

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2018-18331

(P2018-18331A)

(43) 公開日 平成30年2月1日(2018. 2. 1)

(51) Int.Cl.

G06F 21/32 (2013.01)

F I

G06F 21/32

テーマコード (参考)

審査請求 未請求 請求項の数 8 O L (全 14 頁)

(21) 出願番号	特願2016-148564 (P2016-148564)	(71) 出願人	000003078
(22) 出願日	平成28年7月28日 (2016. 7. 28)		株式会社東芝
			東京都港区芝浦一丁目1番1号
		(71) 出願人	598076591
			東芝インフラシステムズ株式会社
			神奈川県川崎市幸区堀川町72番地34
		(74) 代理人	100108855
			弁理士 蔵田 昌俊
		(74) 代理人	100103034
			弁理士 野河 信久
		(74) 代理人	100075672
			弁理士 峰 隆司
		(74) 代理人	100153051
			弁理士 河野 直樹

最終頁に続く

(54) 【発明の名称】 認証プログラム及び認証システム

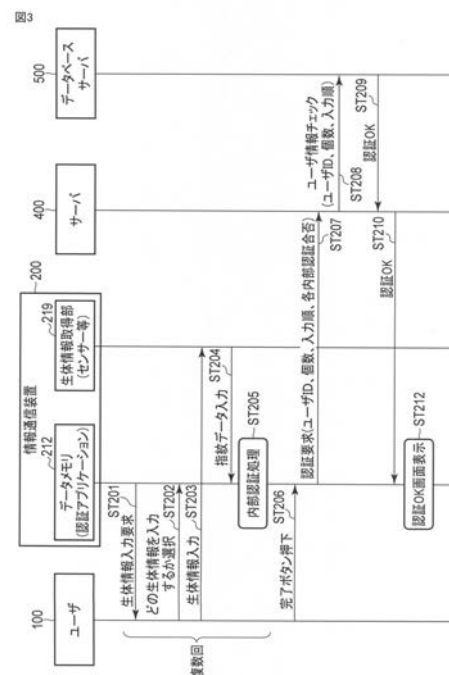
(57) 【要約】

【課題】 安全性に優れた認証プログラムを提供すること

。

【解決手段】 実施形態の認証プログラムは、複数の入力生体情報を順に入力する手順と、識別情報に関連付けられた複数の登録生体情報に基づき、前記複数の入力生体情報を認証する手順と、サーバに対して、認証された前記入力生体情報の入力順を送信する手順と、前記サーバにおける前記入力順と登録された第1認証の認証順との一致判定に基づき前記サーバから返信される第1認証の応答を受信する手順と、前記第1認証の応答の受信に基づき第1の処理を実行する手順と、をコンピュータに実行させる。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

複数の入力生体情報を順に入力する手順と、
識別情報に関連付けられた複数の登録生体情報に基づき、前記複数の入力生体情報を認証する手順と、
サーバに対して、認証された前記入力生体情報の入力順を送信する手順と、
前記サーバにおける前記入力順と登録された第 1 認証の認証順との一致判定に基づき前記サーバから返信される第 1 認証の応答を受信する手順と、
前記第 1 認証の応答の受信に基づき第 1 の処理を実行する手順と、
をコンピュータに実行させる認証プログラム。

10

【請求項 2】

前記識別情報に関連付けて前記複数の登録生体情報を取得する手順と、
前記サーバに対して、前記複数の登録生体情報に対する第 1 認証の認証順を登録する手順と、
をコンピュータに実行させる請求項 1 の認証プログラム。

【請求項 3】

前記サーバに対して、前記入力生体情報の認証結果を送信する手順と、
前記サーバにおける前記入力順と前記第 1 認証の認証順との一致判定、及び前記認証結果が認証失敗を含まないことに基づき前記サーバから返信される前記第 1 認証の応答を受信する手順と、
をコンピュータに実行させる請求項 1 又は 2 の認証プログラム。

20

【請求項 4】

前記サーバにおける前記入力順と登録された第 2 認証の認証順との一致判定に基づき前記サーバから返信される第 2 認証の応答を受信する手順と、
前記第 2 認証の応答の受信に基づき第 2 の処理を実行する手順と、
をコンピュータに実行させる請求項 1 乃至 3 の何れか一つの認証プログラム。

【請求項 5】

前記第 1 認証の認証順は、前記第 1 認証の個数の登録生体情報による前記第 1 認証の個数の入力生体情報の認証順であり、
前記第 2 認証の認証順は、前記第 2 認証の個数の登録生体情報による前記第 2 認証の個数の入力生体情報の認証順である請求項 4 の認証プログラム。

30

【請求項 6】

前記第 1 の処理は、第 1 のメニューを表示する処理であり、
前記第 2 の処理は、第 2 のメニューを表示する処理である請求項 4 の認証プログラム。

【請求項 7】

前記第 1 の処理の要求に応じて、前記第 1 認証の個数の生体情報の入力を要求する手順と、
前記第 2 の処理の要求に応じて、前記第 2 認証の個数の生体情報の入力を要求する手順と、
をコンピュータに実行させる請求項 5 又は 6 の認証プログラム。

40

【請求項 8】

情報処理装置と 1 以上のサーバにより構成される認証システムであって、
前記情報処理装置は、
複数の入力生体情報を順に入力する入力手段と、
識別情報に関連付けられた複数の登録生体情報に基づき、前記複数の入力生体情報を認証する認証手段と、
サーバに対して、認証された前記入力生体情報の入力順を送信し、前記サーバにおける前記入力順と登録された第 1 認証の認証順との一致判定に基づき前記サーバから返信される第 1 認証の応答を受信する第 1 の通信手段と、
前記第 1 認証の応答の受信に基づき第 1 の処理を実行する実行手段と、

50

を備え、
前記サーバは、
前記複数の登録生体情報に対する前記第1認証の認証順を登録する登録手段と、
前記入力順を前記情報処理装置から受信し、前記入力順が前記第1認証の認証順と一致
することを確認した場合、前記第1認証の応答を前記情報処理装置へ送信する第2の通信
手段と、
を備える認証システム。

【発明の詳細な説明】

【技術分野】

【0001】

10

本発明の実施形態は、認証プログラム及び認証システムに関する。

【背景技術】

【0002】

近年、多方面でユーザ認証技術が利用されている。例えば、スマートフォン等の情報処
理装置は、生体情報を利用したユーザ認証機能を備えている。このような情報処理装置は
、ユーザから提示された指紋などの生体情報を指紋認証センサー等で読み取り、読み取っ
た生体情報と登録された生体情報とを照合し、照合結果に基づきユーザを認証することが
できる。

【0003】

また、複数の認証方法を組み合わせて安全性を高める技術が知られている。例えば、複
数の認証方法を組み合わせとして、パスワード認証と生体認証の組み合わせが知られてい
る。

20

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特開2007-156959号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

上記の通り、様々なユーザ認証技術が知られており、また、安全性を高める様々な技術
が提案され実現されている。それでも、安全性についてはまだ不十分な点があり、より安
全性の高いユーザ認証技術が要望されている。

30

【0006】

本発明の目的は、安全性に優れた認証プログラム及び認証システムを提供することであ
る。

【課題を解決するための手段】

【0007】

実施形態の認証プログラムは、複数の入力生体情報を順に入力する手順と、識別情報に
関連付けられた複数の登録生体情報に基づき、前記複数の入力生体情報を認証する手順と
、サーバに対して、認証された前記入力生体情報の入力順を送信する手順と、前記サーバ
における前記入力順と登録された第1認証の認証順との一致判定に基づき前記サーバから
返信される第1認証の応答を受信する手順と、前記第1認証の応答の受信に基づき第1の
処理を実行する手順と、をコンピュータに実行させる。

40

【図面の簡単な説明】

【0008】

【図1】実施形態に係る認証システムの一例を示すブロック図である。

【図2】実施形態に係る登録処理の一例を示す図である。

【図3】実施形態に係る認証処理の一例を示す図である。

【図4】実施形態に係るデータベースサーバに登録されるデータベースの第1例を示す図
である。

50

【図 5】実施形態に係るデータベースサーバに登録されるデータベースの第 2 例を示す図である。

【発明を実施するための形態】

【0009】

図 1 は、実施形態に係る認証システムの一例を示すブロック図である。図 1 に示すように、認証情報通知システムは、携帯電話、スマートフォン、タブレット P C、又はノート P C 等の情報処理装置 2 0 0、サーバ 4 0 0、データベースサーバ 5 0 0 等を備える。情報処理装置 2 0 0、サーバ 4 0 0、及びデータベースサーバ 5 0 0 は相互に通信し、情報を送受信することができる。

【0010】

例えば、情報処理装置 2 0 0 は、制御部 2 1 1、データメモリ 2 1 2、R A M 2 1 3、R O M 2 1 4、I / F (Interface) 2 1 5、入力部 2 1 6、表示部 2 1 7、通信部 2 1 8、生体情報取得部 2 1 9 を備える。

【0011】

制御部 2 1 1 は、C P U (Central Processing Unit) 等により構成され、後述する認証アプリケーションを実行し、認証アプリケーションによる生体情報の登録処理、外部（サーバ等）に対する認証順の登録処理、生体情報の入力処理と認証処理、サーバにおける個人認証結果に基づく各種処理及び動作等を制御する。データメモリ 2 1 2 は、E E P R O M（登録商標）、F R A M（登録商標）、又は F L A S H 等の不揮発性メモリであり、認証アプリケーション及び複数の生体情報等を記憶する。R A M 2 1 3 は、ワーキングメモリとして機能し、R O M 2 1 4 は、制御部 2 1 1 により実行されるプログラムを保持する。

【0012】

例えば、認証アプリケーションは、サービス提供者により提供される情報処理装置向け認証プログラムであり、情報処理装置 2 0 0 にインストールされ、制御部 2 1 1 により実行される。生体情報の登録時に、認証アプリケーションは、後述する生体情報取得部 2 1 9 により取得された生体情報を内部データとして登録する。また、生体情報の認証時に、認証アプリケーションは、ユーザ 1 0 0 から入力される生体情報（入力生体情報）と登録された生体情報（登録生体情報）とを比較し内部認証を実行し、サーバとの通信を行う。

【0013】

なお、本実施形態では、外部からダウンロードされる認証アプリケーションをデータメモリ 2 1 2 が記憶するケースについて説明するが、認証アプリケーションを記憶した R O M 2 1 4 を持たせて情報処理装置 2 0 0 を出荷するようにしてもよい。また、後述する I C カード 3 0 0 のデータメモリ 3 1 2 等が、認証アプリケーション及び複数の登録生体情報を記憶するようにしてもよい。

【0014】

I / F 2 1 5 は、情報処理装置内の各部と通信する。例えば、I / F 2 1 5 は、I C カード 3 0 0 の I / F 3 1 5 と通信する。入力部 2 1 6 は、タッチパネル等で構成され、ユーザ 1 0 0 からの各種入力を受け付ける。なお、入力部 2 1 6 は、キーボード又はマイク等を備え、キーボードからの入力、マイクからの音声入力等を受け付けるようにしてもよい。表示部 2 1 7 は、各種情報を表示する。例えば、表示部 2 1 7 は、タッチパネルに対向配置される液晶ディスプレイ等である。例えば、通信部 2 1 8 は、異なる複数の通信方式をサポートし、3 G / 4 G / L T E（登録商標）等のキャリア通信、及び W i - f i 等の L A N 通信をサポートし、サーバ 4 0 0 又はデータベースサーバ 5 0 0 と通信することができる。生体情報取得部 2 1 9 は、指紋、静脈、顔画像等の生体情報を読み取る各種センサー及びカメラである。なお、生体情報取得部 2 1 9 は、情報処理装置 2 0 0 に内蔵される構成であってもよいし、情報処理装置 2 0 0 に対して着脱可能な構成のものであってもよい。

【0015】

例えば、情報処理装置 2 0 0 は、着脱可能な I C カード 3 0 0 が装填される。例えば、

10

20

30

40

50

ICカード300は、プラスチックカード（基材）により構成され、ICモジュール301（ICチップ）を備え、ICモジュール301は、制御部311、データメモリ312、RAM313、ROM314、I/F315を備える。

【0016】

制御部311は、CPU等により構成され、各種処理、動作を制御する。データメモリ312は、EEPROM（登録商標）、FRAM（登録商標）、又はFLASH等の不揮発性メモリである。RAM313は、ワーキングメモリとして機能し、ROM314は、制御部311により実行されるプログラムを保持する。

【0017】

サーバ400は、汎用コンピュータ等であり、制御部411、データメモリ412、RAM413、ROM414、通信部415を備える。サーバ400は、各情報処理装置200（インストールされた認証アプリケーション）、及びデータベースサーバ500（登録されたデータベース）等と通信する。例えば、サーバ400は、ユーザを認証し、認証済みユーザへオンライン金融取引等のサービスを提供するためのサーバである。

【0018】

データベースサーバ500は、汎用コンピュータ等であり、制御部511、データメモリ512、RAM513、ROM514、通信部515を備える。データベースサーバ500は、サーバ400等と通信し、個人認証処理を実行する。データメモリ512は、データベースを記憶する。例えば、データベースは、各ユーザを認証するための、ユーザ情報（ユーザID含む）、認証する生体情報の個数、認証する生体情報の識別子（どの生体情報か）、認証順（登録順）を含む。

【0019】

なお、本実施形態では、情報処理装置200、及びサーバ400とデータベースサーバ500の複数台のサーバによる認証順の登録処理及び個人認証処理を実現するケースについて説明するが、情報処理装置、及び1台のサーバで登録処理及び個人認証処理を実現するようにしてもよい。

【0020】

以下、生体情報として手の指（指紋）を使う例について説明するが、静脈又は顔画像を使うようにしてもよいし、指、静脈、及び顔画像を組み合わせて使うようにしてもよい。

【0021】

（登録処理）

以下、登録処理の一例について説明する。図2は、実施形態に係る登録処理の一例を示す図である。

【0022】

ユーザ100は、情報処理装置200の入力部216を介して認証アプリケーションを選択する。制御部211は、認証アプリケーションを起動し、制御部211及び認証アプリケーションは、表示部217は、「登録」及び「認証」を表示する。

【0023】

ユーザ100は、入力部216を介して「登録」を選択する。制御部211及び認証アプリケーションは、ユーザ情報（氏名、生年月日等）の第1の登録画面を表示し、ユーザ100は、入力部216を介してユーザ情報を登録（入力）する（ST101）。続いて、制御部211及び認証アプリケーションは、生体情報の登録（入力）を要求する第2の登録画面を表示する（ST102）。例えば、この第2の登録画面は、右手の5本の指と左手の5本の指のイラストを含み、全10本の指から1本ずつ所望の本数の指を選択することを要求する情報を含む。つまり、生体情報の種類を選択することを要求する情報を含む。

【0024】

例えば、ユーザ100が、この第2の登録画面を介して右手親指（第1の指）を選択し（ST103）、生体情報取得部219に対して右手親指を接触させる。生体情報取得部219は、右手親指の指紋情報を読み取り（ST104）、制御部211及び認証アプリ

10

20

30

40

50

ケーションは、この読み取られた情報を右手親指の指紋情報として認識し、データメモリ 212 へ登録する (ST105)。つまり、第1の指の識別情報に関連付けた指紋情報が登録される。

【0025】

さらに、ユーザ100が、この第2の登録画面を介して左手薬指 (第2の指) を選択し (ST103)、生体情報取得部219に対して左手薬指を接触させる。生体情報取得部219は、左手薬指の指紋情報を読み取り (ST104)、制御部211及び認証アプリケーションは、この読み取られた情報を左手薬指の指紋情報として認識し、データメモリ 212 へ登録する (ST105)。つまり、第2の指の識別情報に関連付けた指紋情報が登録される。

10

【0026】

上記した登録作業を複数回繰り返すことにより、識別情報に関連付けた複数の生体情報が登録され、さらにこれら複数の生体情報の登録順 (右手親指 (第1の指) → 左手薬指 (第2の指) → …) が認証順 (認証回数を含んでも良い) として登録される。なお、最初に複数の生体情報だけを登録し、その後、表示部217が登録された複数の生体情報の名称を一覧表示 (右手親指 (第1の指)、左手薬指 (第2の指) 等を一覧表示) し、入力部216を介して複数の生体情報から認証順を指定するようにしてもよい。また、生体情報として、指紋以外に、静脈、顔画像などの生体情報を組み合わせるようにしてもよい。

【0027】

例えば、上記した登録作業を複数回繰り返し、第2の登録画面の「完了」を選択すると (ST106)、制御部211及び認証アプリケーションは、通信部218を介してユーザ登録要求をサーバ400へ送信する (ST107)。例えば、ユーザ登録要求は、ユーザ情報、及び認証順を含む。或いは、ユーザ登録要求は、ユーザ情報、登録生体情報の個数、及び認証順を含む。なお、認証順は、どの部位の生体情報かを示す識別情報 (上記した第1、第2の指の識別情報) により認証順を示す。

20

【0028】

例えば、上記した登録作業を5回繰り返し、異なる5種類の指の指紋情報を順に登録した場合、ユーザ登録要求は、ユーザ情報、登録生体情報の個数 (5個)、及び認証順 (異なる5種類の指の認証順) を含む。

【0029】

また、ユーザ登録要求が、登録用の認証結果を含んでもよい。例えば、登録用の認証結果は、認証成功の情報を含み認証失敗の情報を含まない。つまり、登録用の認証結果は、5回の認証成功を示す情報を含む。この場合、認証成功のみで人物を認証することになる。或いは、登録用の認証結果は、認証成功の情報と認証失敗の情報とを含む。例えば、登録用の認証結果は、1、2、3、5回目の認証は成功で4回目の認証は失敗を示す情報を含む。この場合、認証成功と認証失敗を組み合わせる人物を認証することになる。ユーザ100は、入力部216等を介して登録用の認証結果 (例えば、1、2、3、5回目の認証は成功で4回目の認証は失敗) を入力することができる。

30

【0030】

サーバ400は、情報処理装置200からユーザ登録要求を受信し、データベースサーバ500へユーザ登録要求を送信する (ST108)。データベースサーバ500のデータメモリ512は、ユーザ登録要求に含まれるユーザ情報、及び認証順を登録する。或いは、図4に示すように、データベースサーバ500のデータメモリ512は、ユーザ登録に含まれるユーザ情報、登録生体情報の個数、及び認証順を登録する。なお、ユーザ登録が認証結果を含む場合には、データメモリ512は、各入力生体情報の認証結果も登録する。データベースサーバ500は、ユーザ情報に対応するユーザIDを割り当て、サーバ400へユーザ登録完了 (ユーザID含む) を返信する (ST109)。サーバ400はユーザ登録完了を受信し、情報処理装置200へユーザ登録完了を通知する (ST110)。情報処理装置200はユーザ登録完了を受信し、登録完了を表示し (ST111)、認証アプリケーションはユーザIDを記憶する。

40

50

【0031】

上記の通り、情報処理装置200は、複数の生体情報をデータメモリ212（または312）登録するが、認証順の情報は内部に登録しない。したがって、情報処理装置200から認証順の情報が漏洩することはない。一方、データベースサーバ500は、認証順の情報をデータメモリ512に登録するが、生体情報自身は一切内部に登録しない。したがって、データベースサーバ500から個人情報情報が漏洩することはない。このようにして、生体情報と認証順を分散管理する。つまり、認証順を登録者しか知り得ない情報とし、認証順を秘密鍵としてサーバで管理する。これにより、どちらかの情報が漏洩したとしても、漏洩した一方の情報だけではユーザ認証のための情報を満たせないため、安全性の高い個人認証を実現することができる。

10

【0032】

万一、データベースサーバ500の情報（認証順）が漏れたとしても、この認証順の情報だけでは、個人認証を実現することはできない。また、情報処理装置200が携帯端末の場合、情報処理装置200の盗難等が想定される。このように情報処理装置200が盗まれ、情報処理装置200に登録された一部の生体情報が漏れたとしても、一部の生体情報だけでは、個人認証を実現することはできない。最悪、情報処理装置200に登録された全ての生体情報が漏れたとしても、全ての生体情報をもってしても、認証順の情報が不明のため、不正に個人認証を実現することはできない。

【0033】

また、複数の生体情報の認証結果（認証成功）を用いることで、1つの生体情報の認証結果を用いる場合に比べて、誤った個人認証を防止することができ、個人認証の精度が向上できる（ユーザ本人にもかかわらず、正しくユーザとして認識されないといった誤認識のケースを減少できる）。

20

【0034】

（認証処理）

以下、認証処理について複数の例を挙げて説明する。図3は、実施形態に係る認証処理の一例を示す図である。

【0035】

ユーザ100は、情報処理装置200の入力部216を介して認証アプリケーションを選択する。制御部211は、認証アプリケーションを起動し、制御部211及び認証アプリケーションは、表示部217は、「登録」及び「認証」を表示する。

30

【0036】

ユーザ100は、入力部216を介して「認証」を選択する。制御部211及び認証アプリケーションは、生体情報の入力を要求する第1の入力画面を表示する（ST201）。例えば、この第1の入力画面は、右手の5本の指と左手の5本の指のイラストを含み、全10本の指から1本ずつ所望の本数の指を選択することを要求する情報を含む。つまり、生体情報の種類を選択することを要求する情報を含む。登録ユーザであれば、認証順及び登録個数を知っているので、正しい順序で登録個数分の指を選択することができる。

【0037】

例えば、ユーザ100が、この第1の入力画面を介して右手親指（第1の指）を選択し（ST202）、生体情報取得部219に対して右手親指を接触させる。生体情報取得部219は、右手親指の指紋情報を読み取り（ST203）、制御部211及び認証アプリケーションは、この読み取られた情報を右手親指の指紋情報として認識し、データメモリ212へ入力する（ST204）。

40

【0038】

制御部211及び認証アプリケーションは、内部認証処理を実行する（ST205）。つまり、制御部211及び認証アプリケーションは、データメモリ212に入力された右手親指の指紋情報と、データメモリ212に事前登録された右手親指の指紋情報とを照合し、認証する（認証成功又は認証失敗を判定する）。このとき、制御部211及び認証アプリケーションは、認証結果（認証成功又は認証失敗）を案内（表示等）するようにして

50

もよいし、案内しないようにしてもよい。案内することにより、最終的に個人認証失敗時の対策が立てやすくなる（個人認証失敗の原因が予測し易い）。案内しないことにより、個人認証失敗の原因予測を困難にすることができ、個人認証の安全性を高めることができる。

【0039】

さらに、ユーザ100が、この第1の入力画面を介して左手薬指（第2の指）を選択し（ST202）、生体情報取得部219に対して左手薬指を接触させる。生体情報取得部219は、左手薬指の指紋情報を読み取り（ST203）、制御部211及び認証アプリケーションは、この読み取られた情報を左手薬指の指紋情報として認識し、データメモリ212へ入力する（ST204）。

10

【0040】

制御部211及び認証アプリケーションは、データメモリ212に入力された左手薬指の指紋情報と、データメモリ212に事前登録された左手薬指の指紋情報とを照合し、認証する（認証成功又は認証失敗を判定する）。

【0041】

なお、認証処理において、生体情報の種別の選択は必須ではない。例えば、生体情報の種別の選択がなくても、入力された指紋情報と、データメモリ212に事前登録された複数の指紋情報とを照合し認証に成功すれば、事前登録された指紋情報には生体情報の種別の情報が対応付けられているので、入力された指紋情報の種別を特定することができる。

20

【0042】

上記した認証作業を複数回繰り返すことにより、複数の生体情報の入力順（右手親指（第1の指）→左手薬指（第2の指）→…）と複数の入力生体情報の認証結果（各内部認証可否）が得られる。

【0043】

例えば、上記した認証作業を複数回繰り返し、第1の入力画面の「完了」を選択すると（ST206）、制御部211及び認証アプリケーションは、通信部218を介して認証要求をサーバ400へ送信する（ST207）。例えば、認証要求は、ユーザID、入力生体情報の個数、入力順（入力回数を含んでも良い）、入力生体情報の認証結果（各内部認証可否）を含む。なお、認証要求は、認証された複数の入力生体情報の入力順だけを含み、他の情報を任意で含むようにしてもよい。

30

【0044】

上記した認証作業を5回繰り返し、異なる5種類の指の指紋情報を順に入力した場合、認証要求は、ユーザID、入力生体情報の個数（5個）、各入力生体情報の入力順（異なる5種類の指の入力順）、認証アプリケーションでの各入力生体情報の認証結果（可否。5回分）を含む。

【0045】

サーバ400は、認証要求を受信し、データベースサーバ500へ認証要求を送信する（ST208）。データベースサーバ500は、認証要求に含まれるユーザID、入力生体情報の個数、各入力生体情報の入力順、及び各入力生体情報の認証結果に基づき、個人認証処理を実行する。

40

【0046】

つまり、データベースサーバ500は、入力生体情報の個数と事前登録された登録生体情報の個数が一致すること、入力順と事前登録された認証順が一致すること、及び入力生体情報の認証結果が認証成功を示していること（又は認証失敗を含まないこと）を条件として、個人認証の成功を判定する。或いは、データベースサーバ500は、入力生体情報の個数と事前登録された登録生体情報の個数が一致すること、入力順と事前登録された認証順が一致すること、及び入力生体情報の認証結果（認証成功及び認証失敗を含む）と登録認証結果（認証成功及び認証失敗を含む）が一致することを条件として、個人認証の成功を判定する。なお、データベースサーバ500は、認証された複数の入力生体情報の入力順と事前登録された認証順が一致することだけを条件として、個人認証の成功を判定す

50

るようにしてもよい。

【0047】

データベースサーバ500は、サーバ400へ個人認証成功（応答）を返信する（ST209）。サーバ400は個人認証成功を受信し、情報処理装置200へ個人認証成功を通知する（ST210）。情報処理装置200は個人認証成功を受信し（ST211）、個人認証成功を表示し（ST212）、この受信に基づき所定の処理を実行する。例えば、情報処理装置200は、第1のメニュー画面を表示する。

【0048】

なお、データベースサーバ500は、個人認証失敗時に、個人認証失敗を返信するようにしてもよい。単に、個人認証失敗だけを返信するようにしてもよいし、個人認証失敗の原因を返信するようにしてもよい。例えば、入力生体情報の認証結果に認証失敗が含まれていることを返信する。或いは、入力生体情報の認証結果と登録認証結果の不一致を返信する。或いは、入力順と事前登録された認証順の不一致を返信する。個人認証失敗の原因を返信しなければ個人認証の安全性を高めることができる。個人認証失敗の原因を返信すれば、ユーザ100に入力間違い等を知らせることができる。

【0049】

（第1認証の認証処理）

例えば、図5に示すように、データベースサーバ500のデータベースは、第1認証のための情報として、ユーザ情報（ユーザID含む）、認証する生体情報の個数（例えば3個）、認証順（登録順）、認証する生体情報の識別子（どの生体情報か）、希望結果（認証結果、例えば1、2、3番目認証成功）を含む。なお、希望結果とは、認証可と判断する照合結果、即ち正解を意味する。情報処理装置200は、ユーザに対して第1認証の個数（例えば3個）の入力生体情報を要求（表示案内等）し、第1認証の個数の入力生体情報を順に入力し、事前登録された複数の生体情報に基づき、順に入力された第1認証の個数の入力生体情報を認証する。なお、安全性を高めるために、ユーザに対する第1認証の個数の入力生体情報の要求（表示案内等）を省略してもよい。また、生体情報の入力毎に、どの部位の生体情報を入力するかをユーザが指定（選択）してもよいし、ユーザによる指定を省略するようにしてもよい。ユーザによる指定を省略する場合、入力生体情報がどの部位の生体情報か不明となるが、登録生体情報に対して部位を示す識別情報が対応付けられているので、入力生体情報と登録生体情報とが一致し認証に成功すれば、入力生体情報がどの部位の生体情報か判明する。また、事前登録された生体情報の個数と入力される生体情報の個数（認証の対象となる生体情報の個数）を同数としてもよいし、入力される生体情報の個数が事前登録された生体情報の個数より少なくてもよい。

【0050】

情報処理装置200は、第1認証の個数の入力生体情報の入力順、及び第1認証の個数の入力生体情報の認証結果をサーバ400へ送信する。サーバ400は第1認証の個数の入力生体情報の入力順、及び第1認証の個数の入力生体情報の認証結果をデータベースサーバ500へ送信する。データベースサーバ500は、第1認証の個数の入力生体情報の入力順と第1認証の認証順とが一致し、第1認証の個数の入力生体情報の認証結果と登録認証結果とが一致することを条件として認証成功を示す第1認証の応答をサーバ400へ送信する。サーバ400は第1認証の応答を情報処理装置200へ送信する。情報処理装置200は、第1認証の応答の受信に基づき第1の処理を実行する。例えば、情報処理装置200は、第1のメニュー画面（項目Aを含む）を表示する。

【0051】

なお、登録認証結果は、全ての入力生体情報に対して認証成功であってもよいし（図5参照）、一部の入力生体情報に対して認証成功で、残りの入力生体情報に対して認証失敗であってもよい。つまり、認証成功と認証失敗の組み合わせパターンを登録することにより、安全性を高めることができる。

【0052】

また、情報処理装置200は、ユーザからの第1の処理の選択に対応して第1の処理の

要求を受けた場合に、第 1 認証の個数の生体情報の入力并要求し、上記説明した第 1 認証の認証処理を実行するようにしてもよい。

【0053】

(第 2 認証の認証処理)

上記説明した第 1 認証の認証処理と組み合わせてこの第 2 認証の認証処理を実行するようにしてもよい。

【0054】

例えば、図 5 に示すように、データベースサーバ 500 のデータベースは、第 2 認証のための情報として、ユーザ情報（ユーザ ID 含む）、認証する生体情報の個数（例えば 5 個）、認証順（登録順）、認証する生体情報の識別子（どの生体情報か）、希望結果（認証結果、例えば 1、2、3、4、5 番目の全て認証成功、或いは 1、2、3、5 番目認証成功、4 番目認証失敗）を含む。情報処理装置 200 は、ユーザに対して第 2 認証の個数（例えば 5 個）の入力生体情報を要求し、第 2 認証の個数の入力生体情報を順に入力し、事前登録された複数の生体情報に基づき、順に入力された第 2 認証の個数の入力生体情報を認証する。安全性を高めるために、ユーザに対する第 2 認証の個数の入力生体情報の要求（表示案内等）を省略してもよい。また、生体情報の入力毎に、どの部位の生体情報を入力するかをユーザが指定（選択）してもよいし、ユーザによる指定を省略するようにしてもよい。

【0055】

情報処理装置 200 は、第 2 認証の個数の入力生体情報の入力順、及び第 2 認証の個数の入力生体情報の認証結果をサーバ 400 へ送信する。サーバ 400 は第 2 認証の個数の入力生体情報の入力順、及び第 2 認証の個数の入力生体情報の認証結果をデータベースサーバ 500 へ送信する。データベースサーバ 500 は、認証された第 2 認証の個数の入力生体情報の入力順と第 2 認証の認証順とが一致し、第 2 認証の個数の入力生体情報の認証結果と第 2 認証の登録認証結果とが一致することを条件として認証成功を示す第 2 認証の応答をサーバ 400 へ送信する。サーバ 400 は第 2 認証の応答を情報処理装置 200 へ送信する。情報処理装置 200 は、第 2 認証の応答の受信に基づき第 2 の処理を実行する。例えば、情報処理装置 200 は、第 2 のメニュー画面（項目 B を含む又は項目 A と B を含む）を表示する。例えば、第 1 認証について認証成功が得られた場合には第 1 の項目数の項目が選択可能であり、第 2 認証について認証成功が得られた場合には第 2 の項目数の項目が選択可能である。例えば、第 2 の項目数は第 1 の項目数より多く（第 1 の項目数 < 第 2 の項目数）、第 2 の項目数の項目が第 1 の項目数の項目を含むようにしてもよい。

【0056】

つまり、第 1 認証の認証処理では 3 個の生体情報の認証が得られれば目的の処理（例えば第 1 の項目に対応する第 1 の処理）を実行することができ、第 2 認証の認証処理では 5 個の生体情報の認証が得られれば目的の処理（例えば第 1 の項目に対応する第 1 の処理と第 2 の項目に対応する第 2 の処理）を実行することができる。用途に応じて第 1 又は第 2 認証の認証処理を使い分けることにより、認証処理の煩雑さと安全性の向上についてバランスを取ることができる。なお、第 2 認証の認証順の 1 番目から 3 番目までの認証順が、第 1 認証の認証順と同じであってもよい。或いは、第 1 認証の認証処理と第 2 認証の認証処理における生体認証の個数が同数であってもよい。また、第 1 認証の認証処理及び第 2 認証の認証処理における登録認証結果が、全ての入力生体情報に対して認証成功であってもよいし、一部の入力生体情報に対して認証成功で、残りの入力生体情報に対して認証失敗であってもよい。つまり、認証成功と認証失敗の組み合わせパターンを登録することにより、安全性を高めるようにしてもよい。

【0057】

また、情報処理装置 200 は、ユーザからの第 2 の処理の選択に対応して第 2 の処理の要求を受けた場合に、第 2 認証の個数の生体情報の入力并要求し、上記説明した第 2 認証の認証処理を実行するようにしてもよい。

【0058】

なお、情報処理装置 200、サーバ 400、データベースサーバ 500での全ての処理はいくつかのソフトウェア（上記した認証アプリケーションを含む）によって実行することが可能である。このため、上記処理の手順を実行するいくつかのプログラムを格納したコンピュータ読み取り可能な記憶媒体を通じてこれらプログラムを情報処理装置 200、サーバ 400、データベースサーバ 500へインストールして実行するだけで、上記処理を容易に実現することができる。例えば、情報処理装置 200、サーバ 400、データベースサーバ 500は、上記プログラムをネットワーク経由でダウンロードし、ダウンロードしたプログラムを記憶し、プログラムのインストールを完了することができる。或いは、情報処理装置 200、サーバ 400、データベースサーバ 500は、上記プログラムを情報記憶媒体から読み取り、読み取ったプログラムを記憶し、プログラムのインストールを完了することができる。

10

【0059】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれるものである。

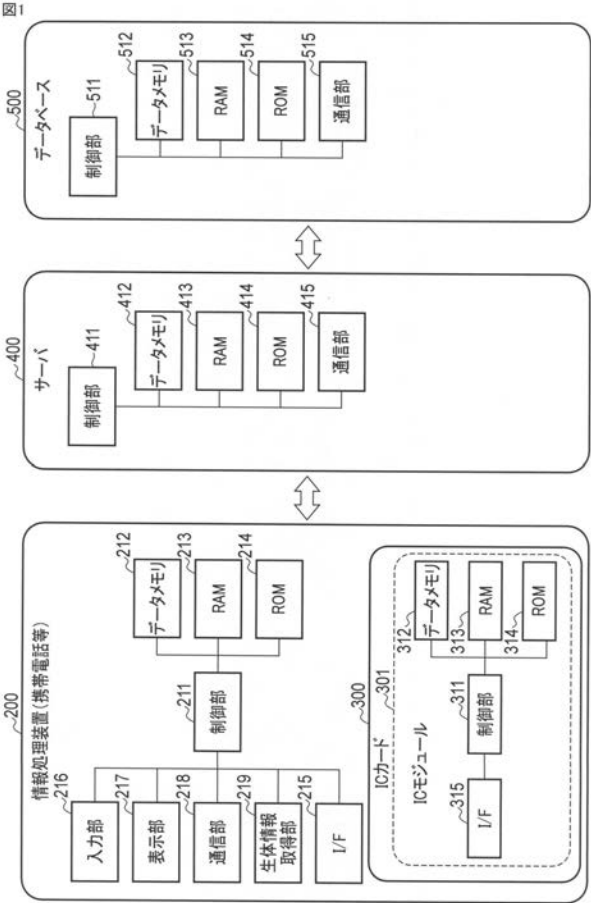
【符号の説明】

【0060】

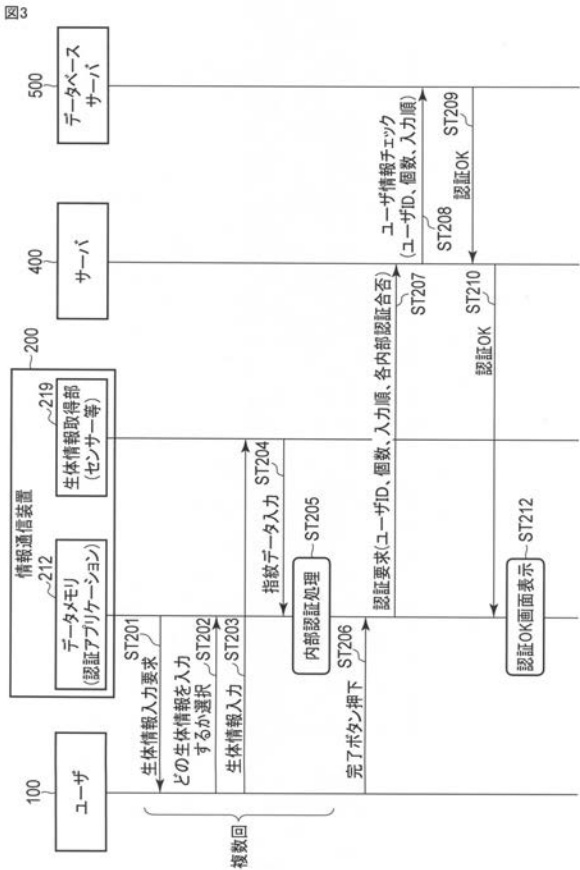
200…情報処理装置、211…制御部、212…データメモリ、213…RAM、214…ROM、215…I/F、216…入力部、217…表示部、218…通信部、219…生体情報取得部、300…ICカード、311…制御部、312…データメモリ、313…RAM、314…ROM、315…I/F、400…サーバ、411…制御部、412…データメモリ、413…RAM、414…ROM、415…通信部、500…データベースサーバ、511…制御部、512…データメモリ、513…RAM、514…ROM、515…通信部。

20

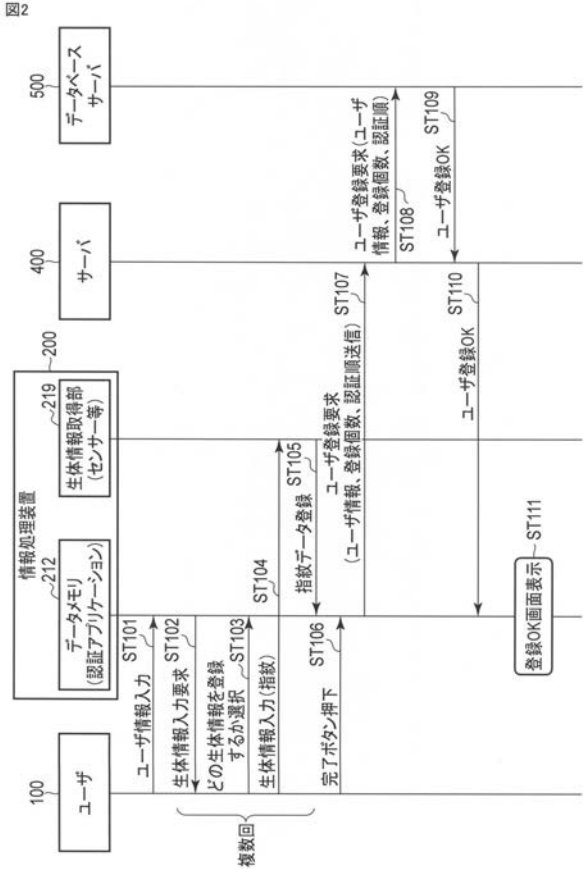
【図 1】



【図 3】



【図 2】



【図 4】

図 4

番号	ユーザID	個数	識別情報				
			1番目	2番目	3番目	...	5番目
1	XXXXX	5	右手 親指指紋	左手 薬指指紋	顔	...	右手 小指指紋
2	YYYYY	2	右手 小指指紋	左手 親指指紋	なし	...	なし

図5

番号	ユーザ ID	種類	個数	識別情報										表示可能項目
				1番目		2番目		3番目		4番目		5番目		
				対象	希望結果	対象	希望結果	対象	希望結果	対象	希望結果	対象	希望結果	
1	XXXXX	第1認証	3	右手・親指指紋	成功	左手・薬指指紋	成功	顔画像	成功	-	-	-	-	A
2	XXXXX	第2認証	5	右手・親指指紋	成功	左手・薬指指紋	成功	顔画像	成功	左手・小指指紋	失敗	右手・小指指紋	成功	AB

フロントページの続き

(74)代理人 100189913

弁理士 鵜飼 健

(72)発明者 岩崎 研吾

神奈川県川崎市幸区小向東芝町 1 番地 東芝ソシオシステムズ株式会社内

(72)発明者 三浦 秀三

東京都港区芝浦一丁目 1 番 1 号 株式会社東芝内