(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6911171号
(P6911171)
(45)発行日　令和3年7月28日(2021.7.28)　(24)登録日　令和3年7月9日(2021.7.9)

(51)Int.Cl.　　F I
G06F 21/32 (2013.01)　G06F 21/32
G06F 21/44 (2013.01)　G06F 21/44　３５０
G06F 21/31 (2013.01)　G06F 21/31

請求項の数 10　(全 12 頁)

(21)出願番号　特願2020-66373(P2020-66373)
(22)出願日　令和2年4月2日(2020.4.2)
審査請求日　令和2年4月2日(2020.4.2)

(73)特許権者　000227205
ＮＥＣプラットフォームズ株式会社
神奈川県川崎市高津区北見方二丁目６番１号
(74)代理人　100103894
弁理士　家入　健
(72)発明者　了正　泰成
神奈川県川崎市高津区北見方二丁目６番１号　ＮＥＣプラットフォームズ株式会社内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】モバイル機器、生体認証制御方法および生体認証制御プログラム

(57)【特許請求の範囲】
【請求項１】
ユーザの生体認証の結果に基づいてロックを解除するか否かを決定するモバイル機器であって、
ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定し、
設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロックを解除する、
ことを特徴とするモバイル機器。
【請求項２】
前記ウェアラブル機器からの無線電波の受信電波強度が強いほど、前記認証閾値の値を、セキュリティレベルが低くなる値に設定する、
ことを特徴とする請求項１に記載のモバイル機器。
【請求項３】
前記ウェアラブル機器からの無線電波の受信電波強度に、さらに前記ウェアラブル機器と自モバイル機器との間の位置関係を示す情報を組み合わせて、前記セキュリティレベルとして適用する前記認証閾値を可変に設定する、
ことを特徴とする請求項１または２に記載のモバイル機器。

【請求項４】
前記ユーザの生体認証が失敗した場合、ロックを解除するための認証モードを、前記ユーザがパスワードを入力するパスワード認証モードに切り替えて、パスワード認証結果に基づいて、ロックを解除するか否かを決定する、
ことを特徴とする請求項１ないし３のいずれかに記載のモバイル機器。
【請求項５】
ロックを解除するための認証モードを、前記パスワード認証モードに切り替えた際に、前記ウェアラブル機器から受信した無線電波の受信電波強度に基づいて、または、前記ウェアラブル機器からの無線電波の受信電波強度に、さらに前記ウェアラブル機器と自モバイル機器との間の位置関係を示す情報を組み合わせた結果に基づいて、前記パスワードの桁数を可変に設定する、
ことを特徴とする請求項４に記載のモバイル機器。
【請求項６】
ユーザの生体認証の結果に基づいてモバイル機器のロックを解除するか否かを決定する生体認証制御方法であって、
前記モバイル機器は、
ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定する認証閾値可変設定ステップと、
設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロックを解除するロック解除ステップと、
を有することを特徴とする生体認証制御方法。
【請求項７】
前記認証閾値可変設定ステップでは、
前記ウェアラブル機器からの無線電波の受信電波強度が強いほど、前記認証閾値の値を、セキュリティレベルが低くなる値に設定する、
ことを特徴とする請求項６に記載の生体認証制御方法。
【請求項８】
前記認証閾値可変設定ステップでは、
前記ウェアラブル機器からの無線電波の受信電波強度に、さらに前記ウェアラブル機器と自モバイル機器との間の位置関係を示す情報を組み合わせて、前記セキュリティレベルとして適用する前記認証閾値を可変に設定する、
ことを特徴とする請求項６または７に記載の生体認証制御方法。
【請求項９】
前記ロック解除ステップでは、
前記ユーザの生体認証が失敗した場合、ロックを解除するための認証モードを、前記ユーザがパスワードを入力するパスワード認証モードに切り替えて、パスワード認証結果に基づいて、ロックを解除するか否かを決定する、
ことを特徴とする請求項６ないし８のいずれかに記載の生体認証制御方法。
【請求項１０】
ユーザの生体認証の結果に基づいてモバイル機器のロックを解除するか否かを決定する動作を前記モバイル機器のコンピュータによって実行する生体認証制御プログラムであって、
前記モバイル機器は、
ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定する認証閾値可変設定工程と、
設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロ

ックを解除するロック解除工程と、
を有することを特徴とする生体認証制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、モバイル機器、生体認証制御方法および生体認証制御プログラムに関し、特に、モバイル機器のロックを解除するために用いる生体認証のセキュリティレベルを制御するモバイル機器、生体認証制御方法および生体認証制御プログラムに関する。
【背景技術】
【０００２】
昨今、スマートフォンや携帯電話やタブレット端末や携帯ノートＰＣ（Personal Computer）等のモバイル機器は、高機能化が進み、各種の重要な情報を取り扱うようになってきており、成りすましによる情報の不正加工や情報の外部への漏洩を防止するためのセキュリティ対策が重要になってきている。
【０００３】
このため、成りすましを防止し、本人であることをより確実に認証する技術として、例えば、特許文献１の特開２０１７－２２４２５１号公報「端末装置および制御プログラム」等に記載されているように、近年のモバイル機器は、指紋認証や顔認証などの生体認証によるロック解除機構を備えており、パスワードやパターンロックを用いる代わりに、個人ごとに異なる生体情報を用いて、本人であることをより確実に確認して、ロックを解除することができるような仕組みが採用されるようになってきている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１７－２２４２５１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
前記特許文献１等に記載されているように、本発明に関連する現状の技術においては、指紋認証や顔認証等の生体認証を用いて、モバイル機器のロックを解除する技術が採用されるようになってきている。
【０００６】
しかしながら、例えば、生体認証として指紋認証を用いる場合は、ユーザの指が水に濡れていた場合や皮膚の状態等により、指紋認証に失敗して、ロックを解除することができない場合が多々発生する。また、顔認証を用いる場合においても、マスクをしている等で顔の特徴を十分に取得することができないような場合には、顔認証に失敗して、ロックを解除することができない。
【０００７】
つまり、現状の生体認証においては、認証の成否を判別するための認証閾値を示すセキュリティレベルとして、あらかじめ定めた一定のレベルが固定的に設定されていて、ユーザの使用状況や使用環境により、ロック解除機構が全く動作しなくなることがある。その結果、対象とするモバイル機器をユーザが使用することができなくなり、ユーザビリティを大いに損なってしまう事態を招いてしまうという解決するべき課題がある。
【０００８】
（本発明の目的）
本発明の目的は、かかる課題に鑑み、生体認証のセキュリティレベルを可変化する仕組みを有するモバイル機器、生体認証制御方法および生体認証制御プログラムを提供することにある。
【課題を解決するための手段】
【０００９】

前述の課題を解決するため、本発明によるモバイル機器、生体認証制御方法および生体認証制御プログラムは、次のような特徴的な構成を採用している。

【００１０】

（１）本発明によるモバイル機器は、

ユーザの生体認証の結果に基づいてロックを解除するか否かを決定するモバイル機器であって、

ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定し、

設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロックを解除する、

ことを特徴とする。

【００１１】

（２）本発明による生体認証制御方法は、

ユーザの生体認証の結果に基づいてモバイル機器のロックを解除するか否かを決定する生体認証制御方法であって、

前記モバイル機器は、

ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定する認証閾値可変設定ステップと、

設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロックを解除するロック解除ステップと、

を有することを特徴とする。

【００１２】

（３）本発明による生体認証制御プログラムは、

ユーザの生体認証の結果に基づいてモバイル機器のロックを解除するか否かを決定する動作を前記モバイル機器のコンピュータによって実行する生体認証制御プログラムであって、

前記モバイル機器は、

ユーザが装着しているウェアラブル機器との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになった該ウェアラブル機器から受信した無線電波の受信電波強度に応じて、前記ユーザの生体認証に関するセキュリティレベルの認証閾値を可変に設定する認証閾値可変設定工程と、

設定した前記認証閾値を適用して実施した前記ユーザの生体認証が成功した場合に、ロックを解除するロック解除工程と、

を有することを特徴とする。

【発明の効果】

【００１３】

本発明のモバイル機器、生体認証制御方法および生体認証制御プログラムによれば、主に、以下のような効果を奏することができる。

【００１４】

モバイル機器のロック状態を解除するための現状の生体認証技術においては、生体認証動作を正常に実施することができない場合が多々あり、モバイル機器を使用するユーザのユーザビリティを大きく損ねていた。これに対して、本発明においては、ユーザが常時装着しているウェアラブル機器からの受信電波強度に基づいて、モバイル機器における生体認証に適用するセキュリティレベルすなわち認証閾値を可変に設定することを可能にしているので、ユーザが意図していない要因により生体認証が失敗してしまうことを減少させ、ユーザビリティの向上を図ることができる。

【図面の簡単な説明】
【００１５】
【図１】本発明に係るモバイル機器の接続構成の一例を示す接続構成図である。
【図２】図１に示したモバイル機器の動作の一例を説明するためのフローチャートである。
【発明を実施するための形態】
【００１６】
以下、本発明によるモバイル機器、生体認証制御方法および生体認証制御プログラムの好適な実施形態について添付図を参照して説明する。なお、以下の説明においては、本発明によるモバイル機器および生体認証制御方法について説明するが、かかる生体認証制御方法をコンピュータにより実行可能な生体認証制御プログラムとして実施するようにしても良いし、あるいは、生体認証制御プログラムをコンピュータにより読み取り可能な記録媒体に記録するようにしても良いことは言うまでもない。また、以下の各図面に付した図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、本発明を図示の態様に限定することを意図するものではないことも言うまでもない。
【００１７】
（本発明の特徴）
本発明の実施形態の説明に先立って、本発明の特徴についてその概要をまず説明する。本発明は、ユーザが常時装着しているウェアラブル機器を利用することにより、該ウェアラブル機器とペアリングしたモバイル機器(スマートフォン、携帯電話、タブレット端末、携帯ノートＰＣ（Personal Computer）等)のロックを解除するために適用するセキュリティレベルを可変に制御することを主要な特徴とする。而して、本発明では、該モバイル機器のセキュリティを保持したまま、ユーザビリティを損なうことなく、該モバイル機器のロックを容易に解除することができる。
【００１８】
ここで、ユーザが常時身に着けているウェアラブル機器とは、例えば、腕時計（スマートウォッチ）、歩数計、血圧・脈拍計、メガネ、ゴーグル、ヘッドセット、ＩＣレコーダ等の情報機器のことである。これら情報機器の装着の形態には、リストバンド型、メガネ型、クリップ型等がある。自身の一つのウェアラブル機器のロックを解除して使用可能な状態に設定すると、Bluetooth（登録商標）やＷｉ－Ｆｉ等の通信機能により、他の情報機器との間で情報の送受信を行うことが可能である。
【００１９】
本発明の特徴についてさらに具体的に説明すると、次の通りである。ユーザは、身に着けている腕時計（スマートウォッチ）等のウェアラブル機器に関し、既に認証処理を行ってロックを解除済みの状態に設定して装着しているものとする。そして、ユーザが例えばスマートフォン等のモバイル機器を使用しようとする際に、該ユーザは、身に着けている認証済みのスマートウォッチ等のウェアラブル機器と、使用しようとする対象のモバイル機器との間で、互いの機器を認証し合うペアリング動作を行うことにより、両機器相互での無線通信が可能な状態に設定する。なお、本発明においては、「ペアリング」という用語を、Bluetooth通信特有の用語として用いているのではなく、Bluetooth通信のみならず、Ｗｉ－Ｆｉ通信等の他の無線通信も含めて用い、ウェアラブル機器とモバイル機器との双方が正しい通信相手として互いに認証し合う動作を行うことを意味している。
【００２０】
その結果、該モバイル機器は、該ウェアラブル機器からの無線電波を特定して受信することができる状態に移行すると、該モバイル機器は、該ウェアラブ機器から受信した無線電波の電波強度に基づいて、該ウェアラブ機器を装着しているユーザと自モバイル機器との間の距離を判別する。そして、該モバイル機器は、判別したユーザ（自モバイル機器を使用しようとしているユーザ）との間の距離に応じて、自モバイル機器のロックを解除するために用いるセキュリティレベルを可変に設定する。
【００２１】

つまり、ペアリング済みのウェアラブル機器からの受信電波強度の判定結果として、自モバイル機器を使用しようとしているユーザとの間の距離が近く、該ユーザが自モバイル機器のすぐ傍に居る状態であることを確認した場合であれば、ロックを解除するセキュリティレベルを或る程度低く設定しても、セキュリティ上の問題は無いものと判断することができる。したがって、自モバイル機器を使用しようとしているユーザからの距離が近ければ、自モバイル機器のロックを解除するためのセキュリティレベルを下げ、遠く離れていれば、セキュリティレベルを上げるように可変に制御する。

【００２２】

（実施形態の構成例）

次に、本発明に係るモバイル機器の実施形態について、その一例を説明する。図１は、本発明に係るモバイル機器の接続構成の一例を示す接続構成図であり、該モバイル機器を使用しようとするユーザが常時装着しているウェアラブル機器との間の接続状態を示している。言い換えると、図１においては、ウェアラブル機器２を常時装着しているユーザ３が、モバイル機器１を使用しようとして、該ユーザ３の生体情報（例えば指紋）を用いた生体認証を実施しようとしている状況を模式的に示している。なお、図１に示すウェアラブル機器２は、モバイル機器１のロックを解除するための生体認証を行うユーザが装着している機器として、例えば、腕時計（スマートウォッチ）のようなリストバンド型の機器を用いている場合を一例として示している。すなわち、図１の例では、ウェアラブル機器２はユーザ３の腕に装着されているものとする。

【００２３】

図１において、ユーザ３が常時装着しているウェアラブル機器２は既に認証済みの状態になっていて、他の機器例えばモバイル機器１との間で、無線電波を用いた無線通信（例えばBluetooth通信やＷｉ－Ｆｉ通信）により情報を送受信することが可能な状態に設定されているものとする。さらに、ウェアラブル機器２とモバイル機器１との間は、互いに相手の機器を通信相手として認証し合うBluetoothやＷｉ－Ｆｉ等の無線通信におけるペアリング動作が実施済みになっていて、互いの間で情報の送受信が可能な状態に設定されている。

【００２４】

また、モバイル機器１は、全体の動作を制御する制御部１０を実装していて、該制御部１０の一つとして、ユーザ３の生体認証を行う生体認証制御部１１を有している。そして、生体認証制御部１１は、生体認証を実施する際のセキュリティレベルを可変に設定することが可能な機能を有している。図１に示す実施形態においては、ウェアラブル機器２から受信した電波強度の「強」「中」「弱」の３段階の強度レベルに応じて、生体認証に関するセキュリティレベルを「低」「中」「高」の３段階に切り替えて設定することができる例を示している。

【００２５】

具体的には、図１に示すように、モバイル機器１は、制御部１０内に実装した不揮発性記憶領域のＲＯＭ（Read-Only Memory）に、セキュリティレベル登録テーブル１２としてウェアラブル機器２からの受信電波強度と生体認証に関するセキュリティレベルとの対応関係をあらかじめ設定登録している。ここで、セキュリティレベル登録テーブル１２の受信電波強度欄１２ａには、ウェアラブル機器２からの受信電波強度が強度閾値ａ以上に高い（強い）「強強度」の場合、強度閾値ａよりも低い（弱い）ものの強度閾値ｂ以上に高い（強い）「中強度」の場合、強度閾値ｂよりも低い（弱い）ものの、生体認証が不可能になる限界である強度閾値ｃ以上に高い（強い）「弱強度」の場合、生体認証が不可能になる限界である強度閾値ｃよりも低い(弱い)「対象外強度」の場合を登録している。

【００２６】

そして、受信電波強度欄１２ａの「強強度」「中強度」「弱強度」「対象外強度」それぞれに対応する形式で、セキュリティレベル登録テーブル１２のセキュリティレベル欄１２ｂには、生体認証に関するセキュリティレベルとして「低レベル」を示す「認証閾値Ａ」、「中レベル」を示す「認証閾値Ｂ」、「高レベル」を示す「認証閾値Ｃ」、生体認証

が不可能の旨を示す「生体認証不可能」をあらかじめ設定登録している。

【００２７】

モバイル機器１において、自モバイル機器１を使用しようとするユーザ３の生体認証を行う生体認証制御部１１は、該ユーザ３が装着しているペアリング済みのウェアラブル機器２から受信した無線電波の電波強度に基づいて、セキュリティレベル登録テーブル１２の設定内容を参照する。そして、ウェアラブル機器２からの受信電波強度が強度閾値ａ以上に高い（強い）「強強度」の場合には、該ウェアラブル機器２を装着しているユーザ３が自モバイル機器１の近傍に位置している状況にあり、自モバイル機器１のロック解除用の生体認証情報をより正確にユーザ３から取得することが可能になるので、生体認証対象として確認するチェック部分を少なく設定してもセキュリティ上の問題は少ないものと判定する。そして、セキュリティレベルとして、確実にかつ迅速に認証を完了させることが可能になるように、生体認証対象として確認するチェック部分を少なくした「低レベル」を示す「認証閾値Ａ」を用いて、該ユーザ３に関する生体認証を実施する。

【００２８】

また、ウェアラブル機器２からの受信電波強度が強度閾値ａよりも低く（弱く）強度閾値ｂ以上に高い（強い）「中強度」の場合は、該ウェアラブル機器２を装着しているユーザ３がモバイル機器１から少し離れた場所に位置している状況にあり、セキュリティレベルとして「中レベル」を示す「認証閾値Ｂ」を用いて、該ユーザ３に関する生体認証を実施する。

【００２９】

また、ウェアラブル機器２からの受信電波強度が強度閾値ｂよりも低く（弱く）、生体認証の限界値の強度閾値ｃ以上に高い（強い）「弱強度」の場合は、該ウェアラブル機器２を装着しているユーザ３がモバイル機器１から離れた場所に位置している状況にあり、セキュリティレベルとして「高レベル」を示す「認証閾値Ｃ」を用いて、該ユーザ３に関する生体認証を実施する。

【００３０】

また、ウェアラブル機器２からの受信電波強度が生体認証の限界値の強度閾値ｃよりもさらに低い（弱い）場合は、生体認証を用いることは不可能な状態にあると判定して、生体認証の代わりに、例えばパスワードによる認証を行う認証モードに切り替える。

【００３１】

（実施形態の動作例の説明）

次に、本発明に係る一実施形態として図１に示したモバイル機器１の動作について、図２のフローチャートを用いて説明する。図２は、図１に示したモバイル機器１の動作の一例を説明するためのフローチャートであり、モバイル機器１において、自モバイル機器１のロックを解除して使用しようとするユーザ３の生体認証を行う生体認証制御部１１に関する動作の一例を示している。なお、モバイル機器１を使用しようとしているユーザ３はウェアラブル機器２を常時装着していて、かつ、該ウェアラブル機器２は、認証済みとしてロックが解除済みの状態に設定され、無線電波を用いて、モバイル機器１等の他の機器との間で情報を送受信する動作を行うことが可能な状態になっているものとする。

【００３２】

図２のフローチャートにおいて、モバイル機器１の生体認証制御部１１は、ユーザ３からの使用要求を受け付けると、まず、当該ユーザ３が装着しているウェアラブル機器２との間のペアリングを実施済みであるか否かを確認する（ステップＳ１）。すなわち、自モバイル機器１とウェアラブル機器２とが通信相手として相互に認証し合うペアリング動作を実施済みであるか否かを確認する。ウェアラブル機器２との間のペアリングを実施済みであることを確認することができなかった場合には（ステップＳ１のＮｏ）、相手のウェアラブル機器２が通信相手として自モバイル機器１に登録済みの機器（すなわち自モバイル機器１の正しい通信相手となる機器）ではなかったか、登録済みの機器であってもウェアラブル機器２の動作が停止していたか、または、ユーザ３がウェアラブル機器２を装着していなかったか、あるいは、装着していてもモバイル機器１との間のペアリング動作が

未実施のままであったか、などの何らかの要因により、ユーザ３の生体情報を用いた認証動作の実施が不適当な状態になっている場合であると判定して、例えばパスワードによる認証を行う動作に移行するために、ステップＳ１１に移行する。

【００３３】

一方、ウェアラブル機器２との間のペアリングを実施済みであって、自モバイル機器１との間の無線電波による情報の送受信が可能な状態になっていることが確認された場合には（ステップＳ１のＹｅｓ）、ステップＳ２に移行して、ウェアラブル機器２から受信した無線電波の電波強度を測定する（ステップＳ２）。なお、ウェアラブル機器２は、前述したように、ロック解除の状態にあって、無線電波を常時送信している状態になっている。

【００３４】

生体認証制御部１１は、ウェアラブル機器２からの無線電波の電波強度を測定すると、セキュリティレベル登録テーブル１２を参照して、ウェアラブル機器２からのモバイル機器１における受信電波強度を、セキュリティレベル登録テーブル１２の受信電波強度欄１２ａの登録内容と比較する。そして、ウェアラブル機器２からのモバイル機器１における受信電波強度が受信電波強度欄１２ａの強度閾値ａ以上に高い「強強度」であった場合には（ステップＳ３のＹｅｓ）、対応するセキュリティレベルとしてセキュリティレベル登録テーブル１２のセキュリティレベル欄１２ｂに設定されている「低レベル」の「認証閾値Ａ」を設定して、設定したセキュリティレベルに応じた生体認証を実施するために、ステップＳ９に移行する（ステップＳ４）。

【００３５】

また、ウェアラブル機器２からのモバイル機器１における受信電波強度が受信電波強度欄１２ａの強度閾値ａよりも低いものの（ステップＳ３のＮｏ）、強度閾値ｂ以上に高い「中強度」であった場合には（ステップＳ５のＹｅｓ）、対応するセキュリティレベルとしてセキュリティレベル登録テーブル１２のセキュリティレベル欄１２ｂに設定されている「中レベル」の「認証閾値Ｂ」を設定して、設定したセキュリティレベルに応じた生体認証を実施するために、ステップＳ９に移行する（ステップＳ６）。

【００３６】

また、ウェアラブル機器２からのモバイル機器１における受信電波強度が受信電波強度欄１２ａの強度閾値ｂよりも低いものの（ステップＳ５のＮｏ）、生体認証の限界値である強度閾値ｃ以上に高い「弱強度」であった場合には（ステップＳ７のＹｅｓ）、対応するセキュリティレベルとしてセキュリティレベル登録テーブル１２のセキュリティレベル欄１２ｂに設定されている「高レベル」の「認証閾値Ｃ」を設定して、設定したセキュリティレベルに応じた生体認証を実施するために、ステップＳ９に移行する（ステップＳ８）。

【００３７】

さらに、ウェアラブル機器２からのモバイル機器１における受信電波強度が受信電波強度欄１２ａの強度閾値ｃよりも低い場合には（ステップＳ７のＮｏ）、ユーザ３の生体情報を使用した認証動作を実施することは不可能であると判定して、例えばパスワードによる認証を行う動作に移行するために、ステップＳ１１に移行する。

【００３８】

ステップＳ９に移行すると、ステップＳ４、ステップＳ６、ステップＳ８のいずれかにおいて設定されたセキュリティレベルに関する認証閾値（「認証閾値Ａ」または「認証閾値Ｂ」または「認証閾値Ｃ」）を適用して、ユーザ３の生体認証を実施する（ステップＳ９）。そして、設定された認証閾値においてユーザ３の生体認証が成功したか否か（すなわち、ロック解除を許可する認証が得られたか否か）を判定する（ステップＳ１０）。ユーザ３の生体認証が成功した場合には（ステップＳ１０のＹｅｓ）、モバイル機器１のロック状態を解除するために、ステップＳ１３に移行する。一方、ユーザ３の生体認証が成功しなかった場合には(ステップＳ１０のＮｏ)、生体認証以外の他の認証モードを用いて、ユーザ３の認証動作を再度実施するために（例えばパスワードによる認証を行う動作に

移行するために）、ステップＳ１１に移行する。

【００３９】

ステップＳ１１に移行すると、生体認証の実施が不可能な場合または生体認証に失敗した場合として、例えば認証用のパスワードの入力をユーザ３に促すメッセージを出力して、認証用のパスワードを入力してもらい、パスワードを使用した認証を実施する（ステップＳ１１）。パスワードを使用した認証が成功した場合には（ステップＳ１２のＹｅｓ）、モバイル機器１のロック状態を解除するために、ステップＳ１３に移行する。一方、パスワードを使用した認証も成功しなかった場合には(ステップＳ１２のＮｏ)、認証に失敗した旨をユーザ３に通知し、モバイル機器１のロック状態を解除することなく、生体認証制御部１１の動作を終了する。

【００４０】

ステップＳ１３に移行すると、認証に成功した旨をユーザ３に通知するとともに、モバイル機器１のロック状態を解除して（ステップＳ１３）、ユーザ３による操作を可能な状態に設定した後、生体認証制御部１１の動作を終了する。

【００４１】

なお、以上の説明においては、ユーザ３が常時装着しているウェアラブル機器２とモバイル機器１との間の距離（すなわちユーザ３とモバイル機器１との間の距離）を、ウェアラブル機器２からの無線電波のモバイル機器１における受信電波強度の値に基づいて、判定している場合を説明した。しかし、本発明は、かかる場合に限るものではなく、例えば、ウェアラブル機器２とモバイル機器１との間の位置関係（すなわちユーザ３とモバイル機器１との間の位置関係）例えばＧＰＳ（Global Positioning System）等の位置情報（緯度経度情報）に関する情報をさらに組み合わせて用いるようにも良い。言い換えると、ウェアラブル機器２からの受信電波強度に、さらにウェアラブル機器２と自モバイル機器１との間の位置関係を示す情報を組み合わせて、セキュリティレベルとして適用する認証閾値を可変に設定するようにしても良い。

【００４２】

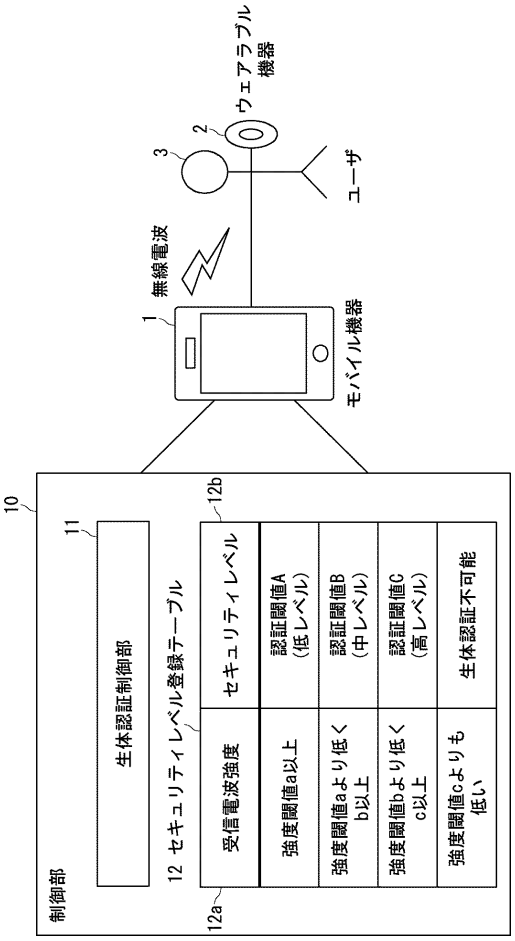
また、ユーザ３が常時装着しているウェアラブル機器２とモバイル機器１との間の距離（さらにウェアラブル機器２とモバイル機器１との位置関係を組み合わせた情報）に基づいて、生体認証に関するセキュリティレベルを示す認証閾値を「低」「中」「高」の３段階に切り替えて設定する場合について説明したが、３段階に限るものではなく、３段階よりも少なくしても良いし、あるいは、３段階以上にさらに増やしても良く、認証閾値を任意の段階数に設定することが可能である。さらには、生体認証に関するセキュリティレベルを示す認証閾値をウェアラブル機器２からの受信電波強度（さらにウェアラブル機器２とモバイル機器１との位置関係を組み合わせた情報）の関数として定義し、該受信電波強度（さらにウェアラブル機器２とモバイル機器１との位置関係を組み合わせた情報）の変化に応じて該認証閾値を連続的に変化させるようにしても良い。つまり、ウェアラブル機器２とモバイル機器１との位置関係を組み合わせた結果も含めても良いが、ウェアラブル機器２からの受信電波強度が強いほど、認証閾値の値を、セキュリティレベルが低くなるような値に設定するようにすれば良い。

【００４３】

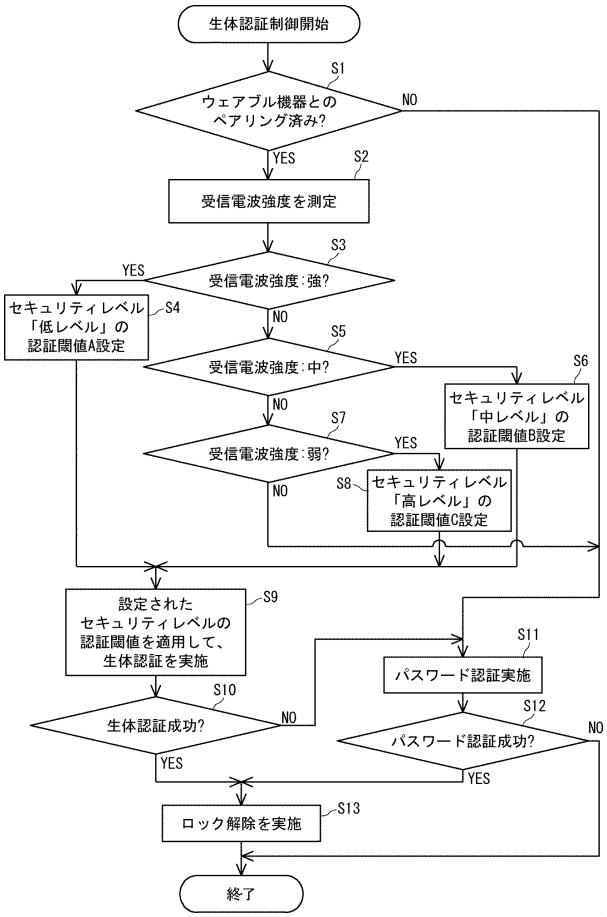
さらに、以上の説明においては、ユーザ３が装着しているウェアラブル機器２とモバイル機器１との間の距離（さらにウェアラブル機器２とモバイル機器１との間の位置関係を組み合わせた情報）に基づいて可変に設定するセキュリティレベルとして、生体認証に適用する認証閾値について説明したが、適用する認証モードとして、生体認証の場合に限るものではない。例えば、生体認証に失敗した場合に、ロック解除用の認証モードとしてパスワード認証に切り替える場合には、該パスワード認証においても、セキュリティレベルを可変に設定するようにしても良い。すなわち、パスワード認証を行う際に、ユーザ３が装着しているウェアラブル機器２とモバイル機器１との間の距離（さらにウェアラブル機器２とモバイル機器１との間の位置関係を組み合わせた情報）に基づいて、ロック解除用として用いるパスワードの桁数を任意の桁数に可変させるようにしても良い。

【００４４】
（実施形態の効果の説明）
以上に詳細に説明したように、本実施形態においては、以下のような効果が得られる。
【００４５】
すなわち、モバイル機器１のロック状態を解除するための現状の生体認証技術においては、生体認証動作を正常に実施することができない場合が多々存在し、モバイル機器１を使用するユーザ３のユーザビリティを大きく損ねていた。これに対して、本実施形態においては、ユーザ３が常時装着しているウェアラブル機器２からの受信電波強度に基づいて、モバイル機器１における生体認証に適用するセキュリティレベルすなわち認証閾値を可変に設定することを可能にしているので、ユーザ３が意図していない要因により生体認証が失敗してしまうことを減少させ、ユーザビリティの向上を図ることができる。
【００４６】
例えば、ユーザ３がモバイル機器１の近傍に位置していて、ウェアラブル機器２からの受信電波強度があらかじめ設定した強度閾値ａ以上に高い場合には、生体認証に適用する認証閾値を「低レベル」の認証閾値Ａに設定することにより、意図しない認証失敗を確実に減らすことができる。
【００４７】
以上、本発明の好適な実施形態の構成を説明した。しかし、かかる実施形態は、本発明の単なる例示に過ぎず、何ら本発明を限定するものではないことに留意されたい。本発明の要旨を逸脱することなく、特定用途に応じて種々の変形変更が可能であることが、当業者には容易に理解できよう。
【符号の説明】
【００４８】
１　　モバイル機器
２　　ウェアラブル機器
３　　ユーザ
１０　制御部
１１　生体認証制御部
１２　セキュリティレベル登録テーブル
１２ａ　受信電波強度欄
１２ｂ　セキュリティレベル欄
【要約】
【課題】生体認証のセキュリティレベルを可変化する仕組みを有するモバイル機器を提供する。
【解決手段】ユーザ３の生体認証の結果に基づいてロックを解除するか否かを決定するモバイル機器１内の制御部１０は、ウェアラブル機器２からの無線電波の受信電波強度に対応させて、ユーザ３の生体認証に関するセキュリティレベルとして適用する認証閾値を可変にあらかじめ設定登録したセキュリティレベル登録テーブル１２を有する。そして、モバイル機器１を使用しようとするユーザ３が常時装着しているウェアラブル機器２との間で通信相手として相互に認証し合うペアリングを実施し、ペアリング済みになったウェアラブル機器２から受信した無線電波の受信電波強度によりセキュリティレベル登録テーブル１２を検索した結果として、対応する認証閾値を取得し、取得した該認証閾値を適用して実施したユーザ３の生体認証が成功した場合に、ロックを解除する。
【選択図】図１

【図１】


ウェアラブル機器
2
3
ユーザ
無線電波
1
モバイル機器
10
制御部
11
生体認証制御部
12 セキュリティレベル登録テーブル
12b
12a
セキュリティレベル
受信電波強度
認証閾値A（低レベル）
強度閾値a以上
認証閾値B（中レベル）
強度閾値aより低くb以上
認証閾値C（高レベル）
強度閾値bより低くc以上
生体認証不可能
強度閾値cよりも低い

【図２】


生体認証制御開始
S1
ウェアブル機器とのペアリング済み?
NO
YES
S2
受信電波強度を測定
S3
受信電波強度:強?
YES
セキュリティレベル「低レベル」の認証閾値A設定
S4
NO
S5
受信電波強度:中?
YES
S6
セキュリティレベル「中レベル」の認証閾値B設定
NO
S7
受信電波強度:弱?
YES
S8
セキュリティレベル「高レベル」の認証閾値C設定
NO
S9
設定されたセキュリティレベルの認証閾値を適用して、生体認証を実施
S10
生体認証成功?
NO
YES
S11
パスワード認証実施
S12
パスワード認証成功?
NO
YES
S13
ロック解除を実施
終了

フロントページの続き

(56)参考文献 特表２０１８－５０４６５９（ＪＰ，Ａ）
特開２０１６－６２１３２（ＪＰ，Ａ）
特開２００７－２４９５８５（ＪＰ，Ａ）
特開２００７－１９７４８（ＪＰ，Ａ）
特開２０１４－１２３２１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１－２１／４６
Ｇ０６Ｔ　７／００
Ａ６１Ｂ　５／１１７