

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第4643043号
(P4643043)

(45) 発行日 平成23年3月2日 (2011.3.2)

(24) 登録日 平成22年12月10日 (2010.12.10)

(51) Int.Cl.

G 0 6 T 7 / 0 0 (2006.01)

F I

G 0 6 T 7 / 0 0 5 1 0 B

請求項の数 5 (全 12 頁)

(21) 出願番号	特願2001-75966 (P2001-75966)	(73) 特許権者	000003078
(22) 出願日	平成13年3月16日 (2001.3.16)		株式会社東芝
(65) 公開番号	特開2002-279424 (P2002-279424A)		東京都港区芝浦一丁目1番1号
(43) 公開日	平成14年9月27日 (2002.9.27)	(74) 代理人	100084618
審査請求日	平成19年12月21日 (2007.12.21)		弁理士 村松 貞男
		(74) 代理人	100092196
			弁理士 橋本 良郎
		(74) 代理人	100091351
			弁理士 河野 哲
		(74) 代理人	100088683
			弁理士 中村 誠
		(74) 代理人	100070437
			弁理士 河井 将次
		最終頁に続く	

(54) 【発明の名称】 個人認証装置および個人認証方法

(57) 【特許請求の範囲】

【請求項 1】

被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する認証手段と、

この認証手段による認証時、前記被認証者の少なくとも顔画像を取得する画像入力手段と、

前記認証手段により前記被認証者が認証された際、そのとき前記画像入力手段により取得された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する認証履歴記憶手段と、

前記認証手段により前記被認証者が認証された際、そのとき前記画像入力手段により取得された当該被認証者の顔画像を含む当該認証結果、および、前記認証履歴記憶手段に記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する表示手段と、

を具備したことを特徴とする個人認証装置。

【請求項 2】

前記認証履歴は、前回認証時の被認証者の顔画像、認証日時および認証場所などで構成されることを特徴とする請求項 1 記載の個人認証装置。

【請求項 3】

被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する認証手段と、

10

20

前記被認証者が自己の少なくとも顔画像を入力する画像入力手段と、

前記認証手段により前記被認証者が認証された際、前記画像入力手段により入力された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する認証履歴記憶手段と、

前記認証手段により前記被認証者が認証された際、前記画像入力手段により入力された当該被認証者の顔画像を含む当該認証結果、および、前記認証履歴記憶手段に記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する表示手段と、

を具備したことを特徴とする個人認証装置。

【請求項 4】

10

被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する第 1 のステップと、

この第 1 のステップによる認証時、前記被認証者の少なくとも顔画像を取得する第 2 のステップと、

前記第 1 のステップにより前記被認証者が認証された際、そのとき前記第 2 のステップにより取得された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する第 3 のステップと、

前記第 1 のステップにより前記被認証者が認証された際、そのとき前記第 2 のステップにより取得された当該被認証者の顔画像を含む当該認証結果、および、前記第 3 のステップにより記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する第 4 のステップと、

20

を具備したことを特徴とする個人認証方法。

【請求項 5】

被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する第 1 のステップと、

前記被認証者が自己の少なくとも顔画像を入力する第 2 のステップと、

前記第 1 のステップにより前記被認証者が認証された際、前記第 2 のステップにより入力された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する第 3 のステップと、

前記第 1 のステップにより前記被認証者が認証された際、前記第 2 のステップにより入力された当該被認証者の顔画像を含む当該認証結果、および、前記第 3 のステップに記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する第 4 のステップと、

30

を具備したことを特徴とする個人認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、たとえば、鍵、磁気カード、ＩＣカードなどの物理的媒体、もしくは、指紋、網膜、虹彩、掌形、顔画像などの生体情報を基に被認証者が本人であるか否かを認証し、その認証結果に基づきセキュリティを重視する建物や部屋への入室管理を行なう個人認証装置および個人認証方法に関する。

40

【0002】

【従来の技術】

最近、たとえば、鍵、磁気カード、ＩＣカードなどの物理的媒体、もしくは、指紋、網膜、虹彩、掌形、顔画像などの生体情報を基に被認証者が本人であるか否かを認証し、その認証結果に基づきセキュリティを重視する建物や部屋への入室管理を行なう個人認証装置が開発されている。

【0003】

【発明が解決しようとする課題】

しかしながら、従来の物理的媒体を用いた個人認証装置では、利用者は「他人が自分の力

50

ードを使って認証されはしないか」、「偽造されたカードで他人が認証されていないか」といった不安を持つことがある。

【0004】

また、生体情報を用いた個人認証装置では、利用者は「知らない間に他の誰かが自分になりすまして認証されているのではないか」といった不安を持つことがある。

【0005】

そこで、本発明は、他の誰かが自分になりすまして認証されていないかどうかを、利用者自身が手間をかけることなく恒常的に確認でき、利用者が安心して、かつ、確信を持って個人認証を行なうことができる個人認証装置および個人認証方法を提供することを目的とする。

10

【0006】

また、本発明は、悪意のある第三者になりすましがあつた場合にそれが判明し易くなり、悪意のある第三者になりすましを抑制する効果が得られる個人認証装置および個人認証方法を提供することを目的とする。

【0007】

また、本発明は、保護者や管理者などが、家族もしくは被管理者の認証履歴を恒常的にチェックでき、認証スコアの低下や認証頻度の異常などの、システムや利用者の異常を早期に発見できるようになる個人認証装置および個人認証方法を提供することを目的とする。

【0008】

さらに、本発明は、認証されたときに表示される認証結果を利用者が選択でき、利用者の満足度を高めることができる個人認証装置および個人認証方法を提供することを目的とする。

20

【0009】

【課題を解決するための手段】

本発明の個人認証装置は、被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する認証手段と、この認証手段による認証時、前記被認証者の少なくとも顔画像を取得する画像入力手段と、前記認証手段により前記被認証者が認証された際、そのとき前記画像入力手段により取得された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する認証履歴記憶手段と、前記認証手段により前記被認証者が認証された際、そのとき前記画像入力手段により取得された当該被認証者の顔画像を含む当該認証結果、および、前記認証履歴記憶手段に記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する表示手段とを具備している。

30

【0010】

また、本発明の個人認証方法は、被認証者が所持する物理的媒体および被認証者の生体情報のうち少なくともいずれか一方を基に前記被認証者が本人であるか否かを認証する第1のステップと、この第1のステップによる認証時、前記被認証者の少なくとも顔画像を取得する第2のステップと、前記第1のステップにより前記被認証者が認証された際、そのとき前記第2のステップにより取得された当該被認証者の顔画像を含む当該認証結果を認証履歴として記憶する第3のステップと、前記第1のステップにより前記被認証者が認証された際、そのとき前記第2のステップにより取得された当該被認証者の顔画像を含む当該認証結果、および、前記第3のステップにより記憶されている前回認証時の被認証者の顔画像を含む認証履歴を前記被認証者に対して表示する第4のステップとを具備している。

40

【0011】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【0012】

まず、第1の実施の形態について説明する。

【0013】

50

図 1 は、第 1 の実施の形態に係る個人認証装置の構成を概略的に示すものである。この個人認証装置は、たとえば、被認証者が本人であるか否かを認証し、その認証結果に基づきセキュリティを重視する建物や部屋への入室管理を行なうもので、被認証者 100 が所持する鍵、磁気カード、IC カードなどの物理的媒体、もしくは、指紋、網膜、虹彩、掌形、顔画像などの生体情報を基に被認証者 100 が本人であるか否かを認証する認証手段としての認証部 101、被認証者 100 の少なくとも顔画像を取得する画像入力手段としての画像入力部 102、認証部 101 により被認証者 100 が認証された際、そのとき画像入力部 102 により取得された当該被認証者 100 の顔画像を含む当該認証結果を認証履歴として記憶する認証履歴記憶手段としての認証履歴記憶部 103、認証部 101 により被認証者 100 が認証された際、そのとき画像入力部 102 により取得された当該被認証者 100 の顔画像を含む当該認証結果、および、認証履歴記憶部 103 に記憶されている前回認証時の被認証者の顔画像を含む認証履歴を被認証者 100 に対して表示する表示手段としての画像合成部 104 および表示部 105、認証部 101 の認証結果に基づき入室管理を行なう部屋のドア 107 を開閉制御するドア制御部 106 によって構成されている。

10

【0014】

以下、全体的な処理の流れについて図 2 に示すフローチャートを参照して説明する。

【0015】

まず、画像入力部 102 は、被認証者（利用者）100 の顔画像を撮像して入力する（ステップ S1）。一方、認証部 101 は、通常の鍵と錠前とによる適合チェック、あるいは、磁気カードや IC カードによる認証など、被認証者 100 が所持する物理的媒体による個人認証を行なうか、あるいは、指紋、網膜、虹彩、掌形、顔画像など、被認証者 100 の生体情報に基づく個人認証を行なう（ステップ S2）。

20

【0016】

なお、認証部 101 における認証方法としては、たとえば、文献 1（坂野鋭，中村逸一．「認証技術の現在と未来」．情報処理，Vol.41,No7,pp.816-822,July 2000.）、あるいは、文献 2（Alex Pentland Tanzeem Choudhury. "Face Recognition for Smart Environments". IEEE Computer Magazine, Vol.49, No.2, pp.50-55, February 2000.）に記載されている認証方法が適用可能である。

【0017】

次に、認証履歴記憶部 103 は、認証部 101 の認証結果、および、そのとき画像入力部 102 で入力された被認証者 100 の顔画像を認証履歴として記憶する（ステップ S3）。この際、認証部 101 の認証結果が成功である（本人であると判断した）場合（ステップ S4）、その認証成功の結果と、認証履歴記憶部 103 内の前回認証時の認証履歴とが画像合成部 104 により画像合成されて表示部 105 に表示され、被認証者 100 に通知される（ステップ S5）とともに、ドア制御部 106 に「ドア開」の命令を与えることによりドア 107 を開放する（ステップ S6）。

30

【0018】

一方、認証部 101 の認証結果が失敗である（本人ではないと判断した）場合（ステップ S4）、ドア 107 は開放せず、認証失敗の結果が画像合成部 104 により表示部 105 に表示される（ステップ S7）。

40

【0019】

ここで、画像合成部 104 により表示部 105 に表示される認証結果と認証履歴の一例を図 3 に示す。図 3 に示すように、今回の認証結果（画像入力部 102 で入力された被認証者 100 の顔画像 B を含む）A を表示するとともに、前回の認証履歴 C を表示する。なお、前回の認証履歴としては、認証の成功 / 失敗、認証日時、認証場所、認証時の被認証者の顔画像などを表示すればよい。

【0020】

このようにして、過去の認証履歴を記憶、表示することで、過去に誰かが自分になりすまして認証を受けようとした（もしくは、認証を受けてしまった）場合、それが履歴として

50

残る。そして、真の利用者が認証を受けた際に、そのなりすましの結果が履歴として表示される。そのため、利用者自身がなりすましが起こったことを発見することができる。

【0021】

逆に、前回認証された結果が確かに利用者自身のものであれば、「前回の認証から今回の認証までに、他人のなりすましは一切なかった」ということが保証されるため、利用者は認証システムを安心と確信を持って使用することができる利点がある。特に、認証時の顔画像が表示されることにより、真の利用者は他人によるなりすましなどの異常に気付きやすくなる。

【0022】

このような確認が認証のたびに、恒常的に他人のなりすましがいないことを確認することができる。そのため、第三者のなりすましが発覚しやすく、そのような行為を抑止する効果も大きい。

【0023】

なお、図4に示すように、前回の認証履歴Cを複数表示するようにしてもよい。この場合、表示する認証履歴の数、認証情報やその形式は、利用者もしくは管理者もしくはその両方が設定することができる。図4において、C1は認証結果、C2は認証時の顔画像である。また、図5に示すように、認証時の顔画像C2を間引きして並べて表示したり、複数の画像入力部で入力された認証者の画像を表示するようにしてもよい。

【0024】

なお、認証部101として顔画像による認証技術を用いる場合、全体的な構成は図6に示すようになる。この場合、認証部101は、被認証者100の顔画像を入力する画像入力部101a、および、この画像入力部101aで入力された顔画像を辞書データと照合することにより被認証者100が本人であるか否かを認証する処理部101bから構成される。なお、画像入力部101aは図1の画像入力部102を兼ねることができるため、必ずしも別途画像入力部を備える必要はない。

【0025】

次に、第2の実施の形態について説明する。

【0026】

図7は、第2の実施の形態に係る個人認証装置の構成を概略的に示すものである。第2の実施の形態は、前述した第1の実施の形態に対して、被認証者100が所持する個人認証情報記録媒体（携帯形情報記録媒体）110に過去（前回）の認証履歴情報を記録する点、および、それに伴い認証履歴記憶部103が認証履歴処理部109に置き換わった点が異なり、その他は第1の実施の形態と同様であるので、以下、異なる点についてだけ説明する。

【0027】

被認証者100は、自身を証明するID情報などが記録されている磁気カードやICカードなどからなるIDカードなどの個人認証情報記録媒体108を所持しており、これを提示して認証を受けるものとする。そして、本実施の形態では、認証時、個人認証情報記録媒体110に過去の認証履歴情報を記録する。

【0028】

個人認証情報読取部110は、被認証者100が提示する個人認証情報記録媒体108からID情報や過去の認証履歴を読取り、認証履歴処理部109に送る。個人認証情報記録部111は、認証履歴処理部109から送られる今回の認証結果（被認証者100の顔画像を含む）を認証履歴として個人認証情報記録媒体108に記録する。

【0029】

以下、全体的な処理の流れについて図8に示すフローチャートを参照して説明する。

【0030】

まず、画像入力部102は、被認証者100の顔画像を撮像して入力する（ステップS11）。これと平行して、被認証者100は、所持する個人認証情報記録媒体108を提示して認証を受ける（ステップS12）。

10

20

30

40

50

【0031】

すなわち、被認証者100は、個人認証情報記録媒体108を個人認証情報読取部110に挿入することにより、個人認証情報読取部110は、その個人認証情報記録媒体108からID情報を読取り、認証履歴処理部109に送る。認証履歴処理部109は、個人認証情報記録媒体108から読取ったID情報を認証部101へ送る。認証部101は、たとえば、個人認証情報記録媒体108から読取ったID情報をあらかじめ登録されているID情報と一致するか否かを照合することにより、被認証者100が本人であるか否かを認証し、その認証結果を認証履歴処理部109へ送る。

【0032】

なお、この場合、認証部101は、個人認証情報記録媒体108のみを基に個人認証を行なってもよいし、被認証者100の指紋などの生体情報を基にした他の認証技術を併用してもよい。

10

【0033】

これと平行して、個人認証情報読取部110は、このときセットされている個人認証情報記録媒体108から過去の認証履歴を読取り、認証履歴処理部109に送る（ステップS13）。また、このとき、認証履歴処理部109は、認証部101の認証結果（今回の認証結果）、および、そのとき画像入力部102で入力された被認証者100の顔画像を認証履歴として、個人認証情報記録部111を介して個人認証情報記録媒体108に記録する（ステップS14）。

【0034】

20

次に、認証履歴処理部109は、認証部101の認証結果が成功である（本人であると判断した）場合（ステップS15）、その認証成功の結果と、個人認証情報記録媒体108から読取った過去（前回認証時）の認証履歴とを画像合成部104により画像合成して表示部105に表示し、被認証者100に通知する（ステップS16）とともに、ドア制御部106に「ドア開」の命令を与えることによりドア107を開放する（ステップS17）。

【0035】

一方、認証部101の認証結果が失敗である（本人ではないと判断した）場合（ステップS15）、ドア107は開放せず、認証失敗の結果が画像合成部104により表示部105に表示される（ステップS18）。

30

【0036】

このようにして、個人認証情報記録媒体108に過去の認証履歴を記録することにより、個人認証装置側で認証履歴を保持し、複数の個人認証装置で認証履歴を共有する必要がなくなるといった利点がある。

【0037】

たとえば、図9に示すように、複数の個人認証装置で個人認証を行なう場合を考える。個人認証情報記録媒体を用いない場合においては、図9（a）に示すように、複数の個人認証装置1，2間で認証履歴記憶部3内の履歴情報を共有するために履歴情報共有手段4が必要であり、有線や無線のネットワークなどを構築する必要がある。

【0038】

40

これに対し、第2の実施の形態のように、個人認証情報記録媒体108を用いる場合においては、図9（b）に示すように、複数の個人認証装置5，6間で履歴情報を共有するための履歴情報共有手段4が不要になり、システムを安価に構築できる。

【0039】

なお、認証部101として顔画像による認証技術を用いる場合、全体的な構成は図10に示すようになる。この場合、認証部101は、被認証者100の顔画像を入力する画像入力部101a、および、この画像入力部101aで入力された顔画像を辞書データと照合することにより被認証者100が本人であるか否かを認証する処理部101bから構成される。なお、画像入力部101aは図7の画像入力部102を兼ねることができるため、必ずしも別途画像入力部を備える必要はない。

50

【 0 0 4 0 】

次に、第 3 の実施の形態について説明する。

【 0 0 4 1 】

図 1 1 は、第 3 の実施の形態に係る個人認証装置の構成を概略的に示すものである。第 3 の実施の形態は、前述した第 1 の実施の形態に対して、個人設定記憶部 1 1 2 が追加された点がり、その他は第 1 の実施の形態と同様であるので、以下、異なる点についてだけ説明する。

【 0 0 4 2 】

個人設定記憶部 1 1 2 は、たとえば、図 1 2 に示すように、ある利用者がどの利用者に対して管理権を持っているかの管理情報を保持する。たとえば、ID 情報 = 3 の利用者が ID 情報 = 6 , 7 の利用者に対して管理権を持っているとする。そして、ID 情報 = 3 の利用者が認証を受けたとすると、画像合成部 1 0 4 は、個人設定記憶部 1 1 2 に保持された図 1 2 の管理情報を参照することにより、図 1 3 に示すように、過去の認証履歴 C として、ID 情報 = 3 の利用者（本人）の認証履歴 C 3 だけでなく、ID 情報 = 6 , 7 の利用者の認証履歴 C 4 をも同時に表示部 1 0 5 に表示する。

10

【 0 0 4 3 】

このような個人認証装置を、たとえば、一般住宅の入口に適用した場合、両親が子供に対して管理権を持つように設定すれば、両親が認証を受けるたびに子供の認証履歴が表示され、子供の ID 情報がなりすましされていないかなどを恒常的に容易に確認することができるようになる。

20

【 0 0 4 4 】

また、このような個人認証装置を、たとえば、オフィスの機密の高い部屋の入口に適用した場合、管理者や上司が他の入室者に対して管理権を持つように設定すれば、管理者が認証を受けるたびに他の入室者の認証履歴が表示され、それらの ID 情報がなりすましされていないかなどを恒常的に容易に確認することができるようになる。

【 0 0 4 5 】

次に、第 4 の実施の形態について説明する。

【 0 0 4 6 】

第 4 の実施の形態に係る個人認証装置の構成は、前述した第 1 の実施の形態と同様であるが、今回の認証結果の表示に用いる被認証者 1 0 0 の顔画像を、被認証者 1 0 0 が選択設定できる点が第 1 の実施の形態とがり、その他は第 1 の実施の形態と同様であるので、以下、異なる点についてだけ説明する。

30

【 0 0 4 7 】

画像合成部 1 0 4 は、画像入力部 1 0 2 が辞書登録時もしくは個人認証の際に取得した、それぞれが表情の異なる複数（本例では 1 2 個）の顔画像 D を、たとえば、図 1 4 に示すように表示部 1 0 5 に表示し、被認証者 1 0 0 に対して好みの顔画像を選択するように案内する。ここで、被認証者 1 0 0 は、図示しないキーボードなどの操作により、表示部 1 0 5 に表示された複数の顔画像の中から自分の好みの顔画像を選択し、自己画像として設定する。

【 0 0 4 8 】

次に、第 5 の実施の形態について説明する。

40

【 0 0 4 9 】

図 1 5 は、第 5 の実施の形態に係る個人認証装置の構成を概略的に示すものである。第 5 の実施の形態は、前述した第 1 の実施の形態に対して、被認証者 1 0 0 が自己の顔画像を入力する画像入力手段としてのスキャナなどの登録画像入力部 1 1 3 が追加された点がり、その他は第 1 の実施の形態と同様であるので、以下、異なる点についてだけ説明する。

【 0 0 5 0 】

被認証者 1 0 0 は、自分で用意した写真などの顔画像を登録画像入力部 1 1 3 により入力し、認証履歴記憶部 1 0 3 内に設定記憶（登録）する。画像合成部 1 0 4 は、今回の認証

50

結果を表示する際、被認証者 1 0 0 の顔画像として認証履歴記憶部 1 0 3 内に登録された顔画像を用いる。

【 0 0 5 1 】

【発明の効果】

以上詳述したように本発明によれば、他の誰かが自分になりすまして認証されていないかどうかを、利用者自身が手間をかけることなく恒常的に確認でき、利用者が安心して、かつ、確信を持って個人認証を行なうことができる個人認証装置および個人認証方法を提供できる。

【 0 0 5 2 】

また、本発明によれば、悪意のある第三者になりすましがあった場合にそれが判明し易くなり、悪意のある第三者になりすましを抑制する効果が得られる個人認証装置および個人認証方法を提供できる。

10

【 0 0 5 3 】

また、本発明によれば、保護者や管理者などが、家族もしくは被管理者の認証履歴を恒常的にチェックでき、認証スコアの低下や認証頻度の異常などの、システムや利用者の異常を早期に発見できるようになる個人認証装置および個人認証方法を提供できる。

【 0 0 5 4 】

さらに、本発明によれば、認証されたときに表示される認証結果を利用者が選択でき、利用者の満足度を高めることができる個人認証装置および個人認証方法を提供できる。

【図面の簡単な説明】

20

【図 1】本発明の第 1 の実施の形態に係る個人認証装置の構成を概略的に示すブロック図。

【図 2】第 1 の実施の形態に係る個人認証装置の全体的な処理の流れについて説明するフローチャート。

【図 3】第 1 の実施の形態における認証結果と認証履歴の表示例を示す図。

【図 4】第 1 の実施の形態における認証結果と認証履歴の別の表示例を示す図。

【図 5】第 1 の実施の形態における認証結果と認証履歴のさらに別の表示例を示す図。

【図 6】第 1 の実施の形態において認証部として顔画像による認証技術を用いた場合の個人認証装置の構成を概略的に示すブロック図。

【図 7】本発明の第 2 の実施の形態に係る個人認証装置の構成を概略的に示すブロック図。

30

【図 8】第 2 の実施の形態に係る個人認証装置の全体的な処理の流れについて説明するフローチャート。

【図 9】第 2 の実施の形態において個人認証情報記録媒体を用いることの効果を説明するための図。

【図 1 0】第 2 の実施の形態において認証部として顔画像による認証技術を用いた場合の個人認証装置の構成を概略的に示すブロック図。

【図 1 1】本発明の第 3 の実施の形態に係る個人認証装置の構成を概略的に示すブロック図。

【図 1 2】第 3 の実施の形態において用いる管理情報の一例を示す図。

40

【図 1 3】第 3 の実施の形態における認証結果と認証履歴の表示例を示す図。

【図 1 4】本発明の第 4 の実施の形態における顔画像選択画面の一例を示す図。

【図 1 5】本発明の第 5 の実施の形態に係る個人認証装置の構成を概略的に示すブロック図。

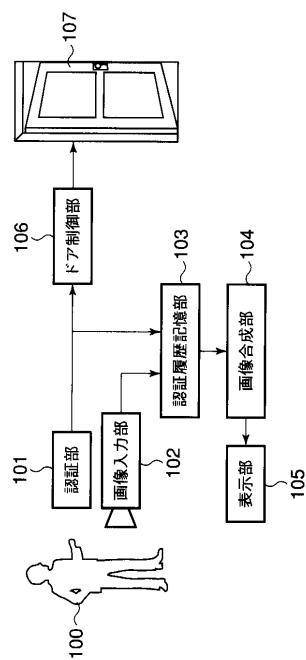
【符号の説明】

1 0 0 ... 被認証者 (利用者)、1 0 1 ... 認証部 (認証手段)、1 0 2 , 1 0 1 a ... 画像入力部 (画像入力手段)、1 0 1 b ... 処理部、1 0 3 ... 認証履歴記憶部 (認証履歴記憶手段)、1 0 4 ... 画像合成部 (表示手段)、1 0 5 ... 表示部 (表示手段)、1 0 6 ... ドア制御部、1 0 7 ... ドア、1 0 8 ... 個人認証情報記録媒体 (携帯形情報記録媒体)、1 0 9 ... 認証履歴処理手段、1 1 0 ... 個人認証情報読取部、1 1 1 ... 個人認証情報記録部、1 1 2 ...

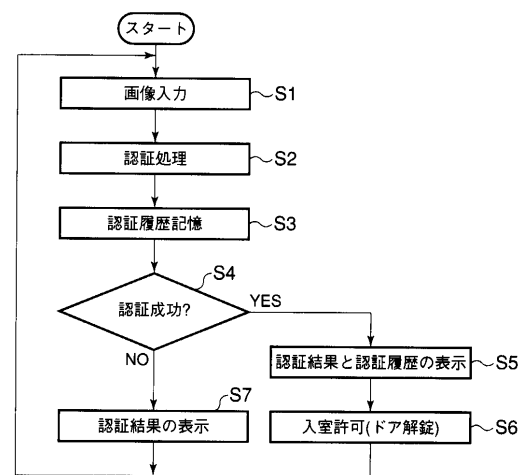
50

個人設定記憶部、113...登録画像入力部（画像入力手段）。

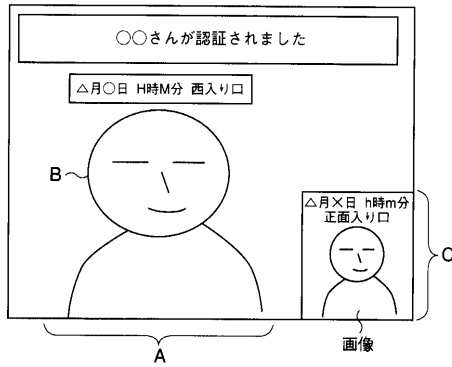
【図1】



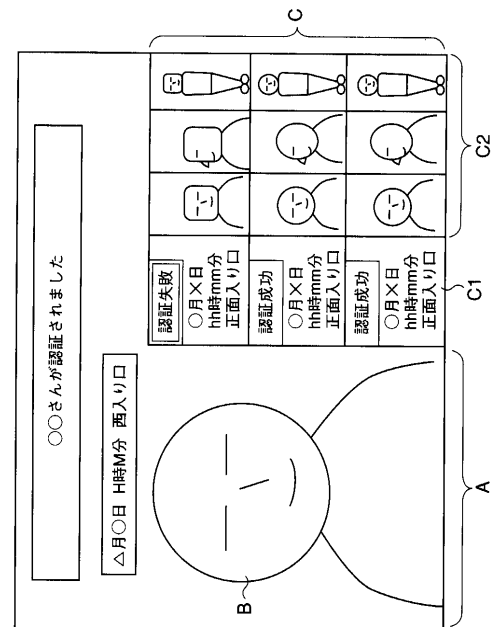
【図2】



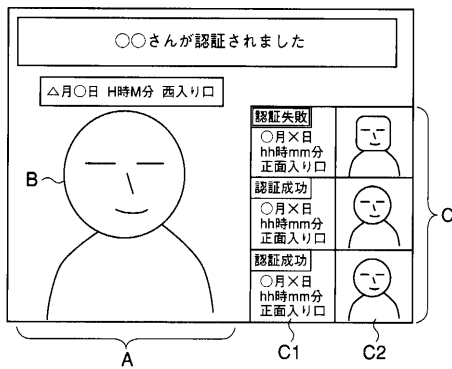
【図 3】



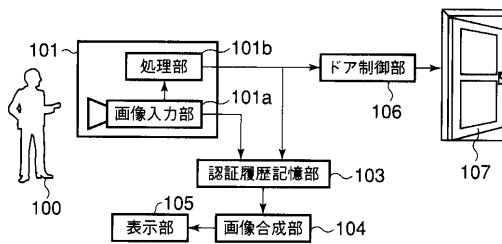
【図 5】



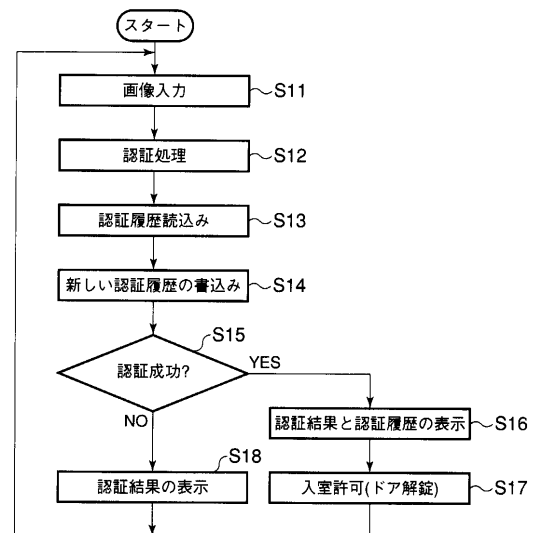
【図 4】



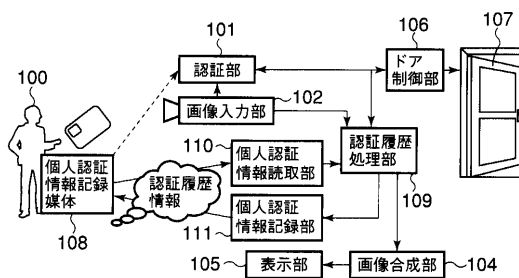
【図 6】



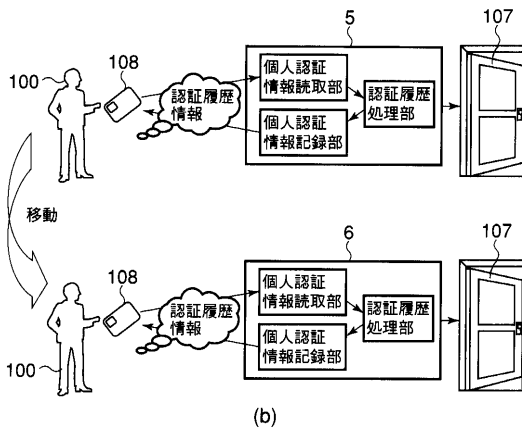
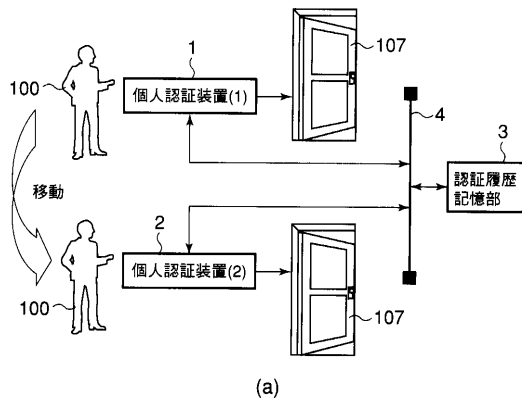
【図 8】



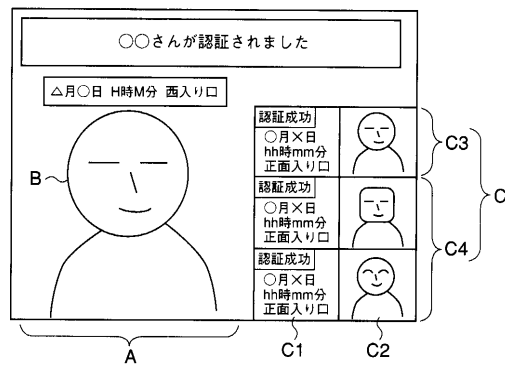
【図 7】



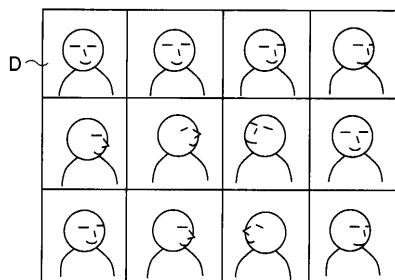
【図 9】



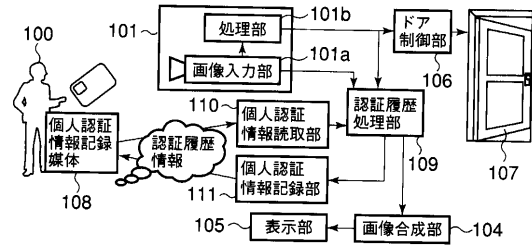
【図 13】



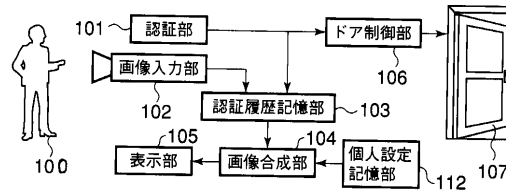
【図 14】



【図 10】



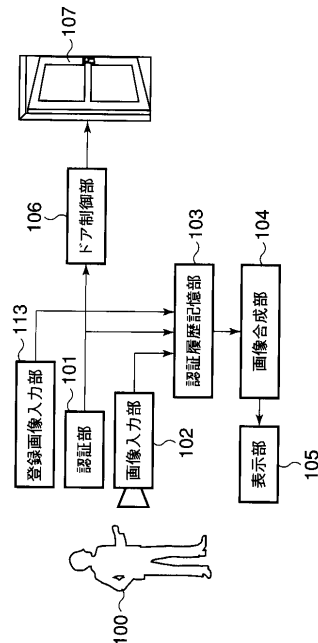
【図 11】



【図 12】

利用者ID	管理対象ID
1	2,3,4,8,10
2	
3	6,7
4	7
...	...

【図 15】



フロントページの続き

(72)発明者 横井 謙太郎

神奈川県川崎市幸区柳町 7 0 番地 株式会社東芝柳町事業所内

審査官 新井 則和

(56)参考文献 特開 2 0 0 2 - 1 4 0 3 0 6 (J P , A)

特開平 0 9 - 3 1 9 8 7 7 (J P , A)

特開昭 6 2 - 2 0 6 6 5 3 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)

G06T 7/00