(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6063859号
(P6063859)
(45)発行日　平成29年1月18日(2017.1.18)　(24)登録日　平成28年12月22日(2016.12.22)

(51)Int.Cl.　F I
G06F 21/32 (2013.01)　G06F 21/32
G06F 21/35 (2013.01)　G06F 21/35

請求項の数 6　(全 13 頁)

(21)出願番号　特願2013-264833(P2013-264833)
(22)出願日　平成25年12月24日(2013.12.24)
(65)公開番号　特開2015-121910(P2015-121910A)
(43)公開日　平成27年7月2日(2015.7.2)
審査請求日　平成28年1月25日(2016.1.25)

(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　100100310
弁理士　井上　学
(74)代理人　100098660
弁理士　戸田　裕二
(74)代理人　100091720
弁理士　岩崎　重美
(72)発明者　喜種　佳司
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　宮司　卓佳

最終頁に続く

(54)【発明の名称】携帯鍵装置及び装置制御方法

(57)【特許請求の範囲】
【請求項１】
制御対象装置と無線通信を行って使用制限の解除を行う携帯鍵装置において、
互いに無線通信を行う第一の鍵装置と第二の鍵装置と、
他の装置と無線通信を行う通信部と、
生体認証成功のコンテキストを保持する生体認証コンテキスト保持部と、
人体への装着を検知する検知部と、
を備え、
前記検知部が、前記第一の鍵装置の人体への装着を検知している場合に、前記生体コンテキスト保持部は、前記生体認証成功のコンテキストを受け付けて保持し、
前記生体認証コンテキスト保持部が生体認証成功のコンテキストを保持している場合であって、前記第一の鍵装置と前記第二の鍵装置の通信が確立されている場合に、前記通信部は、前記制御対象装置の使用制限を解除させる解除信号を発信し、
前記生体認証コンテキスト保持部が生体認証成功のコンテキストを保持している場合であって、前記第一の鍵装置と前記第二の鍵装置の通信が切断されている場合に、前記生体コンテキスト保持部は、前記生体認証成功のコンテキストを保持し続けると共に、前記通信部は、前記解除信号の発信を停止させ、
前記検知部が、前記第一の鍵装置の人体への装着による形状変化を検知することにより人体から外されたことを検知したときに、前記生体コンテキスト保持部は、前記生体認証成功のコンテキストを破棄するとともに、前記通信部は、前記解除信号の発信を停止させ

ることを特徴とする携帯鍵装置。
【請求項２】
請求項１に記載の携帯鍵装置において、
前記制御対象装置が受信していた前記解除信号を受信しなくなった場合、前記使用制限を有効にし、
前記生体認証成功のコンテキストを破棄した場合に、前記通信部が前記第一の鍵装置と前記第二の鍵装置との間で通信を行ったときに前記生体認証にかかる生体情報の入力を要求し、当該生体認証が成功した場合に前記解除信号を発信することを特徴とする携帯鍵装置。
【請求項３】
請求項１に記載の携帯鍵装置において、
前記通信部が、前記第一の鍵装置と前記第二の鍵装置との間で通信を行っているときに、生体認証を行うための生体情報の入力を受け付ける生体情報入力部と、
前記入力された生体情報と、記憶部に記憶された登録生体データとの生体認証処理を行う生体認証部と、
を備え、
当該生体認証処理の成功のコンテキストを、前記生体認証コンテキスト保持部に保持することを特徴とする携帯鍵装置。
【請求項４】
第一の鍵装置と第二の鍵装置から構成される携帯鍵装置が制御対象装置と無線通信を行って使用制限の解除を行う装置制御方法において、
前記鍵装置の検知部が、前記第一の鍵装置の人体への装着を検知している場合に、前記鍵装置の生体コンテキスト保持部は、前記生体認証成功のコンテキストを受け付けて保持し、
前記生体認証コンテキスト保持部が生体認証成功のコンテキストを保持している場合であって、前記第一の鍵装置と前記第二の鍵装置の通信が確立されている場合に、前記鍵装置の通信部は、前記制御対象装置の使用制限を解除させる解除信号を発信し、
前記生体認証コンテキスト保持部が生体認証成功のコンテキストを保持している場合であって、前記第一の鍵装置と前記第二の鍵装置の通信が切断されている場合に、前記生体コンテキスト保持部は、前記生体認証成功のコンテキストを保持し続けるとともに、前記通信部は、前記解除信号の発信を停止させ、
前記検知部が、前記第一の鍵装置の人体への装着による形状変化を検知することにより人体から外されたことを検知した場合に、前記生体コンテキスト保持部は、前記生体認証成功のコンテキストを破棄するとともに、前記通信部は、前記解除信号の発信を停止させることを特徴とする装置制御方法。
【請求項５】
請求項４に記載の装置制御方法において、
前記制御対象装置が、受信していた前記解除信号を受信しなくなった場合、使用制限を有効にし、
前記生体認証成功のコンテキストを破棄した場合に、前記通信部が前記第一の鍵装置と前記第二の鍵装置との間で通信を行ったときに前記生体認証にかかる生体情報の入力を要求し、当該生体認証が成功した場合に前記解除信号を発信することを特徴とする装置制御方法。
【請求項６】
請求項４に記載の装置制御方法において、
前記通信部が、前記第一の鍵装置と前記第二の鍵装置との間で通信を行っている場合に、生体情報入力部は、生体認証を行うための生体情報の入力を受け付け、
前記入力された生体情報と、記憶部に記憶された登録生体データとの生体認証処理を行う生体認証部と、
を備え、

当該生体認証処理の成功のコンテキストを、前記生体認証コンテキスト保持部に保持することを特徴とする装置制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、生体認証技術を用いた携帯型キーデバイスによる装置制御技術に関するものである。

【背景技術】

【０００２】

携帯電話やスマートフォン、タブレットPCなどの携帯デバイスの高機能化が進み、決済や会社業務に使用する機会が増加するに従い、なりすましを防止するセキュリティ技術の重要性が高まっている。

【０００３】

携帯デバイスは、例えば暗証番号やパターンロックなどでロックされている。しかしながら、携帯端末が盗難や紛失等で第三者の手に渡った時に暗証番号やパターンを解析され、携帯デバイスを不正に使用されてしまう可能性がある。

【０００４】

このようなりすましを防止し、確実に本人であることを認証するには、暗証番号やパターンロックの代わりに、個人ごとに異なる生体の特徴を利用した生体認証により本人確認を行うことが有効である。

【０００５】

現在、生体認証の一つである小型の指紋認証装置を内蔵した携帯デバイスが開発されており、生体認証による本人確認を用いて第三者のなりすましによる不正使用を防止している（例えば、特許文献１参照）。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開2009-286343号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかしながら、生体認証においては本人拒否率として規定されるように、本人であるにも関わらず生体入力の仕方や生体情報の変化等によって認証に失敗する場合がある。また、なりすましを防止するために、携帯デバイスのロックを解除する都度に生体の入力を要求される。そのため、暗証番号やパターンロックと比較して使い勝手が悪くなることがある。

【０００８】

また、指紋認証では指先だけを使用するので装置の小型化が可能であり、携帯デバイスに内蔵できているが、指内部の静脈パターンを用いる指静脈認証装置、手のひらを使用する手のひら静脈認証装置や目の虹彩を使用する虹彩認証装置等は、指紋認証と比較して生体の内部情報を使用するので複製しにくい、手あれなどの生体の状態による影響を受けにくい、情報量が多いので指紋認証よりも精度が高い、といったメリットがあるものの、装置の小型化が難しいために携帯デバイスに内蔵することが難しい。

【０００９】

これらの問題点を解決するため、本発明ではワイヤレス通信機能を内蔵し、生体認証による本人確認の利点を生かしつつ認証回数を減らすことができる生体認証技術を用いた携帯型キーデバイスによる装置制御技術を提供する。

【課題を解決するための手段】

【００１０】

本発明の解決手段の一例としては、以下の通りである。

【００１１】
互いに通信するワイヤレス通信機能を搭載する携帯型キーデバイス（ワイヤレスキーデバイス、アプリケーションをインストールした携帯電話やスマートフォン等の携帯デバイス、ワイヤレス通信機能付き生体認証装置など）を二つ用意し、ワイヤレス通信を確立した状態において生体認証動作を行い、生体認証に成功した場合は、いずれかの携帯型キーデバイス内で認証成功のコンテキストを保存し、ロック解除信号発信状態に移行させる。制御対象装置は、ロック解除信号を受信すると、さらなる生体認証は要求せずにロック解除し操作可能になり、該信号を受信しなくなるとロック状態になる。
【００１２】
二つの携帯型キーデバイスのワイヤレス通信が確立されている状態では、携帯デバイスはロック解除信号発信状態とし、ワイヤレス通信が切断された場合は、生体認証成功のコンテキストを破棄し、ロック解除信号発信の停止状態に移行し、再度のロック解除信号発信には、生体認証を要求する。
【発明の効果】
【００１３】
本発明によると、生体認証成功コンテキストを保持してユーザが生体認証する回数を低減し、キーデバイスを置き忘れ等した場合に認証成功コンテキストを破棄することで他人による使用を制限し、使い勝手と安全性の両立を向上できる。
【図面の簡単な説明】
【００１４】
【図１】本発明の実施例にかかるワイヤレス通信を利用した装置制御システムである。
【図２】本発明の実施例にかかるサーバー利用タイプの生体認証装置を用いる装置制御システムである。
【図３】本発明の実施例にかかるウェアラブル生体認証装置を用いる装置制御システムである。
【図４】本発明の実施例にかかるウェアラブルデバイスを用いる装置制御システムである。
【図５】本発明の実施例にかかるウェアラブル生体認証装置である。
【図６】本発明の実施例にかかるウェアラブルデバイスの実施例である。
【図７】本発明の実施例にかかるウェアラブルデバイスの回路例である。
【図８】本発明の実施例にかかる生体認証の動作フロー図である。
【図９】本発明の実施例にかかる携帯デバイスの動作フロー図である。
【図１０】本発明の実施例にかかる制御対象装置の動作フロー図である。
【発明を実施するための形態】
【００１５】
以下、本発明の実施形態について説明する。
【実施例１】
【００１６】
図１に本実施例の全体の概念図を示す。本実施例では、生体認証装置100と、携帯デバイス101と、制御対象装置102～104を使用する。
【００１７】
生体認証装置100は、通信部と生体情報入力部とを備え、予め照合に使用する登録生体データと、接続先の携帯デバイス101の接続情報を登録しておく。登録生体データ、接続情報の登録は、生体認証装置単独、もしくはPC(Personal Computer)等の上位デバイスと接続して登録するものとする。認証する生体としては指静脈を用いて説明するが、指紋、掌紋、掌静脈、虹彩、顔など他の生体認証を用いてもよい。
【００１８】
携帯デバイス101との接続情報は、例えばBluetooth（登録商標）等の無線規格における各装置間のペアリング情報に相当するもので、特定の生体認証装置と特定の携帯デバイスのみが1対1でセキュアにワイヤレス接続を確立できるようにするための接続情報となる。

また、生体認証装置100は電池などを内蔵し、モバイルで使用できる装置とする。

【００１９】

携帯デバイス101は、通信部と、入出力部（例えばタッチパネル付ディスプレイ）と、演算部（プロセッサ）とを備える。

【００２０】

制御対象装置102～104は、本生体認証装置により制御される装置であり、制御対象としては、一例として、PC102のログイン制御や、入退室管理装置103のドア施錠・開閉や、決済端末104の決済処理が該当する。

【００２１】

図８に生体認証装置100の動作フロー図を示す。

【００２２】

ユーザが生体認証装置100の電源をOFFからONにした後（S701～702）、生体認証装置100はワイヤレス通信で携帯デバイス101との接続を開始する（S703）。ワイヤレス通信が一定期間の間に確立されなかった場合は、生体認証装置は電源OFF状態に移行する（S701）。ワイヤレス通信が確立された場合、生体認証装置100はユーザに生体情報の入力を促し、生体認証を行う（S704）。生体認証に成功した場合、生体認証装置100は認証成功のコンテキストを装置内に保存し、認証成功の情報を受取った携帯デバイス101はロック解除状態に移行する（S705,706）。認証に失敗した場合は、生体認証装置100は電源OFF状態に移行する(S701)。コンテキストを保存し、携帯デバイス101がロック解除状態に移行した後、生体認証装置100と携帯デバイス101はワイヤレス通信の状態を監視し続ける(S708)。生体認証装置100と携帯デバイス101間のワイヤレス通信が確立されている間は、携帯デバイス101はロック解除状態を維持し続ける(S709)。ユーザは生体認証装置と携帯デバイスを常時携帯してワイヤレス通信可能な距離にしておくことにより、パスワード入力等のロック解除動作をすることなく携帯デバイスを使用することができる。

【００２３】

生体認証装置100または携帯デバイス101を落したり置き忘れたことにより、通信可能距離以上に生体認証装置100と携帯デバイス101間の距離が離れてワイヤレス通信が途切れた場合は、携帯デバイス101はロック状態に移行し(S710)、生体認証装置101は認証成功のコンテキストを破棄し(S711)、電源OFF状態に移行する。

【００２４】

図９に携帯デバイス101の動作に関するフローチャートを示す。

【００２５】

携帯デバイス101の電源をONにし（S801）、あらかじめ接続情報で登録しておいた生体認証装置100に近づけると、携帯デバイス101と生体認証装置100とは自動でとワイヤレス通信による接続を確立し、生体認証装置100は生体の入力待ち状態となる（S802,S803）。ワイヤレス接続は、暗号鍵交換等によってセキュアに特定の生体認証装置100と特定の携帯デバイス101間で1対1で接続されるものとする。

【００２６】

この状態において、ユーザが生体認証装置100に生体を入力すると、生体認証装置100は入力された生体の生体情報を計測して認証生体データを作成し、その認証生体データと予め登録しておいた登録生体データを照合することにより、生体認証を行う。照合の結果、認証生体データと登録生体データが同一であると判定した場合は認証成功となり、認証成功のコンテキストを生成として装置内に保存するとともに、携帯デバイスに対して認証が成功したことをワイヤレスで送信する。認証に失敗した場合は、生体認証装置は電池の消費量を抑えるために電源OFF状態に移行する。

【００２７】

携帯デバイスは、ワイヤレス通信を監視しながら、認証成功の受信待ちをする（Ｓ804,Ｓ805）。このときに、ワイヤレス通信が途絶えた場合には、ワイヤレス通信監視状態に戻り、生体認証装置100は生体認証を中止する（Ｓ806，Ｓ802）。生体認証に成功した場合、認証成功を受信した携帯デバイス101は、制御対象措置をロック状態からロック解除

状態にするためのロック解除信号の発信を始める（Ｓ807）。

【００２８】

以降、生体認証装置100と携帯デバイス101間のワイヤレス通信が維持されている間、携帯デバイス101はロック解除信号発信状態を保持し、生体認証装置101は認証成功のコンテキストを保持し続ける。

【００２９】

生体認証装置100と携帯デバイス101は、ワイヤレス通信の状態を監視し（S809）、一度でも生体認証装置100と携帯デバイス101間のワイヤレス通信が切断された場合、生体認証装置100は認証成功のコンテキストを破棄して電源OFF状態に移行し、携帯デバイス101はロック信号発信を停止状態に移行する。

【００３０】

図１０に制御対象装置102～104の動作に関するフローチャートを示す。

【００３１】

まずは、制御対象装置を電源ＯＦＦから電源ＯＮにする（Ｓ901, Ｓ902）。この状態で、制御対象装置はロックされている状態であり、すなわち操作を受け付けない。そして、携帯デバイス101からのロック解除信号を待つ。

【００３２】

ロック解除信号を受信すると、携帯デバイスの認証を始め、そのロック解除信号が制御対象装置のためのものであると判定されると認証成功になり、その認証コンテキスを保存する（Ｓ904～Ｓ906）。このときに、さらに携帯デバイス101と通信して、情報を要求してもよい。ここで、生体認証情報のコンテキストをさらに携帯デバイス101に求めることはあっても、ユーザに生体情報を新たに入力要求することは行わない。認証に失敗すると、ロック状態を継続する（Ｓ902）。

【００３３】

認証コンテキストを保存すると、制御対象装置はロックを解除し、操作可能な状態になる（Ｓ907）。そして、ユーザは制御対象装置を使用することができる。

【００３４】

ロック解除の状態で、制御対象装置は携帯デバイス101からのロック解除信号の監視を続け、ロック解除信号を受信しているうちは、操作可能なロック解除状態を継続する（Ｓ909）。ロック解除信号を受信しなくなったら、ロック状態になり操作不能になり、認証コンテキストを廃棄し、ロック解除信号待ちに戻る（Ｓ910，Ｓ911，Ｓ902）。

【００３５】

これら生体認証装置100、携帯デバイス101、制御対象装置102～104の動作により、以下の作用効果を有する。

【００３６】

制御対象装置102～104をロック解除して操作可能にするには、生体認証装置100、携帯デバイス101に加え、生体情報が要求される。これによって、ユーザ本人以外は制御対象装置のロックを解除することができないので、安全性を高くすることができる。

【００３７】

また、制御対象装置としては、ロック解除信号の有無によりロック解除を行っており、ロック解除に際してユーザの身体から新たに生体情報を読み込ませることを要求しない。ユーザーは、生体認証装置100と携帯デバイス101をそれぞれ衣服のポケット等に入れて携行することにより、ワイヤレス通信を確立して生体認証成功コンテキストを保持する。ワイヤレス通信は確立されたままなので携帯デバイスはロック解除信号発信を維持し続けており、ユーザは制御対象装置に近づけばロックを解除することができ、ロック解除する都度に生体情報を読み込ませる必要が無い。

【００３８】

一方で、生体認証装置100または携帯デバイス101を盗難や置き忘れなどで離した場合、携帯デバイス101と生体認証装置100間の距離が通信距離を越えることになり、ワイヤレス通信が切断され、生体認証装置100は認証成功のコンテキストを破棄して電源OFF状態に移

行し、携帯デバイス101はロック解除信号発信を停止する。この状態から復旧するには、生体認証装置100の電源を入れて携帯デバイスと通信し、生体認証を行わなければならない。すなわち、ユーザのみが再びロック解除信号を発信する状態にできる。一方のみ、または両方を別々に第三者が取得しても、生体情報が無いため、使用できない。

【００３９】

ユーザが携行する生体認証装置100と携帯デバイス101は、両方を一緒に落としたり置き忘れることが無いよう、ユーザは別々の衣類ポケットや荷物等で保持することが望ましい。本実施例では、スマートフォンに認証用アプリケーションをインストールして携帯デバイス101としている。これにより、携帯デバイス101を、携帯鍵以外の機能も有するスマートフォンとしても利用することができる。これ以外でも、ユーザが携行できるものであれば、ノートPCやタブレットPCを用いてもよい。

【００４０】

また、携帯デバイス101は、認証の他にもユーザが継続して使用するので、胸ポケットやバッグの中など取り出しやすい場所に入れておくことになる。生体認証装置100は、認証成功後にユーザが使用する必要が無く、携帯デバイス101との間でワイヤレス通信の確立を保持すれば良いだけなので、ズボンのポケットなどのユーザ本人と一体で落しにくい場所に入れておくことが望ましい。もっぱら携帯鍵専用に用いる生体認証端末と、他の用途にも用いる携帯デバイス101との組み合わせであれば、ユーザは、携帯デバイス101は取り出しやすい箇所に、生体認証装置100は邪魔になりにくいまたは落としにくい箇所にと、異なる箇所で携行すると考えられ、一緒に紛失する可能性を低くすることができる。

【００４１】

セキュリティ性を高めるために、生体認証装置100、若しくは携帯デバイス101のワイヤレス通信の電波出力は、１～３ｍ程度の近距離でしか接続を確立できないような出力としても良い。

【００４２】

ロック解除される制御対象装置としては、ワイヤレス機能を搭載したPC102やドア入退管理装置103、決済端末104等と組合わされて使用することができる。

【００４３】

PC102の場合、ログアウト状態にあるPC102にロック解除信号発信状態の携帯デバイス101が近づき、PC102と携帯デバイス101の間でワイヤレス通信で接続し、相互認証が完了した時点でPC102をログオン状態にする。これにより、ユーザはログオンごとに生体認証を行うことなく、一回の生体認証でログオンごとに本人確認を行うのと同じようにPC102にログオンが可能となる。

【００４４】

ドア入退管理103の場合は、ロック解除信号発信状態にある携帯デバイス101がドア入退管理装置に近づき、ワイヤレス通信で接続して相互認証が完了した時点でドアをロック解除状態にする。これにより、PCの場合と同じく、入退室（入室または退室）ごとに生体認証を行うことなく、一回の生体認証で入室ごとに本人確認を行う場合と同じように入退室することが可能となる。

【００４５】

決済端末104の場合は、決済時にロック解除信号発信状態にある携帯デバイスを決済端末104に近づけることで、携帯デバイス101と決済端末104の間でワイヤレス通信で接続し、相互認証が完了して決済を行う。このとき、決済の確認のために、決済端末104に対する簡単な操作を要求してもよい。これにより、ユーザは決済ごとに生体認証を行うことなく、一回の生体認証で決済ごとに本人確認を行う場合と同じように決済することが可能となる。

【００４６】

また、ユーザは生体認証装置100に対して認証成功のコンテキストの有効時間を設定できるようにしても良い。生体認証に成功し、コンテキストを生成してからの時間をカウントし、ユーザが設定した時間が経過した場合に、生体認証装置100内に保存されている認

証成功のコンテキストを破棄し、電源OFF状態に移行する。若しくは、生体認証装置100内に時計を内蔵しておき、ユーザが設定した時刻になった時に、認証装置内の認証成功のコンテキストを破棄し、電源OFF状態に移行する。

【００４７】

ユーザはコンテキスト破棄の時刻を夜に設定しておくと、朝に認証を行って夜まで携帯デバイス101を使用し、退勤後に生体認証装置100と携帯デバイスを一緒に放置しておいても、指定した時間に認証成功のコンテキストを破棄して携帯デバイス101をロック状態に移行させることができる。

【００４８】

また、生体認証装置100と携帯デバイス101のワイヤレス通信の記録を利用すると、生体認証装置、もしくは携帯デバイスを紛失した場合に、紛失した場所を推定することが可能である。生体認証装置と携帯デバイスのワイヤレス接続が途切れた時刻を生体認証装置か携帯デバイスに記録、あるいは携帯デバイス101がネットワーク上のサーバーへ記録し、生体認証装置100や携帯デバイス101を置き忘れ等で紛失した場合にはワイヤレス接続が途切れた時刻を確認し、その時刻のユーザの行動（例えばGPSや入退室記録などによる位置情報）から別デバイスを紛失した場所を推定できる。

【００４９】

上記のように、生体認証装置100、携帯デバイス101の２つの装置とワイヤレス通信を利用することにより、１度の生体認証で、都度の生体認証を行わなくても、制御対象装置の利用ごとの生体認証を行う場合と同じように本人確認を可能とし、本人確認の結果をPCログオンや入退管理、決済などに利用することができる。

【００５０】

なお、後述の実施例で説明するが、互いにワイヤレス通信を行う二つの携帯鍵装置（生体認証装置100と携帯デバイス101）を備え、こられの少なくとも一方に生体認証成功コンテキストを保持する機能を備えていれば、生体情報を入力する機能、登録生体データや生体認証機能を、二つの携帯鍵装置とは別のデバイスに通信可能に設けてもよい。

【実施例２】

【００５１】

実施例２について説明する。実施例２は、実施例１と大部分は同様であり詳細な説明を省略するが、異なる点は次のとおりである。実施例１において登録生体データは生体認証装置100内に登録されているが、生体認証装置100を紛失した場合に、中にある登録生体データも一緒に紛失することになる。

【００５２】

そこで、図２に示すように登録生体データをサーバー105等の生体認証装置100や携帯デバイス101以外の別の場所に保管しておき、生体認証装置100と携帯デバイス101のワイヤレス通信が確立された段階で、携帯デバイス101はサーバー105と通信を行い、登録生体データをサーバー105からダウンロードする形態とする。登録生体データのダウンロードが完了したら、携帯デバイス101はダウンロードした登録生体データを生体認証装置100に送信する。生体認証装置100は、受信した登録生体データを使用して、入力された生体情報との照合を行い、生体認証を行う。

【００５３】

認証が成功した場合、生体認証装置100は生体認証成功のコンテキストを作成し、生体認証装置100内部に保存し、その後、受信した登録生体データを破棄する。その後の処理は、実施例１と同様である。

【００５４】

認証が失敗した場合、生体認証装置100は受信した登録生体データを破棄し、電源OFF状態に移行する。

【００５５】

上記のような方法により、生体認証装置100を紛失しても、登録生体データを守ることが可能となる。

【実施例３】
【００５６】
実施例３について説明する。生体認証装置を腕時計やブレスレット等、ユーザが身に付ける形態にしたウェアラブル生体認証装置106としても良い。実施例１、２では、ワイヤレス通信が途切れたことにより、キーデバイスがユーザから離れたことを検知したが、本実施例では身体に装着するウェアラブルデバイスとすることで、ユーザの身体から離れたことを検知する。
【００５７】
図３にウェアラブル生体認証装置106の概念図を示す。この場合、図５に示すようにウェアラブル生体認証装置106は脈拍計等の生体検知機能107を備え、人体から取り外されたことを検知することができるものとする。もしくは、図６に示すような形状で図７のような回路構成とし、取り外すために開閉機構109を開ける必要がある構造として、開閉機構109で生体からの取り外しを検出する等、人体から取り外すために形状の変化が必要な構造として、その形状変化を検出することによって人体からの取り外しを検出しても良い。
【００５８】
ウェアラブル生体認証装置106は、実施例１、実施例２と同様にユーザが身に付けた状態においてのみ生体認証を行い、認証に成功した場合は認証成功のコンテキストを生成し装置内に保存する。
【００５９】
本実施例ではウェアラブル生体認証装置106が完全にユーザと一体となっているため、ウェアラブル生体認証装置106と携帯デバイス101の間のワイヤレス接続が切断されたとしても、ウェアラブル生体認証装置106を紛失ではないため、生体認証装置100内の認証成功のコンテキストを破棄する必要は無い。
【００６０】
ウェアラブル生体認証装置106内の認証成功のコンテキスト破棄は、ユーザがウェアラブル生体認証装置106を取り外すか、ウェアラブル生体認証装置106に設けられたスイッチ等で指示することでのみとする。
【００６１】
ユーザがウェアラブル生体認証装置106を体に取り付けた状態を維持していた場合、ウェアラブル生体認証装置と携帯デバイスのワイヤレス通信が切断された後に、再び生体認証装置と携帯デバイスが近づくことで再度ワイヤレス通信が確立された時、ウェアラブル生体認証装置は認証成功のコンテキストを保持したままであり、生体認証を行うことなく再び携帯デバイスをロック解除状態とすることができる。
【００６２】
また、本実施例では、携帯デバイス101を用いず、ウェアラブル生体認証装置106が、生体認証成功コンテキストを保持してロック解除信号を発信してもよい。この場合でも、ウェアラブル生体認証装置106がユーザの人体から取り外された場合には、それを検知して生体認証成功コンテキストが破棄されてロック解除信号の発信が停止され、効果を奏する。
【実施例４】
【００６３】
図４に示す実施例は、生体認証装置で生成した認証成功のコンテキストを、さらに別のデバイスに転送して使用する場合の実施例となる。生体認証装置100と携帯デバイス101の他に、ワイヤレス通信機能を持った腕時計やブレスレット等の別のウェアラブルデバイス111を使用する。ウェアラブルデバイス111は、実施例３と同様に生体検知機能や形状変化検知等により、ユーザが身に付けていることを検出する機能を持つものとする。
【００６４】
生体認証装置100は、認証に成功すると認証成功のコンテキストを生成し、それをウェアラブルデバイス111に送信する。ウェアラブルデバイス111がコンテキストを受信して保持し、さらに受信成功を生体認証装置100に返信し、生体認証装置100はこれを受信した時

点で認証成功のコンテキストを破棄する。
【００６５】
ウェアラブルデバイス111は、生体検知機能を使用してユーザが身に付けていることを監視し、ウェアラブルデバイス111がユーザから外された時点で認証成功のコンテキストを破棄する。
【００６６】
認証成功のコンテキストを保持したウェアラブルデバイス111が、ワイヤレス機能を持ったロック状態にある携帯電話やスマートフォン等の携帯デバイス101に近づくと、ウェアラブルデバイスと携帯デバイスの間でワイヤレス接続を確立し、相互で機器認証を行う。機器認証に成功したら、携帯デバイス101はロック解除信号発信状態に移行し、その後はウェアラブルデバイスとのワイヤレス接続が確立している間、ロック解除信号発信状態を維持し続ける。
【００６７】
携帯デバイス101がロック解除信号発信状態にある時は、実施例１と同様に、携帯デバイス101をPC102、ドア入退管理103や決済端末104に使用することができる。
【００６８】
携帯デバイス101を盗難や置忘れなどで紛失した場合、ウェアラブルデバイス111と携帯デバイス101の距離がワイヤレス通信可能な距離以上に離れることによってワイヤレス接続が切断されると、携帯デバイス101はロック解除信号の発信停止状態に移行して第三者が使用不可状態になる。
【００６９】
実施例３と同様に、ウェアラブルデバイス111にはユーザが身に付けていることを検出する機能が備えられているため、携帯デバイス101とのワイヤレス接続が切断された後も、ユーザが身に付けていることを検知し続けている間はユーザと一体であることが保証されるため、ウェアラブルデバイス内部に保存されている認証成功のコンテキストを破棄する必要はなく、再び携帯デバイスとのワイヤレス接続が確立された時は、携帯デバイスはロック解除信号発信状態に移行する。
【００７０】
なお、携帯デバイス101とウェアラブルデバイス111との間のワイヤレス接続が途切れた場合に生体認証成功コンテキストを破棄するようにしてもよいし、ワイヤレス接続切断且つウェアラブルデバイスの取り外しをコンテキスト破棄の条件としてもよい。
【００７１】
本実施例では、ユーザが身に付けるウェアラブルデバイスに生体認証装置を備えないため、静脈認証装置や虹彩認証装置等の筐体寸法は大きめだが認証精度が高精度な生体認証装置を使用することができる。また、ウェアラブルデバイスはワイヤレス通信機能を内蔵するだけで良いので、小型化と省電力化が可能である。
【符号の説明】
【００７２】
１００　生体認証装置
１０１　携帯デバイス
１０２　PC
１０３　ドア入退管理
１０４　決済端末
１０５　サーバー
１０６　ウェアラブル生体認証
１０７　生体検知機能
１０８　リストバンド
１０９　開閉検知機構
１１０　電池
１１１　ウェアラブルデバイス

【図１】

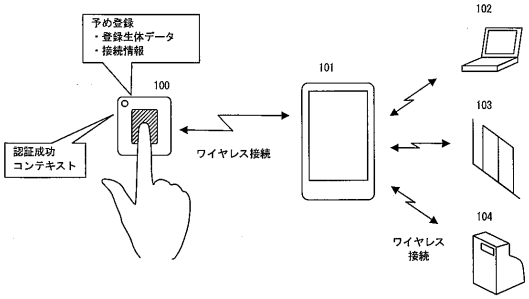

図１

【図２】

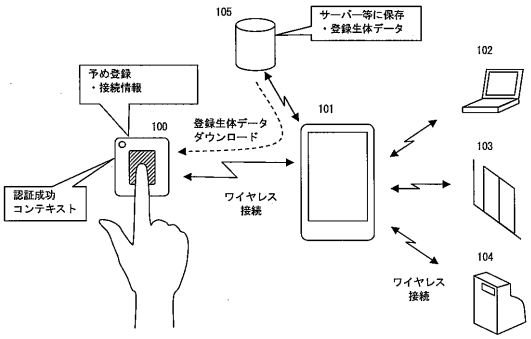

図２

【図３】

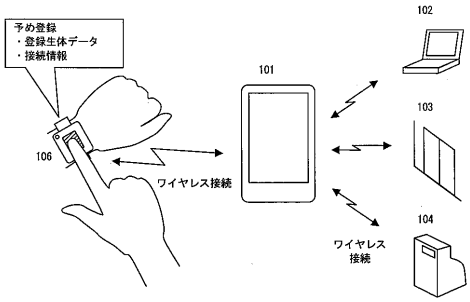

図３

【図４】

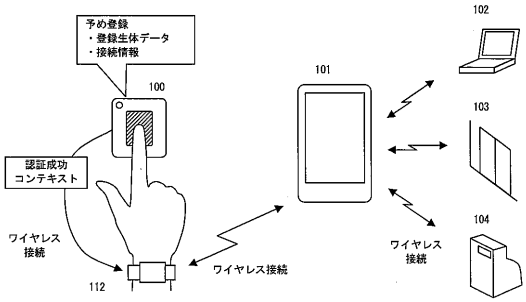

図４

【図５】

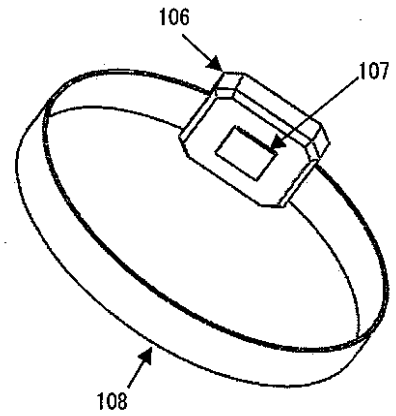

図５

【図６】

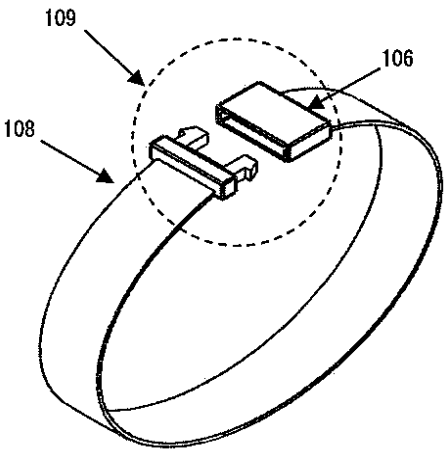

図６

【図７】

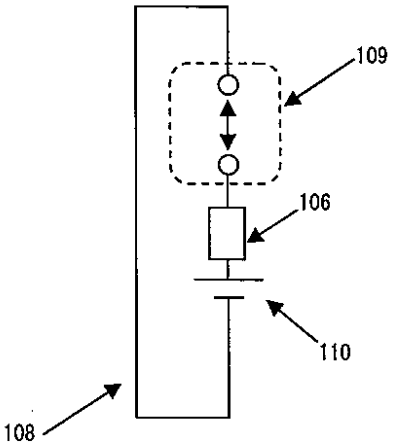

図７

【図８】

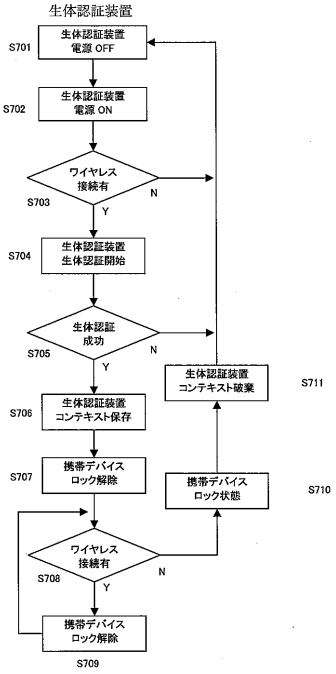

図８

【図９】

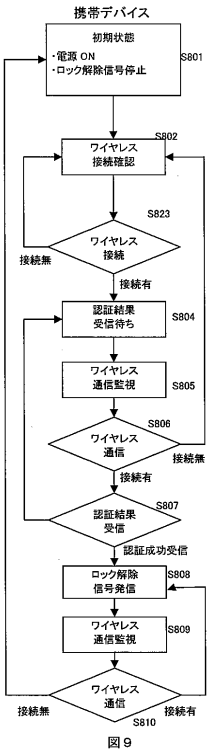

図９

【図１０】

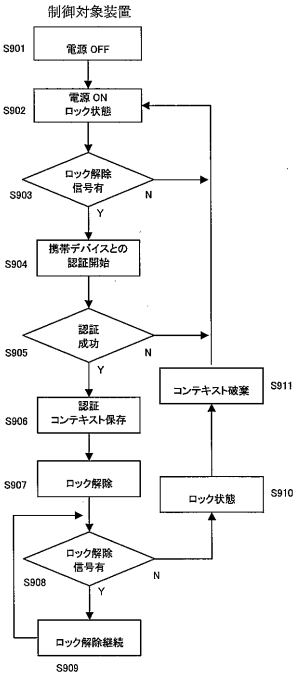

図１０

フロントページの続き

(56)参考文献 特開２００３－０８５１５０（ＪＰ，Ａ）
米国特許出願公開第２００９／００９４６８１（ＵＳ，Ａ１）
特開２００５－０７１２２５（ＪＰ，Ａ）
特開２０１３－０７８１７５（ＪＰ，Ａ）
特開２００３－０５８５０９（ＪＰ，Ａ）
特開２００８－０７３４６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／３０－Ｇ０６Ｆ２１／４６