

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 6 部門第 3 区分

【発行日】平成30年4月26日 (2018.4.26)

【公表番号】特表2017-520033(P2017-520033A)

【公表日】平成29年7月20日 (2017.7.20)

【年通号数】公開・登録公報2017-027

【出願番号】特願2016-558389(P2016-558389)

【国際特許分類】

G 0 6 F 21/35 (2013.01)

H 0 4 L 9/32 (2006.01)

G 0 6 F 3/01 (2006.01)

A 6 1 B 5/11 (2006.01)

A 6 1 B 5/117 (2016.01)

A 6 1 B 5/02 (2006.01)

【 F I 】

G 0 6 F 21/35

H 0 4 L 9/00 6 7 3 D

G 0 6 F 3/01 5 1 4

A 6 1 B 5/10 3 1 0 A

A 6 1 B 5/10 3 1 0 G

A 6 1 B 5/10 3 4 0

A 6 1 B 5/02 C

【手続補正書】

【提出日】平成30年3月15日 (2018.3.15)

【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】

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、外部デバイス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 2】

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、収集するステップであって、前記認証データが、前記収集された動きデータを含むステップをさらに含む、請求項1に記載の方法。

【請求項 3】

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であって、前記関連付け状態が前記関連付け手順の結果に基づくステップをさらに含む、請求項1に記載の方法。

【請求項4】

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3に記載の方法。

【請求項5】

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3に記載の方法。

【請求項6】

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1に記載の方法。

【請求項7】

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、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1に記載の方法。

【請求項8】

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基づき、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、外部デバイス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9】

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み、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8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10】

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ための手段をさらに備え、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8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11】

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9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 1 2】**

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8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 1 3】**

認証要求を受信し、信用証明書を提供し、前記認証要求に基づいて前記信用証明書を送信するための手段をさらに備える、請求項8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 1 4】**

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、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8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 1 5】**

少なくとも1つのプロセッサにより実行されたとき、前記少なくとも1つのプロセッサに請求項1乃至7の何れか1項に記載の方法を実施させる1つまたは複数の命令を記憶した、機械読取可能記憶媒体。