

明 細 書

発明の名称： 認証装置

技術分野

[0001] 本発明の実施形態は、認証装置に関する。

背景技術

[0002] スマートフォン、ドア又はPCなどの機器に無線で接続して機器のロックを解除するウェアラブル端末が提供されている。そのようなウェアラブル端末は、指紋などを用いてユーザを認証して機器のロックを解除する。

[0003] 従来、ウェアラブル端末は、機器のロックを解除する度に指紋などを用いてユーザを認証する必要がある。

先行技術文献

特許文献

[0004] 特許文献1：国際公開第2014／147713号

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するため、ユーザを効果的に認証することができる認証装置を提供する。

課題を解決するための手段

[0006] 実施形態によれば、ユーザを認証する認証装置は、生体センサと、記憶部と、通信インターフェースと、検出機構と、プロセッサと、を備える。生体センサは、生体情報を取得する。記憶部は、認証情報を格納する。通信インターフェースは、外部装置とデータを送受信する。検出機構は、前記認証装置の脱着を検出する。プロセッサは、前記生体センサが取得した生体情報を用いてユーザを認証し、ユーザの認証に成功すると、前記認証情報を前記記憶部に格納し前記認証装置をオフにし、前記通信インターフェースが前記外部装置から磁界を受信すると前記通信インターフェースからの電力を用いて前記認証装置を起動し、前記通信インターフェースを通じて認証コマンドを

受信すると、前記記憶部が前記認証情報を格納している場合、前記通信インターフェースを通じて認証に成功したことを示す認証信号を前記外部装置に送信し、前記検出機構が、前記認証装置がユーザから取り外されたことを検出すると、前記記憶部から前記認証情報を削除する。

図面の簡単な説明

- [0007] [図1]図1は、第1の実施形態に係る認証システムの構成例を示す図である。
- [図2]図2は、第1の実施形態に係るウェアラブル端末の構成例を概略的に示す図である。
- [図3]図3は、第1の実施形態に係るウェアラブル端末の装着例を示す図である。
- [図4]図4は、第1の実施形態に係るウェアラブル端末の構成例を示すブロック図である。
- [図5]図5は、第1の実施形態に係る認証システムの動作例を示すシーケンス図である。
- [図6]図6は、第1の実施形態に係る認証システムの動作例を示すシーケンス図である。
- [図7]図7は、第1の実施形態に係る認証システムの動作例を示すシーケンス図である。
- [図8]図8は、第1の実施形態に係る認証システムの動作例を示すシーケンス図である。
- [図9]図9は、第2の実施形態に係るウェアラブル端末の構成例を概略的に示す図である。
- [図10]図10は、第2の実施形態に係るウェアラブル端末の構成例を示すブロック図である。
- [図11]図11は、第2の実施形態に係る認証システムの動作例を示すシーケンス図である。
- [図12]図12は、第2の実施形態に係る認証システムの動作例を示すシーケンス図である。

実施形態

[0008] 以下、実施形態について、図面を参照して説明する。

(第1の実施形態)

まず、第1の実施形態について説明する。

実施形態に係る認証システムは、所定のユーザが所持するウェアラブル端末とリーダライタとを備える。ウェアラブル端末とリーダライタとが所定の距離に近づくと、両者の間に通信が確立する。ウェアラブル端末は、リーダライタに認証に成功したことを示す認証信号を送信して機器のロックを解除する。

[0009] 図1は、実施形態に係る認証システム1の構成例を示す。図1が示すように、認証システム1は、ウェアラブル端末10とリーダライタ20とを備える。ウェアラブル端末10とリーダライタ20とは、互いに通信可能に接続する。

[0010] ウェアラブル端末10（認証装置）は、ユーザが所持する端末である。ウェアラブル端末10は、リーダライタ20と通信可能な距離に近づくと、リーダライタ20と通信を確立する。ウェアラブル端末10は、予めリーダライタ20とペアリングされているものであってもよい。ここでは、ウェアラブル端末10は、腕時計型の端末である。ウェアラブル端末10については、後に詳述する。

[0011] リーダライタ20（外部装置）は、ウェアラブル端末10と非接触でデータを送受信するためのインターフェース装置である。

[0012] リーダライタ20は、ウェアラブル端末10との無線通信を行うためのアンテナ及び通信制御部などにより構成される。リーダライタ20は、ウェアラブル端末10に対する電源供給、クロック供給、リセット制御及びデータの送受信などを行う。

[0013] このような機能によってリーダライタ20は、ウェアラブル端末10に対する電源供給、ウェアラブル端末10の活性化（起動）、クロック供給、リセット制御、種々のコマンドの送信及び送信したコマンドに対する応答（レ

スポンズ)の受信などを行なう。

[0014] リーダライタ20は、ウェアラブル端末10と通信を確立すると、ユーザを認証するコマンドを送信する。リーダライタ20は、コマンドに対するレスポンスとして、ユーザの認証結果を示すレスポンスを受信する。リーダライタ20は、当該レスポンスを自身に接続する機器に送信する。

当該レスポンスが認証に成功したことを示す場合、機器は、ロックを解除する。たとえば、機器は、スマートフォン、ドア又はPCなどである。なお、機器とリーダライタ20とは、一体的に形成されるものであってもよい。

[0015] 次に、ウェアラブル端末10について説明する。

図2は、ウェアラブル端末10の外観を示す。図2が示すように、ウェアラブル端末10は、バンド11、装着機構12、スイッチ13、アンテナ14、取外機構15、バッテリー16、指紋センサ17、表示機構18及び取外機構19などを備える。

[0016] バンド11は、ウェアラブル端末10の外形を構成する。バンド11は、所定の長さに帯状に形成されている。バンド11は、ユーザの腕に巻き付く。たとえば、バンド11は、ゴム、シリコン又は皮などから構成される。

[0017] バンド11の一端には、装着機構12が設置されている。装着機構12は、ユーザがバンド11を手首に固定するために用いられる部材である。装着機構12は、取外機構19を挿入可能な大きさのリング状の部材である。装着機構12は、取外機構19を挿入されることでユーザの手首にウェアラブル端末10を固定する。

[0018] 装着機構12の内側には、スイッチ13が設置されている。スイッチ13は、取外機構19が装着機構12を通過すると押下される。即ち、スイッチ13は、ユーザがウェアラブル端末10を装着した又は取り外した場合に押下される。スイッチ13は、ウェアラブル端末10の脱着を検出する検出機構として機能する。

[0019] なお、スイッチ13は、トグルスイッチであってもよい。また、スイッチ13は、取外機構19と接触することでオンになるものであってもよい。

[0020] アンテナ１４（通信インターフェース）は、リーダライタ２０とデータを送受信するためのアンテナである。また、アンテナ１４は、リーダライタ２０からの電波によって電力を供給する電源として機能する。

たとえば、アンテナ１４は、Bluetooth（登録商標）接続又はNFC（Near Field Communication）接続をサポートする。

[0021] 取外機構１５は、バンド１１において装着機構１２に近い位置に形成されている。取外機構１５は、ウェアラブル端末１０を脱着するための部材である。取外機構１５は、取外機構１９と脱着可能である。取外機構１５は、装着機構１２を通過した取外機構１９に固定することでウェアラブル端末１０をユーザの手首に固定する。

[0022] バッテリ１６は、ウェアラブル端末１０の各部へ電力を供給する。バッテリー１６は、外部から充電可能な二次電池であってもよい。たとえば、バッテリー１６は、アンテナ１４からの電力によって充電される。また、バッテリー１６は、使い捨てのバッテリーであってもよい。

[0023] 指紋センサ１７（生体センサ）は、バンド１１において装着機構１２に対抗する他端の近くに設置されている。指紋センサ１７は、バンド１１の内側（ユーザの手首に接触する側）に設置されている。

[0024] 指紋センサ１７は、ユーザの手指のいずれかの指から指紋（指紋画像）を取得する。指紋センサ１７は、指から取得した指紋を示す指紋情報を後述するプロセッサ１１１に送信する。指紋情報は、指紋画像であってもよい。また、指紋情報は、指紋画像の特徴量などであってもよい。

[0025] たとえば、指紋センサ１７は、指紋を撮影するための光学センサなどから構成される。また、指紋センサ１７は、静電容量を検出するセンサなどから構成されるものであってもよい。

[0026] 表示機構１８は、プロセッサ１１１から制御に基づいてユーザに情報を表示する。たとえば、表示機構１８は、LED（Light Emitting Diode）などのランプから構成される。また、表示機構１８は、液晶モニタから構成されるものであってもよい。

[0027] 取外機構 19 は、バンド 11 において装着機構 12 と対抗する他端に設置されている。取外機構 19 は、ウェアラブル端末 10 を脱着するための部材である。取外機構 19 は、取外機構 15 と脱着可能である。前述の通り、取外機構 19 は、装着機構 12 を通過した状態で取外機構 15 に固定することでウェアラブル端末 10 をユーザの手首に固定する。

なお、スイッチ 13 は、取外機構 19 に設置されるものであってもよい。

[0028] 図 3 は、ウェアラブル端末 10 がユーザの手首に装着される状態を示す。図 3 が示すように、ユーザは、バンド 11 を手首に巻いた状態で取外機構 19 を装着機構 12 に挿入する。取外機構 19 が装着機構 12 に挿入されると、指紋センサ 17 及び表示機構 18 は、ユーザに向く。ユーザは、取外機構 19 を取外機構 15 に固定することで自身の手首にウェアラブル端末 10 を装着する。

[0029] 次に、ウェアラブル端末 10 の制御系について説明する。

図 4 は、ウェアラブル端末 10 の制御系を示すブロック図である。図 4 が示すように、ウェアラブル端末 10 は、プロセッサ 111、ROM 112、RAM 113、NVM 114、通信部 115、スイッチ 13、アンテナ 14、バッテリー 16、指紋センサ 17 及び表示機構 18 などを備える。

[0030] プロセッサ 111 と、ROM 112、RAM 113、NVM 114、通信部 115、スイッチ 13、アンテナ 14、バッテリー 16、指紋センサ 17 及び表示機構 18 と、は、データバスなどを介して互いに接続する。

[0031] スwitch 13、アンテナ 14、バッテリー 16、指紋センサ 17 及び表示機構 18 は、前述の通りである。

[0032] プロセッサ 111 は、ウェアラブル端末 10 全体の動作を制御する機能を有する。プロセッサ 111 は、内部キャッシュ及び各種のインターフェースなどを備えてもよい。プロセッサ 111 は、内部メモリ、ROM 112 又は NVM 114 が予め記憶するプログラムを実行することにより種々の処理を実現する。

[0033] なお、プロセッサ 111 がプログラムを実行することにより実現する各種

の機能のうちの一部は、ハードウェア回路により実現されるものであってもよい。この場合、プロセッサ 111 は、ハードウェア回路により実行される機能を制御する。

[0034] ROM 112 は、制御プログラム及び制御データなどが予め記憶された不揮発性のメモリである。ROM 112 に記憶される制御プログラム及び制御データは、ウェアラブル端末 10 の仕様に応じて予め組み込まれる。

[0035] RAM 113 は、揮発性のメモリである。RAM 113 は、プロセッサ 111 の処理中のデータなどを一時的に格納する。RAM 113 は、プロセッサ 111 からの命令に基づき種々のアプリケーションプログラムを格納する。また、RAM 113 は、アプリケーションプログラムの実行に必要なデータ及びアプリケーションプログラムの実行結果などを格納してもよい。

[0036] NVM 114（記憶部）は、データの書き込み及び書き換えが可能な不揮発性のメモリである。NVM 114 は、たとえば、HDD（Hard Disk Drive）、SSD（Solid State Drive）又はフラッシュメモリなどから構成される。NVM 114 は、ウェアラブル端末 10 の運用用途に応じて制御プログラム、アプリケーション及び種々のデータなどを格納する。

[0037] また、NVM 114 は、ユーザを認証するためのテンプレートを格納する記憶領域 114a 及び認証に成功したことを示す認証情報を格納する記憶領域 114b などを備える。

[0038] テンプレートは、指紋センサ 17 が取得する指紋情報に対応するテンプレートである。ここでは、テンプレートは、指紋認証を行うためのテンプレートである。たとえば、テンプレートは、ユーザの指紋画像、指紋画像の特徴量又は指紋認証のためのネットワークなどから構成される。

[0039] 認証情報は、プロセッサ 111 が指紋認証に成功したことを示す。たとえば、認証情報は、フラグなどであってもよい。たとえば、記憶領域 114b は、認証情報として、「1」を格納する。

[0040] 通信部 115 は、外部装置とデータを送受信するインターフェースである。たとえば、通信部 115 は、有線又は無線の LAN（Local Area Network

）接続をサポートするものであってもよい。

[0041] なお、ウェアラブル端末１０は、図３及び図４が示すような構成の他に必要に応じた構成を具備したり、ウェアラブル端末１０から特定の構成が除外されたりしてもよい。

[0042] 次に、ウェアラブル端末１０が実現する機能について説明する。プロセッサ１１１が実現する機能は、プロセッサ１１１が内部メモリ、ROM１１２又はNVM１１４などに格納されるプログラムを実行することで実現される。

[0043] まず、プロセッサ１１１は、テンプレートを登録する機能を有する。

ここでは、ユーザは、ウェアラブル端末１０のバンド１１を手首に巻いて取外機構１９を装着機構１２に挿入するものとする。即ち、ユーザは、ウェアラブル端末１０を図３が示す状態にする。

[0044] 取外機構１９が装着機構１２を通過することでスイッチ１３が押下される。スイッチ１３が押下されると、プロセッサ１１１は、バッテリー１６からの電力を用いてウェアラブル端末１０を起動する。ウェアラブル端末１０を起動すると、プロセッサ１１１は、記憶領域１１４aがテンプレートを格納しているかを判定する。

[0045] 記憶領域１１４aがテンプレートを格納していないと判定した場合、プロセッサ１１１は、テンプレートを登録する。

[0046] プロセッサ１１１は、指紋センサ１７に指紋情報を取得させる。ここで、ユーザは、指紋センサ１７に指を接触させる。

[0047] プロセッサ１１１は、指紋センサ１７から指紋情報を取得する。指紋情報を取得すると、プロセッサ１１１は、所定のアルゴリズムに従って、取得された指紋情報からテンプレートを生成する。テンプレートを生成すると、プロセッサ１１１は、生成されたテンプレートを記憶領域１１４aに格納する。

[0048] また、プロセッサ１１１は、指紋センサ１７を用いた指紋認証に成功すると認証情報を格納する機能を有する。

- [0049] ここでは、ユーザは、ウェアラブル端末10のバンド11を手首に巻いて取外機構19を装着機構12に挿入するものとする。即ち、ユーザは、ウェアラブル端末10を図3が示す状態にする。また、記憶領域114aは、テンプレートを格納しているものとする。また、記憶領域114bは、認証情報を格納していないものとする。
- [0050] 取外機構19が装着機構12を通過することでスイッチ13が押下される。スイッチ13が押下されると、プロセッサ111は、バッテリー16からの電力を用いてウェアラブル端末10を起動する。ウェアラブル端末10を起動すると、プロセッサ111は、記憶領域114aがテンプレートを格納しているかを判定する。
- [0051] 記憶領域114aがテンプレートを格納していると判定した場合、プロセッサ111は、記憶領域114bが認証情報を格納しているかを判定する。記憶領域114bが認証情報を格納していないと判定した場合、プロセッサ111は、指紋認証を行う。
- [0052] プロセッサ111は、指紋センサ17に指紋情報を取得させる。ここで、ユーザは、指紋センサ17に指を接触させる。
- [0053] 指紋情報を取得すると、プロセッサ111は、所定のアルゴリズムに従って、記憶領域114aが格納するテンプレートと取得された指紋情報とを比較する。プロセッサ111は、テンプレートと指紋情報とが整合（同定）する場合、指紋認証に成功したと判定する。
- [0054] 指紋認証に成功したと判定すると、プロセッサ111は、記憶領域114bに認証情報を格納する。なお、プロセッサ111は、指紋認証に成功したことを示す情報を表示機構18に表示してもよい。
- [0055] 記憶領域114bに認証情報を格納すると、プロセッサ111は、ウェアラブル端末10をオフにする。後述するように、プロセッサ111は、リーダライタ20からの磁界によって起動可能な状態に移行する。
- [0056] また、プロセッサ111は、テンプレートと指紋情報とが整合しない場合、指紋認証に失敗したと判定する。指紋認証に失敗したと判定すると、プロ

セッサ１１１は、動作を終了する。なお、プロセッサ１１１は、指紋認証に失敗したことを示す情報を表示機構１８に表示してもよい。

[0057] また、プロセッサ１１１は、記憶領域１１４ｂが認証情報を格納している間において、認証に成功したことを示す認証信号をリーダライタ２０に送信する機能を有する。

[0058] ここで、ユーザは、ウェアラブル端末１０をリーダライタ２０の通信範囲に翳すものとする。また、リーダライタ２０は、磁界を出力するものとする。

[0059] アンテナ１４は、リーダライタ２０から磁界を受信する。磁界を受信すると、アンテナ１４は、磁界により生じた電力を供給する。アンテナ１４が電力の供給を開始すると、プロセッサ１１１は、アンテナ１４からの電力を用いてウェアラブル端末１０を起動する。

[0060] ここで、リーダライタ２０は、ユーザを認証する認証コマンドをウェアラブル端末１０に送信するものとする。

[0061] プロセッサ１１１は、アンテナ１４を通じて認証コマンドを受信する。認証コマンドを受信すると、プロセッサ１１１は、記憶領域１１４ｂが認証情報を格納しているかを判定する。

[0062] 記憶領域１１４ｂが認証情報を格納していると判定した場合、プロセッサ１１１は、アンテナ１４を通じて、認証に成功したことを示すレスポンス（認証信号）をリーダライタ２０に送信する。なお、認証信号は、ウェアラブル端末のＩＤなどを格納するものであってもよい。

[0063] なお、プロセッサ１１１は、アンテナ１４を通じて、ウェアラブル端末１０のＮＶＭ１１４が格納するＩＤ（ウェアラブル端末１０のＩＤ）を要求するコマンドをリーダライタ２０から受信するものであってもよい。記憶領域１１４ｂが認証情報を格納している場合、プロセッサ１１１は、アンテナ１４を通じて、当該ＩＤを含むレスポンスをリーダライタ２０に送信する。

[0064] なお、記憶領域１１４ｂが認証情報を格納していないと判定した場合、プロセッサ１１１は、アンテナ１４を通じて、認証に失敗したことを示すレス

ポンスをリーダライタ 20 に送信する。

[0065] また、プロセッサ 111 は、ユーザの手首からウェアラブル端末 10 が取り外されると認証情報を削除する機能を有する。

[0066] ここで、ユーザは、自信の手首からウェアラブル端末 10 を取り外す。即ち、ユーザは、取外機構 19 を取外機構 15 から外す。また、ユーザは、取外機構 19 を装着機構 12 から抜き出す。

また、記憶領域 114 a は、テンプレートを格納しているものとする。また、記憶領域 114 b は、認証情報を格納しているものとする。

[0067] 取外機構 19 が装着機構 12 を通過することでスイッチ 13 が押下される。即ち、スイッチ 13 は、ウェアラブル端末 10 がユーザから取り外されたことを検出する。スイッチ 13 が押下されると、プロセッサ 111 は、バッテリー 16 からの電力を用いてウェアラブル端末 10 を起動する。ウェアラブル端末 10 を起動すると、プロセッサ 111 は、記憶領域 114 a がテンプレートを格納しているかを判定する。

[0068] 記憶領域 114 a がテンプレートを格納していると判定した場合、プロセッサ 111 は、記憶領域 114 b が認証情報を格納しているかを判定する。記憶領域 114 b が認証情報を格納していると判定した場合、プロセッサ 111 は、記憶領域 114 b から認証情報を削除する。

[0069] なお、プロセッサ 111 は、センサなどを用いて取外機構 19 が取外機構 15 から取り外されたことを検知した場合に、記憶領域 114 b から認証情報を削除してもよい。

[0070] 次に、認証システム 1 の動作例について説明する。

まず、認証システム 1 がテンプレートを登録する動作例について説明する。

図 5 は、認証システム 1 がテンプレートを登録する動作例について説明するためのシーケンス図である。

[0071] ここでは、記憶領域 114 a は、テンプレートを格納していないものとする。

- [0072] まず、ユーザは、ウェアラブル端末10を装着する(S11)。ここでは、ユーザは、ウェアラブル端末10を図3の状態にする。
- [0073] ユーザがウェアラブル端末10を装着すると、ウェアラブル端末10のスイッチ13が押下される(S12)。スイッチ13が押下されると、プロセッサ111は、バッテリー16からの電力を用いてウェアラブル端末10を起動する。
- [0074] ウェアラブル端末10を起動すると、プロセッサ111は、指紋センサ17に指紋情報を取得させる(S13)。ここで、ユーザは、自身の指を指紋センサ17に接触させる。指紋センサ17は、ユーザの指から取得した指紋情報をプロセッサ111に送信する(S14)。
- [0075] プロセッサ111は、指紋センサ17からユーザの指紋情報を取得する。指紋情報を取得すると、プロセッサ111は、取得された指紋情報に基づいてテンプレートを生成する(S15)。
- [0076] テンプレートを生成すると、プロセッサ111は、生成されたテンプレートを記憶領域114aに格納する(S16)。生成されたテンプレートを記憶領域114aに格納すると、プロセッサ111は、ウェアラブル端末10をオフにする(S17)。
- [0077] プロセッサ111がウェアラブル端末10をオフにすると、認証システム1は、動作を終了する。
- [0078] 次に、認証システム1が認証情報を格納する動作例について説明する。
図6は、認証システム1が認証情報を格納する動作例について説明するためのシーケンス図である。
- [0079] ここでは、記憶領域114aは、テンプレートを格納しているものとする。また、記憶領域114bは、認証情報を格納していないものとする。
- [0080] まず、ユーザは、ウェアラブル端末10を装着する(S21)。ここでは、ユーザは、ウェアラブル端末10を図3の状態にする。
- [0081] ユーザがウェアラブル端末10を装着すると、ウェアラブル端末10のスイッチ13が押下される(S22)。スイッチ13が押下されると、プロセ

ッサ１１１は、バッテリー１６からの電力を用いてウェアラブル端末１０を起動する。

[0082] ウェアラブル端末１０を起動すると、プロセッサ１１１は、指紋センサ１７に指紋情報を取得させる（Ｓ２３）。ここで、ユーザは、自身の指を指紋センサ１７に接触させる。指紋センサ１７は、ユーザの指から取得した指紋情報をプロセッサ１１１に送信する（Ｓ２４）。

[0083] プロセッサ１１１は、指紋センサ１７からユーザの指紋情報を取得する。指紋情報を取得すると、プロセッサ１１１は、テンプレートと取得された指紋情報と比較して指紋認証を行う（Ｓ２５）。ここでは、プロセッサ１１１は、指紋認証に成功したものとする。

[0084] 指紋認証を行うと、プロセッサ１１１は、認証情報を記憶領域１１４ｂに格納する（Ｓ２６）。認証情報を記憶領域１１４ｂに格納すると、プロセッサ１１１は、ウェアラブル端末１０をオフにする（Ｓ２７）。

[0085] プロセッサ１１１がウェアラブル端末１０をオフにすると、認証システム１は、動作を終了する。

なお、プロセッサ１１１が指紋認証に失敗した場合、認証システム１は、動作を終了する。

[0086] 次に、認証システム１がユーザを認証する動作例について説明する。

図７は、認証システム１がユーザを認証する動作例について説明するためのシーケンス図である。

[0087] ここでは、ユーザは、自身の手首にウェアラブル端末１０を装着しているものとする。また、記憶領域１１４ｂは、認証情報を格納しているものとする。

[0088] ユーザは、ウェアラブル端末１０をリーダライタ２０に翳す（Ｓ３１）。ユーザがウェアラブル端末１０をリーダライタ２０に翳すと、リーダライタ２０は、磁界をウェアラブル端末１０に出力する（Ｓ３２）。なお、リーダライタ２０は、磁界を出力し続けるものであってもよい。

[0089] リーダライタ２０が磁界を出力すると、アンテナ１４は、電力を供給する

(S 3 3)。アンテナ 1 4 が電力の供給を開始すると、プロセッサ 1 1 1 は、アンテナ 1 4 からの電力を用いてウェアラブル端末 1 0 を起動する。

[0090] ウェアラブル端末 1 0 を起動すると、プロセッサ 1 1 1 は、アンテナ 1 4 を通じて初期応答をリーダライタ 2 0 に送信する (S 3 4)。リーダライタ 2 0 は、ウェアラブル端末 1 0 から初期応答を受信する。

[0091] 初期応答を受信すると、リーダライタ 2 0 は、認証コマンドをウェアラブル端末 1 0 に送信する (S 3 5)。ウェアラブル端末 1 0 のプロセッサ 1 1 1 は、アンテナ 1 4 を通じて認証コマンドを受信する。

[0092] 認証コマンドを受信すると、プロセッサ 1 1 1 は、アンテナ 1 4 を通じて認証に成功したことを示すレスポンスをリーダライタ 2 0 に送信する (S 3 6)。リーダライタ 2 0 は、ウェアラブル端末 1 0 から当該レスポンスを受信する。

[0093] リーダライタ 2 0 が当該レスポンスを受信すると、認証システム 1 は、動作を終了する。

なお、記憶領域 1 1 4 b が認証情報を格納していない場合、プロセッサ 1 1 1 は、認証コマンドに対して認証に失敗したことを示すレスポンスを送信する。

[0094] 次に、認証システム 1 が認証情報を削除する動作例について説明する。

図 8 は、認証システム 1 が認証情報を削除する動作例について説明するためのシーケンス図である。

[0095] ここでは、記憶領域 1 1 4 a は、テンプレートを格納しているものとする。また、記憶領域 1 1 4 b は、認証情報を格納しているものとする。

[0096] ユーザは、自信の手首からウェアラブル端末 1 0 を取り外す (S 4 1)。即ち、ユーザは、取外機構 1 9 を装着機構 1 2 から引き抜く。取外機構 1 9 が装着機構 1 2 から引き抜かれると、スイッチ 1 3 が押下される (S 4 2)。スイッチ 1 3 が押下されると、プロセッサ 1 1 1 は、バッテリー 1 6 からの電力を用いてウェアラブル端末 1 0 を起動する。

[0097] ウェアラブル端末 1 0 を起動すると、プロセッサ 1 1 1 は、記憶領域 1 1

4 b から認証情報を削除する (S 4 3)。認証情報を削除すると、プロセッサ 1 1 1 は、ウェアラブル端末 1 0 をオフにする (S 4 4)。

プロセッサ 1 1 1 がウェアラブル端末 1 0 をオフにすると、認証システム 1 は、動作を終了する。

[0098] なお、スイッチ 1 3 は、取外機構 1 9 に設置されるものであってもよい。この場合、スイッチ 1 3 は、取外機構 1 9 が装着機構 1 2 を通過する際に押下される。

[0099] また、スイッチ 1 3 は、バンド 1 1 の内側に設置されるものであってもよい。この場合、スイッチ 1 3 は、バンド 1 1 がユーザの手首に巻き付くと押下される。

[0100] また、スイッチ 1 3 は、ユーザが装着する際又は取り外す際に押下するものであってもよい。

[0101] また、プロセッサ 1 1 1 は、アンテナ 1 4 からの電力の供給とスイッチ 1 3 への押下とが競合する場合、バッテリー 1 6 の電力を用いてウェアラブル端末 1 0 を起動してもよい。

[0102] また、ウェアラブル端末 1 0 は、指紋認証を行うための M P U (micro processing unit) を備えてもよい。この場合、プロセッサ 1 1 1 は、指紋センサ 1 7 が取得した指紋情報を M P U に送信する。M P U は、指紋センサ 1 7 からの指紋情報に基づいて指紋認証を行い、指紋認証の結果をプロセッサ 1 1 1 に送信する。たとえば、M P U は、S E (Secure Element) などである。

[0103] また、プロセッサ 1 1 1 は、指紋以外の生体情報を用いてユーザを認証してもよい。この場合、ウェアラブル端末は、生体センサを備える。たとえば、生体情報は、顔画像、静脈、虹彩、声紋又は筆跡などである。生体情報は、特定の構成に限定されるものではない。

[0104] 以上のように構成されたウェアラブル端末は、装着時にユーザを認証して認証情報を格納する。ウェアラブル端末は、認証情報を格納した状態でオフになる。ウェアラブル端末は、リーダライタからの磁場で起動すると、認証

信号をリーダライタに送信する。その結果、ウェアラブル端末は、装置のロックを解除する度にユーザを認証しなくとも認証信号をリーダライタに送信することができる。また、ウェアラブル端末は、認証情報を格納した後にオフなることで消費電力を抑制することができる。

[0105] また、ウェアラブル端末は、取外時に認証情報を削除する。その結果、ウェアラブル端末は、認証情報を保持した状態で他者に受け渡されることを防止する。よって、ウェアラブル端末は、他者に不正に利用されて機器のロックを解除してしまうことを防止することができる。

(第2の実施形態)

次に、第2の実施形態について説明する。

第2の実施形態に係る認証システムは、ウェアラブル端末10が接触センサを用いてユーザが自身から離れたことを検出すると認証情報を削除する点で第1の実施形態に係るそれと異なる。従って、その他の点については、同一の符号を付して詳細な説明を省略する。

[0106] 図1は、第2の実施形態に係る認証システム1'の構成例を示す。図1が示すように、認証システム1'は、ウェアラブル端末10'とリーダライタ20とを備える。ウェアラブル端末10'とリーダライタ20とは、互いに通信可能に接続する。

[0107] 図9は、ウェアラブル端末10'の外観を示す。図2が示すように、ウェアラブル端末10は、バンド11、装着機構12、スイッチ13、アンテナ14、取外機構15、バッテリー16、指紋センサ17、表示機構18、取外機構19及び接触センサ31などを備える。

[0108] 接触センサ31は、ウェアラブル端末10'がユーザに身に付けられていることを検出する。即ち、接触センサ31は、ウェアラブル端末10'とユーザとの接触を検出する。

[0109] 接触センサ31は、ユーザとの接触（又は、非接触）を示すセンサ信号をプロセッサ111に送信する。なお、接触センサ31は、接触の有無を判定するためのパラメータをプロセッサ111に送信してもよい。

- [0110] たとえば、接触センサ31は、ユーザのバイタル（体温又は脈拍など）を検出するセンサである。また、接触センサ31は、超音波センサ、光学センサ（赤外線センサなど）、圧力センサ又は通電センサなど、ユーザ（又はユーザの皮膚）との接触を検出するものであってもよい。接触センサ31の構成は、特定の構成に限定されるものではない。
- [0111] 図10は、ウェアラブル端末10'の制御系を示すブロック図である。図10が示すように、ウェアラブル端末10'は、プロセッサ111、ROM112、RAM113、NVM114、通信部115、スイッチ13、アンテナ14、バッテリー16、指紋センサ17、表示機構18及び接触センサ31などを備える。
- [0112] プロセッサ111と、プロセッサ111、ROM112、RAM113、NVM114、通信部115、スイッチ13、アンテナ14、バッテリー16、指紋センサ17、表示機構18及び接触センサ31と、は、データバスなどを介して互いに接続する。
- [0113] なお、ウェアラブル端末10'は、図9及び図10が示すような構成の他に必要に応じた構成を具備したり、ウェアラブル端末10'から特定の構成が除外されたりしてもよい。
- [0114] 次に、ウェアラブル端末10'が実現する機能について説明する。プロセッサ111が実現する機能は、プロセッサ111が内部メモリ、ROM112又はNVM114などに格納されるプログラムを実行することで実現される。
- [0115] ウェアラブル端末10'が実現する機能は、ウェアラブル端末10が実現する機能に加えて以下の機能を実現する。
- [0116] プロセッサ111は、ユーザがウェアラブル端末10に接触している状態で指紋認証を行う機能を有する。
- [0117] ここでは、ユーザは、ウェアラブル端末10のバンド11を手首に巻いて取外機構19を装着機構12に挿入するものとする。即ち、ユーザは、ウェアラブル端末10を図3が示す状態にする。また、記憶領域114aは、テ

ンプレートを格納しているものとする。また、記憶領域 114b は、認証情報を格納していないものとする。

- [0118] 取外機構 19 が装着機構 12 を通過することでスイッチ 13 が押下される。スイッチ 13 が押下されると、プロセッサ 111 は、バッテリー 16 からの電力を用いてウェアラブル端末 10 を起動する。ウェアラブル端末 10 を起動すると、プロセッサ 111 は、記憶領域 114a がテンプレートを格納しているかを判定する。
- [0119] 記憶領域 114a がテンプレートを格納していると判定した場合、プロセッサ 111 は、記憶領域 114b が認証情報を格納しているかを判定する。記憶領域 114b が認証情報を格納していないと判定した場合、プロセッサ 111 は、接触センサ 31 にユーザとの接触を検出させる。
- [0120] 接触センサ 31 は、ユーザとの接触（又は、非接触）を示すセンサ信号をプロセッサ 111 に送信する。ここでは、接触センサ 31 は、ユーザとの接触を示すセンサ信号をプロセッサ 111 に送信する。
- [0121] プロセッサ 111 は、ユーザとの接触を示すセンサ信号を接触センサ 31 から受信する。当該センサ信号を受信すると、プロセッサ 111 は、指紋認証を行う。指紋認証及び指紋認証以後の動作は、第 1 の実施形態のそれと同様であるため説明を省略する。
- [0122] また、プロセッサ 111 は、ユーザがウェアラブル端末 10 と離れると、認証情報を削除する機能を有する。
- [0123] ここでは、記憶領域 114b は、認証情報を格納しているものとする。
- [0124] プロセッサ 111 は、接触センサ 31 からのセンサ信号に基づいてユーザが接触センサ 31 から離れたかを判定する。即ち、プロセッサ 111 は、センサ信号がユーザとの非接触を示すかを判定する。
- [0125] ユーザが接触センサ 31 から離れたと判定すると、プロセッサ 111 は、記憶領域 114b から認証情報を削除する。なお、プロセッサ 111 は、ユーザが接触センサ 31 から所定の期間離れたと判定した場合に記憶領域 114b から認証情報を削除してもよい。

- [0126] 次に、認証システム 1' の動作例について説明する。
- [0127] 認証システム 1' がテンプレートを登録する動作例は、第 1 の実施形態に係るそれと同様であるため説明を省略する。
- [0128] 次に、認証システム 1' が認証情報を格納する動作例について説明する。
- 図 11 は、認証システム 1' が認証情報を格納する動作例について説明するためのシーケンス図である。
- [0129] ここでは、記憶領域 114 a は、テンプレートを格納しているものとする。また、記憶領域 114 b は、認証情報を格納していないものとする。
- [0130] まず、ユーザは、ウェアラブル端末 10' を装着する (S41)。ここでは、ユーザは、ウェアラブル端末 10' を図 3 の状態にする。
- [0131] ユーザがウェアラブル端末 10' を装着すると、ウェアラブル端末 10' のスイッチ 13 が押下される (S42)。スイッチ 13 が押下されると、プロセッサ 111 は、バッテリー 16 からの電力を用いてウェアラブル端末 10' を起動する。
- [0132] ウェアラブル端末 10' を起動すると、プロセッサ 111 は、接触センサ 31 にユーザとの接触を検出させる (S43)。接触センサ 31 は、センサ信号をプロセッサ 111 に送信する (S44)。
- [0133] ここでは、接触センサ 31 は、ユーザとの接触を示すセンサ信号をプロセッサ 111 に送信するものとする。
- [0134] プロセッサ 111 は、当該センサ信号を受信する。当該センサ信号を受信すると、プロセッサ 111 は、指紋センサ 17 に指紋情報を取得させる (S45)。ここで、ユーザは、自身の指を指紋センサ 17 に接触させる。指紋センサ 17 は、ユーザの指から取得した指紋情報をプロセッサ 111 に送信する (S46)。
- [0135] プロセッサ 111 は、指紋センサ 17 からユーザの指紋情報を取得する。指紋情報を取得すると、プロセッサ 111 は、テンプレートと取得された指紋情報と比較して指紋認証を行う (S47)。ここでは、プロセッサ 111 は、指紋認証に成功したものとする。

[0136] 指紋認証を行うと、プロセッサ 111 は、認証情報を記憶領域 114 b に格納する (S 48)。

[0137] プロセッサ 111 が認証情報を記憶領域 114 a に格納すると、認証システム 1' は、動作を終了する。

また、接触センサ 31 がユーザとの非接触を示すセンサ信号を送信した場合、プロセッサ 111 は、動作を終了してもよい。また、この場合、プロセッサ 111 は、接触センサ 31 がユーザとの接触を示すセンサ信号を送信するまで待機してもよい。

[0138] また、プロセッサ 111 が指紋認証に失敗した場合、認証システム 1' は、動作を終了する。

[0139] 認証システム 1' がユーザを認証する動作例は、第 1 の実施形態に係るそれと同様であるため説明を省略する。

[0140] 次に、認証システム 1' が認証情報を削除する動作例について説明する。

図 12 は、認証システム 1 が認証情報を削除する動作例について説明するためのシーケンス図である。

[0141] ここでは、記憶領域 114 a は、テンプレートを格納しているものとする。また、記憶領域 114 b は、認証情報を格納しているものとする。

[0142] ここで、ユーザは、手首と接触センサ 31 とを離すものとする。

[0143] 接触センサ 31 は、ユーザとの非接触を示すセンサ信号をプロセッサ 111 に送信する (S 51)。プロセッサ 111 は、当該センサ信号を受信する。

[0144] 当該センサ信号を受信すると、プロセッサ 111 は、記憶領域 114 b から認証情報を削除する (S 52)。

プロセッサ 111 が認証情報を削除すると、認証システム 1 は、動作を終了する。

[0145] なお、プロセッサ 111 は、認証情報を削除した後にウェアラブル端末 10' をオフにしてもよい。

[0146] また、プロセッサ 111 は、第 1 の実施形態と同様に S 41 乃至 S 44 の

動作により認証情報を削除してもよい。

- [0147] また、接触センサ31は、ユーザと接触している間において所定のセンサ信号をプロセッサ111に送信するものであってもよい。接触センサ31は、ユーザと離れるとセンサ信号を送信しないものであってもよい。
- [0148] また、接触センサ31は、ユーザと離れている間において所定のセンサ信号をプロセッサ111に送信するものであってもよい。接触センサ31は、ユーザと接触するとセンサ信号を送信しないものであってもよい。
- [0149] 以上のように構成されたウェアラブル端末は、接触センサによりユーザから離れたことを検出すると認証情報を削除する。その結果、ウェアラブル端末は、認証情報を保持した状態で他者に受け渡されることをより効果的に防止することができる。
- [0150] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。