

明 細 書

発明の名称：

認証装置、認証システム、認証方法および認証プログラム

技術分野

[0001] 本発明は、対象者の認証を行う認証装置、認証システム、認証方法および認証プログラムに関する。

背景技術

[0002] 対象者の認証を行う方法が、各種知られている。古典的な通行手形や割符などの物理的な鍵も認証方法の一つである。また、特許文献１には、ＩＤカードなどのデバイスに格納された電子的な鍵を認証する鍵認証が記載されている。

[0003] しかし、鍵認証は対象者が何らかの形で鍵を携行する必要があるため、不便であることに加え、盗難や紛失による不正アクセスの危険性が高い。それに対し、古典的な合言葉と同様に、対象者と認証者とが暗証番号やパスワード、秘密の質問に対する回答などのキーワードを事前に取り決め、対象者にキーボードやタッチパネルからキーワードを入力させることで認証する方法がある。このような認証方法のことを、以下、キーワード認証と記す。

[0004] キーワード認証は、認証鍵を対象者の記憶に格納するため、携行物が不要という利点から普及している。しかし、キーワードをキーボードやタッチパネルから入力させる場合、対象者が両手に荷物を持っている状況などでは、入力が困難であるという課題がある。また、キーワード認証は、キーボードやタッチパネルからの入力を第三者に盗み見され、キーワードが漏洩して不正アクセスされる危険性が高いという問題もある。

[0005] このような課題に対し、対象者にキーワードを口頭で発話させ、音声認識を介してキーワードの入力を得る方法も考えられる。しかし、キーワードを対象者に発話させると、周囲の第三者にも容易に聴取され易いため、不正アクセスされる危険性がより高まるという問題がある。

- [0006] また、両手が使えない状況で、キーボードやタッチパネルからのキーワード入力を代替する技術として、眼の動きを用いる方法も知られている。特許文献2には、眼球運動を用いた視線入力コミュニケーション方法が記載されている。具体的には、特許文献2には、カメラで眼の開閉を観測し、例えば「右、左、左、右」といった片目の開閉順を暗証番号の代替として認証する認証方法や、視線の方向と瞬きによりキーボードやタッチパネルからの入力を代替させる方法が記載されている。
- [0007] また、特許文献3には、視線入力を用いてユーザ認証処理を行う方法が記載されている。視線入力の場合、視線自体は眼球の動きから周囲の第三者にも推測される可能性があるが、顔の正面に近い角度から眼球を見ないと正確な視線の方向はわからない。そのため、眼球の動きと視線が向いている画像の双方を同時に盗み見ることは困難であるため、この方法は、不正アクセスされる危険性の課題を解決する有効な方式と言える。
- [0008] また、それ以外にも、予め対象者の指紋や顔、虹彩などの生体情報を記録し、これを鍵として認証する生体認証も各種知られている（例えば、特許文献4～6参照）。
- [0009] さらに、認証のセキュリティ強度を向上させるため、複数の要素を用いて認証を行う方法も提案されている。特許文献7には、複数の要素を用いて認証を行う多要素認証方法が記載されている。また、特許文献8には、視線入力を用いたパスワード認証と生体情報による認証とを併用する方法が記載されている。
- [0010] また、第三者が成りすますことが難しい顔認証でも、本人の顔写真や本人の顔を複製した立体人形などを用いて認証を得る成りすましの危険性がある。このような成りすましを防止する方法が特許文献9に記載されている。特許文献9に記載された方法では、対象者の顔画像を複数回取得して顔の変化を確認したり、その過程で、瞬きや口を開けるなどの動作を要求して、人形ではない事を確認したりする。

先行技術文献

特許文献

- [0011] 特許文献1：特開昭63－313288号公報
特許文献2：特開2005－100366号公報
特許文献3：特開2014－92941号公報
特許文献4：特開昭58－176781号公報
特許文献5：特開昭59－194274号公報
特許文献6：特開2001－34754号公報
特許文献7：特開2009－71430号公報
特許文献8：特開2006－277396号公報
特許文献9：特開平11－339048号公報

発明の概要

発明が解決しようとする課題

- [0012] 一方、特許文献2に記載されたような眼の開閉順を暗証番号の代替とする場合、音声と同様に周囲の第三者にも容易に盗み見され易いため、不正アクセスされる危険性が高いという課題がある。
- [0013] この課題に対し、特許文献3に記載された方法では、視線入力を用いてユーザ認証処理が行われるため、不正アクセスされる危険性を低減させることは可能である。しかし、特許文献3に記載された方法では、ユーザ認証用画像が他人に知られてしまった場合、不正アクセスされる可能性が残っている。
- [0014] 一方、上述する生体認証は、いずれもIDカードなどの携行物が不要で、第三者が鍵を盗んで成りすますことが極めて困難という利点を有する。一方、生体認証の方法によっては、特別な入力装置が必要になる場合も存在する。例えば、指紋認証や虹彩認証の場合、特別な入力装置が必定とされ、対象者が指や目を所定の位置に置くなどの動作を要求される。そのため、認証側にとっても対象者にとっても認証時の利便性に課題がある。
- [0015] 一方、生体認証の中でも顔認証は、特別な入力装置を必定とせず、通常のカメラでやや離れた位置から撮影した画像でも認証が可能のため、生体認証

の利点を有しつつ、指紋認証や虹彩認証の様な課題も生じない、極めて利便性が高い認証方式と言える。しかし、このような顔認証でも、照合する対象者の人数が増えると精度上の限界に到達してしまう可能性があり、また、成りすましの問題も残る。

[0016] 特許文献8に記載された方法では、視線入力を用いたパスワード認証だけでなく、声紋情報や顔画像、掌の紋を用いて認証が行われる。しかし、声紋情報や掌の紋を用いた認証方法では、利便性を損ねてしまい、また、顔画像による認証では、上述するような成りすましの問題も依然として残る。

[0017] また、特許文献9には、認証装置が顔画像を複数回取得して成りすまさない事を確認するまで、対象者は認証装置の前で待機を要求されたり、指示に従って瞬きや口を開けるなどの動作を要求されたりすることも記載されている。しかし、このような対応は対象者にとって不便で、快適性を損ねてしまい、結果として利便性を低下させてしまう。

[0018] そこで、本発明は、認証側および対象者の認証時の利便性を向上させつつ、対象者の成りすましを検知して、対象者を高精度で認証することができる認証装置、認証システム、認証方法および認証プログラムを提供することを目的とする。

課題を解決するための手段

[0019] 本発明による認証装置は、対象者の認証を行う認証装置であって、対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力手段と、対象者の顔画像を撮像する撮像装置により撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定する回答特定手段と、特定された回答の正誤判定を行う回答判定手段と、撮像装置により撮像された顔画像から対象者の顔認証を行う顔認証手段と、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う生体判定手段と、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う対象者認証手段とを備えたことを特徴とする。

[0020] 本発明による認証システムは、対象者の認証を行う認証システムであって

、対象者の顔画像を撮像する撮像装置と、対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力手段と、撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定する回答特定手段と、特定された回答の正誤判定を行う回答判定手段と、撮像された顔画像から対象者の顔認証を行う顔認証手段と、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う生体判定手段と、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う対象者認証手段とを備えたことを特徴とする。

[0021] 本発明による認証方法は、対象者の認証を行う認証方法であって、記対象者へ行う質問に対して複数の回答候補を表示装置に出力し、対象者の顔画像を撮像する撮像装置により撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定し、特定された回答の正誤判定を行い、撮像装置により撮像された顔画像から対象者の顔認証を行い、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行い、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行うことを特徴とする。

[0022] 本発明による認証プログラムは、対象者の認証を行うコンピュータに適用される認証プログラムであって、コンピュータに、対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力処理、対象者の顔画像を撮像する撮像装置により撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定する回答特定処理、特定された回答の正誤判定を行う回答判定処理、撮像装置により撮像された顔画像から対象者の顔認証を行う顔認証処理、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う生体判定処理、および、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う対象者認証処理を実行させることを特徴とする。

発明の効果

[0023] 本発明によれば、認証側および対象者の認証時の利便性を向上させつつ、

対象者の成りすましを検知して、対象者を高精度で認証することができる。

図面の簡単な説明

[0024] [図1]本発明による認証システムの第一の実施形態の構成例を示すブロック図である。

[図2]第一の実施形態の認証システムの動作例を示すフローチャートである。

[図3]本発明による認証システムの第二の実施形態の構成例を示すブロック図である。

[図4]第二の実施形態の認証システムの動作例を示すフローチャートである。

[図5]本発明による認証システムの第三の実施形態の構成例を示すブロック図である。

[図6]第三の実施形態の認証システムの動作例を示すフローチャートである。

[図7]視線入力キーワード認証を行う場合の動作例を示す説明図である。

[図8]認証システムを用いた動作例を示すシーケンス図である。

[図9]本発明による認証装置の概要を示すブロック図である。

[図10]本発明による認証システムの概要を示すブロック図である。

発明を実施するための形態

[0025] 本実施形態では、対象者を高精度で認証し、成りすましの危険性を減少させるため、複数の認証方法を併用する。認証方法の併用は、認証精度を高めるだけでなく、成りすましの危険性を減少させる効果もある。例えば、顔認証に加えて、暗証番号による認証を行う方法を想定する。この方法の場合、対象者の顔写真を入手して顔認証に対して成りすましを図ることはできても、暗証番号も入手しないと認証されないため。成りすましの危険性を大幅に減少させる効果がある。

[0026] しかし、認証方法を単に併用させた場合、利点や利便性を損なう可能性もある。例えば、顔認証で精度が不足すると判定された場合、上述するような鍵認証を第2の認証要素とする方法が考えられる。しかし、鍵認証を加えることにより、携行物が不要という顔認証の大きな利点が損なわれてしまう。

[0027] また、他の方法として、上述するようなキーワード認証を、第2の認証要

素とする方法が考えられる。しかし、キーワード認証は手による入力が必要
なため、例えば、両手に荷物を持っている状況でも認証できるという顔認証
の利点が損なわれてしまう。

[0028] さらに、指紋認証や虹彩認証を、第2の認証要素とする方法も考えられる
。しかし、上述する通り、指紋認証や虹彩認証には特別な入力装置が必要に
なるため、認証側にとっての利便性を損なってしまう。

[0029] そこで、本実施形態では、認証されるユーザ（以下、対象者と記す。）の
顔認証に併せて、対象者による回答の正誤判定、および、対象者の生体判定
の結果に基づいて、対象者の認証を行う。なお、本実施形態における認証と
は、対象者を特定することや、対象者が有する権限の有無の判断など、個人
の適否を認証する広い概念を含むものである。

[0030] 初めに、本発明の特徴について簡単に説明する。本発明の第一の特徴とし
て、対象者へ何らかの質問を行い、それに対する複数の回答候補を表示デバ
イス上のランダムな位置に提示することが挙げられる。そして、対象者に回
答を見つめさせ、対象者の視線の方向から選択した回答を認識することで、
選択した回答が正答であることを認証する。なお、以下の説明では、この方式
を、視線入力キーワード認証と記す。

[0031] 視線入力キーワード認証は、キーワード認証におけるキーワードの入力を
、キーボードやタッチパネルを用いた手による入力から、視線による入力に
置き換えたものと言える。これにより、個人を高精度で認証でき、対象者が
鍵認証の様にIDカードなどの携行物を必要としない、というキーワード認
証の特徴を継承しつつ、対象者の両手が塞がっていても情報を入力できる
という効果を有する。

[0032] さらに、キーワード認証におけるキーワード入力を音声認識により行う方
式と、視線入力キーワード認証を行う方式とを比較する。視線入力キーワ
ード認証では、対象者の前方にいる第三者には対象者の視線の方向は識別でき
ても表示デバイス上の回答候補は見えない。また、対象者の後方にいる第三
者には表示デバイス上の回答候補は見えても対象者の視線の方向は見えない

。このように、視線入力キーワード認証は、視線により選択した回答を周囲の第三者に盗み見られる危険性が極めて少ないという効果を有する。

[0033] また、この特徴は、個人認証を受ける対象者に高いセキュリティ性を提供するだけではない。具体的には、個人認証を行う認証側が、第三者からの盗み見や盗聴を遮るための壁や遮蔽物を設ける必要が無く、周囲に第三者が多数いる開放空間でも利用できる、という、一般的なキーワード認証や音声認識によるキーワード認証では得られない利便性を有する。

[0034] さらに、この認証方法を実行するために必要な構成部品として、主に回答候補を提示する表示デバイス、対象者を撮影するカメラ、視線の方向を解析するCPU（Central Processing Unit）等があれば良い。そのため、市販のタブレットやラップトップPCに認証プログラムをインストールするだけでも実現することが可能である。この点において、認証側に高い利便性を提供できる。

[0035] さらに、本発明の第二の特徴として、上述する視線入力キーワード認証と、対象者の顔認証とを併用することが挙げられる。視線入力キーワード認証も、携行物が不要であるとともに、ハンズフリー型であり、指紋認証や虹彩認証のような利便性の課題がない。そのため、視線入力キーワード認証を顔認証と併用する際に、顔認証の利点を損ねることがほとんどないと言える。そのため、視線入力キーワード認証は、顔認証を補強する多要素認証として、他の認証方式との組み合わせでは得られない効果を有する。

[0036] 加えて、視線入力キーワード認証と顔認証のどちらも顔を撮像する1台のカメラを共用できる。そのため、顔認証を多要素認証に補強する際の費用や工事が少ないうえに、顔認証と視線の方向の計測を同時に行うことができる。したがって、対象者および認証側いずれの負担も軽減できるという、単なる組み合わせではない、実用的な効果が得られる。

[0037] さらに、本発明の第三の特徴として、上述する特徴に加え、顔認証と対象者が回答を選択する視線の計測とを並行して複数回行って、顔を認証した人物の視線が移動していることを検証することが挙げられる。これにより、対

象者が人物の生体であることを検証できる。

[0038] なお、顔認証も視線入力キーワード認証も、第三者による成りすましは困難な認証方式である。しかし、例えば、本人の顔を撮影した顔写真や、顔を複製した立体人形を用いて顔認証を行った後に、第三者が入れ替わって視線入力キーワード認証を受けるといふ、時間差を持った成りすましが行われる危険性は残る。

[0039] これに対し、本実施形態では、顔認証と対象者が回答を選択する視線の計測を並行して複数回行って、顔を認証した人物の視線が移動していることを検証する。これにより、本人の顔を撮影した顔写真や、顔を複製した立体人形による成りすましを排除できるという効果が得られる。

[0040] 付言すると、第一の特徴で挙げた顔認証にて複数回の認証を行うだけでは、顔を認証した人物が生体であるとの検証はできない。また、第二の特徴である視線入力キーワード認証にて視線の移動から生体であることを検証するだけでは、キーワードの漏洩による不正アクセスの危険性が残る。一方、上述する三つの特徴を併用することで、これらの課題を網羅できるため、単なる組み合わせでは得られない、特別な効果が得られる。

[0041] 他にも、本発明の特徴として、表示デバイス上に回答候補を提示し、対象者が視線を動かして選択した時刻と、同一時刻に取得した顔画像による顔認証の結果とを取得し、それにより、顔認証で照合した人物の生体であることを検証すること、が挙げられる。

[0042] 対象者が視線を動かして回答を選択している時刻と、同一時刻における顔認証の結果を取得し、顔認証で照合した人物の生体であることを検証することで、上述するような時間差による成りすましを防ぐことができる効果を有する。

[0043] また、本発明の更なる特徴として、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を確認することが挙げられる。これにより、顔認証で照合した人物の生体であることを検証することが可能になる。

[0044] 例えば、本人の顔を複製した立体人形を用いて顔認証の成りすましを行いつつ、第三者が立体人形の顔全体の角度を変更することで立体人形の視線の方向を制御し、視線入力キーワード認証の成りすましを行う、という高度な成りすましも考えられる。

[0045] しかし、本実施形態では、このような高度な成りすましに対しても、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を確認する。そのような構成により、写真や立体人形の顔全体が動いているのではなく、生体が視線を動かしていることを検証できるため、上述するような高度な成りすましを抑制できるという効果が得られる。

[0046] さらに、上記のような追加の特徴を実現する場合でも、必要な構成部品は変わらない。すなわち、市販のタブレットやラップトップPCに認証プログラムをインストールするだけで、上述する機能を実現することが可能である。なお、これらの特徴を、複数の装置や回路、プログラムを用いて実現してもよい。サービス全体として、上述する特徴を実現するための構成要素を満たしていれば、上記と同一の効果を保ったままで、認識側や対象者に高い信頼性と利便性を提供できる。

[0047] 以下、本発明の実施形態を図面を参照して説明する。

[0048] 実施形態1.

図1は、本発明による認証システムの第一の実施形態の構成例を示すブロック図である。本実施形態の認証システム100は、認証装置10と、撮像装置20と、表示装置30とを備えている。なお、撮像装置20は、表示装置30の近傍であって、対象者が表示装置30に対する視認動作を撮像可能な位置に設置される。

[0049] 撮像装置20は、対象者の顔画像を撮像する装置である。撮像装置20は、例えば、映像として時系列に撮像した各フレームの画像を、対象者の顔画像として取得してもよい。また、撮像装置20は、撮像範囲内に人を検知したタイミングで、対象者の顔画像を撮像してもよいし、対象者が認証装置10に対して何らかのアクションを行ったタイミングで、対象者の顔画像を撮

像してもよい。図1に示す例では、認証システム100が、撮像装置20を2台備える場合を例示しているが、撮像装置20は、1台であってもよい。

[0050] 表示装置30は、後述する出力部13の指示に応じて各種情報を出力する。表示装置30は、例えば、ディスプレイ装置や、タブレットなどにより実現される。

[0051] 認証装置10は、記憶部11と、入力部12と、出力部13と、回答特定部14と、回答判定部15と、顔認証部16と、生体判定部17と、対象者認証部18とを含む。

[0052] 記憶部11は、認証装置10が処理に用いる各種情報を記憶する。記憶部11は、例えば、後述する顔認証部16が認証に用いる顔画像や特徴量を記憶していてもよい。また、記憶部11は、対象者に対して行う質問や、その質問に対する回答候補を記憶していてもよい。ここで、回答候補とは、質問に対する正しい回答と、質問に対する誤った回答とを含む情報である。また、質問は、特定された対象者ごとに準備されていてもよい。記憶部11は、例えば、磁気ディスク等により実現される。

[0053] 入力部12は、撮像装置20が撮像した対象者の顔画像の入力を受け付ける。例えば、撮像装置20が複数の場合、入力部12は、顔画像を撮像した撮像装置20を識別する情報と共に、顔画像の入力を受け付けてもよい。

[0054] 出力部13は、対象者へ行う質問に対して複数の回答候補を表示装置30に出力する。具体的には、出力部13は、対象者が現れると、対象者に対する質問と、それに対する複数の回答候補を、表示装置30上のランダムな位置に出力し、対象者に回答を視認する要求を行う。複数の回答候補をランダムな位置に出力することにより、回答を確認する対象者の視線を様々な方向に移動させることが可能になり、後述する生体判定部17が判定を行いやすくなる。

[0055] なお、質問の内容および回答候補の内容は任意であり、予め定められていてもよい。出力部13は、例えば、「ID番号は?」、「暗証番号は?」などの質問を画面などに出力し、それに対する複数の回答候補として、0から

9までの数字を記載したアイコンなどを、表示デバイス上のランダムな位置に出力してもよい。ただし、質問や回答候補は、この例に限定されない。

[0056] なお、質問の内容は表示装置30に出力されなくてもよく、例えば、音声などでスピーカ（図示せず）などから出力されてもよい。

[0057] また、後述する顔認証部16が対象者を認証している場合、出力部13は、対象者固有の質問と、その質問に対応する複数の回答候補を表示装置30に出力してもよい。具体的には、出力部13は、対象者が作成した秘密の質問と、その質問に対する回答候補を出力してもよい。出力部13は、例えば、顔画像と特徴が合致した人物に対して、その人物が事前に作成した「卒業した小学校の名は？」や「母親の旧姓は？」などの秘密の質問と、その質問に対する回答（および誤答）となる回答候補を出力してもよい。このような質問および回答候補を利用することで、認証のセキュリティを高めることが可能になる。

[0058] 回答特定部14は、撮像された顔画像における対象者の視線に基づいて、複数の回答候補の中から質問に対する回答を特定する。すなわち、回答特定部14は、顔画像から視線方向を計測し、対象者の視線の方向から選択した回答を特定する。

[0059] なお、対象者の視線に基づいて対象者が注視する位置を特定する方法は任意である。回答特定部14は、例えば、特許文献2に記載された方法を用いて、対象者が表示装置30で注視する位置を特定してもよい。具体的には、回答特定部14は、対象者の眼球の位置から対象者の視線の方向を計測し、対象者の眼の位置を起点とした視線の方向ベクトルが表示装置30と交わる位置に出力された回答候補を、対象者が選択した回答として特定してもよい。

[0060] なお、実際には人の視線は揺らぐため、回答特定部14は、視線が一定時間留まった位置の回答候補を対象者が選択した回答とみなしてもよい。また、回答特定部14は、対象者が瞬きした直前の視線が示す位置の回答候補を、対象者が選択した回答とみなしてもよい。このような揺らぎを許容するこ

とで、対象者が選択した回答を特定する精度を向上させることができる。

[0061] 回答判定部 15 は、特定された回答の正誤判定を行う。具体的には、回答判定部 15 は、対象者が選択した回答を、事前に登録された正答と照合し、回答の正誤を判定する。回答判定部 15 は、この判定結果により、回答が正しければ認証できたと判定し、回答が誤っていれば認証できなかったと判定する。

[0062] 顔認証部 16 は、撮像された顔画像から対象者の顔認証を行う。顔認証部 16 が対象者の顔認証を行う方法は任意である。顔認証部 16 は、例えば、顔画像から顔の特徴を抽出し、事前に記憶部 11 に記憶された人物の顔の特徴と合致するか否かを判定して、対象者の顔認証を行ってもよい。

[0063] 生体判定部 17 は、撮像された複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う。より詳しくは、生体判定部 17 は、時系列に撮像された複数の顔画像から検知される対象者の視線の方向の変化に基づいて、対象者の生体判定を行う。

[0064] 具体的には、生体判定部 17 は、例えば、撮像装置 20 により撮像された顔画像を時系列に順次受け取り、受け取った顔画像の対象者の視線の方向が変化しているときに、対象者が生体であると判定してもよい。生体判定部 17 は、例えば、視線入力キーワード認証時（すなわち、回答特定部 14 および回答判定部 15 の処理時）に、顔認証部 16 による認証処理を継続させて、その処理結果を受け付けて生体判定を行ってもよい。すなわち、視線入力キーワード認証にて、対象者が出力された回答候補へ視線方向を移動している間にも顔認証を繰り返して行なうことにより、結果として生体判定部 17 は、顔認証で認証した顔画像が、視線を移動させた人物の生体であることを、自動的に検証できる。

[0065] すなわち、視線入力キーワード認証と顔認証とを並行して行うことで、必然的に対象者の視線が移動することから、生体判定部 17 は、この視線の移動を生体判定の要素として利用できることになる。

[0066] 対象者認証部 18 は、回答判定部 15 による正誤判定、生体判定部 17 に

よる生体判定、および、顔認証部 16 による顔認証の結果に基づいて、対象者の認証を行う。具体的には、回答判定部 15 により回答が正しいと判定され、生体判定部 17 により対象者が生体と判定され、顔認証部 16 により対象者が認証された場合に、対象者認証部 18 は、顔認証部 16 が認証した対象者を、適切な対象者と認証し、一つでも上記判定または認証がなされていない場合、否認する。

[0067] なお、本実施形態では、認証システム 100 が、撮像装置 20 を 2 台備える場合を例示している。そこで、回答特定部 14 が、第一の撮像装置で撮像された画像（第一顔画像）を用いて回答を特定し、顔認証部 16 が、第二の撮像装置で撮像された画像（第二顔画像）を用いて顔認証を行ってもよい。このように、処理ごとに顔画像を撮像する撮像装置 20 を設けることで、各処理に適した画像を利用することが可能になる。

[0068] 入力部 12 と、出力部 13 と、回答特定部 14 と、回答判定部 15 と、顔認証部 16 と、生体判定部 17 と、対象者認証部 18 とは、プログラム（認証プログラム）に従って動作するコンピュータのプロセッサ（例えば、CPU、GPU（Graphics Processing Unit））によって実現される。

[0069] 例えば、プログラムは、記憶部 11 に記憶され、プロセッサは、そのプログラムを読み込み、プログラムに従って、入力部 12、出力部 13、回答特定部 14、回答判定部 15、顔認証部 16、生体判定部 17 および対象者認証部 18 として動作してもよい。また、入力部 12、出力部 13、回答特定部 14、回答判定部 15、顔認証部 16、生体判定部 17 および対象者認証部 18 の機能が SaaS（Software as a Service）形式で提供されてもよい。

[0070] また、入力部 12 と、出力部 13 と、回答特定部 14 と、回答判定部 15 と、顔認証部 16 と、生体判定部 17 と、対象者認証部 18 とは、それぞれが専用のハードウェアで実現されていてもよい。また、各装置の各構成要素の一部又は全部は、汎用または専用の回路（circuitry）、プロセッサ等やこれらの組合せによって実現されてもよい。これらは、単一のチップによっ

て構成されてもよいし、バスを介して接続される複数のチップによって構成されてもよい。各装置の各構成要素の一部又は全部は、上述した回路等とプログラムとの組合せによって実現されてもよい。

[0071] また、入力部 1 2、出力部 1 3、回答特定部 1 4、回答判定部 1 5、顔認証部 1 6、生体判定部 1 7 および対象者認証部 1 8 の各構成要素の一部又は全部が複数の情報処理装置や回路等により実現される場合には、複数の情報処理装置や回路等は、集中配置されてもよいし、分散配置されてもよい。例えば、情報処理装置や回路等は、クライアントサーバシステム、クラウドコンピューティングシステム等、各々が通信ネットワークを介して接続される形態として実現されてもよい。

[0072] 次に、本実施形態の認証システム 1 0 0 の動作を説明する。図 2 は、本実施形態の認証システム 1 0 0 の動作例を示すフローチャートである。

[0073] 出力部 1 3 は、対象者へ行う質問に対して複数の回答候補を表示装置に出力する（ステップ S 1）。そして、撮像装置 2 0 が対象者の顔画像を撮像すると、入力部 1 2 は、視線入力キーワード認証を行うため、撮像された顔画像を取得する（ステップ S 2）。回答特定部 1 4 は、撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定する。すなわち、回答特定部 1 4 は、視線方向を計測し（ステップ S 3）、視線方向から選択した回答を認識する（ステップ S 4）。なお、回答が認識されるまで、ステップ S 2 およびステップ S 3 の処理を繰り返す。

[0074] 回答判定部 1 5 は、特定された回答の正誤判定を行う。すなわち、回答判定部 1 5 は、回答の正否を判定する（ステップ S 5）。回答が正しくない場合（ステップ S 5 における N o）、認証装置 1 0 は、認証を否認する。

[0075] 一方、ステップ S 1 からステップ S 5 の処理と並行し、撮像装置 2 0 が対象者の顔画像を撮像すると、入力部 1 2 は、顔認証を行うため、撮像された顔画像を取得する（ステップ S 6）。なお、撮像装置 2 0 は、視線入力キーワード認証用と顔認証用とで異なってもよい。顔認証部 1 6 は、撮像された顔画像から対象者の顔認証を行う。具体的には、顔認証部 1 6 は、顔画

像から特徴を抽出する（ステップS 7）。そして、顔認証部 1 6 は、抽出された特徴が登録された特徴と一致するか否かを判定する（ステップS 8）。抽出された特徴が登録された特徴と一致しなかった場合（ステップS 8 におけるN o）、認証装置 1 0 は、認証を否認する。なお、特徴と一致していると判断されている間、ステップS 6 からステップS 8 の処理を繰り返す。

[0076] 対象者認証部 1 8 は、すべての処理が正しく行われた場合（ステップS 9 におけるY e s）、対象者を認証したと判断する。すなわち、対象者認証部 1 8 は、回答が正しかった場合であって（ステップS 5 におけるY e s）、抽出された特徴が登録された特徴と一致した場合（ステップS 8 におけるY e s）、対象者を認証したと判断する。一方、一部でも処理が正しく行われなかった場合（ステップS 9 におけるN o）、対象者認証部 1 8 は、認証を否認する。

[0077] 以上のように、本実施形態では、出力部 1 3 が、対象者へ行う質問に対して複数の回答候補を表示装置に出力し、回答特定部 1 4 が、撮像装置 2 0 によって撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定すると、回答判定部 1 5 が、特定された回答の正誤判定を行う。一方、顔認証部 1 6 が、撮像装置 2 0 によって撮像された顔画像から対象者の顔認証を行い、生体判定部 1 7 が、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う。そして、対象者認証部 1 8 が、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う。よって、認証側および対象者の認証時の利便性を向上させつつ、対象者の成りすましを検知して、対象者を高精度で認証することができる。

[0078] 具体的には、本実施形態の認証装置 1 0 により、個人を高精度で認証しつつ、不正アクセスや成りすましの危険性が低く、かつ対象者にも認証者にも利便性が高い、認証技術および成りすまし防止技術を提供できる。その第一の理由は、顔認証と視線入力キーワード認証を併用することで、個人を高精度で認証できるためである。

[0079] 第二の理由は、顔画像という対象者の生体情報と、キーワードという対象者の記憶の中にある情報を認証の鍵とすることで、不正アクセスの危険性を極めて少なくしているためである。さらに、その顔画像の一部から特定できる視線が、記憶の中にあるキーワードを選択するために移動する動作として利用でき、その動作に基づいて生体であることを検証するため、不正アクセスや成りすましを極めて困難にすることができる。

[0080] 第三の理由は、上述する2つの認証と成りすまし防止を行う上で、対象者は表示デバイス上に提示された質問への回答を見つめるという、短時間の少ない負荷だけで良いためである。また、対象者は携行物が不要でハンズフリーであり、周囲の第三者からの盗み見や盗聴を心配する必要が無い場合、利便性が極めて高い。

[0081] 第四の理由は、上述する2つの認証と成りすまし防止を行う上で、認証者は表示デバイスと顔画像を撮影するカメラを設置するだけで良いためである。これにより、短時間に高精度の多要素認証および成りすまし防止を行うことができ、周囲の第三者からの盗み見や盗聴を防ぐための壁や遮蔽物の設置が不要であるため、利便性が極めて高い。例えば、市販されているスマートフォンやタブレット、ラップトップPCは、表示デバイスおよび顔画像を撮影するカメラを具備していることが多い。そのため、認証者は、これらの装置にプログラムをインストールすることで、本実施形態の認証装置10を実現できる。

[0082] 実施形態2.

次に、本発明による認証システムの第二の実施形態を説明する。本実施形態では、時間差を利用した成りすましを防止する方法を説明する。まず初めに、本実施形態の概要を説明する。本実施形態では、視線入力キーワード認証を行うための顔画像を取得すると同時に、顔認証を行うための顔画像を取得する。対象者が視線を動かして回答を選択した時刻と、同一時刻の顔画像により顔認証を行うことで、時間差を利用した成りすましを防止する。

[0083] 図3は、本発明による認証システムの第二の実施形態の構成例を示すプロ

ック図である。本実施形態の本実施形態の認証システム２００は、認証装置１１０と、撮像装置２０と、表示装置３０とを備えている。なお、撮像装置２０および表示装置３０の構成については、第一の実施形態と同様である。

[0084] 認証装置１１０は、記憶部１１と、入力部１２と、出力部１３と、回答特定部２４と、回答判定部１５と、顔認証部２６と、生体判定部１７と、対象者認証部２８とを含む。すなわち、本実施形態の認証装置は、回答特定部２４、顔認証部２６および対象者認証部２８が行う処理が、それぞれ、第一の実施形態の回答特定部１４、顔認証部１６および対象者認証部１８と一部異なる。それ以外は、第一の実施形態と同様である。

[0085] 回答特定部２４は、第一の実施形態の回答特定部１４が行う処理に加え、対象者が回答を特定した回答時刻を取得する。顔認証部２６は、第一の実施形態の顔認証部１６が行う処理に加え、回答時刻と同時刻に行われた顔認証の結果を取得する。そして、対象者認証部２８は、対象者が、顔認証で照合した人物の生体であると認証する。

[0086] なお、撮像装置２０が一台の場合、視線入力キーワード認証を行うための顔画像と、顔認証を行うための顔画像とで、同一フレームの画像が用いられればよい。

[0087] 入力部１２と、出力部１３と、回答特定部２４と、回答判定部１５と、顔認証部２６と、生体判定部１７と、対象者認証部２８とは、プログラム（認証プログラム）に従って動作するコンピュータのプロセッサによって実現される。

[0088] 次に、本実施形態の認証システム２００の動作を説明する。図４は、本実施形態の認証システム１００の動作例を示すフローチャートである。図４に例示するフローチャートは、図２に例示するフローチャートと比較し、ステップＳ２とステップＳ６で顔画像を取得する時刻が同一である点において異なる。それ以外については、図２に例示するフローチャート同様である。なお、図２に例示するフローチャートにおいて、ステップＳ２とステップＳ６で顔画像を取得する時刻が同一であることを排除するものではない。

[0089] 以上のように、本実施形態では、第一の実施形態の構成に加え、回答特定部 24 が、対象者が回答を特定した回答時刻を取得し、顔認証部 26 が、回答時刻と同時刻に行われた顔認証の結果を取得し、対象者認証部 28 は、対象者が、顔認証で照合した人物の生体であると認証する。よって、第一の実施形態の効果に加え、成りすましを抑制する効果を高めることができる。

[0090] 実施形態 3.

次に、本発明による認証システムの第三の実施形態を説明する。本実施形態では、成りすましを防止する、より具体的な構成を説明する。まず初めに、本実施形態の概要を説明する。本実施形態では、対象者の顔画像を取得し、その画像から対象者の視線の方向と顔の方向を計測する処理を何度か繰り返す。この結果に対し、視線の方向と顔の方向の相対角度の変化を確認し、一定以上の変化があれば正（すなわち、成りすましではない）と判定し、変化が計測誤差の範囲であれば否（すなわち、成りすまし）と判定する。

[0091] このように判定する利用は、以下の通りである。実際、人間は、表示デバイス上に提示された回答候補の中から正解を探す際に、顔全体の方向を小さく動かしながら、視線を大きく動かして素早く回答を探そうとすることが一般的である。そのため、視線の方向と顔の方向の相対角度の変化を確認することで、より高精度かつ容易に、取得した顔画像が生体の顔であることを検証できる。この特徴は、対象者が回答を探すという 1 つの動作の間に、高精度な顔認証と高精度な成りすまし防止を同時に行えることを示している。すなわち、対象者の利便性および認証者の精度要求に対し、単なる組み合わせではない、特別な効果が得られる。

[0092] 図 5 は、本発明による認証システムの第三の実施形態の構成例を示すブロック図である。本実施形態の本実施形態の認証システム 300 は、認証装置 210 と、撮像装置 20 と、表示装置 30 とを備えている。なお、撮像装置 20 および表示装置 30 の構成については、第一の実施形態および第二の実施形態と同様である。

[0093] 認証装置 210 は、記憶部 11 と、入力部 12 と、出力部 13 と、回答特

定部 14 と、回答判定部 15 と、顔認証部 16 と、生体判定部 37 と、対象者認証部 18 とを含む。すなわち、本実施形態の認証装置は、生体判定部 37 が行う処理が、第一の実施形態の生体判定部 17 と一部異なる。それ以外は、第一の実施形態と同様である。なお、第二の実施形態の各構成に対し、生体判定部 17 の代わりに生体判定部 37 が用いられてもよい。

[0094] 生体判定部 37 は、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を検知して、対象者の生体判定を行う。生体判定部 37 は、上述するように、予め定めた変化量よりも大きな変化を検知したときに、対象者が生体であると判定すればよい。

[0095] 入力部 12 と、出力部 13 と、回答特定部 14 と、回答判定部 15 と、顔認証部 16 と、生体判定部 37 と、対象者認証部 18 とは、プログラム（認証プログラム）に従って動作するコンピュータのプロセッサによって実現される。

[0096] 次に、本実施形態の認証システム 300 の動作を説明する。図 6 は、本実施形態の認証システム 300 の動作例を示すフローチャートである。なお、ステップ S1 からステップ S8 までの処理は、第一の実施形態と同様である。なお、第二の実施形態と同様に、ステップ S2 とステップ S6 で顔画像を取得する時刻が同一であってもよい。

[0097] 本実施形態では、ステップ S1 からステップ S5 の処理、および、ステップ S6 からステップ S8 までの処理と並行して、ステップ S10 からステップ S12 までの処理を行う。具体的には、生体判定部 37 は、顔画像を取得し（ステップ S10）、視線方向と顔の方向を計測する（ステップ S11）。ステップ S10 からステップ S11 の処理を繰り返し、生体判定部 37 は、相対角度変化を確認する（ステップ S12）。

[0098] 相対角度変化が所定以上でない場合（ステップ S12 における No）、認証装置 210 は、認証を否認する。一方、相対角度変化が所定以上の場合（ステップ S12 における Yes）、対象者認証部 18 は、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う（ステップ S9

）。

[0099] なお、第二の実施形態で説明したように、顔認証と視線入力キーワード認証とで、同一の撮像装置20で撮影した同一フレームの顔画像が用いられてもよい。

[0100] 以上のように、本実施形態では、第一の実施形態の構成に加え、生体判定部37が、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を検知して、対象者の生体判定を行う。よって、第一の実施形態の効果に加え、成りすましを抑制する効果を高めることができる。

[0101] 次に、第一の実施形態の認証システム100を用いて具体例を説明する。図7は、視線入力キーワード認証を行う場合の動作例を示す説明図である。対象者31が認証装置10の前に現れると、出力部13が、表示装置30の画面のランダムな位置に、「ID番号は?」、「暗証番号は?」など、複数の質問の候補を出力する。その後、撮像装置20が、対象者31の顔画像を撮像し、回答特定部14および回答判定部15を含む解析部32が、視線33の方向から対象者31が選択した回答を特定する。そして、解析部32は、特定した回答と事前に登録された正答とを照合し、回答の正誤を判定する。この正誤判定により、認証装置10は、回答が正しければ、認証し、誤っていれば否認する。

[0102] なお、第二の実施形態の認証システム200および第三の実施形態の認証システム300でも、同様に処理が行われる。このようなシステムを一体として取り扱うことで、個別に部材を揃えるよりも、設置や保守が容易という効果が得られる。例えば、撮像装置20や、上述する解析部は、上記各実施形態で行われる各用途で共用できる。

[0103] 次に、本発明の認証システムを、認証サービスに用いた場合の動作例を説明する。図8は、認証システムを用いた動作例を示すシーケンス図である。図8に示す例は、対象者417が連動サービス419を利用する場合に、本発明の認証システムを認証サービス418として利用した場合の動作を示す

。すなわち、図8に例示するように、本動作例では、対象者417と、認証サービスと418と、連動サービス419の3つのオブジェクトが存在するものとし、この3つのオブジェクト間でメッセージの交換および実行を行うことで、全体としての認証サービスが提供される。

[0104] 連動サービス419として、例えば、認証結果に応じて預金の預け入れや引き出しを許可するATM (automatic teller machine) サービスや、認証結果に応じて扉やゲートの開閉を行う入場管理サービスなどが挙げられる。

[0105] まず対象者417が認証システムの場所に現れると、認証サービス418は、何らかの方法でこれを検知し、認証サービスを開始する。具体的には、例えば、対象者417が認証開始ボタンなどを押すことにより、認証サービス418が開始を認識しても良いし、認証サービス418がカメラ（撮像装置20）の映像から一定以上の大きさの人の顔を検知して、対象者417が現れたことを認識しても良い。図8に示す例では、これを一般化し、ダイアグラム上にないオブジェクトから認証サービス418へ、ファウンドメッセージ420が送られるとして表記している。

[0106] 認証サービス418は、ファウンドメッセージ420を受け取ると、動作421として質問および回答候補を出力する。具体的には、認証サービス418は、例えば「ID番号は?」、「パスワードは?」といった質問と、0から9までの数字を回答候補として設定し、その回答候補を表示装置30上のランダムな位置に出力する。

[0107] ここで、認証サービス418は、動作421において、対象者の顔認証を実行し、その結果より推定された人物が事前に登録した、例えば「卒業した小学校の名は?」などの秘密の質問を設定し、事前に登録された回答などを回答候補に設定して出力しても良い。

[0108] 次に、認証サービス418は、設定した質問を、メッセージ422として対象者417に送信する。具体的には、認証サービス418は、例えば、質問をスピーカーから音声にて出力してもよく、表示装置30上に質問を表示してもよい。

[0109] メッセージ422として質問を受け取った対象者417は、表示装置30上のランダムな位置に出力された回答候補の中から正答を探し、正答を注視する動作423を行う。この動作423において、対象者417は、視線の方向という態様でメッセージ424を認証サービス418へ繰り返して送ることになる。また、動作423と並行して、認証サービス418は、カメラ（撮像装置20）にて対象者417の顔画像を繰り返し撮像する。図8に示す例では、取得される顔画像をダイアグラム上にないオブジェクトから認証サービス418へ送られるファウンドメッセージ425として表記している。

[0110] 認証サービス418は、メッセージ424およびメッセージ425を受信すると、動作426として、視線の方向から回答を認識して照合する視線入力キーワード認証、顔画像から特徴を抽出して照合する顔認証、および、時系列に変化する視線と顔の向きの相対角度の変化などから成りすまし防止の確認を実行する。そして、認証サービス418は、認証結果をメッセージ427として連動サービス419に通知すると共に、メッセージ428として対象者417へも返信する。認証サービス418は、例えば、告知音やアラーム音などで認証結果を対象者417に伝えてもよい。

[0111] 図8に例示するように、対象者417に要求される動作は、動作423に示す回答候補を選択するという1つの動作である。このように、上述する実施形態では、対象者に回答候補を選択させることで複数の認証を同時に行うことができる。また、対象者にも認証側にも高い信頼性および利便性を提供できる。また、上述する実施形態が、どのような装置や機器に分割されて実現されていてもよい。

[0112] 次に、本発明の概要を説明する。図9は、本発明による認証装置の概要を示すブロック図である。本発明による認証装置80は、対象者の認証を行う認証装置（例えば、認証装置10）であって、対象者へ行う質問に対して複数の回答候補を表示装置（例えば、表示装置30）に出力する出力手段81（例えば、出力部13）と、対象者の顔画像を撮像する撮像装置（例えば、

撮像装置 20) により撮像された顔画像における対象者の視線に基づいて、回答候補の中から質問に対する回答を特定する回答特定手段 82 (例えば、回答特定部 14) と、特定された回答の正誤判定を行う回答判定手段 83 (例えば、回答判定部 15) と、撮像装置により撮像された顔画像から対象者の顔認証を行う顔認証手段 84 (例えば、顔認証部 16) と、複数の顔画像から検知される対象者の視線の変化に基づいて、対象者の生体判定を行う生体判定手段 85 (例えば、生体判定部 17) と、正誤判定、生体判定、および、顔認証の結果に基づいて、対象者の認証を行う対象者認証手段 86 (例えば、対象者認証部 18) とを備えている。

[0113] そのような構成により、認証側および対象者の認証時の利便性を向上させつつ、対象者の成りすましを検知して、対象者を高精度で認証することができる。

[0114] また、回答特定手段 82 は、対象者が回答を特定した回答時刻を取得し、顔認証手段 84 は、回答時刻と同時刻に行われた顔認証の結果を取得し、対象者認証手段 86 は、対象者が、顔認証で照合した人物の生体であると認証してもよい。

[0115] また、生体判定手段 85 は、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を検知して、対象者の生体判定を行ってもよい。

[0116] また、出力手段 81 は、顔認証により認証された対象者固有の質問に対応する複数の回答候補を表示装置に出力してもよい。

[0117] また、回答特定手段 82 は、第一の撮像装置で撮像された第一顔画像における対象者の視線に基づいて回答を特定し、顔認証手段 84 は、第二の撮像装置で撮像された第二顔画像から対象者の顔認証を行ってもよい。

[0118] 図 10 は、本発明による認証システムの概要を示すブロック図である。本発明による認証システム 90 は、対象者の認証を行う認証システム (例えば、認証システム 100) であって、対象者の顔画像を撮像する撮像装置 91 と、図 9 に例示する出力手段 81 と、回答特定手段 82 と、回答判定手段 8

３と、顔認証手段８４と、生体判定手段８５と、対象者認証手段８６とを備えている。

[0119] そのような構成によっても、認証側および対象者の認証時の利便性を向上させつつ、対象者の成りすましを検知して、対象者を高精度で認証することができる。

[0120] 上記の実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

[0121] （付記１）対象者の認証を行う認証装置であって、前記対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力手段と、前記対象者の顔画像を撮像する撮像装置により撮像された当該顔画像における対象者の視線に基づいて、前記回答候補の中から前記質問に対する回答を特定する回答特定手段と、特定された回答の正誤判定を行う回答判定手段と、前記撮像装置により撮像された顔画像から前記対象者の顔認証を行う顔認証手段と、複数の前記顔画像から検知される前記対象者の視線の変化に基づいて、前記対象者の生体判定を行う生体判定手段と、前記正誤判定、前記生体判定、および、前記顔認証の結果に基づいて、対象者の認証を行う対象者認証手段とを備えたことを特徴とする認証装置。

[0122] （付記２）回答特定手段は、対象者が回答を特定した回答時刻を取得し、顔認証手段は、前記回答時刻と同時刻に行われた顔認証の結果を取得し、対象者認証手段は、対象者が、顔認証で照合した人物の生体であると認証する付記１記載の認証装置。

[0123] （付記３）生体判定手段は、対象者が視線を動かして回答を選択している間の、顔の方向に対する視線の相対角度変化を検知して、対象者の生体判定を行う付記１または付記２記載の認証装置。

[0124] （付記４）出力手段は、顔認証により認証された対象者固有の質問に対応する複数の回答候補を表示装置に出力する付記１から付記３のうちのいずれか１つに記載の認証装置。

[0125] （付記５）回答特定手段は、第一の撮像装置で撮像された第一顔画像におけ

る対象者の視線に基づいて回答を特定し、顔認証手段は、第二の撮像装置で撮像された第二顔画像から対象者の顔認証を行う付記 1 から付記 4 のうちのいずれか 1 つに記載の認証装置。

[0126] (付記 6) 対象者の認証を行う認証システムであって、前記対象者の顔画像を撮像する撮像装置と、前記対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力手段と、撮像された前記顔画像における対象者の視線に基づいて、前記回答候補の中から前記質問に対する回答を特定する回答特定手段と、特定された回答の正誤判定を行う回答判定手段と、撮像された前記顔画像から前記対象者の顔認証を行う顔認証手段と、複数の前記顔画像から検知される前記対象者の視線の変化に基づいて、前記対象者の生体判定を行う生体判定手段と、前記正誤判定、前記生体判定、および、前記顔認証の結果に基づいて、対象者の認証を行う対象者認証手段とを備えたことを特徴とする認証システム。

[0127] (付記 7) 対象者の顔画像を撮像する複数の撮像装置を備え、回答特定手段は、第一の撮像装置で撮像された第一顔画像における対象者の視線に基づいて回答を特定し、顔認証手段は、第二の撮像装置で撮像された第二顔画像から対象者の顔認証を行う付記 6 記載の認証システム。

[0128] (付記 8) 対象者の認証を行う認証方法であって、前記対象者へ行う質問に対して複数の回答候補を表示装置に出力し、前記対象者の顔画像を撮像する撮像装置により撮像された当該顔画像における対象者の視線に基づいて、前記回答候補の中から前記質問に対する回答を特定し、特定された回答の正誤判定を行い、前記撮像装置により撮像された顔画像から前記対象者の顔認証を行い、複数の前記顔画像から検知される前記対象者の視線の変化に基づいて、前記対象者の生体判定を行い、前記正誤判定、前記生体判定、および、前記顔認証の結果に基づいて、対象者の認証を行うことを特徴とする認証方法。

[0129] (付記 9) 対象者が回答を特定した回答時刻を取得し、前記回答時刻と同時刻に行われた顔認証の結果を取得し、対象者が、顔認証で照合した人物の生

体であると認証する付記 8 記載の認証方法。

- [0130] (付記 10) 対象者の認証を行うコンピュータに適用される認証プログラムを記憶するプログラム記憶媒体であって、前記コンピュータに、前記対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力処理、前記対象者の顔画像を撮像する撮像装置により撮像された当該顔画像における対象者の視線に基づいて、前記回答候補の中から前記質問に対する回答を特定する回答特定処理、特定された回答の正誤判定を行う回答判定処理、前記撮像装置により撮像された顔画像から前記対象者の顔認証を行う顔認証処理、複数の前記顔画像から検知される前記対象者の視線の変化に基づいて、前記対象者の生体判定を行う生体判定処理、および、前記正誤判定、前記生体判定、および、前記顔認証の結果に基づいて、対象者の認証を行う対象者認証処理を実行させるための認証プログラムを記憶するプログラム記憶媒体。
- [0131] (付記 11) コンピュータに、回答特定処理で、対象者が回答を特定した回答時刻を取得させ、顔認証処理で、前記回答時刻と同時刻に行われた顔認証の結果を取得させ、対象者認証処理で、対象者が、顔認証で照合した人物の生体であると認証させる認証プログラムを記憶する付記 10 記載のプログラム記憶媒体。
- [0132] (付記 12) 対象者の認証を行うコンピュータに適用される認証プログラムであって、前記コンピュータに、前記対象者へ行う質問に対して複数の回答候補を表示装置に出力する出力処理、前記対象者の顔画像を撮像する撮像装置により撮像された当該顔画像における対象者の視線に基づいて、前記回答候補の中から前記質問に対する回答を特定する回答特定処理、特定された回答の正誤判定を行う回答判定処理、前記撮像装置により撮像された顔画像から前記対象者の顔認証を行う顔認証処理、複数の前記顔画像から検知される前記対象者の視線の変化に基づいて、前記対象者の生体判定を行う生体判定処理、および、前記正誤判定、前記生体判定、および、前記顔認証の結果に基づいて、対象者の認証を行う対象者認証処理を実行させるための認証プログラム。

[0133] (付記 1 3) コンピュータに、回答特定処理で、対象者が回答を特定した回答時刻を取得させ、顔認証処理で、前記回答時刻と同時刻に行われた顔認証の結果を取得させ、対象者認証処理で、対象者が、顔認証で照合した人物の生体であると認証させる付記 1 2 記載の認証プログラム。

[0134] 以上、実施形態を参照して本願発明を説明したが、本願発明は上記実施形態に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

産業上の利用可能性

[0135] 本発明は、対象者の認証を行う認証装置に好適に適用される。具体的には、本発明を、金融取引や契約行為などにおける個人認証に用いることが可能である。それだけでなく、本発明を、あるエリアに入場可能な人物を制限するなどのセキュリティ分野や、ある店舗に訪れた人物に特別なサービスを提供するなどの商業分野など、様々な産業分野に適用可能である。

符号の説明

- [0136] 1 0, 1 1 0, 2 1 0 認証装置
- 1 1 記憶部
 - 1 2 入力部
 - 1 3 出力部
 - 1 4, 2 4 回答特定部
 - 1 5 回答判定部
 - 1 6, 2 6 顔認証部
 - 1 7, 3 7 生体判定部
 - 1 8, 2 8 対象者認証部
 - 2 0 撮像装置
 - 3 0 表示装置
 - 1 0 0, 2 0 0, 3 0 0 認証システム