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

特許第6646341号
(P6646341)

(45)発行日　令和2年2月14日(2020.2.14)　(24)登録日　令和2年1月15日(2020.1.15)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/31	
H04L 9/32	(2006.01)	H04L	9/00	675B
G06Q 20/40	(2012.01)	G06Q	20/40	300
G06F 21/44	(2013.01)	G06F	21/44	

請求項の数 20　(全 36 頁)

(21)出願番号　特願2017-551677 (P2017-551677)
(86)(22)出願日　平成28年3月15日 (2016.3.15)
(65)公表番号　特表2018-515011 (P2018-515011A)
(43)公表日　平成30年6月7日 (2018.6.7)
(86)国際出願番号　PCT/CN2016/076415
(87)国際公開番号　WO2016/155497
(87)国際公開日　平成28年10月6日 (2016.10.6)
審査請求日　平成31年3月15日 (2019.3.15)
(31)優先権主張番号　201510155552.4
(32)優先日　平成27年4月2日 (2015.4.2)
(33)優先権主張国・地域又は機関
中国 (CN)

(73)特許権者　505032849
アリババ　グループ　ホウルディング　リミテッド
英国領ケイマン諸島　グランド　ケイマン　ジョージ　タウン　ピーオーボックス　847　ワン　キャピタル　プレイス　フォース　フロア
(74)代理人　100097320
弁理士　宮川　貞二
(74)代理人　100155192
弁理士　金子　美代子
(74)代理人　100131820
弁理士　金井　俊幸
(74)代理人　100100398
弁理士　柴田　茂夫

最終頁に続く

(54)【発明の名称】ユーザを認証する方法及び装置、ウェアラブルデバイスを登録する方法及び装置

(57)【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。
【発明の詳細な説明】
【技術分野】
【０００１】
本願はインターネット技術の分野に関し、特にユーザを認証するための方法及び装置並びにウェアラブルデバイスを登録するための方法及び装置に関する。
【背景技術】
【０００２】
インターネット技術の急速な進歩にともない、ユーザがネットワークを使って行うあらゆる種類の活動、例えば公的業務の処理、娯楽、ショッピング、及び資金管理、は増加の一途にある。ユーザは通常、こうしたサービスを多数のサービスプロバイダから得ている。ユーザは、サービスプロバイダのサーバに登録し、サービスを受ける度にアカウントとパスワードを提供し、サーバがユーザを認証し、対応するサービスを提供する。
【０００３】
ユーザは、セキュリティ面から、同一のアカウント及び同一のパスワードを多くのサービスプロバイダで使うことをできるだけ避けるべきである。ユーザがもっと多くのサービスを受けたいと思うと、サービスプロバイダごとにアカウントとそれに対応するパスワードとを記憶することになり、ユーザの負担は増えてしまう。同時に、生活のあらゆる面でネットワークサービスが益々普及しており、ユーザは常に、認証を得るためにアカウントとパスワードを入力しなければならない。それは煩雑な操作であって、ネットワークサービスを受ける効率を低下させる。
【発明の概要】
【０００４】
上記見地から、本願は、ユーザを認証するための方法を提供し、サーバに適用され、サーバは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サーバに格納し、当該方法は：
端末を通じて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、認証要求は、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、ダウンリンク認証情報とユーザの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端末に対して発行するステップと；
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、アップリンク認証情報は、デバイス認証キーと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、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；
ユーザのサーバ認証キーを用いてダウンリンク認証情報を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、マッチングに成功した場合にユーザが認証を得る、ステップと；を備える。
【０００５】
本願は、ユーザを認証するための方法を提供し、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、当該方法は：
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、認証要求は、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；
サーバの検出指令を受信するステップであって、検出指令は、ダウンリンク認証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；
ダウンリンク認証情報を、検出指令で指定されたウェアラブルデバイスへ送信し、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、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、ダウンリンク認証情報とに応じてウェアラブルデバイスによって生成され、デバイス認証キーは、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；
アップリンク認証情報をともなう検出承認をサーバへ送信するステップと；
アップリンク認証情報と、ダウンリンク認証情報と、サーバ認証キーとに応じて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。
【０００６】
本願は、ウェアラブルデバイスを登録するための方法を提供し、サーバに適用され、当該方法は：
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、登録要求は、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；
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、デバイス認証キーとユーザの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端末に対して発行するステップと；
端末によって返信される書き込み承認を受信し、書き込み指令で指定されたウェアラブルデバイスへのデバイス認証キーの格納に成功したことを書き込み承認が示す場合、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ステップと；を備える。
【０００７】
本願は、ウェアラブルデバイスを登録するための方法を提供し、端末に適用され、当該方法は：
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、登録要求は、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；
サーバの書き込み指令を受信するステップであって、書き込み指令は、デバイス認証キーとユーザの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；
書き込み指令で指定されたウェアラブルデバイス上に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；
書き込み承認をサーバへ送信するステップであって、書き込み承認は、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。
【０００８】
本願は、更にユーザを認証するための装置を提供し、サーバに適用され、サーバは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し、当該装置は：
端末を通じて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、認証要求が、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、認証要求受信ユニットと；
ダウンリンク認証情報を取得し、ダウンリンク認証情報とユーザの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；
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、アップリンク認証情報はデバイス認証キーと、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、デバイス認証キーが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；

ユーザのサーバ認証キーを使用することにより、ダウンリンク認証情報をアップリンク認証情報とマッチングし、マッチングに成功した場合にユーザが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、

【０００９】

本願は、ユーザを認証するための装置を提供し、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、当該装置は：

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、認証要求が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；

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、検出指令がダウンリンク認証情報と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；

検出指令で指定されたウェアラブルデバイスへダウンリンク認証情報を送信し、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、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ダウンリンク認証情報とに応じてウェアラブルデバイスによって生成され、デバイス認証キーは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；

アップリンク認証情報をともなう検出承認を、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：

アップリンク認証情報と、ダウンリンク認証情報と、サーバ認証キーとに応じて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。

【００１０】

本願は、ウェアラブルデバイスを登録するための装置を提供し、サーバに適用され、当該装置は：

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、登録要求は、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；

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、デバイス認証キーとユーザの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；

端末によって返信される書き込み承認を受信し、書き込み指令で指定されたウェアラブルデバイスへのデバイス認証キーの格納に成功したことを書き込み承認が示している場合、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。

【００１１】

本願は、ウェアラブルデバイスを登録するための装置を提供し、端末に適用され、当該装置は：

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、登録要求が、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；

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、書き込み指令が、デバイス認証キーとユーザの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；

書き込み指令で指定されたウェアラブルデバイス上に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、書き込み承認が、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。
【００１２】
本願は、支払方法を提供し、当該方法は：
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、支払い要求は、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、ダウンリンク認証情報とウェアラブルデバイス識別情報とを含む認証指令を支払いクライアント端末に対して発行するステップと；
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、アップリンク認証情報は、デバイス認証キーとダウンリンク認証情報とに応じて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、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；
ユーザのサーバ認証キーを用いてダウンリンク認証情報を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、
マッチングに成功した場合にユーザが認証を得て、認証に成功した後に支払い操作が遂行される。
【００１３】
本願は、支払方法を提供し、当該方法は：
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、支払い要求は、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；
ウェアラブルデバイスが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、サーバによって発行される、ダウンリンク認証情報と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、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；
サーバがアップリンク認証情報に応じてユーザを認証し、認証に成功した後に支払い操作を遂行するために、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し、アップリンク認証情報をサーバへ送信するステップと；を備える。
【００１４】
本願は、ウェアラブルデバイスのための支払い方法を提供し、当該方法は：
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、支払い認証情報は、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；
サーバがアップリンク認証情報に基づきユーザを認証し、認証に成功した後に支払い操作を遂行できるように、支払いクライアント端末がアップリンク認証情報を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、アップリンク認証情報を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。
【００１５】
本願は、支払い装置を提供し、当該装置は：
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、支払い要求が、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、ダウンリンク認証情報とウェアラブルデバイス識別情報とを含む認証指令を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；
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、アップリンク認証情報は、デバイス認証キーとダウンリンク認証情報とに応じて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、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、認証応答受信ユニットと；

ユーザのサーバ認証キーを用いて、ダウンリンク認証情報を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、

マッチングに成功した場合にユーザが認証を得て、認証に成功した後に支払い操作が遂行される。

【００１６】

本願は、支払い装置を提供し、当該装置は：

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、支払い要求が、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；

ウェアラブルデバイスが、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、サーバによって発行される、ダウンリンク認証情報と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、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；

サーバがアップリンク認証情報に応じてユーザを認証し、認証に成功した後に支払い操作を遂行するために、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し、アップリンク認証情報を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。

【００１７】

本願は、更にウェアラブルデバイスのための支払い装置を提供し、当該装置は：

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、支払い認証情報が、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；

サーバがアップリンク認証情報に基づきユーザを認証し、認証に成功した後に支払い操作を遂行するように、支払いクライアント端末がアップリンク認証情報を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、アップリンク認証情報を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。

【００１８】

上記の技術的な解決策から分かることであるが、本願の実施の形態によると、サーバ認証キー及びデバイス認証キーが、サーバ及びウェアラブルデバイス上で設定され、サーバは端末との相互作用を通じ、設定されたサーバ認証キー及び設定されたデバイス認証キーを用いて、指定されたウェアラブルデバイスを認証し、それによりウェアラブルデバイスに対応するユーザに対する認証が達成される。ユーザは、アカウント及びパスワードを記憶することも認証時にアカウント及びパスワードを入力することも何ら必要ない。これにより、ユーザの負担は軽減し、ネットワークサービスを受ける際のユーザの効率が高まる。

【図面の簡単な説明】

【００１９】

【図１】図１は、本願による、アプリケーションシナリオのネットワーク構造図を示す。

【図２】図２は、本願の実施の形態による、サーバに適用される、ユーザを認証するための方法のフローチャートである。

【図３】図３は、本願の実施の形態による、端末に適用される、ユーザを認証するための方法のフローチャートである。

【図４】図４は、本願の実施の形態による、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のフローチャートである。
【図５】図５は、本願の実施の形態による、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のフローチャートである。
【図６】図６は、サーバ、ウェアラブルデバイス、又は端末のハードウェア構造図である。
【図７】図７は、本願の実施の形態による、サーバに適用される、ユーザを認証するための装置の論理構造図である。
【図８】図８は、本願の実施の形態による、端末に適用される、ユーザを認証するための装置の論理構造図である。
【図９】図９は、本願の実施の形態による、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の論理構造図である。
【図１０】図１０は、本願の実施の形態による、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の論理構造図である。
【発明を実施するための形態】
【００２０】
ウェアラブルデバイスは、ユーザが装着できる又はユーザの衣服若しくはアクセサリ、例えば、リストバンド、スマートウォッチ、スマートシューズ、スマート衣服、スマートメガネ、スマートヘルメット、スマートリングなど、に組み込むことができるポータブルデバイスである。ウェアラブルデバイスは、いくつかのコンピューティング機能を有し、ハードウェアインターフェース又は無線ＬＡＮを通じて端末、例えばスマートフォン、タブレットコンピュータ、及びパーソナルコンピュータ、に接続でき、端末との間でデータを交換することにより様々な機能を実施する。
【００２１】
ウェアラブルデバイスは一般に一人のユーザに特化されたデバイスである。ウェアラブルデバイスには、可能な限りいつでもどこでもユーザが装着できるものがある。かかるウェアラブルデバイスは、ユーザそのものをある程度まで代表する。本願の実施の形態は、ユーザを認証する方法を提案する。この方法は、ユーザにアカウントとパスワードを記憶したり頻繁に入力したりする必要もなくウェアラブルデバイスの格納機能及びコンピューティング機能を利用してユーザを認証し、それにより従来技術にともなう問題を解決する。
【００２２】
本願の実施の形態が適用されるネットワーク環境は、図１に示す通りである。ウェアラブルデバイスは、ハードウェアインターフェース又は無線ＬＡＮを通じて端末に接続される。ハードウェアインターフェースは、音声インターフェース、ユニバーサル・シリアル・バス（ＵＳＢ）インターフェースなどであってもよい。無線ＬＡＮは、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｗｉｒｅｌｅｓｓ－Ｆｉｄｅｌｉｔｙ（Ｗｉ－Ｆｉ）、ＺｉｇＢｅｅ（ＺｉｇＢｅｅプロトコル）などであってもよい。端末は、スマートフォン、タブレットコンピュータ、パーソナルコンピュータなどであってもよい。端末は、通信ネットワーク（例えばインターネット及び／又はモバイル通信ネットワーク）を通じてサーバと通信する。ユーザは、端末を用いてサーバにアクセス要求を送信し、サーバは、ユーザを認証する。本願の実施の形態において、端末のタイプ、ウェアラブルデバイスが端末に接続されるハードウェアインターフェース又は無線ＬＡＮプロトコル、通信ネットワークのプロトコル及びネットワーク構造、並びにサーバの具体的な実装は限定されない。
【００２３】
本願の実施の形態において、サーバ上でのユーザを認証するための方法の工程は図２に示す通りであり、端末上でのその工程は図３に示す通りである。
【００２４】
この実施の形態において、サーバは、ユーザのユーザ識別情報と、ウェアラブルデバイスの識別情報と、サーバ認証キーとの対応関係を格納する。ユーザ識別情報は、一意の本

人識別情報であり、サーバにとっては、それに応じてユーザを他のユーザと区別するものであり、例えば、ユーザの名前、登録されたメールなどである。ユーザがモバイル端末に結びつけられている場合、ユーザ識別情報は、ユーザが結びつけられているモバイル端末の番号、国際携帯機器識別番号（ＩＭＩＥ）などであってもよい。ウェアラブルデバイス識別情報はウェアラブルデバイスを一意に表し、採用したデバイスの具体的な種類及び無線ＬＡＮプロトコルの違いによって異なる。ウェアラブルデバイス識別情報は一般に、ウェアラブルデバイスのハードウェアアドレス、例えば、メディアアクセス制御（ＭＡＣ）アドレスであってもよい。サーバ認証キーはサーバ上に格納され、サーバ認証キーを用いる暗号化アルゴリズムに応じてウェアラブルデバイス上に格納されたデバイス認証キーと同一又はそれに対応する。サーバ上に格納されるウェアラブルデバイス識別情報とサーバ認証キーとは互いに１対１に対応する。ユーザが認証用に２つ以上のウェアラブルデバイスを持つことが可能な場合、ユーザ識別情報は、２つ以上のウェアラブルデバイス識別情報及びサーバ認証キーに対応してもよい。更に留意すべきことであるが、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はサーバへローカルに格納されてもよく、サーバへアクセス可能な他の格納デバイス、例えば、ローカルエリアネットワークやクラウドストレージネットワークを格納するためのディスクアレイに格納されてもよく、この実施の形態では限定されない。

【００２５】

端末上では、ステップ３１０において、ユーザの操作に応じて認証要求がサーバへ送信され、この認証要求は、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。

【００２６】

サーバ上では、ステップ２１０において、端末を通じてユーザから送信された認証要求が受信される。

【００２７】

ユーザが端末上で、本人認証が必要なサービス（例えば、ログイン、パーソナルアカウントへのアクセス、支払いなど）をサーバに要求する場合、サーバは、ユーザを認証するための関連情報を端末に要求する。端末は認証要求をサーバへ送信する。この認証要求は、ユーザのユーザ識別情報、又はユーザのウェアラブルデバイス識別情報、又はユーザのユーザ識別情報及びウェアラブルデバイス識別情報をともなう。

【００２８】

サーバが端末からの認証要求を受信した後、認証要求の中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により、どのユーザが認証を要求しているかを判定できる。

【００２９】

サーバ上では、ステップ２２０において、ダウンリンク認証情報が取得され、ダウンリンク認証情報とユーザのウェアラブルデバイス識別情報とをともなう検出指令が端末に対して発行される。

【００３０】

ダウンリンク認証情報は、１つの認証データであっても、サーバ上に格納されたサーバ認証キーを用いて認証データを暗号化した後の暗号文であってもよい。サーバは、例えば、ランダムに認証データを生成したり、ファイル又は画像から一定のバイト数を獲得したりするなど、どのような方法で認証データを得てもよい。サーバは、認証データを自らローカルに生成しても、認証データを別のサーバから取得してもよい。この実施の形態はこれについて限定しない。

【００３１】

端末からの認証要求を受信した後、サーバは、認証要求の中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抽出し、そ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が、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間の格納された対応関係の中に含まれているか否か探し出す。ユーザ識別情報及

び／若しくはウェアラブルデバイス識別情報が含まれていない場合、又は、認証要求の中のユーザ識別情報とウェアラブルデバイス識別情報とが同一のユーザに属していない場合、サーバは端末からの認証要求を拒絶する。そうでない場合、サーバは認証データを取得する。プレーンテキストとしてのダウンリンク認証情報の場合、サーバは、認証データとユーザのウェアラブルデバイス識別情報とを検出指令にカプセル化し、検出指令を端末に対して発行する。暗号文としてのダウンリンク認証情報の場合、サーバは、認証要求の中のユーザ識別情報又はウェアラブルデバイス識別情報に対応するサーバ認証キーを用いて認証データを暗号化してダウンリンク認証情報を生成し、ダウンリンク認証情報とユーザのウェアラブルデバイス識別情報とを検出指令にカプセル化し、検出指令を端末に対して発行する。

【００３２】

端末上では、ステップ３２０において、サーバからの検出指令が受信され、検出指令は、ダウンリンク認証情報及びウェアラブルデバイス識別情報をともなう

【００３３】

端末上では、ステップ３３０において、ダウンリンク認証情報が、検出指令で指定されたウェアラブルデバイスへ送信され、ウェアラブルデバイスから返信されるアップリンク認証情報が受信される。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ダウンリンク認証情報とに応じて、ウェアラブルデバイスによって生成される。

【００３４】

端末はサーバの検出指令を受信し、そこからウェアラブルデバイス識別情報とダウンリンク認証情報とを抽出し、ダウンリンク認証情報を、検出指令で指定されたウェアラブルデバイス（即ち、検出指令の中のウェアラブルデバイス識別情報を持つウェアラブルデバイス）へ送信する。検出指令で指定されたウェアラブルデバイスが端末に未接続である場合、先ず、ウェアラブルデバイスによりサポートされた無線ＬＡＮプロトコルに従って端末とウェアラブルデバイスとの接続を完了させる必要がある。

【００３５】

上述のように、サーバによって指定されたウェアラブルデバイスは、サーバ認証キーと同一又はそれに対応するデバイス認証キーを格納している。ウェアラブルデバイスがダウンリンク認証情報を受信した後、それがプレーンテキストとしてのダウンリンク認証情報である場合、ウェアラブルデバイスは、デバイス認証キーを用いてダウンリンク認証情報を暗号化して暗号文としてのアップリンク認証情報を生成する。また、暗号文としてのダウンリンク認証情報である場合、ウェアラブルデバイスは、デバイス認証キーを用いてダウンリンク認証情報を復号することによりプレーンテキストとしてのアップリンク認証情報を生成する。プレーンテキストとしてのダウンリンク認証情報は、暗号文としてのアップリンク認証情報に対応し、暗号文としてのダウンリンク認証情報は、プレーンテキストとしてのアップリンク認証情報に対応する。ウェアラブルデバイスは、アップリンク認証情報を端末へ返信する。

【００３６】

端末上では、ステップ３４０において、アップリンク認証情報をともなう検出承認がサーバへ送信される。

【００３７】

ウェアラブルデバイスから返信されるアップリンク認証情報を受信した後、端末は、アップリンク認証情報を検出承認内へカプセル化し、この検出承認をサーバへ送信する。検出承認は一般にウェアラブルデバイス識別情報を更にともなう。

【００３８】

サーバ上では、ステップ２３０において、端末から返信される、アップリンク認証情報をともなう検出承認が受信される。

【００３９】

サーバ上では、ステップ２４０において、ユーザのサーバ認証キーを用いてダウンリンク認証情報がアップリンク認証情報とマッチングされ、マッチングに成功した場合、ユー

ザは認証を得る。

【００４０】

サーバは、端末から返信される検出承認を受信し、そこからアップリンク認証情報を抽出し、ユーザのサーバ認証キーを用いてアップリンク認証情報がダウンリンク認証情報とマッチングしているか否か判断してユーザの認証結果を判定する。具体的には、プレーンテキストとしてのアップリンク認証情報の場合、暗号文を生成するための認証データとアップリンク認証情報とを比較することができる、又は、サーバ認証キーを用いて既に暗号化されているアップリンク認証情報をダウンリンク認証情報と比較することができ、それらが同一であればユーザは認証を得ることができ、さもなければ認証を得ることはできない。暗号文としてのアップリンク認証情報の場合、アップリンク認証情報は、サーバ認証キーを用いて復号され、次いでダウンリンク認証情報と比較することができ、それらが同一であればユーザは認証を得ることができ、さもなければ認証を得ることはできない。

【００４１】

サーバは、ユーザが認証を得ることができたか否かを示す認証結果を端末へ返信する。

【００４２】

端末上では、ステップ３５０において、アップリンク認証情報と、ダウンリンク認証情報と、サーバ認証キーとに応じて、サーバによって判定されたユーザ認証結果が受信される。

【００４３】

この実施の形態において、同一又は互いに対応するサーバ認証キー及びデバイス認証キーがサーバ及びウェアラブルデバイス上で設定され、サーバは、端末との相互作用を通じ、ウェアラブルデバイス上に格納されたデバイス認証キー及びサーバ上に格納されたサーバ認証キーを用いて、指定されたウェアラブルデバイスを認証し、それによってウェアラブルデバイスに対応するユーザに対する認証を達成する。ユーザは、アカウントもパスワードも何ら記憶する必要はなく、認証時にアカウントもパスワードも何ら入力する必要もない。これにより、ユーザの負担は減り、ネットワークサービスを受ける際のユーザの効率が高まる。

【００４４】

実施において、ユーザのユーザパブリック（公開）キーをサーバ上に格納してもよく、ユーザのユーザプライベートキーを端末上に格納してもよく、異なるユーザ識別情報は異なるユーザパブリックキー及び異なるユーザプライベートキーを用い、ユーザパブリックキーとユーザプライベートキーとは、非対称暗号化における一対のキーである。サーバ上に格納されるユーザパブリックキーは、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、サーバ認証キーとに対応する。かかる実施において、端末は、格納されたユーザプライベートキーを用いて、検出承認にともなうデータ（アップリンク認証情報を含み、ウェアラブルデバイス識別情報と、ユーザ識別情報と、他のデータとを更に含んでもよい）に署名し、署名した検出承認をサーバへ送信する。サーバは、ユーザのユーザパブリックキーを用いて、検出承認に対して署名検証を行う。検出承認が検証に合格した場合、ステップ２４０が遂行され、アップリンク認証情報がダウンリンク認証情報とマッチングされる。検出承認が署名検証に不合格であった場合、端末には、認証を得られなかったことが通知される。かかる実施は、ユーザが認証のためにウェアラブルデバイスを使用する場合、ウェアラブルデバイスが接続される端末がユーザのユーザプライベートキーを格納している必要があり、それによって、より良好なセキュリティを達成できる。

【００４５】

加えて、サーバ上に格納される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に、端末識別情報を追加し、接続されたウェアラブルデバイスを通じたユーザ認証を行うことができる端末に制約をかけてもよい。かかる状況下において、サーバは、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に加え、端末識別情報を格納する。端末によってサーバへ送信される認証要求は、端末の端末識別情報をともなう。認証要求を受信した後、サーバ

は、格納された対応関係の中から認証要求の中にあるユーザ識別情報又はウェアラブルデバイス識別情報に対応する端末識別情報を探し出し、その端末識別情報を、認証要求を送信するための端末識別情報と比較する。それらが同一である場合、ステップ２２０が遂行されて認証工程は継続する。それらが異なる場合、端末の認証要求は拒絶され、ユーザ認証は失敗である。かかる実施は、ウェアラブルデバイスを、ウェアラブルデバイスを通じてユーザ認証を行うことができる端末に結びつけることと均等である。端末（とりわけ、モバイル端末）も一般にユーザに特化されているので、ウェアラブルデバイスを端末に結びつけることは、ユーザ認証のセキュリティを大幅に高める。

【００４６】

この実施の形態における上記の認証工程は、例えば、ログインの場合のユーザ本人認証、ユーザがパーソナルアカウントにアクセスする場合の本人認証、ユーザが第三者の支払いプラットフォームを通じて支払う場合の本人認証など、ユーザ本人の認証を必要とするどのようなシナリオにも適用可能である。ユーザが認証を得た後、サーバは、シナリオにおけるそれに続くサービスを提供することができ、端末は、シナリオにおけるそれに続く操作を実行する。例えば、この実施の形態を支払いシナリオにおける本人認証のために用いられる場合、端末から支払いサーバへ送信される認証要求は支払い要求である。ユーザが認証を得た後、支払いサーバは、認証を得たユーザに対して支払いサービスを提供できる。ユーザが認証を得たことを示す認証結果をサーバから受信した後、端末は、支払いサーバと協働してユーザの支払い操作を完了させることができる。

【００４７】

この実施の形態において、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サーバ上で予め設定し、対応するデバイス認証キーをウェアラブルデバイス上に予め設定することができる。更に、まず上記の対応関係をサーバ上で生成し、上記認証工程の前に登録工程を通じてデバイス認証キーをウェアラブルデバイス上に書き込むことができる。

【００４８】

本願の別の実施の形態は、ウェアラブルデバイスを登録するための方法を提供する。サーバ上での方法の工程は図４に示す通りであり、端末上でのその工程は図５に示す通りである。

【００４９】

端末上では、ステップ５１０において、ユーザの操作に応じてウェアラブルデバイス登録要求がサーバへ送信される。

【００５０】

サーバ上では、ステップ４１０において、端末を通じてユーザから送信されたウェアラブルデバイス登録要求が受信される。

【００５１】

ユーザは、端末上でウェアラブルデバイスをサーバに登録し、端末は、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。登録要求は、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含む。

【００５２】

サーバ上では、ステップ４２０において、ユーザのサーバ認証キーと、デバイス認証キーとが取得され、デバイス認証キーとユーザの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が端末に対して発行される。

【００５３】

端末のウェアラブルデバイス登録要求を受信した後、サーバは、認証工程におけるアップリンク認証情報又はダウンリンク認証情報のために採用された暗号化アルゴリズムに応じて、暗号化アルゴリズムに用いられ、ウェアラブルデバイス識別情報に対応するサーバ認証キーとデバイス認証キーとを取得する。サーバ認証キーとデバイス認証キーは、１つのキー（例えば、対称暗号化アルゴリズムのキー）であってもよく、一対のキー（例えば、非対称暗号化アルゴリズムのパブリックキー及びプライベートキー）であってもよい。

サーバは、サーバ認証キー及びデバイス認証キーを自ら生成してもよく、サーバ認証キー及びデバイス認証キーを別のサーバから得てもよい。

【００５４】

サーバは、取得したデバイス認証キーと、対応するウェアラブルデバイス識別情報とを書き込み指令内にカプセル化し、書き込み指令を端末へ送信する。

【００５５】

端末上では、ステップ５２０において、サーバからの書き込み指令が受信され、この書き込み指令は、デバイス認証キー及びユーザのウェアラブルデバイス識別情報をともなっている。

【００５６】

端末上では、ステップ５３０において、書き込み指令で指定されたウェアラブルデバイス上にデバイス認証キーを書き込む操作が実行される。

【００５７】

端末がサーバの書き込み指令を受信した後、端末は、書き込み指令の中のデバイス認証キーをウェアラブルデバイスへ送信し、ウェアラブルデバイスにデバイス認証キーを格納するように要求する。異なるウェアラブルデバイス及びその異なる設定許可に応じて、ウェアラブルデバイスは、ユーザが書き込み操作を確認（confirm）した後に限り、デバイス認証キーの格納を完了できる。例えば、リストバンドの場合、ユーザは一般に、確認(confirmation)のためにリストバンドをタップする必要がある。

【００５８】

端末上では、ステップ５４０において、書き込み承認がサーバに送信され、この書き込み承認は、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っている。ウェアラブルデバイスでの書き込み操作が完了した後、端末は、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書き込み承認内にカプセル化し、書き込み承認をサーバへ送信する。

【００５９】

サーバ上では、ステップ４３０において、端末から返信された書き込み承認が受信され、書き込み指令で指定されたウェアラブルデバイスへのデバイス認証キーの格納に成功したことを書き込み承認が示している場合、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が格納され、ウェアラブルデバイスの登録に成功したことになる。書き込み承認にともなうメッセージが、デバイス認証キーの格納が不成功であったという内容であれば、登録工程は失敗である。サーバは登録結果を端末へ送信する。

【００６０】

ウェアラブルデバイスの登録のセキュリティを強化するため、サーバは、端末へ、ユーザのパスワードを提供するように求めることができる。具体的には、サーバは、端末の書き込み承認を受信し、書き込み承認にともなうメッセージが、ウェアラブルデバイスへのデバイス認証キーの格納に成功したという内容である場合、サーバは、パスワード承認要求を端末に対して発行し、端末にウェアラブルデバイス識別情報に対応するユーザ識別情報のパスワードを提供するように求める。端末は、サーバのパスワード承認要求を受信し、ユーザが入力したユーザパスワードをともなうパスワード承認をサーバへ返信する。サーバは、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、ユーザパスワードが正しい場合には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。ウェアラブルデバイスの登録に成功したことになる。ユーザパスワードが正しくない場合、端末の登録要求は拒絶され、登録は失敗となる。サーバは登録結果を端末へ送信する。

【００６１】

実施において、ユーザのユーザパブリックキー及びユーザプライベートキーが登録工程において自動的に生成されてもよい。具体的には、端末によるデバイス認証キーをウェアラブルデバイスへ書き込む操作に成功した後、端末は、アルゴリズムに応じてユーザのユ

ーザパブリックキー及びユーザプライベートキーを生成し、生成したユーザプライベートキーをローカルに格納し、ユーザパブリックキーを書き込み承認内にカプセル化し、書き込み承認をサーバへ送信する。端末がウェアラブルデバイスへのデバイス認証キーの書き込みに成功した後、又はユーザパスワードが正しいことが検証された後、サーバは、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、ユーザパブリックキーとの対応関係を格納する。

【００６２】

一部のアプリケーションシナリオでは、サーバパブリックキー及びサーバプライベートキーがサーバ上に予め設定され、端末プライベートキー及び端末パブリックキーが端末上で予め設定され、その場合、サーバパブリックキーと端末プライベートキーとは一対のキーであり、サーバプライベートキーと端末パブリックキーとは一対のキーである。こうしたシナリオでは、認証方法の実施の形態において、サーバは、格納されたサーバプライベートキーを用いて検出指令に署名し、署名した検出指令を端末へ送信することができる。端末は、格納された端末パブリックキーを用いて、受信した検出指令に対して署名検証を遂行し、検証が失敗した場合には検出指令を拒絶し、その結果、認証は得られない。登録方法の実施の形態において、サーバは、格納されたサーバプライベートキーを用いて書き込み指令に署名し、署名した書き込み指令を端末へ送信できる。端末は、格納された端末パブリックキーを用いて、受信した書き込み指令に対して署名検証を遂行し、検証が失敗した場合には書き込み指令を拒絶し、その結果、登録されない。端末は、格納された端末プライベートキーを用いて書き込み承認に署名し、署名した書き込み承認をサーバへ送信できる。サーバは、格納されたサーバパブリックキーを用いて、受信した書き込み承認に対して署名検証を遂行し、検証が失敗した場合には端末の登録要求を拒絶する。

【００６３】

サーバ及び端末は、ウェアラブルデバイス登録及びユーザ認証のセキュリティを更に強化するため、暗号化されたチャンネルを通じて通信を行ってもよい。例えば、認証方法の実施の形態における検出指令及び検出承認、そして登録方法の実施の形態における書き込み指令及び書き込み承認はいずれも、暗号化されたチャンネルで伝送することができる。採用された暗号化チャンネル及び暗号化方法の実施については従来技術を参照することができ、ここで繰り返さない。

【００６４】

本願の実施の形態において、端末上で稼動する支払いクライアント端末は、支払い工程において、端末に接続されたウェアラブルデバイスを用いてユーザ本人を認証する。この実施の形態の具体的な工程は以下の通りである。

【００６５】

ウェアラブルデバイス上では、支払いクライアント端末の支払い拘束要求が受信され、支払い拘束要求は、ウェアラブルデバイスのデバイス認証キーを含む。ウェアラブルデバイスは、支払いクライアント端末を通じてユーザが発行する支払い拘束要求に応答して、支払い拘束要求がともなうデバイス認証キーをローカルメモリに格納する。

【００６６】

支払いクライアント端末上で支払い操作を行う場合、ユーザは、支払うためのウェアラブルデバイスを選択し、上記ユーザ操作に対する支払いクライアント端末の応答を引き起こし、支払い要求をサーバへ送信する。支払い要求は、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っている。

【００６７】

支払いクライアント端末を通じてユーザから送信された支払い要求を受信した後、サーバは、ダウンリンク認証情報を取得し、ダウンリンク認証情報とウェアラブルデバイス識別情報とを含む認証指令を支払いクライアント端末に対して発行する。

【００６８】

支払いクライアント端末は、サーバから発行された認証指令を受信し、支払い認証情報にダウンリンク認証情報を含ませ、支払い認証情報を認証指令で指定されたウェアラブル

デバイスへ送信する。

【００６９】

ウェアラブルデバイスは、支払いクライアント端末から送信される支払い認証情報を受信し、支払いクライアント端末から送信されるユーザの支払い要求に基づき、支払い認証情報から、サーバによって発行されたダウンリンク認証情報を抽出し、格納されたデバイス認証キー及びダウンリンク認証情報に応じてアップリンク認証情報を生成し、アップリンク認証情報を支払いクライアント端末へ送信する。

【００７０】

支払いクライアント端末は、ウェアラブルデバイスから返信されるアップリンク認証情報を受信し、アップリンク認証情報を認証応答情報に含ませ、認証応答情報をサーバへ送信する。

【００７１】

サーバは、支払いクライアント端末から返信されるアップリンク認証情報をともなう認証応答情報を受信し、ユーザのサーバ認証キーを用いてダウンリンク認証情報をアップリンク認証情報とマッチングさせ、その場合、マッチングに成功すればユーザは認証を得て、認証に成功した後に支払い操作を遂行する。ユーザのサーバ認証キーは、認証指令で指定されたウェアラブルデバイスのデバイス認証キーと同一又はそれに対応する。

【００７２】

この実施の形態において、同一又は互いに対応するサーバ認証キー及びデバイス認証キーがサーバ及びウェアラブルデバイス上で設定され、ウェアラブルデバイスは、デバイス認証キーとサーバ認証キーとを用いて認証され、それによって、ユーザがウェアラブルデバイスを使用して支払いクライアント端末上で支払うことができるように、ウェアラブルデバイスに対応するユーザに対する支払い認証が完了する。ユーザは、アカウントもパスワードも何ら記憶する必要はなく、認証時にアカウントもパスワードも何ら入力する必要もない。これにより、ユーザの負担は軽減し、支払いの効率が高まる。

【００７３】

本願のアプリケーション例では、携帯電話端末上で稼動するクライアント端末アプリケーション（Ａｐｐ）を通じてリストバンドを支払いサーバに登録した後、ユーザは、リストバンドを通じて、ネットワークでの支払いを、アカウントもパスワードも何ら入力することなく完了できる。一対のサーバプライベートキーと端末パブリックキーとに加え、一対のサーバパブリックキーと端末プライベートキーとが支払いサーバ及びクライアント端末Ａｐｐ上で予め設定される。ここで、支払いサーバは、クライアント端末Ａｐｐに対応するサーバ端末プログラムを実行するサーバであっても、クライアント端末Ａｐｐをサポートする第三者の支払いプラットフォームのサーバであってもよい。具体的な工程は以下の通りである。

【００７４】

ユーザは、リストバンド支払いの開設を申し込むために、携帯電話端末上で稼動するクライアント端末Ａｐｐ（以下、「クライアント端末」とする）を通じてウェアラブルデバイス登録要求を支払いサーバへ送信し、クライアント端末は、登録要求におけるユーザ識別情報（支払いサーバ上でのユーザのアカウント）と、携帯電話端末識別情報（ＩＭＥＩ）と、リストバンド識別情報（リストバンドＭＡＣアドレス）とをサーバにアップロードする。

【００７５】

支払いサーバは、所定のアルゴリズムを通じて、リストバンドを認証するための対称キー（即ち、同一のサーバ認証キーとデバイス認証キー）を生成し、予め設定されたサーバプライベートキーを通じて、対称キーと、ユーザ識別情報と、リストバンド識別情報と共に署名し、署名した対称キーと、ユーザ識別情報と、リストバンド識別情報とを書き込み指令内にカプセル化し、書き込み指令を支払いサーバとクライアント端末との間の暗号化されたチャンネルを通じてクライアント端末へ送信する。

【００７６】

サーバ端末の書き込み指令を受信した後、クライアント端末はまず、予め設定される端末パブリックキーに応じて書き込み指令の中のデータの有効性を検証し、データが無効である場合、書き込み指令を直接拒絶する。有効性検証に成功した後、クライアン端末は、書き込み指令で指定されたリストバンドに接続され、接続に成功した後、支払いサーバによって発行された対称キーをリストバンドに書き込む。対称キーをリストバンドへ書き込む工程において、ユーザは、リストバンドをタップして書き込み操作を承認する必要があり、ユーザがリストバンドをタップした後、対称キーがリストバンドの格納領域に書き込まれる。

【００７７】

書き込み操作に成功した後、クライアント端末は、ユーザ識別情報に応じて一対の非対称キー、即ち、ユーザ識別情報に対応するユーザパブリックキーとユーザプライベートキーとを生成する。クライアント端末は、予め設定された端末プライベートキーを通じて書き込み操作に成功であるか否かを示す結果と、リストバンド識別情報と、生成されたユーザパブリックキーとに署名し、署名した情報を書き込み承認内にカプセル化し、暗号化されたチャンネルを通じて書き込み承認を支払いサーバへ送信する。ユーザプライベートキーは、クライアント端末によってローカルに格納される。

【００７８】

クライアント端末の書き込み承認を受信した後、支払いサーバは、予め設定されたサーバパブリックキーを通じてクライアント端末の署名を検証し、検証に失敗した場合、クライアント端末の登録要求を拒絶する。署名検証に成功した後、支払いサーバは、パスワード承認要求をクライアント端末に対して発行し、クライアント端末に支払いサーバ上でのユーザのアカウントのパスワードを提供するように求める。

【００７９】

クライアント端末は、パスワードの入力に関するプロンプト情報をユーザに対して表示し、ユーザは、支払いサーバ上での自身のアカウントのパスワードを入力する。クライアント端末は、受信したパスワードをともなうパスワード承認を支払いサーバへ送信する。

【００８０】

支払いサーバは、パスワード承認の中のユーザパスワードを検証し、検証に成功した後、対称キー（サーバ認証キー）と、ユーザ識別情報と、携帯電話識別情報と、リストバンド識別情報と、クライアント端末によって生成されたユーザパブリックキーとの対応関係を格納し、リストバンドの登録に成功したことをクライアント端末へ通知する。登録工程は終了する。

【００８１】

リストバンドの支払いサーバへの登録に成功した後、ユーザは、リストバンドを通じた支払いを望む場合に、クライアント端末を通じて支払い認証要求をサーバへ送信する。認証要求は、支払いをすべき注文の情報、ユーザ識別情報、携帯電話端末識別情報、及びリストバンド識別情報を含む。

【００８２】

クライアント端末の認証要求を受信した後、支払いサーバは、認証要求の中の携帯電話端末識別情報を認証要求の中のリストバンド識別情報に対応する格納された対応関係の中の携帯電話端末識別情報と比較する。それらが異なる場合、認証要求は拒絶され、支払いは失敗となる。それらが同一である場合、支払いサーバは、ランダムプレーンテキストデータを生成し、プレーンテキストデータをダウンリンク認証情報として用い。支払いサーバは、予め設定されたサーバプライベートキーを用いて、ダウンリンク認証情報と、ユーザ識別情報と、リストバンド識別情報とに署名し、これらを検出指令内にカプセル化し、検出指令を、支払いサーバとクライアント端末との間の暗号化されたチャンネルを通じてクライアント端末へ送信する。

【００８３】

支払いサーバの検出指令を受信した後、クライアント端末はまず、予め設定される端末パブリックキーに応じて検出指令の中の署名データの有効性を検証する。データが無効で

ある場合、検出指令は拒絶され、支払いは失敗となる。署名の有効性検証に成功した後、クライアント端末は、検出指令で指定されたリストバンドに接続され、接続に成功した後、検出指令の中のダウンリンク認証情報をリストバンドへ送信する。リストバンドは、格納された対称キーを用いてダウンリンク認証情報を暗号化してアップリンク認証情報を生成し、アップリンク認証情報をクライアント端末へ返信する。リストバンドによるダウンリンク認証情報を暗号化する工程は、承認のためにユーザがタップする必要はなく、そのため、ユーザの操作を更に減らし、ユーザエクスペリエンスを最適化する。

【００８４】

リストバンドによって生成されたアップリンク認証情報を受信した後、クライアント端末は、ローカルに格納されたユーザプライベートキーを用いてアップリンク認証情報に署名し、署名したデータと署名したリストバンド識別情報とを検出承認内にカプセル化し、検出承認を、クライアント端末と支払いサーバとの間の暗号化チャンネルを通じて支払いサーバへ送信する。

【００８５】

クライアント端末によりアップロードされた検出承認を受信した後、支払いサーバは、検出承認の中のリストバンド識別情報に対応するユーザパブリックキーに応じて、検出承認に対して署名検証を遂行してもよい。署名検証に失敗した場合、認証要求は失敗となる。署名検証に成功した後、支払いサーバは、リストバンド識別情報に対応する対称キーを用いてダウンリンク認証情報を暗号化し、暗号化したデータを検出承認の中のアップリンク認証情報と比較する、即ち、支払いサーバによって暗号化されたダウンリンク認証情報がリストバンドによって暗号化されたダウンリンク認証情報と同一であるか否か比較し、それらが同一である場合、認証成功のメッセージをクライアント端末へ返信し、注文への支払いを続ける。それらが異なる場合、支払いサーバは、認証不成功のメッセージをクライアント端末へ返信する。認証成功のメッセージを受信した後、クライアント端末は、支払いサーバと共にユーザの注文の支払い操作を完了させる。認証不成功のメッセージを受信した場合、クライアント端末はユーザに、認証が不成功なのでこの支払いが完了できない旨通知する。

【００８６】

上記工程の実施に対応し、本願の実施の形態は、サーバに適用されるユーザを認証するための装置、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ユーザを認証するための装置、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、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、サーバに適用される支払い装置、端末に適用される支払い装置、及びウェアラブルデバイスに適用される支払い装置を更に提供する。これらの装置は全て、ソフトウェアによって実施してもよく、ハードウェアによって、又はソフトウェアとハードウェアの組み合わせによって実施してもよい。ソフトウェアの実施を例に取ると、装置は、論理的な意味で、サーバ、端末、又はウェアラブルデバイスのＣＰＵを通じて対応のコンピュータプログラム指令をメモリに読み込み、コンピュータプログラム指令を稼動させることによって形成される。ハードウェアレベルに関して言えば、図６に示すＣＰＵ、メモリ、及び不揮発性メモリに加え、装置が配置される端末又はウェアラブルデバイスは一般に、他のハードウェア、例えば無線信号を送受信するためのチップを更に含み、装置が配置されるサーバは一般に、他のハードウェア、例えばネットワーク通信機能を実施するためのボードカードを更に含む。

【００８７】

図７は、この実施の形態によるユーザを認証するための装置を示す。装置はサーバに適用される。サーバは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。装置は、認証要求受信ユニットと、検出指令発行ユニットと、検出承認受信ユニットと、マッチングユニットとを備え：認証要求受信ユニットは、端末を通じて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、認証要求が、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い；検出指令発行ユニットは、ダウンリンク認証情報を取得し、ダウンリンク認証情報とユーザ

の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端末に対して発行するように構成され；検出承認受信ユニットは、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、アップリンク認証情報はデバイス認証キーと、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、デバイス認証キーがサーバ認証キーと同一又はそれに対応し；マッチングユニットは、ユーザのサーバ認証キーを使用することにより、ダウンリンク認証情報を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、マッチングに成功した場合にユーザが認証を得る。

【００８８】

任意で、サーバは、ユーザのユーザパブリックキーを更に格納する。ユーザパブリックキーは、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、サーバ認証キーとに対応する。ユーザパブリックキーと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る。端末によって返信される検出承認は、端末に格納されるユーザプライベートキーを用いて署名される。装置は、ユーザのユーザパブリックキーに応じて端末の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、検証に失敗した場合、ユーザへの認証は失敗となる。

【００８９】

任意で、サーバは端末識別情報を更に格納する。端末識別情報は、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、サーバ認証キーとに対応する。認証要求が、認証要求を送信するための端末識別情報を更に含む。装置は、認証要求の中のユーザ識別情報又はウェアラブルデバイス識別情報に対応する端末識別情報が認証要求を送信するための端末識別情報と異なる場合、ユーザに対する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。

【００９０】

任意で、サーバはサーバプライベートキーを更に格納する。サーバプライベートキーと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る。装置は、サーバプライベートキーを用いて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。

【００９１】

任意で、サーバは支払いサーバである。認証要求が支払い要求である。装置は、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。

【００９２】

図８は、この実施の形態によるユーザを認証するための装置を示す。装置は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。装置は、認証要求送信ユニットと、検出指令受信ユニットと、アップリンク認証情報ユニットと、検出承認送信ユニットと、認証結果受信ユニットとを備え：認証要求送信ユニットは、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、認証要求が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い；検出指令受信ユニットは、サーバの検出指令を受信するように構成され、検出指令がダウンリンク認証情報とウェアラブルデバイス識別情報とをともない；アップリンク認証情報ユニットは、検出指令で指定されたウェアラブルデバイスへダウンリンク認証情報を送信し、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、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ダウンリンク認証情報とに応じてウェアラブルデバイスによって生成され、デバイス認証キーは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し；検出承認送信ユニットは、アップリンク認証情報をともなう検出承認を、サーバへ送信するように構成され：認証結果受信ユニットとは、アップリンク認証情報と、ダウンリンク認証情報と、サーバ認証キーとに応じて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る。

【００９３】

任意で、端末は、ユーザのユーザプライベートキーを格納し、ユーザプライベートキーと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る。装置は：ユーザのユーザプライベートキーを用いて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。

【００９４】

任意で、端末は、端末パブリックキーを格納する。端末パブリックキーと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る。サーバによって発行される検出指令が、サーバプライベートキーを用いて署名される。装置は、端末パブリックキーに応じてサーバの検出指令に対して署名検証を遂行し、検証が失敗した場合には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。

【００９５】

任意で、認証要求は支払い要求である。ユーザ認証結果が認証の成功であった後に、端末はユーザの支払い操作を完了する。

【００９６】

図９は、この実施の形態によるウェアラブルデバイスを登録するための装置である。装置はサーバに適用される。機能面で分けると、装置は、更に登録要求受信ユニットと、書き込み指令発行ユニットと、書き込み承認受信ユニットとを備え：登録要求受信ユニットは、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、登録要求は、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い；書き込み指令発行ユニットは、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、デバイス認証キーとユーザの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端末に対して発行するように構成され；書き込み承認受信ユニットは、端末によって返信される書き込み承認を受信し、書き込み指令で指定されたウェアラブルデバイスへのデバイス認証キーの格納に成功したことを書き込み承認が示している場合、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ように構成される。

【００９７】

任意で、書き込み承認受信ユニットが、書き込み指令で指定されたウェアラブルデバイスへのデバイス認証キーの格納に成功したことを書き込み承認が示している場合、パスワード承認要求を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；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、ユーザパスワードが正しい場合に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。

【００９８】

任意で、端末によって返信される書き込み承認が、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；パスワード承認受信ユニットが、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、ユーザパスワードが正しい場合に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ように具体的に構成される。

【００９９】

任意で、サーバは、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する。サーバプライベートキーと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、サーバパブリックキーと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る。装置は、サーバプライベートキーを用いて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る。装置は、サーバパブリックキーを用いて端末の書き込み承認に対して署名検証を遂行し、検証が失敗した場合には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。

【０１００】

図１０は、この実施の形態によるウェアラブルデバイスを登録するための装置である。

装置は端末に適用される。機能面で分けると、装置は更に、登録要求送信ユニットと、書き込み指令受信ユニットと、書き込み操作実行ユニットと、書き込み承認送信ユニットとを備え：登録要求送信ユニットは、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、登録要求が、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い；書き込み指令受信ユニットは、サーバの書き込み指令を受信するように構成され、書き込み指令が、デバイス認証キーとユーザのウェアラブルデバイス識別情報とをともない；書き込み操作実行ユニットは、書き込み指令で指定されたウェアラブルデバイス上に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；書き込み承認送信ユニットは、書き込み承認をサーバに送信するように構成され、書き込み承認が、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。

【０１０１】

任意で、装置は、書き込み承認がサーバに送信された後に、サーバのパスワード承認要求を受信し、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。

【０１０２】

任意で、装置は、デバイス認証キーを書き込む操作が移行した後に、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、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、書き込み承認が、ユーザのユーザパブリックキーを更にともなう。

【０１０３】

任意で、端末は、端末パブリックキーと端末プライベートキーとを格納する。端末パブリックキーと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、端末プライベートキーと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る。装置は、端末パブリックキーを用いてサーバの書き込み指令に対して署名検証を遂行し、検証が失敗した場合には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る。装置は、端末プライベートキーを用いて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。

【０１０４】

本願の実施の形態は、支払い装置を提供し、サーバに適用される。機能面で分けると、装置は、支払い要求受信ユニットと、認証指令発行ユニットと、認証応答受信ユニットと、支払いマッチングユニットとを備え、：支払い要求受信ユニットは、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、支払い要求が、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い；認証指令発行ユニットは、ダウンリンク認証情報を取得し、ダウンリンク認証情報とウェアラブルデバイス識別情報とを含む認証指令を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；認証応答受信ユニットは、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、アップリンク認証情報は、デバイス認証キーとダウンリンク認証情報とに応じて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、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し；支払いマッチングユニットは、ユーザのサーバ認証キーを用いて、ダウンリンク認証情報を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、マッチングに成功した場合にユーザが認証を得て、認証に成功した後に支払い操作が遂行される。

【０１０５】

任意で、支払い要求は、支払いクライアント端末上でユーザが選択する、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。

【０１０６】

本願の実施の形態は、支払い装置を提供し、端末に適用される。機能面で分けると、装置は、支払い要求送信ユニットと、認証指令受信ユニットと、認証応答送信ユニットとを備え：支払い要求送信ユニットは、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、支払い要求が、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い；認証指令受信ユニットは、ウェアラブルデバイスが、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、サーバによって発行される、ダウンリンク認証情報と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、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；認証応答送信ユニットは、サーバは、アップリンク認証情報に応じてユーザを認証し、認証に成功した後に支払い操作を遂行するために、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し、アップリンク認証情報をサーバへ送信するように構成される。

【０１０７】

任意で、支払いクライアント端末上でのユーザの支払い操作が具体的には、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。

【０１０８】

本願の実施の形態は、ウェアラブルデバイスのための支払い装置を提供し、ウェアラブルデバイスに適用される。機能面で分けると、支払い装置は、支払い認証情報受信ユニットと、アップリンク認証情報生成ユニットとを備え：支払い認証情報受信ユニットは、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、支払い認証情報が、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み；アップリンク認証情報生成ユニットは、サーバはアップリンク認証情報に基づきユーザを認証し、認証に成功した後に支払い操作を遂行するように、支払いクライアント端末がアップリンク認証情報を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、アップリンク認証情報を支払いクライアント端末へ送信するように構成される。

【０１０９】

任意で、支払い装置は、支払いクライアント端末を通じてユーザによって発行される支払い拘束要求に応答して、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。

【０１１０】

上記は単なる本願の好ましい実施の形態であり、それを用いて本願を制限するものではない。本願の精神及び原理から逸脱せずになされるあらゆる改変、均等物との置き換え、改良等は、本願の保護範囲に包含されるものである。

【０１１１】

典型的な構成では、コンピューティングデバイスは１つ以上のプロセッサ（ＣＰＵ）、入／出力インターフェース、ネットワークインターフェース、及びメモリを含む。

【０１１２】

メモリは、揮発性メモリ、ランダムアクセスメモリ（ＲＡＭ）、及び／又は、例えば読出し専用メモリ（ＲＯＭ）又はフラッシュＲＡＭのようなコンピュータで読取り可能な媒体内の不揮発性メモリなどを含んでよい。メモリはコンピュータで読取り可能な媒体の一例である。

【０１１３】

コンピュータで読取り可能な媒体は、不揮発性又は揮発性媒体、可動又は非可動媒体を含み、また、任意の方法あるいは技術によって情報記憶を実行できる。情報はコンピュータで読取り可能な命令、データ構造、及びプログラム又はその他のデータモジュールであってよい。コンピュータの記憶媒体は、例えば、相変化メモリ（ＰＲＡＭ）、スタティックランダムアクセスメモリ（ＳＲＡＭ）、ダイナミックランダムアクセスメモリ（ＤＲＡＭ）、その他のタイプのランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、電気的消去再書込み可能な読出し専用メモリ（ＥＥＰＲＯＭ）、フラッシュメモリ若しくはその他のメモリ技術、コンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、デ

ジタル多目的ディスク（ＤＶＤ）若しくはその他の光学記憶装置、カセットテープ、磁気テープ／磁気ディスク記憶装置若しくはその他の磁気記憶デバイス、又は任意のその他の非伝送媒体を非限定的に含み、また、アクセス可能な情報を保存するためにコンピューティングデバイスを使用できる。本明細書での定義によれば、コンピュータで読取り可能な媒体は、変調データ信号及び搬送波のような一時的媒体を含まない。

【０１１４】

用語「含む」、「備える」、又はこれらのあらゆる派生形は、非排他的な包含をカバーすることを意図し、一連の要素を含む工程、方法、商品、デバイスは、このような要素を含むだけでなく、明記されていないその他の要素をも含むか、あるいは、その工程、方法、商品、デバイスに固有な要素を更に含む点にも留意されたい。さらなる制限をせずに、表現「～を含む（include a/an…）」によって限定される要素は、その要素を含む工程、方法、商品、デバイスが更に有するその他の同じ要素を除外するものではない。

【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。

【図１】

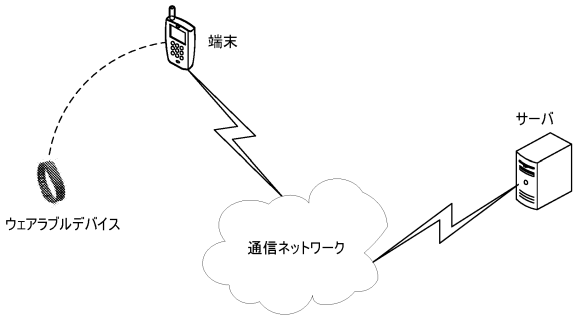

図1

【図２】

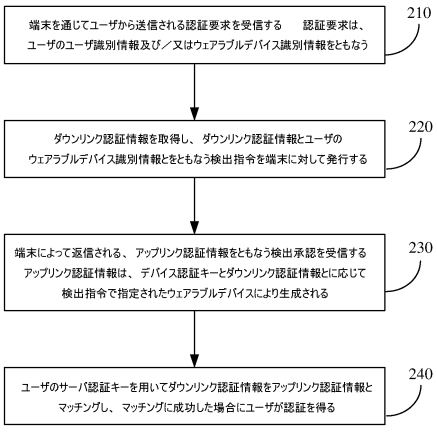

図2

【図３】

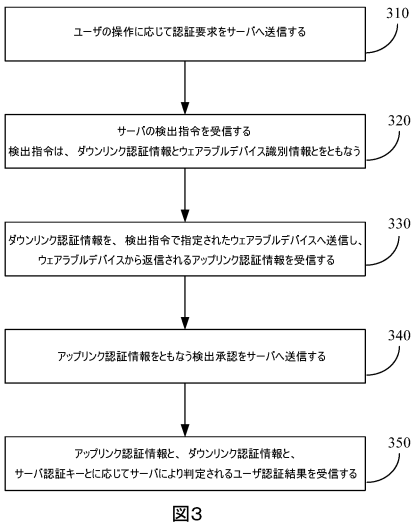

図3

【図４】

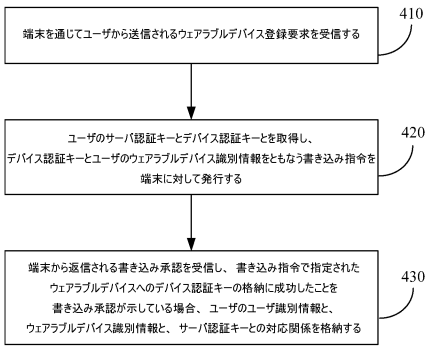

図4

【図５】

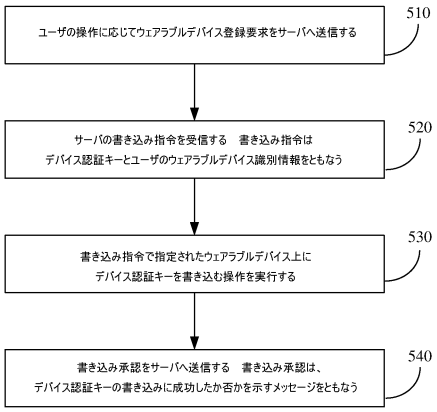

図5

【図６】

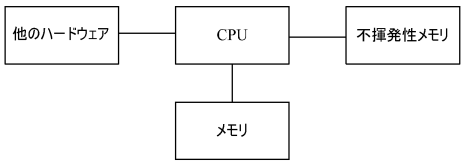

図6

【図７】

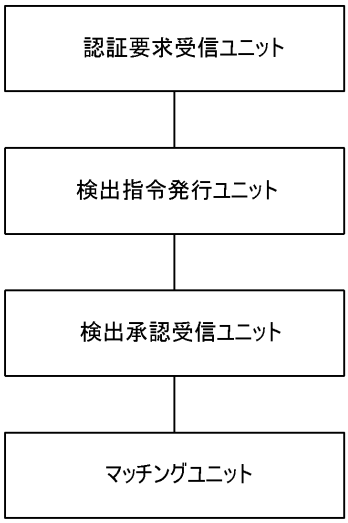

図7

【図８】

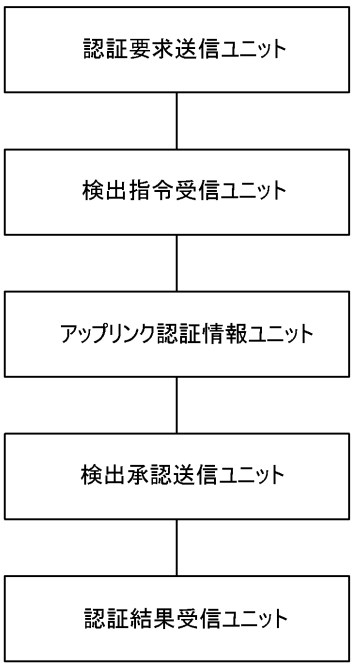

図8

【図９】

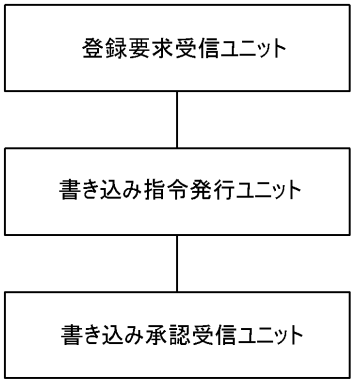
登録要求受信ユニット
書き込み指令発行ユニット
書き込み承認受信ユニット

図9

【図１０】

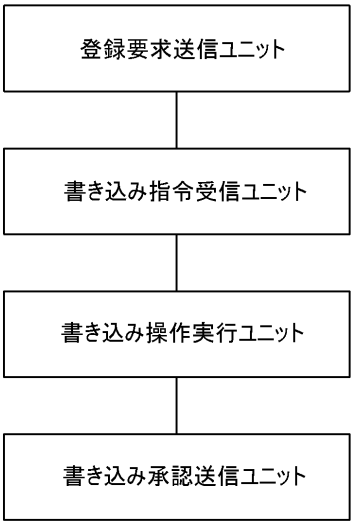
登録要求送信ユニット
書き込み指令受信ユニット
書き込み操作実行ユニット
書き込み承認送信ユニット

図10

フロントページの続き

(72)発明者　ジァン，ロン
中華人民共和国　３１００９９，ハンヂョウ，ナンバー１８　ワンタン　ロード，フアンロン　タイムズ　プラザ，ビルディング　ビー　１７エフ，アンツ　パテント　チーム内

審査官　宮司　卓佳

(56)参考文献　特表２００４－５１８２２９（ＪＰ，Ａ）
特開２００２－３７４２４４（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１５４４６０（ＵＳ，Ａ１）
FIDEL PANIAGUA DIEZ他，TOWARD SELF-AUTHENTICABLE WEARABLE DEVICES，IEEE Wireless Communications，IEEE，２０１５年　2月，p.36-p.43

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３０－２１／４６
Ｇ０６Ｑ　２０／４０
Ｈ０４Ｌ　９／３２