(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第7668324号
(P7668324)
(45)発行日　令和7年4月24日(2025.4.24)　(24)登録日　令和7年4月16日(2025.4.16)

(51)Int.Cl.		FI		
G06T 7/00	*(2017.01)*	G06T	7/00	510A
G06F 16/901	*(2019.01)*	G06F	16/901	
G06F 21/32	*(2013.01)*	G06F	21/32	
G06V 40/10	*(2022.01)*	G06V	40/10	
G09C 1/00	*(2006.01)*	G09C	1/00	650Z

請求項の数 8　(全 20 頁)　最終頁に続く

(21)出願番号　特願2023-190385(P2023-190385)
(22)出願日　令和5年11月7日(2023.11.7)
審査請求日　令和6年3月19日(2024.3.19)

(73)特許権者　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

審査官　小池　正彦

(56)参考文献　米国特許出願公開第２０２１／０３４２４３２（ＵＳ，Ａ１）

最終頁に続く

(54)【発明の名称】認証システム及び認証方法

(57)【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、
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、複数の人に対応する複数のノードであって、それぞれが、対応する人の生体情報から生成されたベクトルデータを含む前記複数のノードを含み、前記複数のノードがリンクで接続されているグラフ構造における前記複数のノードのそれぞれについて、前記ベクトルデータから生成された複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された複数のリンクシェアのうちの１つを記憶し、
前記複数の第２サーバのそれぞれは、
前記ベクトルシェア及び前記リンク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ベクトルデータから生成された複数のベクトルシェアのうちの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ベクトルシェアと、前記シェア記憶部に記憶されている前記ベクトル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と、前記リンクシェアとを前記第１サーバに送信する送信部と

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及び前記リンクシェアを受信する受信部と、
前記受信部が受信した複数の前記演算結果と、複数の前記リンクシェアとを用いて、前記認証対象の人の認証結果を判定する判定部と
を有する、認証システム。
【請求項２】
前記シェア記憶部は、前記グラフ構造に含まれる前記複数のノードのぞれぞれについて、前記ノードを識別可能なノード識別データと、前記ノードに含まれる前記ベクトルデータから生成された前記複数のベクトルシェアのうちの１つと、前記ノードに含まれる前記リンク先データから生成された前記複数のリンクシェアのうちの１つとを記憶する、請求項１に記載の認証システム。
【請求項３】
前記ベクトルデータから生成された前記複数のベクトルシェアによって、前記ベクトルデータを生成可能であり、
前記リンク先データから生成された前記複数のリンクシェアによって、前記リンク先データを生成可能である、請求項１に記載の認証システム。
【請求項４】
前記第１サーバは、前記複数のノードのうちのいずれかを示すノード識別データを前記複数の第２サーバに送信する通知部を有し、
前記受信部は、前記複数の第２サーバのそれぞれから、前記通知部が送信した前記ノード識別データが示すノードに対応する前記演算結果及び前記リンクシェアを受信し、
前記判定部は、前記受信部が受信した複数の前記演算結果によって、前記ノード識別データが示すノードに対応するベクトルデータと、前記認証対象の人のベクトルデータとの距離を算出し、算出した距離が予め定められた距離よりも短い場合、前記認証対象の人が、前記ノード識別データが示すノードに対応する人であると決定する、請求項１から３のいずれか一項に記載の認証システム。
【請求項５】
前記第１サーバは、
前記ノード識別データが示すノードに対応するベクトルデータと前記認証対象の人のベクトルデータとの距離が前記予め定められた距離よりも長い場合、前記受信部が受信した複数の前記リンクシェアから前記リンク先データを生成するリンク生成部
を有し、
前記通知部は、前記リンク生成部によって生成された前記リンク先データが示すリンク先のノードを示すノード識別データを前記複数の第２サーバに送信する、
請求項４に記載の認証システム。
【請求項６】
前記複数の第２サーバのそれぞれは、前記複数のノードの全てを含む第１層と、前記複数のノードのうちの一部のノードを含む第２層とを少なくとも含む階層構造を有する前記グラフ構造における、前記第１層に含まれる前記複数のノードのそれぞれについて、前記ベクトルデータから生成された前記複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された前記複数のリンクシェアのうちの１つを記憶する、請求項１に記載の認証システム。
【請求項７】
前記グラフ構造の前記第２層は公開されており、
前記判定部は、前記第２層を更に用いて、前記認証対象の人の認証結果を判定する、請求項６に記載の認証システム。
【請求項８】
第１サーバと、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、複数の人に対応する複数のノードであって、それぞれが、対応する人の生体情報から生成されたベクトルデータを含む前記複数のノードを含み、前記複数のノードがリンクで接続されているグラフ構造における前記複数のノードのそれぞれについて、前記ベクトルデータから生成された複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された複数のリンクシェアのうちの１つ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ベクトルデータから生成された複数のベクトルシェアのうちの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ベクトルシェアと、前記シェア記憶部に記憶されている前記ベクトル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よる演算結果と、前記リンクシェアとを前記第１サーバに送信する送信段階と、

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及び前記リンクシェアを受信する受信段階と、

前記第１サーバが、前記受信段階において受信した複数の前記演算結果と、複数の前記リンクシェアとを用いて、前記認証対象の人の認証結果を判定する判定段階と

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、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、複数の人に対応する複数のノードであって、それぞれが、対応する人の生体情報から生成されたベクトルデータを含む前記複数のノードを含み、類似するノード同士がリンクで接続されているグラフ構造における、前記複数のノードのそれぞれについて、前記ベクトルデータから生成された複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された複数のリンクシェアのうちの１つを記憶してよい。前記複数の第２サーバのそれぞれは、前記ベクトルシェア及び前記リンクシェアを記憶するシェア記憶部を備えてよい。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ベクトルデータから生成された複数のベクトルシェアのうちの１つを受信するシェア受信部を備えてよい。前記複数の第２サーバのそれぞれは、前記シェア受信部が受信した前記ベクトルシェアと、前記シェア記憶部に記憶されている前記ベクトルシェアとを用いた演算を実行する演算実行部を備えてよい。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と、前記リンクシェアとを前記第１サーバに送信する送信部を備えてよい。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及び前記リンクシェアを受信する受信部を備えてよい。前記第１サーバは、前記受信部が受信した複数の前記演算結果と、複数の前記リンクシェアとを用いて、前記認証対象の人の認証結果を判定する判定部を備えてよい。

【０００４】
前記認証システムにおいて、前記シェア記憶部は、前記グラフ構造に含まれる前記複数のノードのぞれぞれについて、前記ノードを識別可能なノード識別データと、前記ノードに含まれる前記ベクトルデータから生成された前記複数のベクトルシェアのうちの１つと、前記ノードに含まれる前記リンク先データから生成された前記複数のリンクシェアのうちの１つとを記憶してよい。
【０００５】
前記いずれかの認証システムにおいて、前記ベクトルデータから生成された前記複数のベクトルシェアによって、前記ベクトルデータを生成可能であってよく、前記リンク先データから生成された前記複数のリンクシェアによって、前記リンク先データを生成可能であってよい。
【０００６】
前記いずれかの認証システムにおいて、前記第１サーバは、前記複数のノードのうちのいずれかを示すノード識別データを前記複数の第２サーバに送信する通知部を有してよく、前記受信部は、前記複数の第２サーバのそれぞれから、前記ノード識別データ送信部が送信した前記ノード識別データが示すノードに対応する前記演算結果及び前記リンクシェアを受信してよく、前記判定部は、前記受信部が受信した前記複数の演算結果によって、前記ノード識別データが示すノードに対応するベクトルデータと、前記認証対象の人のベクトルデータとの距離を算出し、算出した距離が予め定められた距離よりも短い場合、前記認証対象の人が、前記ノード識別データが示すノードに対応する人であると決定してよい。前記第１サーバは、前記ノード識別データが示すノードに対応するベクトルデータと前記認証対象の人のベクトルデータとの距離が前記予め定められた距離よりも長い場合、前記受信部が受信した複数の前記リンクシェアから前記リンク先データを生成するリンク生成部を有してよく、前記通知部は、前記リンク生成部によって生成された前記リンク先データが示すリンク先のノードを示すノード識別データを前記複数の第２サーバに送信してよい。
【０００７】
前記いずれかの認証システムにおいて、前記複数の第２サーバのそれぞれは、前記複数のノードの全てを含む第１層と、前記複数のノードのうちの一部のノードを含む第２層とを少なくとも含む階層構造を有する前記グラフ構造における、前記第１層に含まれる前記複数のノードのそれぞれについて、前記ベクトルデータから生成された前記複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された前記複数のリンクシェアのうちの１つを記憶してよい。前記グラフ構造の前記第２層は公開されてよく、前記判定部は、前記第２層を更に用いて、前記認証対象の人の認証結果を判定してよい。
【０００８】
本発明の一実施態様によれば、第１サーバと、複数の第２サーバとによって実行される認証方法が提供される。前記認証方法は、前記複数の第２サーバのそれぞれが、複数の人に対応する複数のノードであって、それぞれが、対応する人の生体情報から生成されたベクトルデータを含む前記複数のノードを含み、類似するノード同士がリンクで接続されているグラフ構造における、前記複数のノードのそれぞれについて、前記ベクトルデータから生成された複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された複数のリンクシェアのうちの１つ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ベクトルデータから生成された複数のベクトルシェアのうちの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ベクトルシェアと、前記シェア記憶部に記憶されている前記ベクトル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よる演算結果と、前記リンクシェアとを前記第１サーバに送信する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及び前記リンクシェアを受信する受信段階を備えてよい。前記認証方法は、前記第１サーバが、前記受信段階において受信した複数の前記演算結果と、複数の前記リンクシェアとを用いて、前記認証対象の人の認証結果を判定する判定段階を備えてよい。

【０００９】

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】

【００１０】

【図１】認証システム１０の一例を概略的に示す。

【図２】グラフ構造６００の一例を概略的に示す。

【図３】グラフ構造６００を用いた一般的な認証処理について説明するための説明図である。

【図４】分散数を３とした場合の、ノード６１０に含まれるデータと、ベクトルシェア及びリンクシェアとについて説明するための説明図である。

【図５】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６】サブサーバ２００の機能構成の一例を概略的に示す。

【図７】メインサーバ１００の機能構成の一例を概略的に示す。

【図８】認証システム１０におけるベクトルデータの演算の一例について説明するための説明図である。

【図９】階層構造を備える場合のグラフ構造６００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、登録サーバ４００、又は認証クライアント５００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】

【００１１】

１対多認証を実行する場合において、グラフ探索が有効である。例えば、複数の人に対応する複数のノードであって、それぞれが、対応する人の生体情報から生成されたベクトル情報を含む複数のノードを含み、類似するノード同士がリンクで接続されているグラフ構造を用いることによって、認証対象の人とベクトル情報を比較する対象となるノードの数を適切に低減することができ、効率的な認証を行うことができる。このようなグラフ構造には、多数の人の情報が含まれるうえに、多数の人同士の関係の情報も含まれることになる。そのため、グラフ構造が漏洩することを防止する必要性は非常に高いといえる。本実施形態に係る認証システム１０では、秘密分散技術によってグラフ構造を複数のサーバに分割保存する。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、グラフ構造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。

【００１２】

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。

【００１３】

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。

【００１４】

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。

【００１５】

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、登録サーバ４００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５００を更に備えてもよい。

【００１６】

メインサーバ１００、サブサーバ２００、登録クライアント３００、登録サーバ４００及び認証クライアント５００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。

【００１７】

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。

【００１８】

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。

【００１９】

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。

【００２０】

登録サーバ４００は、ネットワーク２０に有線接続されてよい。登録サーバ４００は、ネットワーク２０に無線接続されてもよい。登録サーバ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。登録サーバ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。登録サーバ４００は、いわゆるサーバ装置によって構成されてよい。登録サーバ４００は、任意の装置上で実現されたサーバであってもよい。

【００２１】

認証クライアント５００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５００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５００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５００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５００は、任意の装置であってよい。例えば、認証クライアント５００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。

【００２２】

登録クライアント３００は、登録対象の人７０の生体情報をセンサによって取得する。登録クライアント３００は、取得した生体情報を登録サーバ４００に送信してよい。登録

クライアント３００は、取得した生体情報の特徴を表す多次元のベクトルデータを生成し、生成したベクトルデータを登録サーバ４００に送信してもよい。

【００２３】

登録サーバ４００は、登録クライアント３００から生体情報を受信した場合に、生体情報からベクトルデータを生成して、記憶する。登録サーバ４００は、登録クライアント３００からベクトルデータを受信した場合、当該ベクトルデータを記憶する。

【００２４】

登録サーバ４００は、複数の人７０のベクトルデータを用いて、複数の人７０の認証に用いるグラフ構造を生成する。登録サーバ４００は、複数の人７０に対応する複数のノードであって、それぞれが、対応する人のベクトルデータを含む複数のノードを含み、複数のノードがリンクで接続されているグラフ構造を生成してよい。グラフ構造においてリンクで接続されるノード同士はベクトルデータの類似するノード同士であってよい。登録サーバ４００は、公知の手法を用いて、このようなグラフ構造を生成してよい。

【００２５】

登録サーバ４００は、生成したグラフ構造における複数のノードのそれぞれについて、ノードに含まれるベクトルデータから複数のベクトルシェアを生成し、リンク先のノードを示すリンク先データから複数のリンクシェアを生成する。登録サーバ４００は、複数のノードのそれぞれについて、複数のベクトルシェア及び複数のリンク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。

【００２６】

複数のサブサーバ２００のそれぞれは、受信したベクトルシェア及びリンクシェアを記憶する。どのベクトルシェア及びリンクシェアがどのサブサーバ２００に記憶されているかは、登録サーバ４００及びメインサーバ１００によって管理されてよい。

【００２７】

認証クライアント５００は、認証対象の人８０の生体情報をセンサによって取得して、人８０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５００は、人８０の生体情報からベクトルデータを生成し、ベクトルデータから複数のベクトルシェアを生成して、複数のサブサーバ２００のそれぞれに送信する。

【００２８】

認証システム１０は、グラフ構造及び秘密分散を用いた生体認証を実行する。

【００２９】

図２は、グラフ構造６００の一例を概略的に示す。グラフ構造６００は、複数の人７０に対応する複数のノード６１０を含む。複数のノード６１０の一つ一つが、複数の人７０の一人一人に対応する。グラフ構造６００において、ノード６１０同士がリンク６２０で接続されている。複数のノード６１０のそれぞれは、対応する人７０の生体情報から生成されたベクトルデータと、リンク先のノードを示すリンク先データとを含む。

【００３０】

図３は、グラフ構造６００を用いた一般的な認証処理について説明するための説明図である。一般的な認証処理では、認証対象の人８０の生体情報から生成された認証対象ベクトルデータ６３０との距離が予め定められた閾値よりも短いノード６１０をグラフ構造６００内で探索する。認証処理の主体は、例えば、複数のノード６１０のうちのいずれかを開始ノード６４０として、開始ノード６４０に含まれるベクトルデータと、認証対象ベクトルデータ６３０との距離を算出して、閾値と比較する。認証処理の主体は、算出した距離が閾値より短い場合、認証対象の人８０が、開始ノード６４０に対応する人７０であると判定して認証成功とする。

【００３１】

認証処理の主体は、算出した距離が閾値より長い場合、開始ノード６４０のリンク先のノード６１０を特定し、リンク先のノード６１０に含まれるベクトルデータと、認証対象ベクトルデータ６３０との距離を算出して、閾値と比較する。算出した距離が閾値より短いノード６１０が存在する場合、認証処理の主体は、認証対象の人８０が、当該ノード６

１０に対応する人７０であると判定して認証成功とする。算出した距離が閾値より短いノード６１０が存在しない場合、認証処理の主体は、リンク先のノード６１０のうち、算出した距離が最も短いノード６１０を特定して、特定したノード６１０のリンク先のノード６１０を特定する。認証処理の主体は、算出した距離が閾値より短いノード６１０を発見するか、複数のノード６１０のうち、認証対象ベクトルデータ６３０との距離が最も短いベクトルデータを含むノード６１０を特定するまで、処理を継続する。算出した距離が閾値より短いノード６１０を発見した場合、認証成功とし、認証対象ベクトルデータ６３０との距離が最も短いノード６１０を特定したが、認証対象ベクトルデータ６３０とベクトルデータとの距離が閾値より長い場合に、認証失敗とする。

【００３２】

本実施形態に係る認証システム１０は、このようなグラフ構造６００を用いた探索を、秘密分散を用いて実現する。例えば、分散数を３とした場合、１つのベクトルデータを３つのベクトルシェアに分割し、１つのリンク先データを３つのリンクシェアに分割して、３つのベクトルシェア及びリンクシェアのペアを、３つのサブサーバ２００で分散管理する。

【００３３】

図４は、分散数を３とした場合の、ノード６１０に含まれるデータと、ベクトルシェア及びリンクシェアとについて説明するための説明図である。ここでは、リンク先がノードＢ、ノードＣ、ノードＤであるノードＡを例に挙げて説明する。

【００３４】

ノードＡは、ノードＡに対応する人７０の生体情報の特徴を表すベクトルデータ６１２と、リンク先であるノードＢ、ノードＣ、ノードＤを示すリンク先データ６２２とを含む。

【００３５】

登録サーバ４００は、ベクトルデータ６１２から３つのベクトルシェア６１４を生成する。３つのベクトルシェア６１４がそろうことによって、ベクトルデータ６１２が復元可能である。

【００３６】

登録サーバ４００は、リンク先データ６２２から３つのリンクシェア６２４を生成する。３つのリンクシェア６２４がそろうことによって、リンク先データ６２２が復元可能である。登録サーバ４００は、例えば、リンク先データ６２２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つのリンクシェア６２４とする。リンクシェア６２４の生成方法は、これに限られない。

【００３７】

登録サーバ４００は、３つのベクトルシェア６１４及びリンクシェア６２４のペアを、３つのサブサーバ２００のそれぞれに送信して、３つのサブサーバ２００のそれぞれに、ノードＡを識別可能なノード識別データと対応付けて、ベクトルシェア６１４及びリンクシェア６２４のペアを記憶させる。

【００３８】

図５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。

【００３９】

登録サーバ４００は、生成部４０２及び変換部４０４を備える。生成部４０２は、複数の人７０のベクトルデータを用いて、グラフ構造６００を生成する。登録サーバ４００は、他の装置によって生成されたグラフ構造６００を取得してもよい。

【００４０】

変換部４０４は、グラフ構造６００における複数のノード６１０のそれぞれについて、ベクトルデータ６１２から複数のベクトルシェア６１４を生成し、リンク先データ６２２から複数のリンクシェア６２４を生成する。変換部４０４は、複数のノード６１０のそれぞれについて、ノード識別データと、複数のベクトルシェア６１４及びリンクシェア６２４のペアのそれぞれとを、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、ノード識別データと、複数のベクトルシェア６１４及びリンクシェア６２４のペアのそれぞれとを、複数のサブサーバ２００のそれぞれに送信してよい。複数のベクトルシェア６１４及びリンクシェア６２４のペアのそれぞれの送信先は、メインサーバ１００に共有されてよい。

【００４１】

認証クライアント５００は、センサ部５０２及び変換部５０４を備える。センサ部５０２は、認証対象の人８０の生体情報８２を取得して、生体情報８２からベクトルデータ８４を生成する。変換部５０４は、ベクトルデータ８４から複数のベクトルシェア８６を生成して、複数のベクトルシェア８６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５０４は、任意の暗号化手法を用いて暗号化した上で、複数のベクトルシェア８６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。複数のベクトルシェア８６の送信先は、登録クライアント３００又はメインサーバ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、認証クライアント５００から受信したベクトルシェア８６と、記憶している複数のベクトルシェア６１４のうちのいずれかのベクトルシェア６１４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、ベクトルシェア８６と、開始ノードに相当するノード６１０に対応するベクトルシェア６１４とに対する演算を実行してよい。複数のノード６１０のうちのどのノード６１０を開始ノードとするかは、登録サーバ４００によって指定されてよく、複数のサブサーバ２００の間で決定されてよく、メインサーバ１００によって指定されてもよい。

【００４３】

複数のサブサーバ２００のそれぞれは、開始ノードに相当するノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出するための演算の一部を実行する。一具体例として、複数のサブサーバ２００のそれぞれは、開始ノードに相当するノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４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２５０と、開始ノードに相当するノード６１０に対応するリンクシェア６２４とをメインサーバ１００に送信する。

【００４４】

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２５０を用いて、開始ノードに相当するノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。例えば、メインサーバ１００は、複数のサブサーバ２００から受信した複数の演算結果２５０を加算することによって、開始ノードに相当するノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出してよい。

【００４５】

メインサーバ１００は、算出した距離が、予め定められた閾値より短い場合、認証対象の人８０が、開始ノードに相当するノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。

【００４６】

メインサーバ１００は、算出した距離が、閾値より長い場合、複数のサブサーバ２００から受信した複数のリンクシェア６２４を用いて、リンク先データ６２２を生成する。メインサーバ１００は、生成したリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。メインサーバ１００は、リンク先データ６２２が示すリンク先のノード６１０のノード識別データを複数のサブサーバ２００に送信してよい。

【００４７】

リンク先データ６２２が示すリンク先のノード６１０が１つである場合、複数のサブサーバ２００のそれぞれは、認証クライアント５００から受信したベクトルシェア８６と、記憶している複数のベクトルシェア６１４のうち、リンク先のノード６１０に対応するベ

クトルシェア６１４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、演算結果２５０と、リンク先のノードに対応するリンクシェア６２４とをメインサーバ１００に送信する。メインサーバ１００は、複数のサブサーバ２００のそれぞれから受信した演算結果２５０を用いて、リンク先のノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。メインサーバ１００は、算出した距離が、予め定められた閾値より短い場合、認証対象の人８０が、リンク先のノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。メインサーバ１００は、算出した距離が、閾値より長い場合、複数のサブサーバ２００から受信した複数のリンクシェア６２４を用いて、リンク先データ６２２を生成する。メインサーバ１００は、生成したリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。

【００４８】

リンク先データ６２２が示すリンク先のノード６１０が複数である場合、複数のサブサーバ２００のそれぞれは、認証クライアント５００から受信したベクトルシェア８６と、複数のリンク先のノード６１０に対応するベクトルシェア６１４のそれぞれ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、複数のリンク先のノード６１０のそれぞれについて、演算結果２５０と、リンク先のノード６１０に対応するリンクシェア６２４とをメインサーバ１００に送信する。メインサーバ１００は、複数のリンク先のノード６１０のそれぞれについて、複数のサブサーバ２００のそれぞれから受信した演算結果２５０を用いて、リンク先のノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。メインサーバ１００は、複数のリンク先のノード６１０のうち、算出した距離が、予め定められた閾値より短いものが存在する場合、人８０が、当該ノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。メインサーバ１００は、算出したいずれの距離も、閾値より長い場合、距離が最も短かったノード６１０に対応する複数のリンクシェア６２４から、リンク先データ６２２を生成する。メインサーバ１００は、生成したリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。

【００４９】

このような処理を繰り返すことによって、認証システム１０は、人８０に対する認証処理を行う。

【００５０】

図６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、シェア受信部２０６、演算実行部２０８、及び送信部２１０を備える。

【００５１】

シェア取得部２０２は、グラフ構造６００における複数のノード６１０のそれぞれの、ノード識別データと、ベクトルデータ６１２から生成された複数のベクトルシェア６１４のうちの１つと、リンク先データ６２２から生成された複数のリンクシェア６２４のうちの１つとを取得する。シェア取得部２０２は、複数のノード６１０のそれぞれの、ノード識別データと、複数のベクトルシェア６１４のうちの１つと、複数のリンクシェア６２４のうちの１つとを、登録サーバ４００から受信してよい。

【００５２】

シェア記憶部２０４は、シェア取得部２０２が取得したノード識別データ、ベクトルシェア６１４及びリンクシェア６２４を記憶する。シェア記憶部２０４は、グラフ構造６００における複数のノード６１０のそれぞれの、ノード識別データ、ベクトルシェア６１４及びリンクシェア６２４を記憶する。複数のサブサーバ２００のシェア記憶部２０４のそれぞれが、グラフ構造６００に含まれる複数のノード６１０のそれぞれについて、ノード識別データと、ベクトルデータ６１２から生成された複数のベクトルシェア６１４のそれぞれと、リンク先データ６２２から生成された複数のリンクシェア６２４のそれぞれとを記憶することになる。

【００５３】
シェア受信部２０６は、認証対象の人８０の生体情報８２から生成されたベクトルデータ８４から生成された複数のベクトルシェア８６のうちの１つを受信する。シェア受信部２０６は、当該ベクトルシェア８６を認証クライアント５００から受信してよい。
【００５４】
演算実行部２０８は、シェア受信部２０６が受信したベクトルシェア８６と、シェア記憶部２０４に記憶されているベクトルシェア６１４とを用いた演算を実行する。演算実行部２０８は、ベクトルシェア８６に対応するノード６１０に対応するベクトルデータ６１２と、ベクトルデータ８４との距離を算出するための演算の一部を実行する。演算実行部２０８は、ベクトルシェア８６とベクトルシェア６１４との距離を算出してよい。演算実行部２０８は、ベクトルシェア８６とベクトルシェア６１４とのユークリッド距離を算出してよい。
【００５５】
演算実行部２０８は、認証対象の人８０の認証処理を実行する場合に、まず、グラフ構造６００に含まれる複数のノード６１０のうちの開始ノードに相当するノード６１０に対応するベクトルシェア６１４と、ベクトルシェア８６とを用いた演算を実行してよい。例えば、登録サーバ４００又はメインサーバ１００によって指定されたノード６１０に対応するベクトルシェア６１４と、ベクトルシェア８６とを用いた演算を実行する。
【００５６】
送信部２１０は、演算実行部２０８による演算結果２５０と、リンクシェア６２４とをメインサーバ１００に送信する。送信部２１０は、演算実行部２０８による演算結果２５０と、演算実行部２０８が演算を行ったベクトルシェア６１４に対応するリンクシェア６２４とを、メインサーバ１００に送信する。
【００５７】
図７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、受信部１０４、判定部１０６、リンク生成部１０８、通知部１１０、及び認証結果出力部１１２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。
【００５８】
対応関係管理部１０２は、グラフ構造６００に含まれる複数のノード６１０のそれぞれについて、ベクトルデータ６１２から生成された複数のベクトルシェア６１４及びリンク先データ６２２から生成された複数のリンクシェア６２４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、複数のノード６１０のそれぞれについて、１つ目のベクトルシェア６１４及びリンクシェア６２４を記憶するサブサーバ２００と、２つ目のベクトルシェア６１４及びリンクシェア６２４を記憶するサブサーバ２００と、３つ目のベクトルシェア６１４及びリンクシェア６２４を記憶するサブサーバ２００とを示す対応関係を記憶する。
【００５９】
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２５０及びリンクシェア６２４を受信する。受信部１０４は、複数のサブサーバ２００のそれぞれの送信部２１０によって送信された、演算結果２５０及びリンクシェア６２４を受信する。
【００６０】
判定部１０６は、受信部１０４が受信した複数の演算結果２５０と、複数のリンクシェア６２４とを用いて、認証対象の人８０の認証結果を判定する。判定部１０６は、受信部１０４が受信した複数の演算結果から、ベクトルデータ６１２とベクトルデータ８４との距離を算出する。例えば、受信部１０４は、複数の演算結果を加算することによって、ベクトルデータ６１２とベクトルデータ８４との距離を算出してよい。判定部１０６は、算出した距離が、予め定められた閾値より短い場合、人８０が、ノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。

【００６１】
算出した距離が、閾値より長い場合、リンク生成部１０８が、受信部１０４が受信した複数のリンクシェア６２４を用いて、リンク先データ６２２を生成する。
【００６２】
通知部１１０は、リンク生成部１０８が生成したリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。通知部１１０は、リンク先データ６２２が示すリンク先のノード６１０のノード識別データを複数のサブサーバ２００に送信してよい。
【００６３】
複数のサブサーバ２００が、開始ノードに相当するノード６１０に対応するベクトルデータ６１２と、ベクトルデータ８４との距離を算出するための演算の一部を実行していた場合、判定部１０６は、複数の演算結果２５０を用いて、開始ノードに相当するノード６１０に対応するベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。判定部１０６は、算出した距離が、予め定められた閾値より短い場合、認証対象の人８０が、開始ノードに相当するノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。算出した距離が、閾値より長い場合、リンク生成部１０８が、受信部１０４が受信した複数のリンクシェア６２４を用いて、リンク先データ６２２を生成する。そして、通知部１１０が、リンク生成部１０８が生成したリンク先データ６２２が示すリンク先のノード６１０のノード識別データを複数のサブサーバ２００に送信する。
【００６４】
当該ノード識別データをサブサーバ２００が受信した場合に、演算実行部２０８は、シェア記憶部２０４に記憶されている複数のベクトルシェア６１４のうちの、ノード識別データが示すノード６１０に対応するベクトルシェア６１４と、ベクトルシェア８６とを用いた演算を実行する。複数のノード識別データを受信した場合、演算実行部２０８は、複数のノード識別データが示す複数のノード６１０のそれぞれについて、対応するベクトルシェア６１４と、ベクトルシェア８６とを用いた演算を実行する。送信部２１０は、演算実行部２０８による演算結果２５０と、ノード識別データが示すノード６１０に対応するリンクシェア６２４とを、メインサーバ１００に送信する。
【００６５】
送信部２１０によって送信された演算結果２５０及びリンクシェア６２４を、受信部１０４が受信した場合、判定部１０６が、判定を実行する。
【００６６】
リンク先のノード６１０が１つである場合、判定部１０６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２５０を用いて、リンク先のノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。判定部１０６は、算出した距離が、予め定められた閾値より短い場合、認証対象の人８０が、リンク先のノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。算出した距離が、閾値より長い場合、リンク生成部１０８が、複数のサブサーバ２００から受信した複数のリンクシェア６２４を用いて、リンク先データ６２２を生成する。そして、通知部１１０が、リンク生成部１０８によって生成されたリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。
【００６７】
リンク先のノード６１０が複数である場合、判定部１０６は、複数のリンク先のノード６１０のそれぞれについて、複数のサブサーバ２００のそれぞれから受信した演算結果２５０を用いて、リンク先のノード６１０に含まれるベクトルデータ６１２と、ベクトルデータ８４との距離を算出する。判定部１０６は、複数のリンク先のノード６１０のうち、算出した距離が、予め定められた閾値より短いものが存在する場合、人８０が、当該ノード６１０に対応する人７０であり、認証成功であることを示す判定結果１５０を生成する。算出したいずれの距離も、閾値より長い場合、リンク生成部１０８が、距離が最も短か

ったノード６１０に対応する複数のリンクシェア６２４から、リンク先データ６２２を生成する。そして、通知部１１０が、リンク生成部１０８によって生成されたリンク先データ６２２が示すリンク先のノード６１０を複数のサブサーバ２００に通知する。

【００６８】

認証システム１０は、算出した距離が閾値より短いノード６１０を発見するか、複数のノード６１０のうち、ベクトルデータ８４との距離が最も短いベクトルデータ６１２を含むノード６１０を特定するまで、処理を継続する。判定部１０６は、算出した距離が閾値より短いノード６１０を発見した場合、認証成功とし、ベクトルデータ８４との距離が最も短いノード６１０を特定したが、ベクトルデータ８４とベクトルデータ６１２との距離が閾値より長い場合に、認証失敗とする。

【００６９】

認証結果出力部１１２は、判定部１０６による判定結果１５０を出力する。認証結果出力部１１２は、例えば、メインサーバ１００が備えるディスプレイに判定結果１５０を表示させる。認証結果出力部１１２は、例えば、ネットワーク２０を介して他の装置に判定結果１５０を送信する。例えば、認証結果出力部１１２は、ネットワーク２０を介して判定結果１５０を認証クライアント５００に送信する。

【００７０】

図８は、認証システム１０におけるベクトルデータの演算の一例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が、下記数式１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。また、認証対象の人８０のベクトルデータ８４が、下記数式２で表すように分散されて複数のサブサーバ２００に提供される。Ｓは分散数を表す。

【００７１】

【数１】

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

【００７２】

【数２】

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

【００７３】

この場合、登録されている人７０のベクトルデータ６１２と、認証対象の人８０のベクトルデータ８４とのユークリッド距離は、図８に示す数式で表すことができる。

【００７４】

複数のサブサーバ２００のそれぞれは、図８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２５０を受信して、複数の演算結果２５０に対して、図８に示すように、１～ｄ次元についての、複数の演算結果２５０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、ベクトルデータ６１２とベクトルデータ８４とのユークリッド距離を算出することができる。

【００７５】

図９は、階層構造を備える場合のグラフ構造６００の一例を概略的に示す。グラフ構造６００は、図９に示すように、階層構造を備えてよい。

【００７６】

図９に示す例において、層６５０は、複数のノード６１０の全てを含む。層６５０は、第１層の一例であってよい。層６５２は、層６５０に含まれる複数のノード６１０のうちの一部の複数のノード６１０を含む。層６５４は、層６５２に含まれる複数のノード６１０のうちの一部の複数のノード６１０を含む。グラフ構造６００は、４つ以上の層を備え

てもよい。層６５２は、第２層の一例であってよい。層６５４は、第２層の一例であってよい。

【００７７】

複数のサブサーバ２００のそれぞれは、グラフ構造６００における、層６５０に含まれる複数のノード６１０のそれぞれについて、ベクトルデータ６１２から生成された複数のベクトルシェア６１４のうちの１つ及びリンク先のノードを示すリンク先データ６２２から生成された複数のリンクシェア６２４のうちの１つを記憶する。複数のサブサーバ２００のそれぞれは、層６５２及び層６５４については、これらのデータを記憶しなくてよい。層６５４は、公開されてもよい。層６５２は、公開されてもよい。

【００７８】

判定部１０６は、層６５０に加えて、層６５２を更に用いたり、層６５２及び層６５４を更に用いたりして、認証対象の人８０の認証結果を判定してもよい。例えば、判定部１０６は、認証対象の人８０の生体情報８２から生成されたベクトルデータ８４によって、層６５４を探索して、ベクトルデータ８４と最も距離が短いノード６１０を特定する。判定部１０６は、図３において説明した一般的な認証処理を実行することによって、層６５４における探索を実行してよい。判定部１０６は、層６５４において特定したノード６１０に対応する、層６５２におけるノード６１０を特定する。

【００７９】

判定部１０６は、層６５２において、当該特定したノード６１０を開始ノードとして、ベクトルデータ８４と最も距離が短いノード６１０を特定する。判定部１０６は、図３において説明した一般的な認証処理を実行することによって、層６５４における探索を実行してよい。判定部１０６は、層６５２において特定したノード６１０に対応する、層６５０におけるノード６１０を特定する。

【００８０】

判定部１０６は、層６５０において、当該特定したノード６１０を開始ノードとして、図５において説明した手法によって、判定処理を行う。

【００８１】

このように、グラフ構造６００の階層構造における上位の層においては、秘密分散を用いた認証を行わずに、一般的な認証処理を行い、下位の層においては、秘密分散を用いた認証を行うことによって、グラフ構造６００の重要部分の秘匿性を維持しつつ、処理を高速化することができる。

【００８２】

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、登録サーバ４００、又は認証クライアント５００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。

【００８３】

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。

【００８４】

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。

【００８５】

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。

【００８６】

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。

【００８７】

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。

【００８８】

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、ＣＰＵ１２１２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。

【００８９】

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。

【００９０】

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。

【００９１】

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。

【００９２】

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。

【００９３】

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）、Ｂｌｕ－ｒａｙ（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。

【００９４】

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。

【００９５】

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。

【００９６】

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。

【００９７】

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】

【００９８】

１０　認証システム、２０　ネットワーク、７０　人、８０　人、８２　生体情報、８４　ベクトルデータ、８６　ベクトルシェア、１００　メインサーバ、１０２　対応関係管理部、１０４　受信部、１０６　判定部、１０８　リンク生成部、１１０　通知部、１１２　認証結果出力部、１５０　判定結果、２００　サブサーバ、２０２　シェア取得部、２０４　シェア記憶部、２０６　シェア受信部、２０８　演算実行部、２１０　送信部、２３０　部分演算、２５０　演算結果、３００　登録クライアント、４００　登録サーバ、４０２　生成部、４０４　変換部、５００　認証クライアント、５０２　センサ部、５０４　変換部、６００　グラフ構造、６１０　ノード、６１２　ベクトルデータ、６１４　ベクトルシェア、６２０　リンク、６２２　リンク先データ、６２４　リンクシェア、６３０　認証対象ベクトルデータ、６４０　開始ノード、６５０　層、６５２　層、６５４　層、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

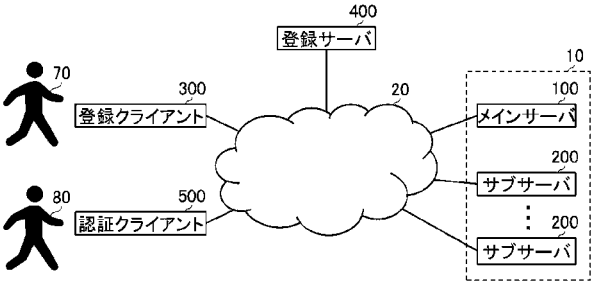
【要約】　（修正有）

【課題】秘密分散技術を適用したグラフ探索による１対多認証を実行する認証システム及び認証方法を提供する。

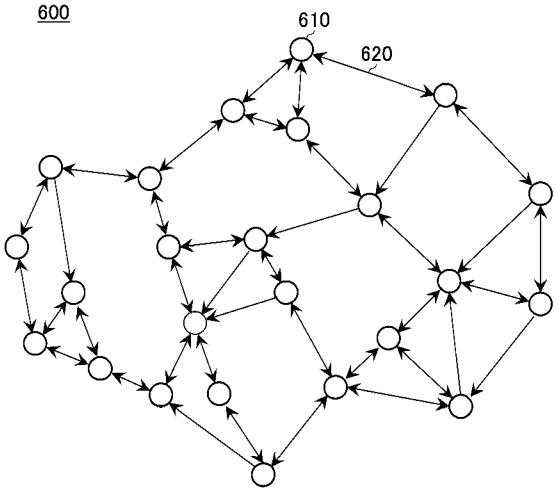
【解決手段】メインサーバと複数のサブサーバを備える認証システムにおいて、複数のサブサーバの夫々は、グラフ構造における複数のノードの夫々について、ベクトルデータから生成された複数のベクトルシェアのうちの１つ及びリンク先のノードを示すリンク先データから生成された複数のリンクシェアのうちの１つを記憶し、ベクトルシェア及びリンクシェアを記憶するシェア記憶部と、認証対象の人の生体情報から生成されたベクトルデータから生成された複数のベクトルシェアのうちの１つを受信するシェア受信部と、シェア受信部が受信したベクトルシェア及びシェア記憶部に記憶されているベクトルシェアを用いた演算を実行する演算実行部と、演算実行部による演算結果及びリンクシェアをメインサーバに送信する送信部と、を有する。

【選択図】図１

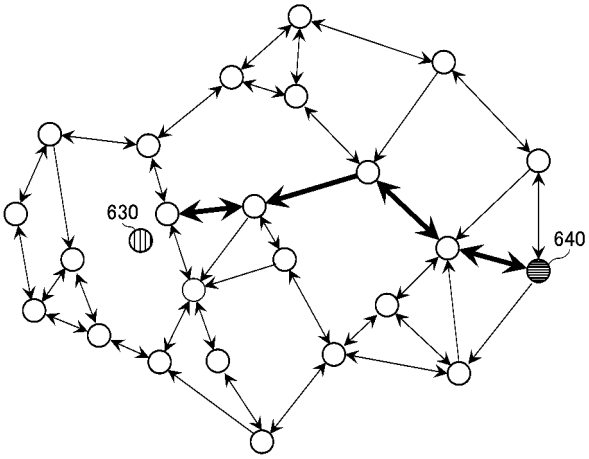
【図１】


400
登録サーバ
10
70
300
登録クライアント
20
100
メインサーバ
200
サブサーバ
80
500
認証クライアント
200
サブサーバ

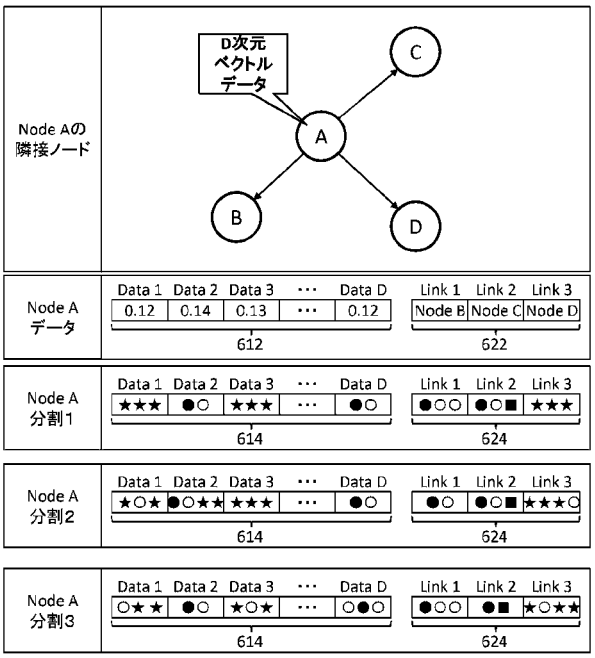
【図２】


600
610
620

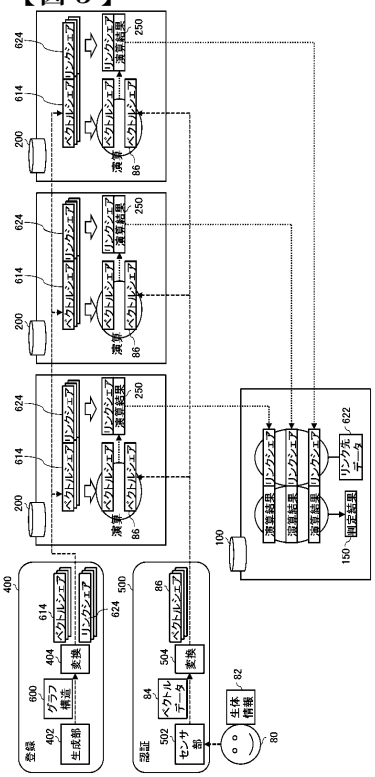
【図３】


600
630
640

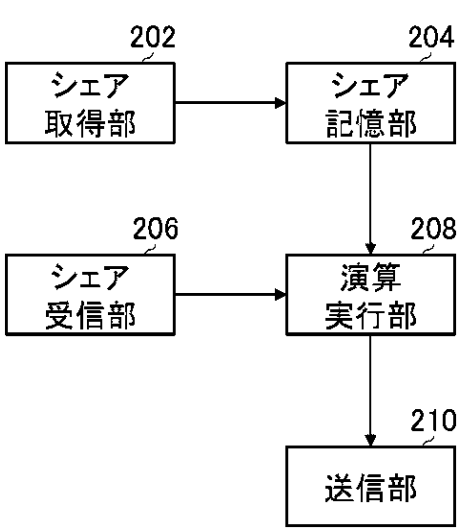
【図４】


Node Aの
隣接ノード
D次元
ベクトル
データ
A
B
C
D
Node A
データ
Data 1 Data 2 Data 3 … Data D
0.12 0.14 0.13 … 0.12
612
Link 1 Link 2 Link 3
Node B Node C Node D
622
Node A
分割1
614
624
Node A
分割2
614
624
Node A
分割3
614
624

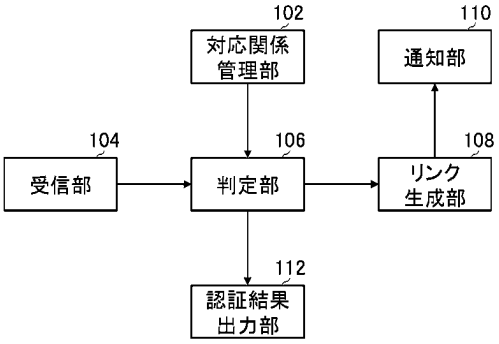
【図５】


登録
認証
ベクトル
データ
センサ
部
生体
情報
グラフ
構築
生成部
変換
ベクトル
シェア
リンク
シェア
演算結果
リンク先
データ
固定装置

【図６】



【図７】



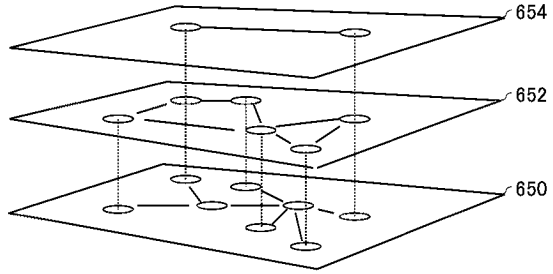
【図８】

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

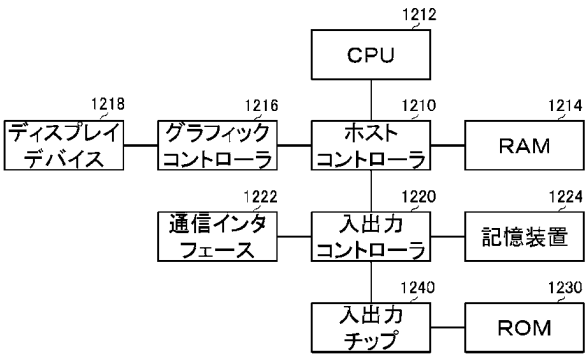
$$= \sqrt{\sum_{i=1}^{d}\left(a_{i,1}(x_i)+a_{i,2}(x_i)+a_{i,3}(x_i)\cdots+a_{i,s}(x_i)-b_{i,1}(y_i)-b_{i,2}(y_i)-b_{i,3}(y_i)\cdots-b_{i,s}(y_i)\right)^2}$$

$$= \sqrt{\sum_{i=1}^{d}\left(\underbrace{a_{i,1}(x_i)-b_{i,1}(y_i)}_{230}+\underbrace{a_{i,2}(x_i)-b_{i,2}(y_i)}_{230}+\underbrace{a_{i,3}(x_i)-b_{i,3}(y_i)}_{230}\cdots+\underbrace{a_{i,s}(x_i)-b_{i,s}(y_i)}_{230}\right)^2}$$

【図９】



【図１０】



フロントページの続き

(51)Int.Cl.			F I		
Ｈ０４Ｌ	9/32	(2006.01)	Ｈ０４Ｌ	9/32	１００Ｄ

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｇ０６Ｔ	７／００
Ｈ０４Ｌ	９／３２
Ｇ０６Ｆ	２１／３２
Ｇ０６Ｆ	１６／９０１
Ｇ０９Ｃ	１／００
Ｇ０６Ｖ	４０／１０