(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2024-60344
(P2024-60344A)
(43)公開日　令和6年5月2日(2024.5.2)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/32	*(2013.01)*	G06F	21/32	
H04L 9/32	*(2006.01)*	H04L	9/32	100D

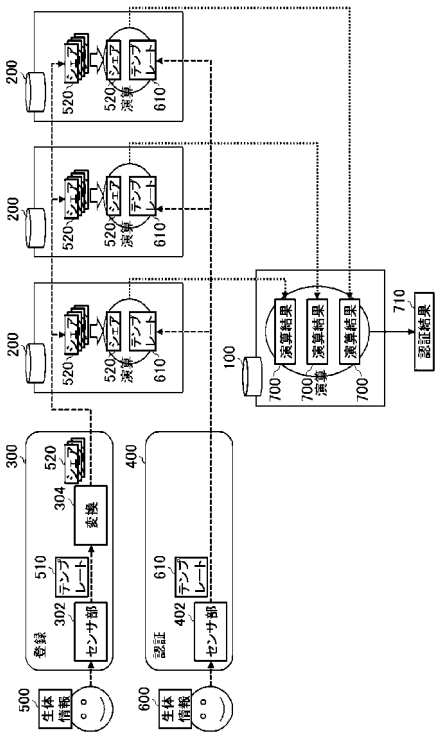
審査請求 有　請求項の数 8　ＯＬ　（全 28 頁）

(21)出願番号　特願2022-167663(P2022-167663)
(22)出願日　令和4年10月19日(2022.10.19)

(71)出願人　501440684
ソフトバンク株式会社
東京都港区海岸一丁目７番１号
(74)代理人　110000877
弁理士法人ＲＹＵＫＡ国際特許事務所
(72)発明者　太田　秀典
東京都港区海岸一丁目７番１号　ソフトバンク株式会社内

(54)【発明の名称】認証システム及び認証方法

(57)【要約】　（修正有）
【課題】ユーザの顔画像を取得して顔画像に含まれる特徴点に関する情報を用いてユーザを認証するシステム及び方法を提供する。
【解決手段】認証システムは、メインサーバ１００と、登録されている人の生体情報から生成されたテンプレートを用いて生成された複数のシェアの夫々を各々が記憶する複数のサブサーバ２００と、を含む。各サブサーバは夫々、シェアを記憶するシェア記憶部、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信部と、テンプレート受信部が受信したテンプレート、シェア記憶部に記憶されているシェアとを用いた演算を実行する演算実行部及び演算実行部による演算結果をメインサーバに送信する演算結果送信部を有する。メインサーバは、サブサーバ夫々から演算結果を受信する演算結果受信部及び演算結果受信部が受信した複数の演算結果を用いて、認証対象の人の認証結果を決定する認証結果決定部を有する。
【選択図】図２



【特許請求の範囲】
【請求項１】
認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信部と、
前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有する、認証システム。
【請求項２】
前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、
前記演算実行部は、前記認証対象の人の前記テンプレートと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、
前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、
前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、
前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項１に記載の認証システム。
【請求項３】
前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項１に記載の認証システム。
【請求項４】
前記第１サーバ及び前記複数の第２サーバは、登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出することによって、前記認証対象の人の認証結果を決定する、請求項１に記載の認証システム。
【請求項５】
前記複数の第２サーバのそれぞれの前記演算実行部は、前記コサイン類似度を算出するための一部の演算を実行し、
前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出する、請求項４に記載の認証システム。
【請求項６】
第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される認証方法であっ

て、
前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶する記憶段階と、
前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信段階と、
前記複数の第２サーバのそれぞれが、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、
前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、
前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、
前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と
を備える、認証方法。
【請求項７】
認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信部と、
前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有する、認証システム。
【請求項８】
前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、
前記演算実行部は、前記シェア受信部が受信した前記認証対象の人の前記シェアと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、
前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、
前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、
前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項７に記載の認証システム。
【請求項９】
前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項７に記載の認証システム。

【請求項１０】
前記第１サーバ及び前記複数の第２サーバは、登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出することによって、前記認証対象の人の認証結果を決定する、請求項７に記載の認証システム。
【請求項１１】
前記複数の第２サーバのそれぞれの前記演算実行部は、前記ユークリッド距離を算出するための一部の演算を実行し、
前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出する、請求項１０に記載の認証システム。
【請求項１２】
第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される認証方法であって、
前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶するシェア記憶段階と、
前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信段階と、
前記複数の第２サーバのそれぞれが、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、
前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、
前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、
前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と
を備える、認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証システム及び認証方法に関する。
【背景技術】
【０００２】
特許文献１には、ユーザの顔画像を取得し、顔画像に含まれる特徴点に関する情報を用いてユーザを認証する技術が記載されている。
［先行技術文献］
［特許文献］
［特許文献１］特開２０２１－１７０２０５号公報
【発明の概要】
【課題を解決するための手段】
【０００３】
本発明の一実施態様によれば、認証システムが提供される。前記認証システムは、第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとを備えてよい。前記複数の第２サーバのそれぞれは、前記シェアを記憶するシェア記憶部を有してよい。前記複数の第２サーバのそれぞれは、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信部を有してよい。前記複数の第２サーバのそれぞれは、前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演

算を実行する演算実行部を有してよい。前記複数の第２サーバのそれぞれは、前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部を有してよい。前記第１サーバは、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部を有してよい。前記第１サーバは、前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部を有してよい。

【０００４】

前記認証システムにおいて、前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶してよく、前記演算実行部は、前記認証対象の人の前記テンプレートと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行してよく、前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信してよく、前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信してよく、前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定してよい。

【０００５】

前記いずれかの認証システムにおいて、前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶してよい。

【０００６】

前記いずれかの認証システムにおいて、前記第１サーバ及び前記複数の第２サーバは、登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出することによって、前記認証対象の人の認証結果を決定してよい。前記複数の第２サーバのそれぞれの前記演算実行部は、前記コサイン類似度を算出するための一部の演算を実行してよく、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出してよい。

【０００７】

本発明の一実施態様によれば、認証方法が提供される。前記認証方法は、第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行されてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶する記憶段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階を備えてよい。前記認証方法は、前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階を備えてよい。前記認証方法は、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階を備えてよい。

【０００８】

本発明の一実施態様によれば、認証システムが提供される。前記認証システムは、第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとを備えてよい。前記複数の第２サーバのそれぞれは、前記シェアを記憶するシェア記憶部を有してよい。前記複数の第２サーバのそれぞれは、認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信部を有してよい。前記複数の第２サーバのそれぞ

れは、前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部を有してよい。前記複数の第２サーバのそれぞれは、前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部を有してよい。前記第１サーバは、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部を有してよい。前記第１サーバは、前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部を有してよい。

【０００９】

前記認証システムにおいて、前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶してよく、前記演算実行部は、前記シェア受信部が受信した前記認証対象の人の前記シェアと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行してよく、前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信してよく、前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信してよく、前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定してよい。

【００１０】

前記いずれかの認証システムにおいて、前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶してよい。

【００１１】

前記いずれかの認証システムにおいて、前記第１サーバ及び前記複数の第２サーバは、登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出することによって、前記認証対象の人の認証結果を決定してよい。前記複数の第２サーバのそれぞれの前記演算実行部は、前記ユークリッド距離を算出するための一部の演算を実行してよく、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出してよい。

【００１２】

本発明の一実施態様によれば、認証方法が提供される。前記認証方法は、第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行されてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶するシェア記憶段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階を備えてよい。前記認証方法は、前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階を備えてよい。前記認証方法は、前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階を備えてよい。　前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階を備えてよい。

【００１３】

なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

【図面の簡単な説明】

【００１４】

【図１】認証システム１０の一例を概略的に示す。
【図２】認証システム１０における処理の流れの一例を概略的に示す。
【図３】認証システム１０における演算内容について説明するための説明図である。
【図４】サブサーバ２００の機能構成の一例を概略的に示す。
【図５】メインサーバ１００の機能構成の一例を概略的に示す。
【図６】認証システム１０における処理の流れの一例を概略的に示す。
【図７】認証システム１０における演算内容について説明するための説明図である。
【図８】サブサーバ２００の機能構成の一例を概略的に示す。
【図９】メインサーバ１００の機能構成の一例を概略的に示す。
【図１０】メインサーバ１００、サブサーバ２００、登録クライアント３００、又は認証クライアント４００として機能するコンピュータ１２００のハードウェア構成の一例を概略的に示す。
【発明を実施するための形態】
【００１５】
従来の生体認証システムでは、人間の身体的特徴や行動的特徴を示す生体データを暗号化した状態でサーバに保存しているが、認証時に生体データを復号化することになり、復号化したときに生体データが盗まれるおそれがある。生体データを変換したまま認証を行うキャンセラブルバイオメトリクスの技術が開発されているが、その多くは、認証精度が悪化したり、長い認証時間を必要とするものである。そのため、変換された生体データであっても、漏洩時に元の生体データが復元されるおそれがあるので、秘密分散技術によってデータを複数のサーバに分割保存し、漏洩時のリスクを低減できることが望ましい。秘密分散技術によれば、一部のサーバからデータが漏洩しても、データを復元できないので、攻撃者は複数のサーバからデータを得なくてはならなくなり、結果として安全性が高まる。本実施形態に係る認証システム１０は、生体認証において、秘密分散を用いたデータ変化を行い、変換した状態で、高速、かつ、認証精度を悪化させない認証を行えるセキュアな技術を提供する。
【００１６】
以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではない。また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。
【００１７】
図１は、認証システム１０の一例を概略的に示す。認証システム１０は、秘密分散を用いた生体認証システムであってよい。
【００１８】
認証システム１０は、メインサーバ１００及び複数のサブサーバ２００を備える。メインサーバ１００は、第１サーバの一例であってよい。サブサーバ２００は、第２サーバの一例であってよい。
【００１９】
認証システム１０は、登録クライアント３００を更に備えてもよい。認証システム１０は、認証クライアント４００を更に備えてもよい。
【００２０】
メインサーバ１００、サブサーバ２００、登録クライアント３００、及び認証クライアント４００は、ネットワーク２０を介して通信してよい。ネットワーク２０は、インターネットを含んでよい。ネットワーク２０は、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）を含んでよい。ネットワーク２０は、移動体通信ネットワークを含んでよい。移動体通信ネットワークは、５Ｇ（５ｔｈ Ｇｅｎｅｒａｔｉｏｎ）通信方式、ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）通信方式、３Ｇ（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ）通信方式、及び６Ｇ（６ｔｈ Ｇｅｎｅｒａｔｉｏｎ）通信方式以降の通信方式のいずれに準拠していてもよい。
【００２１】

メインサーバ１００は、ネットワーク２０に有線接続されてよい。メインサーバ１００は、ネットワーク２０に無線接続されてもよい。メインサーバ１００は、無線基地局を介してネットワーク２０に接続されてよい。メインサーバ１００は、Ｗｉ－Ｆｉ（登録商標）アクセスポイントを介してネットワーク２０に接続されてよい。メインサーバ１００は、いわゆるサーバ装置によって構成されてよい。メインサーバ１００は、任意の装置上で実現されたサーバであってもよい。

【００２２】

サブサーバ２００は、ネットワーク２０に有線接続されてよい。サブサーバ２００は、ネットワーク２０に無線接続されてもよい。サブサーバ２００は、無線基地局を介してネットワーク２０に接続されてよい。サブサーバ２００は、Ｗｉ－Ｆｉアクセスポイントを介してネットワーク２０に接続されてよい。サブサーバ２００は、いわゆるサーバ装置によって構成されてよい。サブサーバ２００は、任意の装置上で実現されたサーバであってもよい。

【００２３】

登録クライアント３００は、ネットワーク２０に有線接続されてよい。登録クライアント３００は、ネットワーク２０に無線接続されてもよい。登録クライアント３００は、無線基地局を介してネットワーク２０に接続されてよい。登録クライアント３００は、Ｗｉ－Ｆｉアクセスポイントを介してネットワーク２０に接続されてよい。登録クライアント３００は、任意の装置であってよい。例えば、登録クライアント３００は、スマートフォン、タブレット端末、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）、登録専用端末、及びサーバ装置等であってよい。

【００２４】

認証クライアント４００は、ネットワーク２０に有線接続されてよい。認証クライアント４００は、ネットワーク２０に無線接続されてもよい。認証クライアント４００は、無線基地局を介してネットワーク２０に接続されてよい。認証クライアント４００は、Ｗｉ－Ｆｉアクセスポイントを介してネットワーク２０に接続されてよい。認証クライアント４００は、任意の装置であってよい。例えば、認証クライアント４００は、スマートフォン、タブレット端末、ＰＣ、認証専用端末、及びサーバ装置等であってよい。

【００２５】

登録クライアント３００は、登録対象の人５０の生体情報をセンサによって取得して、人５０の認証に用いる情報を認証システム１０に送信する。

【００２６】

例えば、登録クライアント３００が、人５０の生体情報からテンプレートを生成し、テンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ２００のそれぞれに送信する。テンプレートは、生体情報の特徴を表す多次元ベクトルの特徴量データである。複数のサブサーバ２００のそれぞれは、受信したシェアを記憶する。どのシェアがどのサブサーバ２００に記憶されているかは、メインサーバ１００によって管理されてよい。

【００２７】

代替例として、登録クライアント３００が、人５０の生体情報からテンプレートを生成して、メインサーバ１００に送信してもよい。メインサーバ１００は、受信したテンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ２００のそれぞれに送信する。なお、これに限らず、登録クライアント３００が、人５０の生体情報からテンプレートを生成して、任意の装置に送信し、当該任意の装置が、受信したテンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ２００のそれぞれに送信してもよい。

【００２８】

代替例として、登録クライアント３００が、人５０の生体情報をメインサーバ１００に送信してもよい。メインサーバ１００は、受信した生体情報からテンプレートを生成し、テンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ

２００のそれぞれに送信する。なお、これに限らず、登録クライアント３００が、人５０の生体情報を、任意の装置に送信し、当該任意の装置が、受信した生体情報からテンプレートを生成し、テンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ２００のそれぞれに送信してもよい。また、登録クライアント３００が、人５０の生体情報を、任意の第１の装置に送信し、当該第１の装置が、受信した生体情報からテンプレートを生成して、任意の第２の装置に送信し、当該第２の装置が、テンプレートから複数のシェアを生成して、複数のシェアのそれぞれを複数のサブサーバ２００のそれぞれに送信してもよい。

【００２９】

認証クライアント４００は、認証対象の人６０の生体情報をセンサによって取得して、人６０の認証に用いる情報を認証システム１０に送信する。例えば、認証クライアント４００は、人６０の生体情報からテンプレートを生成して、複数のサブサーバ２００のそれぞれに送信する。例えば、認証クライアント４００は、人６０の生体情報からテンプレートを生成し、テンプレートから複数のシェアを生成して、複数のサブサーバ２００のそれぞれに送信する。

【００３０】

認証システム１０は、秘密分散を用いた生体認証を実行する。例えば、分散数を３とした場合、元データから第１ハッシュ値及び第２ハッシュ値を減算した値と、第１ハッシュ値と、第２ハッシュ値とを、３つのシェアとして、３つのサブサーバ２００で分散管理する。

【００３１】

認証システム１０は、例えば、ＩＳＯ／ＩＥＣ １９５９２－２：２０１７における５つの方式のいずれかを用いてよい。例えば、認証システム１０は、「Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ」を用いる。認証システム１０は、「Ｒｅｐｌｉｃａｔｅｄ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ」を用いてもよい。認証システム１０は、「Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ」を用いてもよい。認証システム１０は、「Ｒａｍｐ Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ」を用いてもよい。なお、認証システム１０は、「Ｃｏｍｐｕｔａｔｉｏｎａｌ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ」を用いてもよい。本実施形態では、認証システム１０が「Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ」を用いる場合について主に説明する。

【００３２】

認証システム１０は、結果的に、認証対象の人６０のテンプレートと、登録されているテンプレートとの類似度を算出することによって、人６０の認証結果を決定する。認証システム１０は、例えば、認証対象の人６０のテンプレートと、登録されているテンプレートとのコサイン類似度を算出することによって、人６０の認証結果を決定する。

【００３３】

本例において、テンプレートは、ｄ次元ベクトルの特徴量データであり、正規化されているものとする。登録されているテンプレートを下記数式１、人６０のテンプレートを下記数式２で表すと、コサイン類似度は下記数式３によって算出することができる。ｄはベクトル次元数である。

【００３４】

【数１】

$$\vec{x} = (x_1, x_2, x_3, \cdots, x_d)$$

【００３５】

【数２】

$$\vec{y} = (y_1, y_2, y_3, \cdots, y_d)$$

【００３６】
【数３】

$$\cos(\vec{x}, \vec{y}) = \sum_{i=1}^{d} x_i \cdot y_i$$

【００３７】
認証システム１０は、例えば、テンプレート同士のユークリッド距離を算出する。登録されているテンプレートを上記数式１、人６０のテンプレートを上記数式２で表すと、ユークリッド距離は下記数式４によって算出することができる。
【００３８】
【数４】

$$\|\vec{x} - \vec{y}\| = \sqrt{\sum_{i=1}^{d} (x_i - y_i)^2}$$

【００３９】
なお、本実施形態では、認証システム１０が、コサイン類似度を用いる場合と、ユークリッド距離を用いる場合とを主に例に挙げて説明するが、これに限られず、認証システム１０は、マハラノビス距離及びハミング距離等の、他のデータ距離や、他の類似度を用いてもよい。
【００４０】
図２は、認証システム１０における処理の流れの一例を概略的に示す。ここでは、認証システム１０がコサイン類似度を用いる場合の処理の流れについて説明する。
【００４１】
登録クライアント３００は、センサ部３０２及び変換部３０４を備える。センサ部３０２は、登録対象の人５０の生体情報５００を取得して、生体情報５００からテンプレート５１０を生成する。変換部３０４は、テンプレート５１０から複数のシェア５２０を生成して、複数のシェア５２０のそれぞれを、複数のサブサーバ２００のそれぞれに送信する。変換部３０４は、任意の暗号化手法を用いて暗号化した上で、複数のシェア５２０のそれぞれを複数のサブサーバ２００のそれぞれに送信してよい。複数のシェア５２０のそれぞれの送信先は、例えば、メインサーバ１００によって予め指定される。
【００４２】
複数のサブサーバ２００のそれぞれは、登録クライアント３００から受信したシェア５２０を記憶する。サブサーバ２００は、一の登録クライアント３００から複数の人５０のシェア５２０を受信したり、複数の登録クライアント３００からシェア５２０を受信したりすることによって、複数の人５０のそれぞれについて、複数のシェア５２０のうちの１つを記憶する。このように、複数のサブサーバ２００が、複数の人５０のそれぞれの複数のシェア５２０を分散して記憶する。
【００４３】
認証クライアント４００は、センサ部４０２を備える。センサ部４０２は、認証対象の人６０の生体情報６００を取得して、生体情報６００からテンプレート６１０を生成する。センサ部４０２は、テンプレート６１０を複数のサブサーバ２００のそれぞれに送信する。センサ部４０２は、任意の暗号化手法を用いて暗号化した上で、テンプレート６１０

を複数のサブサーバ２００のそれぞれに送信してよい。

【００４４】

複数のサブサーバ２００のそれぞれは、認証クライアント４００から受信したテンプレート６１０と、記憶している複数のシェア５２０のそれぞれとに対する演算を実行する。複数のサブサーバ２００のそれぞれは、テンプレート５１０とテンプレート６１０とのコサイン類似度を算出するための演算の一部を実行する。複数のサブサーバ２００のそれぞれは、演算結果７００をメインサーバ１００に送信する。

【００４５】

メインサーバ１００は、複数のサブサーバ２００のそれぞれから受信した演算結果７００を用いて、人６０の認証結果７１０を決定する。メインサーバ１００は、複数の演算結果７００に対して、結果として、テンプレート５１０とテンプレート６１０とのコサイン類似度が算出されるような演算を実行する。

【００４６】

図３は、認証システム１０における演算内容について説明するための説明図である。ここでは、任意の要素ベクトルx_iが、下記数式５で表すように、複数のサブサーバ２００に秘密分散されて記憶されているものとする。Ｓは分散数を表す。

【００４７】

【数５】

$$x_i = a_{i,1}(x_i) + a_{i,2}(x_i) + a_{i,3}(x_i) \cdots + a_{i,s}(x_i)$$

【００４８】

この場合、登録されている人５０のテンプレート５１０と、認証対象の人６０のテンプレート６１０とのコサイン類似度は、図３に示す数式で表すことができる。

【００４９】

複数のサブサーバ２００のそれぞれは、図３における複数の部分演算２２０のそれぞれを実行する。メインサーバ１００は、複数のサブサーバ２００のそれぞれから部分演算２２０の演算結果７００を受信して、複数の演算結果７００を加算することによって、テンプレート５１０とテンプレート６１０とのコサイン類似度を算出することができる。

【００５０】

このように、図２及び図３に例示する認証システム１０は、一のテンプレート５１０から生成された複数のシェア５２０を複数のサブサーバ２００で分散管理しつつ、サブサーバ２００からメインサーバ１００に対してシェア５２０を送信するのではなく、演算結果７００を送信するように構成される。演算結果７００が仮に漏洩したとしても、演算結果７００からシェア５２０を予測することは基本的にできないことから、全体的なセキュリティレベルを高めることができる。

【００５１】

図４は、サブサーバ２００の機能構成の一例を概略的に示す。サブサーバ２００は、シェア取得部２０２、シェア記憶部２０４、テンプレート受信部２０６、演算実行部２０８、及び演算結果送信部２１０を備える。

【００５２】

シェア取得部２０２は、人５０の生体情報５００から生成されたテンプレート５１０から生成された複数のシェア５２０のうちの１つを取得する。シェア取得部２０２は、複数の人５０のそれぞれについて、人５０の生体情報５００から生成されたテンプレート５１０から生成された複数のシェア５２０のうちの１つを取得してよい。シェア取得部２０２は、取得したシェア５２０をシェア記憶部２０４に記憶させる。

【００５３】

複数のサブサーバ２００のそれぞれが、人５０の生体情報５００から生成されたテンプレート５１０から生成された複数のシェア５２０のそれぞれを記憶することになる。例え

ば、複数のサブサーバ２００のそれぞれが、人５０の生体情報５００から生成されたテンプレート５１０から複数のハッシュ値を減算することによって生成されたシェアと、複数のハッシュ値とを含む複数のシェア５２０のそれぞれを記憶することになる。

【００５４】

例えば、シェア取得部２０２は、登録クライアント３００からシェア５２０を取得する。シェア取得部２０２は、登録クライアント３００からネットワーク２０を介してシェア５２０を受信してよい。シェア取得部２０２は、登録クライアント３００において暗号化されたシェア５２０を受信して、復号化してよい。なお、シェア取得部２０２は、登録クライアント３００において可搬型の記憶媒体に記憶されたシェア５２０を、当該可搬型の記憶媒体から読み出すことによって取得してもよい。

【００５５】

例えば、シェア取得部２０２は、メインサーバ１００からシェア５２０を取得する。シェア取得部２０２は、メインサーバ１００からネットワーク２０を介してシェア５２０を受信してよい。メインサーバ１００は、メインサーバ１００において暗号化されたシェア５２０を受信して、復号化してよい。なお、シェア取得部２０２は、メインサーバ１００において可搬型の記憶媒体に記憶されたシェア５２０を、当該可搬型の記憶媒体から読み出すことによって取得してもよい。

【００５６】

テンプレート受信部２０６は、認証対象の人６０の生体情報６００から生成されたテンプレート６１０を受信する。例えば、テンプレート受信部２０６は、認証クライアント４００において生体情報６００から生成されたテンプレート６１０を、認証クライアント４００からネットワーク２０を介して受信する。テンプレート受信部２０６は、認証クライアント４００において暗号化されたテンプレート６１０をネットワーク２０を介して受信して、復号化してよい。

【００５７】

演算実行部２０８は、テンプレート受信部２０６が受信したテンプレート６１０と、シェア記憶部２０４に記憶されているシェア５２０とを用いた演算を実行する。演算実行部２０８は、図３で例示した、テンプレート６１０とテンプレート５１０とのコサイン類似度を算出するための部分演算２２０を実行する。

【００５８】

１対１認証の場合、演算実行部２０８は、テンプレート受信部２０６が受信したテンプレート６１０と、シェア記憶部２０４に記憶されている１つのシェア５２０とを用いた演算を実行する。例えば、人６０が、特定の人であるかを認証する場合、テンプレート受信部２０６が受信したテンプレート６１０と、当該特定の人のシェア５２０とを用いた演算を実行する。１対多認証の場合、演算実行部２０８は、テンプレート受信部２０６が受信したテンプレート６１０と、シェア記憶部２０４に記憶されている複数のシェア５２０のそれぞれとを用いた演算を実行する。

【００５９】

演算結果送信部２１０は、演算実行部２０８による演算結果７００をメインサーバ１００に送信する。演算結果送信部２１０は、演算結果７００を暗号化してネットワーク２０を介してメインサーバ１００に送信してよい。

【００６０】

図５は、メインサーバ１００の機能構成の一例を概略的に示す。メインサーバ１００は、対応関係管理部１０２、演算結果受信部１０４、認証結果決定部１０６、及び認証結果出力部１０８を備える。なお、メインサーバ１００がこれらの全てを備えることは必須とは限らない。

【００６１】

対応関係管理部１０２は、１つのテンプレート５１０から生成された複数のシェア５２０のそれぞれが、複数のサブサーバ２００のいずれに記憶されているかの対応関係を管理する。例えば、分散数が３である場合、対応関係管理部１０２は、１つ目のシェア５２０

と当該シェア５２０を記憶するサブサーバ２００、２つ目のシェア５２０と当該シェア５２０を記憶するサブサーバ２００、及び３つ目のシェア５２０と当該シェア５２０を記憶するサブサーバ２００との対応関係を記憶する。対応関係管理部１０２は、当該対応関係に従って、登録クライアント３００に対して、複数のシェア５２０のそれぞれの送信先のサブサーバ２００を指示してよい。

【００６２】

このように管理することによって、秘密分散による分散状況におけるコサイン類似度の計算を適切に実行することができる。また、対応関係管理部１０２が管理する対応関係を編集するだけで、サブサーバ２００を追加したり、サブサーバ２００に不具合が発生したりした場合に、容易に対応可能にすることができる。なお、メインサーバ１００が対応関係管理部１０２を備えるのではなく、他の装置が対応関係管理部１０２を備えて、メインサーバ１００が当該他の装置の対応関係管理部１０２にアクセスするようにしてもよい。

【００６３】

演算結果受信部１０４は、複数のサブサーバ２００のそれぞれから演算結果７００を受信する。演算結果受信部１０４は、暗号化された演算結果７００を受信して、復号化してよい。なお、演算結果受信部１０４は、対応関係管理部１０２を参照することによって、どのサブサーバ２００と通信するかを管理してもよい。

【００６４】

認証結果決定部１０６は、演算結果受信部１０４が受信した複数の演算結果７００を用いて、認証対象の人６０の認証結果７１０を決定する。認証結果決定部１０６は、対応関係管理部１０２を参照することによって、どのサブサーバ２００がどのシェアを記憶しているかを管理したり、各シェアのシェアの個数を管理したりしてよい。認証結果決定部１０６は、対応関係管理部１０２を参照することなく、認証結果７１０を決定してもよい。認証結果決定部１０６は、図３に示すように、複数の演算結果７００を加算することによって、テンプレート６１０とテンプレート５１０とのコサイン類似度を算出してよい。認証結果決定部１０６は、算出したコサイン類似度によって、人６０の認証結果７１０を決定する。

【００６５】

１対１認証の場合において、例えば、認証結果決定部１０６は、算出したコサイン類似度が、予め設定された閾値よりも高い場合に、認証ＯＫと判定し、閾値より低い場合に、認証ＮＧと判定する。１対多認証の場合において、例えば、認証結果決定部１０６は、算出した複数のコサイン類似度のうち予め設定された閾値より高いコサイン類似度が存在する場合、人６０が、最も高いコサイン類似度の算出に用いたシェア５２０に対応する人５０であると決定し、算出した複数のコサイン類似度の全てが予め設定された閾値よりも低い場合に、認証ＮＧと判定する。認証結果の決定方法は、これらに限られない。

【００６６】

認証結果出力部１０８は、認証結果決定部１０６によって決定された認証結果７１０を出力する。認証結果出力部１０８は、例えば、メインサーバ１００が備えるディスプレイに認証結果７１０を表示させる。認証結果出力部１０８は、例えば、ネットワーク２０を介して他の装置に認証結果７１０を送信する。例えば、認証結果出力部１０８は、ネットワーク２０を介して認証結果７１０を認証クライアント４００に送信する。

【００６７】

図６は、認証システム１０における処理の流れの一例を概略的に示す。ここでは、認証システム１０がユークリッド距離を用いる場合の処理の流れについて説明する。なお、ここでは、図２に示す認証システム１０とは異なる点を主に説明する。

【００６８】

認証クライアント４００は、センサ部４０２及び変換部４０４を備える。センサ部４０２は、認証対象の人６０の生体情報６００を取得して、生体情報６００からテンプレート６１０を生成する。変換部４０４は、テンプレート６１０から複数のシェア６２０を生成して、複数のシェア６２０のそれぞれを、複数のサブサーバ２００のそれぞれに送信する

。変換部４０４は、任意の暗号化手法を用いて暗号化した上で、複数のシェア６２０のそれぞれを複数のサブサーバ２００のそれぞれに送信してよい。複数のシェア６２０のそれぞれの送信先は、例えば、メインサーバ１００によって予め指定される。

【００６９】

複数のサブサーバ２００のそれぞれは、認証クライアント４００から受信したシェア６２０と、記憶している複数のシェア５２０のそれぞれとに対する演算を実行する。複数のサブサーバ２００のそれぞれは、テンプレート５１０とテンプレート６１０とのユークリッド距離を算出するための演算の一部を実行する。複数のサブサーバ２００のそれぞれは、演算結果７００をメインサーバ１００に送信する。

【００７０】

メインサーバ１００は、複数のサブサーバ２００のそれぞれから受信した演算結果７００を用いて、人６０の認証結果７１０を決定する。メインサーバ１００は、複数の演算結果７００に対して、結果として、テンプレート５１０とテンプレート６１０とのユークリッドが算出されるような演算を実行する。

【００７１】

図７は、認証システム１０における演算内容について説明するための説明図である。ここでは、ｄ次元ベクトルの任意の要素ベクトルｘ$_i$、ｙ$_i$が、下記数式６、数式７で表すように、複数のサブサーバ２００に秘密分散されて記憶されているものとする。Ｓは分散数を表す。

【００７２】

【数６】

$$x_i = a_{i,1}(x_i) + a_{i,2}(x_i) + a_{i,3}(x_i) \cdots + a_{i,s}(x_i)$$

【００７３】

【数７】

$$y_i = b_{i,1}(y_i) + b_{i,2}(y_i) + b_{i,3}(y_i) \cdots + b_{i,s}(y_i)$$

【００７４】

この場合、登録されている人５０のテンプレート５１０と、認証対象の人６０のテンプレート６１０とのユークリッド距離は、図７に示す数式で表すことができる。

【００７５】

複数のサブサーバ２００のそれぞれは、図７における複数の部分演算２３０のそれぞれを実行する。メインサーバ１００は、複数のサブサーバ２００のそれぞれから部分演算２３０の演算結果７００を受信して、複数の演算結果７００に対して、図７に示すように、１～ｄ次元についての、複数の演算結果７００を加算した値を２乗した値を加算した値のルートを計算することによって、テンプレート５１０とテンプレート６１０とのユークリッド距離を算出することができる。

【００７６】

このように、図６及び図７に例示する認証システム１０は、一のテンプレート５１０から生成された複数のシェア５２０を複数のサブサーバ２００で分散管理しつつ、サブサーバ２００からメインサーバ１００に対してシェア５２０を送信するのではなく、演算結果７００を送信するように構成される。演算結果７００が仮に漏洩したとしても、演算結果７００からシェア５２０を予測することは基本的にできないことから、全体的なセキュリティレベルを高めることができる。また、図６及び図７に例示する認証システム１０によれば、認証クライアント４００から複数のサブサーバ２００に対して、複数のシェア６２０を送信することになるので、認証クライアント４００から複数のサブサーバ２００に対

してテンプレート６１０を送信する場合と比較して、セキュリティを向上させることができる。

【００７７】

図８は、サブサーバ２００の機能構成の一例を概略的に示す。ここでは、図４に示すサブサーバ２００とは異なる点を主に説明する。図８に示すサブサーバ２００は、シェア受信部２１２を備える。

【００７８】

シェア受信部２１２は、認証対象の人６０の生体情報６００から生成されたテンプレート６１０から生成された複数のシェア６２０のうちの１つを受信する。例えば、シェア受信部２１２は、認証クライアント４００において生体情報６００から生成されたテンプレート６１０から生成された複数のシェア６２０のうちの１つを、サブサーバ２００からネットワーク２０を介して受信する。シェア受信部２１２は、認証クライアント４００において暗号化されたシェア６２０を、ネットワーク２０を介して受信して、復号化してよい。

【００７９】

演算実行部２０８は、シェア受信部２１２が受信したシェア６２０と、シェア記憶部２０４に記憶されているシェア５２０とを用いた演算を実行する。演算実行部２０８は、図７で例示した、テンプレート６１０とテンプレート５１０とのユークリッド距離を算出するための部分演算２３０を実行する。

【００８０】

１対１認証の場合、演算実行部２０８は、シェア受信部２１２が受信したシェア６２０と、シェア記憶部２０４に記憶されている１つのシェア５２０とを用いた演算を実行する。例えば、人６０が、特定の人であるかを認証する場合、シェア受信部２１２が受信したシェア６２０と、当該特定の人のシェア５２０とを用いた演算を実行する。１対多認証の場合、演算実行部２０８は、シェア受信部２１２が受信したシェア６２０と、シェア記憶部２０４に記憶されている複数のシェア５２０のそれぞれとを用いた演算を実行する。

【００８１】

演算結果送信部２１０は、演算実行部２０８による演算結果７００をメインサーバ１００に送信する。演算結果送信部２１０は、演算結果７００を暗号化してネットワーク２０を介してメインサーバ１００に送信してよい。

【００８２】

図９は、メインサーバ１００の機能構成の一例を概略的に示す。ここでは、図５に示すメインサーバ１００とは異なる点を主に説明する。

【００８３】

認証結果決定部１０６は、演算結果受信部１０４が受信した複数の演算結果７００を用いて、認証対象の人６０の認証結果７１０を決定する。認証結果決定部１０６は、図７に示すように、１～ｄ次元についての複数の演算結果７００を加算した値を２乗した値を、加算した値のルートを計算することによって、テンプレート５１０とテンプレート６１０とのユークリッド距離を算出してよい。認証結果決定部１０６は、算出したユークリッド距離によって、人６０の認証結果７１０を決定する。

【００８４】

１対１認証の場合において、例えば、認証結果決定部１０６は、算出したユークリッド距離が、予め設定された閾値よりも高い場合に、認証ＯＫと判定し、閾値より低い場合に、認証ＮＧと判定する。１対多認証の場合において、例えば、認証結果決定部１０６は、算出した複数のユークリッド距離のうち予め設定された閾値より高いユークリッド距離が存在する場合、人６０が、最も高いユークリッド距離の算出に用いたシェア５２０に対応する人５０であると決定し、算出した複数のユークリッド距離の全てが予め設定された閾値よりも低い場合に、認証ＮＧと判定する。認証結果の決定方法は、これらに限られない。

【００８５】

図１０は、メインサーバ１００、サブサーバ２００、登録クライアント３００又は認証クライアント４００として機能するコンピュータ１２００のハードウェア構成の一例を概略的に示す。コンピュータ１２００にインストールされたプログラムは、コンピュータ１２００を、本実施形態に係る装置の１又は複数の「部」として機能させ、又はコンピュータ１２００に、本実施形態に係る装置に関連付けられるオペレーション又は当該１又は複数の「部」を実行させることができ、及び／又はコンピュータ１２００に、本実施形態に係るプロセス又は当該プロセスの段階を実行させることができる。そのようなプログラムは、コンピュータ１２００に、本明細書に記載のフローチャート及びブロック図のブロックのうちのいくつか又はすべてに関連付けられた特定のオペレーションを実行させるべく、ＣＰＵ１２１２によって実行されてよい。

【００８６】

本実施形態によるコンピュータ１２００は、ＣＰＵ１２１２、ＲＡＭ１２１４、及びグラフィックコントローラ１２１６を含み、それらはホストコントローラ１２１０によって相互に接続されている。コンピュータ１２００はまた、通信インタフェース１２２２、記憶装置１２２４、ＤＶＤドライブ、及びＩＣカードドライブのような入出力ユニットを含み、それらは入出力コントローラ１２２０を介してホストコントローラ１２１０に接続されている。ＤＶＤドライブは、ＤＶＤ－ＲＯＭドライブ及びＤＶＤ－ＲＡＭドライブ等であってよい。記憶装置１２２４は、ハードディスクドライブ及びソリッドステートドライブ等であってよい。コンピュータ１２００はまた、ＲＯＭ１２３０及びキーボードのようなレガシの入出力ユニットを含み、それらは入出力チップ１２４０を介して入出力コントローラ１２２０に接続されている。

【００８７】

ＣＰＵ１２１２は、ＲＯＭ１２３０及びＲＡＭ１２１４内に格納されたプログラムに従い動作し、それにより各ユニットを制御する。グラフィックコントローラ１２１６は、ＲＡＭ１２１４内に提供されるフレームバッファ等又はそれ自体の中に、ＣＰＵ１２１２によって生成されるイメージデータを取得し、イメージデータがディスプレイデバイス１２１８上に表示されるようにする。

【００８８】

通信インタフェース１２２２は、ネットワークを介して他の電子デバイスと通信する。記憶装置１２２４は、コンピュータ１２００内のＣＰＵ１２１２によって使用されるプログラム及びデータを格納する。ＤＶＤドライブは、プログラム又はデータをＤＶＤ－ＲＯＭ等から読み取り、記憶装置１２２４に提供する。ＩＣカードドライブは、プログラム及びデータをＩＣカードから読み取り、及び／又はプログラム及びデータをＩＣカードに書き込む。

【００８９】

ＲＯＭ１２３０はその中に、アクティブ化時にコンピュータ１２００によって実行されるブートプログラム等、及び／又はコンピュータ１２００のハードウェアに依存するプログラムを格納する。入出力チップ１２４０はまた、様々な入出力ユニットをＵＳＢポート、パラレルポート、シリアルポート、キーボードポート、マウスポート等を介して、入出力コントローラ１２２０に接続してよい。

【００９０】

プログラムは、ＤＶＤ－ＲＯＭ又はＩＣカードのようなコンピュータ可読記憶媒体によって提供される。プログラムは、コンピュータ可読記憶媒体から読み取られ、コンピュータ可読記憶媒体の例でもある記憶装置１２２４、ＲＡＭ１２１４、又はＲＯＭ１２３０にインストールされ、ＣＰＵ１２１２によって実行される。これらのプログラム内に記述される情報処理は、コンピュータ１２００に読み取られ、プログラムと、上記様々なタイプのハードウェアリソースとの間の連携をもたらす。装置又は方法が、コンピュータ１２００の使用に従い情報のオペレーション又は処理を実現することによって構成されてよい。

【００９１】

例えば、通信がコンピュータ１２００及び外部デバイス間で実行される場合、ＣＰＵ１

２１２は、ＲＡＭ１２１４にロードされた通信プログラムを実行し、通信プログラムに記述された処理に基づいて、通信インタフェース１２２２に対し、通信処理を命令してよい。通信インタフェース１２２２は、ＣＰＵ１２１２の制御の下、ＲＡＭ１２１４、記憶装置１２２４、ＤＶＤ－ＲＯＭ、又はＩＣカードのような記録媒体内に提供される送信バッファ領域に格納された送信データを読み取り、読み取られた送信データをネットワークに送信し、又はネットワークから受信した受信データを記録媒体上に提供される受信バッファ領域等に書き込む。

【００９２】

また、ＣＰＵ１２１２は、記憶装置１２２４、ＤＶＤドライブ（ＤＶＤ－ＲＯＭ）、ＩＣカード等のような外部記録媒体に格納されたファイル又はデータベースの全部又は必要な部分がＲＡＭ１２１４に読み取られるようにし、ＲＡＭ１２１４上のデータに対し様々なタイプの処理を実行してよい。ＣＰＵ１２１２は次に、処理されたデータを外部記録媒体にライトバックしてよい。

【００９３】

様々なタイプのプログラム、データ、テーブル、及びデータベースのような様々なタイプの情報が記録媒体に格納され、情報処理を受けてよい。ＣＰＵ１２１２は、ＲＡＭ１２１４から読み取られたデータに対し、本開示の随所に記載され、プログラムの命令シーケンスによって指定される様々なタイプのオペレーション、情報処理、条件判断、条件分岐、無条件分岐、情報の検索／置換等を含む、様々なタイプの処理を実行してよく、結果をＲＡＭ１２１４に対しライトバックする。また、ＣＰＵ１２１２は、記録媒体内のファイル、データベース等における情報を検索してよい。例えば、各々が第２の属性の属性値に関連付けられた第１の属性の属性値を有する複数のエントリが記録媒体内に格納される場合、ＣＰＵ１２１２は、当該複数のエントリの中から、第１の属性の属性値が指定されている条件に一致するエントリを検索し、当該エントリ内に格納された第２の属性の属性値を読み取り、それにより予め定められた条件を満たす第１の属性に関連付けられた第２の属性の属性値を取得してよい。

【００９４】

上で説明したプログラム又はソフトウエアモジュールは、コンピュータ１２００上又はコンピュータ１２００近傍のコンピュータ可読記憶媒体に格納されてよい。また、専用通信ネットワーク又はインターネットに接続されたサーバシステム内に提供されるハードディスク又はＲＡＭのような記録媒体が、コンピュータ可読記憶媒体として使用可能であり、それによりプログラムを、ネットワークを介してコンピュータ１２００に提供する。

【００９５】

本実施形態におけるフローチャート及びブロック図におけるブロックは、オペレーションが実行されるプロセスの段階又はオペレーションを実行する役割を持つ装置の「部」を表わしてよい。特定の段階及び「部」が、専用回路、コンピュータ可読記憶媒体上に格納されるコンピュータ可読命令と共に供給されるプログラマブル回路、及び／又はコンピュータ可読記憶媒体上に格納されるコンピュータ可読命令と共に供給されるプロセッサによって実装されてよい。専用回路は、デジタル及び／又はアナログハードウェア回路を含んでよく、集積回路（ＩＣ）及び／又はディスクリート回路を含んでよい。プログラマブル回路は、例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、及びプログラマブルロジックアレイ（ＰＬＡ）等のような、論理積、論理和、排他的論理和、否定論理積、否定論理和、及び他の論理演算、フリップフロップ、レジスタ、並びにメモリエレメントを含む、再構成可能なハードウェア回路を含んでよい。

【００９６】

コンピュータ可読記憶媒体は、適切なデバイスによって実行される命令を格納可能な任意の有形なデバイスを含んでよく、その結果、そこに格納される命令を有するコンピュータ可読記憶媒体は、フローチャート又はブロック図で指定されたオペレーションを実行するための手段を作成すべく実行され得る命令を含む、製品を備えることになる。コンピュータ可読記憶媒体の例としては、電子記憶媒体、磁気記憶媒体、光記憶媒体、電磁記憶媒

体、半導体記憶媒体等が含まれてよい。コンピュータ可読記憶媒体のより具体的な例としては、フロッピー（登録商標）ディスク、ディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、消去可能プログラマブルリードオンリメモリ（ＥＰＲＯＭ又はフラッシュメモリ）、電気的消去可能プログラマブルリードオンリメモリ（ＥＥＰＲＯＭ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、コンパクトディスクリードオンリメモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、ブルーレイ（登録商標）ディスク、メモリスティック、集積回路カード等が含まれてよい。

【００９７】

コンピュータ可読命令は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、又はＳｍａｌｌｔａｌｋ（登録商標）、ＪＡＶＡ（登録商標）、Ｃ＋＋等のようなオブジェクト指向プログラミング言語、及び「Ｃ」プログラミング言語又は同様のプログラミング言語のような従来の手続型プログラミング言語を含む、１又は複数のプログラミング言語の任意の組み合わせで記述されたソースコード又はオブジェクトコードのいずれかを含んでよい。

【００９８】

コンピュータ可読命令は、汎用コンピュータ、特殊目的のコンピュータ、若しくは他のプログラム可能なデータ処理装置のプロセッサ、又はプログラマブル回路が、フローチャート又はブロック図で指定されたオペレーションを実行するための手段を生成するために当該コンピュータ可読命令を実行すべく、ローカルに又はローカルエリアネットワーク（ＬＡＮ）、インターネット等のようなワイドエリアネットワーク（ＷＡＮ）を介して、汎用コンピュータ、特殊目的のコンピュータ、若しくは他のプログラム可能なデータ処理装置のプロセッサ、又はプログラマブル回路に提供されてよい。プロセッサの例としては、コンピュータプロセッサ、処理ユニット、マイクロプロセッサ、デジタル信号プロセッサ、コントローラ、マイクロコントローラ等を含む。

【００９９】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることが可能であることが当業者に明らかである。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【０１００】

特許請求の範囲、明細書、及び図面中において示した装置、システム、プログラム、及び方法における動作、手順、ステップ、及び段階などの各処理の実行順序は、特段「より前に」、「先立って」などと明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。特許請求の範囲、明細書、及び図面中の動作フローに関して、便宜上「まず、」、「次に、」などを用いて説明したとしても、この順で実施することが必須であることを意味するものではない。

【０１０１】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることが可能であることが当業者に明らかである。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【０１０２】

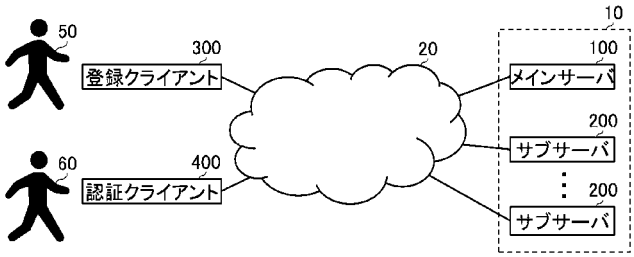
特許請求の範囲、明細書、及び図面中において示した装置、システム、プログラム、及び方法における動作、手順、ステップ、及び段階などの各処理の実行順序は、特段「より前に」、「先立って」などと明示しておらず、また、前の処理の出力を後の処理で用いるのでない限り、任意の順序で実現しうることに留意すべきである。特許請求の範囲、明細書、及び図面中の動作フローに関して、便宜上「まず、」、「次に、」などを用いて説明したとしても、この順で実施することが必須であることを意味するものではない。

【符号の説明】

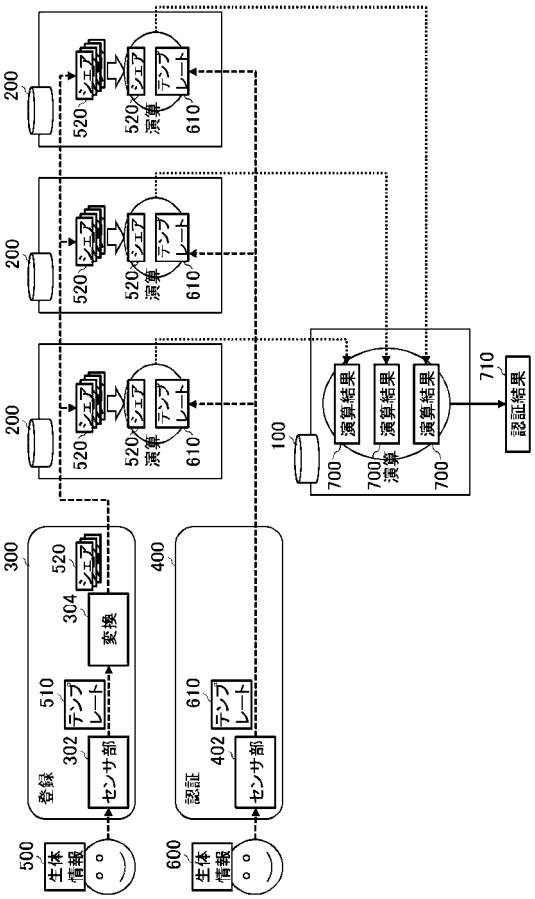
【０１０３】

１０　認証システム、２０　ネットワーク、５０　人、６０　人、１００　メインサーバ、１０２　対応関係管理部、１０４　演算結果受信部、１０６　認証結果決定部、１０８　認証結果出力部、２００　サブサーバ、２０２　シェア取得部、２０４　シェア記憶部、２０６　テンプレート受信部、２０８　演算実行部、２１０　演算結果送信部、２１２　シェア受信部、２２０　部分演算、２３０　部分演算、３００　登録クライアント、３０２　センサ部、３０４　変換部、４００　認証クライアント、４０２　センサ部、４０４　変換部、５００　生体情報、５１０　テンプレート、５２０　シェア、６００　生体情報、６１０　テンプレート、６２０　シェア、７００　演算結果、７１０　認証結果、１２００　コンピュータ、１２１０　ホストコントローラ、１２１２　ＣＰＵ、１２１４　ＲＡＭ、１２１６　グラフィックコントローラ、１２１８　ディスプレイデバイス、１２２０　入出力コントローラ、１２２２　通信インタフェース、１２２４　記憶装置、１２３０　ＲＯＭ、１２４０　入出力チップ

【図１】



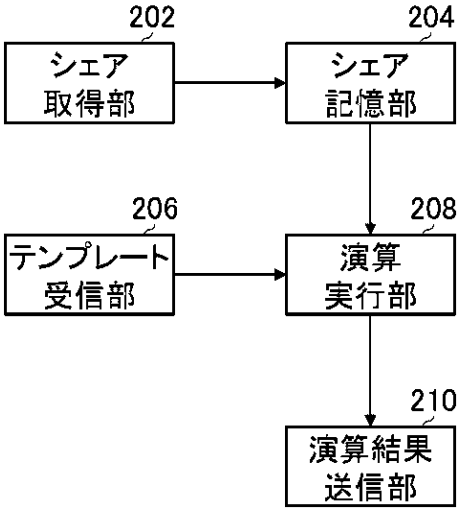
【図２】



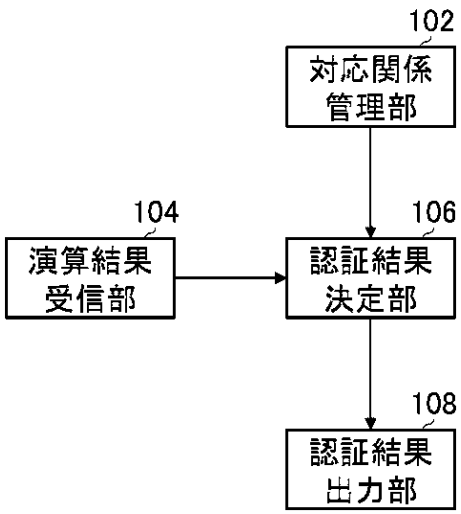
【図３】

$$\cos(\vec{x},\vec{y}) = \sum_{i=1}^{d} x_i \cdot y_i = \sum_{i=1}^{d} \left(a_{i,1}(x_i) + a_{i,2}(x_i) + a_{i,3}(x_i) \cdots + a_{i,s}(x_i)\right) \cdot y_i = \underbrace{\sum_{i=1}^{d} a_{i,1}(x_i) \cdot y_i}_{220} + \underbrace{\sum_{i=1}^{d} a_{i,2}(x_i) \cdot y_i}_{220} + \underbrace{\sum_{i=1}^{d} a_{i,3}(x_i) \cdot y_i}_{220} \cdots + \underbrace{\sum_{i=1}^{d} a_{i,s}(x_i) \cdot y_i}_{220}$$

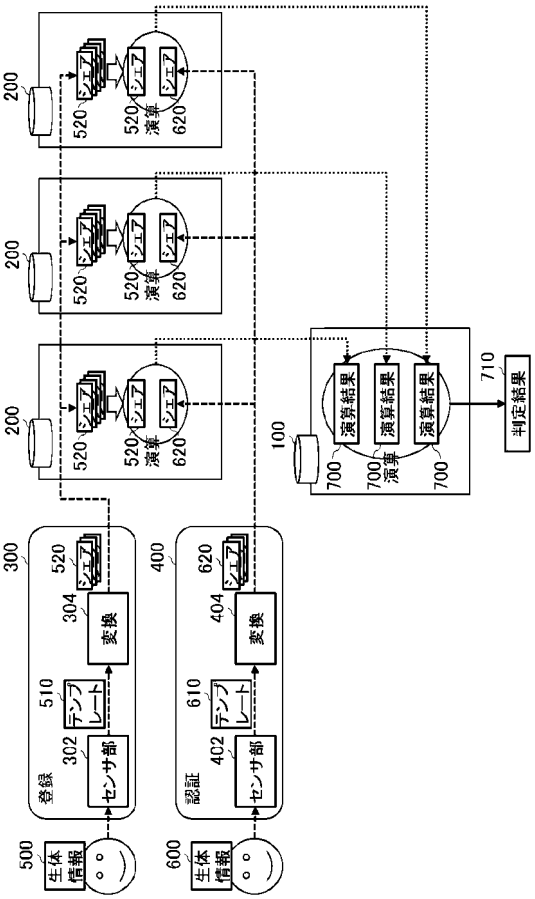
【図４】



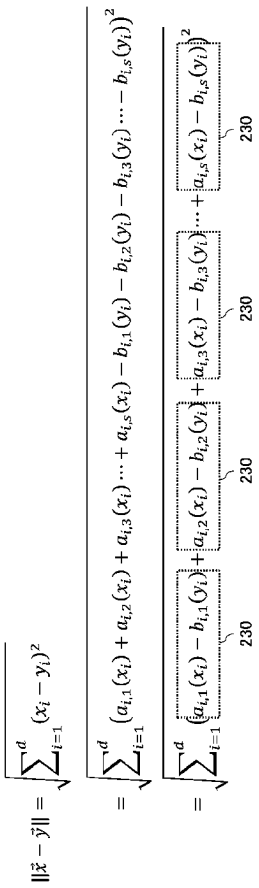
【図５】



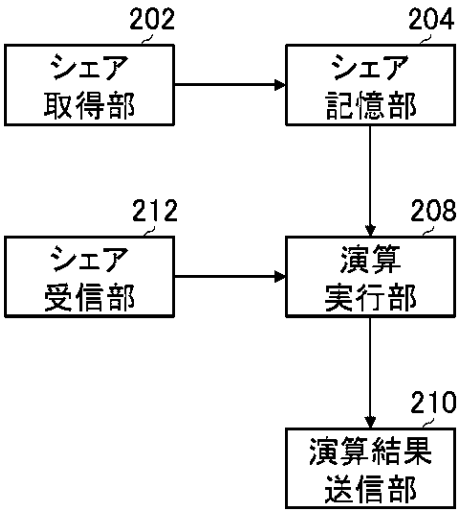
【図６】



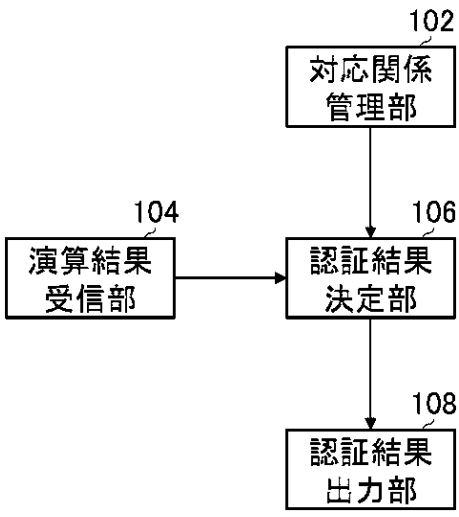
【図７】


$\|\vec{x}-\vec{y}\| = \sqrt{\sum_{i=1}^{d}(x_i-y_i)^2}$
$= \sqrt{\sum_{i=1}^{d}\left(a_{i,1}(x_i)+a_{i,2}(x_i)+a_{i,3}(x_i)\cdots+a_{i,s}(x_i)-b_{i,1}(y_i)-b_{i,2}(y_i)-b_{i,3}(y_i)\cdots-b_{i,s}(y_i)\right)^2}$
$= \sqrt{\sum_{i=1}^{d}\left(\left[a_{i,1}(x_i)-b_{i,1}(y_i)\right]+\left[a_{i,2}(x_i)-b_{i,2}(y_i)\right]+\left[a_{i,3}(x_i)-b_{i,3}(y_i)\right]\cdots+\left[a_{i,s}(x_i)-b_{i,s}(y_i)\right]\right)^2}$
230
230
230
230

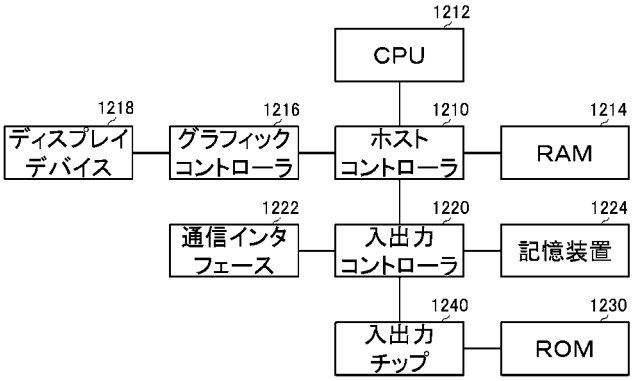
【図８】


200
202
シェア
取得部
204
シェア
記憶部
212
シェア
受信部
208
演算
実行部
210
演算結果
送信部

【図９】


100
102
対応関係
管理部
104
演算結果
受信部
106
認証結果
決定部
108
認証結果
出力部

【図１０】


1200
1212
CPU
1218
ディスプレイ
デバイス
1216
グラフィック
コントローラ
1210
ホスト
コントローラ
1214
RAM
1222
通信インタ
フェース
1220
入出力
コントローラ
1224
記憶装置
1240
入出力
チップ
1230
ROM

【手続補正書】
【提出日】令和5年5月16日(2023.5.16)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信部と、
前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有し、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行部は、前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記コサイン類似度を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出し、算出したコサイン類似度によって、前記認証対象の人の認証結果を決定する、認証システム。
【請求項２】
前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、
前記演算実行部は、前記認証対象の人の前記テンプレートと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、
前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、
前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、
前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項１に記載の認証システム。
【請求項３】
前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値と

を含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項１に記載の認証システム。
【請求項４】
第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される認証方法であって、
前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶する記憶段階と、
前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信段階と、
前記複数の第２サーバのそれぞれが、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、
前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、
前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、
前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と
を備え、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行段階は、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記コサイン類似度を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定段階は、前記複数の第２サーバのそれぞれの前記演算実行段階において実行された前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出し、算出したコサイン類似度によって、前記認証対象の人の認証結果を決定する、認証方法。
【請求項５】
認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信部と、
前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有し、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出すべく、前記

複数の第２サーバのそれぞれの前記演算実行部は、前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記ユークリッド距離を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出し、算出したユークリッド距離によって、前記認証対象の人の認証結果を決定する、認証システム。

【請求項６】

前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、

前記演算実行部は、前記シェア受信部が受信した前記認証対象の人の前記シェアと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、

前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、

前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、

前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項５に記載の認証システム。

【請求項７】

前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項５に記載の認証システム。

【請求項８】

第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される認証方法であって、

前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶するシェア記憶段階と、

前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信段階と、

前記複数の第２サーバのそれぞれが、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、

前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、

前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、

前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と

を備え、

登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行段階は、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記ユークリッド距離を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定段階は、前記複数の第２サーバのそれぞれの前記演算実行段階において実行された前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出し、算出したユークリッド距離によって、前記認証対象の人の認証結果を決定する、認証方法。

【手続補正書】

【提出日】令和5年12月13日(2023.12.13)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ、Ｒｅｐｌｉｃａｔｅｄ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、又はＲａｍｐ Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅを用いた認証を実行する認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信部と、
前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有し、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行部は、前記テンプレート受信部が受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記コサイン類似度を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出し、算出したコサイン類似度によって、前記認証対象の人の認証結果を決定する、認証システム。
【請求項２】
前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、
前記演算実行部は、前記認証対象の人の前記テンプレートと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、
前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、
前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、
前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項１に記載の認証システム。

【請求項３】
前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項１に記載の認証システム。
【請求項４】
第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される、Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ、Ｒｅｐｌｉｃａｔｅｄ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、又はＲａｍｐ Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅを用いた認証方法であって、
前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶する記憶段階と、
前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートを受信するテンプレート受信段階と、
前記複数の第２サーバのそれぞれが、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、
前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、
前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、
前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と
を備え、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのコサイン類似度を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行段階は、前記テンプレート受信段階において受信した前記テンプレートと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記コサイン類似度を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定段階は、前記複数の第２サーバのそれぞれの前記演算実行段階において実行された前記コサイン類似度を算出するための一部の演算結果を統合することによって、前記コサイン類似度を算出し、算出したコサイン類似度によって、前記認証対象の人の認証結果を決定する、認証方法。
【請求項５】
Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ、Ｒｅｐｌｉｃａｔｅｄ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、又はＲａｍｐ Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅを用いた認証を実行する認証システムであって、
第１サーバと、
人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバと
を備え、
前記複数の第２サーバのそれぞれは、
前記シェアを記憶するシェア記憶部と、
認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信部と、

前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行部と、
前記演算実行部による演算結果を前記第１サーバに送信する演算結果送信部と
を有し、
前記第１サーバは、
前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信部と、
前記演算結果受信部が受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定部と
を有し、
登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行部は、前記シェア受信部が受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記ユークリッド距離を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定部は、前記複数の第２サーバのそれぞれの前記演算実行部が実行した前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出し、算出したユークリッド距離によって、前記認証対象の人の認証結果を決定する、認証システム。
【請求項６】
前記シェア記憶部は、複数の人のそれぞれについて、前記複数のシェアのうちの１つのシェアを記憶し、
前記演算実行部は、前記シェア受信部が受信した前記認証対象の人の前記シェアと、前記シェア記憶部に記憶されている複数の前記シェアのそれぞれとを用いた演算を実行し、
前記演算結果送信部は、前記演算実行部による複数の前記演算結果を前記第１サーバに送信し、
前記第１サーバは、前記複数の第２サーバのそれぞれから前記複数の演算結果を受信し、
前記認証結果決定部は、前記演算結果受信部が受信した前記複数の演算結果を用いて、前記認証対象の人の認証結果を決定する、請求項５に記載の認証システム。
【請求項７】
前記複数の第２サーバは、前記人の前記生体情報から生成された前記テンプレートから複数のハッシュ値を減算することによって生成されたシェアと、前記複数のハッシュ値とを含む前記複数のシェアのそれぞれをそれぞれが記憶する、請求項５に記載の認証システム。
【請求項８】
第１サーバと、人の生体情報から生成されたテンプレートから生成された複数のシェアのそれぞれをそれぞれが記憶する複数の第２サーバとによって実行される、Ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ ｆｏｒ ａ ｇｅｎｅｒａｌ ａｄｖｅｒｓａｒｙ ｓｔｒｕｃｔｕｒｅ、Ｒｅｐｌｉｃａｔｅｄ ａｄｄｉｔｉｖｅ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅ、又はＲａｍｐ Ｓｈａｍｉｒ ｓｅｃｒｅｔ ｓｈａｒｉｎｇ ｓｃｈｅｍｅを用いた認証方法であって、
前記複数の第２サーバのそれぞれが、前記シェアをシェア記憶部に記憶するシェア記憶段階と、
前記複数の第２サーバのそれぞれが、認証対象の人の生体情報から生成されたテンプレートから生成された複数のシェアのうちの１つを受信するシェア受信段階と、
前記複数の第２サーバのそれぞれが、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いた演算を実行する演算実行段階と、
前記複数の第２サーバのそれぞれが、前記演算実行段階における演算結果を前記第１サーバに送信する演算結果送信段階と、

前記第１サーバが、前記複数の第２サーバのそれぞれから前記演算結果を受信する演算結果受信段階と、

前記第１サーバが、前記演算結果受信段階において受信した複数の前記演算結果を用いて、前記認証対象の人の認証結果を決定する認証結果決定段階と

を備え、

登録されている人の前記生体情報から生成された前記テンプレートと、前記認証対象の人の生体情報から生成された前記テンプレートとのユークリッド距離を算出すべく、前記複数の第２サーバのそれぞれの前記演算実行段階は、前記シェア受信段階において受信した前記シェアと、前記シェア記憶部に記憶されている前記シェアとを用いて、前記ユークリッド距離を算出するための一部の演算を実行し、前記第１サーバの前記認証結果決定段階は、前記複数の第２サーバのそれぞれの前記演算実行段階において実行された前記ユークリッド距離を算出するための一部の演算結果を統合することによって、前記ユークリッド距離を算出し、算出したユークリッド距離によって、前記認証対象の人の認証結果を決定する、認証方法。