

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B1)

(11) 特許番号

特許第6928191号
(P6928191)

(45) 発行日 令和3年9月1日(2021.9.1)

(24) 登録日 令和3年8月10日(2021.8.10)

(51) Int.Cl. F I
G 0 6 F 21/32 (2013.01) G O 6 F 21/32
A 6 1 B 5/00 (2006.01) A 6 1 B 5/00 1 O 2 A

請求項の数 9 (全 19 頁)

<p>(21) 出願番号 特願2021-39635 (P2021-39635) (22) 出願日 令和3年3月11日(2021.3.11) 審査請求日 令和3年3月11日(2021.3.11) 早期審査対象出願</p>	<p>(73) 特許権者 520154438 末次 功憲 東京都豊島区北大塚1-22-3 社内 (74) 代理人 100162341 弁理士 瀬崎 幸典 (72) 発明者 末次 功憲 東京都豊島区北大塚1-22-3 社内 審査官 小林 秀和</p>
---	--

最終頁に続く

(54) 【発明の名称】 認証システム、プログラム

(57) 【特許請求の範囲】

【請求項1】

本人認証方法の選択を受け付ける入力受付手段と、
 人物の認証処理を実行する認証手段と、
 前記人物の健康状態に関する複数の指標値を取得する取得手段と、
 前記取得手段により取得された前記指標値ごとに前記指標値の推移を示す推移データを生成する生成手段と、
 前記取得手段によりリアルタイムで都度取得される時点の前記指標値を、前記生成手段により生成された前記推移データから推定される前記指標値の正常値と比較して前記人物が異常状態あるいは非常事態にあるか否かを判定する判定手段と、
 前記判定手段の判定結果に基づいて、前記入力手段が受け付けた前記本人認証方法で前記人物の認証を行う制御手段と、を備えた、
 ことを特徴とする認証システム。

【請求項2】

前記認証手段は、前記人物の顔をスキャンすることで取得した顔データをもとに前記人物の顔認証を行う、
 ことを特徴とする請求項1に記載の認証システム。

【請求項3】

前記人物の健康状態に関する前記指標値は、前記人物の心拍数及び体温である、
 ことを特徴とする請求項1又は2に記載の認証システム。

【請求項 4】

前記人物の指紋認証を行う指紋認証手段を更に備え、
 前記制御手段は、前記判定手段で前記人物が正常状態にあると判定される場合であっても、前記指紋認証手段による指紋認証により前記人物が予め登録された人物と判定される場合に、前記認証手段で前記人物の認証を行う、
 ことを特徴とする請求項 1 ないし 3 のいずれか 1 項に記載の認証システム。

【請求項 5】

G P S 電波を受信する受信手段を更に備え、
 前記受信手段で受信された G P S 電波に基づき自装置の位置情報を算出して、算出された前記位置情報が予め登録された場所の条件に一致する場合に、前記認証手段で前記人物の認証を行う、
 ことを特徴とする請求項 1 ないし 4 のいずれか 1 項に記載の認証システム。

10

【請求項 6】

前記場所の条件は、前記人物が認証する場所及び前記人物が認証しない場所である、
 ことを特徴とする請求項 5 に記載の認証システム。

【請求項 7】

一人の第 1 人物、及び、一人の第 2 人物を少なくとも含む、複数人物がそれぞれの予め登録された情報と一致してログインが許可されたグループ認証状態を検出する認証検出手段を更に備え、
 前記認証検出手段により、前記グループ認証状態が検出された場合に、前記認証手段で前記人物の認証を行う、
 ことを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載の認証システム。

20

【請求項 8】

所定の時間内に前記グループ認証状態が検出された場合に、前記認証手段で前記人物の認証を行う、
 ことを特徴とする請求項 7 に記載の認証システム。

【請求項 9】

コンピュータに、
本人認証方法の選択を受け付ける入力受付ステップと、
人物の認証処理を実行する認証ステップと、
前記人物の健康状態に関する複数の指標値を取得する取得ステップと、
前記取得ステップにより取得された前記指標値ごとに前記指標値の推移を示す推移データを生成する生成ステップと、
前記取得ステップによりリアルタイムで都度取得される時点の前記指標値を、前記生成ステップにより生成された前記推移データから推定される前記指標値の正常値と比較して前記人物が異常状態あるいは非常状態にあるか否かを判定する判定ステップと、
前記判定ステップの判定結果に基づいて、前記入力受付ステップで受け付けた前記本人認証方法で前記人物の認証を行う制御ステップと、 を実行させる、
 ことを特徴とするプログラム。

30

【発明の詳細な説明】

40

【技術分野】

【0001】

本発明は、認証技術に関し、特に人を認証する認証システム、プログラムに関する。

【背景技術】

【0002】

ユーザー端末がサーバにアクセスする際に入力データが所定要件を満たした場合にログインを許可するログイン認証システムのプログラムであって、ユーザー端末のカメラを用いてユーザーの顔を撮影する撮影ステップと、撮影した画像データと事前に登録されたユーザーの顔写真データとを画像認証手段によって比較して同一人物の可能性を数値で得る確率値取得ステップと、同一人物の可能性の数値が所定値以上か否かを判定することによ

50

り撮影されたユーザーが登録ユーザーか否かを判定するユーザー判定ステップと、同一人物の可能性の数値が所定値以上であるとき、ユーザー端末のログインを許可するログイン許可ステップと、を具備しているログイン認証システムのプログラムが知られている（特許文献1）。

【0003】

対象者のバイタル値を測定する測定部と、測定部により一日以上測定されたバイタル値から、対象者の一日分の概日リズムを示すモデル情報を生成するモデル情報生成部と、モデル情報の生成後に測定部により測定されるバイタル値と、モデル情報とを比較して、その比較結果により、対象者の概日リズムの乱れの発生の有無を判定する判定部と、を備える健康状態判定システムも知られている（特許文献2）。

10

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特願2020-201595号公報

【特許文献2】特開2020-109616号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

本発明は、ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性を向上させる。

20

【課題を解決するための手段】

【0006】

前記課題を解決するために、請求項1に記載の認証システムは、
本人認証方法の選択を受け付ける入力受付手段と、
 人物の認証処理を実行する認証手段と、
 前記人物の健康状態に関する複数の指標値を取得する取得手段と、
 前記取得手段により取得された前記指標値ごとに前記指標値の推移を示す推移データを生成する生成手段と、

前記取得手段によりリアルタイムで都度取得される時点の前記指標値を、前記生成手段により生成された前記推移データから推定される前記指標値の正常値と比較して前記人物が異常状態あるいは非常事態にあるか否かを判定する判定手段と、

30

前記判定手段の判定結果に基づいて、前記入力手段が受け付けた前記本人認証方法で前記人物の認証を行う制御手段と、を備えた、

ことを特徴とする。

【0007】

請求項2に記載の発明は、請求項1に記載の認証システムにおいて、
 前記認証手段は、前記人物の顔をスキャンすることで取得した顔データをもとに前記人物の顔認証を行う、

ことを特徴とする。

【0008】

請求項3に記載の発明は、請求項1または2に記載の認証システムにおいて、
 前記人物の健康状態に関する前記指標値は、前記人物の心拍数及び体温である、
 ことを特徴とする。

40

【0009】

請求項4に記載の発明は、請求項1ないし3のいずれか1項に記載の認証システムにおいて、

前記人物の指紋認証を行う指紋認証手段を更に備え、

前記制御手段は、前記判定手段で前記人物が正常状態にあると判定される場合であっても、前記指紋認証手段による指紋認証により前記人物が予め登録された人物と判定される場合に、前記認証手段で前記人物の認証を行う、

50

ことを特徴とする。

【0010】

請求項5に記載の発明は、請求項1ないし4のいずれか1項に記載の認証システムにおいて、

GPS電波を受信する受信手段を更に備え、

前記受信手段で受信されたGPS電波に基づき自装置の位置情報を算出して、算出された前記位置情報が予め登録された場所の条件に一致する場合に、前記認証手段で前記人物の認証を行う、

ことを特徴とする。

【0011】

請求項6に記載の発明は、請求項5に記載の認証システムにおいて、

前記場所の条件は、前記人物が認証する場所及び前記人物が認証しない場所である、

ことを特徴とする。

10

【0012】

請求項7に記載の発明は、請求項1ないし6のいずれか1項に記載の認証システムにおいて、

一人の第1人物、及び、一人の第2人物を少なくとも含む、複数人物がそれぞれの予め登録された情報と一致してログインが許可されたグループ認証状態を検出する認証検出手段を更に備え、

前記認証検出手段により、前記グループ認証状態が検出された場合に、前記認証手段で前記人物の認証を行う、

ことを特徴とする。

20

【0013】

請求項8に記載の発明は、請求項7に記載の認証システムにおいて、

所定の時間内に前記グループ認証状態が検出された場合に、前記認証手段で前記人物の認証を行う、

ことを特徴とする。

【0014】

前記課題を解決するために、請求項9に記載のプログラムは、

コンピュータに、

本人認証方法の選択を受け付ける入力受付ステップと、

人物の認証処理を実行する認証ステップと、

前記人物の健康状態に関する複数の指標値を取得する取得ステップと、

前記取得ステップにより取得された前記指標値ごとに前記指標値の推移を示す推移データを生成する生成ステップと、

前記取得ステップによりリアルタイムで都度取得される時点の前記指標値を、前記生成ステップにより生成された前記推移データから推定される前記指標値の正常値と比較して前記人物が異常状態あるいは非常状態にあるか否かを判定する判定ステップと、

前記判定ステップの判定結果に基づいて、前記入力受付ステップで受け付けた前記本人認証方法で前記人物の認証を行う制御ステップと、を実行させる、

ことを特徴とする。

30

40

【発明の効果】

【0015】

請求項1に記載の発明によれば、ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性を向上させることができる。

【0016】

請求項2に記載の発明によれば、人物が本人であることを高い確率で判定できる。

【0017】

請求項3に記載の発明によれば、人物が認証に適した正常な状態であるかを判定することができる。

50

【 0 0 1 8 】

請求項 4 に記載の発明によれば、取得された健康状態に関する指標値が、本人のものであるかを確認することができる。

【 0 0 1 9 】

請求項 5、6 に記載の発明によれば、GPS 認証を行うことで、ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性をより向上させることができる。

【 0 0 2 0 】

請求項 7、8 に記載の発明によれば、グループ認証を行うことで、ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性をより向上させることができる。

【 0 0 2 1 】

請求項 9 に記載の発明によれば、ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性を向上させることができる。

【 図面の簡単な説明 】

【 0 0 2 2 】

【 図 1 】 第 1 実施形態に係る認証システムの全体構成を示す図である。

【 図 2 】 第 1 実施形態に係る認証システムの機能ブロック図である。

【 図 3 】 第 1 実施形態に係る認証システムにおける認証処理の流れを示すフローチャートである。

【 図 4 】 (a) は認証システムのログイン時に撮影された使用者の画像データの例を示す図、(b) は事前に登録された使用者の顔写真データの例を示す図である。

【 図 5 】 第 2 実施形態に係る認証システムの機能ブロック図である。

【 図 6 】 第 2 実施形態に係る認証システムにおける認証処理の流れを示すフローチャートである。

【 図 7 】 第 3 実施形態に係る認証システムの機能ブロック図である。

【 図 8 】 第 3 実施形態に係る認証システムにおける認証処理の流れを示すフローチャートである。

【 図 9 】 第 4 実施形態に係る認証システムの機能ブロック図である。

【 図 1 0 】 第 4 実施形態に係る認証システムにおける認証処理の流れを示すフローチャートである。

【 図 1 1 】 変形例に係る認証システムの全体構成を示す図である。。

【 発明を実施するための形態 】

【 0 0 2 3 】

次に図面を参照しながら、以下に実施形態及び具体例を挙げ、本発明を更に詳細に説明するが、本発明はこれらの実施形態及び具体例に限定されるものではない。

また、以下の図面を使用した説明において、図面は模式的なものであり、理解の容易のために説明に必要な要素以外の図示は適宜省略されている。

【 0 0 2 4 】

「第 1 実施形態」

(1) 認証システムの構成

図 1 は本実施形態に係る認証システム 1 の全体構成を示す図、図 2 は本実施形態に係る認証システム 1 の機能ブロック図である。

以下、図面を参照しながら本実施形態に係る認証システムについて説明する。

【 0 0 2 5 】

図 1 に示す認証システム 1 は、外部システムに対して、端末装置 1 0 を用いてログインを行う本人認証システムである。そして、認証システム 1 は、特に、振込等の資金移動取引を行ったり、各種ウェブサービスを利用する場合に、より本人認証の安全性を高めた顔画像による生体認証を行うことで、端末装置 1 0 によって安全に取引を行うためのシステムである。本実施形態において、本人認証とは、既に本人確認ができている状態であって、なりすまし等を防ぐための確認をいう。

【 0 0 2 6 】

10

20

30

40

50

認証システム 1 は、端末装置 10 と、測定装置 20 とを備える。端末装置 10 は、例えば、無線通信の基地局（不図示）を介してネットワーク NW に接続可能である。また、測定装置 20 は、ネットワーク NW を介して端末装置 10 と通信可能に接続されている。尚、端末装置 10 は、ネットワーク NW に通信接続することなく、スタンドアローンで動作してもよい。

【0027】

端末装置 10 は、例えば、外部システムによるサービスの提供を受けようとする者（以下、使用者ともいう。）が所持する端末であり、例えば、スマートフォンやタブレットに代表されるコンピュータの機能を併せ持った携帯型の装置に限らず、少なくとも所定のアプリケーションを実装した任意の情報処理装置で、ネットワークを介して他の装置と接続

10

できるものであればよい。

図 2 に示すように、端末装置 10 は、制御部 110 と、記憶部 120 と、カメラ 130 と、操作表示部 140 と、通信部 150 と、を備えている。

【0028】

制御部 110 は、記憶部 120 に記憶されているオペレーティングシステムや各種アプリケーションプログラムを適宜読み出して実行することにより、記憶部 120、カメラ 130、操作表示部 140、通信部 150 と協働し各種機能を実行する。

制御部 110 は、入力受付部 111 と、認証処理部 112 と、判定処理部 115 とを備える。

【0029】

入力受付部 111 は、使用者による取引を行うための各種の入力を受け付ける。

例えば、入力受付部 111 は、インターネットバンキングによる取引を行うために外部システムの一例としての銀行サーバにログインするためのログイン情報の入力を受け付ける。

さらに、入力受付部 111 は、本人認証方法の選択を受け付ける。本人認証方法には、例えば、顔画像による生体認証（顔認証）や、ワンタイムパスワードによる認証等がある。

20

【0030】

認証処理部 112 は、入力受付部 111 が受け付けた認証方法に基づき所定の認証処理を行う。

30

認証処理部 112 は、顔検出部 113 と、顔認証処理部 114 とを備える。顔検出部 113 は、使用者がカメラ 130 を操作して、自身の顔をスキャンした画像データを受け取る。また、顔情報記憶部 122 に記憶した顔検出情報を使用して、受け取った画像データから顔を検出し、検出された顔の領域を示す情報、あるいは検出された顔の特徴を示す情報を顔認証処理部 114 へ出力する。

顔認証処理部 114 は、顔情報記憶部 122 に記憶された顔参照情報を使用して、顔検出部 113 により検出された顔に対して顔認証を実行する。

【0031】

判定処理部 115 は、測定装置 20 から受信した使用者の健康状態に関する指標値（以下、単に指標値と記す）ごとに、その指標値に関する測定値を、経時的な変化を示す一連の測定値からなる測定データとして記憶して指標値の各々の測定データを管理する。例えば、記憶した指標値の各々の測定データを解析することにより使用者の健康状態を判定する。

40

【0032】

判定処理部 115 は、指標値取得部 116 と、推移データ生成部 117 と、指標値判定部 118 とを備える。

指標値取得部 116 は、測定装置 20 から、使用者の健康状態を示す複数の指標値の測定値を通信部 150 を介して取得する。本実施形態において、指標値としては、体温、心拍数などの生体指標があり、測定装置 20 は、通信機能を備えた設置型又は携帯型の測定機器等により構成され、例えば、人の体温を測定する携帯型の体温計、人の心拍数を測定

50

するマイクロ波センサを備えた携帯型の心拍数計によって構成される測定部 2 1 と、ネットワーク NW に接続する通信部 2 2 からなる。

【 0 0 3 3 】

指標値取得部 1 1 6 は、測定装置 2 0 で測定された指標値の測定値を通信部 1 5 0 を介して取得し、取得された指標値の測定値は指標値情報記憶部 1 2 3 に記憶される。

推移データ生成部 1 1 7 は、指標値取得部 1 1 6 から複数の指標値の測定値を受け付けると、これらの測定値を用いて、指標値ごとに測定値の推移を示す推移データを生成する。推移データは、例えば、時間ごと又は日ごとに取得された測定値の変化を示すデータとして生成される。

【 0 0 3 4 】

指標値判定部 1 1 8 は、測定装置 2 0 により測定された複数の指標値の推移データから推定される指標値の正常値と、指標値取得部 1 1 6 が都度取得する時点の測定値とを比較して、使用者が正常状態にあるか否かを判定する。例えば、指標値判定部 1 1 8 は、一つの推移データに示される心拍数の正常値と時点の心拍数の差分、又は各測定値の変化率などのパラメータを求め、そのパラメータの値が予め定められた基準を超えたときに、使用者に異常事態あるいは非常事態が発生していると判定する。

使用者の異常事態あるいは非常事態としては、例えば、脅迫等の行為により無理矢理振込等の資金移動取引を強要される場合が想定される。

【 0 0 3 5 】

記憶部 1 2 0 は、制御部 1 1 0 が各種の処理を実行するために必要なプログラム、データ等を記録するための半導体メモリ素子等の記憶領域であり、プログラム記憶部 1 2 1 と、顔情報記憶部 1 2 2 と、指標値情報記憶部 1 2 3 とを備えている。

【 0 0 3 6 】

プログラム記憶部 1 2 1 は、各種のアプリケーションプログラムを記憶する記憶領域であり、外部システムに対する取引、例えば、銀行取引アプリも記憶している。また、本人確認 API、認証 API とを記憶している。

顔情報記憶部 1 2 2 には、本人認証に用いる顔画像情報が記憶されている。

指標値情報記憶部 1 2 3 は、測定装置 2 0 で測定された複数の指標値の測定値（測定データ）が記憶される。

【 0 0 3 7 】

操作表示部 1 4 0 は、情報を表示する表示部としての機能と、使用者の各種操作入力を行う入力部としての機能とを有する。

【 0 0 3 8 】

通信部 1 5 0 は、ネットワーク NW に接続するための通信インターフェースであり、通信部 1 5 0 を介して各種のサーバ、外部システムと通信が可能である。本実施形態においては、指標値取得部 1 1 6 は、測定装置 2 0 からの使用者の健康状態を示す複数の指標値の測定値を通信部 1 5 0 を介して受信する。

【 0 0 3 9 】

(2) 認証システムの動作

図 3 は認証システム 1 における認証処理の流れを示すフローチャート、図 4 (a) は認証システムのログイン時に撮影された使用者の画像データの例を示す図、(b) は事前に登録された使用者の顔写真データの例を示す図である。

以下、図面を参照しながら本実施形態に係る認証システム 1 の動作について説明する。

【 0 0 4 0 】

端末装置 1 0 の制御部 1 1 0 は、ステップ S 1 0 1 で操作表示部 1 4 0 を介してログインを受け付ける (S 1 0 1) と、ステップ S 1 0 2 でカメラ 1 3 0 が起動して、使用者の顔をスキャンする (S 1 0 2) 。例えば、スキャンした画像データには、図 4 (a) に示すように、使用者の顔を含む画像が写っている。

【 0 0 4 1 】

ステップ S 1 0 2 で画像データを取得すると、ステップ S 1 0 3 で、カメラ 1 3 0 でス

10

20

30

40

50

キャンした画像データP1と顔情報記憶部122に記憶された使用者の顔写真データP2とを比較して同一人物の可能性を例えば一致確率等の数値で得る。

顔認証処理部114は、一例として、それぞれの画像データに写っている顔の眼の位置、鼻の位置、口の位置、眉毛の位置を特定し、次に、眼の形状、鼻の形状、口の形状、眉毛の形状、顔の輪郭などを特定する。

これらの要素がどれだけ共通しているか否かを判定し、顔検出部113で取得された画像データP1(図4(a)参照)が、顔情報記憶部122に記憶された使用者の顔写真データP2(図4(b)参照)とを比べて、同一人物である可能性を一致確率として数値で算出する(S103)。

【0042】

そして、ステップS104では、ステップS103で算出された一致確率が所定値以上であるか判定する(S104)。所定値以上であると判定した場合(S104:Yes)はステップS105へ進み、他方、否であると判定した場合(S104:No)はステップS109へ進み、ログインは許可されない(S109)。

例えば、算出された一致確率の値が「95」であり、事前に登録された所定値が「90」である場合、撮影された使用者が登録使用者であると判定する。

【0043】

ステップS104で一致確率が所定値以上であると判定された場合(S104:Yes)、顔認証された使用者の健康状態を判定するために、ステップS105で、使用者の健康状態に関する指標値の測定値を取得する(S105)。

本実施形態において、使用者の健康状態に関する指標値としては、使用者の心拍数及び体温であり、測定装置20で測定された測定値は、通信部150を介して指標値取得部116で取得される。取得された指標値の測定値は、測定日時と関連付けて指標値情報記憶部123に記憶される。

【0044】

そして、ステップS106では、推移データ生成部117で、取得した指標値の測定値を用いて、指標値毎に測定値の推移を示す推移データを生成する(S106)。生成された推移データは指標値情報記憶部123に記憶される。

【0045】

次に、ステップS107で、現在のリアルタイムで取得される指標値の時点の測定値が、推移データから推定される正常値の範囲内にあるか否かを判定する(S107)。例えば、心拍数について、推移データから推定される心拍数の正常値が「60~90回」であり、時点の測定値が「120回」である場合、測定された使用者は正常状態ではないと判定する。正常状態にない場合としては、犯罪者等に脅されている場合が挙げられる。また、心拍数は、睡眠時は低くなることが知られており、例えば「50回」以下である場合、眠っていると判定される。また、指標値として、体温が、例えば「35度~37度」の範囲にない場合も使用者は正常状態ではないと判断される。

【0046】

ステップS107において、時点の指標値が正常値と判定された場合(S107:Yes)、ステップS108へ進み、ログインが許可される(S108)。他方、否であると判定された場合は(S107:No)ステップS109へ進み、ログインは許可されない(S109)。その後、取得した画像データP1は破棄されて認証処理は終了する(S110)。

【0047】

このようにして得られる本実施形態である認証システム1のプログラムは、使用者の端末装置10のカメラ130を用いて使用者の顔をスキャンして使用者の画像データP1を取得する画像データの取得ステップS102と、カメラ130でスキャンした画像データP1と顔情報記憶部122に記憶された使用者の顔写真データP2とを比較して同一人物である一致確率を数値で得る比較ステップS103、一致確率が所定値以上であるか判定する判定ステップS104と、一致確率が所定値以上である場合に、使用者の健康状態に

10

20

30

40

50

関する指標値の測定値を取得する測定値取得ステップS105と、取得した指標値の測定値を用いて、指標値毎に測定値の推移を示す推移データを生成する推移データ生成ステップS106と、指標値の時点の測定値が、推移データから推定される正常値の範囲内にあるか否かが判定する判定ステップS107と、指標値の時点の測定値が正常値である場合に外部システムへログインを許可するログインステップS108とを備えていることにより、ひとつの認証のみで本人認証を行う場合に比べて、セキュリティレベルを高め認証の安全性を向上させることができる。

【0048】

「第2実施形態」

図5は本実施形態に係る認証システム1Aの機能ブロック図である。

10

本実施形態に係る認証システム1Aは、指紋認証を行う指紋認証手段としての指紋認証処理部を備え、顔認証を行う使用者が正常状態にあると判定される場合であっても、指紋認証により使用者が予め登録された人物であると判定された場合に、顔認証による人物の認証を行う点で、第1実施形態に係る認証システム1と異なっている。したがって、第1実施形態と共通する機能を果たす部分については、同一の符号を付して、その詳細な説明は省略する。

【0049】

(1) 認証システムの構成

認証システム1Aは、端末装置10と、測定装置20とを備える。

図5に示すように、端末装置10は、制御部110Aと、記憶部120Aと、カメラ130と、操作表示部140と、通信部150と、を備えている。

20

【0050】

制御部110Aは、記憶部120Aに記憶されているオペレーティングシステムや各種アプリケーションプログラムを適宜読み出して実行することにより、記憶部120A、カメラ130、操作表示部140、通信部150と協働し各種機能を実行する。

制御部110Aは、入力受付部111と、認証処理部112と、判定処理部115と、指紋認証処理部119とを備える。

【0051】

入力受付部111は、使用者による取引を行うための各種の入力を受け付ける。

さらに、入力受付部111は、本人認証方法の選択を受け付ける。本人認証方法には、例えば、顔画像や指紋による生体認証や、ワンタイムパスワードによる認証等がある。

30

【0052】

認証処理部112は、顔検出部113と、顔認証処理部114とを備え、入力受付部111が受け付けた認証方法に基づき所定の認証処理を行う。

顔検出部113は、使用者がカメラ130を操作して自身の顔をスキャンした画像データを受け取る。また、顔情報記憶部122に記憶した顔検出情報を使用して、受け取った画像データから顔を検出し、検出された顔の領域を示す情報、あるいは検出された顔の特徴を示す情報を顔認証処理部114へ出力する。

顔認証処理部114は、顔情報記憶部122に記憶された顔参照情報を使用して、顔検出部113により検出された顔に対して顔認証を実行する。

40

【0053】

判定処理部115は、測定装置20から受信した使用者の健康状態に関する指標値ごとに、その指標値に関する測定値を、経時的な変化を示す一連の測定値からなる測定データとして記憶して指標値の各々の測定データを管理する。例えば、記憶した指標値の各々の測定データを解析することにより使用者の健康状態を判定する。

【0054】

判定処理部115は、指標値取得部116と、推移データ生成部117と、指標値判定部118とを備える。

指標値取得部116は、測定装置20から、使用者の健康状態を示す複数の指標値の測定値を通信部150を介して取得する。本実施形態において、指標値としては、体温、心

50

拍数などの生体指標があり、測定装置 20 は、例えば、人の体温を測定する携帯型の体温計、人の心拍数を測定するマイクロ波センサを備えた携帯型の心拍数計によって構成される測定部 21 と、ネットワーク NW に接続する通信部 22 からなる。指標値取得部 116 で取得された指標値の測定値は指標値情報記憶部 123 に記憶される。

【0055】

推移データ生成部 117 は、指標値取得部 116 から複数の指標値の測定値を受け付けると、これらの測定値を用いて、指標値ごとに測定値の推移を示す推移データを生成する。

【0056】

指標値判定部 118 は、測定装置 20 により測定された複数の指標値の推移データから推定される指標値の正常値と、指標値取得部 116 が都度取得する時点の測定値とを比較して、使用者が正常状態にあるか否かを判定する。

10

【0057】

指紋認証処理部 119 は、取得した指紋イメージ像と指紋情報記憶部 124 に記憶した使用者の指紋情報との比較を行い、指紋の特徴が一致した場合、端末装置 10 の正当使用者であると判断する。

【0058】

記憶部 120 A は、制御部 110 A が各種の処理を実行するために必要なプログラム、データ等を記録するための半導体メモリ素子等の記憶領域であり、プログラム記憶部 121 と、顔情報記憶部 122 と、指標値情報記憶部 123 と、指紋情報記憶部 124 とを備えている。

20

【0059】

プログラム記憶部 121 は、各種のアプリケーションプログラムを記憶する記憶領域であり、外部システムに対する取引、例えば、銀行取引アプリも記憶している。また、本人確認 API、認証 API とを記憶している。

顔情報記憶部 122 には、本人認証に用いる顔画像情報が記憶されている。

指標値情報記憶部 123 は、測定装置 20 で測定された複数の指標値の測定値（測定データ）が記憶される。

指紋情報記憶部 124 には、使用者の指紋情報が記憶されている。

【0060】

30

操作表示部 140 は、情報を表示する表示部としての機能と、使用者の各種操作入力を行う入力部としての機能とを有し、拡張現実（AR）、仮想現実（VR）、混合現実（MR）による 3次元操作、立体ホログラムによる操作を受け付けるものであってもよい。

【0061】

通信部 150 は、ネットワーク NW に接続するための通信インターフェースであり、通信部 150 を介して各種のサーバ、外部システムと通信が可能である。本実施形態においては、指標値取得部 116 は、測定装置 20 からの使用者の健康状態を示す複数の指標値の測定値を通信部 150 を介して受信する。また、指紋認証処理部 119 は、測定装置 20 から通信部 150 を介して指紋イメージ像を取得してもよい。

【0062】

40

（2）認証システムの動作

図 6 は本実施形態に係る認証システム 1 A における認証処理の流れを示すフローチャートである。

以下、図面を参照しながら本実施形態に係る認証システム 1 A の動作について説明する。

【0063】

端末装置 10 の制御部 110 A は、ステップ S201 で操作表示部 140 を介してログインを受け付ける（S201）と、ステップ S202 でカメラ 130 が起動して、使用者の顔をスキャンする（S202）。

【0064】

50

ステップS 2 0 2で画像データを取得すると、ステップS 2 0 3で、カメラ1 3 0でスキャンした画像データP 1と顔情報記憶部1 2 2に記憶された使用者の顔写真データP 2とを比較して同一人物の可能性を一致確率等の数値で得る。

顔認証処理部1 1 4は、顔検出部1 1 3で取得された画像データP 1が、顔情報記憶部1 2 2に記憶された使用者の顔写真データP 2とを比べて、同一人物である可能性を一致確率として数値で算出する(S 2 0 3)。

【0 0 6 5】

そして、ステップS 2 0 4では、ステップS 2 0 3で算出された一致確率が所定値以上であるか判定する(S 2 0 4)。所定値以上であると判定した場合(S 2 0 4 : Y e s)はステップS 2 0 5へ進み、他方、否であると判定した場合(S 2 0 4 : N o)はステップS 2 1 1へ進む。

10

【0 0 6 6】

ステップS 2 0 4で一致確率が所定値以上であると判定された場合(S 2 0 4 : Y e s)、顔認証された使用者の健康状態を判定するために、ステップS 2 0 5で、使用者の健康状態に関する指標値の測定値を取得する(S 2 0 5)。

そして、ステップS 2 0 6では、推移データ生成部1 1 7で、取得した指標値の測定値を用いて、指標値毎に測定値の推移を示す推移データを生成する(S 2 0 6)。生成された推移データは指標値情報記憶部1 2 3に記憶される。

【0 0 6 7】

次に、ステップS 2 0 7で、現在のリアルタイムで取得される指標値の時点の測定値が、推移データから推定される正常値の範囲内にあるか否か判定する(S 2 0 7)。

20

ステップS 2 0 7において、時点の指標値が正常値と判定された場合(S 2 0 7 : Y e s)、ステップS 2 0 8へ進み、指紋情報を取得する(S 2 0 8)。他方、否と判定された場合(S 2 0 7 : N o)、ステップS 2 1 1へ進み、ログインは許可されない(S 2 1 1)。指紋情報は、端末装置1 0が備える指紋センサ(不図示)によって取得される。なお、測定装置2 0が、例えば、指で酸素飽和量と心拍数を測定するパルスオキシメータである場合、測定装置2 0から指標値の測定値を取得する際に、指紋情報も同時に取得することができる。

【0 0 6 8】

そして、ステップS 2 0 9では、取得した指紋情報と指紋情報記憶部1 2 4に記憶されている使用者の指紋情報と照合して指紋認証を行う(S 2 0 9)。指紋情報が一致する場合(S 2 0 9 : Y e s)には、ステップS 2 1 0へ進み、ログインが許可される(S 2 1 0)。他方、否であると判定した場合は(S 2 0 9 : N o)ステップS 2 1 1へ進み、ログインは許可されない(S 2 1 1)。その後、取得した画像データP 1は破棄されて認証処理は終了する(S 2 1 2)。

30

【0 0 6 9】

このようにして認証システム1 Aは、顔認証を行う使用者が正常状態にあると判定される場合であっても、取得された健康状態に関する指標値が本人のものであるかを指紋認証により確認して顔認証による人物の認証を行うことで、よりセキュリティレベルを高め認証の安全性を向上させることができる。

40

【0 0 7 0】

「第3実施形態」

図7は本実施形態に係る認証システム1 Bの機能ブロック図である。

本実施形態に係る認証システム1 Bは、端末装置1 0自身の場所の判定を行なう場所認証処理部1 0 1を備え、顔認証を行う使用者が正常状態にあると判定される場合であっても、場所認証により端末装置1 0が予め登録された場所の条件に一致すると判定された場合に、顔認証による人物の認証を行う点で、第1実施形態に係る認証システム1と異なっている。したがって、第1実施形態と共通する機能を果たす部分については、同一の符号を付して、その詳細な説明は省略する。

【0 0 7 1】

50

(1) 認証システムの構成

認証システム1Bは、端末装置10と、測定装置20とを備える。

図7に示すように、端末装置10は、制御部110Bと、記憶部120Bと、カメラ130と、操作表示部140と、通信部150と、を備えている。

【0072】

制御部110Bは、入力受付部111と、認証処理部112と、判定処理部115と、場所認証処理部101とを備える。

場所認証処理部101は、受信手段の一例としてのGPS受信部102と、場所判定部103からなる。

【0073】

GPS受信部102は、GPS(Global Positioning System)衛星又は屋内GPSからのGPS電波を受信する。

場所判定部103は、定期的にGPS受信部102で受信したGPS電波に基づき端末装置10の場所情報を算出してこの場所情報を端末装置10の現在場所として、端末装置10の現在場所が、登録場所記憶部125に記憶された予め登録された場所の条件と一致するか比較する。予め登録された場所としては、使用者が認証する場所及び使用者が認証しない場所である。

そして、制御部110Bは、現在場所が予め登録された場所の条件と一致しない場合には、端末装置10が、例えば盗難されたものとみなし、顔認証を行う使用者が正常状態であると判定される場合であっても、ログインを不許可とする。

【0074】

(2) 認証システムの動作

図8は本実施形態に係る認証システム1Bにおける認証処理の流れを示すフローチャートである。

以下、図面を参照しながら本実施形態に係る認証システム1Bの動作について説明する。

【0075】

端末装置10の制御部110Bは、ステップS301で操作表示部140を介してログインを受け付ける(S301)と、ステップS302でカメラ130が起動して、使用者の顔をスキャンする(S302)。

【0076】

ステップS302で画像データを取得すると、ステップS303で、カメラ130で撮影した画像データP1と顔情報記憶部122に記憶された使用者の顔写真データP2とを比較して同一人物の可能性を一致確率等の数値で得る。

顔認証処理部114は、顔検出部113で取得された画像データP1が、顔情報記憶部122に記憶された使用者の顔写真データP2とを比べて、同一人物である可能性を一致確率として数値で算出する(S303)。

【0077】

そして、ステップS304では、ステップS303で算出された一致確率が所定値以上であるか判定する(S304)。所定値以上であると判定した場合(S304:Yes)はステップS305へ進み、他方、否であると判定した場合(S304:No)はステップS311へ進む。

【0078】

ステップS304で一致確率が所定値以上であると判定された場合(S304:Yes)、顔認証された使用者の健康状態を判定するために、ステップS305で、使用者の健康状態に関する指標値の測定値を取得する(S305)。

そして、ステップS306では、推移データ生成部117で、取得した指標値の測定値を用いて、指標値毎に測定値の推移を示す推移データを生成する(S306)。生成された推移データは指標値情報記憶部123に記憶される。

【0079】

10

20

30

40

50

次に、ステップ S 3 0 7 で、現在のリアルタイムで取得される指標値の時点の測定値が、推移データから推定される正常値の範囲内にあるか否か判定する (S 3 0 7)。

ステップ S 3 0 7 において、時点の指標値が正常値と判定された場合 (S 3 0 7 : Y e s)、ステップ S 3 0 8 へ進み、場所情報を取得する (S 3 0 8)。場所情報は、GPS 電波を受信することで取得される。他方、否と判定された場合 (S 3 0 7 : N o)、ログインは許可されない (S 3 1 1)。

【 0 0 8 0 】

そして、ステップ 3 0 9 では、取得した場所情報と登録場所記憶部 1 2 5 に記憶されている場所情報と対比して場所認証を行う (S 3 0 9)。場所情報が一致する場合 (S 3 0 9 : Y e s) には、ステップ S 3 1 0 へ進み、ログインが許可される (S 3 1 0)。他方、否であると判定した場合は (S 3 0 9 : N o) ログインは許可されない (S 3 1 1)。その後、取得した画像データ P 1 は破棄されて (S 3 1 2) 認証処理は終了する。

【 0 0 8 1 】

このようにして認証システム 1 B は、顔認証を行う使用者が正常状態にあると判定される場合であっても、場所認証により端末装置 1 0 が予め登録された場所の条件に一致すると判定された場合に、顔認証による人物の認証を行うことで、よりセキュリティレベルを高め認証の安全性を向上させることができる。

【 0 0 8 2 】

「第 4 実施形態」

図 9 は本実施形態に係る認証システム 1 C の機能ブロック図である。

本実施形態に係る認証システム 1 C は、複数人が認証したグループ認証状態を検出する認証検出手段の一例としてのグループ認証検出部 1 0 4 を備え、顔認証を行う使用者が正常状態にあると判定される場合であっても、グループ認証検出部 1 0 4 で、グループ認証状態が検出された場合に、顔認証による人物の認証を行う点で、第 1 実施形態に係る認証システム 1 と異なっている。したがって、第 1 実施形態と共通する機能を果たす部分については、同一の符号を付して、その詳細な説明は省略する。

【 0 0 8 3 】

(1) 認証システムの構成

認証システム 1 C は、端末装置 1 0 と、測定装置 2 0 とを備える。

図 9 に示すように、端末装置 1 0 は、制御部 1 1 0 C と、記憶部 1 2 0 と、カメラ 1 3 0 と、操作表示部 1 4 0 と、通信部 1 5 0 と、を備えている。

【 0 0 8 4 】

制御部 1 1 0 C は、入力受付部 1 1 1 と、認証処理部 1 1 2 と、判定処理部 1 1 5 と、グループ認証検出部 1 0 4 とを備える。

グループ認証検出部 1 0 4 は、複数の使用者がそれぞれ入力受付部 1 1 1 を介して入力されたユーザ ID 及びパスワードが予め登録された情報と一致してログインが許可されたグループ認証状態を検出する。また、係るログインが所定の時間内に受け付けられて認証されたか検出する。

そして、制御部 1 1 0 C は、グループ認証状態が検出されない場合には、端末装置 1 0 が、例えばなりすましによるものとみなし、顔認証を行う使用者が正常状態にあると判定される場合であっても、ログインを不許可とする。

【 0 0 8 5 】

(2) 認証システムの動作

図 1 0 は本実施形態に係る認証システム 1 C における認証処理の流れを示すフローチャートである。

以下、図面を参照しながら本実施形態に係る認証システム 1 C の動作について説明する。

【 0 0 8 6 】

端末装置 1 0 の制御部 1 1 0 C は、ステップ S 4 0 1 で操作表示部 1 4 0 を介してログインを受け付ける (S 4 0 1) と、ステップ S 4 0 2 でカメラ 1 3 0 が起動して、使用者

の顔をスキャンする（S 4 0 2）。

【0 0 8 7】

ステップS 4 0 2で画像データを取得すると、ステップS 4 0 3で、カメラ1 3 0で撮影した画像データP 1と顔情報記憶部1 2 2に記憶された使用者の顔写真データP 2とを比較して同一人物の可能性を一致確率等の数値で得る。

顔認証処理部1 1 4は、顔検出部1 1 3で取得された画像データP 1が、顔情報記憶部1 2 2に記憶された使用者の顔写真データP 2とを比べて、同一人物である可能性を一致確率として数値で算出する（S 4 0 3）。

【0 0 8 8】

そして、ステップS 4 0 4では、ステップS 4 0 3で算出された一致確率が所定値以上であるか判定する（S 4 0 4）。所定値以上であると判定した場合（S 4 0 4：Y e s）はステップS 4 0 5へ進み、他方、否であると判定した場合（S 4 0 4：N o）はステップS 4 1 1へ進む。

【0 0 8 9】

ステップS 4 0 4で一致確率が所定値以上であると判定された場合（S 4 0 4：Y e s）、顔認証された使用者の健康状態を判定するために、ステップS 4 0 5で、使用者の健康状態に関する指標値の測定値を取得する（S 4 0 5）。

そして、ステップS 4 0 6では、推移データ生成部1 1 7で、取得した指標値の測定値を用いて、指標値毎に測定値の推移を示す推移データを生成する（S 4 0 6）。生成された推移データは指標値情報記憶部1 2 3に記憶される。

【0 0 9 0】

次に、ステップS 4 0 7で、現在のリアルタイムで取得される指標値の時点の測定値が、推移データから推定される正常値の範囲内にあるか否か判定する（S 4 0 7）。

ステップS 4 0 7において、時点の指標値が正常値と判定された場合（S 4 0 7：Y e s）、ステップS 4 0 8へ進み、グループ認証状態を検出する（S 4 0 8）。他方、否と判定された場合（S 4 0 7：N o）、ステップS 4 1 1に進み、ログインは許可されない（S 4 1 1）。

【0 0 9 1】

そして、ステップ4 0 9では、グループ認証状態であるか否か判定する（S 4 0 9）。また、所定の時間内にグループ認証が成立したかを更に判定してもよい。グループ認証状態である場合（S 4 0 9：Y e s）には、ステップS 4 1 0へ進み、ログインが許可される（S 4 1 0）。他方、否であると判定した場合は（S 4 0 9：N o）ログインは許可されない（S 4 1 1）。その後、取得した画像データP 1は破棄されて（S 4 1 2）認証処理は終了する。

【0 0 9 2】

このようにして認証システム1 Cは、顔認証を行う使用者が正常状態にあると判定される場合であっても、グループ認証状態であると判定された場合に、顔認証による人物の認証を行うことで、よりセキュリティレベルを高め認証の安全性を向上させることができる。

【0 0 9 3】

「変形例」

図1 1は変形例に係る認証システム1の全体構成を示す図である。

各実施形態においては、認証システム1、1 A、1 B、1 Cは、端末装置1 0が、顔認証処理、判定処理、指認証処理、場所認証処理、グループ認証状態検出を行うとして説明したが、図1 1に示すように、ネットワークNWに認証サーバ3 0を接続して、認証処理、判定処理、指紋認証、場所認証処理、グループ認証状態検出の一部を認証サーバ3 0で行ってもよい。具体的には、指標値取得機能、推移データ生成機能を認証サーバ3 0におき、測定装置2 0で測定された複数の指標値の測定値（測定データ）を認証サーバ3 0で受信し、指標値ごとに測定値の推移を示す推移データを生成する。生成された推移データは、認証サーバ3 0に記憶される。

10

20

30

40

50

端末装置 10 は、通信部 150 を介して、推移データを取得して推移データから推定される指標値の正常値と、認証サーバ 30 が都度取得する時点の測定値とを比較して、使用者が正常状態にあるか否かを判定する。これにより、端末装置 10 の機能を軽減することができる。

【符号の説明】

【0094】

1、1A、1B、1C・・・認証システム

10・・・端末装置

110、110A、110B、110C・・・制御部

101・・・場所認証処理部、104・・・グループ認証検出部、112・・・認証処理部、115・・・判定処理部、119・・・指紋認証処理部 10

120、120A、120B・・・記憶部

130・・・カメラ

140・・・操作表示部

150・・・通信部

20・・・測定装置

30・・・認証サーバ

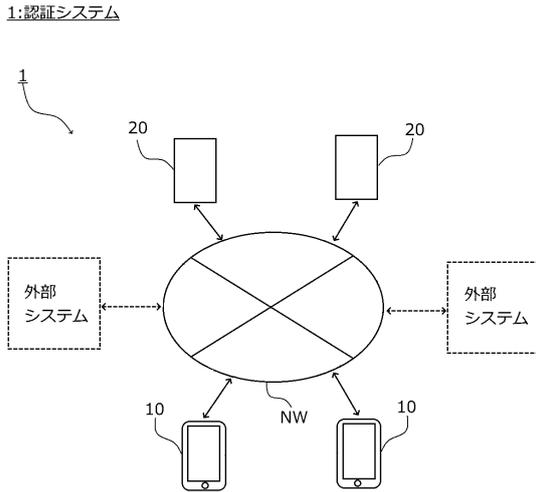
【要約】 (修正有)

【課題】ひとつの認証のみで本人認証を行う場合に比べて、認証の安全性を向上させる認証システム及びプログラムを提供する。 20

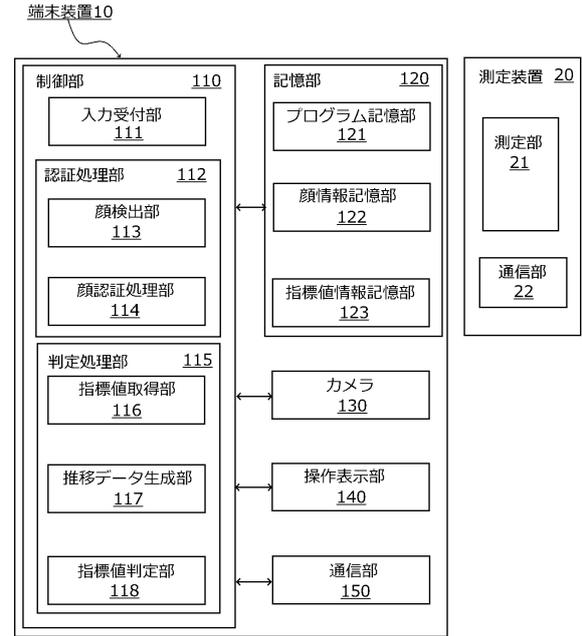
【解決手段】複数の測定装置 20 が、ネットワークを介して複数の端末装置 10 と通信可能に接続されている認証システムにおいて、端末装置 10 は、人物の認証処理を実行する認証処理部 112 と、人物の健康状態に関する指標値を取得する指標値取得部 116 と、指標値取得部 116 により取得された指標値の推移を示す推移データを生成する推移データ生成部 117 と、指標値取得部 116 により取得された指標値が正常であるか否かを、推移データ生成部 117 により生成された推移データに基づいて判定する指標値判定部 118 と、指標値判定部 118 の判定結果に基づいて、認証処理部 112 で人物の認証を行う制御部 110 と、を備える。

【選択図】図 2

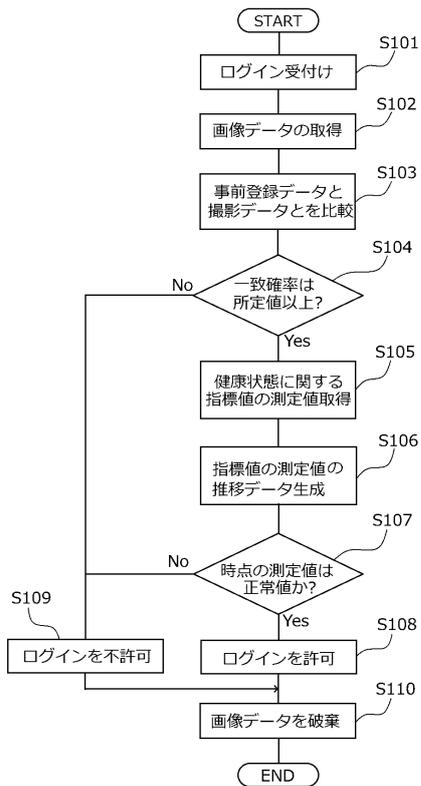
【図1】



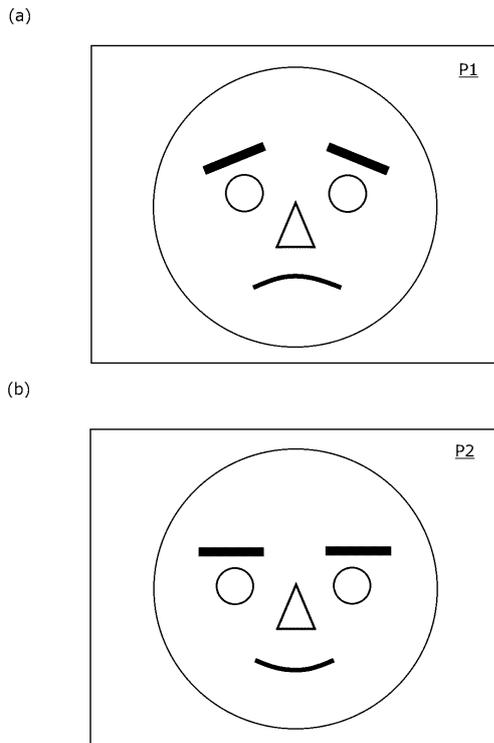
【図2】



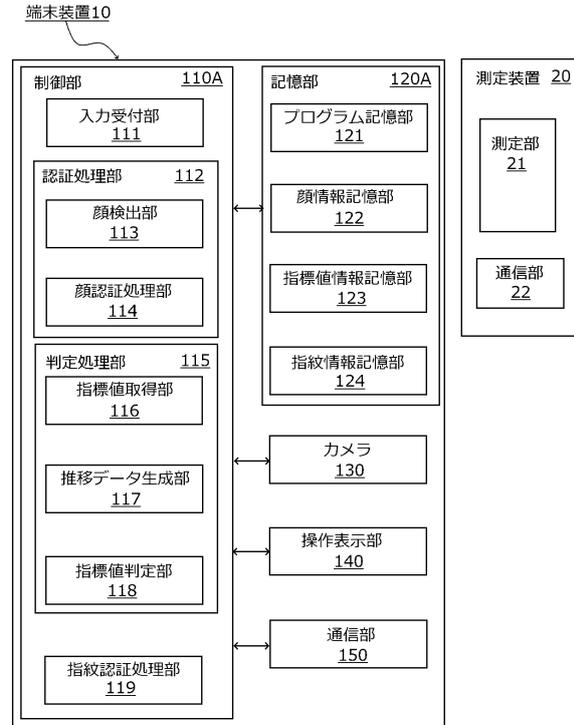
【図3】



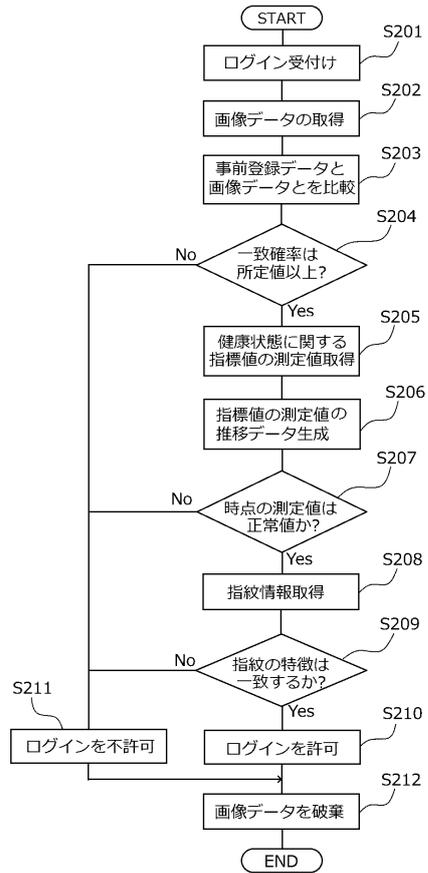
【図4】



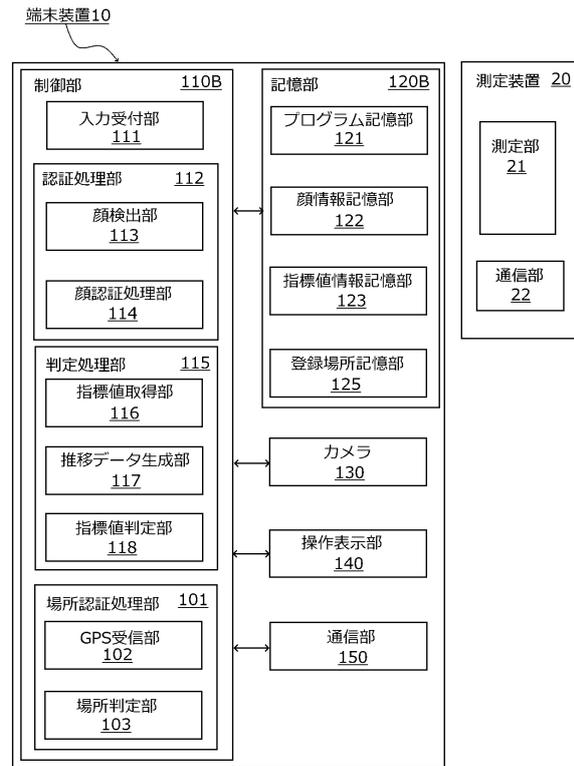
【図5】



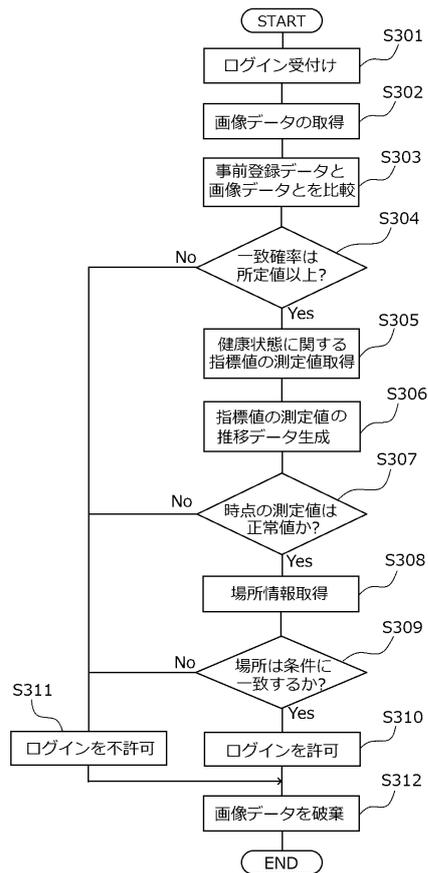
【図6】



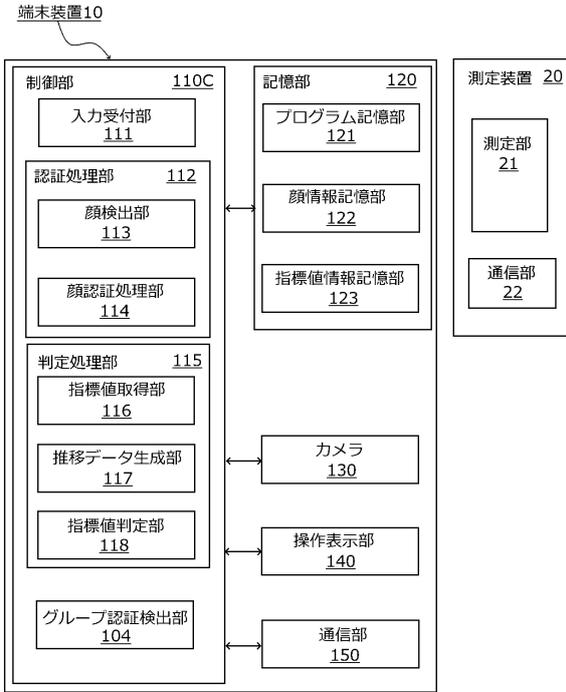
【図7】



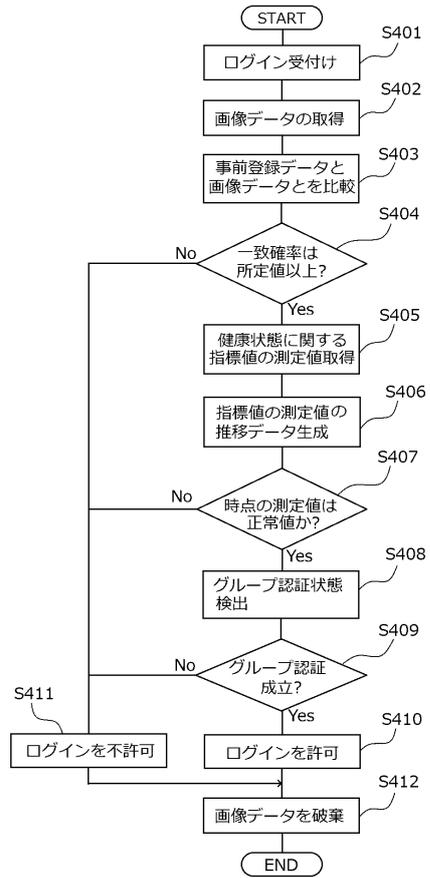
【図8】



【図 9】

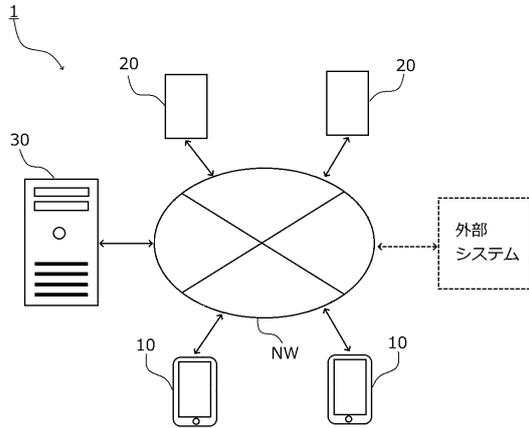


【図 10】



【図 11】

1:認証システム



フロントページの続き

(56)参考文献 特表2013-534652(JP,A)
特開2012-203757(JP,A)
特開2006-336364(JP,A)
特開2010-213326(JP,A)
特表2018-511890(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/32

A61B 5/00