【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７部門第３区分
【発行日】平成31年4月25日(2019.4.25)

【公表番号】特表2018-515011(P2018-515011A)
【公表日】平成30年6月7日(2018.6.7)
【年通号数】公開・登録公報2018-021
【出願番号】特願2017-551677(P2017-551677)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/40　(2012.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/44　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｑ　20/40　３００
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/44

【手続補正書】
【提出日】平成31年3月15日(2019.3.15)
【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】
ユーザのユーザ識別情報と、ウェアラブルデバイス識別情報と、サーバ認証キーとの対応関係を格納するサーバに適用される、前記ユーザを認証するための方法であって：
端末を通じて前記ユーザにより送信された認証要求を受信するステップであって、前記認証要求は、前記ユーザの前記ユーザ識別情報及び／又は前記ウェアラブルデバイス識別情報をともなう、ステップ（２１０）と；
ダウンリンク認証情報を取得し、前記ダウンリンク認証情報と前記ユーザの前記ウェアラブルデバイス識別情報とをともなう検出指令を前記端末に対して発行するステップ（２２０）と；
前記端末によって返信され、アップリンク認証情報をともなう検出承認を受信するステップであって、前記アップリンク認証情報は、デバイス認証キーと前記ダウンリンク認証情報とに応じて、検出指令で指定されたウェアラブルデバイスによって生成され、前記デバイス認証キーは前記サーバ認証キーと同一又はそれに対応する、ステップ（２３０）と；
前記ユーザの前記サーバ認証キーを用いて前記ダウンリンク認証情報を前記アップリンク認証情報とマッチングさせるステップであって、前記マッチングに成功した場合に前記ユーザが前記認証を得る、ステップ（２４０）と；を備える、
ユーザを認証するための方法。
【請求項２】
前記サーバは、前記ユーザのユーザパブリックキーを更に格納し、前記ユーザパブリックキーは、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、前記ユーザパブリックキーと前記端末に格納されるユーザプライベートキーとは一対のキーであり、

前記端末によって返信される前記検出承認は、前記端末に格納される前記ユーザプライベートキーを用いて署名され、
前記方法は、前記ユーザの前記ユーザパブリックキーに応じて前記端末の前記検出承認に対して署名検証を遂行するステップを更に備え、
前記検証に失敗した場合、前記ユーザへの前記認証は失敗となる、
請求項１に記載の方法。
【請求項３】
前記サーバは端末識別情報を更に格納し、前記端末識別情報は前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、
前記認証要求は、前記認証要求を送信するための端末識別情報を更に含み、
前記方法は、前記認証要求の中の前記ユーザ識別情報又は前記ウェアラブルデバイス識別情報に対応する前記端末識別情報が、前記認証要求を送信するための前記端末識別情報と異なる場合、前記ユーザへの前記認証は失敗となるステップを更に備える、
請求項１に記載の方法。
【請求項４】
前記サーバがサーバプライベートキーを更に格納し、前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、
前記方法が、前記サーバプライベートキーを用いて前記検出指令に署名するステップを更に備える、
請求項１乃至３のいずれか一項に記載の方法。
【請求項５】
前記検出指令及び前記検出承認が、前記サーバと前記端末との間の暗号化チャンネルを通じて伝送される、
請求項１乃至３のいずれか一項に記載の方法。
【請求項６】
前記サーバは支払いサーバであり、前記認証要求が支払い要求であり、
前記方法が、前記認証を得たユーザに支払いサービスを提供するステップを更に備える、
請求項１乃至３のいずれか一項に記載の方法。
【請求項７】
端末を通じてユーザによって送信されるウェアラブルデバイス登録要求を受信するステップであって、前記登録要求は、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、ステップ（４１０）と；
前記ユーザのサーバ認証キーと、デバイス認証キーとを取得し、前記デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう書き込み指令を前記端末に対して発行するステップ（４２０）と；
前記端末によって返信される書き込み承認を受信し、前記書き込み指令で指定されたウェアラブルデバイスへの前記デバイス認証キーの格納に成功したことを前記書き込み承認が示す場合、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納するステップ（４３０）と；を有する前記ウェアラブルデバイスを登録するステップを更に備える、
請求項１乃至６のいずれか一項に記載の方法。
【請求項８】
前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納する前記ステップが：
パスワード承認要求を前記端末に対して発行するステップと；
前記端末からユーザパスワードをともなうパスワード承認を受信し、前記ユーザパスワードが正しい場合に前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの前記対応関係を格納するステップと；を備える、
請求項７に記載の方法。

【請求項９】
前記端末によって返信される前記書き込み承認が、前記端末によって生成されるユーザパブリックキーを更に含み、
前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納する前記ステップが、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーと、前記ユーザパブリックキーとの対応関係を格納するステップを更に備える、
請求項７又は８に記載の方法。
【請求項１０】
前記サーバが、サーバプライベートキーとサーバパブリックキーとを更に格納し、
前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、前記サーバパブリックキーと前記端末に格納される端末プライベートキーとは一対のキーであり、
前記方法が、前記サーバプライベートキーを用いて前記書き込み指令に署名するステップを更に備え、
前記方法が、前記サーバパブリックキーを用いて前記端末の前記書き込み承認に対して署名検証を遂行し、前記検証が失敗した場合には前記登録要求を拒絶するステップを更に備える、
請求項７又は８に記載の方法。
【請求項１１】
ユーザのウェアラブルデバイスに接続される端末に適用される、前記ユーザを認証するための方法であって：
前記ユーザの操作に応じて認証要求をサーバへ送信するステップであって、前記認証要求は、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、ステップ（３１０）と；
前記サーバの検出指令を受信するステップであって、前記検出指令は、ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とをともなう、ステップ（３２０）と；
前記ダウンリンク認証情報を、前記検出指令で指定されたウェアラブルデバイスへ送信し、前記ウェアラブルデバイスによって返信されるアップリンク認証情報を受信するステップであって、前記アップリンク認証情報は、格納されたデバイス認証キーと、前記ダウンリンク認証情報とに応じて前記ウェアラブルデバイスによって生成され、前記デバイス認証キーは、前記サーバに格納されるサーバ認証キーと同一又はそれに対応する、ステップ（３３０）と；
前記アップリンク認証情報をともなう検出承認を前記サーバへ送信するステップ（３４０）と；
前記アップリンク認証情報と、前記ダウンリンク認証情報と、前記サーバ認証キーとに応じて前記サーバによって判定されるユーザ認証結果を受信するステップ（３５０）と；
を備える、
ユーザを認証するための方法。
【請求項１２】
前記端末が前記ユーザのユーザプライベートキーを格納し、前記ユーザプライベートキーと前記サーバに格納されるユーザパブリックキーとは一対のキーであり、
前記方法が、前記ユーザの前記ユーザプライベートキーを用いて前記検出承認に署名するステップ更に備える、
請求項１１に記載の方法。
【請求項１３】
前記端末が端末パブリックキーを格納し、前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、
前記サーバによって発行される前記検出指令は、前記サーバプライベートキーを用いて署名され、

前記方法が、前記端末パブリックキーに応じて前記サーバの前記検出指令に対して署名検証を遂行し、前記検証に失敗した場合は前記検出指令を拒絶するステップを更に備える、
請求項１１又は１２に記載の方法。
【請求項１４】
前記認証要求が支払い要求であり、前記ユーザ認証結果が前記認証の成功であった後に、前記端末が前記ユーザの支払い操作を完了する、
請求項１１又は１２に記載の方法。
【請求項１５】
ユーザの操作に応じて、ウェアラブルデバイス登録要求をサーバへ送信するステップであって、前記登録要求は、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、ステップ（５１０）と；
前記サーバの書き込み指令を受信するステップであって、前記書き込み指令は、デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう、ステップ（５２０）と；
前記書き込み指令で指定されたウェアラブルデバイス上に前記デバイス認証キーを書き込む操作を実行するステップ（５３０）と；
書き込み承認を前記サーバへ送信するステップであって、前記書き込み承認は、前記デバイス認証キーの書き込みに成功したか否かを示すメッセージをともなう、ステップ（５４０）と；を備える、前記ウェアラブルデバイスを登録するステップを更に備える、
請求項１１乃至１４のいずれか一項に記載の方法。
【請求項１６】
前記書き込み承認が前記サーバへ送信された後に、前記サーバのパスワード確認要求を受信し、前記ユーザによって入力されたユーザパスワードをともなうパスワード確認承認を前記サーバへ返信するステップを更に備える、
請求項１５に記載の方法。
【請求項１７】
前記方法が、前記デバイス認証キーを書き込む前記操作に成功した後に、前記ユーザのユーザプライベートキーとユーザパブリックキーとを生成し、前記ユーザプライベートキーを格納するステップを更に備え、
前記書き込み承認が、前記ユーザの前記ユーザパブリックキーを更にともなう、
請求項１５又は１６に記載の方法。
【請求項１８】
前記端末が、端末パブリックキーと端末プライベートキーとを格納し、
前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、
前記端末プライベートキーと前記サーバに格納されるサーバパブリックキーとは一対のキーであり、
前記方法が、前記端末パブリックキーを用いて前記サーバの前記書き込み指令に対して署名検証を遂行し、前記検証に失敗した場合には前記書き込み指令を拒絶するステップを更に備え、
前記方法が、前記端末プライベートキーを用いて前記書き込み承認に署名するステップを更に備える、
請求項１５又は１６に記載の方法。
【請求項１９】
前記ユーザのユーザ識別情報と、ウェアラブルデバイス識別情報と、サーバ認証キーとの対応関係を格納するサーバに適用される、前記ユーザを認証しウェアラブルデバイスを登録するための装置であって：
請求項１乃至１０のいずれか一項に記載の方法を実行するように構成された複数のユニットを備える、

前記ユーザを認証しウェアラブルデバイスを登録するための装置。
【請求項２０】
ユーザのウェアラブルデバイスに接続される端末に適用される、前記ユーザを認証しウェアラブルデバイスを登録するための装置であって：
請求項１１乃至１８のいずれか一項に記載の方法を実行するように構成された複数のユニットを備える、
ユーザを認証しウェアラブルデバイスを登録するための装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０１１５
【補正方法】変更
【補正の内容】
【０１１５】
当業者は、本願の実施の形態を、方法、システム、コンピュータプログラム製品として提供できることを理解すべきである。したがって、本願の実施の形態は、完全なハードウェアの実施の形態、完全なソフトウェアの実施の形態、又はソフトウェアとハードウェアの組み合わせの実施の形態の形態で実施できる。更に、本願は、１つ以上のコンピュータで使用可能な記憶媒体（磁気ディスクメモリ、ＣＤ－ＲＯＭ、光学メモリなどを非限定的に含む）上で実施できるコンピュータプログラム製品（コンピュータで使用可能なプログラムコードを含む）の形態を採ることができる。
［第１の局面］
ユーザのユーザ識別情報と、ウェアラブルデバイス識別情報と、サーバ認証キーとの対応関係を格納するサーバに適用される、前記ユーザを認証するための方法であって：
端末を通じて前記ユーザにより送信された認証要求を受信するステップであって、前記認証要求は、前記ユーザの前記ユーザ識別情報及び／又は前記ウェアラブルデバイス識別情報をともなう、ステップと；
ダウンリンク認証情報を取得し、前記ダウンリンク認証情報と前記ユーザの前記ウェアラブルデバイス識別情報とをともなう検出指令を前記端末に対して発行するステップと；
前記端末によって返信され、アップリンク認証情報をともなう検出承認を受信するステップであって、前記アップリンク認証情報は、デバイス認証キーと前記ダウンリンク認証情報とに応じて、検出指令で指定されたウェアラブルデバイスによって生成され、前記デバイス認証キーは前記サーバ認証キーと同一又はそれに対応する、ステップと；
前記ユーザの前記サーバ認証キーを用いて前記ダウンリンク認証情報を前記アップリンク認証情報とマッチングさせるステップと；を備え、
前記マッチングに成功した場合に前記ユーザが前記認証を得る、
上記のステップを備える、ユーザを認証するための方法。
［第２の局面］
前記サーバは、前記ユーザのユーザパブリックキーを更に格納し、前記ユーザパブリックキーは、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、前記ユーザパブリックキーと前記端末に格納されるユーザプライベートキーとは一対のキーであり、
前記端末によって返信される前記検出承認は、前記端末に格納される前記ユーザプライベートキーを用いて署名され、
前記方法は、前記ユーザの前記ユーザパブリックキーに応じて前記端末の前記検出承認に対して署名検証を遂行ステップを更に備え、
前記検証に失敗した場合、前記ユーザへの前記認証は失敗となる、
第１の局面に記載の方法。
［第３の局面］
前記サーバは端末識別情報を更に格納し、前記端末識別情報は前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、

前記認証要求は、前記認証要求を送信するための端末識別情報を更に含み、
前記方法は、前記認証要求の中の前記ユーザ識別情報又は前記ウェアラブルデバイス識別情報に対応する前記端末識別情報が、前記認証要求を送信するための前記端末識別情報と異なる場合、前記ユーザへの前記認証は失敗となるステップを更に備える、
第１の局面に記載の方法。
［第４の局面］
前記サーバがサーバプライベートキーを更に格納し、前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、
前記方法が、前記サーバプライベートキーを用いて前記検出指令に署名するステップを更に備える、
第１の局面乃至第３の局面のいずれか一項に記載の方法。
［第５の局面］
前記検出指令及び前記検出承認が、前記サーバと前記端末との間の暗号化チャンネルを通じて伝送される、
第１の局面乃至第３の局面のいずれか一項に記載の方法。
［第６の局面］
前記サーバは支払いサーバであり、前記認証要求が支払い要求であり、
前記方法が、前記認証を得たユーザに支払いサービスを提供するステップを更に備える、
第１の局面乃至第３の局面のいずれか一項に記載の方法。
［第７の局面］
ユーザのウェアラブルデバイスに接続される端末に適用される、前記ユーザを認証するための方法であって：
前記ユーザの操作に応じて認証要求をサーバへ送信するステップであって、前記認証要求は、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、ステップと；
前記サーバの検出指令を受信するステップであって、前記検出指令は、ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とをともなう、ステップと；
前記ダウンリンク認証情報を、前記検出指令で指定されたウェアラブルデバイスへ送信し、前記ウェアラブルデバイスによって返信されるアップリンク認証情報を受信するステップであって、前記アップリンク認証情報は、格納されたデバイス認証キーと、前記ダウンリンク認証情報とに応じて前記ウェアラブルデバイスによって生成され、前記デバイス認証キーは、前記サーバに格納されるサーバ認証キーと同一又はそれに対応する、ステップと；
前記アップリンク認証情報をともなう検出承認を前記サーバへ送信するステップと；
前記アップリンク認証情報と、前記ダウンリンク認証情報と、前記サーバ認証キーとに応じて前記サーバによって判定されるユーザ認証結果を受信するステップと；を備える、
ユーザを認証するための方法。
［第８の局面］
前記端末が前記ユーザのユーザプライベートキーを格納し、前記ユーザプライベートキーと前記サーバに格納されるユーザパブリックキーとは一対のキーであり、
前記方法が、前記ユーザの前記ユーザプライベートキーを用いて前記検出承認に署名するステップ更に備える、
第７の局面に記載の方法。
［第９の局面］
前記端末が端末パブリックキーを格納し、前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、
前記サーバによって発行される前記検出指令は、前記サーバプライベートキーを用いて署名され、
前記方法が、前記端末パブリックキーに応じて前記サーバの前記検出指令に対して署名

検証を遂行し、前記検証に失敗した場合は前記検出指令を拒絶するステップを更に備える、
第７の局面又は第８の局面に記載の方法。
［第１０の局面］
前記認証要求が支払い要求であり、前記ユーザ認証結果が前記認証の成功であった後に、前記端末が前記ユーザの支払い操作を完了する、
第７の局面又は第８の局面に記載の方法。
［第１１の局面］
サーバに適用される、ウェアラブルデバイスを登録するための方法であって：
端末を通じてユーザによって送信されるウェアラブルデバイス登録要求を受信するステップであって、前記登録要求は、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、ステップと；
前記ユーザのサーバ認証キーと、デバイス認証キーとを取得し、前記デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう書き込み指令を前記端末に対して発行するステップと；
前記端末によって返信される書き込み承認を受信し、前記書き込み指令で指定されたウェアラブルデバイスへの前記デバイス認証キーの格納に成功したことを前記書き込み承認が示す場合、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納するステップと；を備える、
ウェアラブルデバイスを登録するための方法。
［第１２の局面］
前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納する前記ステップが：
パスワード承認要求を前記端末に対して発行するステップと；
前記端末からユーザパスワードをともなうパスワード承認を受信し、前記ユーザパスワードが正しい場合に前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの前記対応関係を格納するステップと；を備える、
第１１の局面に記載の方法。
［第１３の局面］
前記端末によって返信される前記書き込み承認が、前記端末によって生成されるユーザパブリックキーを更に含み、
前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納する前記ステップが、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーと、前記ユーザパブリックキーとの対応関係を格納するステップを更に備える、
第１１の局面又は第１２の局面に記載の方法。
［第１４の局面］
前記サーバが、サーバプライベートキーとサーバパブリックキーとを更に格納し、
前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、前記サーバパブリックキーと前記端末に格納される端末プライベートキーとは一対のキーであり、
前記方法が、前記サーバプライベートキーを用いて前記書き込み指令に署名するステップを更に備え、
前記方法が、前記サーバパブリックキーを用いて前記端末の前記書き込み承認に対して署名検証を遂行し、前記検証が失敗した場合には前記登録要求を拒絶するステップを更に備える、
第１１の局面又は第１２の局面に記載の方法。
［第１５の局面］
端末に適用される、ウェアラブルデバイスを登録するための方法であって：
ユーザの操作に応じて、ウェアラブルデバイス登録要求をサーバへ送信するステップで

あって、前記登録要求は、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、ステップと；
前記サーバの書き込み指令を受信するステップであって、前記書き込み指令は、デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう、ステップと；
前記書き込み指令で指定されたウェアラブルデバイス上に前記デバイス認証キーを書き込む操作を実行するステップと；
書き込み承認を前記サーバへ送信するステップであって、前記書き込み承認は、前記デバイス認証キーの書き込みに成功したか否かを示すメッセージをともなう、ステップと；
を備える、
ウェアラブルデバイスを登録するための方法。
［第１６の局面］
前記書き込み承認が前記サーバへ送信された後に、前記サーバのパスワード確認要求を受信し、前記ユーザによって入力されたユーザパスワードをともなうパスワード確認承認を前記サーバへ返信するステップを更に備える、
第１５の局面に記載の方法。
［第１７の局面］
前記方法が、前記デバイス認証キーを書き込む前記操作に成功した後に、前記ユーザのユーザプライベートキーとユーザパブリックキーとを生成し、前記ユーザプライベートキーを格納するステップを更に備え、
前記書き込み承認が、前記ユーザの前記ユーザパブリックキーを更にともなう、
第１５の局面又は第１６の局面に記載の方法。
［第１８の局面］
前記端末が、端末パブリックキーと端末プライベートキーとを格納し、
前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、
前記端末プライベートキーと前記サーバに格納されるサーバパブリックキーとは一対のキーであり、
前記方法が、前記端末パブリックキーを用いて前記サーバの前記書き込み指令に対して署名検証を遂行し、前記検証に失敗した場合には前記書き込み指令を拒絶するステップを更に備え、
前記方法が、前記端末プライベートキーを用いて前記書き込み承認に署名するステップを更に備える、
第１５の局面又は第１６の局面に記載の方法。
［第１９の局面］
ユーザのユーザ識別情報と、ウェアラブルデバイス識別情報と、サーバ認証キーとの対応関係を格納するサーバに適用される、前記ユーザを認証するための装置であって：
端末を通じて前記ユーザにより送信される認証要求を受信するように構成された認証要求受信ユニットであって、前記認証要求が、前記ユーザの前記ユーザ識別情報及び／又は前記ウェアラブルデバイス識別情報をともなう、認証要求受信ユニットと；
ダウンリンク認証情報を取得し、前記ダウンリンク認証情報と前記ユーザの前記ウェアラブルデバイス識別情報とをともなう検出指令を前記端末に対して発行するように構成された検出指令発行ユニットと；
前記端末により返信され、アップリンク認証情報をともなう検出承認を受信するように構成された検出承認受信ユニットであって、前記アップリンク認証情報はデバイス認証キーと、前記ダウンリンク認証情報とに応じて前記検出指令で指定されたウェアラブルデバイスによって生成され、前記デバイス認証キーが前記サーバ認証キーと同一又はそれに対応する、検出承認受信ユニットと；
前記ユーザの前記サーバ認証キーを使用することにより、前記ダウンリンク認証情報を前記アップリンク認証情報とマッチングし、前記マッチングに成功した場合に前記ユーザ

が前記認証を得るように構成されたマッチングユニットと；を備える、
ユーザを認証するための装置。
［第２０の局面］
前記サーバが、前記ユーザのユーザパブリックキーを更に格納し、前記ユーザパブリックキーは、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、前記ユーザパブリックキーと前記端末に格納されるユーザプライベートキーとは一対のキーであり、
前記端末によって返信される前記検出承認は、前記端末に格納される前記ユーザプライベートキーを用いて署名され、
前記装置が、前記ユーザの前記ユーザパブリックキーに応じて前記端末の前記検出承認に対して署名検証を遂行するように構成された検出承認検証ユニットを更に備え、
前記検証に失敗した場合、前記ユーザへの前記認証は失敗となる、
第１９の局面に記載の装置。
［第２１の局面］
前記サーバが端末識別情報を更に格納し、前記端末識別情報は、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとに対応し、
前記認証要求が、前記認証要求を送信するための端末識別情報を更に含み、
前記装置が、前記認証要求の中の前記ユーザ識別情報又は前記ウェアラブルデバイス識別情報に対応する前記端末識別情報が前記認証要求を送信するための前記端末識別情報と異なる場合、前記ユーザに対する前記認証が失敗となることを検証するように構成された端末識別情報検証ユニットを更に備える、
第１９の局面に記載の装置。
［第２２の局面］
前記サーバがサーバプライベートキーを更に格納し、前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、
前記装置が、前記サーバプライベートキーを用いて前記検出指令に署名するように構成された検出指令署名ユニットを更に備える、
第１９の局面乃至第２１の局面のいずれか一項に記載の装置。
［第２３の局面］
前記サーバが支払いサーバであり、前記認証要求が支払い要求であり、
前記装置が、前記認証を得たユーザに支払いサービスを提供するように構成された支払いサービスユニットを更に備える、
第１９の局面乃至第２１の局面のいずれか一項に記載の装置。
［第２４の局面］
ユーザのウェアラブルデバイスに接続される端末に適用される、前記ユーザを認証するための装置であって：
前記ユーザの操作に応じて、認証要求をサーバへ送信するように構成された認証要求送信ユニットであって、前記認証要求が前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、認証要求送信ユニットと；
前記サーバの検出指令を受信するように構成された検出指令受信ユニットであって、前記検出指令がダウンリンク認証情報と前記ウェアラブルデバイス識別情報とをともなう、検出指令受信ユニットと；
前記検出指令で指定されたウェアラブルデバイスへ前記ダウンリンク認証情報を送信し、前記ウェアラブルデバイスによって返信されるアップリンク認証情報を受信するように構成されたアップリンク認証情報ユニットであって、前記アップリンク認証情報は、格納されたデバイス認証キーと前記ダウンリンク認証情報とに応じて前記ウェアラブルデバイスによって生成され、前記デバイス認証キーは前記サーバに格納されるサーバ認証キーと同一又はそれに対応する、アップリンク認証情報ユニットと；
前記アップリンク認証情報をともなう検出承認を、前記サーバへ送信するように構成された検出承認送信ユニットと：

前記アップリンク認証情報と、前記ダウンリンク認証情報と、前記サーバ認証キーとに応じて前記サーバにより判定されるユーザ認証結果を受信するように構成された認証結果受信ユニットと；を備える、
ユーザを認証するための装置。
［第２５の局面］
前記端末が、前記ユーザのユーザプライベートキーを格納し、前記ユーザプライベートキーと前記サーバに格納されるユーザパブリックキーとは一対のキーであり、
前記装置が、前記ユーザの前記ユーザプライベートキーを用いて前記検出承認に署名するように構成された検出承認署名ユニットを更に備える、
第２４の局面に記載の装置。
［第２６の局面］
前記端末が、端末パブリックキーを格納し、前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、
前記サーバによって発行される前記検出指令が、前記サーバプライベートキーを用いて署名され、
前記装置が、前記端末パブリックキーに応じて前記サーバの前記検出指令に対して署名検証を遂行し、前記検証が失敗した場合には前記検出指令を拒絶するように構成された検出指令検証ユニットを更に備える、
第２４の局面又は第２５の局面に記載の装置。
［第２７の局面］
前記認証要求は支払い要求であり、前記ユーザ認証結果が前記認証の成功であった後に、前記端末が前記ユーザの支払い操作を完了する、
第２４の局面又は第２５の局面に記載の装置。
［第２８の局面］
サーバに適用される、ウェアラブルデバイスを登録するための装置であって、
端末を通じてユーザによって送信されるウェアラブルデバイス登録要求を受信ように構成された登録要求受信ユニットであって、前記登録要求は、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、登録要求受信ユニットと；
前記ユーザのサーバ認証キーと、デバイス認証キーとを取得し、前記デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう書き込み指令を前記端末に対して発行するように構成された書き込み指令発行ユニットと；
前記端末によって返信される書き込み承認を受信し、前記書き込み指令で指定されたウェアラブルデバイスへの前記デバイス認証キーの格納に成功したことを前記書き込み承認が示している場合、前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの対応関係を格納するように構成された書き込み承認受信ユニットと；を備える、
ウェアラブルデバイスを登録するための装置。
［第２９の局面］
前記書き込み承認受信ユニットが：
前記書き込み指令で指定された前記ウェアラブルデバイスへの前記デバイス認証キーの格納に成功したことを前記書き込み承認が示している場合、パスワード承認要求を前記端末に対して発行するように構成されたパスワード承認要求発行モジュールと；
前記端末からユーザパスワードをともなうパスワード承認を受信し、前記ユーザパスワードが正しい場合に前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの前記対応関係を格納するように構成されたパスワード承認受信モジュールと；を備える、
第２８の局面に記載の装置。
［第３０の局面］
前記端末によって返信される前記書き込み承認が、前記端末によって生成されるユーザパブリックキーを更に含み、

前記パスワード承認受信ユニットが、前記端末からユーザパスワードをともなうパスワード承認を受信し、前記ユーザパスワードが正しい場合に前記ユーザの前記ユーザ識別情報と、前記ウェアラブルデバイス識別情報と、前記サーバ認証キーとの前記対応関係を格納するように具体的に構成された、
第２８の局面又は第２９の局面に記載の装置。
［第３１の局面］
前記サーバが、サーバプライベートキーとサーバパブリックキーとを更に格納し、
前記サーバプライベートキーと前記端末に格納される端末パブリックキーとは一対のキーであり、前記サーバパブリックキーと前記端末に格納される端末プライベートキーとは一対のキーであり、
前記装置が、前記サーバプライベートキーを用いて前記書き込み指令に署名するように構成された書き込み指令署名ユニットを更に備え、
前記装置が、前記サーバパブリックキーを用いて前記端末の前記書き込み承認に対して署名検証を遂行し、前記検証が失敗した場合には前記登録要求を拒絶するように構成された書き込み承認検証ユニットを更に備える、
第２８の局面又は第２９の局面に記載の装置。
［第３２の局面］
端末に適用される、ウェアラブルデバイスを登録するための装置であって：
ユーザの操作に応じて、ウェアラブルデバイス登録要求をサーバへ送信するように構成された登録要求送信ユニットであって、前記登録要求が、前記ユーザのユーザ識別情報とウェアラブルデバイス識別情報とをともなう、登録要求送信ユニットと；
前記サーバの書き込み指令を受信するように構成された書き込み指令受信ユニットであって、前記書き込み指令が、前記デバイス認証キーと前記ユーザの前記ウェアラブルデバイス識別情報とをともなう、書き込み指令受信ユニットと；
前記書き込み指令で指定されたウェアラブルデバイス上に前記デバイス認証キーを書き込む操作を実行するように構成された書き込み操作実行ユニットと；
書き込み承認を前記サーバに送信するように構成された書き込み承認送信ユニットであって、前記書き込み承認が、前記デバイス認証キーの書き込みに成功したか否かを示すメッセージをともなう、書き込み承認送信ユニットと；を備える、
ウェアラブルデバイスを登録するための装置。
［第３３の局面］
前記書き込み承認が前記サーバに送信された後に、前記サーバのパスワード承認要求を受信し、前記ユーザによって入力されたユーザパスワードをともなうパスワード承認を前記サーバへ返信するように構成されたパスワード承認要求受信ユニットを更に備える、
第３２の局面に記載の装置。
［第３４の局面］
前記装置は、前記デバイス認証キーを書き込む前記操作が移行した後に、前記ユーザのユーザプライベートキーとユーザパブリックキーとを生成し、前記ユーザプライベートキーを格納するように構成されたユーザキー生成ユニットを更に備え、
前記書き込み承認が、前記ユーザの前記ユーザパブリックキーを更にともなう、
第３２の局面又は第３３の局面に記載の装置。
［第３５の局面］
前記端末が、端末パブリックキーと端末プライベートキーとを格納し、前記端末パブリックキーと前記サーバに格納されるサーバプライベートキーとは一対のキーであり、前記端末プライベートキーと前記サーバに格納されるサーバパブリックキーとは一対のキーであり、
前記装置は、前記端末パブリックキーを用いて前記サーバの前記書き込み指令に対して署名検証を遂行し、前記検証が失敗した場合には前記書き込み指令を拒絶するように構成された書き込み指令検証ユニットを更に備え、
前記装置は、前記端末プライベートキーを用いて前記書き込み承認に署名するように構

成された書き込み承認署名ユニットを更に備える、
第３２の局面又は第３３の局面に記載の装置。
［第３６の局面］
支払い方法であって：
支払いクライアント端末を通じてユーザによって送信される支払い要求を受信するステップであって、前記支払い要求は、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、ステップと；
ダウンリンク認証情報を取得し、前記ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とを含む認証指令を前記支払いクライアント端末に対して発行するステップと；
前記支払いクライアント端末によって返信され、アップリンク認証情報をともなう認証応答情報を受信するステップであって、前記アップリンク認証情報は、デバイス認証キーと前記ダウンリンク認証情報とに応じて前記認証指令で指定されたウェアラブルデバイスによって生成され、前記デバイス認証キーは、サーバ認証キーと同一又はそれに対応する、ステップと；
前記ユーザの前記サーバ認証キーを用いて前記ダウンリンク認証情報を前記アップリンク認証情報とマッチングするステップと；を備え
前記マッチングに成功した場合に前記ユーザが前記認証を得て、前記認証に成功した後に支払い操作が遂行される、
支払い方法。
［第３７の局面］
前記支払い要求は、前記支払いクライアント端末上で前記ユーザが選択したウェアラブルデバイスによって支払うことを示す情報により引き起こされる、
第３６の局面に記載の方法。
［第３８の局面］
支払い方法であって：
支払いクライアント端末上でのユーザの支払い操作に応答してサーバへ支払い要求を送信するステップであって、前記支払い要求は、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、ステップと；
前記ウェアラブルデバイスが前記ウェアラブルデバイスによって格納されたデバイス認証キーと前記ダウンリンク認証情報とを用いてアップリンク認証情報を生成するために、前記サーバによって発行される、ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とを含む認証指令を受信し、前記ダウンリンク認証情報をウェアラブルデバイスへ送信するステップと；
前記サーバが前記アップリンク認証情報に応じて前記ユーザを認証し、前記認証に成功した後に支払い操作を遂行するために、前記ウェアラブルデバイスによって返信される前記アップリンク認証情報を受信し、前記アップリンク認証情報を前記サーバへ送信するステップと；を備える、
支払い方法。
［第３９の局面］
前記支払いクライアント端末上での前記ユーザの前記支払い操作が具体的には、前記ユーザによって選択されウェアラブルデバイスによって支払うことを示す操作である、
第３８の局面に記載の支払い方法。
［第４０の局面］
ウェアラブルデバイスのための支払い方法であって：
支払いクライアント端末によって送信される支払い認証情報を受信するステップであって、前記支払い認証情報は、前記支払いクライアント端末によって送信されるユーザの支払い要求に基づきサーバによって発行されるダウンリンク認証情報を含む、ステップと；
前記サーバが前記アップリンク認証情報に基づき前記ユーザを認証し、前記認証に成功した後に支払い操作を遂行できるように、前記支払いクライアント端末が前記アップリン

ク認証情報を前記サーバへ送信するために、格納されたデバイス認証キーと前記ダウンリンク認証情報とに基づきアップリンク認証情報を生成し、前記アップリンク認証情報を前記支払いクライアント端末へ送信するステップと；を備える、
ウェアラブルデバイスのための支払い方法。
［第４１の局面］
前記支払いクライアント端末を通じて前記ユーザによって発行される支払い拘束要求に応答して、前記支払い拘束要求がともなうデバイス認証キーを格納するステップを更に備える、
第４０の局面に記載の方法。
［第４２の局面］
支払い装置であって：
支払いクライアント端末を通じてユーザによって送信される支払い要求を受信するように構成された支払い要求受信ユニットであって、前記支払い要求が、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、支払い要求受信ユニットと；
ダウンリンク認証情報を取得し、前記ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とを含む認証指令を前記支払いクライアント端末に対して発行するように構成された認証指令発行ユニットと；
前記支払いクライアント端末によって返信され、アップリンク認証情報をともなう認証応答情報を受信するように構成された認証応答受信ユニットであって、前記アップリンク認証情報は、デバイス認証キーと前記ダウンリンク認証情報とに応じて前記認証指令で指定されたウェアラブルデバイスによって生成され、前記デバイス認証キーは前記サーバ認証キーと同一又はそれに対応する、認証応答受信ユニットと；
前記ユーザの前記サーバ認証キーを用いて、前記ダウンリンク認証情報を前記アップリンク認証情報とマッチングするように構成された支払いマッチングユニットと；を備え、
前記マッチングに成功した場合に前記ユーザが前記認証を得て、前記認証に成功した後に支払い操作が遂行される、
支払い装置。
［第４３の局面］
前記支払い要求は、前記支払いクライアント端末上で前記ユーザが選択する、ウェアラブルデバイスにより支払いを行うことを示す情報によって引き起こされる、
第４２の局面に記載の装置。
［第４４の局面］
支払い装置であって：
支払いクライアント端末上でのユーザの支払い操作に応答して支払い要求をサーバへ送信するように構成された支払い要求送信ユニットであって、前記支払い要求が、前記ユーザのユーザ識別情報及び／又はウェアラブルデバイス識別情報をともなう、支払い要求送信ユニットと；
前記ウェアラブルデバイスが、前記ウェアラブルデバイスによって格納されたデバイス認証キーと前記ダウンリンク認証情報とを用いてアップリンク認証情報を生成するために、前記サーバによって発行される、ダウンリンク認証情報と前記ウェアラブルデバイス識別情報とを含む認証指令を受信し、前記ダウンリンク認証情報をウェアラブルデバイスへ送信するように構成された認証指令受信ユニットと；
前記サーバが前記アップリンク認証情報に応じて前記ユーザを認証し、前記認証に成功した後に支払い操作を遂行するために、前記ウェアラブルデバイスによって返信される前記アップリンク認証情報を受信し、前記アップリンク認証情報を前記サーバへ送信するように構成された認証応答送信ユニットと；を備える、
支払い装置。
［第４５の局面］
前記支払いクライアント端末上での前記ユーザの前記支払い操作が、具体的には、前記

ユーザによって選択される、ウェアラブルデバイスによって支払いを行うことを示す操作である、
第４４の局面に記載の装置。
［第４６の局面］
ウェアラブルデバイスのための支払い装置であって：
支払いクライアント端末によって送信される支払い認証情報を受信するように構成された支払い認証情報受信ユニットであって、前記支払い認証情報が、前記支払いクライアント端末によって送信されるユーザの支払い要求に基づきサーバによって発行されるダウンリンク認証情報を含む、支払い認証情報受信ユニットと；
前記サーバが前記アップリンク認証情報に基づき前記ユーザを認証し、前記認証に成功した後に支払い操作を遂行するように、前記支払いクライアント端末が前記アップリンク認証情報を前記サーバへ送信するために、格納されたデバイス認証キーと前記ダウンリンク認証情報とに基づきアップリンク認証情報を生成し、前記アップリンク認証情報を前記支払いクライアント端末へ送信するように構成されたアップリンク認証情報生成ユニットと；を備える、
ウェアラブルデバイスのための装置。
［第４７の局面］
前記支払いクライアント端末を通じて前記ユーザによって発行される支払い拘束要求に応答して、前記支払い拘束要求がともなうデバイス認証キーを格納するように構成された支払い拘束ユニットを更に備える、
第４６の局面に記載の装置。