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

特許第6535548号
(P6535548)

(45)発行日　令和1年6月26日(2019.6.26)　(24)登録日　令和1年6月7日(2019.6.7)

| (51)Int.Cl. | | | F I | | |
|---|---|---|---|---|---|
| G06T | 1/00 | (2006.01) | G06T | 1/00 | 400H |
| A61B | 5/1171 | (2016.01) | A61B | 5/1171 | 100 |
| G06T | 7/00 | (2017.01) | G06T | 7/00 | 510E |

請求項の数 6　(全 20 頁)

(21)出願番号　特願2015-168466(P2015-168466)
(22)出願日　平成27年8月28日(2015.8.28)
(65)公開番号　特開2017-45346(P2017-45346A)
(43)公開日　平成29年3月2日(2017.3.2)
審査請求日　平成29年11月22日(2017.11.22)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100098660
弁理士　戸田　裕二
(72)発明者　長坂　晃朗
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　三浦　直人
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　松田　友輔
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

最終頁に続く

(54)【発明の名称】生体認証装置および方法

(57)【特許請求の範囲】

【請求項１】

手首に装着されるバンド部を備える生体認証装置において、

前記バンド部が形成する輪の内側に向けて所定の波長帯域の光を照射する光源部と、

前記バンド部が形成する輪の内側を広角撮影する撮像部と、

静脈パターンの特徴量を記憶する記憶部と、

前記撮像部が広角撮影した画像から静脈パターンの特徴量を抽出し、当該抽出した特徴量と、前記記憶部に記憶された特徴量とを比較し、当該比較の結果、類似度が所定値を上回る場合に、当該生体認証装置を活性化する制御を実行するＣＰＵと、

所定の操作により前記撮像部を手首に対し遠方に移動させる移動機構と、

を備え、

前記移動機構は、前記撮像部を手首に対し遠方に所定距離を移動させた際の位置で前記撮像部の移動を一時的に制限する機構を備え、

前記移動機構は、前記バンド部を弾性体とすることにより形成され、

前記所定距離は、前記撮像部の位置が撮像適正位置となるように前記バンド部の伸縮帳の限界距離が設定されている、ことを特徴とする生体認証装置。

【請求項２】

請求項１に記載の生体認証装置において、

前記バンド部が手首の外縁に輪を形成して閉じた状態か否かを検出する装着確認部を更に備え、

前記ＣＰＵは、前記閉じた状態が検出された場合には、当該生体認証装置の活性化状態を維持する制御を実行し、前記バンド部が手首の外縁に輪を形成して閉じていない状態が検出された場合には、当該生体認証装置の活性化状態を解除する制御を実行することを特徴とする生体認証装置。

【請求項３】

請求項２に記載の生体認証装置において、

前記バンド部の所定箇所が二重構造を形成し、

前記ＣＰＵは、撮影された画像から静脈パターンの特徴量を抽出する処理において、撮影された画像に含まれる前記バンド部の画像情報を除外するフィルタ処理を実行することを特徴とする生体認証装置。

【請求項４】

請求項１に記載の生体認証装置と、サーバと、入場ゲート装置と、を備える入場管理システムにおいて、

前記サーバは、生体認証装置の識別子を記憶するＤＢと、

前記入場ゲート装置から受信した生体認証装置の識別子を前記ＤＢから検索する検索部と、

前記入場ゲート装置に前記検索の結果を送信する送信部と、を備え、

前記入場ゲート装置は、活性化状態の生体認証装置から当該生体認証装置の識別子を受信し、当該識別子を前記サーバに送信する送受信部と、

前記サーバから受信した情報に基づきゲートの開閉を制御する制御部と、を備えることを特徴とする入場管理システム。

【請求項５】

請求項１に記載の生体認証装置と、入場ゲート装置と、を備える入場管理システムにおいて、

前記入場ゲート装置は、生体認証装置の識別子を記憶するＤＢと、

活性化状態の生体認証装置から当該生体認証装置の識別子を受信する受信部と、

当該受信した識別子を前記ＤＢから検索する検索部と、

当該検索の結果に基づきゲートの開閉を制御する制御部と、を備えることを特徴とする入場管理システム。

【請求項６】

請求項１に記載の生体認証装置と、入場ゲート装置と、を用いた入場管理方法において、

前記入場ゲート装置が、活性化状態の生体認証装置から当該生体認証装置の識別子を受信し、

受信した識別子を、生体認証装置の識別子が記憶されているＤＢから検索し、

当該検索の結果に基づきゲートの開閉を制御する、ことを特徴とする入場管理方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、人間の生体情報を利用して個人を認証する装置および方法に関する。

【背景技術】

【０００２】

近年、ウェアラブル情報端末やヘルスケア向け端末など、腕に巻き付けて装着するリストバンド型の情報デバイスが注目を集めている。こうしたリストバンド型デバイスは、個人が常時身に着け続ける特性から、健康情報やGPSを用いた移動情報など個人のプライバシーに関わる情報を容易に収集し記録・管理・活用できる。また、個人と一体化して常時稼働している電子デバイスであることから、無線通信など電子的な手段を用いることで、装着した状態のままで特別な動作を行わなくても容易に電子マネーの決済や電子チケットの確認等が可能になる。そのため、個人の権利を証明する、利便性の高い個人ＩＤ発信機としての用途も期待されている。

【０００３】
一方、こうした個人情報と密接に関わるデバイスには、情報を保護するセキュリティ技術の搭載が不可欠である。上述した用途のうち、前者のプライバシー情報を扱うことについては、個人情報へのアクセスを本人以外ができないようにすることが肝要であり、後者のＩＤ発信についても本人が意図しない送信ができないよう保護する必要がある。そのため、情報アクセスや情報発信を行う際、確実に本人がその意思を持っていることを確認できるような本人認証手段をデバイスに装備することが求められている。
【０００４】
また、リストバンドのような、小型で持ち運びが容易なデバイスの場合、紛失や盗難に遭うリスクが高いことから、本人の手から離れた場合には即座にデバイスの動作をロックできる仕組みを取り込むことも重要である。さらには、電子チケット等の大規模な商用サービスでの利用を考えた場合、発券者側にとっても不正転売等で本人以外が利用できる状況は望ましくないため、チケットを購入した本人が確実に装着していることをより厳密に保証できることが望まれている。特に不正転売の場合は、本人が不正に加担することも想定する必要がある。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開2002-312324
【発明の概要】
【発明が解決しようとする課題】
【０００６】
特許文献１において提示された手首の静脈パターンの利用方法には、生体認証手段としての性能面において改善の余地がある。具体的には、特許文献１では、バンドの裏側に装備したラインセンサで静脈パターンを観測するが、かかる手法では、個人を判別するのに十分な面積のパターンを観測することができない。
【０００７】
一般に、静脈パターンによる認証では、複数の静脈の走行線が織りなす網目紋様の個人性に着目して認証を行うが、バンドの幅程度の範囲では数本の静脈が横切るだけで網目紋様にはならず、その中から個人特徴を抽出することは難しい。網目紋様が形成されるには少なくとも手首全体を計測する必要がある。
【課題を解決するための手段】
【０００８】
上記の課題を解決するため、本願発明における生体認証装置は、バンド部が形成する輪の内側に向けて所定の波長帯域の光を照射する光源部と、バンド部が形成する輪の内側を広角に撮影する撮像部と、静脈パターンの特徴量を記憶する記憶部と、撮像部が広角に撮像した画像から静脈パターンの特徴量を抽出し、抽出した特徴量と、記憶部に記憶された特徴量とを比較し、比較の結果、類似度が所定値を上回る場合に、生体認証装置を活性化する制御を実行するＣＰＵと、を備える。
【発明の効果】
【０００９】
本願発明によれば、手首の静脈が網目模様を形成するための十分な面積を撮影することができ、認証精度を向上させることが可能となる。
【図面の簡単な説明】
【００１０】
【図１】リストバンド型デバイスの外見を示す図である。
【図２】リストバンド型デバイスの概略を示す図である。
【図３】リストバンド型デバイスの利用形態の一例を示す図である。
【図４】装着時および定常状態におけるリストバンドの構造を示す図である。
【図５】リストバンド型デバイスの利用形態の一例を示す図である。

【図６】リストバンド型デバイスの利用形態の一例を示す図である。
【図７】リストバンド型デバイスの演算部が実行する処理を示すフロー図である。
【図８】撮像された画像からノイズ情報を除去する処理を説明するための図である。
【図９】リストバンド型デバイスの利用形態の一例を示す図である。
【図１０】リストバンド型デバイスの利用形態の一例を示す図である。
【図１１】リストバンド型デバイスを利用したサービスの一例を示す図である。
【図１２】リストバンド型デバイスを利用したサービスの一例を示す図である。
【発明を実施するための形態】
【００１１】
以下、本発明の実施形態の例を、図面を用いて説明する。
【実施例１】
【００１２】
本実施例では、リストバンド型デバイスを装着した手首の静脈パターンを用いた本人認証手段によって、本人が正しく装着したときのみ本体の制御権限の拡張と無効化が行える生体認証方法の例を説明する。図１は本発明を実現するリストバンド型デバイスの外観の一例であり、図２は、図１のデバイスの構成に関する概略図である。
【００１３】
図１は、腕時計に似た形態としたリストバンド型デバイスの例であり、腕時計同様、大きく本体１００とバンド１０３の２つの部品から構成される。
【００１４】
本体１００には、タッチパネル操作が可能なディスプレイ１０１が搭載され、必要に応じて物理的に動作指示可能なボタン１０２も用意される。本体１００の内部には演算ユニットが搭載され、一般のスマートホンのようにアプリケーションの実行や情報提示、通信等を行うことができる。
【００１５】
バンド１０３には、手首の掌側の面に当たる部分に、カメラ１０４と光源１０５が配置されている。手首の静脈を撮影するためには、可視光であれば緑の波長帯域とカメラ、あるいは波長700nm-1000nm程度の近赤外線に感度のあるカメラとその波長域の光源の組合せが好適である。近赤外線を利用する場合、カメラには近赤外域以外の波長の光をカットするフィルタを装着することで、静脈パターン以外の余計な情報が撮影画像に映り込むのを抑制することができる。
【００１６】
また、リストバンドにはバンドを一周するように導線が装備され、微小の電流を流すことで導通の確認ができるようになっている。リストバンド型デバイスの着脱の際、バンド部を開放したり留めたりするための嵌合部１０６は導線の接合部にもなっており、バンド部を閉じると導通し、開くと断線状態になる。この導通状態はリストバンド型デバイス本体の演算装置で電気的にチェックできる。バンド部の長さは個人の手首の太さに合わせて調整可能であり、初期設定時に腕から容易に抜けない長さに調節する。この導線の材料に抵抗を持ったものを用いることで、導線の長さに応じて抵抗値が増加し、この特性を利用することでバンド部の全周長を電気的に計測することができる。認証用データの登録時に、この抵抗値を記憶しておけば、登録後にバンド部を伸ばし、容易に腕から抜けやすくして不正な第三者への貸与を行うといったことを抑止できる。具体的には、抵抗値確認で変更があった場合、認証を行えないようにする。
【００１７】
図２は、図１のデバイス構成に関する概略図である。
【００１８】
デバイス本体に内蔵された演算部２００は、さらにＣＰＵ２０１、メモリ２０２、秘密記憶領域２０３、インタフェース(I/F)２０４から構成され、内部バスによって相互に接続される。これらは、高速化等の目的で、相互に専用バスで接続される場合もある。
【００１９】

ＣＰＵ２０１はプログラムを実行する演算装置である。後述する認証処理もこのＣＰＵが実行する。

【００２０】

メモリ２０２は処理プログラム本体や処理に必要なデータを格納する。恒久的に保持したいデータは、図中には記載しないが、フラッシュメモリなどの記録媒体と接続して書き込みや読み出しを行うこともできる。

【００２１】

秘密記憶領域２０３は、特別な権限、典型的には暗号鍵等による特別なアクセス方法を知らないと外部から読み書きできない特殊なメモリであり、本人の静脈パターンデータなど保護優先度の高い情報の格納や、後述するサービス提供者によるデバイス認証に利用する。

【００２２】

インタフェース２０４は、演算部と他の様々な機能ブロックとをつなぎ、データのやり取りを行うためのものである。たとえば通信部２０５と接続した場合には、演算部から各種の通信が行えるようになる。通信の種類としては、スマートホンなどの親機として設定されたデバイスとの間でデータの授受をしてもよいし、直接インターネットに接続して情報を得てもよい。また、無線で通信可能なセキュリティ装置と通信を行ってもよい。たとえば、PKI (Public Key Infrastructure)のようにデバイス内に秘匿した秘密鍵を使って、本デバイスがPKIで守られた情報やサービスにアクセスする権限を正当に持つことを証明するプロセスを採用すれば、信頼性の高い取引を行うことができる。具体的には、買い物の際、本リストバンド型デバイスを近づけるだけで、このデバイスに紐づけられた決済権限に基づいて、安全に取引を成立させることができる。上記PKIにおける鍵は秘密記憶領域２０３内で厳重に管理され、デバイスの所有者本人でも容易に改変することができない設定とするのが望ましい。

演算部２００には、インタフェース２０４を介して、手首の静脈パターンを利用した個人認証を行うための機能ブロックが接続されている。

【００２３】

画像入力器２０６は、カメラ１０４と接続され、手首３００の静脈パターンを撮影し、デジタルデータとして演算部に伝える。

【００２４】

画像入力器２０６は、カメラの出力信号を演算部で扱い易い形式に変換する機能を持つ。撮影画像はメモリ２０２に格納され、ＣＰＵ２０１がこれを処理する。この際、光量制御部２０７に接続された光源１０５が手首に光を照射し、ＣＰＵ２０１が実行するプログラムによって、撮影画像において静脈パターンが最も鮮明になるよう、光源の出力をフィードバック制御する。

【００２５】

光量制御部２０７は指定された値に対応する強度で光源が光を放つよう、ＰＷＭ(Pulse Width Modulation)制御等により出力する電気のエネルギー量を調節する機能を持つ。

【００２６】

また、上述のバンド嵌合部１０６も同様にインタフェース２０４を介して接続され、手首への装着状態を演算部から常時モニタリングできるようになっている。

【００２７】

図２には、他にも、装着状態をより多角的かつ正確に検出するための各種センサを併記してある。バンドの手首への接触を検出するタッチセンサ２０８、手首からどれくらい離れたかを検出する距離センサ２０９、などである。別の実施例で利用する生体認証センサ２１０もここで記載してある。

【００２８】

タッチディスプレイ１０１は、リストバンド型デバイス装着ユーザからの指示の入力や情報の提示を行うために用いられる。

【００２９】

図３は、本発明の利用形態の一例を示す図である。具体的には、リストバンド型デバイスを手首に装着する動作の中で本人認証を行うケースを想定しており、腕３００が掌側を上に向けた状態で描かれている。

【００３０】

線３０１は静脈を示し、手首全体に広がって、全体で大きな網目模様を形成している。この網目模様は個人差があることがわかっており、パターン形状の違いで個人識別が可能である。しかしながら、この部位の静脈は太く、複数存在する静脈同士の距離は数ミリメートルないし数センチメートルに及び、静脈の曲率半径は大きく、分岐の間隔も同様に数センチメートルになることも珍しくない。そのため、バンド部の幅程度の範囲の静脈パターンを観測しただけでは、個人を特徴づける静脈間の位置関係や屈曲、分岐といった情報が十分に含まれない。したがって、十分な精度を得るためには、図中の３０２で示したように比較的広範囲の静脈パターンを撮影する必要がある。

そこで、静脈パターンを広範囲に撮影するため、手首からの距離をとり、広角カメラにて撮影する。カメラ自体は近年小型化が進んでおり、リストバンド型デバイスの中に図１のようにして収めることが可能である。また、カメラのレンズに広角なものを選ぶことで、手首からの距離が数センチメートル程度でも手首全体を撮影することができる。

【００３１】

なお、本発明における広角カメラとは、カメラと被写体との距離が短くても広い範囲を撮影できる、すなわち広角撮影が可能なカメラを意味する。広角撮影に適したレンズをカメラに装着することで、広角カメラとなる。但し、短い被写体距離で広い範囲を撮影できるレンズほど撮影画像の歪みや周辺の明るさ不足といった画質への悪影響があるため、手首全体が撮影でき、かつ操作に不自由がない程度に手首との距離を短くできる適切なレンズを採用する必要がある。また、静脈パターンを鮮明に撮影するため、専用の光源をカメラの周囲に用意し、手首に向けて照射する。静脈を流れる血液中のヘモグロビンは、近赤外線を吸収する特性があり、手首に近赤外線を当てると、表皮から皮下に浸透し後方散乱によって光は戻ってくるが、そのうち静脈部分から戻る光については吸収によって減衰し、相対的に暗く映る。この特性によって静脈パターンをコントラストよく撮影することができる。このような反射光撮影方式の場合、生体内部に浸透し後方散乱する戻り光だけでなく、表皮で反射して静脈の存在とは関係なしに戻ってくる光もあり、それが静脈パターンのコントラストを低下させたり、表皮付近にある傷や肌荒れを強調したりして認証精度に影響を与える場合がある。手首の静脈は、その先の掌や指の静脈に比べて太く、表皮も相対的に薄いため後方散乱光が強く、反射光方式でも高いコントラストを得やすいが、より画質を高めるためには、たとえば偏光フィルタを組み合わせることで、反射光の影響を抑えるようにしてもよい。また、強い光がスポットのように当たると、その光点が静脈パターン特徴の抽出に悪影響を与えることもあるので、手首全体に分散して光が照射されるよう光源と手首との間に拡散板などを配置するとよい。

【００３２】

図４は、装着時および定常状態におけるリストバンド型デバイスの構造を示す図である。

【００３３】

先に述べたように、図３は、リストバンド型デバイスを手首に装着する際に本人認証を行うケースを想定している。このケースの場合、装着の際に、図４に示すように、まずバンド部１０３の一方（ここでは本体１００のある側）が手首の甲側に密着した状態となり、次いで掌側にある嵌合部１０６で分離したバンド部を再結合する手順をとる。この際、リストバンド型デバイス中の、カメラが内蔵された部分４０１の素材がその形態を崩さない程度の硬度を有し、そのカメラ内蔵部がバンド内のジョイント４０２を支点として稼働するように設計することが望ましい。そのようにすることで、装着時にはカメラ部分が手首の真上に位置すると同時に、手首とカメラの間に距離を確保した状況を作り出すことができる。装着の瞬間に認証を行うことで、リストバンド型デバイスを使用するユーザは、認証を行うための余計な操作なしに、装着時の自然な動作の中に認証操作を組み込むこと

ができる。

【００３４】

このとき、バンド部を最大に開いた状態で、カメラが手首を向き、焦点も合い、さらにはそこに正しく光が照射されるよう光源の向きを規定（図４中に示したカメラと光源から伸びる矢印）しておくことで、装着時にはただバンド部を最大に開くことで、常に同じ距離、同じ画角の静脈撮影画像を得ることができる。このとき、バンド部の回転を最大位置で一時的にロックする機構を設ければ、認証時のカメラ部の揺れが抑えられ、より安定的に撮影ができ、精度の高い認証を行うことができる。

【００３５】

認証が成功したときには、バンド部の本体側に設けられたタッチセンサ４００にて腕との接触状態を判定する。この接触状態が維持されたままバンド部が閉じられ、嵌合部１０６の接合による導通が検出できた場合には、本人が正しく装着したと看做し、リストバンド型デバイス本体の制御権限を拡張する。

【００３６】

ここで、タッチセンサ４００による確認を必要としたのは、本人が装着し認証に成功した後、第三者に不正に貸与する可能性を考慮したためである。すなわち、タッチセンサ４００はリストバンド型デバイスを貸し与えるときに生ずる腕からのデバイス着脱を検出するために用いられる。このとき、図のような小面積のタッチセンサひとつだけでは、たとえばタッチセンサに第三者の指等を当て、腕に触れているものと見せかけた上で登録者本人の手首静脈で認証を行い、そのまま第三者が指を当てたまま持ち去るといった方法で不正の抜け道とされる可能性がある。そこで、リストバンド型デバイスのバンド部全体に複数のタッチセンサ、もしくは面状に接触を検知できる大面積のタッチセンサを装備し、手首に巻きついた状態であることを厳密に検出することで不正のリスクをさらに低減することができる。

【００３７】

この他にも、センサを多角的に組み合わせることや、認証用のカメラで捉えた手首静脈パターンが、バンドが閉じられるまで連続的に撮影され存在し続けることを確認する等により、認証した本人の腕からデバイスが移動していないことを精度よく検出することが可能である。

【００３８】

ここで、デバイス本体の制御権限の拡張とは、具体的には、デバイスが対応できるサービスを広げるモード切り替えのことである（活性化と呼ぶこともある）。たとえば、買い物等の決済時には少額のプリペイド分までしか利用できないが、この拡張状態であれば、クレジット機能を用いた高額な決済まで行える、といった具合である。権限拡張を本人認証の結果として行うことで、本人以外は実行されたくないサービスでも、本デバイスを装着しているだけで安全かつ手間無く当該サービスを利用することが可能である。

【００３９】

デバイスが制御権限拡張状態に入ると、ディスプレイ１０１に、権限が拡張されたことを示すインジケータが表示され、ユーザはいつでも制御権限の状態を確認することができることとなる。一方、リストバンド型デバイスを外すと、タッチセンサ４００が腕を検知できなくなり、さらに嵌合部１０６も断線するため、それらいずれか一方もしくは両方を検知して即座に制御権限拡張が無効化される。これによって、リストバンド型デバイスが何者かに強奪されたような場合でも制御権限が即座に無効化され、被害を最小限に食い止めることができる。

【００４０】

図５は、図３で示した手首静脈認証の派生形態である。図３の構成では、装着動作と認証が一体化しており、装着時に一度認証に成功すれば装着中は制御権限が拡張された状態が維持されることを前提としている。これにより権限拡張に関する特別な操作を省略し、簡便な使い勝手を提供している。

【００４１】

しかしながら、用途によっては、ユーザ自身の判断で、権限拡張や無効化を随時行えるようにしたい場合もある。図５の形態は、それを可能にするものであり、リストバンド型デバイスを装着した状態で、バンド部の一部を引っ張る操作で手首の静脈パターンによる認証ならびに権限拡張を随時行えるようにする。

【００４２】

図５に示した構成例では、バンド部の一部が伸縮可能な部材５００で構成されており、装着された定常状態からバンド部の一部をつまんで引っ張ると、カメラ部が手首から離れ、静脈パターンを撮影するに好適な距離に到達する。

【００４３】

部材５００は、カメラ部が適正位置に達したところで伸びなくなるよう伸縮長が調整されており、ユーザが力任せに引っ張っても適正位置を通り過ぎることがないようになっている。また、ユーザがバンド部のどこを引っ張ればよいかわかりやすいように、バンド部の一部には把手５０１をつけることができる。把手５０１を用いることでユーザにとってバンド部が掴み易くなる効果があるほか、把手をカメラ部の近傍に配置することで、指で掴む箇所とカメラ部とを一致させることができ、指で感じる引っ張り限界距離と、カメラ側の適正撮影距離とをより正確に合わせることができる。

【００４４】

一方、部材５００をバネのような弾性素材にすることで、認証が完了すれば、自律的に元の位置に戻すこともできる。これによって、指でバンドを引っ張って認証し、終われば指を離すだけといった簡便な操作で認証を行うことができる。

【００４５】

尚、上記の形態は、バンド部を引っ張ったときに輪が広がり、その瞬間であれば、容易に腕からリストバンド型デバイスを抜き取ることが可能になってしまう。そのため、認証中は上述したタッチセンサ４００による接触検知、もしくは認証用カメラの連続撮影により、撮影される画像に大きな変化がないこと確認することを基本原理とする静止検知を実行し、腕からの抜き取りが認められれば制御権限拡張は行わないように設定することが望ましい。

【００４６】

尚、制御権限拡張状態の切り替えについては、認証動作と必ずしも同期させる必要はない。すなわち、一度拡張状態になり、その後連続装着が確認されていれば、装着が続いている間はボタン操作だけで拡張と解除を相互に移行できるようにしてもよい。これによって、リストバンド型デバイスの本人確認手段としての利用許可期間をユーザ自身が自由かつ簡単に設定できる。

【００４７】

図６は、図５からさらに派生した形態の一例である。バンド部からカメラ部を引っ張ったときに輪が広がって腕からデバイスが抜き取ることが物理的にできないよう、バンド部を二層構造とし、カメラ部のみ独立して離れるようにしている。二層構造とするため、手首の上にはバンドの一層目６００が残され、バンド部を腕から抜くことが困難であり、かつ装着中かどうかを導通により確認し続けることができる。

【００４８】

一方で、この一層目部材の存在が手首の静脈パターンの撮影に悪影響を与えることがある。具体的には、６００が不透明な素材であれば静脈パターンがバンド部の太さ分だけ隠されることになる。パターンの一部が大きく損なわれた状態で正確な認証は困難である。

【００４９】

そこで、一層目６００を透明な素材とし、静脈パターンが映るようにする。あるいは、一層目６００を非常に細いワイヤー等で構成することで、隠されるパターンの面積を最低限にし、認証精度の劣化を抑える。あるいは、ワイヤー部分を特殊な色や模様とすることで、静脈パターン撮影の際、その特定の色や模様を使ってワイヤー部分を容易に検出可能とし、その部分を認証時のパターン照合の対象から明示的に除外することで精度をさらに改善することができる。

【００５０】
同様の処理は、一層目６００を透明な素材とした場合にも有効であり、透明な素材でも端の部分は線として映りやすいため、それを同様に除外する。一層目と二層目の間をつなぐ部材の剛性が十分に高ければ、カメラの撮影画像中に映る一層目は常に同じ位置に見えるため、予め透明素材の境界線が映り込む部分を記憶しておくことで、境界線に当たる部分を計算によって検出できる。同様の手法でワイヤー部分の検出を行うことも可能である。
【００５１】
図７は、以上で述べてきた利用形態を実現するリストバンド型デバイスの演算部で実行される認証プログラムのフローチャートの一例である。特に図３の利用形態に即した処理の流れとなっている。
【００５２】
処理７０１は認証プログラムのスタートポイントを示し、処理７０２で初期化を行う。初期化処理では、端末のオペレーションシステムの起動、アプリや各種機能ブロックの初期化を行い、認証以外の端末本来の機能を実行できる状態にする。
【００５３】
処理７０３では、処理７０２の初期化処理の途中、もしくは終了後に、認証に関わる端末の状態について、本デバイスのハードやソフトに変更が加わっていないかセルフチェックを行う。これは前述したように、たとえば端末の電源が切れた状態でバンド部のバンド長を伸ばしておき、腕から容易に抜けやすくした状態で起動することにより、制御権限拡張後、容易に第三者へのデバイスを引き渡しやすくするといった不正改造を防止するためである。具体的には、長さに応じて抵抗値が変わる線材で導通をチェックし、抵抗値を記憶することで変更を検知する。あるいは、図１の嵌合部１０６で互いに接合する１組のジョイント部品のうち少なくとも一方がバンド部上を移動可能とし、それによってバンド部が形成する輪の大きさを調節する形式をとる場合には、そのジョイント部品の位置で決まる輪の円周長で決まる抵抗値を用いる。このバンド長の他にも、認証用カメラの向きが反転して、バンド部の外側を向いていないか等、本人の手首に装着されていなくても認証が成功してしまう恐れのある不正改造をチェックする。
【００５４】
処理７０４は、処理７０３の結果、デバイスの整合性が確認できなった場合に、デバイスの起動自体や認証機能を無効化したり、本人の生体情報の再登録を促す等の処理を行う。
【００５５】
処理７０５では、デバイスが腕に装着された状態になっているかどうかをチェックする。チェックにあたっては、バンド部が輪を形成して導通があること、タッチセンサ４００が腕と近接距離にあること、等を判定に用いる。これらのチェックは常時行うと電力を消費し、デバイスのバッテリー持ち時間を低下させるため、１秒ごとといったように、バンド部の不正な着脱を見逃さない範囲で間隔を置き、電力を消費しない状態を設ける。こうして行った装着チェックにおいて、バンド部が腕に装着された状態と検出されれば、特に何もせず待機状態に戻り、所定の周期で処理７０５を繰り返す。
【００５６】
なお、図７の例では処理７０５を処理７０３の後に実施するように記載しているが、所定の条件下では処理７０５を省略可能である。すなわち、デバイスの制御権限が拡張された活性化状態である場合に限り処理７０５を実施することとしてもよい。
【００５７】
処理７０６では、処理７０５で装着状態でないことが検出された場合に、制御権限拡張状態のデバイスの権限拡張を、即座に無効化する。この際、ディスプレイ１０１に表示する権限状態を、無効状態を示すものに変更する処理を、併せて行ってもよい。
【００５８】
処理７０７以降では、手首の静脈パターンを用いた認証を実行する。但し、バンド部が

外れた状態の間中ずっと認証をトライし続ける必要はなく、適切なタイミングでのみ処理を行えばよい。これにより、不必要な電力消費や、手首の静脈がまったく映らないことが明らかな状態で認証を試みる無駄を省くことができる。不必要な条件での認証を行わないことは、認証精度を高める効果もある。ここでの適切なタイミングとは、具体的には、図４左側の図に示したような、リストバンド型デバイスの一部が腕に近接し、かつバンド部が最大に開いた状態を指す。この状態であれば、手首静脈をボケなく、適切な照明方向で撮影することができる。最大に開いた状態かどうかは、ジョイント４０２が最大回転した場合に接点が入るような機構を設けておくことで容易に検出可能である。

【００５９】

処理７０７では、手首の静脈パターンの撮影を行う。すでに述べている通り、基本的に光源１０５で手首を照らし、それをカメラ１０４にて撮影する。こうした光を利用する撮影方式では、屋外で太陽の下で認証を行う場合等に、外光の影響を強く受けて画質が劣化しやすい。このとき、外光よりも十分に強い人工光を与えれば、撮影される画像においては人工光の影響が支配的になる。もちろん、光を強くすると電力消費が増えるため、非常に短い間隔でフラッシュ的に光源を光らせ、露光時間を短く設定（1/1000秒程度）したカメラにて撮影を行うことで、外光の影響を抑えることができる。また、操作性の観点からは、カメラ部をあまり遠くまで離さなくても認証できることが望ましい。至近距離で手首をなるべく広く撮るためには、広角撮影が不可欠である。但し、広角撮影の場合、撮影画像が歪んだり（樽型歪み等）、画像の周辺部ほど暗くなったりしやすくなる。これはすなわち、カメラ位置と手首との僅かなずれが生じただけで、撮影される画像の歪み方が大きく異なることを意味し、同じ手首を撮影した画像であっても、歪んだままの画像から抽出した特徴同士は照合が難しくなる。

【００６０】

処理７０８は、前述の歪みや明るさムラを正規化し、特徴抽出する処理である。この処理により、安定した認証が可能となる。なお、特徴抽出処理は、静脈認証技術に用いられている一般的な処理で対応可能である。

【００６１】

また同様に、撮影画像中には、対象とする静脈パターン以外にも背景や手首表面の皺といったノイズとなる情報が映り込んでいる。処理７０８では、それを除去するフィルタ処理を併せて行うことで、認証をさらに安定させることができる。このうち、背景と手首とを切り分ける簡便かつ高精度な方法として、リストバンド型デバイス自体の映り込みを利用することができる。詳細は、図８で後述する。

【００６２】

処理７０９では、得られた静脈パターン特徴を、予め登録しておいた本人の静脈パターン特徴と比較し、類似性を判定する処理である。具体的には、得られた静脈パターン特徴と、予め登録しておいた静脈パターン特徴の類似度が所定値を上回るか否かを判定する。当該処理で、所定値を上回る場合には処理７１０に進み、そうでなければ処理７０５にループする。

【００６３】

処理７１０では、デバイスの制御権限拡張を行い、ディスプレイ１０１にその状態を示す表示を行い、処理７０５にループする。図７のフローチャートでは、認証処理は１回だけとしているが、処理７０７から７０９を何度か繰り返し実施してもよい。そうすることで、本人を間違って拒否する確率を低減することができる。この場合、繰り返しは５秒～１０秒程度の一定時間内で終わるようにし、それ以上は本人ではなく第三者が成り済ましを図ろうとしている確率が高いと判定し、連続して試行されないようにするとよい。

【００６４】

なお、上記フローチャートでは、図３もしくは図４の利用形態を想定して説明したが、図５の利用形態も基本的な流れは共通である。例えばデバイスが装着状態のとき、認証を行いたいタイミングで認証処理７０７～７１０を実行すればよい。もちろん、把手５０１等でカメラ部が引っ張られたことを自動的に検出して、認証処理が始まるよう設定しても

構わない。この場合、把手５０１にスイッチ機能を設けても良いし、伸縮可能な部材５００に、バンド部が伸びたことを検出する機構を設けても良い。いずれにしても、カメラ部が引っ張られた状態をＣＰＵ２０１が検知し、認証プログラムを自動実行する。

【００６５】

また、これまでの説明では、リストバンド型デバイスの演算部２００の中ですべての処理を実行する例を示したが、小型のデバイスに内蔵できるＣＰＵの性能は十分なものを用意できない場合もある。そこで、負荷のかかる処理の一部を、たとえば、より大型のスマートホンやクラウド上のサーバで実行してもよい。但し、生体情報は保護すべき情報であるので、装置外に送信するときは情報を暗号化する、もしくはデータを分割して個々の単位では個人を特定できないようにした上で異なるサーバに割り振って実行し最後に統合する、といった工夫が必要である。

【００６６】

図８は、前述の処理７０８において、リストバンド型デバイス自体の映り込みを利用してノイズ情報を除去する処理を説明するための図である。この図は、リストバンド型デバイスのカメラから撮影した手首と静脈パターンの例を示している。

【００６７】

この例の撮像画像中には、中央に腕３００が映っており、その上に静脈パターン３０１が見えていて、腕以外の部分は認証には不必要な背景となっている。この画像にはバンド部１０３が映っており、嵌合部１０６も見えている。バンド部は通常の背景には存在しないため、その特殊性を利用して、バンド部の存在する部分を腕と背景との境界線であると精度良く判定することができる。

【００６８】

バンド部は腕の一部にかかっているだけであるが、腕の輪郭は滑らかに連続的な弧を描くため、バンド部との境界部分を基点にして連続的にエッジを辿ることで精度良く腕領域を切り分けることができる。こうして切り出された腕領域の中から静脈パターンを抽出し、認証に用いる。

【００６９】

尚、図８の撮影例では、バンド部が画像内に最も大きく収められるよう、カメラの撮影画像が一般に横長であることを利用し、腕が縦になって映る形で撮影している。こうした観点に寄らず、腕の静脈パターンが広範囲に撮影できることを重視する場合には、腕の輪郭線が収まるように撮影しながら、撮影画像中の腕の占有面積が最も大きくなるよう、腕が横に映る形で撮影してもよい。

【実施例２】

【００７０】

実施例１では、リストバンド型デバイスを装着した状態でのみ観測できる手首の生体情報を用いることで、本人が装着したときだけデバイスが活性化される方式について述べたが、図９に示す方式では、デバイスを装着する部位の生体情報に限らなくても、デバイスを装着した本人が認証を行っていることを判定する方法について述べる。

【００７１】

図９では、リストバンド型デバイス１００において、装着した腕とは異なる別の腕の指先の情報を用いて認証を行っている。

【００７２】

図中の１０２は、図１の説明時には単なるボタンスイッチとしていたが、その位置に生体認証センサ２０１が埋め込まれたものとして、操作例を描いている。そして、この認証センサ２０１が実施例１の手首静脈認証と同じ役割を担うことになる。

【００７３】

しかしながら、この場合、リストバンド型デバイスの正当な権利者本人でなくても、成り済まそうとする者が腕にリストバンド型デバイスを装着し、正当な権利者が認証センサに指先を当てて認証を成功させてしまえば、その後は制御権限拡張が維持されたままになってしまう。権利者が不正に加担しなくても、指紋認証等の生体の生死を問わない認証方

式の場合、権利者の指を切って盗み取り、認証が成功させられるリスクもある。
【００７４】
そこで、認証センサ２０１での認証時に、装着者本人の指が使われているかを厳密に判定できる機構を用意する。
【００７５】
すなわち、リストバンド型デバイス装着者本人の指かどうかを判定するため、個人の身体のどこででも観測可能な共通の生体情報に着目する。たとえば、心拍や脈拍は、心臓の鼓動に伴う電気パルスや血流の変化が、場所により強弱はあれども身体のどこからでも検知できる。したがって、こうした身体に共通の生体情報が、リストバンド型デバイスが装着されている腕と、認証に用いる指先とから等しく検出できた場合、本人が正しく認証を行っているものと判定できる。特に心拍、脈拍の場合は、生きている人間の一部としてつながっている必要があり、生体の一部を切り取ったりしても認証は不可能である。
【００７６】
図１０は、上記を実現するリストバンド型デバイスの構成の一例である。バンド部の腕と接する面には既出のタッチセンサ４００に加えて、心拍・脈拍センサ１０００が備わっている。このセンサ１０００によって、装着されている腕から心拍・脈拍情報を検出する。
【００７７】
一方、デバイス本体の表側には認証センサ２０１が組み込まれている。指紋や静脈パターンといった、個人を識別可能な生体情報を採取すると同時に、心拍・脈拍も取得できるセンサを用いる。指紋センサの場合であれば、一般的な静電容量式のセンサの周り、もしくは一部に、医療用測定機器であるパルスオキシメータの脈拍測定の原理を簡略化した、光センサと発光光源との対をコンパクトに一体実装してもよい。これによって指紋と脈拍とが同時に得られる。この実装方式は計測する原理が異なるため、それぞれの生体情報観測が相互に干渉しにくいという利点がある。
【００７８】
また別の認証方法として、指先の静脈パターンを認証に用いる方法もある。指先に近赤外光を透過もしくは反射させ、カメラで指先の静脈パターンを撮影する。これを使って本人認証を行う。このとき、近赤外光は血液中のヘモグロビンを吸収する特性があるため、指先の撮影画像は、指先に含まれるヘモグロビン量、すなわち血液量に応じて全体の明るさが変化する。心臓の拍動に応じて血流は脈動し、指先の血液量も同様に脈動するため、指先の撮影画像の全体輝度を時系列に解析すると、脈拍が求まる。
【００７９】
したがって、指先の静脈を本人確認に用いると、認証用のセンサと脈拍検出用のセンサを共通にできて低コスト化が図れるほか、本人確認に用いている撮像画像そのものから脈拍が求まるので、その脈拍情報が本人のものといえる信頼性が極めて高い。
【００８０】
こうして腕と指先の２ヶ所から得た心拍や脈拍が同一身体から検出されたかどうかを判定する。簡便な解析方法としては、２ヶ所の心拍のパルスが同期していることを確認する方法がある。特に脈拍の場合、部位によって心臓からの距離の違いで血液の到達する時刻がずれるので遅延は生ずるが、血液量が増えたり減ったりする周期は共通である。脈拍の波形をさらに詳細に解析し、個人を特徴づける情報を抽出して照合を行うことで、さらに同一身体の情報であることを厳密に確認することもできる。
【００８１】
尚、認証処理実施例１の利用形態向けに説明した処理フローと同様であり、認証処理の具体的な方法のみ異なる。したがって、バンド部の装着検知処理は共通であり、装着時に認証処理を行うことで制御権限が拡張され、外すと解除される点も同様である。
【実施例３】
【００８２】
上記で述べたリストバンド型デバイスについて、そのデバイスの正当な利用権限を有す

る本人の生体情報が正しく登録され、さらには、そのデバイスが出力する本人確認用の情報と正しく紐づけられているかを厳密に保証するシステム運営方法について説明する。

【００８３】

本発明のリストバンド型デバイスは、生体情報の登録をデバイス所有者本人が行うことを想定している。しかしながらその場合、デバイスに登録された情報がユーザ本人のものであることを保証することが難しい。より望ましくは、サービス事業者が、ユーザがデバイスに生体情報や本人確認情報を登録する過程を逐一見届けた上で情報の信頼性を担保する必要があるが、多数のユーザに活用してもらおうとした場合、それに要する時間とコストが膨大になる。より迅速かつ効率的に確認できる方法が必要である。そこで、生体情報や本人確認情報の登録と、それらの正当性の確認とを分離し効率化を図る。

【００８４】

以上で示してきたように、本発明のリストバンド型デバイスにおいては、デバイス本体が制御権限拡張状態にあるときは、少なくとも装着している本人が生体登録したと、高い確率で判定できる。そこで、正当性を確認する際には、ユーザに事前に制御権限拡張状態にしてもらい、最初にそれを確認できれば、あとは運転免許証やパスポート等の身分証明書で一般的な本人確認を行い、その情報とリストバンド型デバイスに登録された本人確認情報が一致することを確かめるだけでよい。そして、デバイスに認証済みの署名を書き込めば、その先はデバイスの登録情報が変更されない限り、署名と権限拡張状態の２つのチェックで本人が使用していることを保証できる。認証する側にとっても、登録作業まで見届ける必要がなくなり、デバイスの認証がスムーズに行える。この際、たとえば、リストバンド型デバイスが容易に腕から外れるような長さに調整されているなど不正の画策が疑われる場合は、デバイスの認証を行わないこともできる。

【００８５】

もちろん、登録情報や署名が容易に書き換えられるようでは意味がない。図２のブロック図の中で示したように、リストバンド型デバイス内の演算部には、秘密記憶領域２０３が設けられている。この記憶領域は、広く使われているＩＣカードと同様、物理的にも論理的にも厳重に保護され、一部の領域はアクセスするために非公開の特別な手順を必要とするよう設定ができ、データも暗号化して格納する。この記憶領域２０３に生体情報と本人確認情報を格納しておくことで、本体が盗まれても、生体情報を容易に改竄されたり置き換えられたりできなくなる。この記憶領域２０３の一部に、本デバイスのセキュリティ機能を利用しようとする特定のサービス事業者だけが読み書きできる記憶領域を設け、本デバイスについて、正当な本人の生体情報と、その本人を表す本人確認情報とが正しく紐づけられていると、その事業者が確認した場合に、このデバイスが信頼済みであることを証明する署名を書き込んでおく。この署名は、リストバンド型デバイスの持ち主でも、他の第三者でもアクセスできないよう保護される。署名を行ったサービス事業者は、厳格な本人確認が必要なサービスを提供する際、リストバンド型デバイス内での本人認証によって制御権限拡張がされているかどうかに加え、自らが秘密領域内に書き込んだ署名の確認も行う。このようにデバイス自体の認証を行うことによって、本人以外の成り済ましをさらに効果的に防ぐことができる。この署名は、サービス事業者自身が個別に行っても良いし、複数の事業者が共通に用いることを目的に、公に認知された認証機関によって署名を行うようにしてもよい。

【００８６】

図１１は、本発明のデバイスを用いた自動改札サービスの一例である。ユーザは本デバイスを装着し、制御権限拡張状態にしておけば、本デバイスと改札機との間で、秘密が保持された無線回線によって通信が行われ、改札機にカードをかざす操作も必要なしに通過ができる。

【００８７】

具体的には、まず改札機から検札のリクエストがリストバンド型デバイスに届き、リストバンド型デバイスが契約しているサービス事業者からのリクエストかどうかを確認する。そうであれば秘密記憶領域２０３にアクセスして、そのサービスに対応する事業者もし

くはその事業者が委託している公的認証機関が書きこんだ署名を読み出し、デバイスが制御権限拡張状態であることを示す署名情報とともに、改札機に送信する。改札機側は２つの署名情報を分析し、両者とも正当と認められれば、サービスを提供する。この場合は、ゲートを閉じることなく通し、ユーザへの課金が必要であれば課金を行う。

【００８８】

こうしたリストバンド型デバイスを用いて本人確認が容易になると、これまで時間がかかるとか、不自由な操作をユーザに求められない等の理由で適用できなかった場所やサービスでも本人確認を使えるケースが広がる。マーケティングにおいては客の行動を示す様々な情報を掻き集めビッグデータ解析を行うが、誰がどのような行動をとったかの情報の信頼性が高まるほど、より付加価値の高い解析結果が得られる可能性がある。

【００８９】

以上の説明では、リストバンド型デバイスを例にして述べたが、リストバンド型デバイスを足首に適用したり、よりスケールダウンした指輪型デバイスに用いたりするなど、バンド付きのデバイスであれば同様に利用可能であることは言うまでもない。

【００９０】

図１２は、本発明におけるデバイスを利用したチケットレス入場サービスの概略図である。本サービスでは、事前に自宅や店舗窓口等で、鉄道や航空機等の切符やイベントのチケットを購入しておくと、利用当日に本発明のリストバンド型デバイスを装着しているだけで乗車や入場が可能になる。

【００９１】

ここでは自宅でイベントのチケットをネット購入し、会場にデバイスを使って入場する例について順を追って説明する。ユーザはまず自宅やコンビニ等の窓口でインターネットに接続されたコンピュータ１２０１やタブレット端末等を用い、チケットを購入するためのインターネットサイトのサーバ１２０２にアクセスする。チケット購入手続きは、基本的には現在広く行われている一般的な方法に準拠する。次に、ホームページ画面から、参加したいイベントの種類を選び、その開催日時を選択し、クレジットカードや振り込みといった支払い方法を決めて決済する。このとき、リストバンド型デバイスを使って本人認証を行うことで、住所やメールアドレスといった個人情報の入力を省略することができる。デバイスにクレジットカード情報を紐づけておけば、決済情報の入力も省略できる。この本人認証にあたっては、リストバンド型デバイスとコンピュータ１２０１との間に通信手段を設け（Wi-FiやBluetooth(登録商標)といった標準プロトコルを利用できる）、アプリケーションを通じてデータ転送を可能にする。そして、リストバンド型デバイスとサーバ１２０２の間でも直接もしくは間接的に通信可能とする。この状態で、ユーザは上述した方法でデバイスの制御権限拡張を行うことで、デバイス１００とサーバ１２０２の間で最も安全な手段が選択されて認証が行われる。たとえば、デバイスのＩＤ情報をそのまま送るのではなく、何らかの方法で暗号化したり、チャレンジレスポンス方式で認証を行う等により、不正なデバイスが通信内容を横取りしたり成り済ましたりするのを防ぐ。こうしてリストバンド型デバイスを本人が装着している状態と確認でき、そのリストバンド型デバイスで認証された本人情報を取得できれば、それに紐づけてサーバは、リクエストされたイベントに対応するチケットを発行する。尚、リストバンド型デバイスによる決済を行う場合には、ユーザの意思と関係なく処理が行われてしまわないように、デバイス１００上に確認用のメッセージを表示し、それに対する確認の操作を行わない限り決済に進めなくする等の安全性を高める工夫を加えることができる。

【００９２】

チケット発行が正常に完了すると、リストバンド型デバイスで認証された本人情報とチケット情報（イベント種別や日時など）と当該デバイスの識別子とが組にされてサーバ１２０２が管理するデータベース１２０３へ格納される。ここで管理される本人情報は、デバイス１００を一意に対応づけられればよいので、名前や住所といった個人情報自体を含む必要はない。不用意な情報流出を防ぐためには、格納する情報を最小限に制限するとよい。

【００９３】
イベント当日は、リストバンド型デバイスを装着し制御権限拡張状態にしたユーザが、イベント会場に設置された改札機に近づくと、図１１を用いて説明したような通信が行われ、本人確認が実行される。改札機は、リストバンド型デバイスから読み取った本人確認情報と、開場中のイベント情報と、当該リストバンドデバイス型デバイスの識別子とを合わせてサーバ１２０２に送る。サーバはデータベース１２０３に事前格納された情報と照合して、真正のチケットであるかどうかを判定し、照合結果を改札機に送信する。但し、ネットワーク経由による判定は、一定の通信時間を必要とし、一度に大量の来場者が集中するような大規模イベントの場合、処理しきれずに改札口で大行列を作る可能性がある。ここで、改札は一般にイベントごとに行うことが多く、一つのイベント当たりの入場者数は、サーバで管理すべき入場者全体の数に比べれば圧倒的に少ないため、改札機に搭載できるコンピュータの能力でも十分に記憶し処理することができる。そこで、予めサーバ１２０２から、イベントごとの来場者のデータのみを、改札機に内蔵、もしくはイベント会場に設置され、改札機と高速接続が可能なコンピュータにダウンロードしておき、そのコンピュータによってチケットの有効判定処理を行う。イベントごとにデータは入れ替えられてローカルに処理可能となり、通信時間を抑えた、高速なスループットで判定が実現される。

【００９４】
以上の方法により、サーバまたは改札機によりチケットが有効と判定されると、改札機はその旨を伝えるメッセージ表示もしくはランプや音等による通知を行い、ユーザに応答する。もし、無効と判定された場合には、警報を発し、必要に応じてフラッパーゲートなどの物理的な遮断機でユーザの通過を阻止する。但し、本発明の改札機では、従来のような紙やカードのような形のある媒体を所定位置にかざすといった操作が不要のため、ユーザにとっては、リストバンド型デバイスを付け忘れたのか、リストバンド型デバイスの制御権限拡張をし忘れたのか、あるいはリストバンド型デバイス自体に不具合があったのか、無効とされる理由が多様でわかりにくいという問題がある。そこで、無効の理由を改札機の画面や音声アナウンス等を使ってより具体的に伝えるようにする。

【００９５】
本発明のデバイスを用いれば、他にも様々な機能を提供することができる。たとえば、オフィスや自宅のコンピュータに、制御権限拡張されたリストバンド型デバイスをかざすだけでログインできるようになる。デバイスが制御権限拡張状態でコンピュータに十分近接して存在していれば、その間はそのコンピュータから接続する、認証が必要な様々なサーバに対しても自動的に当人の権限で接続することを許可するようにしてもよい。また、コンピュータからデバイスが一定距離以上離れた場合には自動的に画面をロックしたり、システムからログアウトし、また近づくと自動でログインしたりするような設定にすることもできる。デバイスとの距離は、たとえば、リストバンド型デバイスとコンピュータとの間の通信電波強度などで測定することができる。

【００９６】
同様に、コンピュータだけでなく、店舗の決済端末や銀行の自動現金預払機（ＡＴＭ）、あるいは自動車や住宅といった用途にも適用可能である。制御権限拡張状態であれば、現在よりも利用限度額を増やした電子マネー機能を提供したり、ＡＴＭに近づけば、金額を入力するだけで現金をおろすことができるようにしたりと利便性を高められる。もちろん、車や住宅の鍵替わりにすることもできる。

【００９７】
このように、本発明により、本人が装着していることがより正確に判定できるＩＤ発信デバイスが実現でき、他人でも簡単に使えてしまう従来のＩＤカード等に比べ、暗証番号の入力などといった、これまで本人確認厳格化のためにユーザに強いてきた様々な面倒な手順を省くことが可能である。

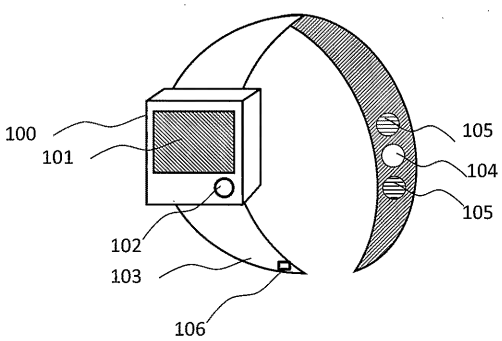
【符号の説明】

【００９８】

１０３：バンド部　１０４：撮像部　１０５：光源部　２０１：ＣＰＵ　２０２：メモリ
２０３：記憶領域

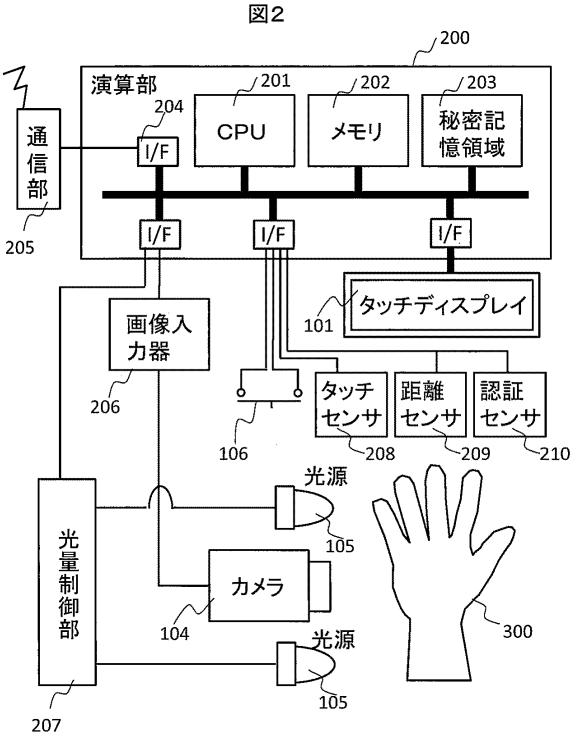
【図１】

図1



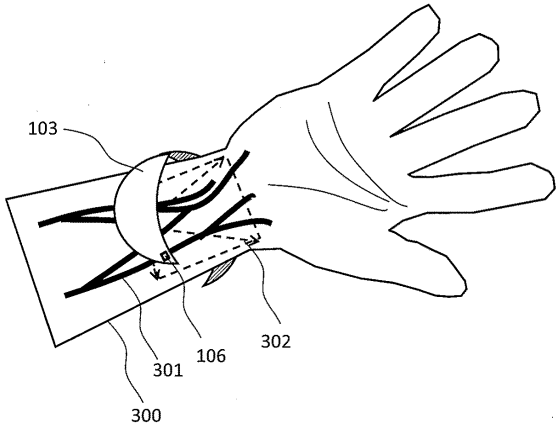

【図２】

図2



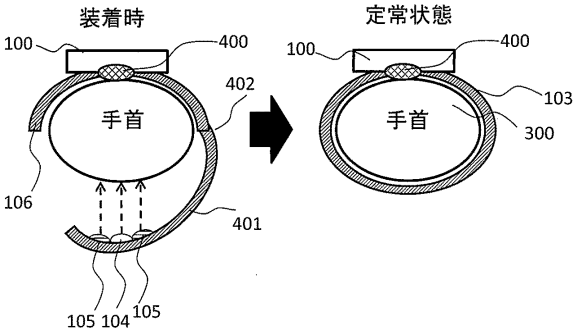
【図３】

図3



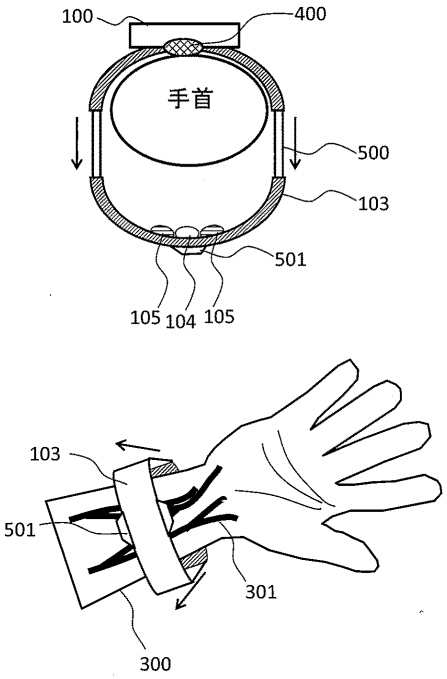

【図４】

図4



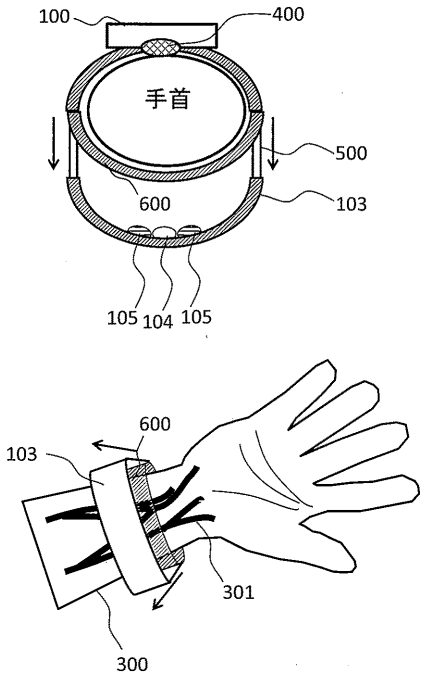

【図５】

図5



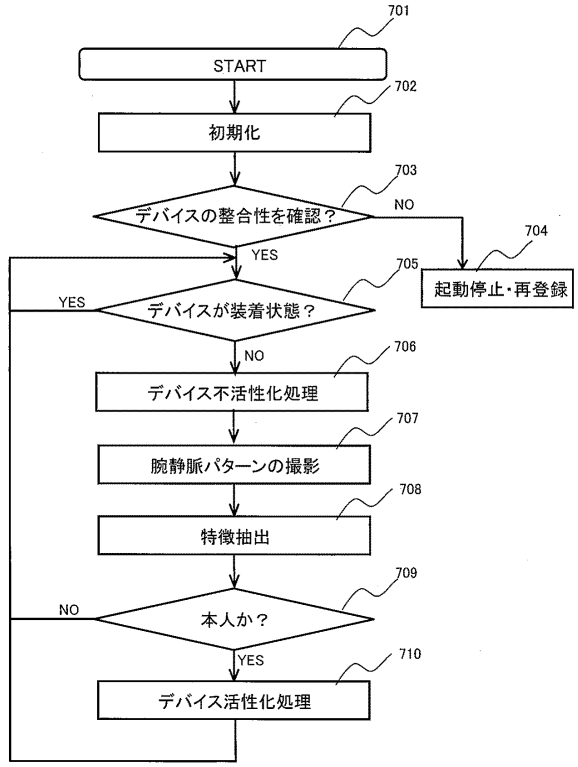

【図６】

図6



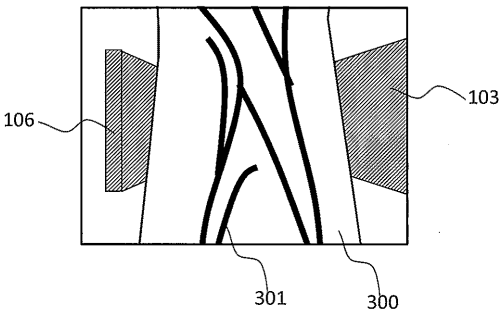
【図７】

図7



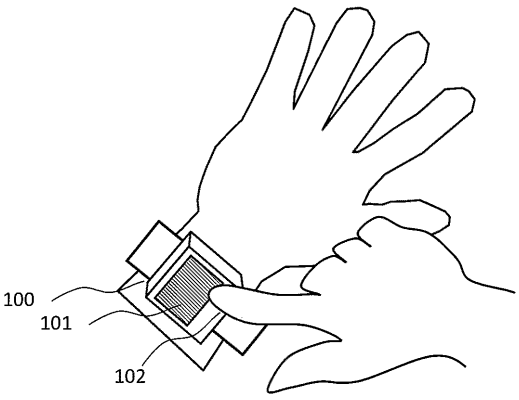

【図８】

図8



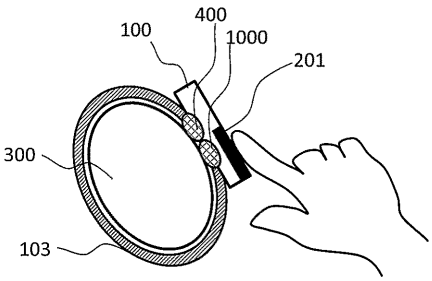

【図９】

図9



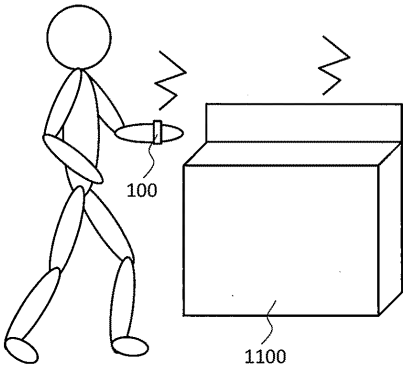

【図１０】

図10



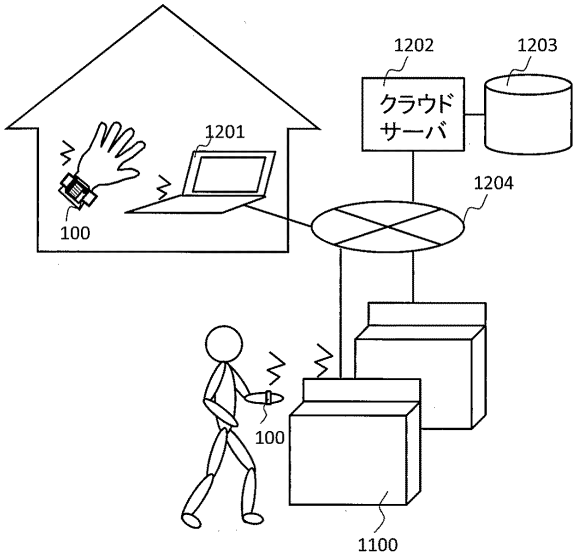
【図１１】

図11




【図１２】

図12



フロントページの続き

(72)発明者　高田　晋太郎
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　宮武　孝文
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

審査官　岡本　俊威

(56)参考文献　特開２００２－３１２３２４（ＪＰ，Ａ）
特開２０１７－０２７５９４（ＪＰ，Ａ）
特開２００６－０４８６６７（ＪＰ，Ａ）
特表２００５－５２８６６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｔ　　１／００
Ｇ０６Ｔ　　７／００
Ａ６１Ｂ　　５／１１７１