用証明書と関連付けられてもよく、そのような信用証明書は、ウェア

ラブルアイデンティティマネージャ内に記憶されてもよいことが理解されるべきである。ウェアラブルアイデンティティマネージャデバイスがペアリングデバイスと関連付けられたとき、ペアリングデバイスのユーザは、長期アクセス信用証明書を入力し、それは、(たとえば、典型的には、Bluetooth（登録商標）、近接場、またはWiFiの動作のセキュアモードによって与えられるもののようなセキュア接続を介して)ウェアラブルアイデンティティマネージャデバイスに送信される。送信された信用証明書は、記憶された信用証明書と比較され、それらが一致するかどうかが決定される。一致がある場合、ウェアラブルアイデンティティマネージャデバイスは、それ自体をペアリングデバイスに関連付ける要求を受け付ける。ウェアラブルアイデンティティマネージャデバイスは、オプションで、異なるユーザに関連付けられた複数の独立した長期アクセス信用証明書を記憶し、対応する個人または信用証明書の記憶されたセットは、これらの長期信用証明書のうちの1つを使用して正確な認証によってアクセス可能にされる。パスワード、PIN、または同様の信用証明書は、長期信用証明書として使用され得る。代替的には、生体測定テンプレートは、生体認証をサポートするために記憶され得る。正常な関連付けの後、しかし、対応する関連付け解除の前、ユーザは、別のプロファイルおよび関連する長期信用証明書を追加するため、または長期信用証明書を変更もしくは消去するため、ペアリングデバイスからウェアラブルアイデンティティマネージャデバイスにコマンドを送ることができる。

【００４３】

本開示のさらに別の態様では、ウェアラブルアイデンティティマネージャデバイスに関連付けられたハードウェアは、指紋センサ、ユーザの声を識別するために使用されるマイクロホン、または他のそのようなセンサなどの、生体測定センサを備える。典型的な商業展開では、動作の速度とエラー率の低下との間のトレードオフは、一般的に、比較的低いセキュリティまたは高いセンサコストとをもたらすが、説明する開示は、頻繁なユーザ認証を必要とせず、ウェアラブルアイデンティティマネージャデバイスがユーザに関連付けられているときの関連付け段階でのみ必要とする。したがって、生体測定センサの示度と記憶されたテンプレートとの間の適合の非常に高い要求を出すことができる。結果として、優れた使い勝手を依然として達成しながら、エラー率もしくは生体測定センサのコスト、またはその両方を低減することができ、ユーザがウェアラブルアイデンティティマネージャデバイスを装着し始めるときにのみ、ユーザは、認証する必要がある。通常の生体認証は、ユーザが操作するのに1秒の何分の一よりも長くかかる場合、望ましくない可能性があるが、典型的なユーザは、この文脈におけるはるかにより多く関わる認証を許容する可能性がある。これは、関連付けがあまり頻繁ではないためと、それが典型的には、取引を完了するなどの目標を達成するためにユーザが急がされているときに実行されないための両方のためである。同じ理由で、説明した生体認証方法の代わりに複雑な知識ベースまたは記憶力ベースの認証方法を使用することも許容される可能性があり、これは、したがって、強化されたセキュリティ、または、典型的なパスワードがするよりも高い再現率を有する認証方法の選択を可能にする。

【００４４】

別の企図される実施態様では、ウェアラブルアイデンティティマネージャデバイスは、ユーザアイデンティティの代わりにアカウントもしくは偽名に関連付けられ、または、本明細書の他の実施態様について説明したように、ユーザアクションによって支払われるもしくは引き渡される資金の表現を伝える。

【００４５】

例示的なハードウェア実施態様

次に図6を参照すると、処理システム614を用いるウェアラブルアイデンティティマネージャデバイス600のための例示的なハードウェア実施態様を示す概念図が提供されており、ウェアラブルアイデンティティマネージャデバイス600は、たとえば、図1～図5を参照して説明したウェアラブルアイデンティティマネージャデバイスのいずれかを含む任意の無線対応デバイス内に実装されてもよい。本開示の様々な実施態様によれば、要素、もしくは要素の任意の部分、または要素の任意の組合せは、1つまたは複数のプロセッサ604を

含む処理システム614を用いて実装されてもよい。プロセッサ604の例は、マイクロプロセッサ、マイクロコントローラ、デジタル信号プロセッサ(DSP)、フィールドプログラマブルゲートアレイ(FPGA)、プログラマブル論理デバイス(PLD)、状態機械、ゲートロジック(gated logic)、ディスクリートハードウェア回路、および本開示全体にわたって記述される種々の機能性を実行するように構成された他の適切なハードウェアを含む。すなわち、ウェアラブルアイデンティティマネージャデバイス600内で利用されるプロセッサ604は、以下で説明し、図6に示すプロセッサの任意の1つまたは複数を実装するために使用されてもよい。

【００４６】

この例では、処理システム614は、バス602によって全体的に表されるバスアーキテクチャで実装されてもよい。バス602は、処理システム614の特定の用途および全体的な設計制約に応じて、サービス指向アーキテクチャ(SOA(service oriented architecture))バスを含む任意の数の相互接続バスおよびブリッジを含んでもよい。バス602は、(プロセッサ604によって全般に表される)1つまたは複数のプロセッサ、メモリ605、および(コンピュータ可読媒体606によって全般に表される)コンピュータ可読媒体を含む、様々な回路を互いにリンクする。バス602はまた、タイミングソース、周辺機器、電圧調整器、および電力管理回路などの、様々な他の回路とリンクしてもよく、これらは、当該技術分野で周知であり、したがってこれ以上説明しない。バスインターフェース608は、バス602とトランシーバ610との間のインターフェースを実現する。トランシーバ610は、伝送媒体を介して様々な他の装置と通信するための手段を実現する。装置の性質に応じて、ユーザインターフェース612(たとえば、キーパッド、ディスプレイ、スピーカ、マイクロホン、ジョイスティック)も設けられてもよい。

【００４７】

本開示の一態様では、コンピュータ可読媒体606は、図示のように、ウェアラブルアイデンティティマネージャデバイスを介してユーザを認証することを容易にするために、様々な命令606aおよび/または606bを含むように構成される。同様の態様では、そのような認証は、代わりに、図示のように、回路620および/または630のいずれかにプロセッサ604を結合することによって、ハードウェアを介して実施され得る。さらに、認証は、命令606aおよび/または606bの任意の組合せ、ならびに回路620および/または630の任意の組合せによって実行されてもよいことが企図される。本開示の特定の態様では、命令606aおよび回路620は、ウェアラブルアイデンティティマネージャデバイス600がユーザによって装着されているかどうかに基づいて、ユーザとウェアラブルアイデンティティマネージャデバイス600との間の関連付け状態を決定するように構成された検出器構成要素に向けられ、命令606bおよび回路630は、ユーザ認証を決定することを容易にするように構成された決定構成要素に向けられる。

【００４８】

この目的のため、ウェアラブルアイデンティティマネージャデバイス600は、様々な方法のいずれかでユーザ認証を容易にするように構成されてもよいことが理解されるべきである。第1の態様では、そのような認証は、ユーザのアイデンティティを検証するために、ウェアラブルアイデンティティマネージャデバイス600によって追跡される動きデータ(たとえば、自動販売機の取引を検証するために、ユーザの手を振る)を利用することを含む。この特定の実施態様について、命令606bおよび/または回路630は、さらに、ウェアラブルアイデンティティマネージャデバイス600の運動に関連付けられた動きデータを監視するように構成されたセンサ構成要素を備えてもよい。トランシーバ構成要素610は、そのとき、他の認証データ(たとえば、支払情報)とともに、関連付け状態に基づいて、動きデータを(たとえば、自動販売機に)送信するように構成されてもよい。

【００４９】

第2の態様では、ユーザ認証は、ペアリングデバイス(たとえば、ペアリングデバイス330)を介して企図される。ここで、そのようなペアリングデバイスは、プロキシデバイスとして機能してもよく、ウェアラブルアイデンティティマネージャデバイス600によってペ

アリングデバイスに提供される認証データは、ペアリングデバイスを介して外部デバイス(たとえば、PoS端末)によって要求されるユーザ認証を容易にすることが企図される。この実施態様について、命令606bおよび/または回路630は、さらに、ウェアラブルアイデンティティマネージャデバイス600をペアリングデバイスとペアリングするように構成されたペアリング構成要素を備えてもよい。トランシーバ構成要素610は、そのとき、関連付け状態に基づいて、ペアリングデバイスに認証データ(たとえば、支払情報)を送信するように構成されてもよい。

【００５０】

図6の残りの要素に戻って参照すると、プロセッサ604は、バス602を管理すること、および、コンピュータ可読媒体606上に記憶されたソフトウェアの実行を含む全体的な処理を担当することが理解されるべきである。ソフトウェアは、プロセッサ604によって実行されると、処理システム614に任意の特定の装置の以下で説明する様々な機能を実行させる。コンピュータ可読媒体606は、ソフトウェアを実行するときにプロセッサ604によって操作されるデータを記憶するためにも使用され得る。

【００５１】

処理システム内の1つまたは複数のプロセッサ604は、ソフトウェアを実行してもよい。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語、または他のものと呼ばれようとそうでなかろうと、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアモジュール、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行ファイル、実行のスレッド、プロシージャ、機能などを意味すると幅広く解釈されるべきである。ソフトウェアは、コンピュータ可読媒体606上に存在してもよい。コンピュータ可読媒体606は、非一時的コンピュータ可読媒体であり得る。非一時的コンピュータ可読媒体は、例として、磁気記憶デバイス(たとえば、ハードディスク、フロッピー(登録商標)ディスク、磁気ストリップ)、光ディスク(たとえば、コンパクトディスク(CD)またはデジタル多用途ディスク(DVD))、スマートカード、フラッシュメモリデバイス(たとえば、カード、スティック、またはキードライブ(key drive))、ランダムアクセスメモリ(RAM)、読出し専用メモリ(ROM)、プログラマブルROM(PROM)、消去可能PROM(EPROM)、電気的消去可能なPROM(EEPROM)、レジスタ、リムーバブルディスク、ならびに、コンピュータによってアクセスされ、読み取られるソフトウェアおよび/または命令を格納するための任意の他の適切な媒体を含む。コンピュータ可読媒体はまた、例として、搬送波、伝送路、ならびに、コンピュータによってアクセスされ、読み取られるソフトウェアおよび/または命令を送信するための任意の他の適切な媒体を含んでもよい。コンピュータ可読媒体606は、処理システム614の中に、もしくは処理システム614の外に存在し得、または処理システム614を含む複数のエンティティにわたって分散され得る。コンピュータ可読媒体606は、コンピュータプログラム製品において具現化することができる。例として、コンピュータプログラム製品は、パッケージング材料内のコンピュータ可読媒体を含む場合がある。当業者は、本開示全体にわたって提示される説明した機能性を、特定の用途と全体のシステムに課せられた全体的な設計制約とに応じてどのように最適に実装するかを認識するであろう。

【００５２】

次に図7を参照すると、検出器回路620および検出器命令606aの各々は、複数のサブ構成要素のいずれかを介してウェアラブルアイデンティティマネージャ600とのユーザの関連付け状態を確認することを容易にすることが理解されるべきである。たとえば、検出器回路620は、関連付けサブ回路710と、関連付け解除サブ回路720とを備えてもよく、検出器命令606aは、関連付け命令712と関連付け解除命令722とを備えてもよい。ここで、関連付けサブ回路710および関連付け命令712は、最初は、関連付け手順を介してウェアラブルアイデンティティマネージャデバイス600にユーザを関連付けることに向けられる。そのような関連付け手順は、(たとえば、ユーザインターフェースを介して)直接ウェアラブルアイデンティティマネージャデバイス600を介して、または(たとえば、ペアリングデバイス

330を介して)関連付けデバイスを介して実行され得ることが企図される。本開示の特定の態様では、関連付けサブ回路710および/または関連付け命令712は、ウェアラブルアイデンティティマネージャデバイス600および/または関連付けデバイスを介して、ローカルに記憶されたパスワードをユーザによって入力されたパスワードと一致させるように構成されてもよい。本開示の別の態様では、関連付けサブ回路710および/または関連付け命令712は、ウェアラブルアイデンティティマネージャデバイス600の関連付け運動に対応するデータを、関連付けデバイスの運動に対応する関連付けデバイスから受信されたデータと一致させるように構成されてもよい。代替的には、ウェアラブルアイデンティティマネージャデバイス600の運動を関連付けデバイスの運動と比較するのではなく、ウェアラブルアイデンティティマネージャデバイス600の運動は、所定の関連付け運動(たとえば、ウェアラブルアイデンティティマネージャデバイス600を左右に振る)に対応する内部に記憶されたデータと比較され得る。

【００５３】

次に図8を参照すると、ウェアラブルアイデンティティマネージャデバイスにユーザを関連付けることを容易にする例示的なプロセス800を示すフローチャートが提供されている。本開示の一態様では、手順800は、関連付けサブ回路710および/または関連付け命令712を介してウェアラブルアイデンティティマネージャデバイス600によって実行されてもよいことが企図される。手順800は、ウェアラブルアイデンティティマネージャデバイス600が、関連付けデバイスが必要かどうかを決定する行為810で開始する。

【００５４】

関連付けデバイスを持たないユーザを関連付けるためのいくつかの実施態様が企図されることが理解されるべきである。たとえば、関連付けデバイスが必要とされない/望まれない場合、手順800は、関連付けデータのためにユーザ活動が監視される行為815に進む。この目的のため、そのような関連付けデータは、たとえば、(たとえば、キーボードを介して入力された)パスワード入力、(たとえば、マイクロホンを介して受信された)音声コマンド、および/または(たとえば、加速度計によって追跡された)運動を含む、ユーザアクションに関連付けられた様々なタイプのデータのいずれかを含んでもよいことが理解されるべきである。関連付けデータが行為825で受信されると、手順800は、関連付けデータが(たとえば、入力されたパスワードを内部に記憶されたパスワードと比較して)分析される行為840に進む。手順800は、次いで、分析に基づいて(たとえば、入力されたパスワードが内部に記憶されたパスワードと一致するかどうかに基づいて)関連付け状態が決定される行為850で終了する。

【００５５】

多くの場合、しかしながら、関連付けデバイスは、実際に必要とされる/望まれる。たとえば、ウェアラブルアイデンティティマネージャデバイス600は、パスワードを入力するためのユーザインターフェースを欠いている可能性があるので、ユーザインターフェースを有する関連付けデバイスを利用することが必要とされる可能性がある。ウェアラブルアイデンティティマネージャデバイス600がユーザインターフェースを含んでいる場合でも、そのようなインターフェースのフォームファクタは、パスワードを入力することを厄介にする可能性がある。

【００５６】

手順800に戻って参照すると、関連付けデバイスがこのように行為810で必要とされる/望まれる場合、ウェアラブルアイデンティティマネージャデバイス600は、次いで、関連付けデバイスとの接続が確立される行為820に進む。ここで、そのような接続は、(たとえば、Bluetooth（登録商標）接続を介する)ワイヤレス接続または(たとえば、ユニバーサルシリアルバス接続を介する)ワイヤード接続であってもよいことが理解されるべきである。接続されたら、ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為830において関連付けデバイスから関連付けデータを受信し始めてもよく、関連付けデータは、次いで、行為840で(たとえば、受信されたパスワードを内部に記憶されたパスワードと比較して)分析される。手順800は、次いで、関連付け状態が分析に基づいて(た

とえば、受信されたパスワードが内部に記憶されたパスワードと一致するかどうかに基づいて)決定される行為850で終了する。

【００５７】

また、より安全な関連付け手順を要求する認証(たとえば、しきい値量を超える購入、機密の電子メールアカウント、など)について、ウェアラブルアイデンティティマネージャデバイス600と関連付けデバイスの両方を介して確認されたデータを利用することが望ましいことがある。たとえば、図5を参照して説明したウェアラブルアイデンティティマネージャデバイス500と同様に、関連付け手順は、関連付けデバイスおよびウェアラブルアイデンティティマネージャデバイス600を同期して監視することを含んでもよく、行為830で受信された関連付けデータは、ウェアラブルアイデンティティマネージャデバイス600と関連付けデバイスの両方からの動きデータを含む。行為840では、関連付けデバイスおよびウェアラブルアイデンティティマネージャデバイス600の個々の運動は、次いで、この動きデータに基づいて比較される。運動が(たとえば、横断した時間および経路において)実質的に同様であるとみなされる場合、ユーザは、次いで、行為850でウェアラブルアイデンティティマネージャデバイス600に関連付けられる。

【００５８】

図7に戻って参照すると、図示のように、検出器回路620は、さらに、関連付け解除サブ回路720を備えてもよく、検出器命令606aは、さらに、関連付け解除命令722を含んでもよい。ここで、関連付け解除サブ回路720および関連付け解除命令722は、ウェアラブルアイデンティティマネージャデバイス600がもはやユーザによって装着されていないことを検出した際に、ウェアラブルアイデンティティマネージャデバイス600からユーザを関連付け解除することに向けられる。本開示の特定の態様では、ウェアラブルアイデンティティマネージャデバイス600は、1つまたは複数のセンサ構成要素に結合されてもよく、関連付け解除サブ回路720および/または関連付け解除命令722は、そのようなセンサから受信したデータに基づいて、ウェアラブルアイデンティティマネージャデバイス600が装着されているかどうかを推論するように構成されてもよい。この目的のため、たとえば、(たとえば、ウェアラブルアイデンティティマネージャデバイス100などのブレスレットがアンロックされるようになっているときを検出する)留め金センサ、(たとえば、リングと指との間の圧力を検出する)圧力センサ、(たとえば、体温を検出する)温度センサ、(たとえば、心拍を検出する)脈拍センサ、または(たとえば、伸縮性ブレスレットが伸ばされているときを検出する)伸縮センサを含む、任意の1つまたは複数の様々なタイプのセンサ構成要素が使用されてもよいことが理解されるべきである。

【００５９】

次に図9を参照すると、ウェアラブルアイデンティティマネージャデバイスからユーザを関連付け解除することを容易にする例示的なプロセス900を示すフローチャートが提供されている。本開示の一態様では、手順900は、関連付け解除サブ回路720および/または関連付け解除命令722を介してウェアラブルアイデンティティマネージャデバイス600によって実行されてもよいことが企図される。手順900は、それが関連付け状態にあることをウェアラブルアイデンティティマネージャデバイス600が検出する行為910で開始する。ウェアラブルアイデンティティマネージャデバイス600が関連付け状態に入ると、手順900は、ウェアラブルアイデンティティマネージャデバイス600に結合された関連付け解除センサが監視される行為920に進む。ここで、先に述べたように、そのような監視は、たとえば、留め金センサ、圧力センサ、温度センサ、脈拍センサ、または伸縮センサを含む、1つまたは複数の様々なタイプのセンサからデータを取得することを含んでもよい。この目的のため、ユーザによって装着されているウェアラブルアイデンティティマネージャデバイス600と一致するしきい値(たとえば、しきい値圧力値、しきい値温度値、など)が、特定の関連付け解除センサに割り当てられてもよく、ウェアラブルアイデンティティマネージャデバイス600が装着されているかどうかについての推論は、受信したセンサ値をそのようなしきい値と比較することに基づく。行為930では、ウェアラブルアイデンティティマネージャデバイス600は、次いで、関連付け解除センサのいずれかがトリガされたかど

うかを決定する。関連付け解除センサが実際にトリガされている場合、プロセス900は、ウェアラブルアイデンティティマネージャデバイス600がユーザから関連付け解除されることになる行為940で終了する。そうでなければ、関連付け解除センサがトリガされていない場合、プロセス900は、関連付け解除センサが監視され続ける行為920にループバックする。

【００６０】

次に図10を参照すると、決定回路630および決定命令606bの各々は、複数のサブ構成要素のいずれかを介してユーザ認証を決定することを容易にすることができることが理解されるべきできある。たとえば、決定回路630は、センササブ回路1010と、ペアリングサブ回路1020と、信用証明書マネージャサブ回路1030と、セキュリティサブ回路1040とを備えてもよく、決定命令606bは、センサ命令1012と、ペアリング命令1022と、信用証明書マネージャ命令1032と、セキュリティ命令1042とを含んでもよい。先に述べたように、ウェアラブルアイデンティティマネージャデバイス600によって横断された経路に対応する動きデータ(たとえば、自動販売機取引を検証するためにユーザの手を振る)は、ユーザを認証するために利用されてもよい。ここで、センササブ回路1010および/またはセンサ命令1012は、複数の動きセンサデバイス(たとえば、加速度計、ジャイロ、など)のいずれかを介してそのような動きデータを監視するように構成されてもよい。

【００６１】

さらなる態様では、ウェアラブルアイデンティティマネージャデバイス600はまた、ユーザを認証するために他のタイプのデータを利用するように構成されてもよいことが企図される。たとえば、ウェアラブルアイデンティティマネージャデバイス600によって経験される運動に対応する動きデータに加えて、センササブ回路1010および/またはセンサ命令1012は、ウェアラブルアイデンティティマネージャデバイス600に結合された1つまたは複数の他の構成要素からデータを取得するように構成されてもよい。そのような構成要素は、たとえば、ボタン(たとえば、認証は、ユーザの手を振りながらタッチスクリーンボタンを押下することを含んでもよい)、全地球測位システム(GPS)デバイス(たとえば、認証は、ユーザが振りながらユーザの位置を確認することを含んでもよい)、またはマイクロホン(たとえば、認証は、ユーザの手を振りながら、音声コマンドを言うことを含んでもよい)を含んでもよい。ウェアラブルアイデンティティマネージャデバイス600によって提供される認証データは、したがって、任意のこれらまたは他の構成要素からのセンサデータを含んでもよく、そのような認証データは、要求デバイス(たとえば、PoS端末、ペアリングデバイス、など)にユーザのアイデンティティを確認するのを容易にする。

【００６２】

次に図11を参照すると、センサデータがユーザ認証を容易にするために利用される例示的なプロセス1100を示すフローチャートが提供されている。本開示の一態様では、手順1100は、ウェアラブルアイデンティティマネージャデバイス600によって実行されてもよいことが企図される。手順1100は、ウェアラブルアイデンティティマネージャデバイス600が認証要求を受信する行為1110で開始する。ここで、そのような要求は、要求エンティティ(たとえば、PoS端末)から直接的に受信されてもよく、またはプロキシデバイス(たとえば、ペアリングデバイス)を介して要求エンティティから間接的に受信されてもよいことが企図される。認証要求を受信すると、手順1100は、ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられているかどうかを決定するために行為1120に進む。ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられていない場合、手順1100は、行為1125で、認証要求が拒絶されて終了する。代替的には、要求を拒絶するのではなく、ウェアラブルアイデンティティマネージャデバイス600は、関連付け状態にある間、単に認証要求を受信するように構成されてもよい。

【００６３】

しかしながら、ウェアラブルアイデンティティマネージャデバイス600が実際にユーザに関連付けられている場合、手順1100は、認証要求が構文解析される行為1130に進む。要求を構文解析することによって、ウェアラブルアイデンティティマネージャデバイス600

は、行為1140で、要求に関連付けられた様々な認証パラメータを確認することができる。行為1150では、ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為1140で識別された特定の認証パラメータに対応するセンサデータを取得する。たとえば、1つの認証要求は、上下運動に対応する動きデータを単に要求してもよく、別の認証要求は、上下運動に対応する動きデータに加えて音声コマンドを要求してもよい。ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為1160で要求エンティティに認証データを送信し、認証データは、動きデータを含む。

【００６４】

図10に戻って参照すると、図示のように、決定回路630は、さらに、ペアリングサブ回路1020を備えてもよく、決定命令606bは、さらに、ペアリング命令1022を含んでもよい。ここで、ペアリングサブ回路1020およびペアリング命令1022は、ウェアラブルアイデンティティマネージャデバイス600をペアリングデバイス(たとえば、ペアリングデバイス330)とペアリングすることに向けられる。さらに、ペアリングサブ回路1020および/またはペアリング命令1022は、ウェアラブルアイデンティティマネージャデバイス600が、ペアリングされたデバイスを介して開始されたユーザ取引を認証するために使用され得るように、そのようなペアリングを容易にするように構成されてもよいことが企図される。

【００６５】

次に、図12を参照すると、ペアリングデバイスがユーザ認証を容易にするために利用される例示的なプロセス1200を示すフローチャートが提供されている。本開示の一態様では、手順1200は、ウェアラブルアイデンティティマネージャデバイス600によって実行されてもよいことが企図される。手順1200は、ウェアラブルアイデンティティマネージャデバイス600がペアリングデバイスとペアリングされる行為1210で開始する。次に、行為1220では、ウェアラブルアイデンティティマネージャデバイス600は、ペアリングデバイスを介して要求エンティティから認証要求を受信する。たとえば、取引がオンライン購入である場合、要求エンティティは、オンライン販売業者であり、ペアリングされたデバイスは、ブラウザアプリケーションを実行しているデバイス(たとえば、ラップトップ、スマートフォン、など)である。認証要求を受信すると、手順1200は、ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられているかどうかを決定するために、行為1230に進む。ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられていない場合、手順1200は、行為1235で認証要求が拒絶されて終了する。

【００６６】

しかしながら、ウェアラブルアイデンティティマネージャデバイス600が実際にユーザに関連付けられている場合、手順1200は、要求に関連付けられた様々な認証パラメータが確認される行為1240に進む。行為1250では、ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為1240で識別された特定の認証パラメータに対応する認証データを取得する。ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為1260においてペアリングデバイスに認証データを送信し、そのような送信は、要求エンティティにユーザを認証するためにペアリングデバイスを介して手動で個人情報を入力する必要性を排除する。

【００６７】

再び図10を参照すると、図示のように、決定回路630は、さらに、信用証明書マネージャサブ回路1030およびセキュリティサブ回路1040を備えてもよく、決定命令606bは、さらに、信用証明書マネージャ命令1032およびセキュリティ命令1042を含んでもよい。ここで、信用証明書マネージャサブ回路1030および信用証明書マネージャ命令1032は、ユーザに関連付けられた信用証明書を提供することに向けられ、セキュリティサブ回路1040およびセキュリティ命令1042は、認証要求に関連付けられたセキュリティレベルを確認することに向けられる。さらに、ウェアラブルアイデンティティマネージャデバイス600は、認証要求から確認されたセキュリティレベルに基づいて要求エンティティに提供されるユーザ信用証明書の量を制限するために、信用証明書マネージャサブ回路1030、信用証明書マネージャ命令1032、セキュリティサブ回路1040、および/またはセキュリティ命令1042の任

意の組合せを利用するように構成されてもよいことが企図される。本開示の特定の態様では、信用証明書は、ユーザアクションまたは、認証要求から推定された実行コンテキストとのうちの少なくとも一方に基づいて提供され、セキュリティレベルは、ユーザの好みの設定、実行コンテキスト、または1つもしくは複数の過去の実行コンテキストのうちの少なくとも1つに従って確認される。さらに、以下でより詳細に説明するように、セキュリティレベルは、複数の可能なセキュリティレベルから選択されてもよい。

【００６８】

次に図13を参照すると、ユーザ認証を容易にするために、確認されたセキュリティレベルに従って信用証明書が送信される例示的なプロセス1300を示すフローチャートが提供されている。本開示の一態様では、手順1300は、ウェアラブルアイデンティティマネージャデバイス600によって実行されてもよいことが企図される。手順1300は、ウェアラブルアイデンティティマネージャデバイス600が認証要求を受信する行為1310で開始する。認証要求を受信すると、手順1300は、ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられているかどうかを決定するために行為1320に進む。ウェアラブルアイデンティティマネージャデバイス600がユーザに関連付けられていない場合、手順1300は、行為1325において認証要求が拒絶されて終了する。

【００６９】

しかしながら、ウェアラブルアイデンティティマネージャデバイス600が実際にユーザに関連付けられている場合、手順1300は、認証要求が構文解析される行為1330に進む。要求を構文解析することによって、ウェアラブルアイデンティティマネージャデバイス600は、行為1340で要求に関連付けられた適切なセキュリティレベルを選択することができる。先に述べたように、そのようなセキュリティレベルは、複数の可能なセキュリティレベルから選択されてもよく、選択は、様々な要因(たとえば、ユーザの好みの設定、実行コンテキスト、および/または1つもしくは複数の過去の実行コンテキスト、など)のいずれかにによって決まる。行為1350では、ウェアラブルアイデンティティマネージャデバイス600は、次いで、行為1340で選択されたセキュリティレベルに従って信用証明書を取得する。手順1300は、次いで、行為1360で、ウェアラブルアイデンティティマネージャデバイス600がセキュリティレベルに基づいて要求エンティティに信用証明書を送信して終了する。

【００７０】

セキュリティの例示的なレベル

開示されたウェアラブルアイデンティティインフラストラクチャは、様々なレベルのセキュリティのいずれをも容易にすることができることが理解されるべきである。特定の態様では、しかしながら、セキュリティの3つの例のレベル、近接度検証、暗黙の保証、および明示的な確認が企図される。これら3つのレベルのセキュリティおよび対応するペアリング方法の各々は、以下で説明され、ペアリング方法は、局とウェアラブルアイデンティティマネージャデバイスとの間のプロトコルのコンテキスト内で説明される。

【００７１】

この例では、近接度検証は、アクセス権を有するアイデンティティに関連付けられたアイデンティティマネージャが、ユーザが対話するオブジェクト(たとえば、電話、マウス、など)に近接していることを検証することに単純に依存しているので、セキュリティの3つのレベルのうちで最低であるとみなされる。ペアリングに関して、電話、マウス、ドアノブ、販売時点端末、などのどれであれ、局は、ウェアラブルアイデンティティマネージャデバイスにウェイクアップ信号を送信してもよく、ウェアラブルアイデンティティマネージャデバイスは、ウェアラブルアイデンティティマネージャデバイスに関連付けられたアイデンティティの表現を含む肯定応答で応答する。この表現は、静的な一意の識別子、仮名、ローリングコードからの出力、または暗号化トークンであってもよい。

【００７２】

次に図14を参照すると、ウェアラブルアイデンティティマネージャと局との間の例示的な近接度ベースの検証を示す概略図が提供されている。最も低いセキュリティレベルでは

、近接度検証は、取引を続行するのに十分であることが企図される。特定の実施態様では、局は、アイデンティティマネージャによって受信されるウェイクアップ信号を送信し、それにアイデンティティアサーション(assertion)で応答させる。ウェイクアップ信号は、アイデンティティマネージャによって保持されるホワイトリストと比較される局のアイデンティティの指標を含むことができる。一致がある場合、アイデンティティアサーションは、局に関連付けられた鍵と、局に送信された暗号文とを使用して暗号化される。ここで、局は、アイデンティティマネージャがその以前のアイデンティティから関連付け解除されているかどうかを知らないので、明白な確認応答から単にアイデンティティを推論することは、専用チャネルにもかかわらず、不可能であることに留意すべきである。

【００７３】

セキュリティの3つのレベルのうち、暗黙の保証は、中間レベルとみなされる。暗黙の保証は、近接度検証を通過したアイデンティティマネージャに関連付けられたユーザのもっともらしいユーザ意図を決定することに依存する。これは、加速度計データを、暗黙のユーザアクション(たとえば、ユーザがそうすることを要求されずに行っているアクション)に対応するデータと比較することによって得られ得る。そのようなアクションの例は、アプリケーションまたはリソースを選択するために画面をタップすることと、ラップトップのキーボードをタイプすることと、ドアノブを回すこととを含む。ペアリングに関して、暗黙の保証は、2つの信号(たとえば、2つの加速度計トレース、1つの加速度計トレースおよび関連するクリックタイミング信号、など)の比較を必要とする。そのような比較は、ある意味で、そのユーザを正確に表す責任があるアイデンティティマネージャによって実行されてもよく、結果は、上記で説明したように、アイデンティティマネージャに関連付けられたアイデンティティの表現とともに局に伝達されてもよい。

【００７４】

セキュリティの最も高いレベルは、アクションの明示的なユーザ確認から得られ、ユーザのアイデンティティマネージャはまた、近接度検証を通過している。明示的な確認の2つの例は、ユーザが(スマートブレスレットを装着するために使用される手で)電話を振ることと、販売時点端末の画面上で合図することであり、検出された画面の運動またはスタイラス加速度計データは、アイデンティティマネージャによって生成された加速度計データと比較される。明示的な確認と暗黙の保証との間の違いは、ペアリングの観点から、主に、上記で説明した2つの信号の比較から得られる一致に関連付けられた確実性にある。すなわち、明示的な確認のために、より多くの量の信号が比較される必要がある。信号の比較の1つの実用的な実施態様は、ありそうなエントロピーの量を決定する単純な形態のエントロピーメータと、持続的な背景運動について調整することと、比較を実行する前に十分な量の信号を収集することとを含む。代替的には、2つの信号は、十分な合意があるまで(ウィンドウ法を使用して)比較され、その時点で、確認が生成され、送信される。

【００７５】

特定の態様では、セキュリティレベルが、タスクのタイプまたはその持続時間を選択することによって、所望のレベルに調整され得ることが企図される。ここで、追加の要件が運動に対して置かれることを除いて暗黙の保証のプロトコルと実質的に同様のプロトコルが使用され得る。次に図15を参照すると、暗黙の保証および明示的な確認のための例示的な方式が提供されている。局は、ウェイクアップ信号を送ることによって開始する。アイデンティティマネージャがウェイクアップ信号を受信するとすぐに、ウェアラブルアイデンティティマネージャは、運動m_1を測定する。同時に、局は、運動m_2を測定する。ウェイクアップ信号の時間期間T内で、局は、測定された運動m_2およびその公開鍵Pへの関与(commitment)を送信する。関与は、m_2、P、および局がランダムに選択した数rの暗号化ハッシュ関数を適用することによって計算され得る。時間Tがウェイクアップ信号から経過した後、局は、値$(m_2;P;r)$を明らかにする。アイデンティティマネージャは、3つの事実、(1)関与がウェイクアップ信号の時間T内に受信されたこと、(2)関与が明らかにされた値に対応すること、および(3)運動m_1およびm_2が互いに十分に一致すること、を検証する。明示的な確認について、運動が追加の要件を満たすことも検証される。これらの条件のすべて

が満たされた場合、アイデンティティマネージャは、公開鍵Pを使用して暗号化されたアイデンティティアサーションを準備し、結果として生じた暗号文を局に送信する。

【００７６】

多くのPoS取引について、ユーザ署名を要求することは、所望の明示的な確認であってもよいことが留意される。すなわち、PoS取引のためのユーザ認証は、上述した、アイデンティティマネージャによって生成された加速度計データの、検出されたPoS画面運動またはスタイラス加速度計データとの一致を必要としてもよい。次に図16～図17を参照すると、ウェアラブルアイデンティティマネージャデバイスによって容易にされるPoS取引の例示的な署名認証が提供される。図16～図17に示すように、そのような認証は、ウェアラブルアイデンティティマネージャデバイス1600を装着しながら、スタイラス1612で販売時点タッチスクリーン1610上にユーザの署名を署名するようにユーザに要求してもよい。図16では、たとえば、ユーザの署名の最初のストロークが示されており、ウェアラブルアイデンティティマネージャデバイス1600によって生成された加速度計データは、販売時点タッチスクリーン1610によって取り込まれた最初のストローク、および/またはスタイラス1612の運動に対応する加速度計データと一致させられる。さらに、ウェアラブルアイデンティティマネージャデバイス1600によって横断された検出された経路が、販売時点画面1610および/またはスタイラス1612によって検出された署名ストロークに対応する信号と一致するかどうかについて、決定が行われる。

【００７７】

いくつかの実施態様では、そのような信号と、ウェアラブルアイデンティティマネージャデバイス1600によって横断された経路との同時検出が要求されてもよい。たとえば、図17に示すように、ユーザがユーザの名前を署名するときにウェアラブルアイデンティティマネージャデバイス1600によって横断される経路は、実質的に水平であってもよく、そのような経路は、ユーザがユーザの名前を署名し始めた時刻t_1から、ユーザがユーザの名前を署名するのを完了した時刻t_2まで追跡される。ここで、t_1からt_2までのウェアラブルアイデンティティマネージャデバイス1600の実質的に水平の経路は、t_1からt_2までの販売時点タッチスクリーン1610によって取り込まれた署名ストロークおよび/またはt_1からt_2までの署名と一致するスタイラス1612の運動に対応する加速度計データと一致させられてもよい。PoS支払の認証は、次いで、そのような一致が所定の信頼度の範囲内であるかどうかを確認することによって少なくとも部分的に基づいてもよい。

【００７８】

本明細書で開示される態様によるPoS取引の様々な例示的な認証をここで説明する。第1の例では、ユーザは、ユーザの利き手の手首にウェアラブルアイデンティティマネージャデバイスを装着し、ウェアラブルアイデンティティマネージャデバイスは、ユーザに以前に関連付けられており、したがってユーザのアイデンティティの表現をすでに記憶していると仮定する。この例について、PoS端末は、関連するスタイラスを有する画面と、画面上のスタイラスの時間ベースのトレースを記録するために使用されるソフトウェアとを備えるレガシー端末である。PoS端末はまた、ネットワークに接続され、ワイヤレス無線送信機を備える。ここで、ユーザは、スタイラスを手に取ることによって開始し、それを画面に近づける。この結果として、係合信号が、ワイヤレス無線送信機を使用して送信され、係合信号は、ウェアラブルアイデンティティマネージャデバイスによって受信される。ウェアラブルアイデンティティマネージャデバイスは、次いで、識別に関連付けられた動作のモードに入る。

【００７９】

次に、ユーザは、PoS端末画面上のボックス内にユーザの名前を署名するように促される。同時に、識別に関連付けられた動作のモードに入っているウェアラブルアイデンティティマネージャデバイスは、ウェアラブルアイデンティティマネージャデバイスの運動を(たとえば、加速度計データを介して)記録し、その運動は、時間-空間シリーズの形式で一時的に保存される。PoS端末上のソフトウェアは、次いで、画面上のスタイラスの時間ベースのトレースの関数を計算し、それを、ワイヤレス無線送信機を使用してウェアラブ

ルアイデンティティマネージャデバイスに送信する。

【００８０】

ウェアラブルアイデンティティマネージャデバイスは、次いで、時間-空間シリーズと時間ベースのトレースとの間の比較に基づいて、それらが互いに所定の信頼度の範囲内で対応するのかどうかについて決定を行う。2つの要素が互いに匹敵することが決定された場合、ウェアラブルアイデンティティマネージャデバイスは、「成功」状態に入る。そうでなければ、ウェアラブルアイデンティティマネージャデバイスは、いくらかのしきい値時間の間、同じ状態にとどまり、潜在的に、追加の信号を受信し、追加の比較を実行する。ウェアラブルアイデンティティマネージャデバイスが成功状態に入ることなく、時間しきい値に達した場合、ウェアラブルアイデンティティマネージャデバイスは、ユーザがスタイラスを手に取る前の状態に戻る。

【００８１】

ウェアラブルアイデンティティマネージャデバイスが成功状態に入った場合、ウェアラブルアイデンティティマネージャデバイスは、PoS端末に関連付けられた無線送信機に成功信号を通信する。例示的な実施態様では、この信号は、ユーザに関連付けられた財源の1つまたは複数の選択に関連付けられた情報を含む。少なくとも2つの選択が利用可能である場合、PoS画面は、これらをユーザに対して表示するために使用され、これは、ユーザがユーザの好みのソースを選択することを可能にする。代替的には、そのような情報は、別のリポジトリから受信される。

【００８２】

成功信号は、さらに、アイデンティティ情報と、好ましくは、ウェアラブルアイデンティティマネージャデバイスまたはユーザアイデンティティに関連付けられた仮名、および使用回数または時間などの、なりすましまたは再生ができないアイデンティティアサーションとを含んでもよいことが企図される。この例では、取引金額と、選択された財源とを示す情報は、アイデンティティ情報とともにバックエンドエンティティに送信される。バックエンドは、次いで、どのようなユーザがどの程度の金額をどのような財源から請求されるべきなのかを決定する。

【００８３】

第2の例示的な使用シナリオでは、第1の例に関連して上記で開示した初期パラメータの多くは、再び仮定される。すなわち、ユーザは、ユーザの利き手の手首にウェアラブルアイデンティティマネージャデバイスを装着し、ウェアラブルアイデンティティマネージャデバイスは、ユーザに以前に関連付けられており、したがってユーザのアイデンティティの表現をすでに記憶していることが仮定される。PoS端末は、再び、ネットワークに接続され、関連するスタイラスを有する画面と、画面上のスタイラスの時間ベースのトレースを記録するために使用されるソフトウェアと、ワイヤレス無線送信機とを備える。ユーザがスタイラスをPoS画面に近づけると、係合信号は、再び、ウェアラブルアイデンティティマネージャデバイスに送信され、係合信号は、ウェアラブルアイデンティティマネージャデバイスに、識別に関連付けられた動作モードに入らせる。

【００８４】

この例では、スタイラスは、加速度計を使用してその運動を決定し、この加速度計データを含む信号は、次いで、識別に関連付けられたモードで動作しているウェアラブルアイデンティティマネージャデバイスに送られる。しかしながら、ウェアラブルアイデンティティマネージャデバイスはまた、加速度計を備え、加速度計は、受信したスタイラス加速度計信号と比較される運動ベースの信号を生成する。ウェアラブルアイデンティティマネージャデバイスが識別モードに入った後、いくらかの時間しきい値の前に、これらが互いに対応するように決定された場合、ウェアラブルアイデンティティマネージャデバイスは、成功状態に入る。システムは、次いで、上記の第1の例で説明したのと同じ手順に従って進む。

【００８５】

第3の例では、自動販売機シナリオが企図される。第1および第2の例と同様に、ユーザ

は、ユーザの利き手の手首にウェアラブルアイデンティティマネージャデバイスを装着し、ウェアラブルアイデンティティマネージャデバイスは、ユーザに以前に関連付けられており、したがって、ユーザのアイデンティティの表現をすでに記憶していることが再び仮定される。ウェアラブルアイデンティティマネージャデバイスは、さらに、加速度計を備えてもよく、加速度計は、ウェアラブルアイデンティティマネージャデバイスによって横断された経路を追跡し、記録するために使用され得る。

【００８６】

この例では、自動販売機は、ユーザ選択を検出するユーザインターフェースと、ユーザが自動販売機に接近したとき、係合信号を送るように構成された無線送信機とを有する。この係合信号は、次いで、ウェアラブルアイデンティティマネージャデバイスによって受信され、これは、ウェアラブルアイデンティティマネージャデバイスを識別モードに入らせる。自動販売機は、次いで、ユーザ選択を検出し、係合されているボタンまたはレバーに関連付けられたタイミングおよび加速度データなどの、相互作用を特徴づける信号をウェアラブルアイデンティティマネージャに送信する。従来の販売時点デバイスはまた、もちろん、この単純化されたユーザ体験手法を使用することができ、ユーザは、単に、たとえば、取引を確定するために、クリックまたは振ることを必要とする。

【００８７】

相互作用を特徴づける信号を受信したら、この特定の取引でユーザを認証するために、ウェアラブルアイデンティティマネージャデバイスは、受信した信号を、ウェアラブルアイデンティティマネージャデバイスによって横断された経路に対応する内部に記憶された加速度計データと比較する。ウェアラブルアイデンティティマネージャデバイスが識別モードに入った後、いくらかの時間しきい値の前に、そのような検出された対応がある場合、ウェアラブルアイデンティティマネージャデバイスは、成功状態に入る。

【００８８】

ウェアラブルアイデンティティマネージャデバイスが成功状態に入った場合、ウェアラブルアイデンティティマネージャデバイスは、自動販売機の無線送信機に成功信号を通信する。そのような成功信号は、さらに、アイデンティティ情報と、好ましくは、ウェアラブルアイデンティティマネージャデバイスまたはユーザアイデンティティに関連付けられた仮名、および使用回数または時間などの、なりすましまたは再生ができないアイデンティティアサーションとを含んでもよいことが企図される。この例では、取引金額および選択された財源を示す情報は、自動販売機によって、アイデンティティ情報とともにバックエンドエンティティに送信される。バックエンドは、次いで、どのようなユーザがどの程度の金額をどのような財源から請求されるべきなのかを決定する。

【００８９】

例示的な利益

当業者は、様々な利益が本明細書で開示された態様を実施することによって達成され得ることを容易に理解するであろう。例示的な利益の非網羅的なリストを以下に提供する。

【００９０】

第1の例示的な利益は、ユーザは、(おそらく、アイデンティティマネージャがユーザに関連付けられるときに、ユーザのアイデンティティマネージャに対して認証する以外に)任意の信用証明書を使用する習慣がないので、ユーザがフィッシング攻撃に対して保護されることである。ユーザはまた、アイデンティティマネージャは、認証を要求する局にどのような従来の信用証明書も伝達しないので、そのような攻撃から保護されるであろう。

【００９１】

別の例示的な利益は、ユーザが、マルウェアに対してある程度保護されることである。これは、アイデンティティマネージャとその周囲との間の非常に制約されたインターフェースは、アイデンティティマネージャが破損するのをより困難にするためである。具体的には、ユーザは、ユーザのアイデンティティマネージャに任意のソフトウェアをインストールする可能性が低いので、脆弱性のクラス全体が回避される。

【００９２】

本明細書で開示された態様のさらなる利益は、弱い信用証明書に関するものである。すなわち、信用証明書は、関連付け段階でのみ使用されるので、信用証明書の品質は、あまり問題にはならない。これは、弱い信用証明書の潜在的な使用を、対象となるアイデンティティマネージャに物理的にアクセスできる人に限定する。

【００９３】

また、アイデンティティマネージャまたは関連するプロキシのいずれかが、パスワードマネージャとして機能する場合、これはまた、アイデンティティマネージャと直接互換性がないサイトでパスワードを管理するタスクからユーザを解放する。潜在的なマルウェア攻撃に対する関連する解決策の露出は、まず第1に、どのようなエンティティがパスワードマネージャとして機能しているかに依存し、それが電話である場合、パスワードマネージャが安全な実行環境で動作しているかどうかに依存する。

【００９４】

ユーザはまた、サイトの侵害に対していくらかの強化したセキュリティを得ることができる。たとえば、アイデンティティマネージャによって送信された取引トークンは、盗まれた場合、使いみちがない。ローリングコードの出力は、たとえば、デジタル署名に基づく暗号化トークンがそうであるように、そのような利益を提供する。

【００９５】

例示的なウェアラブルアイデンティティ認証の使用シナリオ

第1の例示的な使用シナリオでは、ユーザは、上記で説明したように、ウェアラブルアイデンティティマネージャデバイスのブレスレット構成と、2つの電話、ユーザが主に仕事のために使用する1つと、ユーザが主に私事のために使用する別の1つとを有する。両方の電話は、認証プロセスのために使用されるインストールされたソフトウェアを有する。仕事用電話は、ユーザの雇用者によってインストールされたマスタデータ管理(MDM(master data management))アプリケーションを有し、自宅の個人用電話は、アプリケーションストアからユーザによってダウンロードされた個人的なアプリケーションを有する。MDMアプリケーションと個人的アプリケーションの両方は、ユーザに関連付けられた暗号化ユーザプロファイルをダウンロードし、電話とブレスレットとの間の関連付けプロセスのために使用される信用証明書を登録することよって構成されている。ビジネス電話について、この信用証明書は、ビジネス電話上の指紋センサに関連付けられた生体測定テンプレートである。個人用電話に関して、それは、パスワードである。これらの信用証明書の両方は、安全な方法で記憶される(たとえば、安全なストレージ内に、またはハッシュされ、記憶される)。

【００９６】

典型的な朝に、ユーザは、起床し、シャワーを浴び、次いでユーザのブレスレットを付けることになる。ユーザがブレスレットの留め金を閉じると、ブレスレットのウェアラブルアイデンティティマネージャは、自動的に関連付け段階に置かれる。これは、ユーザが1メートルよりもわずかに短くてもよい電話の無線距離内に達したとき、ユーザの個人用電話を起動させる。個人用電話は、ブレスレットのウェアラブルアイデンティティマネージャによって放射された低電力Bluetooth（登録商標）信号を検出し、これが、以前にBluetooth（登録商標）ペアリングされたユニットのためのものであることを決定し、接続を作成する。Bluetooth（登録商標）接続が確立された後、電話の画面は、「アリスのブレスレットに接続」というメッセージを表示し、たとえば、「アリスのブレスレットのためのパスワードを入力してください」というテキストをすぐに続けてもよい。ユーザは、次いで、ユーザの個人用電話の画面上の小さいボックス内にユーザのパスワードをタイプする。これは、電話によって、パスワードをハッシュし、ハッシュされたパスワードを、ブレスレットと電話の関連付けに関連する以前に記憶されたパスワードと比較することによって検証される。ユーザは、次いで、電話を、ユーザがブレスレット装着している手で振る。電話内の加速度計は、ユーザが以前に入力したパスワードが正確だった場合にのみ、加速度計出力から信号ダイジェストを計算し、これをブレスレットに送る。電話はまた、これがユーザのパスワードであるという指示を、ブレスレットのウェアラブルアイデンテ

ィティマネージャに送信する。この通信のすべては、Bluetooth（登録商標）接続に関連する対称暗号化を使用して安全化される。ブレスレット内の加速度計はまた、動きに基づいて信号を生成し、ブレスレットのウェアラブルアイデンティティマネージャは、電話から受信したダイジェストを生成した信号と比較し、これらが互いに対応した場合、ウェアラブルアイデンティティマネージャは、関連付けを受け入れ、今(電話によってそこに伝達された)ユーザによって装着されていることを記憶する。

【００９７】

朝食後、ユーザは、ユーザの個人用電話上でユーザの電子メールをチェックするためにログインすることを望む。ユーザは、電子メールアプリケーションを起動し、(ユーザは、電子メールアプリケーションが使用されていないとき、電子メールアプリケーションがロックモードになるように設定しており、アクセスするために認証を必要とするので)電子メールアプリケーションは、認証を必要とすることを示す。ユーザは、ユーザのブレスレットを装着しているので、ユーザは、そうでなければユーザがユーザの電子メールにアクセスするために使用しなければならないPINを入力する必要はない。代わりに、ユーザは、ブレスレットを有する手を使用して電話を優しく振る。ユーザの電子メールリーダアプリケーションは、数ある中で、ユーザのブレスレットのウェアラブルアイデンティティマネージャに関連付けられた認証ライブラリを使用し、認証ライブラリは、ウェアラブルアイデンティティマネージャとの通信セッションを開始し、通信セッションは、安全なチャネルを介して、ブレスレットがユーザによって装着されていることを電話に通信する。認証ライブラリは、メールアプリケーションをアンロックし、それは、ユーザがユーザの電子メールを読むことを可能にする。

【００９８】

その後、ユーザは、ユーザの銀行口座にアクセスすることを望み、ユーザの銀行に関連するバンキングアプリケーションを起動する。バンキングアプリケーションは、個人用電話上で実行され、また、上記で説明した認証ライブラリを使用する。バンキングアプリケーションが開始されると、バンキングアプリケーションは、ログインを要求する。ユーザは、次いで、ユーザの電話を優しく振り、ユーザのブレスレットのウェアラブルアイデンティティマネージャとのセッションが開始される。上記で説明したものと同様に、ウェアラブルアイデンティティマネージャは、信号を個人用電話に送信し、信号は、アプリケーションライブラリに関連付けられたコードによって処理される。アプリケーションライブラリは、パスワードマネージャ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)を呼び出し、ユーザが電話を使用していることを示す。パスワードマネージャは、ユーザの銀行へのアクセスである読出しのコンテキストを決定し、ユーザの名前および信用証明書を記憶するために使用される安全なリポジトリからユーザのユーザ名およびパスワードを検索する。これらは、バンキングアプリケーションへの入力であり、バンキングアプリケーションは、それらを受信すると、それらを、ユーザの銀行によってすでに開始されたセキュアソケットレイヤ(SSL(secure sockets layer))セッションを介して伝達する。ユーザの銀行は、これが正しいログインであることを検証し、口座へのアクセスを許可し、ユーザの個人用電話上のバンキングアプリケーションと通信する。

【００９９】

その後、ユーザは、ログアウトし、次いで、仕事に行く途中で地下鉄に向かう。出発する前に、ユーザは、ビジネス用電話をつかむ。ユーザのカレンダをチェックするためにそれにログインする代わりに、ユーザは、ユーザがブレスレットを装着している手でビジネス用電話を優しく振る。ビジネス用電話はまた、ウェアラブルアイデンティティマネージャとすでにペアリングされており、ウェアラブルアイデンティティマネージャとのBluetooth（登録商標）セッションを開始する。ブレスレットは、個人用電話にすでに関連付けられており、それを行うことによって、ユーザによって装着されていることがインプリントされているので、ユーザの個人用電話とブレスレットのウェアラブルアイデンティティマネージャとの間の、上記で説明した関連付けは、必要ない。ウェアラブルアイデンティティマネージャは、この事実をビジネス用電話に伝達し、ビジネス用電話は、次いで、自

動的にアンロックされる(PINは、必要ない)。

【０１００】

ユーザは、ユーザのスケジュールを見て、ユーザが地下鉄に乗る前にコーヒーのための時間を有することを認識する。ユーザは、ユーザの近所のカフェに行き、コーヒーを注文し、認証するためにユーザの手を振る。ユーザのブレスレットは、販売時点コンピュータとのBluetooth（登録商標）接続を確立し、販売時点コンピュータは、ユーザが記憶されたファイナンシャル(financial)を有することを検証し、ユーザのクレジットカード上で自動的に3ドル請求する。

【０１０１】

ユーザのコーヒーを購入した後、ユーザは、地下鉄まで歩く。ユーザが改札を通過するとき、ユーザは、改札を通過するためにユーザの手を振る必要はなく、トークンを提供するか、登録されたブレスレットを装着する必要がある。ここで、ユーザは、ユーザのブレスレットを登録していると仮定する。改札がユーザの通過を許可する前に、改札は、ユーザのブレスレットとの接続を開始し、暗号化チャネルを介して送信された識別値を取得し、この値は、ユーザのアカウントに関連付けられる。ユーザの残高は、自動補充のためのしきい値(ユーザは、これを10ドルに設定する)よりも高いので、ユーザのクレジットカードに対する課金は必要なく、ユーザの残高は、地下鉄運賃の金額だけ単に減少される。

【０１０２】

30分後、ユーザは、職場に到着する。ユーザのオフィスでは、回転ドアは、ユーザのブレスレット内のウェアラブルアイデンティティマネージャとの接続を作成し、ユーザが登録された従業員であることを決定し、次いでユーザを通す。ユーザがユーザの机に着席したとき、ユーザのコンピュータは、ユーザの仕事用電話に対するWiFiを介する接続を確立し、仕事用電話は、次に、ユーザのブレスレットのウェアラブルアイデンティティマネージャとの接続を確立する。ユーザの電話内のパスワードマネージャは、ウェアラブルアイデンティティマネージャが、電話から受信した加速度計信号を、内蔵加速度計によって生成された信号と比較した後、ウェアラブルアイデンティティマネージャによってアンロックされる。もちろん、実質的に同じであることに加えて、それらは、また、いくらかの運動、この場合、短い振りを示す必要がある。ユーザの電話のパスワードマネージャは、ユーザのコンピュータをアンロックし、ユーザは、パスワードでログインする必要はない。

【０１０３】

ウェアラブルアイデンティティマネージャのこれらの使用のいくつかでは、振りが必要であり、他のものでは、振りは必要ではなかったことに留意すべきである。これは、ウェアラブルアイデンティティマネージャへの接続を行うソフトウェアによって決定され、加速度計信号が伝達されるか、または、振りが必要ないことの指示が伝達される。ペアリングされたデバイスのみがウェアラブルアイデンティティマネージャによって受け入れられるので、不正デバイスが不適切な信号を伝達することは不可能である。また、同様の振るアクションがユーザのウェアラブルアイデンティティマネージャによって登録されないので、ユーザの銀行口座にアクセスしたい誰かがユーザの電話を振ることは不可能である。このように、ユーザは、一日中どのような信用証明書を入力する必要もない。ユーザが家に帰ったとき、ユーザは、ブレスレットを外し、ブレスレットは、ここで、任意の認証に参加する前に、再びユーザに関連付けられる必要がある状態にそれ自体を自動的に置く。したがって、ユーザが友人に会うために外出している間にユーザの家に侵入する強盗は、強盗がユーザの電話の1つも盗んだとしても、強盗は、関連付けプロセスを正常に通過するためにユーザとして認証することができないので、ユーザのアカウントを使用することができない。

【０１０４】

第2の例示的な使用シナリオでは、ユーザは、リストバンドが開閉されたときを検出する腕時計構成のウェアラブルアイデンティティマネージャデバイスをちょうど購入した。ユーザがリストバンドを最初に閉じたとき、ウェアラブルデバイスマネージャは、それ自体を設定状態に置く。ユーザは、腕時計製造業者のウェブサイトからコンパニオンアプリ

ケーションをダウンロードし、これをユーザの電話にインストールする。ユーザがアプリケーションを起動すると、アプリケーションは、ユーザの腕時計をユーザの電話に関連付けるために、ユーザが腕時計のための名前を入力し、パスワードを選択することを要求する。(ユーザの電話は、生体測定センサを持っていない。)これを行った後、ユーザの電話に関連付けられたウェアラブルアイデンティティマネージャは、ユーザが入力した情報に関連付けられ、ログインするために使用され得る。

【０１０５】

ユーザがその日より後にユーザの電話を使用してオンラインオークションサイトを訪れたとき、ユーザの電話上の認証ライブラリは、ユーザがパスワードマネージャ内に記録されていない場所にログインしていることを決定し、ユーザがこのユーザ名およびパスワードがパスワードマネージャ内に記憶されることを望む場合、ユーザがユーザの電話を装着している手首の手を使用してユーザの電話を振るようにユーザに要求する。ユーザは、このアイデアを気に入り、ユーザの手を振る。ユーザがオークションサイトを訪れた次のとき、ユーザのユーザ名とパスワードの両方は、ユーザの電話のパスワードマネージャによってオートフィルされ、ユーザは、ログインすることになるので、ユーザは、ユーザのユーザ名およびパスワードを使用してログインする必要はない。

【０１０６】

しかしながら、ユーザはまた、ユーザのラップトップを使用して様々なアカウントにログインする。ユーザは、ユーザのラップトップブラウザにブラウザプラグインをダウンロードする。ブラウザプラグインは、ユーザの電話を、ユーザが標準のBluetooth（登録商標）ペアリングプロトコルを使用しているラップトップコンピュータにペアリングするようにユーザに要求する。ブラウザプラグインは、次いで、ユーザの電話上のパスワードマネージャに関連付けられたリポジトリをコピーする許可を要求する。ユーザは、ブラウザプラグインにこの許可を与えない。プラグインは、次いで、ユーザの電話上のパスワードマネージャを使用することを要求し、ユーザは、これに同意する。結果として、ユーザの電話上のパスワードマネージャは、必要なとき、ユーザのラップトップとペアリングするように構成される。

【０１０７】

ユーザがユーザのラップトップ上でオークションサイトを訪れたとき、ユーザのラップトップ上のルーチンは、これがログインセッションであることを決定し、ユーザの電話およびその上のパスワードマネージャとの接続を確立する。パスワードマネージャは、パスワードマネージャがこのドメインのために記憶されたユーザ名および信用証明書を有することを決定し、ユーザの腕時計のウェアラブルアイデンティティマネージャとの接続を開始する。ユーザは、ユーザの手を優しく振り、ウェアラブルアイデンティティマネージャは、ウェアラブルアイデンティティマネージャが電話から受信した信号が、オンボード加速度計を使用してウェアラブルアイデンティティマネージャ自体が生成した信号と一致することを決定する。この結果として、および前に説明したものと同様の方法で、ユーザの電話のパスワードマネージャは、ラップトップ上のオークションサイトのためのパスワードを使用する許可を取得する。結果として、ユーザ名および信用証明書は、安全な接続を介してラップトップに伝達され、または代替的には、オークションサイトへのセッションを開始するために使用され、このセッションは、次いで、ラップトップに引き渡され、ユーザは、ログインされる。

【０１０８】

ユーザが後にユーザのラップトップ上でユーザの銀行のウェブサイトを訪れ、ログインしたとき、ユーザがインストールしたブラウザプラグイン内のルーチンは、ユーザがログインしていることを決定する。ルーチンは、ユーザの電話上のパスワードリポジトリにユーザ名および信用証明書を追加する要求を表示している。これは、ユーザのコンピュータの画面上に表示される。ユーザは、この要求を受け入れ、ユーザのラップトップから送られたユーザ名および信用証明書をユーザの電話上のパスワードマネージャに伝達するためにユーザの電話を振る。

【０１０９】
このシナリオでは、以前のユーザ(以下、「アリス」)および現在のユーザ(以下、「ボブ」)は、友達であり、アリスは、ときどきボブのラップトップを使用する。アリスがボブのラップトップを使用し、サイトを訪れる、またはログインを必要とするアプリケーションを使用するとき、ボブのラップトップは、それが関連付けられたどのような電話が存在するのかを決定することになる。アリスが、アリスとボブの両方が使用するオークションサイトを訪れたとき、ボブのラップトップは、アリスの電話とボブの電話の両方が存在することを決定し、ログインを完了するために両方の電話とのセッションをセットアップする。ボブは、ラップトップを使用していないが、アリスは、ラップトップを使用しているので、アリスがコンピュータ上のログイン画面を見たとき、アリスは、アリスの電話を手に取る。アリスは、アリスのウェアラブルアイデンティティマネージャに関連付けられたブレスレットをアリスが装着している手首の手で電話に一振りを与え、したがって、アリスの電話は、認証が完了したことを示す信号を取得し、アリスの電話は、ボブのラップトップ上でアリスをログインするためにそのパスワードマネージャルーチンに係合する。
【０１１０】
ボブは、ときどきボブの電話を使用する別のユーザ、シンディとも友達である。ボブの電話は、ボブのプロファイルとシンディのプロファイルの両方を含むパスワードマネージャを有する。シンディがボブの電話を使用して、またはボブの電話に接続されたコンピュータを使用してリソースにアクセスしたとき、ボブの電話上のパスワードマネージャは、ボブまたはシンディのどちらのプロファイルを選択するのかを決定し、シンディの腕時計とペアリングされたボブの電話がシンディの腕時計から確認信号を受信した後、シンディのプロファイルに決定する。この信号は、ボブの電話およびシンディの腕時計上で生成された加速度計信号を比較することによって生成される。
【０１１１】
ある日、シンディは、本当にボブに腹を立て、ボブの電話からの信号を承認しないようにシンディの電話を設定する。シンディは、シンディの腕時計とペアリングされており、腕時計のマスタデバイスであるシンディ自身の電話を使用してこれを行う。ボブの電話は、シンディの腕時計のマスタデバイスではなく、シンディの電話に関連付けられているだけなので、ボブは、ボブが望んでも、シンディの腕時計における設定を変更することができない。次の日、シンディは、自分の心を変化させ、ボブの電話とのセッションを再び可能にするようにシンディの電話を再設定する。しかしながら、ボブはまた、ボブのパスワードマネージャに関連付けられたリポジトリからシンディのプロファイルを消去するようにボブの電話を再設定しているので、シンディは、認証を実行するためにボブの電話を使用することができない。シンディは、シンディのプロファイルを再び追加するようにボブに頼み、ボブは、同意する。ボブは、ボブの腕時計内のウェアラブルアイデンティティマネージャを使用して、ボブの手の振りでボブの電話に認証し、次いで、シンディがシンディのプロファイルを追加することを承認する。シンディは、シンディの暗号化されたプロファイルをシンディが使用するクラウドストレージからダウンロードし、それを追加する。クラウドストレージは、シンディの腕時計から発生し、ユーザが、シンディがシンディのプロファイルを追加することを承認した後にボブの腕時計に通信された、暗号化された要求を含む要求をボブの電話から受信するので、クラウドストレージは、ダウンロードを要求しているのがシンディであることを知る。シンディは、シンディの手に電話を取り、それを振り、暗号化された要求は、クラウドストレージ場所の情報とともに、ボブの電話上のパスワードマネージャによって受信され、使用される。シンディは、ここで、ボブの電話を再び使用することができる。
【０１１２】
シンディが数週間後にタブレットコンピュータを買ったとき、シンディは、タブレットコンピュータをシンディの腕時計とペアリングし、ボブの電話について行った方法と同様に、シンディの新しいタブレットのパスワードマネージャがクラウドストレージからシンディのプロファイルの暗号化されたコピーをダウンロードするのを、振りを使用して認証

する。暗号化は、これらの場合の両方において、盗み聞きする人がデータを学習するのを妨げ、SSLなどの技術を使用する。

【０１１３】

第3の例示的な使用シナリオでは、デイブは、加速度計を持たないことを除いて以前に説明したブレスレットおよび腕時計と同様の機能を有する腕時計を有する。代わりに、腕時計は、デイブが要求に賛成したときにデイブが押すことができるボタンを有する。デイブがデイブの電話を腕時計とペアリングしたとき、電話と腕時計の両方は、それらの画面上に番号を表示し、デイブは、これらが互いに対応することを確認するためにそれらの番号を比較する。それらは、対応するので、デイブは、承認するためにボタンを押し、それらは、互いに関連付けられる。

【０１１４】

後に、デイブは、デイブの電話を取り除き、電話は、それが再び関連付けられることを必要とするときの状態に戻る。デイブは、再びペアリングを行い、それは、もう一度電話に関連付けられる。デイブは、次いで、デイブの電話を使用してサイトにログインすることを望み、サイトは、デイブの電話に要求を送る。メッセージがデイブの電話に表示され、ボタンを押すことによってログイン要求を承認するか、または、デイブが要求を承認したくない場合、単に、ボタンを押すことなく3秒間待機するようにデイブに要求する。デイブは、ボタンを押し、デイブの腕時計は、信号を電話に送り、信号は、パスワードマネージャに伝達されたとき、適切なユーザ名および信用証明書の検索を開始し、サイトへのデイブのログインが続く。

【０１１５】

後に、デイブは、ウェアラブルアイデンティティマネージャを有するネックレスを与えられる。これは、ちょうどデイブの電話のように、加速度計を有する。それらをペアリングするために、デイブは、単にネックレスを付け、デイブの手の中の電話、デイブがネックレスをデイブと関連付けるために使用している電話とともに歩く。デイブが電話を振らず、単に自分の手の中の電話とともに歩くことを除いて、アリスのブレスレットがそれ自体をアリスの電話と関連付けたのと同じ方法で、ネックレスは、それ自体を電話に関連付ける。電話の加速度計出力とネックレスの加速度計出力とは比較され、それらが互いに対応することの決定が行われ、その後、ネックレスは、デイブに関連付けられる。その後、デイブは、アイデンティティのソースとしてデイブのネックレスを使用して、購入を実行することを望む。デイブは、デイブの電話の画面上の「購入を承認する」ボタンを押し、前後に小さく2、3歩歩くか、または前後に優しく振り、ウェアラブルアイデンティティマネージャおよびパスワードマネージャが、「購入を承認する」ボタンを押したのと同じ人によって使用されていることを検証することを可能にする。

【０１１６】

デイブのネックレスの場合には、ネックレスが、認証を行うためにアカウントに関連付けられることを再度必要とする状態にネックレスが置かれ得るように、ネックレスが、装着者のアイデンティティ情報を記憶し、ネックレスが外されたときを検出するためのみに使用される追加の小型のバッテリを有するとき、この比較は、デイブの電話において実行される。ネックレスの無線送信機は、ちょうど無線周波数識別(RFID)トークンのように、信号の送信と信号の受信の両方のために、背景無線信号によって電力供給される。

【０１１７】

しばらくの間、ネックレスを装着した後、デイブは、ネックレスをアリスに貸し、アリスは、ネックレスをアリスの電話に関連付け、ネックレスをアリスのブレスレットの代わりに使用する。アリスがネックレスをデイブに返したとき、ネックレスは、デイブがネックレスを付けたとき、ネックレス自体をデイブおよびデイブの電話に関連付ける。

【０１１８】

第4の例示的な使用シナリオでは、本明細書で開示された態様は、従来のログインプロセスを置換えるように実施される。電話などのモバイルデバイス上で、ユーザは、(たとえば、電話を取り上げる、その画面に触れる、またはボタンを押すことによって)単に電

話を起動することによってログインプロセスを開始してもよい。プロセスはまた、ユーザがアプリケーションを開始することによって、またはアプリケーションによって参照されるリソースにアクセスすることを試みることによって開始されてもよい。例示的なリソースは、ユーザのアドレス帳、電子メール、(最近かけられた電話のリストなどの)利用ログファイル、写真または写真のディレクトリ、および市外電話をかける能力である。デスクトップまたはラップトップは、同様の方法でアクセスされてもよく、マウス、マウスパッド、またはキーボードは、保証または確認を得るために使用されるべきデータを収集する役割を引き受ける。

【０１１９】

異なるリソースはまた、異なるセキュリティレベルに関連付けられてもよく、たとえば、ユーザは、電話をアンロックするために中間のセキュリティレベル、(起動されたら)その電子メールリーダにアクセスするために低いセキュリティレベル、利用ログへのアクセスを得るために高いセキュリティレベルを要求してもよい。同じユーザは、次いで、ユーザの仕事用コンピュータにログインするために高いセキュリティレベルを要求してもよいが、家庭用コンピュータは、そもそも人々の小さいグループによってのみアクセス可能であるので、ユーザの家庭用コンピュータにログインするために中間のセキュリティレベルのみを必要としてもよい。ユーザまたはユーザの雇い主はまた、異なるタイプのアクセスに対して異なるレベルのセキュリティを割り当ててもよい。

【０１２０】

アイデンティティマネージャまたは関連するプロキシのいずれかが、アイデンティティマネージャ技術と互換性がないサイトのためのパスワードマネージャとして機能する特定のログインの場合も企図される。ここで、ログインセッションは、これらのデバイスの1つによって、その促進デバイスにセッションの秘密を公開することなく調整(moderate)されてもよい。

【０１２１】

第5の例示的な使用シナリオでは、本明細書で開示された態様は、オンライン支払であるか販売時点支払であるかにかかわらず、支払を容易にするために実装される。オンライン支払を実行するために、ユーザは、チェックアウトボタンをクリックすることによって支払プロセスを開始する。低および中リスクの購入について、これは、中間のレベルのセキュリティを提供するので、十分であり得る。しかしながら、高リスクの購入について、明示的な確認が、その代わりに必要とされる可能性がある。ここで、値、商品のタイプ、ユーザの購入履歴、購入が開始された場所などの多くの要因が、取引のリスクレベルに影響する可能性がある。要求されるセキュリティのレベルは、ユーザ、商人、金融機関、またはそれらの組合せによって選択されてもよい。たとえば、ユーザは、最小レベルのセキュリティのためにユーザの好みを設定してもよいが、これらは、商人または金融機関によって設定されたポリシーによって選択的に強化されてもよい。販売時点取引について、明示的な確認は、ユーザが販売時点端末上にユーザの署名を署名し、動きがユーザのアイデンティティマネージャの動きと相関されたとき、得られてもよい。これは、ユーザの意図の保証(係争中の取引のために有用であり得る)を提供するだけでなく、何人かの可能なユーザのうちのどの1人が取引に関連付けられるべきかを識別するのを助けることもできる。地下鉄運賃の支払などの他のタイプの支払は、近接度検証よりも高いセキュリティを必要としない可能性がある。

【０１２２】

第6の例示的な使用シナリオでは、本明細書で開示された態様は、属性目的のために実装される。この目的のため、タッチスクリーンに関連付けられた加速度計トレースをブレスレットの加速度計トレースと比較することによって、複数のユーザが同時にタッチスクリーンに触れたときであっても、スクリーンに対するユーザ対話を帰属させることができ、これは、ゲーミング環境の新しいタイプを生じさせることができることが留意される。これはまた、ユーザが同時に2つのブレスレットを装着することが意味を成すいくつかの使用シナリオのうちの1つであり得る。ゲームのコンテキストでは、ユーザアイデンティ

ティにアクションを帰属させることが必要でない可能性があるが、ある形式の擬似匿名がより実用的である可能性がある。

【０１２３】

例示的なネットワーク環境および分散環境

当業者は、コンピュータネットワークの一部として、または分散コンピューティング環境内に展開され得、任意の種類のデータストアに接続され得る任意のコンピュータまたは他のクライアントまたはサーバデバイスに関連して、コンピューティングデバイスを利用するための様々な実施態様および本明細書に記載の関連する態様が実装され得ることを理解することができる。さらに、当業者は、そのような態様が、任意の数のメモリまたは記憶ユニットと、任意の数の記憶ユニットにわたって生じる任意の数のアプリケーションおよびプロセスとを有する任意のコンピュータシステムまたは環境において実装され得ることを理解するであろう。これは、限定はしないが、リモートまたはローカルストレージを有するネットワーク環境または分散コンピューティング環境内に配備されるサーバコンピュータおよびクライアントコンピュータを有する環境を含む。

【０１２４】

図18は、例示的なネットワークまたは分散コンピューティング環境の非限定的な概略図を提供する。分散コンピューティング環境は、コンピューティングオブジェクトまたはデバイス1810、1812、などと、コンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などとを備え、これらのコンピューティングオブジェクトまたはデバイスは、アプリケーション1830、1832、1834、1836、1838によって表されるように、プログラム、方法、データストア、プログラマブルロジック、などを含んでもよい。コンピューティングオブジェクトまたはデバイス1810、1812、など、およびコンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などは、PDA(携帯情報端末)、オーディオ/ビデオデバイス、モバイル電話、MP3プレーヤ、ラップトップ、などの異なるデバイスを備えてもよいことが理解され得る。

【０１２５】

各コンピューティングオブジェクトまたはデバイス1810、1812、など、およびコンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などは、直接または間接的に、通信ネットワーク1840によって、1つまたは複数の他のコンピューティングオブジェクトまたはデバイス1810、1812、など、およびコンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などと通信することができる。図18中には単一の要素として示されているが、ネットワーク1840は、図18のシステムにサービスを提供する他のコンピューティングオブジェクトおよびコンピューティングデバイスを備えてもよく、ならびに/または、図示されていない複数の相互接続されたネットワークを表してもよい。各コンピューティングオブジェクトまたはデバイス1810、1812、など、または1820、1822、1824、1826、1828、などはまた、様々な実施態様による、開示された態様と通信するのに適した、または開示された態様の実装に適した、API(アプリケーションプログラミングインターフェース)、または他のオブジェクト、ソフトウェア、ファームウェア、および/またはハードウェアを利用することができるアプリケーション1830、1832、1834、1836、1838などのアプリケーションを含むことができる。

【０１２６】

分散コンピューティング環境をサポートする様々なシステム、構成要素、およびネットワーク構成が存在する。たとえば、コンピューティングシステムは、ローカルネットワークまたは広域分散ネットワークによって、ワイヤードまたはワイヤレスシステムによって互いに接続され得る。任意のネットワークインフラストラクチャが、様々な実施態様において説明したように技術に付随された例示的な通信のために使用され得るが、現在、多くのネットワークは、広域分散コンピューティングのためのインフラストラクチャを提供し、多くの異なるネットワークを包含するインターネットに結合されている。

【０１２７】

したがって、クライアント/サーバ、ピアツーピア、またはハイブリッドアーキテクチ

ャなどの、ネットワークトポロジおよびネットワークインフラストラクチャのホストが使用され得る。クライアント/サーバアーキテクチャ、特にネットワークシステムでは、クライアントは、通常、別のコンピュータ、たとえば、サーバによって提供される共有ネットワークリソースにアクセスするコンピュータである。任意のコンピュータが、状況に応じて、クライアント、サーバ、またはその両方とみなされ得るが、図18の例示では、非限定的な例として、コンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などは、クライアントとして考えられ得、コンピューティングオブジェクトまたはデバイス1810、1812、などは、サーバとして考えられ得、コンピューティングオブジェクトまたはデバイス1810、1812、などは、コンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などからのデータの受信、データの記憶、データの処理、コンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などへのデータの送信などのデータサービスを提供する。これらのコンピューティングデバイスのいずれかは、データを処理してもよく、または、1つまたは複数の実施態様について本明細書で説明した態様および関連技術を関係させてもよいサービスまたはタスクを要求してもよい。

【０１２８】

サーバは、典型的には、インターネットまたはワイヤレスネットワークインフラストラクチャなどの、リモートまたはローカルネットワークを介してアクセス可能なリモートコンピュータシステムである。クライアントプロセスは、第1のコンピュータシステムにおいてアクティブであってもよく、サーバプロセスは、第2のコンピュータシステムにおいてアクティブであってもよく、通信媒体を介して互いに通信し、分散機能を提供し、複数のクライアントがサーバの情報収集能力を利用することを可能にする。ユーザプロファイルに従って利用される任意のソフトウェアオブジェクトは、スタンドアロンで、または複数のコンピューティングデバイスまたはオブジェクトにわたって分散されて提供され得る。

【０１２９】

通信ネットワーク/バス1840がインターネットであるネットワーク環境では、たとえば、コンピューティングオブジェクトまたはデイバス1810、1812、などは、コンピューティングオブジェクトまたはデバイス1820、1822、1824、1826、1828、などが、HTTPなどのいくつかの公知のプロトコルのいずれかを介して通信するウェブサーバであり得る。上述したように、分散コンピューティング環境の特徴であり得るように、コンピューティングオブジェクトまたはデイバス1810、1812、などはまた、コンピューティングオブジェクトもしくはデバイス1820、1822、1824、1826、1828、などとして、またはその逆に働いてもよい。

【０１３０】

例示的コンピューティングデバイス

上述したように、上記の実施態様のうちのいくつかは、任意のデバイスに適用され、本明細書で開示された態様を実装することを容易にするために、コンピューティングデバイスを含むことが望ましい可能性がある。したがって、すべての種類のハンドヘルド、ポータブル、および他のコンピューティングデバイスおよびコンピューティングオブジェクトは、本明細書に記載の様々な実施態様に関連して使用することが企図されることが理解される。したがって、図19において以下で説明する以下の汎用リモートコンピュータは、一例であり、本開示の実施態様は、ネットワーク/バスの相互運用性および相互作用を有する任意のクライアントで実装されてもよい。

【０１３１】

必須ではないが、実施態様のいずれかは、部分的には、デバイスまたはオブジェクトのためのサービスの開発者による使用のために、オペレーティングシステムを介して実装され得、および/または、動作可能な構成要素に関連して動作するアプリケーションソフトウェア内に含まれ得る。ソフトウェアは、クライアントワークステーション、サーバ、または他のデバイスなどの、1つまたは複数のコンピュータによって実行される、プログラ

ムモジュールなどの、コンピュータ実行可能命令の一般的な文脈で説明されることがある。当業者は、ネットワーク相互作用が、様々なコンピュータシステム構成およびプロトコルで実施され得ることを理解するであろう。

【０１３２】

図19は、したがって、1つまたは複数の実施態様が実装され得る適切なコンピューティングシステム環境1900の一例を示すが、上記で明らかになったように、コンピューティングシステム環境1900は、適切なコンピューティング環境の単なる一例であり、実施態様のいずれかの使用または機能の範囲に関するいかなる限定も示唆することを意図していない。コンピューティング環境1900は、例示的なコンピューティング環境1900で例示した構成要素の任意の1つまたは組合せに関する任意の依存性または要件を有するものとして解釈されるべきではない。

【０１３３】

図19を参照し、本明細書における1つまたは複数の実施態様を実装するための例示的なリモートデバイスは、ハンドヘルドコンピュータ1910の形態における汎用コンピューティングデバイスを含むことができる。ハンドヘルドコンピュータ1910の構成要素は、限定はしないが、処理ユニット1920と、システムメモリ1930と、システムメモリを含む様々なシステム構成要素を処理ユニット1920に結合するシステムバス1921とを含んでもよい。

【０１３４】

コンピュータ1910は、典型的には、様々なコンピュータ可読媒体を含み、コンピュータ1910によってアクセスされ得る任意の利用可能な媒体であり得る。システムメモリ1930は、読出し専用メモリ(ROM)および/またはランダムアクセスメモリ(RAM)などの、揮発性および/または不揮発性メモリの形態におけるコンピュータ記憶媒体を含んでもよい。例として、限定ではなく、メモリ1930はまた、オペレーティングシステムと、アプリケーションプログラムと、他のプログラムモジュールと、プログラムデータとを含んでもよい。

【０１３５】

ユーザは、入力デバイス1940を介してコンピュータ1910にコマンドおよび情報を入力してもよい。モニタまたは他のタイプの表示デバイスも、出力インターフェース1950などのインターフェースを介してシステムバス1921に接続される。モニタに加えて、コンピュータはまた、出力インターフェース1950を介して接続され得る、スピーカおよびプリンタなどの他の周辺出力デバイスを含んでもよい。

【０１３６】

コンピュータ1910は、リモートコンピュータ1970などの、1つまたは複数の他のリモートコンピュータとの論理接続を使用して、ネットワークまたは分散環境で動作してもよい。リモートコンピュータ1970は、パーソナルコンピュータ、サーバ、ルータ、ネットワークPC、ピアデバイスもしくは他の共通ネットワークノード、または、任意の他のリモート媒体消費もしくは送信デバイスであってもよく、コンピュータ1910に関連する上記で説明した要素のいずれかまたはすべてを含んでもよい。図19中に示す論理接続は、ローカルエリアネットワーク(LAN)またはワイドエリアネットワーク(WAN)などのネットワーク1971を含むが、また、他のネットワーク/バスを含んでもよい。そのようなネットワーキング環境は、家庭、オフィス、企業規模のコンピュータネットワーク、イントラネット、およびインターネットにおいて一般的である。

【０１３７】

上述したように、例示的な実施態様は、様々なコンピューティングデバイス、ネットワーク、および広告アーキテクチャに関連して説明されているが、基礎となる概念は、本明細書で開示された態様を実装するのに望ましい任意のネットワークシステムおよび任意のコンピューティングデバイスまたはシステムに適用されてもよい。

【０１３８】

本明細書に記載の1つまたは複数の態様を実装する複数の方法、たとえば、本明細書で開示された態様をアプリケーションが実装することを可能にする、適切なAPI、ツールキット、ドライバコード、オペレーティングシステム、コントロール、スタンドアロン、ま

たはダウンロード可能ソフトウェアオブジェクト、などが存在する。実施形態は、API(または、他のソフトウェアオブジェクト)の観点から、ならびに、説明した実施態様の1つまたは複数による、本明細書で開示された態様を実装することを容易にするソフトウェアまたはハードウェアオブジェクトの観点から企図されてもよい。本明細書に記載の様々な実施態様は、完全にハードウェアにおける態様、部分的にハードウェアおよび部分的にソフトウェアにおける態様、ならびにソフトウェアにおける態様を有してもよい。

【０１３９】

「例示的」という語は、本明細書では、例、事例、または例示として役立つことを意味するために使用される。誤解を避けるため、本明細書で開示された主題は、そのような例に限定されない。加えて、「例示的」として本明細書に記載された任意の態様または設計は、必ずしも他の態様または設計よりも好ましいまたは有利であるとして解釈されず、当業者に周知の同等の例示的な構造および技術を排除することを意味しない。さらに、「含む」、「有する」、「含有する」という用語、および他の同様の語が、詳細な説明または特許請求の範囲のいずれかにおいて使用される限り、誤解を避けるために、そのような用語は、任意の追加のまたは他の要素を排除することなく、オープンな転換語として「備える」という用語の同様に包括的であることが意図される。

【０１４０】

上述したように、本明細書に記載の様々な技法は、ハードウェア、もしくはソフトウェア、または、適切な場合には、両方の組合せに関連して実装されてもよい。本明細書で使用する場合、「構成要素」、「システム」、などの用語は、同様に、ハードウェア、ハードウェアおよびソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかのコンピュータ関連のエンティティを指すことが意図される。たとえば、構成要素は、限定はしないが、プロセッサ上で実行されているプロセス、プロセッサ、オブジェクト、実行ファイル、実行のスレッド、プログラム、および/またはコンピュータであってもよい。例示として、コンピュータ上で実行されているアプリケーションとコンピュータの両方は、構成要素であり得る。1つまたは複数の構成要素は、プロセスおよび/または実行のスレッド内に存在してもよく、構成要素は、1つのコンピュータ上に局在化されてもよく、および/または2つ以上のコンピュータ間に分散されてもよい。

【０１４１】

前述のシステムは、いくつかの構成要素の間の相互作用に関して説明されている。そのようなシステムおよび構成要素は、これらの構成要素もしくは指定されたサブ構成要素、指定された構成要素もしくはサブ構成要素のいくつか、および/または追加の構成要素を、上記の様々な順列および組合せに従って含むことができることが理解され得る。サブ構成要素はまた、(階層的な)親構成要素内に含まれるのではなく、他の構成要素に通信可能に結合された構成要素として実装され得る。加えて、1つまたは複数の構成要素は、集合的な機能性を提供する単一の構成要素に組み合わされてもよく、またはいくつかの別個のサブ構成要素に分割されてもよく、管理層などの任意の1つまたは複数の中間層は、統合された機能性を提供するために、そのようなサブ構成要素に通信可能に結合するために提供されてもよいことに留意されたい。本明細書に記載の任意の構成要素はまた、本明細書には具体的に記載されていないが、当業者には一般的に知られている1つまたは複数の他の構成要素と相互作用してもよい。

【０１４２】

上記で説明した例示的なシステムを考慮して、開示された主題に従って実装されてもよい方法論は、様々な図のフローチャートを参照して理解され得る。説明を簡単にする目的のため、方法論は、一連のブロックとして示され、説明されているが、特許請求された主題は、ブロックの順序によって限定されず、いくつかのブロックは、本明細書に示し、記載されたものと異なる順序で、および/または他のブロックと同時に生じてもよいことが理解され、認識されるべきである。非連続または分岐フローがフローチャートを介して示されている場合、同じまたは同様の結果を達成する様々な他の分岐、フローパス、およびブロックの順序が実装されてもよいことが理解され得る。さらに、すべての図示のブロッ

クが、以下で説明する方法論を実装するために必要とされるわけではない可能性がある。

【０１４３】

いくつかの実施態様では、クライアント側の視点が示されているが、誤解を避けるために、対応するサーバの視点が存在し、またはその逆であることが理解されるべきである。同様に、方法が実施される場合、ストレージと、1つまたは複数の構成要素を介してその方法を実施するように構成された少なくとも1つのプロセッサとを有する対応するデバイスが提供され得る。

【０１４４】

様々な実施態様が、様々な図面の好ましい実施態様に関連して説明されているが、他の同様の実施態様が使用されてもよく、または、修正および追加が、同じ機能を実行するための説明した実施態様に対して、そこから逸脱することなくなされ得ることが理解されるべきである。さらに、上記で説明した実施態様の1つまたは複数の態様は、複数の処理チップまたはデバイス内に、またはそれらにわたって実装されてもよく、ストレージは、同様に、複数のデバイスにわたって影響を受けてもよい。したがって、本発明は、任意の単一の実施態様に限定されるべきではない。

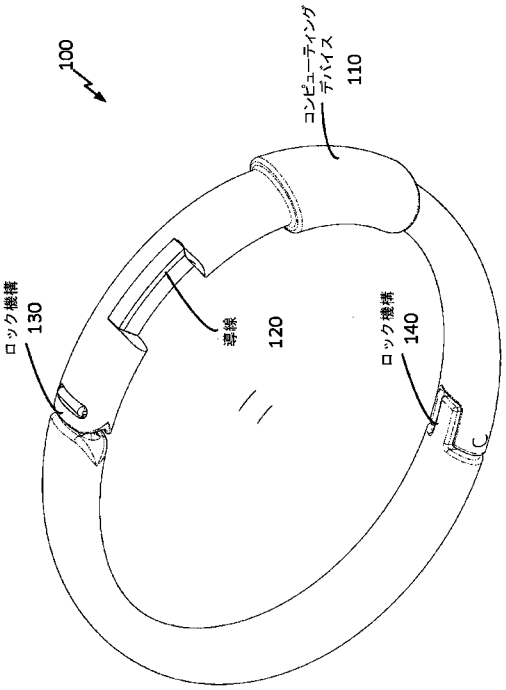
【符号の説明】

【０１４５】

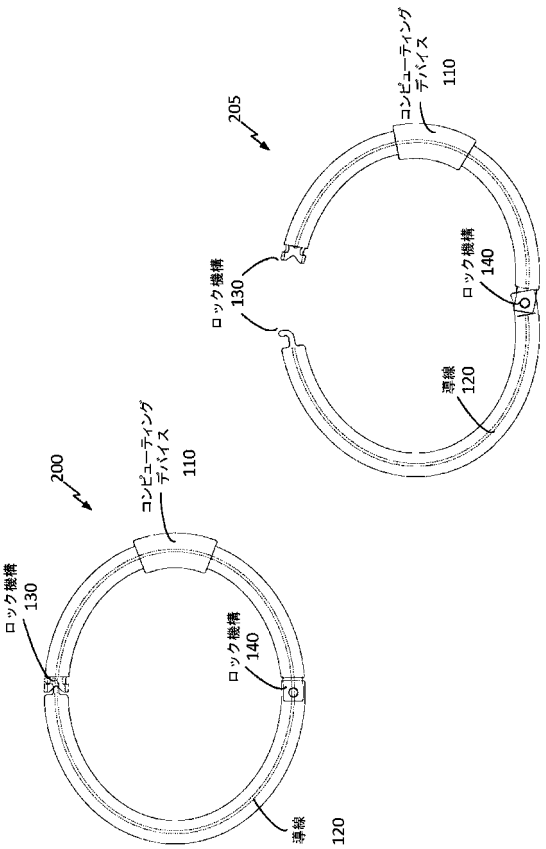
100 ウェアラブルアイデンティティマネージャデバイス
110 コンピューティングデバイス
120 導線
130 第1のロック機構、ロッキング機構
140 第2のロック機構、ロッキング機構
200 ロック構成
205 アンロック構成
300 環境
310 ネットワーク
320 ウェアラブルアイデンティティマネージャデバイス
330 ペアリングデバイス
340 外部デバイス
500 ウェアラブルアイデンティティマネージャデバイス
510 ペアリングデバイス
600 ウェアラブルアイデンティティマネージャデバイス
602 バス
604 プロセッサ
605 メモリ
606 コンピュータ可読媒体
606a 命令、検出器命令
606b 命令、決定命令
608 バスインターフェース
610 トランシーバ、トランシーバ構成要素
612 ユーザインターフェース
614 処理システム
620 回路、検出器回路
630 回路、決定回路
710 関連付けサブ回路
712 関連付け命令
720 関連付け解除サブ回路
722 関連付け解除命令
1010 センササブ回路
1012 センサ命令

1020 ペアリングサブ回路
1022 ペアリング命令
1030 信用証明書マネージャサブ回路
1032 信用証明書マネージャ命令
1040 セキュリティサブ回路
1042 セキュリティ命令
1600 ウェアラブルアイデンティティマネージャデバイス
1610 販売時点タッチスクリーン
1612 スタイラス
1810 コンピューティングオブジェクトまたはデバイス
1812 コンピューティングオブジェクトまたはデバイス
1820 コンピューティングオブジェクトまたはデバイス
1822 コンピューティングオブジェクトまたはデバイス
1824 コンピューティングオブジェクトまたはデバイス
1826 コンピューティングオブジェクトまたはデバイス
1828 コンピューティングオブジェクトまたはデバイス
1830 アプリケーション
1832 アプリケーション
1834 アプリケーション
1836 アプリケーション
1838 アプリケーション
1840 通信ネットワーク、ネットワーク
1900 コンピューティングシステム環境
1910 ハンドヘルドコンピュータ、コンピュータ
1920 処理ユニット
1921 システムバス
1930 システムメモリ
1940 入力デバイス
1950 出力インターフェース
1970 リモートコンピュータ
1971 ネットワーク

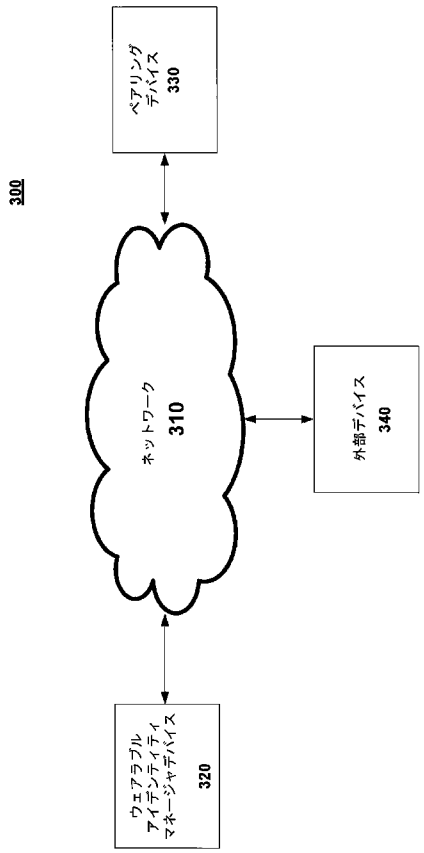
【図１】


100
コンピューティングデバイス 110
ロック機構 130
導線 120
ロック機構 140

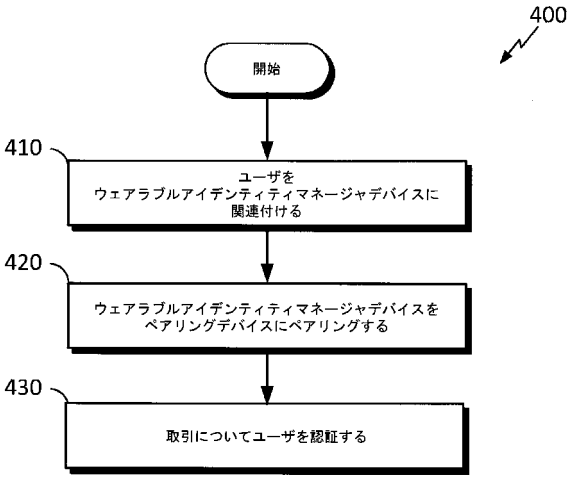
【図２】


205
コンピューティングデバイス 110
ロック機構 130
ロック機構 140
導線 120
200
コンピューティングデバイス 110
ロック機構 130
ロック機構 140
導線 120

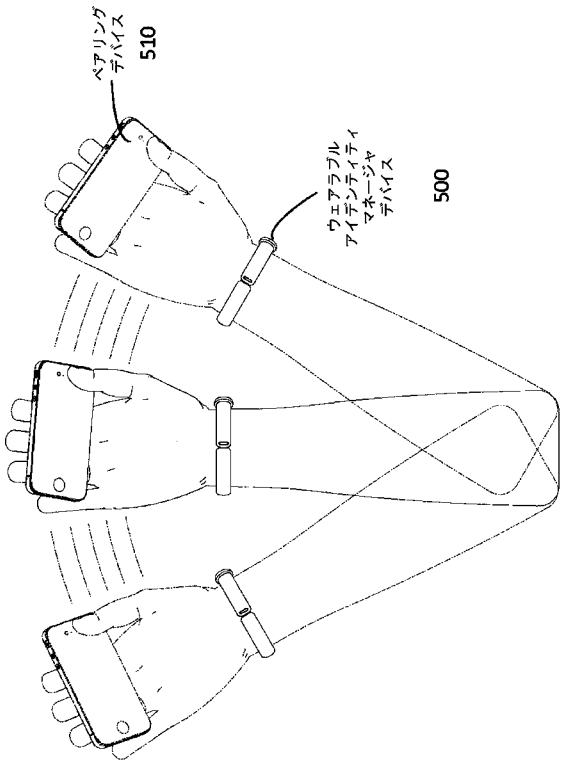
【図３】


300
ペアリングデバイス 330
ネットワーク 310
外部デバイス 340
ウェアラブルアイデンティティマネージャデバイス 320

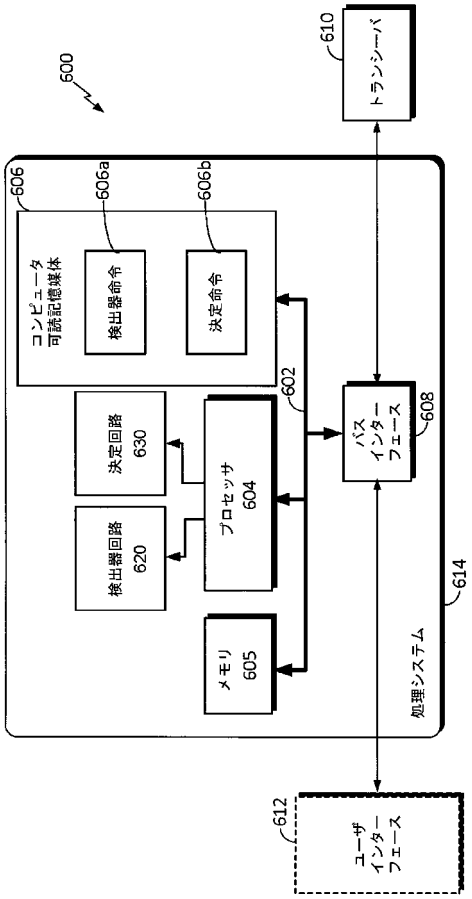
【図４】


400
開始
410
ユーザをウェアラブルアイデンティティマネージャデバイスに関連付ける
420
ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスにペアリングする
430
取引についてユーザを認証する

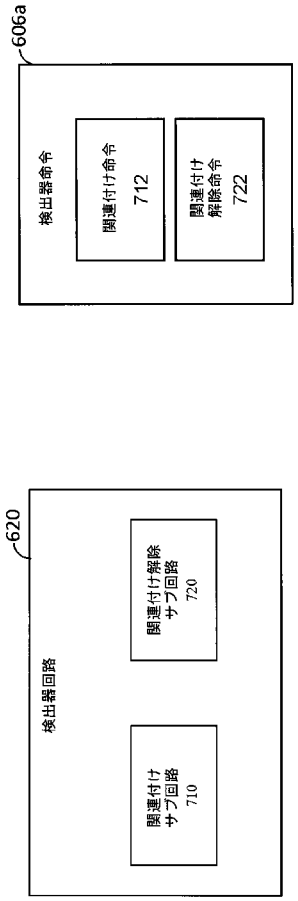
【図５】


ペアリング
デバイス
510
ウェアラブル
アイデンティティ
マネージャ
デバイス
500

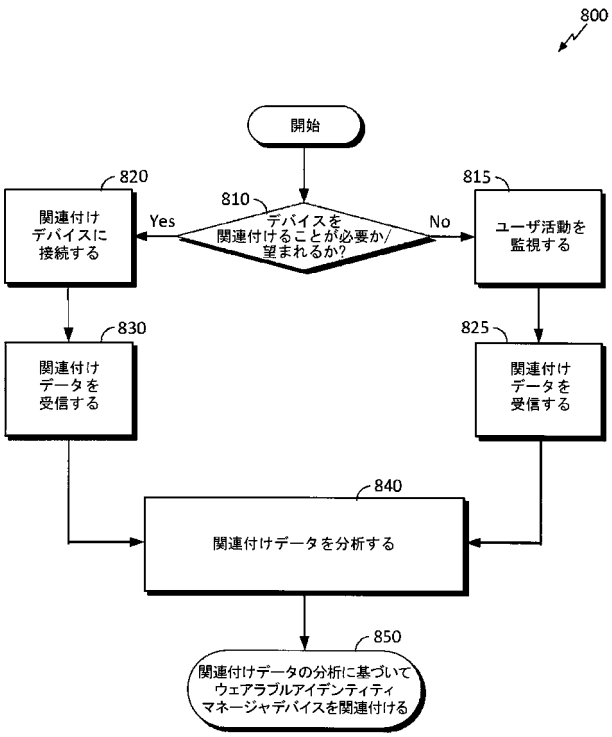
【図６】


600
610
トランシーバ
606
606a
606b
コンピュータ
可読記憶媒体
検出器命令
決定命令
602
決定回路
630
検出器回路
620
プロセッサ
604
バス
インター
フェース
608
メモリ
605
614
処理システム
612
ユーザ
インター
フェース

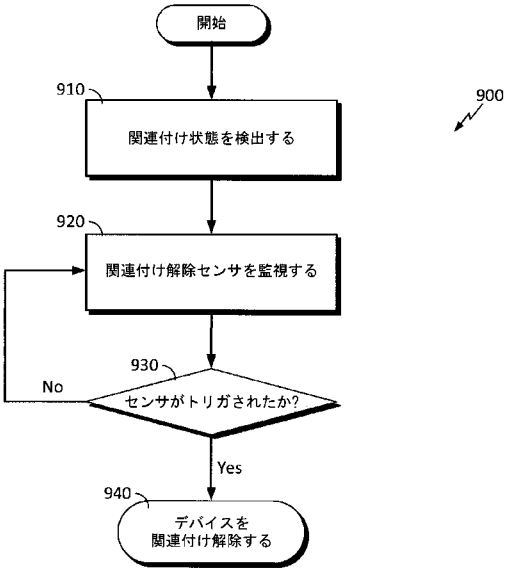
【図７】


606a
検出器命令
関連付け命令
712
関連付け
解除命令
722
620
検出器回路
関連付け解除
サブ回路
720
関連付け
サブ回路
710

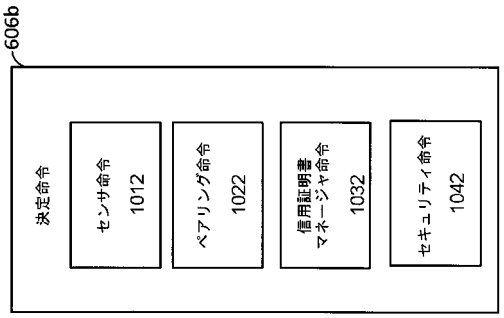
【図８】

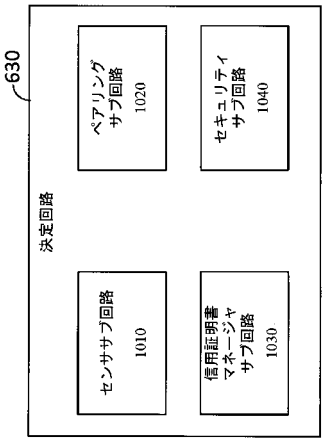

800
開始
820
関連付け
デバイスに
接続する
Yes
810
デバイスを
関連付けることが必要か/
望まれるか?
No
815
ユーザ活動を
監視する
830
関連付け
データを
受信する
825
関連付け
データを
受信する
840
関連付けデータを分析する
850
関連付けデータの分析に基づいて
ウェアラブルアイデンティティ
マネージャデバイスを関連付ける

【図９】

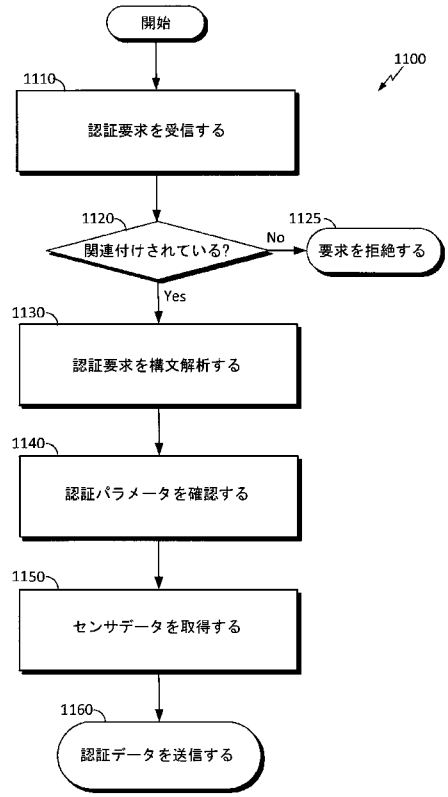


【図１０】

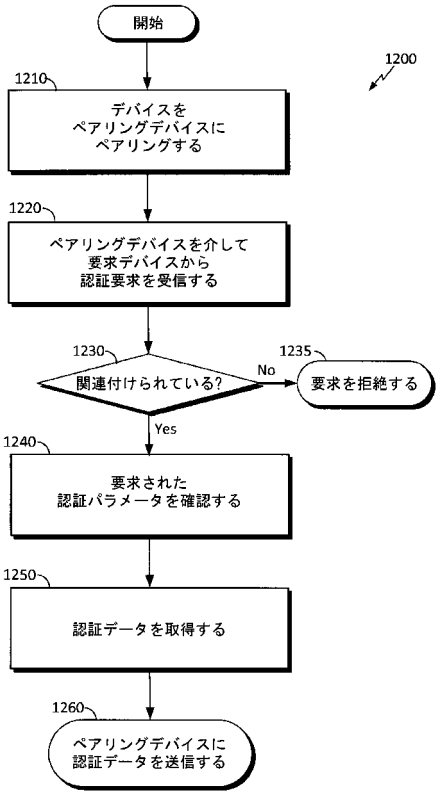




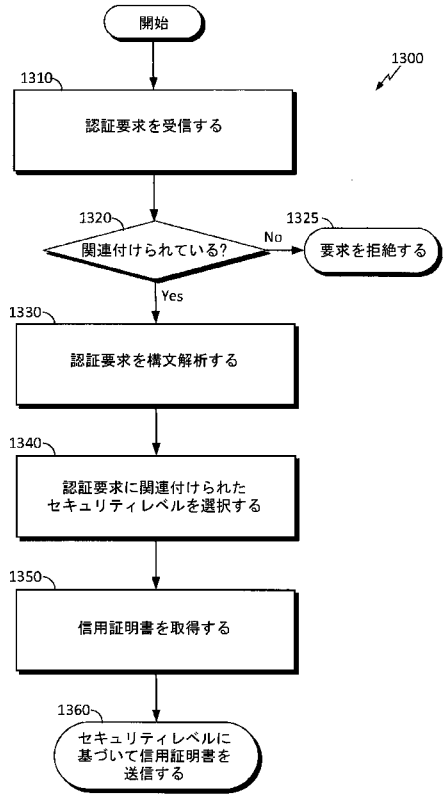
【図１１】



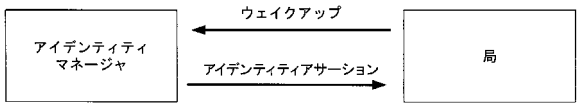
【図１２】



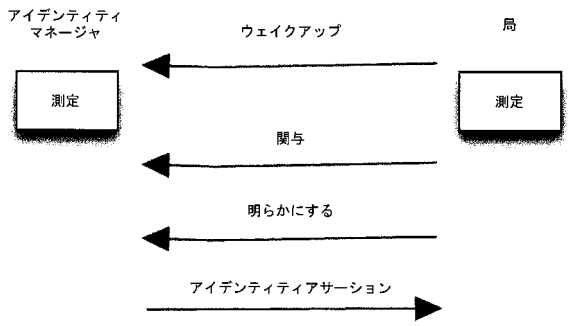
【図１３】



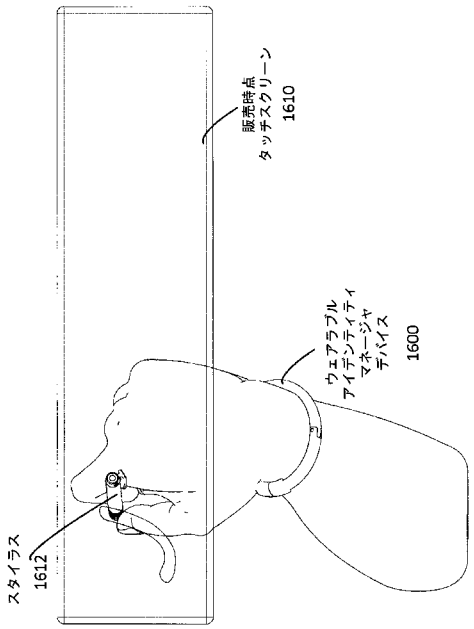
【図１４】



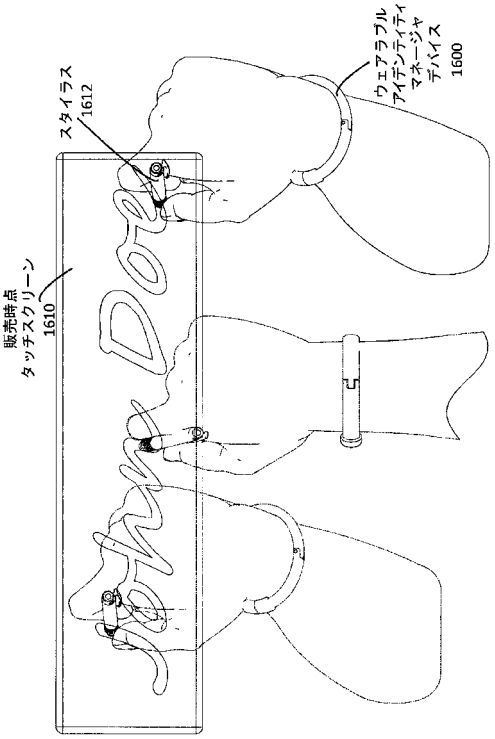
【図１５】



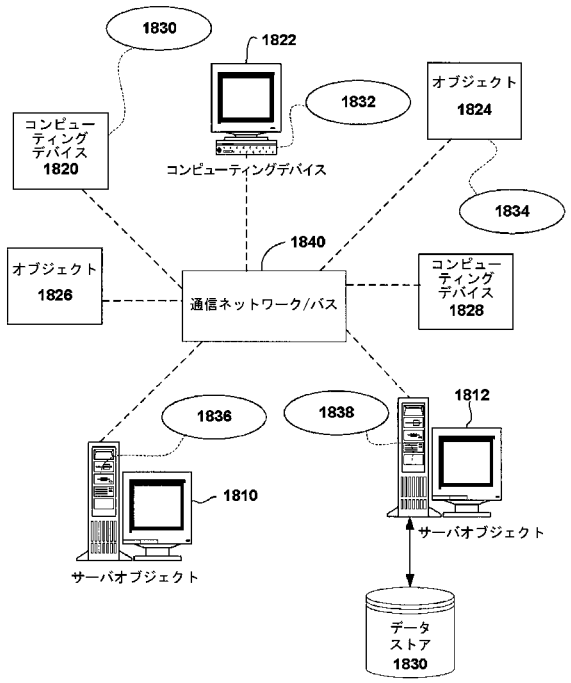
【図１６】



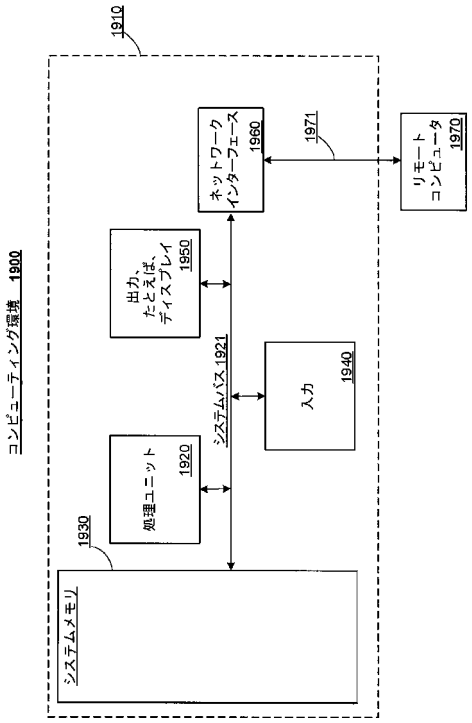
【図１７】



【図１８】



【図１９】



【手続補正書】
【提出日】平成28年10月5日(2016.10.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ウェアラブルアイデンティティマネージャデバイスであって、
メモリと、
前記メモリに通信可能に結合されたプロセッサと
を備え、前記プロセッサが、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づいて、ユーザと前記ウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定することと、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングすることであって、前記ペアリングデバイスが、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスのためのプロキシデバイスとして動作するように構成されている、ことと、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスから前記ペアリングデバイスに認証データを送信することであって、前記認証データが、前記ペアリングデバイスを介する外部デバイスに対するユーザ認証を容易にする、ことと

を行うように構成された、ウェアラブルアイデンティティマネージャデバイス。
【請求項２】
前記プロセッサが、
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視し、収集するようにさらに構成され、前記認証データが、前記収集された動きデータを含む、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項３】
前記プロセッサが、関連付け手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けるように構成され、前記関連付け状態が前記関連付け手順の結果に基づく、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項４】
前記動きデータが、前記ウェアラブルアイデンティティマネージャデバイスによって横断された定義された経路を含む、請求項2に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項５】
前記プロセッサが、ジャイロ、全地球測位システム(GPS)デバイス、タッチ感知センサ、またはマイクロホンのうちの少なくとも1つからセンサデータを取得するようにさらに構成され、前記認証データが前記センサデータをさらに備える、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項６】
前記プロセッサが、留め金センサ、圧力センサ、温度センサ、脈拍センサ、動きセンサ、または伸縮センサのうちの少なくとも1つから取得されたデータに基づいて、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを推論するようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項７】
前記プロセッサが、
認証要求を受信することと、
信用証明書を提供することと、
前記認証要求に基づいて前記信用証明書を送信することと
を行うようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項８】
前記プロセッサが、
認証要求を受信することと、
前記認証要求に関連付けられたセキュリティレベルを確認することと、
前記セキュリティレベルに基づいて前記認証データを送信することと
を行うようにさらに構成された、請求項1に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項９】
1つまたは複数の命令が記憶されている非一時的機械可読記憶媒体であって、前記1つまたは複数の命令が、少なくとも1つのプロセッサによって実行されると、前記少なくとも1つのプロセッサに、
ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を確認することであって、前記関連付け状態が、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づいて確認される、ことと、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングすることであって、前記ペアリングデバイスが、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデン

ティティマネージャデバイスのためのプロキシデバイスとして動作するように構成されている、ことと、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスから前記ペアリングデバイスに認証データを送信することであって、前記認証データが、前記ペアリングデバイスを介する外部デバイスに対するユーザ認証を容易にする、ことと
を行わせる、非一時的機械可読記憶媒体。
【請求項１０】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視し、収集させる命令をさらに含み、前記認証データが、前記収集された動きデータを含む、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１１】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、認証手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けさせる命令をさらに備え、前記関連付け状態が前記認証手順の結果に基づく、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１２】
前記関連付け手順が、ローカルに記憶されたパスワードを、関連付けデバイスから受信されたパスワードと一致させることを含む、請求項11に記載の非一時的機械可読記憶媒体。
【請求項１３】
前記関連付け手順が、前記ウェアラブルアイデンティティマネージャデバイスの関連付け運動を、関連付けデバイスの運動に対応する受信されたデータと一致させること含む、請求項11に記載の非一時的機械可読記憶媒体。
【請求項１４】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
認証要求を受信することと、
ユーザアクション、または前記認証要求から推定された実行コンテキストのうちの少なくとも1つに基づいて、信用証明書を提供することと
を行わせる命令をさらに備える、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１５】
前記1つまたは複数の命令が、前記少なくとも1つのプロセッサに、
認証要求を受信することと、
前記認証要求に関連付けられたセキュリティレベルを確認することと、
前記セキュリティレベルに基づいて前記認証データを提供することと
を行わせる命令をさらに備える、請求項9に記載の非一時的機械可読記憶媒体。
【請求項１６】
前記セキュリティレベルが、ユーザの好みの設定、実行コンテキスト、または1つもしくは過去の実行コンテキストのうちの少なくとも1つに従って確認される、請求項15に記載の非一時的機械可読記憶媒体。
【請求項１７】
ワイヤレス通信を容易にする方法であって、
ユーザとウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するステップであって、前記決定するステップが、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを決定するステップを含む、ステップと、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするステップと、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスから前記ペアリングデバ

イスに認証データを送信するステップであって、前記認証データが、前記ペアリングデバイスを介する外部デバイスに対するユーザ認証を容易にする、ステップと
を含む方法。
【請求項１８】
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視するステップをさらに含み、前記認証データが前記動きデータを含む、請求項17に記載の方法。
【請求項１９】
関連付け手順を介して前記ウェアラブルアイデンティティマネージャデバイスを前記ユーザに関連付けるステップをさらに含み、前記関連付け状態が、前記関連付け手順の結果に基づく、請求項17に記載の方法。
【請求項２０】
前記関連付け手順が、ローカルに保存されたパスワードを、関連付けデバイスから受信されたパスワードと一致させるステップを含む、請求項19に記載の方法。
【請求項２１】
前記関連付け手順が、前記ウェアラブルアイデンティティマネージャデバイスの関連付け運動を、関連付けデバイスの運動に対応する受信されたデータと一致させるステップを含む、請求項19に記載の方法。
【請求項２２】
前記ユーザに関連付けられた信用証明書を記憶するステップと、
認証要求に応じて前記ペアリングデバイスに前記信用証明書を提供するステップと
をさらに含む、請求項17に記載の方法。
【請求項２３】
前記認証要求に関連付けられたセキュリティレベルを確認するステップと、
前記セキュリティレベルに基づいて、前記ペアリングデバイスに送信される信用証明書の量を制限するステップと
をさらに含む、請求項22に記載の方法。
【請求項２４】
ウェアラブルアイデンティティマネージャデバイスであって、
ユーザと前記ウェアラブルアイデンティティマネージャデバイスとの間の関連付け状態を決定するための手段であって、前記関連付け状態が、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに部分的に基づく、手段と、
前記ウェアラブルアイデンティティマネージャデバイスをペアリングデバイスとペアリングするための手段であって、前記ペアリングデバイスが、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスのためのプロキシデバイスとして動作するように構成されている、手段と、
前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかに基づいて、前記ウェアラブルアイデンティティマネージャデバイスから前記ペアリングデバイスに認証データを送信するための手段であって、前記認証データが、前記ペアリングデバイスを介する外部デバイスに対するユーザ認証を容易にする、手段と
を備えるウェアラブルアイデンティティマネージャデバイス。
【請求項２５】
前記ウェアラブルアイデンティティマネージャデバイスの運動に関連付けられた動きデータを監視する手段をさらに備え、前記認証データが前記動きデータを含む、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２６】
前記動きデータが、前記ウェアラブルアイデンティティマネージャデバイスによって横断された定義された経路を含む、請求項25に記載のウェアラブルアイデンティティマネージャデバイス。

【請求項２７】
前記監視するための手段が、ジャイロ、タッチ感知センサ、またはマイクロホンのうちの少なくとも1つからセンサデータを受信するための手段をさらに備え、前記認証データが、前記センサデータをさらに含む、請求項25に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２８】
前記決定するための手段が、留め金センサ、圧力センサ、温度センサ、または伸縮センサのうちの少なくとも1つから受信されたデータに基づいて、前記ウェアラブルアイデンティティマネージャデバイスが装着されているかどうかを推論するための手段をさらに備える、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項２９】
認証要求を受信するための手段と、
前記認証要求に関連付けられたセキュリティレベルを確認するための手段と
をさらに備え、前記送信するための手段が、前記セキュリティレベルに基づいて前記ペアリングデバイスに前記認証データを送信するための手段を備える、請求項24に記載のウェアラブルアイデンティティマネージャデバイス。
【請求項３０】
前記確認するための手段が、複数の可能なセキュリティレベルから前記セキュリティレベルを選択するための手段を備える、請求項29に記載のウェアラブルアイデンティティマネージャデバイス。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/023719

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/35 H04W12/06 A61B5/00 G06F1/16 G06F21/32
G06F3/0346
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
G06F H04W A61B

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, 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 Y	US 2003/025603 A1 (SMITH EDWIN DEREK [US]) 6 February 2003 (2003-02-06) the whole document	17,24 1-16, 18-23, 25-30

Y	RENE MAYRHOFER ET AL: "Shake Well Before Use: Authentication Based on Accelerometer Data", 13 May 2007 (2007-05-13), PERVASIVE COMPUTING; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 144 - 161, XP019079249, ISBN: 978-3-540-72036-2 the whole document	1-16, 18-23, 25-30

	-/--	

[X] Further documents are listed in the continuation of Box C. [X] 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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 June 2015	16/06/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/023719

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2013/079609 A1 (GEMALTO SA [FR]) 6 June 2013 (2013-06-06) page 7, line 5 - line 20 page 9, line 23 - line 30 -----	13,21
A	ALFRED KOBSA ET AL: "Serial hook-ups", PROCEEDINGS OF THE 5TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY, SOUPS '09, 1 January 2009 (2009-01-01), page 1, XP055194285, New York, New York, USA DOI: 10.1145/1572532.1572546 ISBN: 978-1-60-558736-3 the whole document -----	1-30

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/023719

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003025603 A1	06-02-2003	US 2003025603 A1	06-02-2003
		WO 03012665 A1	13-02-2003
WO 2013079609 A1	06-06-2013	CN 104081440 A	01-10-2014
		EP 2600319 A1	05-06-2013
		EP 2791916 A1	22-10-2014
		JP 2015506131 A	26-02-2015
		KR 20140098837 A	08-08-2014
		US 2014325614 A1	30-10-2014
		WO 2013079609 A1	06-06-2013

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.		F I			テーマコード（参考）
Ａ６１Ｂ　5/02	*(2006.01)*	Ａ６１Ｂ	5/10	３４０	
		Ａ６１Ｂ	5/02	Ｃ	

(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

Ｆターム(参考) 5E555 AA11 AA53 BA04 BB38 BC16 CA41 CA44 CB66 FA00
5J104 AA07 KA01 KA16 NA02 NA37 NA38 NA43 PA01 PA07 PA10