(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7100334号
(P7100334)

(45)発行日　令和4年7月13日(2022.7.13)

(24)登録日　令和4年7月5日(2022.7.5)

(51)国際特許分類
Ｇ０６Ｔ　7/00　(2017.01)

ＦＩ
Ｇ０６Ｔ　7/00　５１０Ｆ

請求項の数　4　（全13頁）

(21)出願番号　特願2020-512627(P2020-512627)
(86)(22)出願日　平成30年11月30日(2018.11.30)
(86)国際出願番号　PCT/JP2018/044252
(87)国際公開番号　WO2020/110306
(87)国際公開日　令和2年6月4日(2020.6.4)
審査請求日　令和2年3月6日(2020.3.6)
審判番号　不服2021-5404(P2021-5404/J1)
審判請求日　令和3年4月26日(2021.4.26)
早期審査対象出願

(73)特許権者　506214633
株式会社ショーケース
東京都港区六本木一丁目９番９号
(74)代理人　100104776
弁理士　佐野 弘
(72)発明者　▲高▼野 茂治
東京都港区六本木一丁目９番９号 株式会社ショーケース内
(72)発明者　カダカ ナラヤン
東京都港区六本木一丁目９番９号 株式会社ショーケース内
(72)発明者　元島 拓也
東京都港区六本木一丁目９番９号 株式会社ショーケース内
合議体

最終頁に続く

(54)【発明の名称】　認証装置、認証方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
利用者の本人認証に用いる認証装置であって、
撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証する第一の認証手段と、
該第一の認証手段による認証の可否の結果を表示手段に表示させる第一の認証結果表示手段と、
前記第一の認証手段における前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う利用者を撮影し、該撮影した映像に基づいて前記利用者を認証する第二の認証手段と、
該第二の認証手段による認証の可否の結果を表示手段に表示させる第二の認証結果表示手段と、
前記利用者の顔の画像が記録される記録手段と
を備え、
前記第一の認証手段は、前記撮影装置が撮影した前記利用者の顔の画像と前記記録手段に記録された前記利用者の顔の画像とを比較する比較処理を行い、
前記第一の認証手段と前記第一の認証結果表示手段とは、
前記比較処理の結果、前記第一の認証手段が両方の前記顔の画像が同一人物の前記顔の画像であることを認識した場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功したことを表示させると共に、前記第一の認証手段が前記認証を成功したものとする

第一の成功処理、
及び、
前記比較処理の結果、前記第一の認証手段が前記両方の顔の画像が前記同一人物の顔の画像であることを認識できない場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第一の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第一の不成功処理、
を行い、
前記第二の認証手段は、前記第一の認証手段による前記認証が成功した後に前記利用者に対して所定の動作を要求する情報が出力されて、該所定の動作を要求する情報の出力の後に前記撮影装置が撮影した前記利用者の顔の静止画像と、前記第一の認証手段における前記比較処理で用いられた前記顔の画像とからそれぞれ所定の特徴点の情報を抽出し、それぞれの前記特徴点の差分情報によって前記利用者が前記所定の動作を行ったかを判断する判断処理を行い、
前記第二の認証手段と前記第二の認証結果表示手段とにおいては、
前記判断処理の結果、前記第二の認証手段が前記特徴点の差分情報において前記要求された動作に対応した所定の静止状態を検出した場合に、前記第二の認証結果表示手段が、前記表示手段に認証に成功したことを表示させると共に前記第二の認証手段が前記認証を成功したものとする第二の成功処理、
及び、
前記判断処理の結果、前記第二の認証手段が、前記要求された動作に対応した所定の静止状態を検出しなかった場合に、前記第二の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第二の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第二の不成功処理、
を行い、
前記第一の認証手段における前記第一の成功処理ののちに前記第二の認証手段における前記第二の成功処理が行われた場合に、前記利用者の認証が成功したものとすることを特徴とする、認証装置。
【請求項２】
前記撮影装置を備えた、前記利用者が使用する利用者端末が備えるＷｅｂブラウザとの間で通信を行う通信手段と、
前記通信手段を用いた通信により、前記Ｗｅｂブラウザに前記撮影装置を操作する命令を含むＨＴＭＬコードを送信することにより前記撮影装置を操作する撮影装置操作手段と、
を備えることを特徴とする、請求項１記載の認証装置。
【請求項３】
撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証する第一の認証手段と、
該第一の認証手段による認証の可否の結果を表示手段に表示させる第一の認証結果表示手段と、
前記第一の認証手段における前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う利用者を撮影し、該撮影した映像に基づいて前記利用者を認証する第二の認証手段と、
該第二の認証手段による認証の可否の結果を表示手段に表示させる第二の認証結果表示手段と、
前記利用者の顔の画像が記録される記録手段と
を備え、前記利用者の本人認証に用いる認証装置が行う認証方法であって、
前記利用者の顔が撮影された画像を前記記録手段に記録する記録ステップと、
前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を第一の認証手段に認証させる第一の認証ステップと、

該第一の認証ステップにおける認証の可否の結果を表示手段に表示させる第一の認証結果表示ステップと、
前記第一の認証ステップにおける前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う前記利用者を撮影し、該撮影した映像に基づいて前記利用者を第二の認証手段に認証させる第二の認証ステップと、
該第二の認証ステップにおける認証の可否の結果を表示手段に表示させる第二の認証結果表示ステップと、
を備え、
前記第一の認証ステップにおいては、
前記第一の認証手段が、前記撮影装置が撮影した前記利用者の顔の画像と前記記録手段に記録された前記利用者の顔の画像とを比較する比較処理を行い、
前記第一の認証手段と前記第一の認証結果表示手段とが、
前記比較処理の結果、前記第一の認証手段が両方の前記顔の画像が同一人物の前記顔の画像であることを認識した場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功したことを表示させると共に、前記第一の認証手段が前記認証を成功したものとする第一の成功処理、
及び、
前記比較処理の結果、前記第一の認証手段が前記両方の顔の画像が前記同一人物の顔の画像であることを認識できない場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第一の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第一の不成功処理、
を行い、
前記第二の認証ステップにおいては、
前記第二の認証手段が、前記第一の認証ステップにおける前記認証が成功した後に前記利用者に対して所定の動作を要求する情報が出力されて、該所定の動作を要求する情報の出力の後に前記撮影装置が撮影した前記利用者の顔の静止画像と、前記第一の認証ステップにおける前記比較処理で用いられた前記顔の画像とからそれぞれ所定の特徴点の情報を抽出し、それぞれの前記特徴点の差分情報によって前記利用者が前記所定の動作を行ったかを判断する判断処理を行い、
前記第二の認証手段と前記第二の認証結果表示手段とにおいては、
前記判断処理の結果、前記第二の認証手段が前記特徴点の差分情報において前記要求された動作に対応した所定の静止状態を検出した場合に、前記第二の認証結果表示手段が、前記表示手段に認証に成功したことを表示させると共に前記第二の認証手段が前記認証を成功したものとする第二の成功処理、
及び、
前記判断処理の結果、前記第二の認証手段が、前記要求された動作に対応した所定の静止状態を検出しなかった場合に、前記第二の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第二の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第二の不成功処理、
を行い、
前記第一の認証ステップにおける前記第一の成功処理ののちに前記第二の認証ステップにおける前記第二の成功処理が行われた場合に、前記利用者の認証が成功したものとすることを特徴とする、認証方法。

【請求項４】

コンピュータを請求項１又は２のいずれかに記載の認証装置として機能させることを特徴とする、コンピュータ読み込み可能なプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】
本発明は、利用者の映像に基づいて認証を行う認証装置、認証方法、及びプログラムに関する。
【背景技術】
【０００２】
利用者の顔をカメラ等の撮影装置により撮影し、予め記録された画像、動画等の映像と比較して認証する装置として、例えば特許文献１の顔認証装置が知られている。
【０００３】
顔認証は利用者本人の生体的な特徴により認証行うことができ、鍵やパスワードが不要となるので利便性が高く、かつ、安全性の高い認証方法として有用である。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２００８－１４６５３９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
顔認証は前述の通り、鍵やパスワードが不要なため利便性が高い認証方法であるが、従来の顔認証装置では、カメラの前に利用者の顔写真をかざす等により不正なアクセスが可能であるという問題があった。
【０００６】
この発明は上記の問題に鑑みてなされたものであり、顔認証の利便性を損なうことなく不正アクセスを効果的に防止できる認証装置、認証方法、及びプログラムを提供する点にある。
【課題を解決するための手段】
【０００７】
かかる課題を解決するために、請求項１の発明に係る認証装置は、利用者の本人認証に用いる認証装置であって、撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証する第一の認証手段と、該第一の認証手段による認証の可否の結果を表示手段に表示させる第一の認証結果表示手段と、前記第一の認証手段における前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う利用者を撮影し、該撮影した映像に基づいて前記利用者を認証する第二の認証手段と、該第二の認証手段による認証の可否の結果を表示手段に表示させる第二の認証結果表示手段と、前記利用者の顔の画像が記録される記録手段と
を備え、前記第一の認証手段は、前記撮影装置が撮影した前記利用者の顔の画像と前記記録手段に記録された前記利用者の顔の画像とを比較する比較処理を行い、前記第一の認証手段と前記第一の認証結果表示手段とは、前記比較処理の結果、前記第一の認証手段が両方の前記顔の画像が同一人物の前記顔の画像であることを認識した場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功したことを表示させると共に、前記第一の認証手段が前記認証を成功したものとする第一の成功処理、及び、前記比較処理の結果、前記第一の認証手段が前記両方の顔の画像が前記同一人物の顔の画像であることを認識できない場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第一の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第一の不成功処理、を行い、前記第二の認証手段は、前記第一の認証手段による前記認証が成功した後に前記利用者に対して所定の動作を要求する情報が出力されて、該所定の動作を要求する情報の出力の後に前記撮影装置が撮影した前記利用者の顔の静止画像と、前記第一の認証手段における前記比較処理で用いられた前記顔の画像とからそれぞれ所定の特徴点の情報を抽出し、それぞれの前記特徴点の差分情報によって前記利用者が前記所定の動作を行ったかを判断する判断処理を行い、前記第二の認証手段と前記第二の認証結果表示手段とに

おいては、前記判断処理の結果、前記第二の認証手段が前記特徴点の差分情報において前記要求された動作に対応した所定の静止状態を検出した場合に、前記第二の認証結果表示手段が、前記表示手段に認証に成功したことを表示させると共に前記第二の認証手段が前記認証を成功したものとする第二の成功処理、及び、前記判断処理の結果、前記第二の認証手段が、前記要求された動作に対応した所定の静止状態を検出しなかった場合に、前記第二の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第二の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第二の不成功処理、を行い、前記第一の認証手段における前記第一の成功処理ののちに前記第二の認証手段における前記第二の成功処理が行われた場合に、所定の表示手段に前記利用者の認証が成功したものとすることを特徴とする。

【０００８】

請求項２の発明は、請求項１に記載の構成において、前記撮影装置を備えた、前記利用者が使用する利用者端末が備えるＷｅｂブラウザとの間で通信を行う通信手段と、前記通信手段を用いた通信により、前記Ｗｅｂブラウザに前記撮影装置を操作する命令を含むＨＴＭＬコードを送信することにより前記撮影装置を操作する撮影装置操作手段と、を備えることを特徴とする。

【００１０】

請求項３の発明に係る認証方法は、撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証する第一の認証手段と、該第一の認証手段による認証の可否の結果を表示手段に表示させる第一の認証結果表示手段と、前記第一の認証手段における前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う利用者を撮影し、該撮影した映像に基づいて前記利用者を認証する第二の認証手段と、該第二の認証手段による認証の可否の結果を表示手段に表示させる第二の認証結果表示手段と、前記利用者の顔の画像が記録される記録手段とを備え、前記利用者の本人認証に用いる認証装置が行う認証方法であって、前記利用者の顔が撮影された画像を前記記録手段に記録する記録ステップと、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を第一の認証手段に認証させる第一の認証ステップと、該第一の認証ステップにおける認証の可否の結果を表示手段に表示させる第一の認証結果表示ステップと、前記第一の認証ステップにおける前記認証に成功した場合に、前記利用者に所定の動作を要求するとともに、前記撮影装置を操作して前記動作を行う前記利用者を撮影し、該撮影した映像に基づいて前記利用者を第二の認証手段に認証させる第二の認証ステップと、該第二の認証ステップにおける認証の可否の結果を表示手段に表示させる第二の認証結果表示ステップと、を備え、前記第一の認証ステップにおいては、前記第一の認証手段が、前記撮影装置が撮影した前記利用者の顔の画像と前記記録手段に記録された前記利用者の顔の画像とを比較する比較処理を行い、前記第一の認証手段と前記第一の認証結果表示手段とにおいては、前記比較処理の結果、前記第一の認証手段が両方の前記顔の画像が同一人物の前記顔の画像であることを認識した場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功したことを表示させると共に、前記第一の認証手段が前記認証を成功したものとする第一の成功処理、及び、前記比較処理の結果、前記第一の認証手段が前記両方の顔の画像が前記同一人物の顔の画像であることを認識できない場合に、前記第一の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第一の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第一の不成功処理、を行い、前記第二の認証ステップにおいては、前記第二の認証手段が、前記第一の認証ステップにおける前記認証が成功した後に前記利用者に対して所定の動作を要求する情報が出力されて、該所定の動作を要求する情報の出力の後に前記撮影装置が撮影した前記利用者の顔の静止画像と、前記第一の認証ステップにおける前記比較処理で用いられた前記顔の画像とからそれぞれ所定の特徴点の情報を抽出し、それぞれの前記特徴点の差分情報によって前記利用者が前記所定の動作を行ったかを判断する判断処理を行

い、前記第二の認証手段と前記第二の認証結果表示手段とが、前記判断処理の結果、前記第二の認証手段が前記特徴点の差分情報において前記要求された動作に対応した所定の静止状態を検出した場合に、前記第二の認証結果表示手段が、前記表示手段に認証に成功したことを表示させると共に前記第二の認証手段が前記認証を成功したものとする第二の成功処理、及び、前記判断処理の結果、前記第二の認証手段が、前記要求された動作に対応した所定の静止状態を検出しなかった場合に、前記第二の認証結果表示手段が前記表示手段に認証に成功しなかったことを表示させると共に、前記第二の認証手段が、前記撮影装置を操作して利用者の顔を撮影し、該撮影した映像に基づいて前記利用者を認証することを所定回数繰り返す第二の不成功処理、を行い、前記第一の認証ステップにおける前記第一の成功処理ののちに前記第二の認証ステップにおける前記第二の成功処理が行われた場合に、前記利用者の認証が成功したものとすることを特徴とする。

【００１１】

請求項４の発明に係るプログラムは、コンピュータ読み取り可能なプログラムであって、コンピュータを請求項１又は２に記載の認証装置として機能させることを特徴とする。

【発明の効果】

【００１２】

本発明の構成によれば、第一の認証手段により利用者の顔を撮影した映像に基づく認証に成功した後に、第二の認証手段により利用者の動作を撮影し、当該撮影した映像に基づく認証を行う。第一及び第二の認証手段の何れも利用者を撮影した映像に基づいて認証を行うので、顔認証の利便性を損なうことなく、不正アクセスを効果的に防止することができる。

【図面の簡単な説明】

【００１３】

【図１】実施の形態に係る認証装置全体の構成を概念的に示すブロック図である。

【図２】実施の形態に係る認証処理の流れを概念的に示すフロー図である。

【図３】実施の形態において、第一の認証手段による認証を行う際の画面構成を概念的に示す図である。

【図４】実施の形態において、第二の認証手段による認証を行う際の画面構成を概念的に示す図である。

【発明を実施するための形態】

【００１４】

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。

【００１５】

図１は、本発明の実施の形態に係る認証装置１００全体の構成を概念的に示すブロック図である。本実施の形態に係る認証装置１００は、利用者端末２００を使用する利用者の本人認証を行う機能を提供するものである。

【００１６】

図１で示すように、認証装置１００は、第一の認証手段１１０と、第二の認証手段１２０と、記録手段１３０と、通信手段１４０と、撮影装置操作手段１５０を備えている。

【００１７】

本実施の形態において、認証装置１００は、後述するネットワーク３００を介して後述する利用者端末２００と通信可能に接続されている。認証装置１００と利用者端末２００はＨｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ（ＨＴＴＰ）を用いて通信を行うことで、認証装置１００をサーバ、利用者端末２００をクライアントとするいわゆるＷｅｂアプリケーションとして認証機能を利用者に提供するよう構成されている。なお、本実施の形態では上記の構成としたが、認証処理の全体を認証装置１００のみで行うように構成してもよい。また、認証装置１００と利用者端末２００の通信に使用するプロトコルの周知のプロトコルを選択してよい。プロトコルにＨＴＴＰを使用する場合、暗号化された通信上でＨＴＴＰによるやり取りを行うＨｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ　Ｓｅｃｕｒｅ（ＨＴＴＰＳ）等を用いてもよい。

【００１８】
本実施の形態において、認証装置１００は周知のサーバ用コンピュータを用いて構成されている。本実施の形態では、コンピュータの二次記憶装置に後述する認証方法を実行するプログラムが予め記憶されており、当該プログラムをメモリにロードしてＣＰＵが実行することにより、当該コンピュータを認証装置１００として機能させるものである。
【００１９】
上記のとおり、本実施の形態では認証装置１００はサーバ用途のコンピュータを用いて構成されているが、認証装置１００に用いるコンピュータは適宜選択してよい。例えば、認証装置１００として一般的なパーソナル・コンピュータを用いてよいし、或いは、タブレット・コンピュータ等の携帯端末を用いて認証装置１００を構成するようにしてもよい。認証装置１００のハードウェア的な構成は、認証装置１００に要求される性能、耐久性、信頼性その他に応じて任意に変更してよい。
【００２０】
第一の認証手段１１０は、利用者が用いる利用者端末２００の撮影装置２１０を後述する撮影装置操作手段１５０により操作して利用者の顔を撮影し、当該撮影した映像に基づいて利用者を認証する。なお、映像として画像すなわち静止画を用いるか、或いは動画を用いるかは任意に選択してよい。
【００２１】
第二の認証手段１２０は、上記の第一の認証手段１１０による認証に成功した場合に、利用者に所定の動作を行わせ、後述する撮影装置操作手段１５０により利用者端末２００の撮影装置２１０を操作して撮影し、当該撮影した映像に基づいて利用者を認証する。上記第一の認証手段１２０と同様に、第二の認証手段１１０が扱う映像が画像であるか動画であるかは任意に選択してよい。
【００２２】
記録手段１３０は、第一の認証手段１１０が行う認証処理において、認証時に後述する撮影装置２１０が撮影した映像を比較する映像を記録する。本実施の形態では、認証装置１００が備える二次記憶装置の一部領域をもって記録手段１３０を構成しているが、記録手段１３０をどのように構成するかは適宜変更が可能であり、例えばリレーショナル・データベース・マネージメント・システム（ＲＤＢＭＳ）を用いて記録手段１３０を構築してもよい。
【００２３】
通信手段１４０は、後述するネットワーク３００を介して利用者端末２００と通信を行う。本実施の形態は前述の通りWebアプリケーションとして構築されており、通信手段１４０は利用者端末２００のＷｅｂブラウザ２３０とＨＴＴＰにより通信を行う。
【００２４】
撮影装置操作手段１５０は、後述する撮影装置２１０を操作して利用者を撮影する。本実施の形態は前述の通りＷｅｂアプリケーションとして構築されており、認証時に撮影装置２１０を操作する命令を含むＨｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＨＴＭＬ）コードを利用者端末２００に送信して、撮影装置２１０を操作する。なお、上記命令は送信するＨＴＭＬコードに直接記載されていてもよいし、ＨＴＭＬコードから上記命令を含むスクリプト等のプログラムを参照するように記載されていてもよい。
【００２５】
利用者端末２００は、認証処理を行う利用者が使用する端末である。前述のように、本実施の形態はＷｅｂアプリケーションによる認証処理を行うが、利用者端末２００は当該Ｗｅｂアプリケーションにおけるクライアントとして機能する。利用者端末２００は撮影装置２１０、表示装置２２０、Ｗｅｂブラウザ２３０を備えている。
【００２６】
本実施の形態において、利用者端末２００はスマートフォン等の携帯端末を用いて構成される。利用者端末２００のＷｅｂブラウザ２３０により認証装置１００の所定のアドレスにアクセスすると後述する認証処理が開始される。なお、本実施の形態における利用者端

末２００は、撮影装置２１０、表示装置２２０、及びＷｅｂブラウザ２３０を備えているコンピュータであれば、一般的なパーソナル・コンピュータ等周知のコンピュータを用いてよい。

【００２７】

撮影装置２１０は、利用者を撮影するカメラである。本実施の形態では利用者端末２００としてスマートフォン等の携帯端末を用いており、当該携帯端末が備えるカメラを撮影装置２１０として用いる。利用者端末２００として一般的なパーソナル・コンピュータ等を用いる場合には、当該パーソナル・コンピュータ等に接続したＷｅｂカメラ等を撮影装置２１０として用いることができる。

【００２８】

表示装置２２０は、後述するＷｅｂブラウザ２３０の画面を表示するディスプレイである。本実施の形態では利用者端末２００としてスマートフォン等の携帯端末を用いており、当該携帯端末が備えるタッチパネル・ディスプレイを表示装置２２０として用いる。

【００２９】

Ｗｅｂブラウザ２３０は、後述のネットワーク３００を介して認証装置１００と通信し、認証装置１００から送信されたＨＴＭＬコードに基づいて所定の画面を表示装置２２０に描画する。

【００３０】

ネットワーク３００は、認証装置１００と利用者端末２００を通信可能に接続するネットワークである。本実施の形態におけるネットワーク３００は認証装置１００と利用者端末２００が使用するプロトコルによる通信が可能であれば、例えばインターネット等の広域ネットワークであってもよいし、局所的なローカル・エリア・ネットワーク（ＬＡＮ）であってもよい。また、有線ネットワークであってもよいし、無線ネットワークでもよいし、これらを組み合わせたネットワークであってもよい。

【００３１】

以上が、本実施の形態における認証装置１００全体の構成である。次いで、本実施の形態における認証の処理について説明する。

【００３２】

図２は、本実施の形態において、認証装置１００による認証処理の流れを概念的に示したフロー図である。本実施の形態では、Ｓ１０１～Ｓ１０４からなる第一の認証ステップＳ１００と、Ｓ２０１～Ｓ２０４からなる第二の認証ステップＳ２００の二段階からなる認証方法により利用者を認証する。

【００３３】

第一の認証ステップＳ１００は、利用者の顔を撮影し、当該撮影した映像に基づいて利用者を認証するステップである。

【００３４】

利用者端末２００のＷｅｂブラウザ２３０が認証装置１００にアクセスすると、認証装置１００は認証画面を構成するＨＴＭＬコードをＨＴＴＰレスポンス・メッセージとして利用者端末２００に送信する。利用者端末２００のＷｅｂブラウザ２３０は当該ＨＴＭＬコードに基づいて、認証画面を表示装置２２０に描画する（Ｓ１０１参照）。

【００３５】

図３は、本実施の形態における、認証画面Ｗ１００の画面構成を模式的に示した図である。図３で示すように、利用者端末２００の表示装置２２０には、Ｗｅｂブラウザ２３０により描画された認証画面Ｗ１００が全画面表示されており、認証画面Ｗ１００は撮影装置２１０が撮影する映像を表示する映像領域Ｗ１０１と、認証装置１００から利用者に向けて発信するメッセージを表示するメッセージ領域Ｗ１０２を備えている。

【００３６】

前述のステップＳ１０１において、認証装置１００から送信されたＨＴＭＬコードには、顔を撮影する旨を表示する文言の情報（たとえば、顔を撮影する旨を表示する文言をＷｅｂブラウザ２３０にテキスト表示するためのデータやイメージ表示するためのデータなど

）と、利用者端末２００の撮影装置２１０を操作するための命令が含まれている。利用者端末２００のＷｅｂブラウザ２３０は上記文言をメッセージ領域Ｗ１０２に表示する。図３においては、メッセージ領域Ｗ１０２に「中央に顔を合わせてください。撮影を行います。」というテキスト情報が表示された状態が示されている。そして、撮影装置操作手段１５０は、上記命令に基づいて撮影装置２１０を操作し、利用者の顔を撮影する（Ｓ１０２参照）。図３には、利用者端末２００を使用する利用者がステップＳ１０１で要求された動作である、顔を画面（すなわちＷｅｂブラウザ２３０）の中央に位置させて撮影している状態が示されている。

【００３７】

本実施の形態では、認証装置１００の記録手段１３０により、利用者の顔を撮影した映像が予め記録されている。認証装置１００の第一の認証手段１１０は、前述のステップＳ１０２で撮影した映像と、予め記録手段１３０により記録した映像とを比較して利用者を認証する（Ｓ１０３参照）。なお、具体的な比較の方法については周知の方法を用いてよく、例えば、利用者の顔を撮影した映像から利用者の特徴（たとえば特徴点の情報）を検出し、当該検出した特徴により認証を行う（たとえば、撮影装置２１０が撮影した映像から検出した特徴点の情報と、記録手段１３０に記録された映像から検出された特徴点の情報とを用いて、それらの特徴点の差分情報によって、撮影装置２１０が撮影した利用者端末２００の利用者が記録手段１３０に記録された写真の人物と同一人物かを判断する方法などがこれに該当する。ただし、これ以外のどのような方法を用いて判断がおこなわれてもよい。）ようにしてもよい。

【００３８】

前述のステップＳ１０３の結果、すなわち、第一の認証ステップによる認証に成功したか否かについて認証装置１００が認証の成否を示す文言を利用者端末２００に送信し、これを受信した利用者端末２００のＷｅｂブラウザ２３０が認証画面Ｗ１００のメッセージ領域Ｗ１０２に表示する（Ｓ１０４参照）。

【００３９】

本実施の形態では、上記第一の認証ステップによる認証が失敗した場合には、処理をＳ１０２から再度実行して、再度認証処理を行うことができる。認証に失敗した場合に再実行できるように構成するか否か、また、再実行する場合の回数等については、任意に選択してよい。

【００４０】

第一の認証ステップＳ１００による認証に成功した場合、認証装置１００は第二の認証ステップＳ２００を開始する。

【００４１】

第二の認証ステップＳ２００が開始されると、認証装置１００が利用者端末２００に利用者に所定の動作を行う旨、要求する文言の情報（たとえば、要求する文言をＷｅｂブラウザ２３０にテキスト表示するためのデータやイメージ表示するためのデータなど）を送信する。当該文言の情報は、利用者端末２００のＷｅｂブラウザ２３０により、認証画面Ｗ１００のメッセージ領域Ｗ１０２に表示される（Ｓ２０１）。所定の動作は、例えば利用者が片目を瞑るウィンク動作や、ピースサインその他のポーズを取る動作を適宜選択してよい。図４においては、メッセージ領域Ｗ１０２に「左目をウィンクしてください。撮影を行います。」というテキスト情報が表示された状態が示されている。

【００４２】

ステップＳ２０１で要求した動作を利用者が行うと、撮影装置操作手段１５０が利用者端末２００の撮影装置２１０を操作し、要求した動作を行う利用者を撮影する（Ｓ２０２参照）。図４には、利用者端末２００を使用する利用者がステップＳ２０１で要求された動作である、左目をウィンクした状態（かつ、Ｗｅｂブラウザ２３０上で顔画像が左右反転して表示された状態）で撮影している状態が示されている。

【００４３】

図４は、前述のステップＳ２０１及びＳ２０２において、動作を行う利用者を撮影装置２

１０で撮影する際の認証画面Ｗ１００画面構成を模式的に示した図である。図２で示すように、認証装置１００から送信された所定の動作を行う旨要求する文言はメッセージ領域Ｗ１０２に表示され、当該要求に従って利用者が動作を行うと、利用者端末２００の撮影装置２１０により当該動作を行う利用者が撮影される。

【００４４】

本実施の形態では、第二の認証手段１２０は、撮影された映像を検証する処理を行い、利用者端末２００を使用する利用者が所定の処理を行ったか否かを確認する（Ｓ２０３参照）。

【００４５】

ステップＳ２０３における具体的な比較の方法は、具体的には、たとえば、撮影装置２１０がステップＳ１０２で撮影した映像から検出した特徴点の情報と、ステップＳ２０２で撮影した映像から検出された特徴点の情報とを用いて、それらの特徴点の差分情報によって、利用者端末２００の利用者が要求された所定の動作を行ったか否かを判断する方法などがこれに該当する。このような手順を用いれば、利用者端末２００を使用する利用者が実際に利用者端末２００をリアルタイムで操作していることを確認できる。ゆえに、たとえば、不正なログインを行おうとする悪意の第三者が、利用者端末２００を使用する利用者の顔写真を撮影装置２１０で撮影することで第一の認証ステップＳ１００の認証に成功した場合であっても、第二の認証ステップＳ２００で認証が失敗することになる。そして、このような、悪意の第三者が、利用者の顔写真等を用いた不正な操作によって不正な認証操作を行って不正なログインを成功させてしまうことを防止できる。

【００４６】

なお、ステップＳ２０３の手順においては、上記以外のどのような方法を用いて、利用者端末２００を使用する利用者が所定の動作が行ったか否かの判断が行われてもよい。たとえば、記録手段１３０に、利用者の動作後の顔写真も記録しておき、ステップＳ２０２で撮影した映像を、記録手段１３０に記録された、利用者の動作後の顔写真と比較検証するような方法であってもよい。

【００４７】

認証装置１００は、ステップＳ２０３における、第二の認証手段１２０による認証が完了すると、その成否を示す文言を利用者端末２００に送信する（Ｓ２０４）。認証に成功した場合は、本実施の形態における認証処理を完了する。認証に失敗した場合は、ステップＳ２０１から再度第二の認証ステップＳ２００を開始する。なお、第二の認証ステップＳ２００を再実行するか否か、及び、再実行する回数等については前述のステップＳ１０４と同様に、任意に設定してよい。また、ステップＳ２００による認証失敗時に、ステップＳ１００から再実行するようにしてもよい。

【００４８】

以上が、本実施の形態における認証処理の流れである。本実施の形態では、第一の認証ステップＳ１００により利用者の顔を撮影した映像に基づく認証に成功した後に、第二の認証ステップＳ２００により利用者の動作を撮影し、当該撮影した映像に基づく認証を行う。第一の認証ステップＳ１００及び第二の認証ステップＳ２００の何れも利用者を撮影した映像に基づいて認証を行うので、顔認証の利便性を損なうことなく、不正アクセスを効果的に防止することができる。

【００４９】

本実施の形態では、撮影装置２１０を備えた、利用者が使用する利用者端末２００が備えるＷｅｂブラウザ２３０との間で通信を行う通信手段１４０と、通信手段１４０を用いた通信により、Ｗｅｂブラウザ２３０に撮影装置２１０を操作する命令を含むＨＴＭＬコードを送信することにより撮影装置２１０を操作する撮影装置操作手段１５０とを備えることにより、を特徴とする、認証装置１００と利用者端末２００との物理的な離接状態に関わらず、利用者が利用者端末２００のＷｅｂブラウザ２３０から認証のための操作を行うことで、簡易かつ確実に利用者を撮影した映像に基づいて認証を行うことが可能となる。

【００５０】

本実施の形態では、認証装置１００は、さらに、利用者の顔を予め撮影した映像を記録する記録手段１３０を備え、第一の認証手段１１０は、利用者の顔を撮影した映像と、記録手段１３０に記録した映像を比較することにより認証を行うことにより、撮影した映像を記録した映像と対比して、双方が近似するか否かによって認証の成否を決定できるので、精度の高い認証を行うことができる。

【００５１】

本実施の形態の説明は以上であるが、本発明の構成は上記実施の形態に限られるものではない。例えば、本実施の形態では、第二の認証ステップＳ２００による認証に失敗した場合にのみＳ２０１から再開するよう構成しているが、第二の認証ステップＳ２００を、利用者に行わせる動作を変更しながら複数回実行するようにしてもよい。

【００５２】

たとえば、上記の実施の形態では、認証装置１００を利用者端末２００と別の場所に設けてネットワーク３００で接続する構成としたが、認証装置１００を利用者端末２００に組み込んだ態様としてもよい。

【００５３】

またたとえば、上記の実施の形態では、利用者端末２００を使用する利用者の認証に本発明を用いたが、利用者端末２００以外の構成、たとえば、特定の部屋や特定の空間（たとえばイベント会場やスタジアムや鉄道の駅構内など）に入室したり入場したりする入室者や入場者の顔認証を行う構成に本発明の認証装置１００を適用してもよい。また、利用者端末２００以外の通信機器や電気機器のログインや利用者認証などに本発明の認証装置１００を適用してもよい。この場合、認証装置１００は、上記の実施の形態と同様に、入室者や入場者が入室したり入場したりする場所とは別の場所に設けてネットワーク３００によって接続する構成としてもよいし、入室者や入場者が入室したり入場したりする場所に設けられていてもよい。

【００５４】

その他の具体的な構成も本実施の形態に限られるものではなく、本発明の趣旨を逸脱しない範囲において様々な変更が可能である。

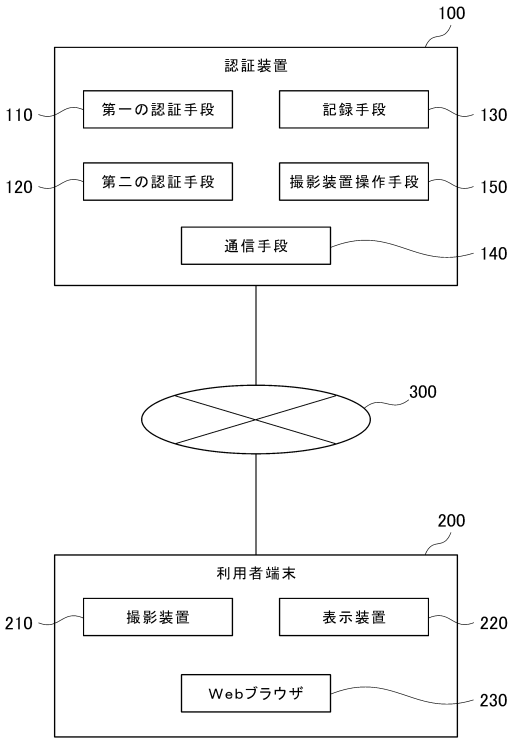
【符号の説明】

【００５５】

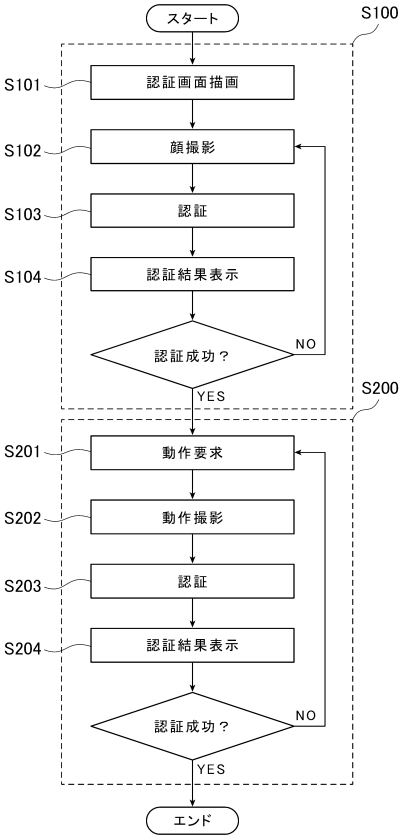
１００　認証装置
１１０　第一の認証手段
１２０　第二の認証手段
１３０　記録手段
１４０　通信手段
１５０　撮影装置操作手段
２００　利用者端末
２１０　撮影装置
２２０　表示装置
２３０　Ｗｅｂブラウザ
３００　ネットワーク

【図面】

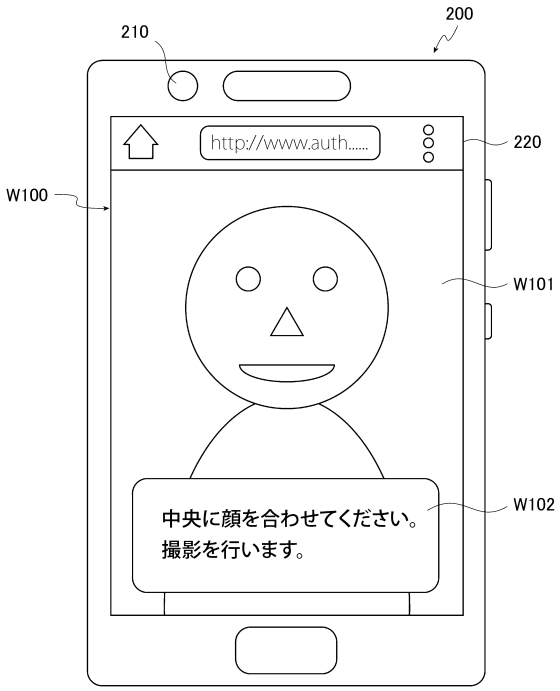
【図１】


100
認証装置
第一の認証手段
110
記録手段
130
第二の認証手段
120
撮影装置操作手段
150
通信手段
140
300
200
利用者端末
撮影装置
210
表示装置
220
Webブラウザ
230

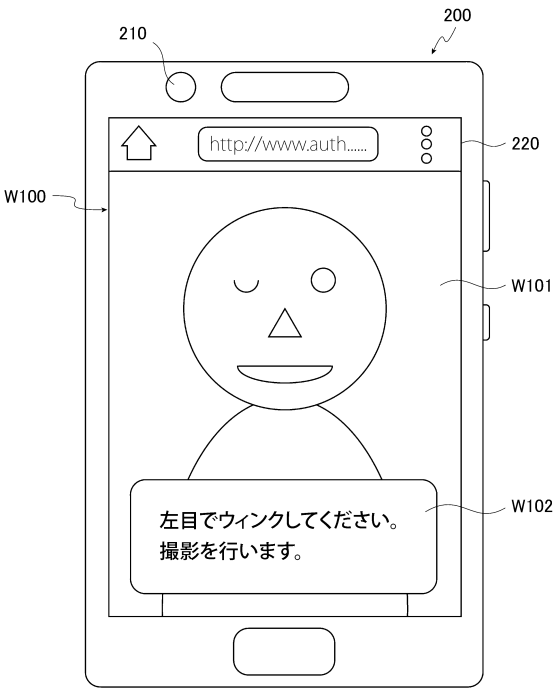
【図２】


スタート
S100
S101
認証画面描画
S102
顔撮影
S103
認証
S104
認証結果表示
認証成功？
NO
YES
S200
S201
動作要求
S202
動作撮影
S203
認証
S204
認証結果表示
認証成功？
NO
YES
エンド

【図３】


200
210
http://www.auth.....
220
W100
W101
中央に顔を合わせてください。
撮影を行います。
W102

【図４】


200
210
http://www.auth.....
220
W100
W101
左目でウィンクしてください。
撮影を行います。
W102

フロントページの続き

審判長　畑中 高行
審判官　新井 寛
審判官　渡辺 努
(56)参考文献　特開２０１５－１７６５５５（ＪＰ，Ａ）
特開２０１２－１０９９７６（ＪＰ，Ａ）
特開２００４－１１０８１３（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
G06T 7/00