

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2008-223351
(P2008-223351A)

(43) 公開日 平成20年9月25日(2008.9.25)

(51) Int.Cl.	F I	テーマコード (参考)
E05B 49/00 (2006.01)	E05B 49/00 R	2E250
E05B 65/00 (2006.01)	E05B 65/00 E	3E048
E05B 65/02 (2006.01)	E05B 65/02 B	3K100
E05G 1/04 (2006.01)	E05B 65/02 D	4C038
G07F 17/12 (2006.01)	E05G 1/04	5B043

審査請求 未請求 請求項の数 7 O L (全 15 頁) 最終頁に続く

(21) 出願番号 特願2007-63731 (P2007-63731)
(22) 出願日 平成19年3月13日 (2007.3.13)

(71) 出願人 506077119
株式会社フロントフューチャー
群馬県高崎市飯塚町454-2
(74) 代理人 100104396
弁理士 新井 信昭
(72) 発明者 永井 和美
群馬県高崎市飯塚町454-2 株式会社
フロントフューチャー内
(72) 発明者 永塚 徹
群馬県佐波郡玉村町大字上之手2103
株式会社英技研内
Fターム(参考) 2E250 AA01 AA14 AA16 BB05 CC12
CC16 CC21 CC25 CC26 DD08
DD09 DD10 EE02 EE06 FF08
FF18 GG07 GG14 GG15
最終頁に続く

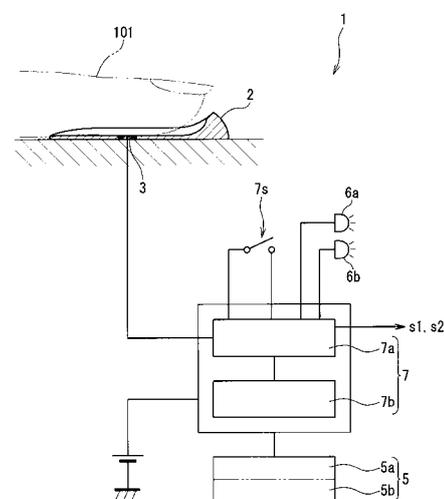
(54) 【発明の名称】 生体認証装置及び生体認証保管庫

(57) 【要約】 (修正有)

【課題】管理者によるロック解除の事実を利用者が知ることができるようにすることによって、管理者に心理的圧力をかけて不正な生体認証を未然防止する。

【解決手段】記憶部5を有する生体認証装置1において、当該記憶部には少なくとも1人の管理者生体情報を登録可能、かつ、1人のみの利用者生体情報を登録可能に構成する。登録された利用者生体情報は、利用者生体情報が認証された場合にのみ削除可能であって、管理者生体情報が認証された場合は、利用者生体情報は削除されない。利用者生体情報が削除されない状態で認証されたことはランプ6a、6bにより外部報知され、認証を受けようとした利用者が知りうるので、管理者に対して心理的圧力を与えることによって管理者の不正認証を抑止する。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

生体情報を検出するための生体センサーと、
当該生体センサーから予め入力された生体情報を登録するための記憶部と、
当該記憶部に記憶された生体情報と当該生体センサーから再入力された再入力生体情報とを照合して一致又は不一致を判定し一致したときに解錠信号を出力する生体認証部と、
を含めて構成してある生体認証装置において、
当該記憶部が、少なくとも 1 人分の管理者生体情報を登録可能な管理者記憶部と 1 人分のみの利用者生体情報を登録可能な利用者記憶部とを含めて構成してあり、
当該生体認証部が、
管理者生体情報を当該管理者記憶部に登録させるための管理者モードと利用者生体情報を当該利用者記憶部に登録させるための利用者モードとの間で切替可能に、さらに、
管理者モードにおいて少なくとも 1 人分の管理者生体情報が当該管理者記憶部に登録されていることを前提に、利用者モードにおいて当該生体センサーから入力された利用者生体情報を当該利用者記憶部に登録させた後又は登録と同時に施錠信号を出力するように、
さらに、
解錠信号を、利用者モードにおける管理者又は利用者の再入力生体情報との一致した場合にのみ出力するとともに、生体情報の一致が利用者に係るものである場合にのみ当該利用者記憶部に登録させてある利用者生体情報を消去させるように構成してある
ことを特徴とする生体認証装置。

10

20

【請求項 2】

前記管理者記憶部が、各管理者について出力された解錠信号について、解錠信号ごとに少なくとも日時を当該解錠信号出力に係る管理者と関連付けて記憶可能に構成してあることを特徴とする請求項 1 記載の生体認証装置。

【請求項 3】

前記生体情報が、指紋であり、
当該生体認証部が、当該生体センサーが検出した指紋情報における特徴点の位置、種類及び向きを照合するマニユシャ方式によって指紋照合するように構成してある
ことを特徴とする 1 又は 2 記載の生体認証保管庫。

【請求項 4】

前記生体認証部が、1 回のみ指紋照合によって認証可否を決定するように構成してある
ことを特徴とする請求項 3 記載の生体認証保管庫。

30

【請求項 5】

保管庫本体と、
当該保管庫本体に対して開閉する扉と、
当該保管庫本体に対する当該扉のロック及びロック解除を行うためのロック機構と、を含めて構成してあり、
当該ロック機構が、請求項 1 乃至 4 何れか記載の生体認証装置の利用者記憶部に利用者生体情報に記憶されたときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある
ことを特徴とする請求項 1 乃至 4 何れか記載の生体認証装置を備える生体認証保管庫。

40

【請求項 6】

前記ロック解除が、管理者の生体認証による場合であるときに、ロック解除を外部報知するための報知装置を設けてある
ことを特徴とする請求項 5 記載の生体認証保管庫。

【請求項 7】

データを電子的に保管するための保管庫と、
当該保管庫を電子的にロック及びロック解除を行うための電子キーと、を含めて構成してあり、

50

当該電子キーが、請求項 1 乃至 4 何れか記載の生体認証装置の利用者記憶部に利用者生体情報に記憶されたときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある

ことを特徴とする請求項 1 乃至 4 何れか記載の生体認証装置を備える生体認証保管庫。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、たとえば、金庫、集合住宅用簡易ポスト、コインロッカー等の物品を保管する保管庫、さらに、パソコンやUSBメモリー等のデータを電子的に保管する保管庫、に主として用いられる生体認証装置、及び、そのような生体認証装置を備える生体認証保管庫に関する。

10

【背景技術】

【0002】

たとえば、金庫やコインロッカーのような物の保管庫、さらには、パソコンやUSBメモリーのような電子データの保管庫の中には、利用者を制限するための生体認証装置が取り付けられたものがある（特許文献 1 参照）。特許文献 1 に記載された生体認証装置は、利用者の生体情報と記憶手段に記憶された記憶情報との照合結果に基づいて駆動手段を駆動させ扉のロックを解除するように構成されている。上述した生体認証装置は、利用者以外の第三者（本件明細書では「管理者」という）も、利用者と同様にロック又はロック解除できるように設定されるのが普通である。たとえば、利用者に事故があったとき、利用者が不在であるときに、その生体認証装置が設けられた保管庫のロックを利用者以外の誰も解除することができないとすると、余りにも不便であり実用性に欠けるからである。住宅の鍵にたとえれば、利用者である居住者が持つ鍵の他に、当該住宅の管理者が持つ鍵（マスターキー）を持つ場合の、管理者が上記第三者に該当する。利用者が、たとえば、鍵を紛失したときに、管理者（管理人）に頼んでマスターキーを使ってロック解除してもらうことができないとすると、紛失した鍵が見つからない限り永久に住宅に入ることができないことになる。マスターキーの必要性が理解されよう。

20

【特許文献 1】特開 2002 - 276222 号公報（段落 0004 以下、図 1 参照）

【発明の開示】

【発明が解決しようとする課題】

30

【0003】

しかしながら、先の住宅の例で述べたマスターキーの存在は、他方では管理者の不正の温床となりかねない。つまり、利用者が知らないうちに、金庫やコインロッカーを管理者によってロック解除されたり、パソコンの中身を管理者に覗かれたりする恐れがある。貴重品を預かるためのロッカーを、その管理者がマスターキーを使ってロック解除し、中に入れられていたキャッシュカードの情報を盗んだ（スキミングした）事件がかつてあった。ロック解除したロッカーは、マスターキーを使って再びロックしてしまえば、利用者はロック解除された事実を知ることがない。まして、盗まれたものが物理的なものであれば、利用者もその紛失に気が付くであろうが、キャッシュカード情報のような電子データでは気が付きようがない。このような事態は何らかの方法によって改善しなければならないが、これまでに有効な改善方法は提供されていない。本発明が解決しようとする課題は、上記例のように管理者が存在する場合に、管理者によるロック解除が行われたときに、その事実を利用者が知ることができるようにすることによって、管理者に心理的圧力をかけて不正なロック解除を未然防止することを目的とする。

40

【課題を解決するための手段】

【0004】

上述した課題を解決するために発明者は、管理者によるロック解除は、その利便性や実用性の上で不可欠であるものの、管理者によるロック解除を利用者が知ることができるようにすることが必須であると考えた。利用者の意思の届かないところでロック解除されたことを利用者が知ることによって、管理者に対する抑止作用を発揮させようとした。すな

50

わち、利用者以外には管理者しかロック解除できないという限られた環境の中において、利用者以外の者によってロック解除されればそのロック解除した者は自ずと管理者ということになるから、管理者は不正にロック解除することに心理的圧力を受ける。この心理的圧力を抑止力として不正なロック解除を防ぐのである。本発明は、利用者以外の第三者がロック解除した場合に、同第三者による再度のロックを不能とすることによって、ロック解除のままとなった状態を利用者が知ることによって、間接的に第三者によるロック解除を抑止できるように構成した。発明の詳しい内容は、項を改めて説明する。なお、何れかの請求項記載の発明を説明するに当たって行う用語の定義等は、その記載方法や記載順等にかかわらず、かつ、その性質上可能な範囲において他の請求項記載の発明にも適用があるものとする。

10

【0005】

(請求項1記載の発明の特徴)

請求項1記載の発明に係る生体認証装置(以下、適宜「請求項1の認証装置」という)は、生体情報を検出するための生体センサーと、当該生体センサーから予め入力された生体情報を登録するための記憶部と、当該記憶部に登録された生体情報と当該生体センサーから再入力された再入力生体情報とを照合して一致又は不一致を判定し一致したときに解錠信号を出力する生体認証部と、を含めて構成してある。ここで、当該記憶部は、少なくとも1人分の生体情報を登録可能な管理者記憶部と1人分のみの生体情報を登録可能な利用者記憶部とを含めて構成してある。また、当該生体認証部は、管理者生体情報を当該管理者記憶部に登録させるための管理者モードと利用者生体情報を当該利用者記憶部に登録させるための利用者モードとの間で切替可能に、さらに、管理者モードにおいて少なくとも1人分の管理者生体情報が当該管理者記憶部に登録されていることを前提に、利用者モードにおいて当該生体センサーから入力された利用者生体情報を当該利用者記憶部に登録させた後又は登録と同時に施錠信号を出力するように、さらに、解錠信号を、利用者モードにおける管理者又は利用者の再入力生体情報との一致した場合にのみ出力するとともに、生体情報の一致が利用者に係るものである場合にのみ当該利用者記憶部に登録させてある利用者生体情報を消去させるように構成してある。

20

【0006】

ここで、「生体情報」とは、指紋、声紋、静脈パターン、顔、虹彩、角膜、DNAパターン等のうち、少なくとも一つについての情報のことをいう。たとえば、指紋と静脈パターンのように複数の情報を組み合わせた情報であってもよい。生体情報の種類に合わせて生体センサーの種類も適宜選択される。管理者記憶部には単数又は複数的人数分の生体情報を記憶させることができる一方、利用者記憶部には一人分の生体情報しか記憶させることができない。つまり、二人目の利用者生体情報を記憶させる余地はどこにもない。

30

【0007】

請求項1の認証装置によれば、利用者記憶部に登録された生体情報と生体センサーを介して入力された利用者の再入力生体情報とを照合してそれらの一致不一致を生体認証部が照合する。照合の結果が一致したときは生体認証部から解錠信号が出力され、不一致のときは解錠信号が出力されない。管理者記憶部が管理者生体情報を登録するのは、生体認証部が管理者モードにあるときのみであって、利用者モードにあるときの管理者記憶部は登録を行わない。これとは逆に、利用者記憶部が利用者生体情報を登録するのは、生体認証部が利用者モードにあるときのみであって、管理者モードにあるときの利用者記憶部は登録を行わない。請求項1の認証装置の作動は、少なくとも1人分の管理者生体情報の登録が前提である。管理者の存在を前提とする認証装置だからである。利用者記憶部による利用者生体情報の登録されたことを示す施錠信号は、たとえば、金庫やUSBメモリー等のロックのトリガー信号として、また、解錠信号の出力は、同ロック解除のトリガー信号として、それぞれ利用することができる。解錠信号は、利用者モードにおける管理者生体情報の一致、さらに、利用者モードにおける利用者生体情報の一致において出力される。管理者モードは、管理者生体情報の登録にのみ利用可能であって、解錠信号出力には無関係である。解錠信号が出力され、かつ、その解錠信号出力の契機が利用者に係るものである

40

50

場合にのみ利用者記憶部に登録させてある利用者生体情報が消去される。その解錠信号出力の契機が管理者に係るものである場合の利用者生体情報は消去されない。消去されないから利用者記憶部に新たな生体情報（利用者生体情報又は管理者生体情報）を登録することはできない。すなわち、管理者生体情報によって解錠信号を出力させたときの管理者は、生体情報を登録できないから再度ロックの契機を得ることができない。つまり、管理者が利用者になりすますことを防止する。上記例でいえば、一旦ロック解除された金庫やUSBメモリー等は、開けたままの状態になり、管理者が再度ロックすることができない。開けたままの状態はセキュリティの面から見ると必ずしも好ましいことではないが、開けたままの状態はやがて解錠信号を出力させようとする利用者に発見されることが確実である。生体情報の認証という極めて高度な認証方式の下で解錠信号を出力させられるのは利用者以外の限られた者、すなわち、管理者だけといえることから、利用者に無断で解錠信号を出力させれば、その出力させた者はほぼ管理者に相違ないことになる。解錠信号を出力させたことが、その後、解錠信号を出力させようとした利用者に発見されることが確実である状態を作り出すことによって心理的圧力をかけ不正意図を持った管理者による解錠信号の出力を有効に抑止する。

10

【0008】

（請求項2記載の発明の特徴）

請求項2記載の発明に係る生体認証装置（以下、適宜「請求項2の認証装置」という）には、請求項1の認証装置の基本構造を備えさせた上で、前記管理者記憶部を、各管理者について出力された解錠信号について、解錠信号ごとに少なくとも日時を当該解錠信号出力に係る管理者と関連付けて記憶可能に構成することができる。

20

【0009】

請求項2の認証装置によれば、請求項1の認証装置の作用効果に加え、解錠信号の出力が管理者の操作によるものである場合に、どの管理者がいつ出力させたのかを管理者記憶部を閲覧することによって把握可能な状態を構成することができる。把握可能な状態は管理者に対する心理的圧力となり、これが、管理者による解錠信号の出力をさらに有効に抑制する。

【0010】

（請求項3記載の発明の特徴）

請求項3記載の発明に係る生体認証装置（以下、適宜「請求項3の認証装置」という）には、請求項1又は2の認証装置の基本構造を備えさせた上で、次のとおり構成することができる。すなわち、前記生体情報を、指紋とする。ここで、当該生体認証部が、当該生体センサーが検出した指紋情報における特徴点の位置、種類及び向きを照合するマニューシャ方式によって指紋照合するように構成してある。

30

【0011】

請求項3の認証装置によれば、請求項1又は2の認証装置の作用効果をマニューシャ方式で実現する。マニューシャ方式以外の方式を排除する趣旨ではないが、マニューシャ方式であれば、たとえば、指紋全体を照合するパターンマッチング方式に比べ本人受入率に差はないものの他人受入率において好ましい性能を一般に期待できることから、本発明において採用した。

40

【0012】

（請求項4記載の発明の特徴）

請求項4記載の発明に係る生体認証装置（以下、適宜「請求項4の認証装置」という）には、請求項3の認証装置の基本構造を備えさせた上で、前記生体認証部が、1回のみの指紋照合によって認証可否を決定するように構成することができる。

【0013】

請求項4の認証装置によれば、請求項3の認証装置の作用効果に加え、指紋照合の操作を必要最小限のものとするすることができる。すなわち、たとえば、パターンマッチング方式と比べたマニューシャ方式は、一般に、本人受入率は100%に近く劣るものではない一方、他人受入率が100分の1前後と桁違いに低いから複数回の指紋照合を経なくても充

50

分な他人排除効を得ることができるからである。なお、必要に雄応じて、複数回の指紋照合を排除する趣旨ではないことは言うまでもない。

【0014】

(請求項5記載の発明の特徴)

請求項5記載の発明に係る生体認証保管庫(以下、適宜「請求項5の保管庫」という)は、請求項1乃至4何れかの認証装置を備える保管庫である。請求項5の保管庫は、保管庫本体と、当該保管庫本体に対して開閉する扉と、当該保管庫本体に対する当該扉のロック及びロック解除を行うためのロック機構と、を含めて構成してある。ここで、当該ロック機構が、請求項1乃至4何れか記載の生体認証装置が施錠信号を出力したときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある。上記保管庫として、たとえば、金庫、各種ロッカー、机の引き出し、倉庫、自動車のトランク、オートバイの荷台に取り付ける保管庫がある。

10

【0015】

請求項5の保管庫によれば、保管庫本体に対する扉のロック又はロック解除を請求項1乃至4何れかの認証装置における登録作用及び認証作用に依存させることができる。ロック又はロック解除を直接行うのはロック機構であるが、このロック機構によるロックは同認証装置が施錠信号を出力したときであり、同じくロック解除は同認証装置から解錠信号が出力されたときである。請求項1乃至4何れかの認証装置の作用効果により、請求項5の保管庫の扉は利用者がロックを行うことができ、また、利用者及び管理者がロック解除を行うことができることになる。管理者がロック解除すると管理者による再度のロックができないので、管理者による不正意図を持ったロック解除を有効抑止することができる。

20

【0016】

(請求項6記載の発明の特徴)

請求項6記載の発明に係る生体認証保管庫(以下、適宜「請求項6の保管庫」という)は、請求項5の認証装置の基本構造を備えさせた上で、前記ロック解除が、管理者の生体認証による場合であるときに、ロック解除を外部報知するための報知装置を設けておくことができる。管理者の生体認証による場合に加え、利用者の生体認証による場合も、そのロック解除を外部報知するための報知装置を併せて設けることもできる。報知装置による報知方法には、たとえば、視覚に訴えるためのランプの点灯や点滅、聴覚に訴えるための警告音発生、通信ラインを介して監視用コンピュータへの連絡等がある。

30

【0017】

請求項6の保管庫によれば、請求項5の保管庫の作用効果に加え、管理者の生体認証に基づくロック解除が行われたときに、その事実を外部報知することによって、外部の目を保管庫に向けさせて不正なロック解除を抑止することが出来る。不正ではなく必要に応じたロック解除も外部報知の対象となるが、不正ではないので管理者には何ら問題は生じない。

【0018】

(請求項7記載の発明の特徴)

請求項7記載の発明に係る生体認証保管庫(以下、適宜「請求項7の保管庫」という)は、請求項1乃至4何れかの認証装置を備える保管庫である。請求項7の保管庫は、データを電子的に保管するための保管庫と、当該保管庫を電子的にロック及びロック解除を行うための電子キーと、を含めて構成してある。

40

当該電子キーが、請求項1乃至4何れか記載の生体認証装置の利用者記憶部に利用者生体情報に記憶されたときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある。ここで、当該電子キーが、請求項1乃至4何れか記載の生体認証装置が施錠信号を出力したときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある。上記保管庫として、たとえば、パーソナルコンピュータ(ハードディスク)、USBメモリー、PDA(Personal Digital Aid)、携帯電話等の電子機器がある。この場合の電

50

子キーとして、たとえば、上記電子機器を作動させるためのソフト上のキーがある。

【0019】

請求項7の保管庫によれば、保管庫本体に対する扉のロック又はロック解除を請求項1乃至4何れかの認証装置における登録作用及び認証作用に依存させることができる。ロック又はロック解除を直接行うのは電子キーであるが、この電子キーによるロックは同認証装置が施錠信号を出力したときであり、同じくロック解除は同認証装置から解錠信号が出力されたときである。請求項1乃至4何れかの認証装置の作用効果により、請求項5の保管庫の扉は利用者がロックを行うことができ、また、利用者及び管理者がロック解除を行うことができることになる。管理者がロック解除すると管理者による再度のロックができないので、管理者による不正意図を持ったロック解除を有効抑止することができる。

10

【発明の効果】

【0020】

生体認証装置又は生体認証装置を備える保管庫に管理者が存在する場合に、管理者によるロック解除が行われたときに、その事実を利用者が知ることができるので、その心理的圧力により管理者の不正なロック解除を未然防止することができる。

【発明を実施するための最良の形態】

【0021】

各図を参照しながら、本発明を実施するための最良の形態（以下、「本実施形態」という）について説明する。本実施形態に係る生体認証装置は、指紋情報を生体情報とする指紋認証装置である。図1は指紋認証装置を備える保管庫の正面図である。図2は、図1に示す指紋認証装置のA-A断面図と電気的構成とを示す図である。図3は、マニユシャ方式を説明するための図である。図4は、記憶部の記憶内容を示す図である。図5は、管理者登録をする手順を示すフローチャートである。図6は、施錠手順を示すフローチャートである。図7は、解錠手順を示すフローチャートである。図8は、本実施形態の変形例を示す正面図である。

20

【0022】

（指紋認証装置の概略構造）

図1及び2を参照しながら、指紋認証装置の概略構造について説明する。指紋認証装置1は、指紋センサー（生体センサー）3と、記憶部5と、指紋認証部7と、から概ね構成してある。指紋センサー3は、指101の皮膚表面103（図3参照）の3次元パターンによる光強度を2次元的に検出するセンサーである。符号2は、指紋センサー3を保持するとともに、指101が指紋センサーに対する適正位置に来るようにガイドするための指ガイドを示している。指紋センサー3によって検出された指紋パターンが、指紋情報（生体情報）となる。記憶部5は、RAMによって構成してあり、その記憶エリアを2つに分けてある。その2つの記憶エリアのうち一方の記憶エリアを管理者の指紋情報（管理者指紋情報）をその管理者と関連付けて登録するための管理者記憶部5aとして、また、他方の記憶エリアを利用者の指紋情報（利用者指紋情報）をその利用者に関連付けて登録するための利用者記憶部5bと、して使用できるように構成してある。指紋認証部7は、画像プロセッサ7aとパターン認識ユニット7bとにより構成してある。画像プロセッサ7aは、指紋センサー3から入力された指紋情報を画像処理するためのものである。パターン認識ユニット7bは、画像プロセッサ7aによって生成された指紋パターンの特徴（後述）を抽出し、抽出された特徴を所定の登録情報（後述する）と比較することによって、その一致不一致を判定し一致した場合にその一致を示す解錠信号を出力するように構成してある。なお、指紋認証装置1を稼働させるための電源は、電池でもよいし商用電源でもよい。

30

40

【0023】

また、指紋認証部7は、指紋センサー3から入力された管理者指紋情報及び利用者指紋情報を記憶部5（管理者記憶部5a、利用者記憶部5b）に登録させる機能を有している。登録させるときの指紋認証部7は、指紋情報の種類に合わせて管理者モードと利用者モードの2種類のモードに切り替えることができるようになっている。管理者モードは、管

50

理者指紋情報を登録したり削除したりするときのモードであり、利用者モードは、利用者指紋情報を登録するときのモードである。モードの切替は、スイッチ7sを介して行うようになっている。スイッチ7sは、上述したモード切替と電源スイッチとしての機能を兼ね備えている。すなわち、スイッチ7sを押すと電源がオンとなり利用者モードがスタートする。利用者モードの状態ですwitch7sを所定時間（たとえば、10秒間）押し続けることにより管理者モードがスタートし、さらに続けて所定時間（たとえば、5秒間）押し続けることにより管理者登録の削除が行われるようにプログラム設定してある。さらに、指紋認証部7には、図1及び2に示すように、利用者指紋情報の登録の有無を視覚的に確認できるようにするためのランプ6a及びランプ6bを接続しておくことが好ましい。この場合において、ランプ6aは利用者指紋情報の登録がない場合にのみ点灯するように、また、ランプ6bは同じく登録がある場合にのみ点灯するように、それぞれ構成してある。

【0024】

（記憶部の内容）

図2及び4を参照しながら、管理者記憶部5a及び利用者記憶部5bの内容について説明する。図2が示す管理者記憶部5aには、少なくとも1人の管理者の管理者ID(K1, K2, K3)、指紋情報(図4に示す「)は指紋情報ありの意)が登録可能、さらに、ロック解除(解錠信号の出力)の日時(図4では、管理者K1が2007年月日の20時18分に解錠)が併せて登録可能に構成されている。管理者指紋情報を登録した管理者の数は、少なくとも1人いれば足りるが、複数人(本実施形態では3人)とすることもできる。他方、利用者記憶部5bには1人分(図4の「R」)の利用者指紋情報のみ登録可能であり、複数人分の指紋情報を登録することはできない。なお、図4に示す利用者Rの指紋登録欄は空白であるから利用者指紋登録が行われていない状態、つまり、保管庫51(図1参照)が空き状態を示している。利用者指紋登録が行われれば、利用者Rの指紋登録欄に「)が付与されることになる。

【0025】

（指紋の認証方式）

図3を参照しながら、指紋の認証方式について説明する。本実施形態では、指紋センサー3が検出した指紋情報における特徴点の位置、種類及び向きを照合するマニューシャ方式を採用した。パターンマッチ方式等に比べて本人受入率において差異なく他人受入率において格段に低い(識別力が高い)からである。マニューシャ方式では、図3に示すような指紋パターン105が有する端点(指紋の終点)105a、分岐点(指紋が分岐する点)105b及び三角州(指紋が三方に伸びる点)105cを特徴点として捉え、これらの特徴点の位置、種類及び向きを照合して両指紋情報の一致不一致を判定する方式である。マニューシャ方式によれば、1回の照合において本人受入率がほぼ99.96%、同じく他人受入率がほぼ0.0001%であると一般にいわれている。非常に高精度であるといえよう。

【0026】

（指紋認証装置の適用例）

図1及び2を参照しながら、指紋認証装置1の適用例について説明する。図1に示す符号51は保管庫を示し、保管庫51は正面開口の箱型の保管庫本体53と、保管庫本体53の正面開口を閉鎖開放する扉55と、から外觀構成してある。保管庫本体53に対する扉55の開閉は、保管庫本体53に向かって側端に設けたヒンジ54, 54の働きによる。扉55の向かって左側には、扉55の開閉を行うための開閉ノブ57を取り付けてある。開閉ノブ57は、破線で示すロック機構58の一部を構成する。ロック機構58は、保管庫本体53に対して扉55をロックするための機構である。ロック機構58は、扉55側に設けたソレノイド58a及びソレノイド58aから出沒するプランジャー58bと、保管庫本体53側に設けた係止片58cから概ね構成してある。ソレノイド58aは、進出したときに係止片58cに引っ掛かって扉55の開放を阻止するとともに、没入したときに同引っ掛かりを解除して扉55の開放を許容する。ソレノイド58aの制御は、指紋

認証装置 1 によって行われるようになっている。具体的な制御方法については、指紋認証装置 1 の処理手順の中で説明する。符号 5 9 は、保管庫本体 5 3 の上面に取り付けた吊り下げ取っ手を示す。

【 0 0 2 7 】

(指紋認証装置の処理手順)

図 1 乃至 6 を参照しながら、保管庫 5 1 に取り付けられた指紋認証装置 1 の処理手順について説明する。処理を行うプログラムは、指紋認証部 7 に格納されている、その指紋認証部 7 が実行することにより以下に述べる処理が行われるようになっている。処理は、管理者の指紋情報の登録から始まる。指紋認証装置 1 は、少なくとも 1 人の管理者の存在を前提として作動するようになっているからである。前述したように管理者指紋情報の登録は、切り替えによって指紋認証部 7 を管理者モードとしたときに行うことができる。通常状態の指紋認証部 7 は利用者モードになっており、指紋認証部 7 が備えるスイッチ 7 s を、10 秒間押し続けることによって管理者モードに切り替えられるようになっている。また、本実施形態では、管理者モードに切り替えられた状態から、スイッチ 7 s をさらに 5 秒間押し続けることによって管理者モードの中で既に登録された管理者指紋情報を削除できるように構成してある。

【 0 0 2 8 】

以下、図 5 に示すフローチャートを主として参照しながら、保管庫 5 1 (指紋認証装置 1) の処理手順を具体的に説明する。ここでの保管庫 5 1 は、未使用であることを前提とする。スイッチ 7 s (図 1 及び 2 参照) が押されると指紋認証装置 1 の電源をオンして (S 1)、ランプ 6 a を点灯させる (S 2)。指紋認証装置 1 は利用者モードにある。ここで、スイッチ 7 s が連続して 10 秒間、管理者によって押され続けられた場合の指紋認証部 7 は、利用者モードから管理者モードへの切替を行う (S 3 , S 5)。管理者モードへ切り替えられたところで、スイッチ 7 s が、さらに、5 秒間、管理者によって押され続けられた場合の指紋認証部 7 は、管理者記憶部 5 a の登録を全部削除する (S 9)。ここでは、初期設定であるから削除されるべき管理者指紋情報が存在しないが、存在している場合はその登録人数に関わらず全員の管理者指紋情報が削除される。全員分を削除するように構成したのは、そもそも個別削除を否定する趣旨ではないが個別削除を可能とすると削除対象の選択等の手順が必要となり煩雑であるから、そのような煩雑な手順を省略するためである。S 7 において 5 秒間の押され続けがなかった場合は、S 9 を飛び越えて S 1 1 へ進む。S 1 1 における指紋認証部 7 は、管理者指紋情報の入力を待ち、入力されたところでその入力された管理者指紋情報を管理者記憶部 5 a に登録させる (S 1 3)。登録を完了した指紋認証部 7 は、所定時間 (本実施形態では 10 秒間) の経過を待って電源を自動的オフにする (S 1 5、S 1 7)。電源の自動オフは節電のためである。電源オフにより、ランプ 6 a が自動消灯し、上記プログラムを終了する。管理者を複数名登録する場合は、S 1 以下の手順で再度登録することができる。管理者記憶部 5 a には、登録の順番に従い個々の管理者指紋情報が登録される。図 4 に示すように、ここでは K 1 及び K 2 の 2 名を登録した。

【 0 0 2 9 】

次は、図 6 に示すフローチャートを参照しながら、利用者モードにある指紋認証部 7 の処理手順について説明する。スイッチ 7 s (図 1 及び 2 参照) が押されると指紋認証装置 1 の電源をオンして (S 2 1)、ランプ 6 a を点灯させる (S 2 3)。ランプ 6 a の点灯が保管庫 5 1 の空きを示す。したがって、扉 5 5 を開けて保管庫本体 5 3 の前面開口を開放し、保管物 (図示を省略) を中に入れ扉 5 5 を閉鎖することができる。指紋認証装置 1 は、今、利用者モードにある。ここで指紋認証部 7 は、管理者記憶部 5 a をサーチして管理者指紋登録の有無を確認し、管理者指紋登録があった場合は S 2 7 へ進む。管理者指紋登録がなかった場合は、点灯しているランプ 6 a を点滅させ (S 2 8) S 3 7 へ進む。点滅状態が 10 秒間続くと電源がオフされランプ 6 a は自動消灯する (S 3 7、S 3 9)。ここで S 2 7 に戻る。S 2 7 では、指紋センサー 3 からの利用者指紋情報の入力を待ち、入力があったら入力された利用者指紋情報を利用者記憶部 5 b に登録する (S 2 9)。登録

10

20

30

40

50

したところで使用中を示すランプ6 bを点灯させるとともに、点灯しているランプ6 aを消灯させる(S 3 1, S 3 3)。さらに、利用者指紋情報の登録が完了した旨を示す施錠信号s 1を出力する(S 3 5)。施錠信号s 1の出力により利用者記憶部5 bの登録エリアは満杯になり、それ以上の登録ができない状態になる。上述したS 2 9 ~ S 3 5は、同時に行ってもよいし図6に示す順番と異なる順番で実行させてもよい。施錠信号s 1は、ソレノイド5 8 aを励起してプランジャー5 8 bを進出させて係止片5 8 cに係止させる(図1参照)。この係止により保管庫本体5 3に対して扉5 5がロックされた状態になる。施錠信号s 1を出力した指紋認証部7は、所定時間(本実施形態では10秒間)の経過を待って電源を自動的オフにする(S 3 7、S 3 9)。電源オフにより、点灯していたランプ6 bが自動消灯する。

10

【0030】

図7を参照しながら、保管庫5 1の解錠手順について説明する。保管庫5 1の解錠は管理者指紋情報を登録してある管理者K 1及び管理者K 2と、利用者Rの3人だけである(図4参照)。まず、スイッチ7 sが押されて電源がオンとなったところで(S 5 1)、指紋認証装置1は、ランプ6 bを点灯させる(S 5 3)。ランプ6 bの点灯は、保管庫5 1が使用中であることを示す。モードは、利用者モードである。ここで指紋認証部7は指紋センサー3からの指紋情報の入力を待ち(S 5 5)、入力されたところでその入力された指紋情報と記憶部5(管理者記憶部5 a、利用者記憶部5 b)に登録されている指紋情報(管理者指紋情報、利用者指紋情報)の各々と照合を行う(S 5 7)。指紋照合の結果、指紋が一致の場合はS 6 1へ進み、不一致(不明瞭も含む)の場合はS 8 1へ進む。S 6 1へ進んだ指紋認証部7は、その一致に係る指紋が管理者のものか、又は、利用者のものかを判定する。判定は、一致に係る登録指紋情報の登録エリアが、管理者記憶部5 aなのか、又は、利用者記憶部5 bなのかをサーチすることによって行う(図4参照)。

20

【0031】

S 6 1において入力された指紋が利用者のものである場合において、指紋認証部7は、点灯していたランプ6 bを消灯させるとともにランプ6 aを点灯させる(S 6 3、S 6 5)。S 6 1で利用者のもとと判断された場合はその時点で利用者モードも解除され、したがって、ランプ6 bの消灯が「空き」を示す機能もキャンセルされる。ここで指紋認証部7は、解錠信号s 2を出力するとともに利用者記憶部5 bに登録されている利用者指紋情報を削除する(S 6 7、S 6 9)。解錠信号s 2はソレノイド5 8 a(図1参照)を励起してプランジャー5 8 bを後退させ、その結果、係止片5 8 cとの係止を解除する。つまり、扉5 5が解錠された状態にする。扉5 5の解錠は、利用者の行為によるものであって管理者の行為によるものではないから、それまでに管理者による不正解錠がなかったことになる。不正解錠があったなら、不正解錠を行った管理者はその扉5 5を再度施錠できないので、利用者が解錠しようとしたときに扉5 5が解錠状態にあったはずであるが、上記場合には解錠状態になかったからである。利用者指紋情報を削除した指紋認証部7は、その10秒間後に電源をオフにする(S 7 3、S 7 5)。電源オフにより、ランプ6 aも消灯する。S 6 9の利用者指紋情報削除により、保管庫5 1の「空き」状態が確定する。

30

【0032】

S 5 9の説明に戻る。S 5 9において指紋照合の結果一致しなかった場合の指紋認証部7は、その旨を管理者又は利用者に知らせるためにランプ6 bを点滅させる(S 8 1)。5秒間の点滅の後、ランプ6 bを消灯させ(S 8 3、S 8 5)、S 5 3へ戻り通常の点灯を行わせる。次は、S 6 1の説明に戻る。S 6 1において、照合した指紋が管理者のものである場合の指紋認証部7は、ランプ6 aとランプ6 bとを交互点滅させ(S 8 7)、S 8 9へ進む。保管庫5 1が解錠され、その解錠が利用者ではなく管理者であることを外部報知するためである。管理者による解錠が何らかの正当理由に基づくものであれば管理者にとって外部報知は何ら心理的圧力を受ける要因とはならないが、不正解錠である場合はそれを強く受ける。心理的圧力は、管理者の不正解錠を抑止する有効な力となる。S 8 9における指紋認証部7は、利用者記憶部5 aを検索して指紋が照合した管理者(たとえば、図4に示す管理者K 1)の特定を行い(S 8 9)、その特定した管理者と関連付けて解錠

40

50

日時を管理者記憶部 5 a 登録する (S 9 1)。解錠日時の登録は、 S 8 7 で行ったランプ点滅とともに、不正解錠の心理的圧力を管理者に与えるためである。解錠日時の登録を終えた指紋認証部 7 は、解錠信号 s 2 を出力してから (S 9 3) S 7 3 へ進み 1 0 秒後に電源をオフする (S 7 5)。これによって、ランプ 6 a 及びランプ 6 b も消灯する。

【 0 0 3 3 】

S 6 1 において管理者側と利用者側とに分岐された後、両者間で最も特徴的な差異は、利用者指紋情報削除の有無である (S 6 9)。指紋認証部 7 から解錠信号 s 2 が出力され、かつ、その解錠信号出力の契機が利用者に係るものである場合にのみ利用者記憶部 5 b に登録させてある利用者指紋情報が消去される。その解錠信号出力の契機が管理者に係るものである場合の利用者指紋情報は消去されない。消去されないから利用者記憶部 5 b に新たな指紋情報を登録することはできない。すなわち、管理者指紋情報によって解錠信号 s 2 を出力させたときの管理者は、自分の指紋情報を登録できないから再度ロックの契機を得ることができない。つまり、管理者が利用者になりすますことを防止する。開けたままの状態はセキュリティの面から見ると必ずしも好ましいことではないが、開けたままの状態はやがて解錠信号を出力させようとする利用者に見られることが確実である。指紋情報の認証という極めて高度な認証方式の下で解錠信号を出力させられるのは利用者以外の限られた者、すなわち、管理者だけといえることから、利用者に無断で解錠信号 s 2 を出力させれば、その出力させた者はほぼ管理者に相違ないことになる。解錠信号 s 2 を出力させたことが、解錠信号 s 2 を出力させようとした利用者に見られることが確実である状態を作り出すことによって心理的圧力をかけ不正意図を持った管理者による解錠信号の出力を有効に抑制する。

【 0 0 3 4 】

(本実施形態の変形例)

図 8 を参照しながら、本実施形態の変形例 (以下、「本変形例」という) について説明する。本変形例に係る保管庫は、データを電子的に保管するための U S B 本体 (保管庫) 6 1 と、 U S B 本体を電子的にロック及びロック解除を行うためのプログラム上の電子キー 6 3 と、を含めて構成してある。電子キー 6 3 は、指紋センサー 3 をその一部とする指紋認証装置 1 によって構成してある。電子キー 6 3 は、本実施形態におけるロック機構 5 8 と同様な機能を果たし、指紋認証装置 1 の利用者記憶部に利用者生体情報に記憶されたときにロックを行うように、また、前記解錠信号が出力されたときにロック解除を行うように、構成してある。なお、本実施形態が備えるスイッチ 7 s は、本変形例ではソフト上で起動させるように構成してある。したがって、 U S B 本体 6 1 は、物理的なスイッチを有しない。

【 図面の簡単な説明 】

【 0 0 3 5 】

【 図 1 】指紋認証装置を備える保管庫の正面図である。

【 図 2 】図 1 に示す指紋認証装置の A - A 断面図と電氣的構成とを示す図である。

【 図 3 】マニユシャ方式を説明するための図である。

【 図 4 】記憶部の記憶内容を示す図である。

【 図 5 】管理者登録をする手順を示すフローチャートである。

【 図 6 】施錠手順を示すフローチャートである。

【 図 7 】解錠手順を示すフローチャートである。

【 図 8 】本実施形態の変形例を示す正面図である。

【 符号の説明 】

【 0 0 3 6 】

1	指紋認証装置
3	指紋センサー
5	記憶部
5 a	管理者記憶部
5 b	利用者記憶部

10

20

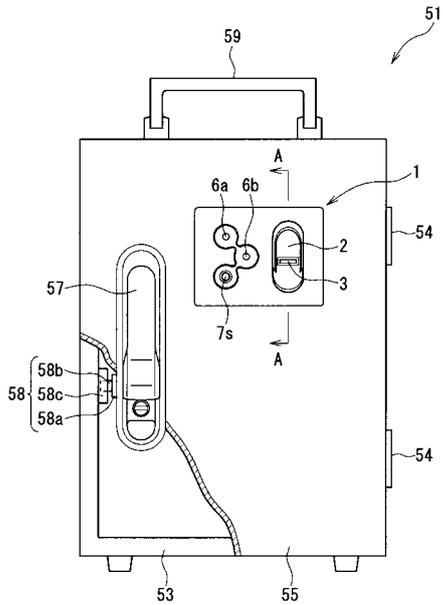
30

40

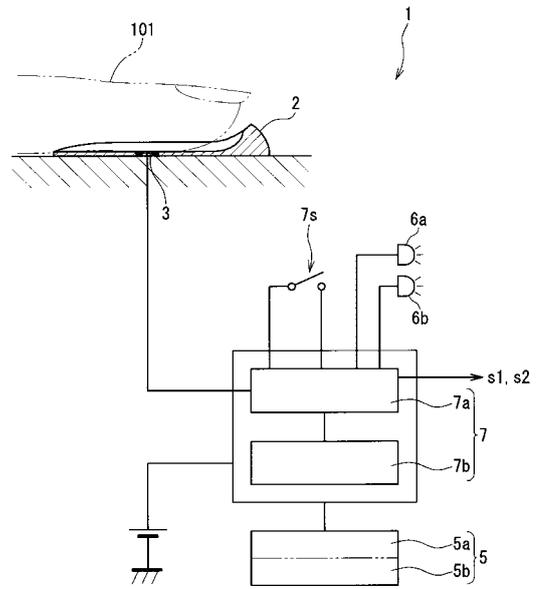
50

- 6 a , 6 b ランプ
- 7 指紋認証部
- 7 s スイッチ
- 5 1 保管庫
- 5 3 保管庫本体
- 5 5 扉
- 5 7 開閉ノブ
- 5 8 ロック機構
- 5 9 吊り下げ取っ手
- 6 3 電子キー
- 1 0 1 指
- 1 0 3 皮膚表面
- 1 0 5 指紋パターン
- K 1 , K 2 管理者
- R 利用者

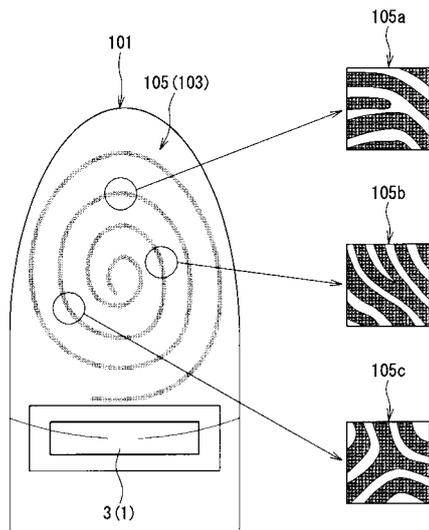
【 図 1 】



【 図 2 】



【 図 3 】



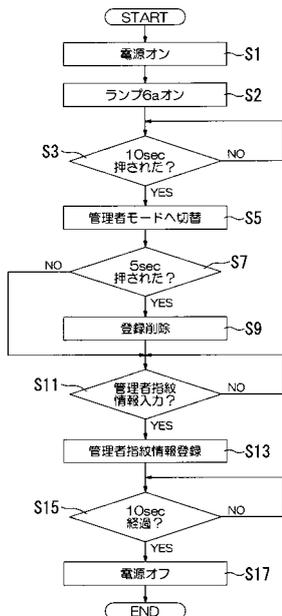
【 図 4 】

5

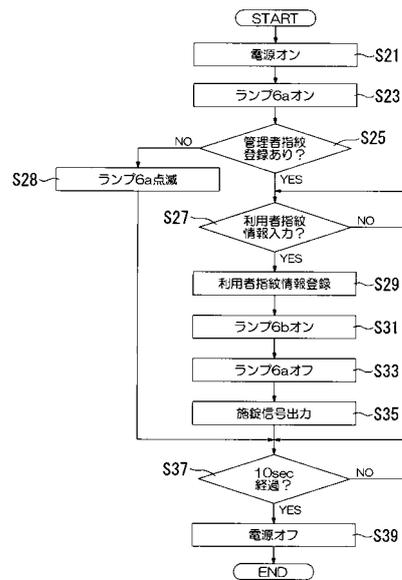
	指紋登録	解錠日時
K1	○	2007年△月□日 20:18
K2	○	
K3		
R		

5a (bracketed rows K1-K3)
5b (bracketed row R)

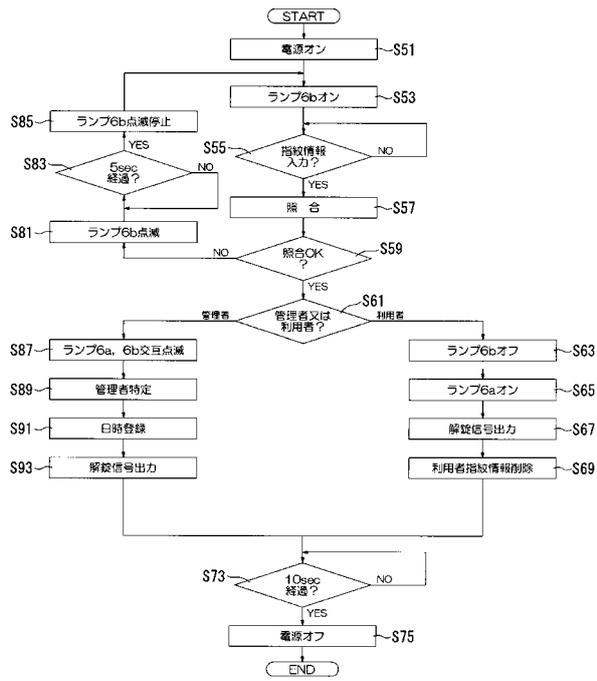
【 図 5 】



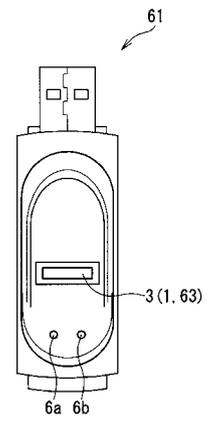
【 図 6 】



【 図 7 】



【 図 8 】



フロントページの続き

(51)Int.Cl.	F I	テーマコード(参考)
A 4 7 G 29/122 (2006.01)	G 0 7 F 17/12	
G 0 6 T 7/00 (2006.01)	A 4 7 G 29/122	Z
A 6 1 B 5/117 (2006.01)	G 0 6 T 7/00	5 1 0 B
	A 6 1 B 5/10	3 2 2

Fターム(参考) 3E048 CA03 CA17
3K100 CA45 CA49
4C038 FF01 FF05 FG01 VA07 VB13
5B043 AA04 AA09 BA01 BA02 BA03 BA04 CA05 DA05 DA06 EA06
EA07 EA08 FA06 FA07 FA10 GA02