

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6979135号
(P6979135)

(45) 発行日 令和3年12月8日(2021.12.8)

(24) 登録日 令和3年11月16日(2021.11.16)

(51) Int.Cl. F I
G O 6 F 21/31 (2013.01) G O 6 F 21/31

請求項の数 6 (全 20 頁)

(21) 出願番号	特願2020-547230 (P2020-547230)	(73) 特許権者	512000857
(86) (22) 出願日	令和2年2月6日(2020.2.6)		徳山 真旭
(86) 国際出願番号	PCT/JP2020/004582		東京都文京区本駒込4-49-6
(87) 国際公開番号	W02021/019807	(74) 代理人	100095407
(87) 国際公開日	令和3年2月4日(2021.2.4)		弁理士 木村 満
審査請求日	令和2年9月9日(2020.9.9)	(74) 代理人	100132883
(31) 優先権主張番号	特願2019-141648 (P2019-141648)		弁理士 森川 泰司
(32) 優先日	令和1年7月31日(2019.7.31)	(74) 代理人	100148633
(33) 優先権主張国・地域又は機関	日本国(JP)		弁理士 桜田 圭
		(74) 代理人	100147924
			弁理士 美恵 英樹
		(74) 代理人	100201352
			弁理士 豊田 朝子
		(72) 発明者	徳山 真旭
			東京都文京区千駄木3-28-9 9F
			最終頁に続く

(54) 【発明の名称】 端末装置、情報処理方法、及びプログラム

(57) 【特許請求の範囲】

【請求項1】

複数の認証情報を取得する認証用情報取得部と、
前記認証用情報取得部で取得した複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定する認証判定部と、
前記認証判定部で認証が成功したと判定した場合に、前記認証用情報取得部で取得した複数の認証情報により、保存されている複数の認証情報を更新する認証用情報更新部とを備え、
前記認証判定部は、バックグラウンドにおいて、前記認証用情報取得部で取得した一の認証情報が予め定められた認証閾値を下回る場合に認証が成功したと判定し、前記一の認証情報が前記認証閾値以上、且つ、予め定められた認証許容値以下の場合に、前記認証用情報取得部で取得した二の認証情報に基づいて認証が成功したか否かを判定し、前記二の認証情報に基づく認証の結果に応じて、認証間隔の時間を変更する、

端末装置。

【請求項2】

前記認証判定部は、さらに、前記一の認証情報が前記認証許容値以上、または、前記二の認証情報に基づく認証を失敗と判定した場合に、前記認証用情報取得部で取得した三の認証情報に基づいて認証が成功したか否かを判定する、

請求項1に記載の端末装置。

【請求項3】

前記端末装置は、端末装置の傾きの角度を検出する傾き検出部を備え、

前記認証判定部は、ユーザが前記端末装置を使用している状態で、前記傾き検出部で検出された端末装置の角度が、保存されている角度と異なる場合、または、前記認証間隔の時間が経過した場合、前記認証用情報取得部で取得した複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定する、

請求項 1 または 2 に記載の端末装置。

【請求項 4】

複数の認証情報を取得する認証用情報取得部と、

自身の傾きの角度を検出する傾き検出部と、

前記認証用情報取得部で取得した複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定する認証判定部と、

10

前記認証判定部で認証が成功したと判定した場合に、前記認証用情報取得部で取得した複数の認証情報により、保存されている複数の認証情報を更新する認証用情報更新部とを備え、

前記認証判定部は、ユーザが自身を使用している状態で、前記傾き検出部で検出された自身の角度が、保存されている角度と異なる場合、または、予め定められた認証間隔の時間が経過した場合、バックグラウンドにおいて、前記認証用情報取得部で取得した一の認証情報が予め定められた認証閾値を下回る場合に認証が成功したと判定し、前記一の認証情報が前記認証閾値以上、且つ、予め定められた認証許容値以下の場合に、前記認証用情報取得部で取得した二の認証情報に基づいて認証が成功したか否かを判定する、

20

端末装置。

【請求項 5】

端末装置において実行される情報処理方法であって、

複数の認証情報を取得し、

取得した前記複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定し、

前記認証が成功したと判定された場合に、取得した前記複数の認証情報により、保存されている複数の認証情報を更新し、

バックグラウンドにおいて、取得した一の認証情報が予め定められた認証閾値を下回る場合に認証が成功したと判定し、前記一の認証情報が前記認証閾値以上、且つ、予め定められた認証許容値以下の場合に、取得した二の認証情報に基づいて認証が成功したか否かを判定し、前記二の認証情報に基づく認証の結果に応じて、認証間隔の時間を変更する、

30

情報処理方法。

【請求項 6】

コンピュータに、

複数の認証情報を取得する処理、

取得した前記複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定する処理、

前記認証が成功したと判定された場合に、取得した前記複数の認証情報により、保存されている複数の認証情報を更新する処理、

40

バックグラウンドにおいて、取得した一の認証情報が予め定められた認証閾値を下回る場合に認証が成功したと判定し、前記一の認証情報が前記認証閾値以上、且つ、予め定められた認証許容値以下の場合に、取得した二の認証情報に基づいて認証が成功したか否かを判定し、前記二の認証情報に基づく認証の結果に応じて、認証間隔の時間を変更する処理、

を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、端末装置、情報処理方法、及びプログラムに関する。

50

【背景技術】

【0002】

通常、端末装置は、不正使用を防止するための認証機能を備え、認証が成功した場合に各機能を使用可能としている。認証処理には、一般的なパスワードに加え、各種の生体情報等も活用されている。しかし、生体情報は、誤認識が多く、正当な使用者を認証できない場合が生じる。そこで、例えば特許文献1には、1つの生体情報による認証ができなかった場合に、複数の生体情報を複合して認証したり、生体情報とログイン専用ICカード、暗証番号等の非生体情報とを複合して認証する技術が開示されている。

【先行技術文献】

【特許文献】

10

【0003】

【特許文献1】特開2016-040684号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

特許文献1に開示された技術では、認証できなかった場合、認証処理に用いられる複数の生体情報及び複数の非生体情報をそれぞれ、順番に使用者が入力している。例えば、指紋認証ができなかった場合、静脈認証、ログイン専用ICカードによるログイン、暗証番号の入力等を順番に入力することになる。このため、認証における使用者の操作負担が大きいという課題がある。

20

【0005】

本発明は上述の課題を解決するものであり、認証における使用者の操作負担を軽減することができる端末装置、情報処理方法、及び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】

【0006】

上記の目的を達するため、本発明に係る端末装置は、複数の認証情報を取得する認証用情報取得部と、認証用情報取得部で取得した複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定する認証判定部と、認証判定部で認証が成功したと判定した場合に、認証用情報取得部で取得した複数の認証情報により、保存されている複数の認証情報を更新する認証用情報更新部とを備える。認証判定部は、バックグラウンドにおいて、認証用情報取得部で取得した一の認証情報が予め定められた認証閾値を下回る場合に認証が成功したと判定し、一の認証情報が認証閾値以上、且つ、予め定められた認証許容値以下の場合に、認証用情報取得部で取得した二の認証情報に基づいて認証が成功したか否かを判定し、二の認証情報に基づく認証の結果に応じて、認証間隔の時間を変更する。

30

【発明の効果】

【0007】

本発明に係る端末装置によれば、バックグラウンドにおいて、取得した複数の認証情報のうち少なくとも一つの認証情報または複数の認証情報に基づいて、認証が成功したか否かを判定することができるので、認証における使用者の操作負担を軽減することができる。

40

【図面の簡単な説明】

【0008】

【図1】本発明の実施の形態に係る端末装置の正面図

【図2】図1に示す端末装置のブロック図

【図3】図1に示す端末装置のハードウェア構成の一例を示す図

【図4】図1に示す端末装置の情報処理ブロックの図

【図5A】図4に示す端末装置から取得する認証用生体情報データベースのテーブルを示す図

【図5B】図4に示す端末装置から取得する認証用振舞情報データベースのテーブルを示す図

50

す図

【図5C】図4に示す端末装置の傾き情報テーブルを示す図

【図6A】実施の形態に係る認証処理のフローチャート

【図6B】図6Aに示す認証処理のフローチャートの続きのフローチャート

【発明を実施するための形態】

【0009】

以下に、本発明を実施するための形態に係る端末装置、情報処理方法、及びプログラムについて、図面を参照して詳細に説明する。なお、図中同一または相当する部分には同一符号を付す。

【0010】

本実施の形態に係る端末装置1は、ユーザ本人の顔の画像、指紋、声紋等の生体情報と、ユーザが端末装置1を操作する際の特有の挙動、操作状態等による振舞情報とに基づいて、ユーザ本人を認証し、端末装置1における各種機能を実行することができるようにした装置である。端末装置1において行われるユーザの認証処理は、端末装置1の稼働中、バックグラウンドで実行されるとともに、ユーザの生体情報と振舞情報とを更新していくことにより、認証の制度を向上させることができる処理である。

【0011】

端末装置1の正面図を、図1に示す。端末装置1は、いわゆるスマートフォンであり端末装置1は、正面にユーザの顔を撮影するインカメラ11Aと、スピーカ12Aと、通話用のマイクであるマイクロフォン12Bと、端末装置1の傾きを検出する傾き検出部13と、操作入力部14及び表示部19を兼ねるタッチパネルと、ユーザの指紋を検出する左指紋センサ15A及び右指紋センサ15Bと、端末装置1の現在位置を検出する位置検出部16とを備える。また、端末装置1は、背面に、ユーザから見た人間、風景、物体等を撮影することができるメインカメラ11Bを備える。

【0012】

ここで、以下では、インカメラ11Aとメインカメラ11Bとを総称して、撮影部11と称する。以下では、スピーカ12Aと、通話用のマイクであるマイクロフォン12Bとを総称して、音声入出力部12と称する。また、以下では、左指紋センサ15A及び右指紋センサ15Bを総称して、指紋検出部15と称する。

【0013】

図2は、端末装置1の構成を示すブロック図である。端末装置1は、通信部10と、撮影部11と、音声入出力部12と、傾き検出部13と、操作入力部14と、指紋検出部15と、位置検出部16と、端末記憶部17と、端末制御部18と、表示部19とを備える。

【0014】

通信部10は、図示せぬ通信網を介して外部のサーバ、クラウド等と通信し、各種データの送受信をするデータ通信部と、図示せぬ基地局との間で、電話通信用の無線信号を送受信する音声通信部とを含む。データ通信部は、無線LAN(Local Area Network)、Wi-fi(登録商標)、Bluetooth(登録商標)等を用いて構成することができる。また、音声通信部は、基地局との間で、電話通信用の無線信号を送受信する通信機器を用いて構成することができる。

【0015】

撮影部11は、図1に示したインカメラ11Aとメインカメラ11Bとを含む。撮影部11には、CCD(Charge Coupled Device)、CMOS(Complementary Metal Oxide Semiconductor)イメージセンサ等の撮像素子を用いたカメラ、ビデオカメラ等、静止画または動画を撮影し、撮影した静止画または動画を取得することが可能な各種カメラを用いることができる。

【0016】

音声入出力部12は、図1に示したスピーカ12Aと、マイクロフォン12Bとを含む。スピーカ12Aは、音声通話で受信した音声、通信網を介して外部から取得した音楽デ

10

20

30

40

50

ータ等を入力する。マイクロフォン 12B は、ユーザの音声をピックアップする装置である。

【0017】

傾き検出部 13 は、端末装置 1 の傾き、揺れ等を検出することができる装置である。傾き検出部 13 は、加速度センサ、角度センサ、地磁気を検出する磁気センサ等の端末装置 1 の傾きを検出できる各種センサを用いて構成することができる。なお、傾き検出部 13 を構成するセンサの個数及び種類は、単数又は複数のどちらでもよい。

【0018】

操作入力部 14 は、図 1 に示したユーザからの操作を入力することができる装置である。指紋検出部 15 は、ユーザの指紋を検出するセンサである。指紋検出部 15 は、図 1 に示した左指紋センサ 15A 及び右指紋センサ 15B を含む。なお、指紋検出部 15 には、指紋センサに限らず、ユーザの指紋を検出することができるセンサ、機器等であれば、いずれのものを用いてもよい。

10

【0019】

位置検出部 16 は、端末装置 1 の現在位置を検出することができる装置である。位置検出部 16 は、GPS (Global Positioning System) 等の、端末装置 1 の現在位置を検出することができる機器を用いて構成することができる。

【0020】

端末記憶部 17 は、ユーザの認証処理を行うための認証処理プログラム 170 と、端末装置 1 で取得したユーザの生体情報をまとめた認証用生体情報データベース 171 と、端末装置 1 で取得したユーザの振舞情報をまとめた認証用振舞情報データベース 172 と、端末装置 1 の傾き状態を記憶するための傾き情報テーブル 173 とを備える。また、端末記憶部 17 には、端末装置 1 で実行される各種アプリケーションのプログラムが記憶されている。

20

【0021】

認証処理プログラム 170 は、端末装置 1 で取得したユーザの生体情報及び振舞情報に基づいてユーザを認証する処理を行うプログラムである。認証用生体情報データベース 171 は、ユーザの生体情報に関する情報と認証に用いる認証値とを保存するためのデータベースである。

【0022】

認証用振舞情報データベース 172 は、端末装置 1 を操作する際のユーザ特有の振舞に関する情報、認証の合格条件等を保存するためのデータベースである。ここで、ユーザ特有の振舞とは、ユーザが端末装置 1 を操作する際の挙動、表示部 19 の画面とユーザの顔の距離、キーストローク、持ち方、端末装置 1 が使用される位置、特定の通信網への接続回数、特定のアプリケーションの起動、操作等、ユーザ固有のものをいう。

30

【0023】

傾き情報テーブル 173 は、傾き検出部 13 により検出された端末装置 1 の傾き角度と、取得日時、取得のための待機時間を記憶するためのテーブルである。なお、認証処理プログラム 170 と、認証用生体情報データベース 171 と、認証用振舞情報データベース 172 と、傾き情報テーブル 173 とについては、その詳細を後述する。

40

【0024】

端末制御部 18 は、端末記憶部 17 に記憶された各種プログラムを実行する。また、端末制御部 18 は、通信部 10 と、撮影部 11 と、音声入出力部 12 と、傾き検出部 13 と、操作入力部 14 と、指紋検出部 15 と、位置検出部 16 とから各種データを取得して処理し、端末記憶部 17 の各種データベース、テーブルに記憶する。また、端末制御部 18 は、撮影部 11 に撮影する指示を送信することで、任意のタイミングで撮影部 11 に撮影をさせることができる。

【0025】

表示部 19 は、端末制御部 18 で実行される各種プログラムの処理内容を表示する。また、表示部 19 は、撮影部 11 で撮影された静止画、動画等の画像、操作入力部 14 から

50

入力されたデータ等を表示することもできる。表示部 19 は、操作入力部 14 上に積層されており、図 1 に示したタッチパネルを構成する。

【0026】

次に、端末装置 1 のハードウェア構成の一例を、図 3 を参照しつつ説明する。端末装置 1 は、各種プログラムを実行するプロセッサ 21 と、各種プログラムを展開するためのメモリ 22 と、各種表示用データを出力する表示コントローラ 23 と、各種表示用データを表示する表示機器 24 と、撮影部 11、音声入出力部 12 等を接続するための I/O ポート 25 と、各種プログラム及び各種データを記憶する記憶機器 26 と、外部と通信し各種データを送受信する通信機器 27 とを備える。このプロセッサ 21 と、メモリ 22 と、表示コントローラ 23 と、表示機器 24 と、I/O ポート 25 と、記憶機器 26 と、通信機器 27 とは、データバス 28 を介して相互に接続されている。

10

【0027】

プロセッサ 21 は、記憶機器 26 に記憶された各種プログラムを読み出してメモリ 22 に展開し、実行する。プロセッサ 21 は、CPU (Central Processing Unit)、MPU (Micro-processing Unit) 等の処理装置を用いて構成することができる。また、メモリ 22 は、RAM (Random Access Memory)、フラッシュメモリ等の揮発性または不揮発性の半導体メモリといった記憶素子および記憶媒体を用いて構成することができる。

【0028】

表示コントローラ 23 は、表示機器 24 に各種表示用データを出力するコントローラである。表示コントローラ 23 は、ビデオカード、GPU (Graphics Processing Unit)、グラフィックボード等の映像信号出力装置を用いて構成することができる。また、表示機器 24 は、LCD (Liquid Crystal Display)、有機 EL (Electroluminescence) モニタ等の表示装置を用いて構成することができる。

20

【0029】

I/O ポート 25 は、撮影部 11 と、音声入出力部 12 と、傾き検出部 13 と、操作入力部 14 と、指紋検出部 15 と、位置検出部 16 とを接続することができる接続用ポートである。I/O ポート 25 には、USB (Universal Serial Bus) ポート、IEEE 1394 ポート等、機器を接続可能な各種ポートを用いて構成することができる。

30

【0030】

記憶機器 26 は、プロセッサ 21 で実行する各種プログラム、各種プログラムで使用するための各種データを記憶する機器である。記憶機器 26 は、HDD (Hard Disk Drive)、SSD (Solid State Drive) 等の記憶装置を用いて構成することができる。

【0031】

通信機器 27 は、図示せぬ通信網を介して外部のサーバ、クラウド等と通信し、各種データの送受信をするデータ通信部と、図示せぬ基地局との間で、電話通信用の無線信号を送受信する音声通信部とを含む。データ通信部は、無線 LAN、Wi-Fi (登録商標)、Bluetooth (登録商標) 等を用いて構成することができる。また、音声通信部は、基地局との間で、電話通信用の無線信号を送受信する通信機器を用いて構成することができる。

40

【0032】

上述のプロセッサ 21 により、図 2 に示した端末装置 1 の端末記憶部 17 に記憶された認証処理プログラム 170 を実行することにより、端末制御部 18 に図 4 に示す情報処理ブロックが実現される。これにより、端末装置 1 は、ユーザ本人の顔の画像、指紋、声紋等の生体情報と、ユーザが端末装置 1 を操作する際の特有の挙動、操作状態等による振舞情報とに基づいて、ユーザ本人を認証し、端末装置 1 における各種機能を実行することができる。

50

【 0 0 3 3 】

情報処理ブロックは、通信部 1 0、撮影部 1 1 等から認証用の生体情報及び振舞情報を取得する認証用情報取得部 1 8 1 と、ユーザを本人か否か認証する認証判定部 1 8 2 と、表示部 1 9 に認証結果を表示させる認証結果表示部 1 8 3 と、認証判定部 1 8 2 からの指示により端末記憶部 1 7 に記憶される各種データベース及びテーブルの情報を更新する認証用情報更新部 1 8 4 とを備える。

【 0 0 3 4 】

認証用情報取得部 1 8 1 は、通信部 1 0、撮影部 1 1 等から認証用の生体情報及び振舞情報を取得する。認証判定部 1 8 2 は、認証用情報取得部 1 8 1 から取得した認証用の生体情報及び振舞情報と、端末記憶部 1 7 の各種データベースに記憶された認証値、合格条件等に基づいて、ユーザの認証を行う。認証結果表示部 1 8 3 は、認証判定部 1 8 2 からユーザの認証結果を受信し、表示部 1 9 に認証結果に応じてメッセージ、画像等を表示させる。認証用情報更新部 1 8 4 は、認証判定部 1 8 2 からの指示に基づいて、端末記憶部 1 7 に記憶された各種データベース、テーブルに記憶されたデータを更新する。なお、認証用情報取得部 1 8 1 で取得される生体情報及び振舞情報は、請求の範囲における認証情報の一例である。また、認証用情報取得部 1 8 1 で取得される各生体情報は、請求の範囲における一の情報及び三の情報の一例である。認証用情報取得部 1 8 1 で取得される各振舞情報は、請求の範囲における二の情報の一例である。

【 0 0 3 5 】

次に、端末記憶部 1 7 に記憶される認証用生体情報データベース 1 7 1 と、認証用振舞情報データベース 1 7 2 と、傾き情報テーブル 1 7 3 との各テーブルの構成について、図 5 A から図 5 C を参照しつつ以下に説明する。まず、認証用生体情報データベース 1 7 1 のテーブルには、図 5 A に示すように、顔、音声等の生体情報の種類と、ユーザ本人の生体情報である登録情報と、登録情報と図 4 に示した認証用情報取得部 1 8 1 で取得した生体情報とを比較して求める認証値が記憶されている。認証用生体情報データベース 1 7 1 のテーブルに記憶されている登録情報は、ユーザ本人の生体情報である。登録情報には、端末装置 1 で認証処理を行う前に予め登録された情報であり、ユーザ本人を認証できた場合に更新される。登録情報には、例えば、生体情報の種類が顔であれば顔画像から求めた特徴量が、生体情報の種類が音声であれば音声データまたは音声データから求めた特徴量または音声データとその特徴量の両方が、生体情報の種類が虹彩であれば虹彩データが、生体情報の種類が指紋であれば指紋の画像から求めた特徴量が、それぞれ記憶されている。

【 0 0 3 6 】

本実施の形態において、生体情報の類似の判定は、認証値により行われる。認証値は、登録情報と、図 4 に示した認証用情報取得部 1 8 1 で取得した生体情報とを比較した結果を基に求められる値である。認証値は、登録情報と認証用情報取得部 1 8 1 で取得した生体情報とが類似する場合に 0 に近づき、類似しない場合に 1 に近づく。認証用生体情報データベース 1 7 1 には、認証値の平均値と、認証値を判定するための閾値である認証閾値と、認証閾値にユーザがグレーな場合を示す認証許容範囲値を含めた認証許容値とが含まれる。

【 0 0 3 7 】

まず、認証値の平均値は、登録情報と、認証用情報取得部 1 8 1 で取得した生体情報とを比較し求められた認証値の平均の値である。認証閾値は、登録情報と、認証用情報取得部 1 8 1 で取得した生体情報とを比較し、比較した結果を基に求められた認証値が、この値以下の場合、ユーザをユーザ本人と判定するための基準となる値である。認証閾値は、ユーザの認証の状況に合わせて変動する値であり、予め上限値が定められている。上限値は、その値以上となった場合、ユーザをユーザ本人と生体情報のみで認証すべきではないとされる値である。例えば、認証閾値のデフォルト値を、登録情報と認証用情報取得部 1 8 1 で取得した生体情報とが類似する場合に近づく認証値 0 と類似しない場合に近づく認証値 1 との間の 0 . 4 とする。この場合、認証閾値の上限値は、認証閾値のデフォルト値

10

20

30

40

50

に、類似する場合に近づく認証値 0 と、類似しない場合に近づく認証値 1 との一割の半分である 0.5 を加えた値、すなわち、0.45 とする。

【0038】

また、認証許容値は、登録情報と認証用情報取得部 181 で取得した生体情報とを比較し、比較した結果を基に求められた認証値が、この値以上の場合、ユーザをユーザ本人ではないと判定するための基準となる値である。認証許容値は、上述のとおり認証閾値にユーザがグレーな場合を示す認証許容範囲値を含めた値である。このため、認証許容値は、認証閾値と認証許容範囲値との変動に応じて、変動する値である。認証許容値には、予め上限値が定められており、これを最大認証許容値と呼ぶ。最大認証許容値は、この値以上の場合、ユーザを他人と判断すべきとされる値である。例えば、最大認証許容値は、登録情報と認証用情報取得部 181 で取得した生体情報とが類似する場合に近づく認証値 0 と、類似しない場合に近づく認証値 1 との中間の 0.5 とする。

10

【0039】

認証閾値と認証許容値との間の値を認証許容範囲値という。認証許容範囲値は、ユーザがユーザ本人か否かがグレーな場合を示す値である。認証値が認証許容範囲値内である場合、ユーザがユーザ本人か否かを生体情報だけで判断せず、ユーザ特有の振舞情報を含めて判断する。具体的には、認証値が認証許容範囲値内である場合、ユーザ特有の振舞情報が合格条件に合致している場合に、ユーザ本人と認証する。また、認証値が認証許容範囲値内である場合、ユーザ特有の振舞情報が合格条件に合致していない場合に、ユーザ本人と認証しないものとする。振舞情報によるユーザの認証を、以下では、補助認証と称する。認証許容範囲値は、この範囲に収まる認証値であればユーザ本人として概ね考えても良いと思われる値を、予め定めたものである。認証許容範囲値は、例えば、登録情報と認証用情報取得部 181 で取得した生体情報とが類似する場合に近づく認証値 0 と、類似しない場合に近づく認証値 1 との一割以下の 0.08 とする。なお、認証閾値が上限値になった場合、認証許容範囲値は、最大認証許容値から認証閾値の上限値を引いた値とする。例えば、認証閾値の上限値を 0.45 とし、最大認証許容値を 0.5 とした場合、認証許容範囲値は 0.05 となる。したがって、認証閾値が上限値になっている場合、認証許容範囲値の値は、認証閾値が上限値になっていない場合よりも小さな値をとる。

20

【0040】

次に、認証用振舞情報データベース 172 のテーブルについて、図 5B を参照しつつ、以下に説明する。認証用振舞情報データベース 172 のテーブルには、通信接続、イベント実行等のユーザの振舞の種類と、図 4 に示した認証用情報取得部 181 で取得した取得情報と、各振舞における最新状況と、各振舞の合格条件とが記憶されている。取得情報には、例えば、振舞の種類が通信接続であれば接続先のアドレス、SSID (Service Set Identifier)、BSSID (Basic Service Set Identifier) 等が、振舞の種類がイベント実行であれば予めスケジュール帳に保存されたイベントの行われる場所の名称、住所等の場所情報が、振舞の種類が顔と端末装置との距離であれば距離が、デバイス接続であれば接続先のデバイスを示す名称、ID (Identifier) 等が、それぞれ記憶されている。

30

【0041】

各振舞における最新状況は、例えば、振舞の種類が通信接続であれば、取得情報に示された通信接続先にこれまで接続等された合計回数である。通信接続先への接続等の合計回数は、初期値が 0 であり、通信接続先への接続等により回数が加算されていく。また、振舞の種類がイベント実行であれば、取得情報に記憶されている場所とユーザの現在地との間の距離が記憶される。振舞の種類が顔と端末装置 1 との距離であれば、それまでユーザがユーザ本人と認証された際に算出された顔と端末装置 1 との距離の平均距離が記憶される。顔と端末装置 1 との平均距離は、ユーザがユーザ本人と認証される度に更新される。なお、顔と端末装置 1 との平均距離の初期値は、図 5A に示した生体情報を、端末装置 1 でユーザ本人の認証を行う前に予め登録する際に求められた距離とする。

40

【0042】

50

また、振舞の種類がデバイス接続であれば、取得情報に記憶された名称、ID等が示すデバイスに接続されているか否かが記憶されている。デバイス接続は、例えば、Bluetooth（登録商標）によりペア設定されたデバイスと端末装置1との接続である。各振舞の合格条件は、各振舞の信頼性を担保できる条件を予め定めた条件である。

【0043】

次に、傾き情報テーブル173のテーブルを、図5Cに示す。傾き情報テーブル173は、図4に示した傾き検出部13から取得された端末装置1の傾きを示す角度と、その角度を取得した取得日時、傾きを検出するためのインターバルとなる待機時間とを記憶している。端末装置1の傾きを示す角度は、待機時間が経過する毎に図4に示した認証用情報取得部181により傾き検出部13から取得され、更新される。また、その角度を更新する際、角度を取得した取得日時も更新される。

10

【0044】

本実施の形態に係る端末装置1は、電源投入後処理のイニシャライズ処理の実行が完了すると、もしくは、スリープ状態から復帰すると、認証が成功するまで各機能の操作を許さないロック状態に入る。このロック状態に入る、若しくは、各機能の操作を行う際に認証が要求されると、図2に示した端末制御部18は、端末記憶部17に記憶された認証処理プログラム170を実行し、ユーザがユーザ本人か否かを判別する。端末制御部18により実行される認証処理プログラム170の処理について、図6A及び図6Bに示す認証処理のフローチャートを参照しつつ、以下に説明する。

【0045】

20

まず、図6Aを参照する。本実施の形態においては、生体情報としてユーザの顔画像を用いるものとする。図4に示した認証用情報取得部181は、撮影部11に端末装置1を操作しているユーザの顔写真を撮影させる。具体的には、認証用情報取得部181は、端末装置1の正面に向き合っているユーザの顔写真を、インカメラ11Aで撮影させる。認証用情報取得部181は、撮影部11から撮影したユーザの顔写真を取得する（ステップS101）。認証用情報取得部181は、取得したユーザの顔写真がブレていないか判定する（ステップS102）。ユーザの顔写真がブレていた場合（ステップS102；NO）、認証用情報取得部181は、撮影部11にユーザの顔写真の撮影をリトライさせる（ステップS103）。また、ユーザの顔写真がブレていなかった場合（ステップS102；YES）、認証用情報取得部181は、撮影部11に撮影させたユーザの顔写真からユーザの顔が検出できるか判定する（ステップS104）。

30

【0046】

ユーザの顔写真からユーザの顔が検出できない場合（ステップS104；NO）、認証用情報取得部181は、撮影部11にユーザの顔写真の撮影をリトライさせる（ステップS103）。なお、ユーザの顔写真からユーザの顔が検出できない場合、今操作しているユーザにこれ以上操作をさせないようにロックをかける、他の認証方法を利用する旨のメッセージを表示する等をしてよい。また、ユーザの顔写真からユーザの顔が検出できた場合（ステップS104；YES）、認証用情報取得部181は、検出したユーザの顔の画像の特徴量を求める。認証用情報取得部181は、求めたユーザの顔の画像の特徴量を認証判定部182に送信する。

40

【0047】

認証判定部182は、図2に示した端末記憶部17に記憶されている認証用生体情報データベース171を取得する。認証判定部182は、図6Aに示した認証用生体情報データベース171のテーブルから、生体情報の種類のうち「顔」に対応付けられた登録情報に記憶された顔画像の特徴量と、認証値の認証許容値及び認証閾値を取得する。認証判定部182は、認証用生体情報データベース171から取得した登録情報の顔画像の特徴量と、認証用情報取得部181から受信した顔画像の特徴量とを比較し、比較の結果を基に顔の認証値を求める。認証判定部182は、求めた顔の認証値が認証用生体情報データベース171から取得した認証閾値以上か否かを判定する（ステップS105）。

【0048】

50

求めた顔の認証値が認証閾値以上の場合（ステップS105；YES）、認証判定部182は、求めた顔の認証値が認証用生体情報データベース171から取得した認証許容値以下か否かを判定する（ステップS106）。求めた顔の認証値が認証許容値以下の場合（ステップS106；YES）、端末装置1を使用しているユーザがユーザ本人か否かグレーであるため、認証判定部182は振舞情報による認証である補助認証を実行する。まず、認証判定部182は、認証用情報取得部181に通信部10から現在接続している通信接続先を取得させる。認証判定部182は、認証用情報取得部181から、取得させた通信部10の現在の通信接続先を受信する。

【0049】

続いて、認証判定部182は、図2に示した端末記憶部17から認証用振舞情報データベース172を取得する。認証判定部182は、図5Bに示した認証用振舞情報データベース172のテーブルに記憶されている振舞の種類のうち「通信接続」に対応つけられた取得情報、回数、合格条件を取得する。例えば、図5Bに示すように、「通信接続」の取得情報にはSSIDであるABC_WLANと123WLANとが記憶されている。このABC_WLANでは、接続した回数に31回、合格条件として接続回数が100回以上と記憶されている。また、123WLANでは、接続した回数に157回、合格条件として接続回数が100回以上と記憶されている。なお、以下では合格条件を満たす場合を信頼するものと呼び、合格条件を満たさない場合を信頼しないものと呼ぶ。

【0050】

認証判定部182は、認証用情報取得部181から受信した通信部10の現在の通信接続先と、認証用振舞情報データベース172から取得した取得情報とを比較し、現在の通信接続先が信頼する接続先か否かを判定する（ステップS107）。ここで、例えば、通信部10の現在の通信接続先としてSSIDのABC_WLANが取得されているものとする。認証用振舞情報データベース172に記憶された振舞の種類「通信接続」の取得情報におけるABC_WLANは、接続した回数が31回であり、合格条件の接続回数が100回以上である。このため、現在の通信接続先は信頼する通信接続先ではないため（ステップS107；YES）、信頼するイベントを実行しているか否かを判定する（ステップS108）。

【0051】

認証判定部182は、認証用情報取得部181に操作入力部14から直前に実行したイベントの内容を取得させる。認証判定部182は、端末装置1に備えられたカレンダーから現在の日時に予定があるか否かと、その予定が行われる場所の情報とを取得する。認証判定部182は、その日に予定が無かった場合、信頼するイベントの実行ではないものとし（ステップS108；YES）、顔と端末装置1との距離を算出する（ステップS109）。また、その日に予定があった場合、認証判定部182は、認証用情報取得部181に位置検出部16から、現在の位置情報を取得させる。続いて、認証判定部182は、図2に示した端末記憶部17から認証用振舞情報データベース172を取得する。

【0052】

認証判定部182は、図5Bに示した認証用振舞情報データベース172のテーブルに記憶されている振舞の種類のうち、「イベント実行」に対応つけられた取得情報と合格条件とを取得する。例えば、図5Bに示すように、「イベント実行」の取得情報にはイベントが行われる場所として「×公園」及び「×映画館」が記憶され、その両方の合格条件として「距離が100m以内」と記憶されているものとする。

【0053】

ここで、例えば、端末装置1に備えられたカレンダーに、現在の日時に行われるイベントの場所として「×公園」が記憶されているものとする。認証判定部182は、認証用情報取得部181に位置検出部16から取得させた現在の位置情報と、現在の日時に行われるイベントの場所である「×公園」の位置情報とを比較する。例えば、現在の位置情報と、イベントの場所である「×公園」の位置情報との間の距離が113mとする。この場合、信頼するイベントの実行ではないものとし（ステップS108；YES）、顔と

10

20

30

40

50

端末装置 1 との距離を算出する (ステップ S 1 0 9)。ユーザの顔と端末装置 1 との距離は、図 1 に示したインカメラ 1 1 A で撮影した端末装置 1 の正面に向き合うユーザの顔写真における、ユーザの顔の占める割合に基づいて算出する。

【 0 0 5 4 】

続いて、認証判定部 1 8 2 は、図 2 に示した端末記憶部 1 7 から認証用振舞情報データベース 1 7 2 を取得する。認証判定部 1 8 2 は、図 5 B に示した認証用振舞情報データベース 1 7 2 のテーブルに記憶されている振舞の種類のうち「顔と端末装置との距離」に対応つけられた平均距離、合格条件を取得する。例えば、図 5 B に示すように、「顔と端末装置との距離」の平均距離には 2 6 2 mm、合格条件に平均距離のプラスマイナス 2 0 mm 以内と記憶されている。

10

【 0 0 5 5 】

認証判定部 1 8 2 は、ステップ S 1 0 9 で算出したユーザの顔と端末装置 1 との距離が、認証用振舞情報データベース 1 7 2 から取得した合格条件に設定された設定範囲内か否か判定する (ステップ S 1 1 0)。具体的には、認証用振舞情報データベース 1 7 2 から取得した平均距離は 2 6 2 mm、合格条件は、平均距離のプラスマイナス 2 0 mm 以内であるので、2 4 2 mm から 2 8 2 mm の範囲か否かを判定する。

【 0 0 5 6 】

ステップ S 1 0 9 で算出したユーザの顔と端末装置 1 との距離が、2 4 2 mm から 2 8 2 mm の範囲である場合 (ステップ S 1 1 0 ; Y E S)、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証する。認証判定部 1 8 2 は、認証用情報更新部 1 8 4 に、図 2 に示した認証用生体情報データベース 1 7 1 及び認証用振舞情報データベース 1 7 2 に記憶された各種データを更新させる (ステップ S 1 1 1)。

20

【 0 0 5 7 】

具体的には、認証用情報更新部 1 8 4 は、図 5 A に示した認証用生体情報データベース 1 7 1 のテーブルの生体情報の種類「顔」に対応つけられた登録情報を、登録情報に記憶されていた顔画像の特徴量に認証判定部 1 8 2 が認証用情報取得部 1 8 1 から受信した顔画像の特徴量を加え、更新する。続いて、認証用情報更新部 1 8 4 は、図 5 B に示した認証用振舞情報データベース 1 7 2 のテーブルの振舞の種類「通信接続」に対応つけられた最新状況に記憶されている回数に 1 を加え、更新する。また、認証用情報更新部 1 8 4 は、図 5 B に示した認証用振舞情報データベース 1 7 2 のテーブルに記憶されている振舞の種類「顔と端末装置との距離」に対応つけられた最新状況を、記憶されている平均距離とステップ S 1 0 9 で算出された「顔と端末装置との距離」とから求めた平均距離で更新する。

30

【 0 0 5 8 】

このように、認証用生体情報データベース 1 7 1 に記憶された生体情報、及び、認証用振舞情報データベース 1 7 2 に記憶された振舞情報を更新することにより、ユーザの生体情報及び振舞情報の精度が向上する。このため、ユーザの認証の精度を向上させることができる。

【 0 0 5 9 】

また、認証判定部 1 8 2 により求められた顔の認証値が、認証値の認証閾値以上でない場合 (ステップ S 1 0 5 ; N O)、認証判定部 1 8 2 は、認証用情報取得部 1 8 1 に通信部 1 0 から現在接続している通信接続先を取得させる。認証判定部 1 8 2 は、認証用情報取得部 1 8 1 から、取得させた通信部 1 0 の現在の通信接続先を受信する。続いて、認証判定部 1 8 2 は、図 2 に示した端末記憶部 1 7 から認証用振舞情報データベース 1 7 2 を取得する。認証判定部 1 8 2 は、図 5 B に示した認証用振舞情報データベース 1 7 2 のテーブルに記憶されている振舞の種類のうち「通信接続」に対応つけられた取得情報、回数、合格条件を取得する。認証判定部 1 8 2 は、認証用情報取得部 1 8 1 から受信した通信部 1 0 の現在の通信接続先と、認証用振舞情報データベース 1 7 2 から取得した取得情報とを比較し、現在の通信接続先が信頼する接続先か否か判定する (ステップ S 1 1 2)。

40

【 0 0 6 0 】

50

ここで、例えば、通信部 10 の現在の通信接続先として S S I D の 1 2 3 W L A N が取得されているものとする。認証用振舞情報データベース 1 7 2 に記憶された振舞の種類「通信接続」の取得情報における 1 2 3 W L A N は、接続した回数が 1 5 6 回であり、合格条件の接続回数が 1 0 0 回以上である。このため、現在の通信接続先は信頼する通信接続先であるため（ステップ S 1 1 2 ; Y E S ）、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証する。その後、認証判定部 1 8 2 は、認証間隔を現在の認証間隔よりも長くする（ステップ S 1 1 3 ）。これは、現在の通信接続先が信頼する通信接続先であれば、ユーザ本人は自宅、職場等の信頼する環境に居るものと考えられるためである。この場合、認証間隔を現在の認証間隔よりも長くし、認証の頻度を下げ必要最低限の回数認証を行うようにすれば良い。

10

【 0 0 6 1 】

ここで、例えば、通信部 10 の現在の通信接続先として S S I D の A B C _ W L A N が取得されているものとする。認証用振舞情報データベース 1 7 2 に記憶された振舞の種類「通信接続」の取得情報における A B C _ W L A N は、接続した回数が 3 1 回であり、合格条件の接続回数が 1 0 0 回以上である。このため、現在の通信接続先は信頼する通信接続先ではないため（ステップ S 1 1 2 ; N O ）、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証せず、認証間隔を現在の認証間隔よりも長くしない。

【 0 0 6 2 】

ここで、ステップ S 1 0 7 において、例えば、通信部 10 の現在の通信接続先として S S I D の 1 2 3 W L A N が取得されているものとする。認証用振舞情報データベース 1 7 2 に記憶された振舞の種類「通信接続」の取得情報における 1 2 3 W L A N は、接続した回数が 1 5 6 回であり、合格条件の接続回数が 1 0 0 回以上である。このため、現在の通信接続先は信頼する通信接続先であるため（ステップ S 1 0 7 ; N O ）、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証する。

20

【 0 0 6 3 】

また、ここで、ステップ S 1 0 8 において、例えば、端末装置 1 に備えられたカレンダーに、現在の日時に行われるイベントの場所として「映画館」が記憶されているものとする。認証判定部 1 8 2 は、認証用情報取得部 1 8 1 に位置検出部 1 6 から取得させた現在の位置情報と、現在の日時に行われるイベントの場所である「映画館」の位置情報とを比較する。例えば、現在の位置情報と、イベントの場所である「映画館」の位置情報との間の距離が 7 2 m とする。この場合、信頼するイベントの実行であるものとし（ステップ S 1 0 8 ; N O ）、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証する。

30

【 0 0 6 4 】

認証判定部 1 8 2 は、認証間隔を現在の認証間隔よりも長くする（ステップ S 1 1 3 ）。認証判定部 1 8 2 は、ユーザの顔と端末装置 1 との距離を算出する（ステップ S 1 1 4 ）。続いて、認証判定部 1 8 2 は、図 2 に示した端末記憶部 1 7 から認証用振舞情報データベース 1 7 2 を取得する。認証判定部 1 8 2 は、ステップ S 1 1 4 で算出したユーザの顔と端末装置 1 との距離が、認証用振舞情報データベース 1 7 2 から取得した合格条件に設定された設定範囲内か否か判定する（ステップ S 1 1 5 ）。ステップ S 1 0 9 で算出したユーザの顔と端末装置 1 との距離が、設定範囲である場合（ステップ S 1 1 5 ; Y E S ）、認証判定部 1 8 2 は、端末装置 1 を使用しているユーザをユーザ本人と認証する。認証判定部 1 8 2 は、認証用情報更新部 1 8 4 に、図 2 に示した認証用生体情報データベース 1 7 1 及び認証用振舞情報データベース 1 7 2 に記憶された各種データを更新させる（ステップ S 1 1 1 ）。

40

【 0 0 6 5 】

具体的には、認証用情報更新部 1 8 4 は、図 5 A に示した認証用生体情報データベース 1 7 1 のテーブルの生体情報の種類「顔」に対応つけられた登録情報を、登録情報に記憶されていた顔画像の特徴量にステップ S 1 0 5 で認証判定部 1 8 2 が認証用情報取得部 1 8 1 から受信した顔画像の特徴量を加え、更新する。

50

【0066】

続いて、認証情報更新部184は、図5Bに示した認証用振舞情報データベース172のテーブルの振舞の種類「通信接続」に対応つけられた、最新状況に記憶されている回数に1を加え、更新する。続いて、認証情報更新部184は、認証用振舞情報データベース172のテーブルの振舞の種類「イベント実行」に対応つけられた最新状況を、ステップS108；NOで求めたイベントの場所と端末装置1との間の距離を書き込み、更新する。また、認証情報更新部184は、図5Bに示した認証用振舞情報データベース172のテーブルに記憶されている振舞の種類「顔と端末装置との距離」に対応つけられた最新状況を、最新状況に記憶されている平均距離とステップS114で算出された「顔と端末装置との距離」とから求められた平均距離で更新する。

10

【0067】

ステップS114で算出したユーザの顔と端末装置1との距離が、設定範囲でない場合（ステップS115；NO）、認証判定部182は、認証情報更新部184に、図2に示した認証用生体情報データベース171及び認証用振舞情報データベース172に記憶された各種データを更新させない。

【0068】

また、認証判定部182により求められた顔の認証値が、認証値の認証許容値以下でない場合（ステップS106；NO）、及び、ステップS110で顔と端末装置との距離が設定範囲内でなかった場合（ステップS110；NO）、認証判定部182は、端末装置1を使用しているユーザをユーザ本人ではないと判断する。認証判定部182は、図4に示した認証結果表示部183に、表示部19へ認証できなかった旨を表示させる。続いて、認証判定部182は、端末装置1に備えられている既存の生体認証手段を呼び出す。ここでは、既存の生体認証手段として指紋認証を呼び出すものとする。認証判定部182は、指紋認証を実行する（ステップS116）。

20

【0069】

指紋認証ができた場合（ステップS117；YES）、認証判定部182からの指示により、認証情報取得部181は、撮影部11に端末装置1を操作しているユーザの顔写真を撮影させる。認証情報取得部181は、撮影部11から撮影したユーザの顔写真の画像を取得し、ユーザの顔の画像の特徴量を求める。認証情報取得部181は、認証判定部182に求めたユーザの顔の画像の特徴量を送信する。認証判定部182は、受信したユーザの顔の画像の特徴量を図4に示した認証情報更新部184に送信する。認証情報更新部184は、受信したユーザの顔の画像の特徴量を、図5Aに示した認証用生体情報データベース171のテーブルの生体情報の種類「顔」に対応つけられた登録情報に記憶されていた顔画像の特徴量に加え、更新する（ステップS118）。認証判定部182は、ステップS101へ戻り、ステップS101以降のステップを実行する。

30

【0070】

また、指紋認証ができなかった場合（ステップS117；NO）、認証判定部182は、図4に示した認証結果表示部183に、表示部19へ認証できなかった旨を表示させる。続いて、認証判定部182は、図4に示した認証結果表示部183にログイン画面を表示部19に表示させる（ステップS119）。

40

【0071】

ここで、図6Bに移動する。認証判定部182は、生体認証及び補助認証が予め定められた設定回数成功したか否かを判定する（ステップS120）。この設定回数は、例えば、連続で10回、端末装置1が起動してから合計で20回等、任意の回数である。生体認証及び補助認証が予め定められた設定回数成功した場合（ステップS120；YES）、認証判定部182は、設定回数分の認証で求められた顔の認証値の平均値を求める（ステップS121）。具体的には、認証判定部182は、図2に示した認証用生体情報データベース171を、端末記憶部17から取得する。認証判定部182は、図6Aに示した認証用生体情報データベース171のテーブルから、生体情報の種類のうち「顔」に対応付けられた認証値の平均値を取得する。認証判定部182は、ステップS105で求めた顔

50

の認証値と、認証用生体情報データベース171から取得した認証値の平均値とを足して2で割り、顔の認証値の平均値を算出する。また、生体認証及び補助認証が予め定められた設定回数成功しなかった場合（ステップS120；NO）、ステップS121からステップS123の処理をスキップし、ステップS124へ進む。

【0072】

認証判定部182は、ステップS121で求めた顔の認証値の平均値を、認証用情報更新部184に送信する。認証用情報更新部184は、受信した顔の認証値の平均値と、予め設定された認証閾値の上限値とを比較する。顔の認証値の平均値が予め設定された認証閾値の上限値以上である場合、認証用情報更新部184は、図6Aに示した認証用生体情報データベース171のテーブルの、生体情報の種類のうち「顔」に対応付けられた認証閾値に、認証閾値の上限値を書き込み、更新する。また、顔の認証値の平均値が予め設定された認証閾値の上限値以下である場合、認証用情報更新部184は、図6Aに示した認証用生体情報データベース171のテーブルの、生体情報の種類のうち「顔」に対応付けられた認証閾値に、ステップS121で求めた顔の認証値の平均値を書き込み、更新する（ステップS122）。

10

【0073】

続いて、認証用情報更新部184は、認証許容値を更新する（ステップS123）。具体的には、ステップS121で求めた顔の認証値の平均値が、予め設定された認証閾値の上限値以上である場合、認証用情報更新部184は、予め設定された最大認証許容値を認証許容値とする。また、ステップS121で求めた顔の認証値の平均値が、予め設定された認証閾値の上限値以下である場合、ステップS121で求めた顔の認証値の平均値とデフォルトの認証許容範囲値とを足した値が最大認証許容値以下であれば、その足した値を認証許容値とする。ステップS121で求めた顔の認証値の平均値とデフォルトの認証許容範囲値とを足した値が最大認証許容値以上であれば、最大認証許容値を認証許容値とする。認証用情報更新部184は、図2に示した認証用生体情報データベース171を、端末記憶部17から取得する。認証用情報更新部184は、図6Aに示した認証用生体情報データベース171のテーブルの、生体情報の種類のうち「顔」に対応付けられた認証許容値に、求めた認証許容値を書き込み、更新する。

20

【0074】

図4に示した認証用情報取得部181は、傾き検出部13から端末装置1の傾きの角度を取得する。続いて、認証用情報取得部181は、図示しないタイマから現在の日時情報を取得する（ステップS124）。認証用情報取得部181は、取得した端末装置1の傾きの角度と現在の日時情報とを認証判定部182に送信する。認証判定部182は、受信した端末装置1の傾きの角度と現在の日時情報とを、認証用情報更新部184に送信する。認証用情報更新部184は、図2に示した端末記憶部17に記憶された傾き情報テーブル173に、受信した端末装置1の傾きの角度と現在の日時情報とを書き込み、保存する（ステップS125）。

30

【0075】

認証判定部182は、図5Cに示した傾き情報テーブル173のテーブルに記憶されている待機時間を取得する。認証判定部182は、認証用情報取得部181に取得した待機時間を送信する。認証用情報取得部181は、受信した待機時間の間、通信部10、撮影部11等からのデータの取得を待機する（ステップS126）。待機時間が終了すると、認証用情報取得部181は、傾き検出部13から端末装置1の傾きの角度を取得する。続いて、認証用情報取得部181は、図示しないタイマから現在の日時情報を取得する（ステップS127）。認証用情報取得部181は、取得した端末装置1の傾きの角度と現在の日時情報とを認証判定部182に送信する。

40

【0076】

認証判定部182は、図5Cに示した傾き情報テーブル173のテーブルに記憶されている端末装置1の角度を取得する。認証判定部182は、認証用情報取得部181から受信した端末装置1の傾きの角度と、傾き情報テーブル173から取得した端末装置1の角

50

度とを比較し、角度が変化してないか否かを判定する（ステップS128）。端末装置1の角度の変化が、予め定められた設定値の角度、例えば、30度以上の場合（ステップS128；NO）、認証判定部182は、ユーザにより端末装置1が動かされ何某かの操作が行われたものと判断し、図6Aに示したステップS101に戻る。その後、認証判定部182は、ステップS101以降の処理を実行する。

【0077】

また、端末装置1の角度の変化が、予め定められた設定値の角度以下の場合（ステップS128；YES）、認証判定部182は、ユーザにより端末装置1が動かされていないものと判断する。続いて、認証判定部182は、ユーザを認証するタイミングになったか否かを判定する（ステップS129）。ユーザを認証するタイミングは、予め設定された認証間隔の時間が経過したタイミングである。ユーザを認証するタイミングになっている場合（ステップS129；YES）、認証判定部182は、図6Aに示したステップS101に戻る。その後、認証判定部182は、ステップS101以降の処理を実行する。ユーザを認証するタイミングになっていない場合（ステップS129；NO）、認証判定部182はステップS125に戻る。認証判定部182は、ステップS125からステップS129までの処理を実行する。

【0078】

なお、上記の実施の形態において、生体情報から求められた認証値と認証閾値とが同じ値となった場合には、生体情報から求められた認証値が認証閾値以下、または、生体情報から求められた認証値が認証閾値以上の、どちらの場合として、認証が成功したか否かを判定してもよい。また、生体情報から求められた認証値と認証許容値とが同じ値となった場合には、生体情報から求められた認証値が認証許容値以下、または、生体情報から求められた認証値が認証許容値以上の、どちらの場合として、認証が成功したか否かを判定してもよい。

【0079】

以上の通り、上記実施の形態に係る端末装置1は、ユーザ本人の顔の画像、指紋、声紋等の生体情報と、ユーザが端末装置1を操作する際の特有の挙動、操作状態等による振舞情報とに基づいて、ユーザ本人を認証し、端末装置1における各種機能を実行することができる。また、端末装置1において行われるユーザの認証処理は、端末装置1の稼働中、バックグラウンドで実行されるとともに、ユーザの生体情報と振舞情報とを更新していくことにより、認証の制度を向上させることができる。これにより、使用者の操作負担を軽減しつつ、セキュリティを確保することができる。

【0080】

（変形例1）

上記の実施の形態において、ユーザの生体情報による認証として、ユーザの顔画像による認証と指紋認証とを使用した。これに限らず、ユーザの生体情報による認証は、声紋認証、虹彩認証等、いずれの方法であってもよい。また、上記の実施の形態においては、補助認証を使用する判定の条件としてユーザの顔画像による認証だけを使用した。複数の生体情報により判定してもよい。

【0081】

（変形例2）

上記の実施の形態では、ユーザの認証処理を図2に示した認証処理プログラム170を実行することにより実現するものとした。この認証処理プログラム170で行われる各ステップの全部または一部を、ASIC（Application Specific Integrated Circuit）、システムLSI（Large-scale Integration）等の半導体チップ、各種回路素子により構成される回路等により実現するようにしてもよい。

【0082】

（変形例3）

上記の実施の形態において、補助認証の判定条件として信頼する接続先への接続、信頼

10

20

30

40

50

するイベントの実行、ユーザの顔と端末装置 1 との顔の距離を用いた。これに限らず、他の方法を用いる又は含めても良い。例えば、ユーザ本人が所有するデバイスと端末装置 1 とを Bluetooth (登録商標) で接続しているか否かを判定し、接続している場合にユーザ本人と認証する。Bluetooth (登録商標) により接続される機器を使用するためには、機器同士を「ペアリング」する必要がある。このため、Bluetooth (登録商標) による機器の接続は、個人の特定性が強く、補助認証として利用することでユーザ本人を認証することが可能である。また、さらに、図 2 に示した位置検出部 36 により取得したユーザの行動ルートのパターン、規則性等により、ユーザ本人か否かを判定し、行動ルートのパターン、規則性等が一致する場合にユーザ本人と認証としてもよい。

10

【0083】

(変形例 4)

上記の実施の形態においては、補助認証のうち、一つの認証が成功した場合に、ユーザ本人と認証した。これに限らず、複数の補助認証がすべて成功した場合にのみユーザ本人と認証するようにしてもよい。これにより、さらに認証の精度を高めることができる。

【0084】

(変形例 5)

上記の実施の形態において、生体認証及び補助認証が成功した場合、図 6 A に示したフローチャートのステップ S 1 1 3 において認証判定部 1 8 2 は、認証間隔を現在の認証間隔よりも長くし、認証の頻度を下げている。しかしながら、これに限らず、生体認証及び補助認証が成功した場合、認証間隔を現在の認証間隔よりも長くせずにおき、認証の頻度を下げなくてもよい。具体的には、図 6 A に示したフローチャートのステップ S 1 1 3 を行わなくてもよい。

20

【0085】

(変形例 6)

上記の実施の形態において、ユーザの認証が成功し、ユーザが継続的に端末装置 1 を操作し続ける状態、且つ端末装置 1 の傾きの変更がない場合、ユーザ本人が端末装置 1 を操作し続けているものと判断することができる。この場合、生体認証の認証閾値及び認証許容値を緩めに設定する、認証間隔を長くする等してもよい。こうすることにより、ユーザ本人に対する必要最低限の認証をバックグラウンドで行いつつ、端末装置 1 のリソースの利用を節約する事ができる。

30

【0086】

(変形例 7)

上記の実施の形態において、予め定められた認証間隔によりバックグラウンドでの認証を行うようにした。これに限らず、認証のタイミング及び間隔を定めず、ランダムにバックグラウンドで認証を行うようにしてもよい。例えば、端末装置 1 に搭載されている各種センサの何れかにより、端末装置 1 の位置の変更、傾きの変更などの空間的な変化があった場合に、随時認証を行うようにしてもよい。また、ユーザが端末装置 1 に対し特別な処理を行うための操作、イレギュラーな操作等を行った場合に、認証を行うようにしてもよい。

40

【0087】

また、本発明の実施の形態に係る端末装置 1 は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、端末装置 1 における各機能を実現するためのプログラムを、コンピュータが読み取り可能な CD-ROM (Compact Disc Read Only Memory)、DVD-ROM (Digital Versatile Disc Read Only Memory) などの記録媒体に格納して配布し、このプログラムをコンピュータにインストールすることにより、上述の各機能を実現することができるコンピュータを構成してもよい。そして、各機能を OS (Operating System) とアプリケーションとの分担、または OS とアプリケーションとの協同により実現する場合には、アプリケーションのみを記録媒体に格納して

50

もよい。

【0088】

本発明は、本発明の広義の精神と範囲を逸脱することなく、様々な実施の形態及び変形が可能とされるものである。また、上述した実施の形態は、この開示を説明するためのものであり、本発明の範囲を限定するものではない。すなわち、本発明の範囲は、実施の形態ではなく、請求の範囲によって示される。そして請求の範囲内及びそれと同等の開示の意義の範囲内で施される様々な変形が、この開示の範囲内とみなされる。

【0089】

本出願は、2019年7月31日に出願された、日本国特許出願特願2019-141648号に基づく。本明細書中に日本国特許出願特願2019-141648号の明細書、特許請求の範囲、図面全体を参照として取り込むものとする。

10

【産業上の利用可能性】

【0090】

本発明は、端末装置に好適に利用することができる。

【符号の説明】

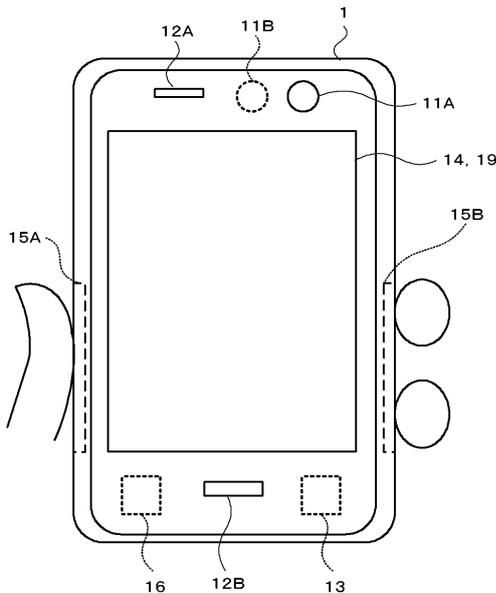
【0091】

1 端末装置、10 通信部、11 撮影部、11A インカメラ、11B メインカメラ、12 音声入出力部、12A スピーカ、12B マイクロフォン、13 傾き検出部、14 操作入力部、15 指紋検出部、15A 左指紋センサ、15B 右指紋センサ、16 位置検出部、17 端末記憶部、18 端末制御部、19 表示部、21 プロセッサ、22 メモリ、23 表示コントローラ、24 表示機器、25 I/Oポート、26 記憶機器、27 通信機器、28 データバス、170 認証処理プログラム、171 認証用生体情報データベース、172 認証用振舞情報データベース、173 傾き情報テーブル、181 認証用情報取得部、182 認証判定部、183 認証結果表示部、184 認証用情報更新部。

20

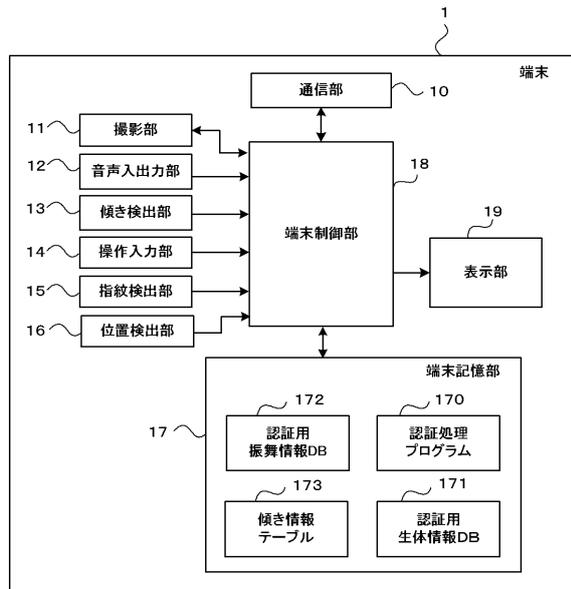
【図1】

図1

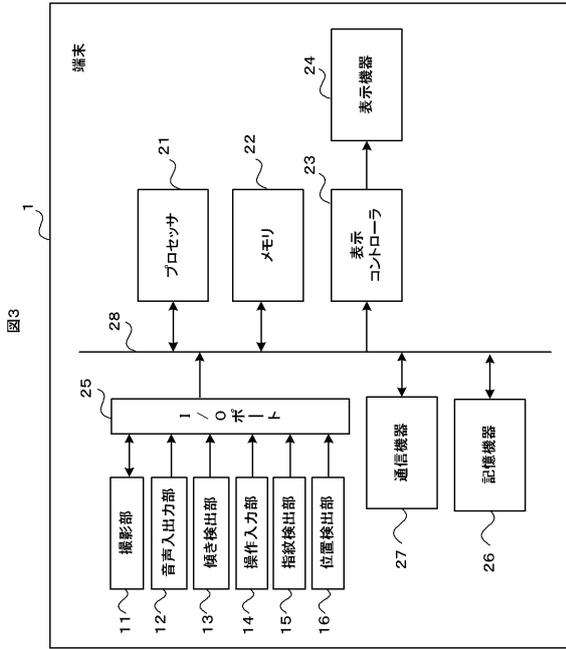


【図2】

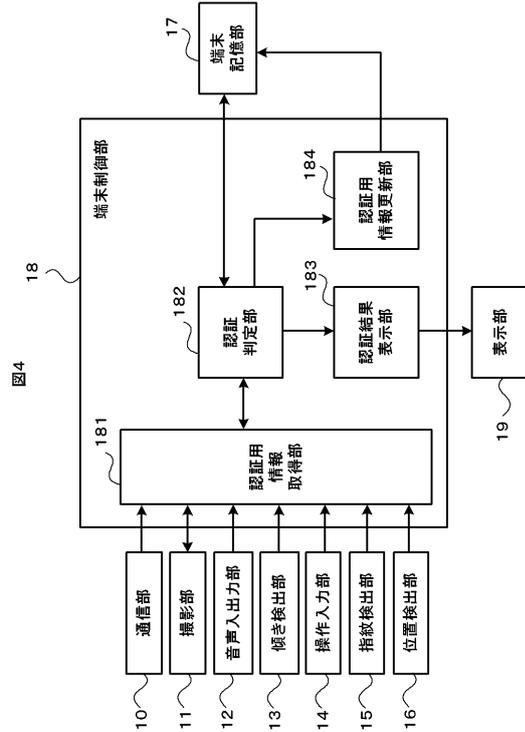
図2



【図3】



【図4】



【図5A】

図5A

認証用生体情報DB 171

生体情報の種類	登録情報	認証値の平均値	認証許容値	認証閾値
顔	AAA	0.44	0.48	0.40
音声		0.32	0.38	0.27
虹彩	●○◎△	0.49	0.55	0.42
指紋	×○××	0.39	0.41	0.30
⋮	⋮	⋮	⋮	⋮

【図5B】

図5B

認証用振舞情報DB 172

振舞の種類	取得情報	最新状況	合格条件
通信接続	ABC,WLAN	31回	接続回数が100回以上
通信接続	123WLAN	157回	接続回数が100回以上
イベント実行	○×公園	113m	距離が100m以内
イベント実行	△●映画館	72m	距離が100m以内
顔と端末装置との距離	—	262mm	距離±20mm以内
デバイス接続	DEFGH	接続中	接続中
⋮	⋮	⋮	⋮

【図5C】

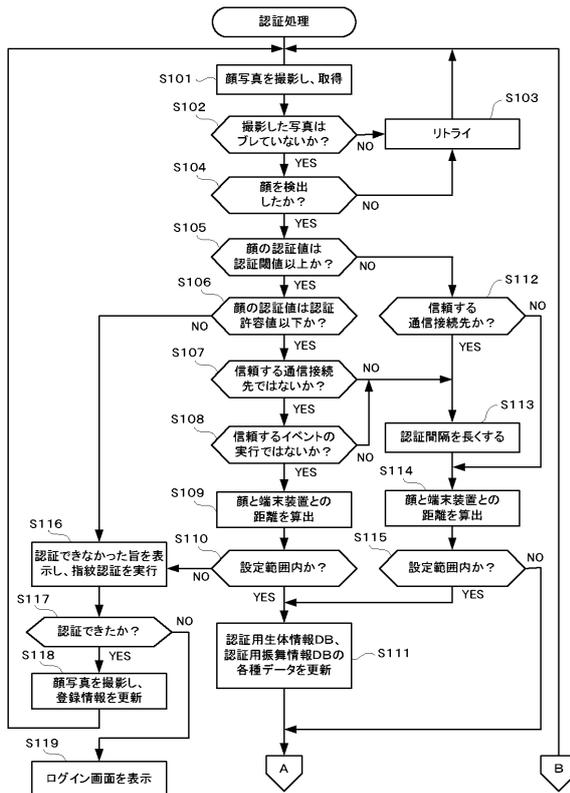
図5C

傾き情報テーブル 173

角度	取得日時	待機時間
127度	2019/07/12 11:25:32	0.5sec

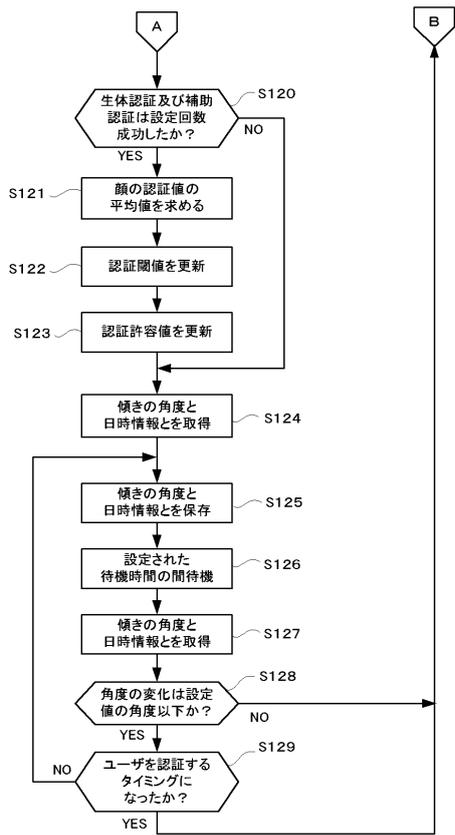
【図6A】

図6A



【図6B】

図6B



フロントページの続き

審査官 平井 誠

- (56)参考文献 特開2001-338295(JP,A)
特表2018-507461(JP,A)
特開2008-310743(JP,A)
特開2011-118561(JP,A)
特開2006-259925(JP,A)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/31