(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7294431号
(P7294431)

(45)発行日　令和5年6月20日(2023.6.20)

(24)登録日　令和5年6月12日(2023.6.12)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)		Ｈ０４Ｌ	9/32　２００Ｃ
Ｇ０６Ｆ　21/32　(2013.01)		Ｇ０６Ｆ	21/32

請求項の数　9　（全26頁）

(21)出願番号　特願2021-546103(P2021-546103)
(86)(22)出願日　令和1年9月18日(2019.9.18)
(86)国際出願番号　PCT/JP2019/036523
(87)国際公開番号　WO2021/053749
(87)国際公開日　令和3年3月25日(2021.3.25)
審査請求日　令和4年3月11日(2022.3.11)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100141519
弁理士　梶田 邦之
(72)発明者　一色 寿幸
東京都港区芝五丁目７番１号 日本電気株式会社内
審査官　金沢 史明

最終頁に続く

(54)【発明の名称】　情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラム

(57)【特許請求の範囲】

【請求項１】

登録のための第１入力データの第１コミットメントと、前記第１入力データが予め定められた入力データ空間に含まれていることのゼロ知識証明を示す第１証明データとを生成する登録データ生成装置と、

前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶装置と、

前記第１コミットメントと前記第１証明データの検証を行う登録データ検証装置と、

前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、

認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていることのゼロ知識証明及び前記第２入力データと前記登録データ記憶装置に記憶されている前記登録データの類似度が予め定められた受理範囲に含まれていることのゼロ知識証明を示す第２証明データと、を生成する認証データ生成装置と、

前記第２コミットメントと前記第２証明データの検証を行う認証データ検証装置と

を備えた情報照合システム。

【請求項２】

請求項１に記載の情報照合システムであって、

前記登録データ生成装置が生成する前記第１証明データの一部又は全部が、ゼロ知識証

明によるデータである
　ことを特徴とする情報照合システム。
【請求項３】
　請求項１又は２に記載の情報照合システムであって、
　前記認証データ生成装置が生成する前記第２証明データの一部又は全部が、ゼロ知識証明によるデータである
　ことを特徴とする情報照合システム。
【請求項４】
　請求項１～３のいずれか１項に記載の情報照合システムであって、
　前記登録データ記憶装置に記憶された前記登録データが、前記第１入力データの前記第１コミットメントを含む
　ことを特徴とする情報照合システム。
【請求項５】
　請求項１～４のいずれか１項に記載の情報照合システムであって、
　前記認証用データ記憶装置に記憶された認証用データが、前記第１入力データの前記第１コミットメントを生成する際に用いた乱数を含む
　ことを特徴とする情報照合システム。
【請求項６】
　請求項１～５のいずれか１項に記載の情報照合システムであって、
　前記登録データ生成装置が生成する前記第１コミットメントの一部又は全部が、パラメータｇ、ｈ、Ｎ、前記第１入力データｘ、乱数ｒに対して、ｇ＾ｘ・ｈ＾ｒ ｍｏｄ Ｎである
　ことを特徴とする情報照合システム。
【請求項７】
　請求項１～６のいずれか１項に記載の情報照合システムであって、
　前記認証データ生成装置が生成する前記第２コミットメントの一部又は全部が、パラメータｇ、ｈ、Ｎ、前記第２入力データｙ、乱数ｒに対して、ｇ＾ｙ・ｈ＾ｒ ｍｏｄ Ｎである
　ことを特徴とする情報照合システム。
【請求項８】
　登録のための第１入力データの第１コミットメントと、前記第１入力データが予め定められた入力データ空間に含まれていることのゼロ知識証明を示す第１証明データとを生成する登録データ生成処理と、
　前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶処理と、
　前記第１コミットメントと前記第１証明データの検証を行う登録データ検証処理と、
　前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、
　認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていることのゼロ知識証明及び前記第２入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることのゼロ知識証明を示す第２証明データと、を生成する認証データ生成処理と、
　前記第２コミットメントと前記第２証明データの検証を行う認証データ検証処理と
を含む情報照合方法。
【請求項９】
　登録のための第１入力データの第１コミットメントと、前記第１入力データが予め定められた入力データ空間に含まれていることのゼロ知識証明を示す第１証明データとを生成する登録データ生成処理と、
　前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶処理と、

前記第１コミットメントと前記第１証明データの検証を行う登録データ検証処理と、
前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていることのゼロ知識証明及び前記第２入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることのゼロ知識証明を示す第２証明データと、を生成する認証データ生成処理と、
前記第２コミットメントと前記第２証明データの検証を行う認証データ検証処理と
をコンピュータに実行させる情報照合プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムに関する。

【背景技術】

【０００２】

個人認証は、被登録者と被認証者の同一性を確認する手段である。事前に保存される被登録者に関する情報と、認証の都度取得される被認証者に関する情報を突き合わせることによって認証が実施される。

【０００３】

個人認証の一手法である生体認証では顔や指紋や虹彩などの身体的特徴などを利用して認証を行う。より具体的には、生体から特徴量と呼ばれるデータを抽出して認証に用いる。生体から抽出される特徴量は抽出の都度少しずつ異なる。そのため、認証時には、被登録者から抽出された特徴量と、被認証者から抽出された特徴量とを比較し、それらが十分に類似していると認められれば認証成功となる。類似度の判定方法は特徴量抽出の手法に依存するが、一般的な手法では、特徴量はベクトルの形で表され、類似度は２つの特徴量の内積（正規化相関）、ユークリッド距離、ハミング距離等によって算出され、類似度が予め定められた範囲に含まれる場合に十分に類似していると判定する。

【０００４】

パスワード等の記憶による認証やＩＣカード等の所持による認証と比べ、認証情報を入力するために記憶や所持などのユーザの能動的な準備が不要である利便性の高さや、認証情報を他人に使用されにくい安全性の高さなどが生体認証のメリットである。特徴量抽出法などの技術の進展や生体情報を採取できるセンサ機能（例えばカメラなど）を搭載した機器（例えばスマートフォン、タブレット端末など）の普及に伴い、近年、個人認証の手段として、生体認証の利用が進んでいる。

【０００５】

また、生体認証技術においてゼロ知識証明を用いた例が知られている。例えば、特許文献１では、生体認証システム等において、認証サーバに対し、自分が正しい変換パラメータを知っていることを、変換パラメータに関する知識を与えずに証明する変換パラメータ証明機能が開示されている。また、特許文献１では、このような証明を、ゼロ知識証明などを用いて実現可能なことが開示されている（例えば、段落［００４２］及び段落［００５１］参照）。

【先行技術文献】

【特許文献】

【０００６】

【文献】特開２００８－０９２４１３号公報

【非特許文献】

【０００７】

【文献】Taher ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms." IEEE transactions on information theory 31.4 (1

985): 469-472.
【発明の概要】
【発明が解決しようとする課題】
【０００８】
加法準同型公開鍵暗号方式などの暗号方式を利用した情報照合システムでは、入力データを暗号化により秘匿しているため、生体から生成されていないデータを用いた攻撃が想定される。このような生体から生成されていないデータから生成した登録データ又は認証データを用いた攻撃に対して安全な方式が要望される。
【０００９】
例えば、生体から生成されていないデータを入力として、登録するためのデータを生成することや、認証を受けるためのデータを生成することも可能である。上述の加法準同型公開鍵暗号方式を利用した情報照合システム生体では、入力データを暗号化により秘匿していることから、上述の攻撃の例として、生体から生成されていないデータを用いて登録データを生成することにより、多くの生体特徴量と一致して認証受理と判定されうる登録データを生成すること、及び、認証時に利用された生体特徴量に関する情報を取得又は漏洩させるよう試みることなどの攻撃も想定される。また、生体から生成されていないデータを入力として認証を受けるデータを生成することにより、認証受理と判定され得るデータ（認証されるデータ）を生成することや、登録されている生体特徴量に関する情報を取得又は漏洩させるよう試みる攻撃も想定される。
【００１０】
また、このような課題は、生体情報に限らず、予め定められたデータ空間とは別のデータ空間のデータから生成した登録データ又は認証データを用いた攻撃に対しても同様なことが言える。ここで、データ空間とは、例えば、生体情報など、登録するデータ又は認証されるデータを構成するデータ（値）がとり得る値の範囲、性質などをいう。
【００１１】
本発明の目的は、情報の照合において、予め定められたデータ空間とは別のデータ空間のデータから生成した登録データ又は認証データを用いた攻撃に対しても安全な情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムを提供することにある。一例として、本発明の目的のひとつは、生体情報を利用した情報の照合において、生体から生成されていないデータを用いた攻撃に対して安全な方式を提供することにある。
【課題を解決するための手段】
【００１２】
本発明の情報照合システムは、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成装置と、第１コミットメントと第１証明データの一部又は全部を記憶する認証用データ記憶装置と、第１コミットメントと第１証明データの検証を行う登録データ検証装置と、第１コミットメントと第１証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、認証されるための第２入力データの第２コミットメントと、第２入力データが上記予め定められた入力データ空間に含まれていること及び第２入力データと上記登録データ記憶装置の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成装置と、第２コミットメントと第２証明データの検証を行う認証データ検証装置と備える。
【００１３】
本発明のクライアント端末は、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを含む登録データを生成する登録データ生成部と、第１コミットメントと第１証明データの一部又は全部を記憶する認証用データ記憶部と、認証されるための第２入力データの第２コミットメントと、第２入力データが予め定められた入力データ空間に含まれていること及び第２入力データと登録データの類似度が予め定められた受理範囲に含まれてい

ることを示す第２証明データとを生成する認証データ生成部とを備える。
【００１４】
本発明のサーバは、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを入力し、第１コミットメントと第１証明データの検証を行う登録データ検証部と、認証されるための第２入力データの第２コミットメントと、第２入力データが予め定められた入力データ空間に含まれていること及び第２入力データと登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データと入力し、第２コミットメントと第２証明データの検証を行う認証データ検証部との少なくとも一方を備える。
【００１５】
本発明の情報照合方法は、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成処理と、第１コミットメントと第１証明データの一部又は全部を記憶する認証用データ記憶処理と、第１コミットメントと第１証明データの検証を行う登録データ検証処理と、第１コミットメントと第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、認証されるための第２入力データの第２コミットメントと、第２入力データが上記予め定められた入力データ空間に含まれていること及び第２入力データと上記登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成処理と、第２コミットメントと第２証明データの検証を行う認証データ検証処理とを含む。
【００１６】
本発明の情報照合プログラムは、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成処理と、第１コミットメントと第１証明データの一部又は全部を記憶する認証用データ記憶処理と、第１コミットメントと第１証明データの検証を行う登録データ検証処理と、第１コミットメントと第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、認証されるための第２入力データの第２コミットメントと、第２入力データが上記予め定められた入力データ空間に含まれていること及び第２入力データと上記登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成処理と、第２コミットメントと第２証明データの検証を行う認証データ検証処理とをコンピュータに実行させる。
【発明の効果】
【００１７】
本発明によると、情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全な情報照合システム、クライアント端末、サーバ、情報照合方法、及び情報照合プログラムを提供することができる。一例として、本発明によると、生体情報を利用した情報の照合において、生体から生成されていないデータを用いた攻撃に対して安全な方式を提供することが可能である。なお、本発明により、当該効果の代わりに、又は当該効果とともに、他の効果が奏されてもよい。
【図面の簡単な説明】
【００１８】
【図１】本発明の実施形態に係る情報照合システムの具体的な構成を示すブロック図である。
【図２】本実施形態における登録処理のフローチャートである。
【図３】本実施形態における照合処理のフローチャートである。
【図４】本実施形態における装置のハードウェア構成を示すブロック図である。
【図５】本実施形態における情報照合システムの一例を示すブロック図である。
【図６】本実施形態におけるクライアント端末の一例を示すブロック図である。

【図７】本実施形態におけるサーバの一例を示すブロック図である。
【発明を実施するための形態】
【００１９】
以下、添付の図面を参照して本発明の実施形態を詳細に説明する。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。
【００２０】
説明は、以下の順序で行われる。
１．関連技術
２．本発明の実施形態の概要
３．実施形態
３．１．システムの構成
３．２．登録及び照合の動作
３．３．実施例１
３．４．実施例２
４．その他
【００２１】
＜＜１．関連技術＞＞
個人認証は、被登録者と被認証者の同一性を確認する手段である。事前に保存される被登録者に関する情報と、認証の都度取得される被認証者に関する情報を突き合わせることによって認証が実施される。
【００２２】
個人認証の一手法である生体認証では顔や指紋や虹彩などの身体的特徴などを利用して認証を行う。より具体的には、生体から特徴量と呼ばれるデータを抽出して認証に用いる。生体から抽出される特徴量は抽出の都度少しずつ異なる。そのため、認証時には、被登録者から抽出された特徴量と、被認証者から抽出された特徴量とを比較し、それらが十分に類似していると認められれば認証成功となる。類似度の判定方法は特徴量抽出の手法に依存するが、一般的な手法では、特徴量はベクトルの形で表され、類似度は２つの特徴量の内積（正規化相関）、ユークリッド距離、ハミング距離等によって算出され、類似度が予め定められた範囲に含まれる場合に十分に類似していると判定する。
【００２３】
パスワード等の記憶による認証やＩＣカード等の所持による認証と比べ、認証情報を入力するために記憶や所持などのユーザの能動的な準備が不要である利便性の高さや、認証情報を他人に使用されにくい安全性の高さなどが生体認証のメリットである。特徴量抽出法などの技術の進展や生体情報を採取できるセンサ機能（例えばカメラなど）を搭載した機器（例えばスマートフォン、タブレット端末など）の普及に伴い、近年、個人認証の手段として、生体認証の利用が進んでいる。
【００２４】
一方で、生体認証には、生涯不変である生体情報はもし漏洩したとしても変更できないというデメリットもある。また、生体特徴量は、欧州の一般データ保護規則や日本の個人情報保護法において、個人情報に該当すると定められている。個人情報に該当するデータは、保管や外部提供等の取扱いに制限がある。また、法令等による制限だけでなく、社会的に受容されるための配慮も求められることが多い。一般に、個人情報保護の観点から、検証者（例えば認証サーバなど）側がユーザの生体情報に関する情報を保持しない生体認証方式が望ましい。その上で、ユーザが持つ端末（例えばスマートフォンなど）への攻撃も考慮し、ユーザの保持する端末がマルウェア等に乗っ取られた場合であっても生体情報が復元できない方式が望ましい。
【００２５】
そこで、生体情報を秘匿して保存し、秘匿したまま認証結果を判定できる生体認証手法が盛んに研究されている。秘匿したままの判定を実現する手段として、加法準同型性を有

する公開鍵暗号方式を利用する手法が知られている。

【００２６】

公開鍵暗号方式は、鍵生成アルゴリズム（ＫｅｙＧｅｎ）、暗号化アルゴリズム（Ｅｎｃ）、及び復号アルゴリズム（Ｄｅｃ）の３つのアルゴリズムで構成される。鍵生成アルゴリズムは、セキュリティパラメータと呼ばれる鍵の強度を表すパラメータを用いて、暗号化鍵ｅｋ及び復号鍵ｄｋを生成する。この動作は、セキュリティパラメータをκとすると、次式のように表すことができる。

ＫｅｙＧｅｎ（κ）→（ｅｋ，ｄｋ）

暗号化アルゴリズムは、暗号化鍵ｅｋにより平文のメッセージｍを暗号化した結果である暗号文ｃを生成する。これは次式のように表すことができる。

Ｅｎｃ（ｅｋ，ｍ）→ｃ

復号アルゴリズムは、復号鍵ｄｋにより暗号文ｃを復号した結果であるｍ'を生成する。これは次式のように表すことができる。

Ｄｅｃ（ｄｋ，ｃ）→ｍ'

【００２７】

公開鍵暗号方式は正しく暗号文を復号できる必要がある。すなわち、鍵生成アルゴリズムで生成された任意の暗号化鍵ｅｋ及び復号鍵ｄｋのペアに対し、任意のメッセージｍを暗号化鍵ｅｋで暗号化した結果である暗号文ｃを復号鍵ｄｋによって復号した結果ｍ'はｍと等しくなる必要がある。すなわち、ＫｅｙＧｅｎ（κ）→（ｅｋ，ｄｋ）に対し、任意のｍについて

Ｄｅｃ（ｄｋ，Ｅｎｃ（ｅｋ，ｍ））→ｍ

が成り立つ必要がある。

【００２８】

公開鍵暗号方式では、暗号化鍵を持っていれば誰でも暗号化アルゴリズムを実行可能であるが、復号鍵なしでは復号アルゴリズムは実行できない。

【００２９】

準同型性を有する公開鍵暗号方式（以下では、準同型公開鍵暗号と呼ぶ）は、公開鍵暗号の各アルゴリズムに加え、準同型演算アルゴリズム（Ｈｏｍ）を有する。

【００３０】

準同型演算アルゴリズムは、暗号化鍵ｅｋにより、入力された複数の暗号文c_1、c_2に対応するメッセージの演算結果の暗号文を生成する。入力できるメッセージが２つである場合、次式のように表すことができる。

Ｈｏｍ（ｅｋ，c_1，c_2）→ｃ

【００３１】

例えば、加法準同型性を有する公開鍵暗号の場合、メッセージm_1の暗号化鍵ｅｋによる暗号文c_1と、メッセージm_2の暗号化鍵ｅｋによる暗号文c_2と、から生成される暗号文ｃはm_1+m_2の暗号文である。すなわち、ＫｅｙＧｅｎ（κ）→（ｅｋ，ｄｋ）に対し、任意のm_1とm_2について、

Ｅｎｃ（ｅｋ，m_1）→c_1，Ｅｎｃ（ｅｋ，m_2）→c_2

とすると、

Ｄｅｃ（ｄｋ，Ｈｏｍ（ｅｋ，c_1，c_2））→m_1+m_2

が成り立つ。

【００３２】

加法準同型性を有する公開鍵暗号として、楕円曲線Ｅｌｇａｍａｌ暗号などが知られている。非特許文献1に開示されている楕円曲線Ｅｌｇａｍａｌ暗号の各アルゴリズムは次のように動作する。

【００３３】

鍵生成アルゴリズムは、まず、セキュリティパラメータκを入力として受け取る。次に、κビットの素数ｑをランダムに選び、楕円曲線Ｅ上の位数がｑである群の生成元Ｇを選ぶ。次に、１以上ｑ未満の整数ｘを一様ランダムに選択し、Ｈ＝［ｘ］Ｇとする。最後に

、暗号化鍵ｅｋ＝（κ，ｑ，Ｅ，Ｇ，Ｈ）及び復号鍵ｄｋ＝（ｅｋ，ｘ）を出力する。
【００３４】
暗号化アルゴリズムは、まず、暗号化鍵ｅｋ＝（κ，ｑ，Ｇ，ｇ，Ｈ）及びメッセージｍを入力として受け取る。次に、１以上ｑ未満の整数ｒを一様ランダムに選択し、C_a：＝［ｒ］Ｇ、C_b：＝［ｍ］Ｇ＋［ｒ］Ｈとする。最後に、暗号文ｃ＝（C_a，C_b）を出力する。
【００３５】
復号アルゴリズムは、まず、復号鍵ｄｋ＝（ｅｋ，ｘ）及び暗号文ｃ＝（C_a，C_b）を入力として受け取る。次に、Ｍ'＝C_b－［ｘ］C_aを計算する。最後に、復号結果ｍ'＝$Dlog_G$（Ｍ'）を出力する。ただし、Ｄｌｏｇは、$Dlog_G$（［ｘ］Ｇ）＝ｘとなる関数である。
【００３６】
メッセージｍの暗号文ｃ＝（C_a，C_b）＝（［ｒ］Ｇ，［ｍ］Ｇ＋［ｒ］Ｈ）に対し、楕円Ｅｌｇａｍａｌ暗号の復号アルゴリズムにより、暗号文ｃをｍに正しく復号できることを、次式によって確認できる。

$$M' = C_b - [x] \cdot C_a = ([m]G + [r]H) - [x] \cdot ([r]G) = [m]G + [r]([x] \cdot G) - [x] \cdot ([r]G) = [m]G$$

【００３７】
準同型演算アルゴリズムは、まず、暗号化鍵ｅｋ＝（κ，ｑ，Ｇ，ｇ，ｈ）及び第一の暗号文c_1＝（$C_{1,a}$，$C_{1,b}$）及び第二の暗号文c_2＝（$C_{2,a}$，$C_{2,b}$）を入力として受け取る。次に、C_a＝$C_{1,a}$＋$C_{2,a}$，C_b＝$C_{1,b}$＋$C_{2,b}$を計算する。最後に、準同型演算結果ｃ＝（C_a，C_b）を出力する。
【００３８】
メッセージm_1の暗号文（$C_{1,a}$＝［ｒ］Ｇ，$C_{1,b}$＝［m_1］Ｇ＋［ｒ］Ｈ）及びメッセージm_2の暗号文（$C_{2,a}$＝［ｓ］Ｇ，$C_{2,b}$＝［m_2］Ｇ＋［ｓ］Ｈ）に対し、次の２式が成り立つ。

$$C_a = [r+s] \cdot G$$

$$C_b = [m_1+m_2]G + [r+s]H$$

したがって、ｃはm_1＋m_2の暗号文であり、楕円曲線Ｅｌｇａｍａｌ暗号は加法準同型性を有する。
【００３９】
加法準同型暗号を利用した情報照合システムの概要を以下に説明する。
【００４０】
情報照合システムでは、入力データはｎ次元自然数ベクトルとする（ｎは自然数）。つまり、入力データをｘ＝（ｘ１，ｘ２，・・・，ｘｎ）とする。また、入力データｘと入力データｙの類似度をｓｉｍ（ｘ，ｙ）と表す。一般的に、ｓｉｍ（ｘ，ｙ）は、両データｘ、ｙの二乗ユークリッド距離、ハミング距離、正規化相関などが用いられる。これらは加法準同型性を用いて、暗号化したまま計算できることが知られている。
【００４１】
（登録段階）
入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）の各ｘｉ（ｉ＝１～ｎ）を加法準同型暗号で暗号化する。すなわち，｛Ｅｎｃ（ｅｋ，ｘｉ）｝を生成し、記憶しておく。
【００４２】
（認証段階）
入力データｙ＝（ｙ１，ｙ２，…，ｙｎ）の各ｙｉ（ｉ＝１～ｎ）と、準同型演算Ｈｏｍを用いて、ｘとｙの暗号化類似度Ｅｎｃ（ｅｋ，ｓｉｍ（ｘ，ｙ））を計算する。
【００４３】
暗号化類似度Ｅｎｃ（ｅｋ，ｓｉｍ（ｘ，ｙ））を復号し、類似度を得ることで、認証受理又は不受理の判定を行う。
【００４４】

ここで、入力データとして生体特徴量を想定すると、多くの生体認証方式では、入力データの空間が予め定められている。すなわち、各ｘｉの値は、予め定められたａ以上ｂ以下の自然数であり、ｘはｎ次元ベクトルであることが決められている。例えば、類似度をハミング距離とする生体認証方式では、各ｘｉは０又は１であり、次元数ｎは１０２４、２０４８などと決められている。

【００４５】

一方で、加法準同型暗号の平文空間（暗号化できるメッセージの空間）は、セキュリティパラメータにより決められるものであって、入力データの空間と必ずしも一致しない。例えば、類似度をハミング距離とする情報照合システム（例えば生体認証など）では、各ｘｉは０又は１であるが、用いる加法準同型暗号の平文空間は２０４８ビットの素数ｑで割った余りの集合であることがしばしば考えられる。

【００４６】

入力データの空間と、暗号方式の平文空間が一致しないことを利用した攻撃に対しても安全なシステムが要望されている。一般に、このような攻撃が行われていることを検知することは困難である。

【００４７】

前述の例では、類似度としてハミング距離を用いた情報照合システムの場合で説明したが、他の類似度メトリック（例えば、二乗ユークリッド距離や正規化相関など）を用いた場合でも、同様の攻撃が可能であることが知られている。また、前述の例では、加法準同型暗号を用いた場合で説明したが、他の準同型暗号（乗法、Ｓｏｍｅｗｈａｔ、完全）や線形マスクを用いた場合でも、同様の攻撃に対して安全であることが望ましい。

【００４８】

＜＜２．本発明の実施形態の概要＞＞

まず、本発明の実施形態の概要を説明する。

【００４９】

（１）技術的課題

情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全なシステム等が望ましい。

【００５０】

（２）技術的特徴

本発明の実施形態において、例えば、情報照合システムは、登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成装置と、第１コミットメントと第１証明データの一部又は全部を記憶する認証用データ記憶装置と、第１コミットメントと第１証明データの検証を行う登録データ検証装置と、第１コミットメントと第１証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、認証されるための第２入力データの第２コミットメントと、第２入力データが予め定められた入力データ空間に含まれていること及び第２入力データと登録データ記憶装置の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成装置と、第２コミットメントと第２証明データの検証を行う認証データ検証装置とを備える。

【００５１】

これにより、情報の照合において、登録及び認証のためのデータの一方のデータ空間と、他方のデータ空間が異なる攻撃に対しても安全なシステムが提供される。

【００５２】

なお、上述した技術的特徴は本発明の実施形態の具体的な一例であり、当然ながら、本発明の実施形態は上述した技術的特徴に限定されない。

【００５３】

本発明を実施するための形態について図面を参照して詳細に説明する。尚、各図面及び明細書記載の各実施形態において、同様の構成要素には同一の符号を付与し、説明を適宜

省略する。
【００５４】
＜＜３．実施形態＞＞
＜３．１．システムの構成＞
図５は、本実施形態に係る情報照合システム１の一例を示すブロック図である。また、図１は、本実施形態に係る情報照合システム１の具体的な構成を示すブロック図である。
【００５５】
例えば、図５に示すように、情報照合システム１は、例えば、登録データ生成装置１００と、登録データ検証装置２００と、登録データ記憶装置３００と、認証用データ記憶装置４００と、認証データ生成装置５００と、認証データ検証装置６００を有する。ただし、上記各装置は、別々の装置として実装することも可能であり、一部又は全てを同一の装置内に実装することも可能である。
【００５６】
また、例えば、登録データ生成装置１００と、認証用データ記憶装置４００と、認証データ生成装置５００は同一のクライアント端末内に実装し、登録データ検証装置２００と、登録データ記憶装置３００と、認証データ検証装置６００は各サーバに分けて実装することもでき、これにより、クライアント・サーバ型の認証システムを実現することが可能である。
【００５７】
図６は、本実施形態におけるクライアント端末の一例を示すブロック図である。具体例として図６に示すように、クライアント端末２は、登録データ生成装置１００と、認証用データ記憶装置４００と、認証データ生成装置５００とを有する。
【００５８】
図７は、本実施形態におけるサーバの一例を示すブロック図である。図７に示すように、サーバ３は、登録データ検証装置２００と認証データ検証装置６００のうち、いずれか一方又は両方の装置を有する。なお、サーバ３は、登録データ記憶装置３００を含んでもよいし、登録データ記憶装置３００と外部接続されていてもよい。
【００５９】
なお、情報照合システム１を構成する登録データ生成装置１００、登録データ検証装置２００、登録データ記憶装置３００、認証用データ記憶装置４００、認証データ生成装置５００、及び、認証データ検証装置６００は、それぞれ、登録データ生成部、登録データ検証部、登録データ記憶部、認証用データ記憶部、認証データ生成部、及び、認証データ検証部と称されてもよく、ひとつ又は複数のノード（装置）が、上述の各部のひとつ又は複数を有してもよい。
【００６０】
登録データ生成装置１００は、例えば、コミットメント生成部１０１と、証明生成部１０２と、認証用データ生成部１０３とを有する。コミットメント生成部１０１は、入力データ（第１入力データ）と、パラメータとを入力し、入力データに基づくコミットメント（第１コミットメント）を生成する。ここで、入力データは、登録するためのデータ（登録データ）であり、例えば生体情報である。ここでの入力データは、本明細書において、第１入力データ又は入力データｘとも称される。パラメータは、例えばコミットメントを求める際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。証明生成部１０２は、入力データと、パラメータと、生成されたコミットメントとを入力し、入力データが予め定められた入力データ空間に含まれていることを示す証明データ（第１証明データ）を生成する。ここでのパラメータは、例えばゼロ知識証明により証明データを生成する際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。証明データは、例えば後述するゼロ知識証明による求めることができる。認証用データ生成部１０３は、生成されたコミットメントと、生成された証明データと、登録データ検証装置２００の登録データ生成部から受信した、登録データの識別子（ＩＤ）とを入力し、認証用データを生成する。認証用データは、例えば、登録

データの識別子（ＩＤ）と、上述の入力データ（第１入力データ）のコミットメント（第１コミットメント）を生成する際に用いた乱数等を含むことができる。

【００６１】

登録データ検証装置２００は、例えば、証明検証部２０１と、登録データ生成部２０２とを有する。証明検証部２０１は、パラメータと、登録データ生成装置１００から受信したコミットメントと、証明データとを入力し、入力データが入力データ空間に含まれていることを検証する。ここで、パラメータは、例えば、入力データが入力データ空間に含まれていることを検証する際に用いるパラメータである。入力されるパラメータの種類は予め定められることができる。登録データ生成部２０２は、パラメータと、登録データ生成装置１００から受信したコミットメントと、証明データと、検証の結果に基づいて、登録データに対する識別子（ＩＤ）と、登録データとを生成する。ここで、入力されるパラメータの種類は予め定められることができる。例えば、登録データとして登録するパラメータでもよい。ここで、登録データは、上述の入力データ（第１入力データ）のコミットメント（第１コミットメント）と証明データ（第１証明データ）の一部又は全部を含むことができる。

【００６２】

登録データ記憶装置３００は、登録データの識別子（ＩＤ）と、登録データとを入力し、それらを対にして（関連づけて）、すなわち（ＩＤ、登録データ）を記憶する。

【００６３】

認証用データ記憶装置４００は、登録データ生成装置１００の認証用データ生成部１０３が生成した認証用データを受信し、認証用データを記憶する。

【００６４】

認証データ生成装置５００は、例えば、認証要求部５０１と、コミットメント生成部５０２と、証明生成部５０３と、認証データ生成部５０４とを有する。認証要求部５０１は、認証用データ記憶装置４００から受信（抽出）した認証用データに含まれる識別子（ＩＤ）を入力し、識別子（ＩＤ）を含む認証要求を生成する。コミットメント生成部５０２は、認証要求に対して認証データ検証装置６００から受信したチャレンジと、パラメータと、認証用データと、入力データ（第２入力データ）とを入力し、コミットメント（第２コミットメント）を生成する。ここで、入力データは、認証を受けるデータであり、登録データと照合されるデータであり、例えば生体情報である。ここでの入力データは、本明細書において、第２入力データ又は入力データｙとも称される。証明生成部５０３は、入力データと、パラメータと、コミットメントとを入力し、入力データが入力データ空間に含まれていること、及び、入力データと登録データとの類似度が予め定められた受理範囲に含まれることを示す証明データ（第２証明データ）を生成する。認証データ生成部５０４は、コミットメントと、証明データとを入力し、認証データを生成する。

【００６５】

認証データ検証装置６００は、例えば、チャレンジ生成部６０１と、証明検証部６０２と、認証結果生成部６０３と、を有する。チャレンジ生成部６０１は、認証データ生成装置５００から受信した認証要求を入力する。また、チャレンジ生成部６０１は、認証要求に含まれる登録データの識別子（ＩＤ）に対応した登録データを、登録データ記憶装置３００から受信（抽出）し、所定のパラメータと、登録データからチャレンジを生成する。証明検証部６０２は、パラメータと、認証データ生成装置５００から受信した認証データと、チャレンジとを入力する。また、証明検証部６０２は、認証データに含まれる証明データを検証し、検証結果を生成する。認証結果生成部６０３は、検証結果に基づき認証結果を生成する。

【００６６】

＜３．２．登録及び照合の動作＞

次に、図２及び図３を参照して、本実施形態における情報照合システム１の動作について説明する。図２は、入力データの登録の動作を表し、図３は、入力データと登録データの照合の動作を表す。なお、本実施形態において、データの送付（送信）及び受信は、各

装置間で直接的に送受信されてもよいし、一方の装置が適宜の記憶部にデータを記憶し、他方の装置がデータを読み出すなど間接的な手法でデータを伝達してもよい。

【００６７】

初めに、登録の動作を説明する。まず、登録データ生成装置１００のコミットメント生成部１０１は、上述の入力データとパラメータを取得する（ステップＡ１）。なお、パラメータは、セキュリティパラメータ、受理範囲、及び、入力データのとりうる範囲（空間）を含む公開情報であり、その生成手段は特に限定されない。例えば、登録データ検証装置２００又は認証データ検証装置６００がパラメータ生成機能を有していてもよいし、情報照合システム１の外部で生成してもよい。

【００６８】

コミットメント生成部１０１は、上述の入力データと、パラメータとを入力し、コミットメントを生成する（ステップＡ２）。証明生成部１０２は、上述の入力データと、パラメータと、コミットメントを入力し、入力データが予め定められた入力データ空間に含まれていることを示す証明データを生成し、コミットメントと証明データを登録データ検証装置２００に送付する（ステップＡ３）。

【００６９】

登録データ検証装置２００の証明検証部２０１は、コミットメントと証明データを登録データ生成装置から受信する（ステップＡ３）。証明検証部２０１は、証明データの検証を行う（ステップＡ４）。例えば、証明検証部２０１は、所定のパラメータと、コミットメントと、証明データを入力する。証明検証部２０１は、証明データの検証を行い、検証が失敗（不受理）の場合、処理を停止する。一方、証明検証部２０１は、検証が成功（受理）の場合、登録データの識別子（ＩＤ）を生成し、登録データ生成装置１００に送付する。ここで、識別子（ＩＤ）は、登録データ固有の識別子であり、生成手段は限定されない。例えば、識別子（ＩＤ）の生成の度に増加するカウンター値であってもよいし、乱数値であってもよい。

【００７０】

登録データ生成部２０２は、コミットメント及び証明データを入力し、登録データを生成する（ステップＡ５）。登録データ生成部２０２は、識別子（ＩＤ）及び登録データを、登録データ記憶装置３００に送付する（ステップＡ６）。識別子（ＩＤ）及び登録データを受信した登録データ記憶装置３００は、（ＩＤ，登録データ）の対を記憶する（ステップＡ７）。

【００７１】

登録データ生成装置１００の認証用データ生成部１０３は、ステップＡ４において登録データ検証装置２００から送信された識別子（ＩＤ）と、コミットメントと、証明データから、認証用データを生成する（ステップＡ８）。認証用データ生成部１０３は、認証用データを認証用データ記憶装置４００に送付する（ステップＡ９）。認証用データを受信した認証用データ記憶装置４００は、認証用データを記憶する（ステップＡ１０）。

【００７２】

次に、照合の動作を、図３を用いて説明する。まず、認証データ生成装置５００の認証要求部５０１は、入力データｙと、パラメータとを入力し、さらに認証用データ記憶装置４００から認証用データを受信する（ステップＢ１）。認証要求部５０１は、入力データｙと、パラメータと、認証用データから認証要求を生成し、生成された認証要求を認証データ検証装置６００に送付する（ステップＢ２）。

【００７３】

認証データ検証装置６００のチャレンジ生成部６０１は、認証要求に含まれる識別子（ＩＤ）に対応した登録データを登録データ記憶装置３００から受信（抽出）し、さらに、パラメータを入力してチャレンジを生成し、チャレンジを認証データ生成装置５００に送付する（ステップＢ３）。

【００７４】

認証データ生成装置５００のコミットメント生成部５０２は、チャレンジと、入力デー

タｙと、パラメータと、認証用データを入力し、コミットメントを生成する（ステップＢ４）。証明生成部５０３は、コミットメントと、チャレンジと、入力データｙと、パラメータと、認証用データを入力し、入力データｙが予め定められた入力データの空間に含まれることと、及び、入力データｙと登録データｘの類似度が受理範囲に含まれることを示す証明データを生成する（ステップＢ５）。認証データ生成部５０４は、コミットメントと、証明データを入力し、認証データを生成し、認証データを認証データ検証装置６００に送付する（ステップＢ６）。

【００７５】

認証データ検証装置６００の証明検証部６０２は、認証データと、登録データと、チャレンジと、パラメータを入力し、認証データに含まれる証明データの検証を行い、検証結果を生成する（ステップＢ７）。認証結果生成部６０３は、検証結果を入力し、認証結果を生成し、出力する（ステップＢ８）。

【００７６】

＜３．３．実施例１＞

次に、本実施形態における情報照合システム１の動作の実施例１について説明する。本実施例では、類似度として正規化相関を用いる場合について説明する。入力データは以下の条件を満たすことを仮定する。

【００７７】

（１） 入力データはｎ次元整数ベクトルである。すなわち、ｘ＝（ｘ１，ｘ２，・・・，ｘｎ）であり、各ｘｉは整数とする。

（２） 各ｘｉはａ以上ｂ以下の整数とする。すなわち、ａ≦ｘｉ≦ｂを満たす。ここで、ａ、ｂは予め定められた値であり、例えば整数でもよい。

（３） ｘは正規化されている。すなわち、すべての入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）に対して、$(x_1)^2+(x_2)^2+\cdots+(x_n)^2=A$（Ａは０以上の定数）を満たす。

（４） 入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）と入力データｙ＝（ｙ１，ｙ２，・・・，ｙｎ）が認証受理となるならば、ｘとｙの内積$<x, y>=x_1y_1+x_2y_2+\cdots+x_ny_n$が受理範囲Θに含まれる。

（５） 入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）と入力データｙ＝（ｙ１，ｙ２，・・・，ｙｎ）が認証不受理となるならば、ｘとｙの内積$<x, y>=x_1y_1+x_2y_2+\cdots+x_ny_n$が受理範囲Θに含まれない。

【００７８】

さらに、本実施例では、Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントを利用する。コミットメント（Ｃｏｍｍｉｔ，Ｏｐｅｎ）とは、コミットメントフェーズとオープンフェーズの２つからなるプロトコルである。コミットメントフェーズでは、送信者はある値ｖと乱数ｒを用いて、コミットメントＣｏｍ（ｖ，ｒ）を生成し、受信者に送付する。オープンフェーズでは、送信者はｖ及びｒを受信者に送ることにより、コミットメントＣｏｍ（ｖ，ｒ）をオープンする。ここで、コミットメントは秘匿性及び束縛性を満たすことが望ましい。秘匿性とは、コミットメントＣｏｍ（ｖ，ｒ）からｖに関する情報が得られないという性質である。束縛性とは、Ｃｏｍ（ｖ，ｒ）を、$v' \neq v$としてオープンすることができない、という性質である。Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントは、秘匿性及び束縛性を満たすコミットメント方式であることが知られている。

【００７９】

Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントを説明する。まず、セキュリティパラメータとしてｋ，ｌ，ｔ，ｓが与えられる。現時点では安全性のために、ｋは１０２４以上、ｌは８０以上、ｔは１６０以上、ｓは８０以上の値が推奨されるが、これら以外の値でもよい。また、パラメータとして、ｇ，ｈ，Ｎが与えられている。ここでＮはｋビットの素数ｐ，ｑの積である。ｇ，ｈはそれぞれＮで割った余りの集合Z_Nからランダムに選ばれた元であり、$g=h^x \bmod N$を満たすｘや、$h=g^y \bmod N$を満たすｙは公開されていないこととする。ここで，g^xはｇのｘ乗を意味し、ｍｏｄ Ｎは

Ｎの剰余を意味する。
【００８０】
（コミットメントフェーズ）
入力をvとし、Ｃｏｍ（ｖ，ｒ）＝ｇ＾ｖ・ｈ＾ｒ ｍｏｄ Ｎをコミットメントとする。
【００８１】
（オープンフェーズ）
ｖ，ｒを送付する。
【００８２】
次に、本実施例で用いるゼロ知識証明について説明する。まず、ゼロ知識証明とは、ある人（証明者）が他の人（検証者）に、ある命題が真であることを証明する際に、真であること以外の情報を漏らさずに証明する手法をいう。本実施例では、知識のゼロ知識証明、範囲のゼロ知識証明、及び、２乗のゼロ知識証明を用いる。
【００８３】
例として、離散対数の知識のゼロ知識証明を説明する。ここで、証明者はｇ＾ｘ ｍｏｄ Ｎに対する離散対数ｘを知っているものとし、ｇ＾ｘを知る検証者にｘの知識をゼロ知識証明するものとする。Ｈをハッシュ関数とする。
【００８４】
（証明段階）
（１） ランダムにｗを［１，２＾｛ｌ＋ｔ＋ｓ｝－１］から選ぶ。
（２） ｃ＝Ｈ（ｇ＾ｗ）を計算する。
（３） Ｄ＝ｗ＋ｃ・ｓを計算する。
（４） （ｃ，Ｄ）を検証者に送る。
【００８５】
（検証段階）
（１） ｃ＝Ｈ（ｇ＾Ｄ・（ｇ＾ｘ）＾｛－ｃ｝）が成り立つことを確認する。成り立っていたら受理、成り立っていなかったら不受理とする。
【００８６】
次に、Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントを用いた２乗のゼロ知識証明及び範囲のゼロ知識証明を説明する。
【００８７】
まず、２乗のゼロ知識証明を説明する。証明者は、Ｃｏｍ（ｘ＾２，ｒ）＝ｇ＾｛ｘ＾２｝・ｈ＾ｒがｘの2乗のコミットメントであることを、Ｃｏｍ（ｘ＾２，ｒ）を知る検証者にゼロ知識証明する。Ｈをハッシュ関数とする。
【００８８】
（証明段階）
（１） 乱数ｒ２をランダムに［－２＾ｓ・Ｎ＋１，２＾ｓ・Ｎ－１］から選び、Ｆ＝Ｃｏｍ（ｘ，ｒ２）＝ｇ＾｛ｘ｝・ｈ＾｛ｒ２｝ ｍｏｄ Ｎを計算する。
（２） ｒ３＝ｒ－ｒ２・ｘを計算し、Ｅ＝Ｆ＾ｘ・ｈ＾｛ｒ３｝ ｍｏｄ Ｎを計算する。
（３） ｗを［１，２＾｛ｌ＋ｔ｝・Ｎ－１］から、ηＦを［１，２＾｛ｌ＋ｔ＋ｓ｝・Ｎ－１］から、ηＥを［１，２＾｛ｌ＋ｔ＋ｓ｝・Ｎ－１］からそれぞれランダムに選び、ＷＦ＝ｇ＾｛ｗ｝・ｈ＾｛ηＦ｝ ｍｏｄ Ｎ、ＷＥ＝Ｆ＾｛ｗ｝・ｈ＾｛ηＥ｝ ｍｏｄ Ｎを計算する。さらに、ｃ＝Ｈ（ＷＦ｜｜ＷＥ）を計算し、Ｄ＝ｗ＋ｃ・ｘ、ＤＦ＝ηＦ＋ｃ・ｒ２、ＤＥ＝ηＥ＋ｃ・ｒ３を計算する。
（４） （Ｆ，ｃ，Ｄ，ＤＦ，ＤＥ）を検証者に送付する。
【００８９】
（検証段階）
（１） ｃ＝Ｈ（ｇ＾Ｄ・ｈ＾｛ＤＦ｝Ｆ＾｛－ｃ｝ ｍｏｄ Ｎ｜｜Ｆ＾｛Ｄ｝・ｈ＾｛ＤＥ｝・Ｅ＾｛－ｃ｝ ｍｏｄ Ｎ）を確認する。等号が成り立っていたら受理、成り立っていなかったら不受理とする。
【００９０】

次に、範囲のゼロ知識証明を説明する。証明者はＥ＝Ｃｏｍ（ｘ，ｒ）＝ｇ＾ｘ・ｈ＾ｒ ｍｏｄ Ｎがａ≦ｘ≦ｂのコミットメントであることを、Ｃｏｍ（ｘ，ｒ）及びａ，ｂを知る検証者にゼロ知識証明する。なお、Ｈをハッシュ関数とする。ｆｌｏｏｒ（ｘ）をｘの小数点以下切り捨てを意味する関数とする。

【００９１】

（証明段階）

（１） ｘの知識のゼロ知識証明を行う。

（２） Ｅ１＝Ｅ／ｇ＾ａ ｍｏｄ ＮとＥ２＝ｇ＾ｂ／Ｅ ｍｏｄ Ｎを計算する。また，ｘ１＝ｘ－ａ，ｘ２＝ｂ－ｘとする。

（３） ｘ１１＝ｆｌｏｏｒ（√（ｘ１））、ｘ１２＝ｘ１－（ｘ１１）＾２、ｘ２１＝ｆｌｏｏｒ（√（ｘ２））、ｘ２２＝ｘ２－（ｘ２１）＾２とする。

（４） ｒ１１とｒ２１を［－２＾ｓ・Ｎ＋１，２＾ｓ・Ｎ－１］から，それぞれランダムに選ぶ。ｒ１２＝ｒ－ｒ１１，ｒ２２＝－ｒ－ｒ２１とする。

（５） Ｅ１１＝Ｃｏｍ（（ｘ１１）＾２，ｒ１１）、Ｅ１２＝Ｃｏｍ（（ｘ１２），ｒ１２）、Ｅ２１＝Ｃｏｍ（（ｘ２１）＾２，ｒ２１）、Ｅ２２＝Ｃｏｍ（（ｘ２２）＾２，ｒ２２）とする。

（６） Ｅ１１，Ｅ２１を検証者に送る。検証者は、Ｅ１２＝Ｅ１／Ｅ１１、Ｅ２２＝Ｅ２／Ｅ２１を計算する。

（７） Ｅ１１とＥ２１がそれぞれｘ１１，ｘ２１の二乗であることを、二乗のゼロ知識証明を用いて証明する。

（８） ｗ１，ｗ２を［０，２＾｛ｔ＋ｌ｝・２√（ｂ－ａ）］、η１，η２を［－２＾｛ｔ＋ｌ＋ｓ｝Ｎ＋１，２＾｛ｔ＋ｌ＋ｓ｝Ｎ－１］からランダムに選ぶ。Ｗ１＝ｇ＾｛ｗ１｝・ｈ＾｛η１｝ ｍｏｄ Ｎ，Ｗ２＝ｇ＾｛ｗ２｝・ｈ＾｛η２｝ ｍｏｄ Ｎを計算する。

（９） ｃ＝Ｈ（Ｗ１，Ｗ２）を計算する。

（１０） Ｄ１１＝ｗ１＋ｘ１２・ｃ，Ｄ１２＝η１＋ｒ１２・ｃ，Ｄ２１＝Ｗ２＋ｘ２２・ｃ，Ｄ２２＝η２＋ｒ２２・ｃを計算し、（ｃ，Ｄ１１，Ｄ１２，Ｄ２１，Ｄ２２）を検証者に送付する。

【００９２】

（検証段階）

（１） 証明のステップ１における知識のゼロ知識証明及びステップ７における二乗のゼロ知識証明をそれぞれ検証する。１つでも不受理があれば、検証の処理を停止する。

（２） ｃ＝Ｈ（ｇ＾｛Ｄ１１｝・ｈ＾｛Ｄ１２｝・Ｅ１２＾｛－ｃ｝，ｇ＾｛Ｄ２１｝・ｈ＾｛Ｄ２２｝・Ｅ２２＾｛－ｃ｝）が成立することを確認する。等号が成り立っていたら受理の検証結果，成り立っていなかったら不受理の検証結果を出力する。

【００９３】

次に、本実施例の情報照合システム１の登録の動作について説明する。まず、登録データ生成装置１００は、入力として、パラメータと入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）を受け取る（ステップＡ１）。

【００９４】

コミットメント生成部１０１は、ｉ＝１，…，ｎに対して、以下の処理を行う。

（１） Ｅｉ＝Ｃｏｍ（ｘｉ，ｒｉ），Ｆｉ＝Ｃｏｍ（（ｘｉ）＾２，ｒ'ｉ）を生成する（ステップＡ２）。すなわち、入力データに基づくコミットメントを生成する。ここで、ｒｉは、ステップＡ１で入力されたパラメータに含まれてもよい。

【００９５】

証明生成部１０２は、ｉ＝１，…，ｎに対して、以下の処理を行う（ステップＡ３）。

（１） 次の４つのゼロ知識証明を行う。（１）Ｅｉを用いて、ｘｉの知識証明，（２）Ｅｉを用いて、ａ≦ｘｉ≦ｂであることのゼロ知識証明，（３）Ｆｉを用いて、ｘｉの二乗のゼロ知識証明。

（２） さらに、Ｆ１，…，Ｆｎを用いて、（４）Σ（ｘｉ）＾２＝（ｘ１）＾２＋（ｘ

２）＾２＋…＋（ｘｎ）＾２＝Ａであることのゼロ知識証明を生成する。これはＦ１・Ｆ２・…・Ｆｎ＝ｇ＾｛Σ（ｘｉ）＾2｝・ｈ＾｛Σ（ｒ'ｉ）｝であるため、Ｆ１・Ｆ２・…・Ｆｎ／ｇ＾Ａ＝ｈ＾｛Σ（ｒ'ｉ）｝となり、Σ（ｒ'ｉ）の知識のゼロ知識証明を用いて実現できる。

【００９６】

証明生成部１０２は、コミットメントと証明データを、登録データ検証装置２００に送付する（ステップＡ３）。

【００９７】

コミットメントと証明データを受信した登録データ検証装置２００の証明検証部２０１は、上述の（１）から（３）のゼロ知識証明の検証を行う。１つでも検証不受理であれば検証の処理を停止する。一方、すべて検証受理であれば、証明検証部２０１は、登録データの識別子（ＩＤ）を生成し、識別子（ＩＤ）を登録データ生成装置１００に送付する（ステップＡ４）。

【００９８】

登録データ生成部２０２は、コミットメント｛Ｅｉ｝を登録データとする（ステップＡ５）。登録データ生成部２０２は、識別子（ＩＤ）と登録データの対（ＩＤ，登録データ）を登録データ記憶装置３００に送付する（ステップＡ６）。登録データ記憶装置３００は、（ＩＤ，登録データ）を記憶する（ステップＡ７）。

【００９９】

ステップＡ４において識別子（ＩＤ）を受信した登録データ生成装置１００の認証用データ生成部１０３は、（ＩＤ，｛ｒｉ｝）を認証用データとして生成する（ステップＡ８）。認証用データ生成部１０３は、認証用データを認証用データ記憶装置４００に送付する（ステップＡ９）。認証用データ記憶装置４００は、認証用データを記憶する（ステップＡ１０）。

【０１００】

次に、本実施例の情報照合システム１の照合の動作について説明する。まず、認証データ生成装置５００の認証要求部５０１は、入力データｙ＝（ｙ１，ｙ２，．．．，ｙｎ）と、パラメータとを入力として受け取り、認証用データ記憶装置４００から認証用データ（ＩＤ，｛ｒｉ｝）を受信（抽出）する（ステップＢ１）。一例として、入力データｙともにログインＩＤ又はユーザの識別番号等を入力し、これらに関連づけられて記憶された認証用データを読み出してもよい。

【０１０１】

認証要求部５０１は、認証要求として、登録データの識別子（ＩＤ）を含むＲｅｑｕｅｓｔを認証データ検証装置６００に送付する（ステップＢ２）。

【０１０２】

チャレンジ生成部６０１は、識別子（ＩＤ）に対応する登録データ（ＩＤ、｛Ｅｉ｝）を登録データ記憶装置３００から受信（抽出）し、ランダムな値ｃを用いて、｛（Ｅｉ）＾ｃ｝，ｈ＾ｃをチャレンジとし、チャレンジを認証データ生成装置５００に送付する（ステップＢ３）。

【０１０３】

認証データ生成装置５００のコミットメント生成部５０２は、各ｉ＝１，２，…，ｎに対して、以下の処理を行う。

（１）　Ｃｏｍ（ｙｉ，Ｒｉ）＝ｇ＾｛ｙｉ｝・ｈ＾｛Ｒｉ｝ ｍｏｄ Ｎ、Ｃｏｍ（（ｙｉ）＾２，Ｒ'ｉ）＝ｇ＾｛（ｙｉ）＾2｝・ｈ＾｛Ｒ'ｉ｝ ｍｏｄ Ｎ、Ｃｏｍ（ｘｉｙｉ，Ｒ”ｉ）＝（（Ｅｉ）＾ｃ）＾｛ｙｉ｝・ｈ＾｛Ｒ”ｉ｝ ｍｏｄ Ｎを計算する（ステップＢ４）

【０１０４】

証明生成部５０３は、各ｉ＝１，２，…，ｎに対して以下の処理を行う。

（１）　（１）Ｃｏｍ（ｙｉ，Ｒｉ）を用いて、ｙｉの知識のゼロ知識証明，（２）Ｃｏｍ（ｙｉ，Ｒｉ）を用いて、ａ≦ｙｉ≦ｂの範囲のゼロ知識証明，（３）Ｃｏｍ（（ｙｉ

）＾２，Ｒ'ｉ）を用いて、ｙｉの二乗のゼロ知識証明。
（２）　次に、（４）Σ（ｙｉ）＾２＝（ｙ１）＾２＋（ｙ２）＾２＋…＋（ｙｎ）＾２＝Ａであることのゼロ知識証明を生成する。これは登録の時と同様の方法で実現できる。
（３）　次に、Ｃｏｍ（ｘｉｙｉ，Ｒ”ｉ）を用いて、（５）＜ｘ，ｙ＞が受理範囲Θに含まれることのゼロ知識証明を生成する。これも登録の時と同様の方法で実現できる。すなわち、Ｃｏｍ（ｘ１ｙ１，Ｒ”１）・Ｃｏｍ（ｘ２ｙ２，Ｒ”２）・…・Ｃｏｍ（ｘｎｙｎ，Ｒ”ｎ）＝ｇ＾｛ｃ＜ｘ，ｙ＞｝（ｈ＾｛ｃ｝）＾｛Σ（ｙｉ・ｒｉ）＋Σ（Ｒ”ｉ）｝であるため、ｈ＾ｃに対して、Σ（ｙｉ・ｒｉ）＋Σ（Ｒ”ｉ）の知識のゼロ知識証明を生成する（ステップＢ５）。

【０１０５】
　認証データ生成部５０４は、コミットメントと（１）から（５）の証明を証明データとして、認証データ検証装置６００に送付する（ステップＢ６）。

【０１０６】
　証明検証部６０２は、（１）から（５）の証明を検証し、すべてが受理であれば検証結果を受理にし、そうでなければ検証結果を不受理にする（ステップＢ７）。ここで、（４）の検証は、Ｃｏｍ（（ｙ１）＾２，Ｒ'１）・Ｃｏｍ（（ｙ２）＾２，Ｒ'２）・…・Ｃｏｍ（（ｙｎ）＾２，Ｒ'ｎ）＝ｇ＾｛Σ（ｙｉ）＾２｝・ｈ＾｛Σ（Ｒ'ｉ）｝ｍｏｄ Ｎであるため、Ｃｏｍ（（ｙ１）＾２，Ｒ'１）・Ｃｏｍ（（ｙ２）＾２，Ｒ'２）・…・Ｃｏｍ（（ｙｎ）＾２，Ｒ'ｎ）／ｇ＾｛Ａ｝として、ゼロ知識証明の検証を行うことにより実現できる。同様にして（５）の検証は、受理範囲Θに含まれる値θに対して、Ｃｏｍ（ｘ１ｙ１，Ｒ”１）・Ｃｏｍ（ｘ２ｙ２，Ｒ”２）・…・Ｃｏｍ（ｘｎｙｎ，Ｒ”ｎ）／ｇ＾｛ｃθ｝として、ゼロ知識証明の検証を行うことにより実現できる。

【０１０７】
　認証結果生成部６０３は、検証結果が受理であれば、認証結果を受理とし、そうでなければ認証結果を不受理とする（ステップＢ８）。

【０１０８】
　なお、本実施例の説明では、ｘ、ｙのすべての次元に対して、ｘｉ（又はｙｉ）がａ≦ｘｉ≦ｂであることを証明しているが、その一部（例えば半分など）を証明するのでもよい。証明させる次元の選び方は限定されない。例えば、証明させる次元を登録データ検証装置２００又は認証データ検証装置６００がランダムに選んでもよい。

【０１０９】
　また、本実施例の説明では、各ゼロ知識証明を独立に行うように説明しているが、並列に実行する際によく知られた効率化を行ってもよい。例えば、各ゼロ知識証明の中でハッシュ関数の計算を行っているが、それを１度に合わせて計算してもよい。同様に、各ゼロ知識証明の中でｘｉ又はｙｉに関する知識の証明を行っているが、それを１度にまとめてしまっても構わない。

【０１１０】
　さらに、本実施例の説明では、登録データ生成装置１００及び認証データ生成装置５００がハッシュ関数を用いてｃを計算しているが、それを登録データ検証装置２００及び認証データ検証装置６００が生成した乱数値ｃと置き換えてもよい。このとき検証時に確認する式は、ハッシュ値の一致を確認するのではなく、ｃに関係する計算結果の一致を確認するものと変わる。

【０１１１】
　なお、本実施例の説明では、入力データが入力データの空間に含まれることや、入力データと登録データの類似度が受理範囲に含まれることを、それぞれゼロ知識証明を用いて証明しているが、すべてを秘匿する必要のない場合は、コミットメントのオープンを実行してもよい。例えば入力データの各次元の値の二乗和が定数Ａであることは、コミットメントに用いられた乱数を明らかにすることでも容易に検証できる。

【０１１２】
　＜３．４．実施例２＞

次に、本実施形態における情報照合システム１の動作の実施例２について説明する。
【０１１３】
本実施例では、類似度として二乗ユークリッド距離を用いる場合について説明する。入力データは以下の条件を満たすことを仮定する。
（１） 入力データはｎ次元整数ベクトルである。すなわち、ｘ＝（ｘ１，ｘ２，・・・，ｘｎ）であり、各ｘｉは整数とする。
（２） 各ｘｉはａ以上ｂ以下の整数とする。すなわち、ａ≦ｘｉ≦ｂを満たす。
（３） 入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）と入力データｙ＝（ｙ１，ｙ２，・・・，ｙｎ）が認証受理となるならば、ｘとｙのユークリッド距離の二乗ｄ（ｘ，ｙ）＝（ｘ１－ｙ１）＾２＋（ｘ２－ｙ２）＾２＋…＋（ｘｎ－ｙｎ）＾２が受理範囲Θに含まれる。
（４） 入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）と入力データｙ＝（ｙ１，ｙ２，・・・，ｙｎ）が認証不受理となるならば、ｘとｙのユークリッド距離の二乗ｄ（ｘ，ｙ）＝（ｘ１－ｙ１）＾２＋（ｘ２－ｙ２）＾２＋…＋（ｘｎ－ｙｎ）＾２が受理範囲Θに含まれない。
【０１１４】
次に、本実施例の情報照合システム１の登録の動作について説明する。まず、登録データ生成装置１００は、入力として、パラメータと入力データｘ＝（ｘ１，ｘ２，・・・，ｘｎ）を受け取る（ステップＡ１）。
【０１１５】
コミットメント生成部１０１は、ｉ＝１，…，ｎに対して、以下の処理を行う。すなわち、Ｅｉ＝Ｃｏｍ（ｘｉ，ｒｉ），Ｆｉ＝Ｃｏｍ（（ｘｉ）＾２，ｒ'ｉ）を生成する（ステップＡ２）。
【０１１６】
証明生成部１０２は、ｉ＝１，…，ｎに対して、以下の処理を行う（ステップＡ３）。すなわち、次の３つのゼロ知識証明を行う。（１）Ｅｉを用いて、ｘｉの知識証明，（２）Ｅｉを用いて、ａ≦ｘｉ≦ｂであることのゼロ知識証明，（３）Ｆｉを用いて、ｘｉの二乗のゼロ知識証明。
【０１１７】
証明生成部１０２は、コミットメントと証明データを登録データ検証装置２００に送付する（ステップＡ３）。
【０１１８】
コミットメントと証明データを受信した登録データ検証装置２００の証明検証部２０１は、上述の（１）から（３）のゼロ知識証明の検証を行う。証明検証部２０１は、１つでも検証不受理であれば検証の処理を停止する。一方、すべて検証受理であれば、証明検証部２０１は、登録データの識別子（ＩＤ）を生成し、識別子（ＩＤ）を登録データ生成装置１００に送付する（ステップＡ４）。
【０１１９】
登録データ生成部２０２は、（｛Ｅｉ｝、Ｆ＝Ｆ１・Ｆ２・…・Ｆｎ）を登録データとする（ステップＡ５）。登録データ生成部２０２は、識別子（ＩＤ）と登録データの対（ＩＤ，登録データ）を登録データ記憶装置３００に送付する（ステップＡ６）。登録データ記憶装置３００は、（ＩＤ，登録データ）を記憶する（ステップＡ７）。
【０１２０】
ステップＡ４において識別子（ＩＤ）を受信した登録データ生成装置１００の認証用データ生成部１０３は、（ＩＤ，｛ｒｉ｝，ｒ'＝Σ（ｒ'ｉ））を認証用データとして生成する（ステップＡ８）。認証用データ生成部１０３は、認証用データを認証用データ記憶装置４００に送付する（ステップＡ９）。認証用データ記憶装置４００は、認証用データを記憶する（ステップＡ１０）。
【０１２１】
次に、本実施例の情報照合システム１の照合の動作について説明する。まず、認証デー

タ生成装置５００の認証要求部５０１は、入力データｙ＝（ｙ１，ｙ２，．．．，ｙｎ）と、パラメータとを入力として受け取り、認証用データ記憶装置４００から認証用データ（ＩＤ，｛ｒｉ｝，ｒ'）を受信（抽出）する（ステップＢ１）。一例として、入力データｙともにログインＩＤ又はユーザの識別番号等を入力し、これらに関連づけられて記憶された認証用データを読み出してもよい。

【０１２２】

認証要求部５０１は、認証要求として、登録データの識別子（ＩＤ）を含むＲｅｑｕｅｓｔを認証データ検証装置６００に送付する（ステップＢ２）。

【０１２３】

チャレンジ生成部６０１は、識別子（ＩＤ）に対応する登録データ（ＩＤ、｛Ｅｉ｝，Ｆ）を登録データ記憶装置３００から受信（抽出）し、ランダムな値ｃを用いて、｛（Ｅｉ）＾ｃ｝，ｈ＾ｃをチャレンジとし、チャレンジを認証データ生成装置５００に送付する（ステップＢ３）。

【０１２４】

認証データ生成装置５００のコミットメント生成部５０２は、各ｉ＝１，２，…，ｎに対して、以下の処理を行う。

（１）　Ｃｏｍ（ｙｉ，Ｒｉ）＝ｇ＾｛ｙｉ｝・ｈ＾｛Ｒｉ｝ ｍｏｄ Ｎ、Ｃｏｍ（（ｙｉ）＾２，Ｒ'ｉ）＝ｇ＾｛（ｙｉ）＾２｝・ｈ＾｛Ｒ'ｉ｝ ｍｏｄ Ｎ、Ｃｏｍ（ｘｉｙｉ，Ｒ”ｉ）＝（（Ｅｉ）＾ｃ）＾｛ｙｉ｝・ｈ＾｛Ｒ”ｉ｝ ｍｏｄ Ｎを計算する（ステップＢ４）。

（２）　次に、証明生成部５０３は、各ｉ＝１，２，…，ｎに対して以下の処理を行う。

（３）　（１）Ｃｏｍ（ｙｉ，Ｒｉ）を用いて、ｙｉの知識のゼロ知識証明，（２）Ｃｏｍ（ｙｉ，Ｒｉ）を用いて、ａ≦ｙｉ≦ｂの範囲のゼロ知識証明，（３）Ｃｏｍ（（ｙｉ）＾２，Ｒ'ｉ）を用いて、ｙｉの二乗のゼロ知識証明。

（４）　次に、Ｃｏｍ（ｘｉｙｉ，Ｒ”ｉ）と、Ｃｏｍ（（ｙｉ）＾２，Ｒ'ｉ）と、｛ｒｉ｝と、ｒ'を用いて、（４）ｄ（ｘ，ｙ）が受理範囲Θに含まれることのゼロ知識証明を生成する。これは、Ｃｏｍ（Σ（（ｘｉ）＾２），ｒ'）・Ｃｏｍ（（ｙ１）＾２，Ｒ'１）・…・Ｃｏｍ（（ｙｎ）＾２，Ｒ'ｎ）・（Ｃｏｍ（（ｘ１ｙ１，Ｒ”１）・Ｃｏｍ（ｘ２ｙ２，Ｒ”２）・…・Ｃｏｍ（ｘｎｙｎ，Ｒ”ｎ））＾｛－２／ｃ｝）＝ｇ＾｛Σ（ｘｉ）＾２＋Σ（ｙｉ）＾２－２＜ｘ，ｙ＞｝（ｈ）＾｛ｒ'＋Σ（Ｒ'ｉ）＋Σ（ｙｉ・ｒｉ）＋Σ（Ｒ”ｉ）｝であるため、ｈに対して、ｒ'＋Σ（Ｒ'ｉ）＋Σ（ｙｉ・ｒｉ）＋Σ（Ｒ”ｉ）の知識のゼロ知識証明を生成する（ステップＢ５）。

【０１２５】

認証データ生成部５０４は、コミットメントと（１）から（４）の証明を証明データとして、認証データ検証装置６００に送付する（ステップＢ６）。

【０１２６】

証明検証部６０２は、（１）から（４）の証明を検証し、すべてが受理であれば検証結果を受理にし、そうでなければ検証結果を不受理にする（ステップＢ７）。

【０１２７】

認証結果生成部６０３は、検証結果が受理であれば、認証結果を受理とし、そうでなければ認証結果を不受理とする（ステップＢ８）。

【０１２８】

本実施例の説明では、ｘ、ｙのすべての次元に対して、ｘｉ（又はｙｉ）がａ≦ｘｉ≦ｂであることを証明しているが、その一部（例えば半分など）を証明するのでもよい。証明させる次元の選び方は問わない。例えば、証明させる次元を登録データ検証装置２００又は認証データ検証装置６００がランダムに選んでもよい。

【０１２９】

また、本実施例の説明では、各ゼロ知識証明を独立に行うように説明しているが、並列に実行する際によく知られた効率化を行ってもよい。例えば、各ゼロ知識証明の中でハッシュ関数の計算を行っているが、それを１度に合わせて計算してもよい。同様に、各ゼロ

知識証明の中でｘｉ又はｙｉに関する知識の証明を行っているが、それを１度にまとめてしまっても構わない。

【０１３０】

さらに、本実施例の説明では、登録データ生成装置１００及び認証データ生成装置５００がハッシュ関数を用いてｃを計算しているが、それを登録データ検証装置２００及び認証データ検証装置６００が生成した乱数値ｃと置き換えてもよい。このとき検証時に確認する式は、ハッシュ値の一致を確認するのではなく、ｃに関係する計算結果の一致を確認するものと変わる。

【０１３１】

なお、本実施例の説明では、入力データが入力データの空間に含まれることや、入力データと登録データの類似度が受理範囲に含まれることを、それぞれゼロ知識証明を用いて証明しているが、すべてを秘匿する必要のない場合は、コミットメントのオープンを実行してもよい。

【０１３２】

（効果）

上述した本実施形態における効果のひとつは、生体から生成されていないデータを入力データとして、登録データを生成することや、認証データを生成することを不可能にしていることである。また、これにより、より安全な情報照合システム１を実現することが可能になる。また、例えば、ステップＡ２及びＡ３によって、入力データが予め定められた入力データの空間にあることをゼロ知識証明を用いて検証できる。

【０１３３】

上述した本実施形態では、登録データはＦｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントのコミットメントと識別子（ＩＤ）である。Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏコミットメントは情報理論的な秘匿性を満たすことが知られており、生体特徴量のコミットメントは乱数と見分けがつかないことが数学的に示されている。したがって、万が一コミットメントが漏洩したとしても、生体特徴量は漏洩しない。また、認証用データは、コミットメント生成時に使用した乱数と識別子ＩＤである。明かに、認証用データから生体特徴量に関する情報は漏洩しない。

【０１３４】

＜＜４．その他＞＞

図４は、装置のハードウェア構成を示すブロック図である。上述の各装置は、物理的に以下の構成を有することができる。装置１０は、例えば、入力部１１と、出力部１２と、記憶部１３と、処理部１４とを有する。

【０１３５】

入力部１１は、データ、情報、信号等を入力する。入力部１１は、例えば、他の装置からデータ等を受信するインターフェース、ユーザからの入力を受け付ける操作部、生体情報を読み取る読取装置などでもよい。出力部１２は、データ、情報、信号等を出力する。出力部１２は、例えば、他の装置へデータ等を送信するインターフェース、画面を表示する表示部などでもよい。記憶部１３は、装置１０の動作のためのプログラム及びパラメータ、並びに様々なデータを、一時的に又は恒久的に記憶する。処理部１４は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）などの１つ以上のプロセッサで構成される。処理部１４は、例えば記憶部１３に記憶されたプログラムを実行して、上述の各装置の動作を行ってもよい。プログラムは、上述の各装置の動作をプロセッサに実行させるためのプログラムであってもよい。

【０１３６】

上記実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

【０１３７】

（付記１）

登録のための第１入力データの第１コミットメントと、第１入力データが予め定められ

た入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成装置と、
前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶装置と、
前記第１コミットメントと前記第１証明データの検証を行う登録データ検証装置と、
前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶装置と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていること及び前記第２入力データと前記登録データ記憶装置の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成装置と、
前記第２コミットメントと前記第２証明データの検証を行う認証データ検証装置と
を備えた情報照合システム。
【０１３８】
（付記２）
付記１に記載の情報照合システムであって、
前記登録データ生成装置が生成する第１証明データの一部又は全部が、ゼロ知識証明によるデータである
ことを特徴とする情報照合システム。
【０１３９】
（付記３）
付記１又は２に記載の情報照合システムであって、
前記認証データ生成装置が生成する前記第２証明データの一部又は全部が、ゼロ知識証明によるデータである
ことを特徴とする情報照合システム。
【０１４０】
（付記４）
付記１～３のいずれか１項に記載の情報照合システムであって、
前記登録データ記憶装置に記憶された前記登録データが、前記第１入力データの前記第１コミットメントを含む
ことを特徴とする情報照合システム。
【０１４１】
（付記５）
付記１～４のいずれか１項に記載の情報照合システムであって、
前記認証用データ記憶装置に記憶された認証用データが、前記第１入力データの前記第１コミットメントを生成する際に用いた乱数を含む
ことを特徴とする情報照合システム。
【０１４２】
（付記６）
付記１～５のいずれか１項に記載の情報照合システムであって、
前記登録データ生成装置が生成する前記第１コミットメントの一部又は全部が、パラメータｇ、ｈ、Ｎ、前記第１入力データｘ、乱数ｒに対して、ｇ＾ｘ・ｈ＾ｒ ｍｏｄ Ｎである
ことを特徴とする情報照合システム。
【０１４３】
（付記７）
付記１～６のいずれか１項に記載の情報照合システムであって、
前記認証データ生成装置が生成する前記第２コミットメントの一部又は全部が、パラメータｇ、ｈ、Ｎ、前記第２入力データｙ、乱数ｒに対して、ｇ＾ｙ・ｈ＾ｒ ｍｏｄ Ｎである

ことを特徴とする情報照合システム。
【０１４４】
（付記８）　登録のための第１入力データの第１コミットメントと、前記第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを含む登録データを生成する登録データ生成部と、
前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶部と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていること及び前記第２入力データと前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成部と
を備えたクライアント端末。
【０１４５】
（付記９）
登録のための第１入力データの第１コミットメントと、前記第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを入力し、前記第１コミットメントと前記第１証明データの検証を行う登録データ検証部と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていること及び前記第２入力データと登録データ記憶部の登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データと入力し、前記第２コミットメントと前記第２証明データの検証を行う認証データ検証部と
の少なくとも一方を備えたサーバ。
【０１４６】
（付記１０）
登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成処理と、
前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶処理と、
前記第１コミットメントと前記第１証明データの検証を行う登録データ検証処理と、
前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記予め定められた入力データ空間に含まれていること及び前記第２入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成処理と、
前記第２コミットメントと前記第２証明データの検証を行う認証データ検証処理と
を含む情報照合方法。
【０１４７】
（付記１１）
登録のための第１入力データの第１コミットメントと、第１入力データが予め定められた入力データ空間に含まれていることを示す第１証明データとを生成する登録データ生成処理と、
前記第１コミットメントと前記第１証明データの一部又は全部を記憶する認証用データ記憶処理と、
前記第１コミットメントと前記第１証明データの検証を行う登録データ検証処理と、
前記第１コミットメントと前記第１証明データの一部又は全部を登録データとして記憶する登録データ記憶処理と、
認証されるための第２入力データの第２コミットメントと、前記第２入力データが前記

予め定められた入力データ空間に含まれていること及び前記第２入力データと登録データ記憶部の前記登録データの類似度が予め定められた受理範囲に含まれていることを示す第２証明データとを生成する認証データ生成処理と、
　前記第２コミットメントと前記第２証明データの検証を行う認証データ検証処理と
をコンピュータに実行させる情報照合プログラム。
【産業上の利用可能性】
【０１４８】
　前述の通り、各実施形態の技術により、カメラ等のセンサで取得した生体情報と、データベースに保存されている一人又は複数人の生体情報とを、両者の持つ生体情報を互いに秘匿したまま、安全に照合することが可能である。センサの管理者（組織）と、データベースの管理者（組織）が異なる場合に、効果的である。
【０１４９】
　各実施形態の技術は例えば、スマートフォン等を用いてリモートのサーバに対して生体認証を行う際に利用可能である。ユーザ自身が保持するスマートフォンに認証用データを、サーバに登録データをそれぞれ登録し、認証を行う際にスマートフォンで生体情報を採取し、記憶している認証用データを用いて、認証データの生成を行い、サーバがユーザを認証することが可能となる。
【０１５０】
　スマートフォンを用いたリモート生体認証の利用例として、ネットショッピングや会員サービスの利用などが挙げられる。本技術を用いれば、サーバはユーザの生体情報に関して、同一生体であるか否か以外の情報を得ることなく、スマートフォンの生体認証機能を用いてユーザ認証を行うことが可能である。したがって、サーバからのユーザ情報の漏洩リスクを低減できる。
【符号の説明】
【０１５１】
１００　　登録データ生成装置（登録データ生成部）
２００　　登録データ検証装置（登録データ検証部）
３００　　登録データ記憶装置（登録データ記憶部）
４００　　認証用データ記憶装置（認証用データ記憶部）
５００　　認証データ生成装置（認証データ生成部）
６００　　認証データ検証装置（認証データ検証部）

【図面】

【図１】

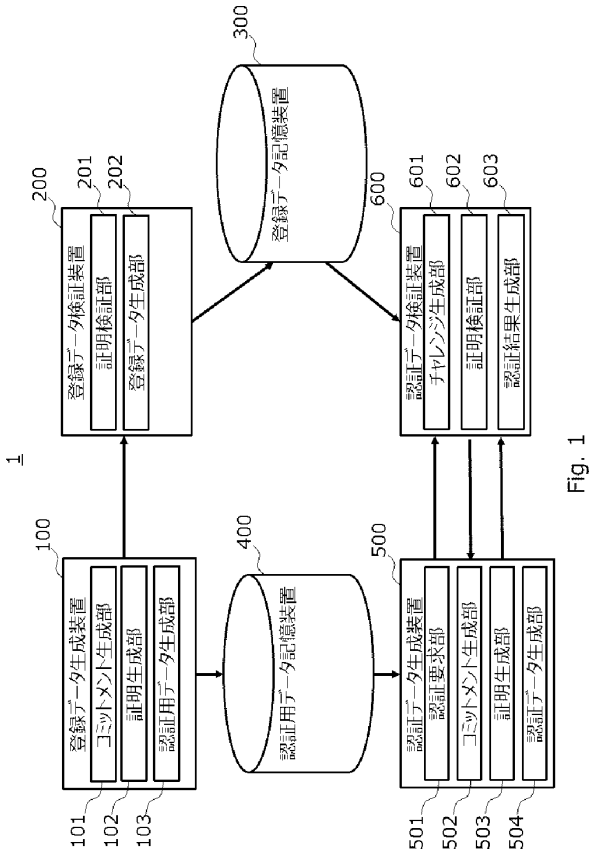

Fig. 1

【図２】

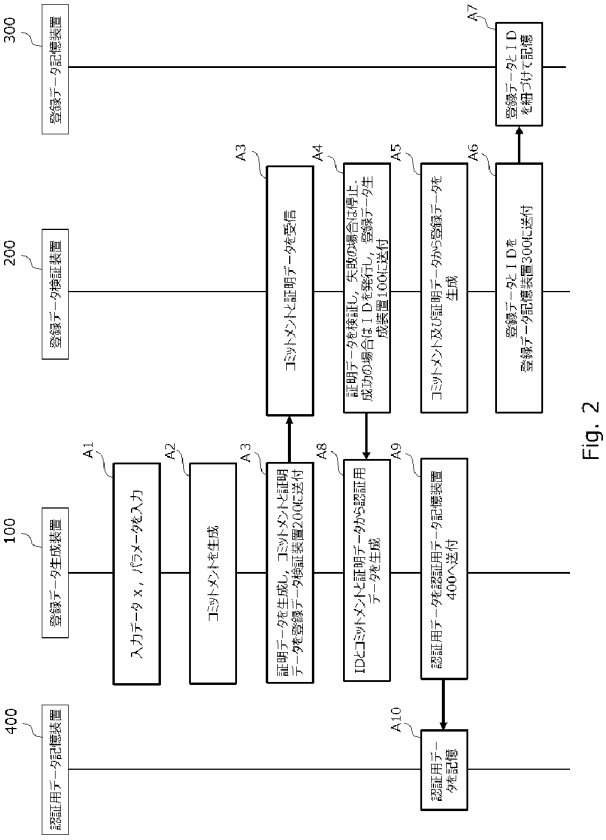

Fig. 2

【図３】

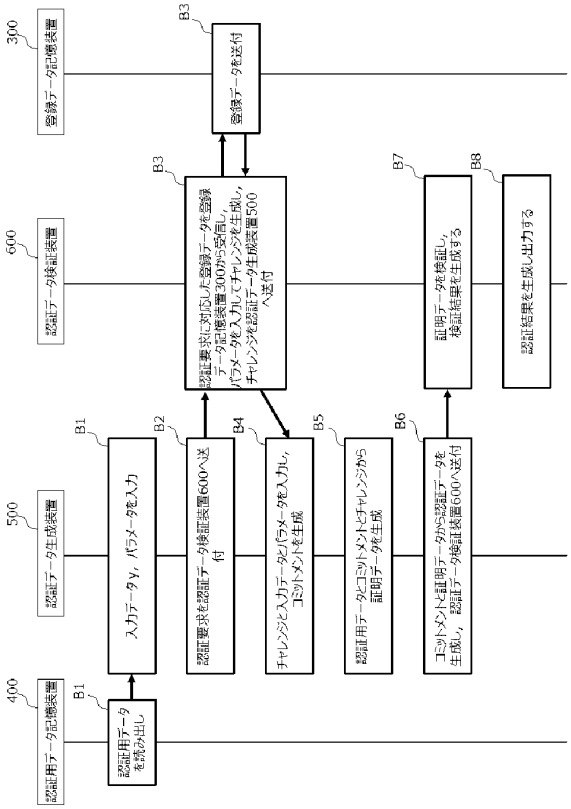

Fig. 3

【図４】

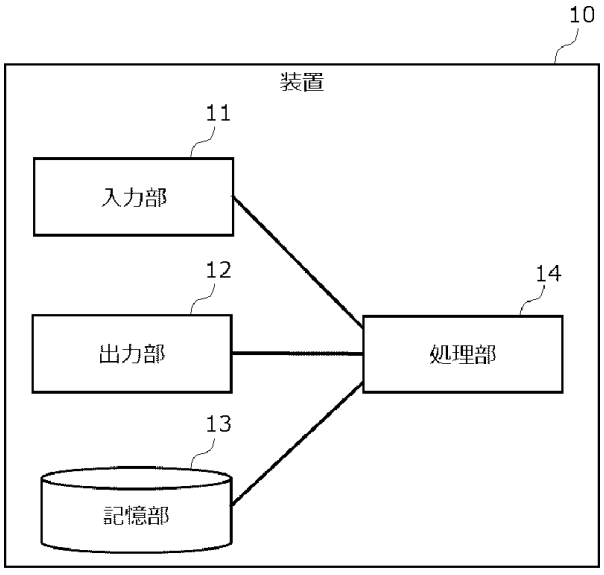

Fig. 4

【図５】

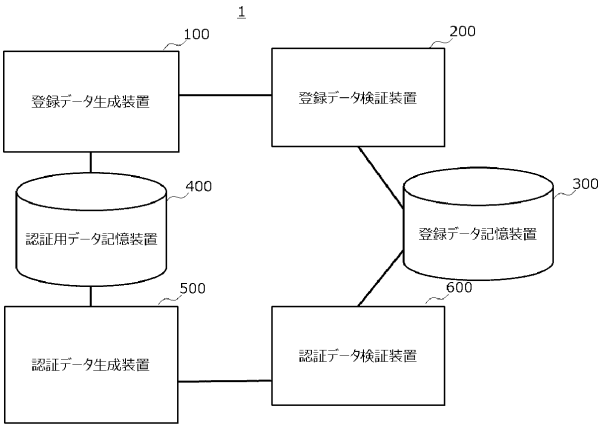

Fig. 5

【図６】

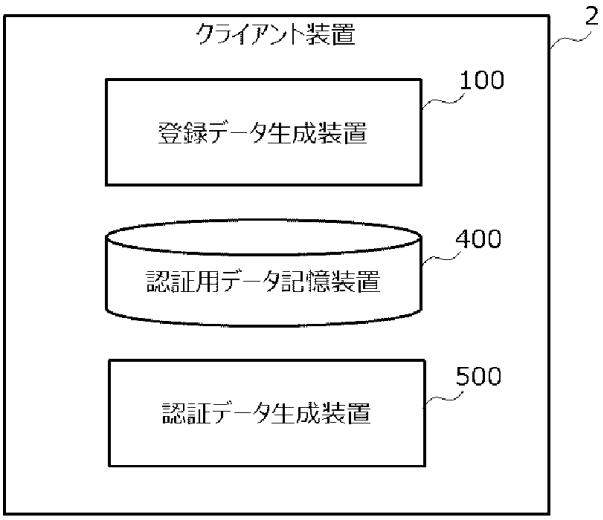

Fig. 6

【図７】

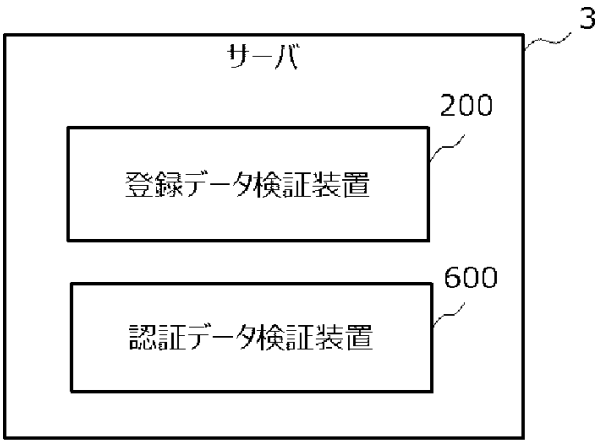

Fig. 7

フロントページの続き

(56)参考文献 国際公開第２０１１／１４８９０２（WO，Ａ１）
特開２０１８－０１４６２２（ＪＰ，Ａ）
国際公開第２０１２／０４２７７５（WO，Ａ１）
米国特許出願公開第２０１９／００２０４８２（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／３２