

明 細 書

発明の名称：生体参照情報登録システム、装置及びプログラム 技術分野

[0001] 本発明の実施形態は、生体参照情報登録システム、装置及びプログラムに関する。

背景技術

[0002] ネットワークを介した通信やサービスを実現する際に、通信相手を認証することは重要な技術要素とされている。近年、オープンなネットワーク環境の普及や、分散されたサービス・リソースの連携技術の発達に伴い、認証対象の範囲がユーザから使用機器端末までに拡大してきている。

[0003] 特に、認証対象者が個人である場合に、個人が本人か否かを確認する技術が現在注目されている。通常、認証では認証実行する際に、認証対象者を厳密に識別又は照合することが要件として挙げられる。このとき、認証対象者が個人である場合、個人が本人か否かを厳密に確認する本人確認技術が必要になる。

[0004] 現在、本人確認を実施する有望な技術として、バイオメトリック認証（生体認証）技術が挙げられる。生体認証は、個々人が有する固有の身体的特徴又は特性を事前に登録した生体情報（以下、生体参照情報という）と照合し、本人か否かを確認するための技術である。生体情報としては、指紋や虹彩、網膜、顔、音声、キーストローク、サインなどが利用されている。

[0005] 生体認証は、パスワードなどの既存の認証方法と異なり、忘却や紛失といった心配の無い生体情報を利用するため、ユーザの負荷を軽減できる。生体情報は複製が困難なものを前提としており、ユーザの成り済ましなどの防止策に有効である。

[0006] また、現在インターネットに代表されるオープンネットワークが普及し、電子商取引などにおいてネットワーク越しに通信相手を認証する方法として生体認証を利用しようとする動きが高まってきている。身分証明などの分野

でも生体認証を利用して、身分証明書の所有者の本人確認を行うことが検討されている。

[0007] このような動きに対し、ネットワークを介して生体認証を行う技術として、生体認証向けの認証コンテキストを用いて行う技術が知られている。具体的には例えば、クライアント側での生体認証に関係するプロセス内容を、生体認証向けの認証コンテキスト（生体認証コンテキスト）情報に纏めて、ネットワーク越しの検証者へ通知する技術が特許文献 1 に開示されている。

[0008] また、生体認証をネットワーク上で利用する場合に、非対称暗号方式に基づいた公開鍵基盤（PKI : Public Key Infrastructure）を用いる方法が知られている。例えば、生体認証の真正性の基準となるクレデンシャル（Credential）である生体参照情報（Biometric Reference Template）と、公開鍵証明書とを関連付ける方法が知られている。この生体参照情報は、生の生体情報（Biometric Raw Data）に特徴抽出処理などを施した情報を指し、照合処理の基準情報となる。但し、照合アルゴリズムによっては、生の生体情報を生体参照情報として用いるものも存在する。既知な代表的技術としては、RFC（request for comments）3739 の標準仕様 X.509 などが知られている。X.509 は、公開鍵証明書に生体参照情報との関連性を表す情報（生体参照情報のハッシュ値）をオプションとして含めることを規定している。また、ISO（International Organization for Standardization）／IEC（International Electrotechnical Commission）24701 においても、BRT 証明書（Biometric Reference Template Certificate）として、生体参照情報のハッシュ値に対してデジタル署名を施したデータを規定している。

[0009] 以上のような生体認証と PKI との組合せとしては、生体認証と、公開鍵証明書を利用したエンティティ認証とを連鎖させることにより、ネットワーク上での利用者認証（本人確認）を間接的に実施する技術が知られている。

[0010] また、生体参照情報を生成するための基情報（生の生体情報など）は、個人の身体的特徴といったセンシティブ（機微）な情報であるため、そのプラ

イバシ性についても考慮する必要がある。このため、生体認証の処理自体を認証対象者側で実施し、生体参照情報等の情報を認証者側に保管しない方法なども考えられている。この方法では、前述したような公開鍵証明書と生体参照情報とを関連付けることにより、生体参照情報のライフサイクル管理を間接的に実施することが可能である。

[0011] しかしながら、以上のような生体認証の技術では、生体参照情報を生体認証システムに登録する際に、任意のクライアント環境からネットワークを介しての登録を行うことができないという不都合がある。

[0012] 例えば、登録する生体参照情報を認証対象者側又は検証者側のいずれで管理する場合でも、生体参照情報を作成するため、認証対象者が検証者の指定する店舗等を訪問し、検証者側が用意したデバイス（生体情報スキャナ等）により生の生体情報を採取する必要がある。これは、クライアント環境の品質と安全性とを一定水準に保つ必要があるためである。すなわち、品質の悪い生体参照情報の登録を阻止して照合精度を一定水準に維持するため、検証者側が用意したクライアント環境により生体情報を採取する必要がある。但し、認証対象者に物理的な移動を強制し、認証対象者の負担を増大させる不都合がある。

[0013] このような不都合を解消する観点から、照合精度を一定水準に維持しつつ、任意のクライアント環境からネットワークを介して生体参照情報を登録するための技術が特許文献2に開示されている。

先行技術文献

特許文献

[0014] 特許文献1：特許第4956096号公報

特許文献2：特開2009-169517号公報

発明の概要

発明が解決しようとする課題

[0015] しかしながら、特許文献2に開示された技術は、本発明者の検討によれば

、生体参照情報を格納するデバイス（可搬媒体など）と生体認証システムとの間で予め秘密情報を共有する必要がある、生体認証システムに密接に関連付けられたデバイスにより運用されると推察される。

[0016] すなわち、特定の生体認証システムは、当該生体認証システムで発行された生体参照情報（及び／又は生体参照情報を保証する情報）のみを登録可能なデバイスを運用すると推察される。このような運用の場合、利用者は、生体認証システム毎に対応するデバイスを保有する必要があるため、負担が大きくなる。

[0017] 本発明が解決しようとする課題は、デバイスと生体認証システムとの間で予め秘密情報を共有せずに、ネットワークを介して生体参照情報を保証及び格納し得る生体参照情報登録システム、装置及びプログラムを提供することである。

課題を解決するための手段

[0018] 実施形態の生体参照情報登録システムは、ネットワークを介して互いに通信可能な生体参照情報格納装置と生体参照情報証明書生成装置とを備えている。前記生体参照情報登録システムは、認証対象者の生体参照情報を前記生体参照情報格納装置に登録する。

[0019] 前記生体参照情報格納装置は、第1秘密鍵記憶手段、チャレンジ情報受信手段、生体参照情報生成手段、ハッシュ値生成手段、第1署名生成手段、生体認証コンテキスト生成手段、生体認証コンテキスト送信手段、証明書受信手段、第1抽出手段、ハッシュ値検証手段、生体認証コンテキスト検証手段、格納手段及び書込手段を備えている。

[0020] 前記第1秘密鍵記憶手段は、自装置の第1秘密鍵を記憶する。

[0021] 前記チャレンジ情報受信手段は、前記生体参照情報証明書生成装置からチャレンジ情報を受信する。

[0022] 前記生体参照情報生成手段は、前記認証対象者から採取した生体情報に基づいて生体参照情報を生成する。

[0023] 前記ハッシュ値生成手段は、前記生体参照情報のハッシュ値を生成する。

- [0024] 前記第1署名生成手段は、前記第1秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第1デジタル署名を生成する。
- [0025] 前記生体認証コンテキスト生成手段は、前記チャレンジ情報、前記生体参照情報のハッシュ値、及び前記第1デジタル署名を含む生体認証コンテキストを生成する。
- [0026] 前記生体認証コンテキスト送信手段は、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信する。
- [0027] 前記証明書受信手段は、前記生体参照情報のハッシュ値及び前記生体認証コンテキストと、当該生体参照情報のハッシュ値及び前記生体認証コンテキストに対する第2デジタル署名とを含む生体参照情報証明書を前記生体参照情報証明書生成装置から受信する。
- [0028] 前記第1抽出手段は、前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出する。
- [0029] 前記ハッシュ値検証手段は、前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証する。
- [0030] 前記生体認証コンテキスト検証手段は、前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証する。
- [0031] 前記格納手段は、前記生体参照情報及び前記生体参照情報証明書を格納するための手段である。
- [0032] 前記書込手段は、前記ハッシュ値検証手段及び前記生体認証コンテキスト検証手段による検証結果がそれぞれ正当性を示す場合、前記生体参照情報及び前記生体参照情報証明書を前記格納手段に書込む。
- [0033] 前記生体参照情報証明書生成装置は、アカウント記憶手段、第2秘密鍵記憶手段、チャレンジ情報送信手段、生体認証コンテキスト受信手段、第2抽出手段、チャレンジ情報検証手段、署名検証手段、第2署名生成手段、証明書生成手段、証明書書込手段及び証明書送信手段を備えている。

- [0034] 前記アカウント記憶手段は、前記認証対象者のユーザID及び前記生体参照情報証明書を互いに関連付けて記憶するための記憶手段である。
- [0035] 前記第2秘密鍵記憶手段は、自装置の第2秘密鍵を記憶している。
- [0036] 前記チャレンジ情報送信手段は、前記チャレンジ情報を生成して当該チャレンジ情報を前記生体参照情報格納装置に送信する。
- [0037] 前記生体認証コンテキスト受信手段は、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信する。
- [0038] 前記第2抽出手段は、前記受信した生体認証コンテキストからチャレンジ情報を抽出する。
- [0039] 前記チャレンジ情報検証手段は、前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証する。
- [0040] 前記署名検証手段は、前記受信した生体認証コンテキスト内の第1デジタル署名を前記第1秘密鍵に対応する第1公開鍵に基づいて検証する。
- [0041] 前記第2署名生成手段は、前記チャレンジ情報検証手段及び前記署名検証手段による検証結果がそれぞれ正当性を示す場合、前記第2秘密鍵に基づいて、前記受信した前記生体参照情報のハッシュ値及び前記生体認証コンテキストに対する前記第2デジタル署名を生成する。
- [0042] 前記証明書生成手段は、前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第2デジタル署名を含む前記生体参照情報証明書を生成する。
- [0043] 前記証明書書込手段は、前記生成された生体参照情報証明書を、前記認証対象者のユーザIDに関連付けて前記アカウント記憶手段に書き込む。
- [0044] 前記証明書送信手段は、前記生成された生体参照情報証明書を前記生体参照情報格納装置に送信する。

図面の簡単な説明

- [0045] [図1]図1は、第1の実施形態に係る生体参照情報登録システムの構成例を示す模式図である。
- [図2]図2は、同実施形態における生体参照情報格納装置の構成例を示す模式

図である。
[図3]図3は、同実施形態における生体認証コンストラクトの構成例を示す模式図である。
[図4]図4は、同実施形態における有効化情報一時保存部を説明するための模式図である。
[図5]図5は、同実施形態における有効化情報一時保存部を説明するための模式図である。
[図6]図6は、同実施形態における生体参照情報証明書生成装置の構成例を示す模式図である。
[図7]図7は、同実施形態における生体参照情報証明書の構成例を示す模式図である。
[図8]図8は、同実施形態におけるアカウント管理部を説明するための模式図である。
[図9]図9は、同実施形態における動作を説明するためのシーケンス図である。
。
[図10]図10は、同実施形態における動作を説明するためのシーケンス図である。
[図11]図11は、第2の実施形態に係る生体参照情報登録システムの構成例を示す模式図である。
[図12]図12は、同実施形態における生体情報採取装置の構成例を示す模式図である。
[図13]図13は、同実施形態における生体参照情報格納装置の構成例を示す模式図である。
[図14]図14は、同実施形態における第1生体認証コンストラクトの構成例を示す模式図である。
[図15]図15は、同実施形態における第2生体認証コンストラクトの構成例を示す模式図である。
[図16]図16は、同実施形態における生体参照情報証明書の構成例を示す模式図である。

式図である。

[図17]図 1 7 は、同実施形態における動作を説明するためのシーケンス図である。

発明を実施するための形態

[0046] 以下、各実施形態について図面を用いて説明する。なお、以下の各装置は、それぞれハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、図 1 及び図 1 1 に示す如き、予めネットワーク又は非一時的なコンピュータ読取可能な記憶媒体 (non-transitory computer-readable storage medium) M 1 ~ M 5 からコンピュータにインストールされ、当該コンピュータのプロセッサに実行されることにより、当該コンピュータに各装置の機能を実現させるためのプログラムが用いられる。

[0047] <第 1 の実施形態>

図 1 は第 1 の実施形態に係る生体参照情報登録システムの構成例を示す模式図である。この生体参照情報登録システムは、ネットワーク N w を介して互いに通信可能な生体参照情報格納装置 1 0 及び生体参照情報証明書生成装置 2 0 を備えている。生体参照情報格納装置 1 0 と生体参照情報証明書生成装置 2 0 とは、任意の接続形態によって接続される。生体参照情報登録システムは、認証対象者の生体参照情報を生体参照情報格納装置 1 0 に登録する。なお、生体参照情報登録システムは、生体参照情報格納システムと読み替えてもよい。また、「登録」の語は、適宜、「格納」又は「記憶」等と読み替えてもよい。

[0048] 生体参照情報格納装置 1 0 は、図 2 に示すように、入出力部 1 1、制御部 1 2、生体情報採取部 1 3、生体参照情報生成部 1 4、生体認証コンテキスト生成部 1 5、有効化判定部 1 6、有効化情報一時保存部 1 7 及び情報格納部 1 8 を備えている。生体参照情報格納装置 1 0 は、I C (Integrated Circuit: 集積回路) カードや携帯電話などのように、耐タンパ性を有し、計算能力を持つデバイスであることが望ましい。

- [0049] 入出力部 11 は、例えば CUI (Command User Interface) や GUI (Graphical User Interface) のように外部からの命令に応じて、生体参照情報格納装置 10 上の特定処理を実行させ、データを入出力する機能部である。入出力部 11 から入出力（送受信）されるデータとしては、例えば、ユーザ ID、パスワード、登録開始要求、チャレンジ情報、生体参照情報のハッシュ値、生体認証コンテキスト及び生体参照情報証明書などがある。
- [0050] 制御部 12 は、生体参照情報格納装置 10 における処理全般を制御するための機能部であり、生体参照情報格納装置 10 内でのイベントやデータを制御する。制御部 12 は、生体参照情報格納装置 10 の各機能部に対して命令を実行したり、処理に必要なデータを受け渡したりする。なお、当該機能を省略して、他の各機能部間で直接的な呼び出しを行ってもよい。
- [0051] 生体情報採取部 13 は、認証対象者の生体情報を採取するための機能である。
- [0052] 生体参照情報生成部 14 は、生体情報採取部 13 により採取した生体情報に基づいて生体参照情報を生成するための機能部である。
- [0053] 生体認証コンテキスト生成部 15 は、生体参照情報格納装置 10 が実施した生体認証に関する処理を保証するための生体認証コンテキストを生成するための機能部である。本実施形態では、生体参照情報生成部 14 及び情報格納部 18 が保証対象となる。生体認証コンテキストの好適な例としては、ISO/IEC 24761 形式の生体認証コンテキストが挙げられる。本実施形態では、生体認証コンテキストが生体参照情報と関連づけられる。例えば、生体認証コンテキスト C が ISO/IEC 24761 形式である場合、図 3 に示すように、生体参照情報のハッシュ値が、生体認証コンテキスト C に含められる。
- [0054] 生体認証コンテキスト生成部 15 は、例えば、以下の各機能 (f15-1) ~ (f15-4) をもっている。
- [0055] (f15-1) 自装置の第 1 秘密鍵を記憶する第 1 秘密鍵記憶機能。なお、第 1 秘密鍵記憶機能は、例えば、第 1 秘密鍵を記憶する記憶領域と、当該記憶領

域に第 1 秘密鍵を書込む機能とを含んでいる。

- [0056] (f15-2) 生体参照情報のハッシュ値を生成するハッシュ値生成機能。ハッシュ値は、ハッシュアルゴリズムに依存した固定データ長をもっている。
- [0057] (f15-3) 第 1 秘密鍵に基づいて、チャレンジ情報及び生体参照情報のハッシュ値に対する第 1 デジタル署名を生成する第 1 署名生成機能。
- [0058] (f15-4) チャレンジ情報、生体参照情報のハッシュ値、及び第 1 デジタル署名を含む生体認証コンテキスト C を生成する生体認証コンテキスト生成機能。
- [0059] 有効化判定部 16 は、生体参照情報及び生体参照情報証明書 R C を有効化するための機能部である。有効化情報一時保存部 17 に保存された生体参照情報及び生体認証コンテキストと、生体参照情報証明書生成装置 20 から取得した生体参照情報証明書とを検証することにより、生体参照情報及び生体参照情報証明書 R C の有効化を判定し、有効であると判定されたら生体参照情報及び生体参照情報証明書 R C を情報格納部 18 に格納し、有効とする。
- [0060] 有効化判定部 16 は、例えば、以下の各機能(f16-1)～(f16-4)をもっている。
- [0061] (f16-1) 生体参照情報証明書 R C から生体参照情報のハッシュ値及び生体認証コンテキスト C を抽出する第 1 抽出機能。
- [0062] (f16-2) 抽出したハッシュ値を、生成したハッシュ値に基づいて検証するハッシュ値検証機能。
- [0063] (f16-3) 抽出した生体認証コンテキストを、生成した生体認証コンテキストに基づいて検証する生体認証コンテキスト検証機能。
- [0064] (f16-4) ハッシュ値検証機能(f16-2)及び生体認証コンテキスト検証機能(f16-3)による検証結果がそれぞれ正当性を示す場合、生体参照情報及び生体参照情報証明書を情報格納部 18 に書込む書込機能。
- [0065] 有効化情報一時保存部 17 は、生体参照情報生成部 14 が生成した生体参照情報と、生体認証コンテキスト生成部 15 が生成した生体認証コンテキストとを、一時的に保存するための機能部である。保存された情報は、有効化

判定部 16 によって、生体参照情報及び生体参照情報証明書 R C の有効化判定に利用される。この有効化情報一時保存部 17 で実現する機能は、情報格納部 18 の機能として備えてもよい。

[0066] 有効化情報一時保存部 17 は、例えば、図 4 及び図 5 に示すように、管理番号、生体参照情報、生体参照情報のハッシュ値、生体認証コンテキスト及び生体参照情報証明書を互いに関連付けて保存可能となっている。なお、管理番号は適宜、省略してもよい。有効化情報一時保存部 17 は、例えば、生体参照情報、生体参照情報のハッシュ値、生体認証コンテキスト及び生体参照情報証明書 R C を互いに関連付けて記述するデータテーブルを記憶する記憶領域として実施可能となっている。図 4 に示す例では、管理番号 1, 2 の行に示すように、有効な生体参照情報証明書が関連付けて保存されている。また、管理番号 3 の行に示すように、有効でない生体参照情報証明書は保存されていない。なお、管理番号は、適宜、省略してもよい。ここで、生体参照情報、生体参照情報のハッシュ値、生体認証コンテキスト及び生体参照情報証明書は、2 桁 16 進数文字列のバイナリデータとして表記した例を示している。なお、図 4 及び図 5 中、生体認証コンテキスト及び生体参照情報証明書は、同じデータに見えるが、図示を省略した後方のデータが異なっている（データフォーマットが決まっているので、先頭の方のデータが同一になる。）。

[0067] 情報格納部 18 は、生体参照情報及び生体参照情報証明書 R C を格納するための機能部である。生体参照情報証明書 R C は、生体参照情報証明書生成装置 20 により生成される、生体参照情報を保証するための情報である。生体参照情報証明書 R C の好適な例としては、I S O / I E C 24761 で規定される B R T 証明書などが挙げられる。本実施形態では、具体的な生体参照情報証明書として、B R T 証明書を用いた例を説明する。

[0068] 生体参照情報証明書生成装置 20 は、図 6 に示すように、入出力部 21、制御部 22、生体認証コンテキスト検証部 23、証明書生成部 24 及びアカウント管理部 25 を備えている。

- [0069] 入出力部 21 は、生体参照情報格納装置 10 の入出力部 11 と同様な機能部であり、生体参照情報証明書生成装置 20 上の特定処理を実行させ、データを入出力する機能部である。入出力部 21 から入出力（送受信）されるデータとしては、例えば、ユーザ ID、パスワード、登録開始要求、チャレンジ情報、生体参照情報のハッシュ値、生体認証コンテキスト及び生体参照情報証明書などがある。
- [0070] 制御部 22 は、生体参照情報格納装置 10 の制御部 12 と同様な機能部であり、生体参照情報証明書生成装置 20 における処理全般を制御するための機能部であり、生体参照情報証明書生成装置 20 置内でのイベントやデータを制御する。
- [0071] 生体認証コンテキスト検証部 23 は、生体参照情報格納装置 10 と相互作用することにより得られた生体認証コンテキスト C を検証するための機能部である。生体認証コンテキスト C が ISO/IEC 24761 形式である場合、公開鍵暗号方式または MAC（Message Authentication Code）によるチャレンジアドレスポンス認証のためのチャレンジ情報（ランダムな値）を生体参照情報格納装置 10 に送信し、生体参照情報格納装置 10 より得られた生体認証コンテキスト C のデジタル署名値または MAC 値の正当性を検証し、生体認証コンテキスト C に記載された生体処理内容を検証する。
- [0072] 生体認証コンテキスト検証部 23 は、例えば、以下の各機能 (f23-1)～(f23-4) をもっている。
- [0073] (f23-1) チャレンジ情報を生成して当該チャレンジ情報を生体参照情報格納装置 10 に送信するチャレンジ情報送信機能。
- [0074] (f23-2) 受信した生体認証コンテキスト C からチャレンジ情報を抽出する第 2 抽出機能。
- [0075] (f23-3) 抽出したチャレンジ情報を、送信したチャレンジ情報に基づいて検証するチャレンジ情報検証機能。チャレンジ情報検証機能は、例えば、2 つのチャレンジ情報を比較し、両者が一致した場合に正当性を示す検証結果を得る。

- [0076] (f23-4) 受信した生体認証コンテキスト内の第1デジタル署名を第1秘密鍵に対応する第1公開鍵に基づいて検証する署名検証機能。
- [0077] 証明書生成部24は、図7に示すように、生体参照情報格納装置10より送信される生体参照情報のハッシュ値と生体認証コンテキストCとを含む生体参照情報証明書RCを生成するための機能部である。
- [0078] 証明書生成部24は、例えば、以下の各機能(f24-1)～(f24-3)をもっている。
- [0079] (f24-1) 自装置の第2秘密鍵を記憶した第2秘密鍵記憶機能。なお、第2秘密鍵記憶機能は、例えば、第2秘密鍵を記憶する記憶領域と、当該記憶領域に第2秘密鍵を書込む機能とを含んでいる。
- [0080] (f24-2) チャレンジ情報検証機能(f23-3)及び署名検証機能(f23-4)による検証結果がそれぞれ正当性を示す場合、第2秘密鍵に基づいて、受信した生体参照情報のハッシュ値及び生体認証コンテキストCに対する第2デジタル署名を生成する第2署名生成機能。
- [0081] (f24-3) 生体参照情報のハッシュ値、生体認証コンテキスト及び第2デジタル署名を含む生体参照情報証明書RCを生成する証明書生成機能。
- [0082] アカウント管理部25は、認証対象者のアカウントを特定し、生成した生体参照情報証明書RCを認証対象者のアカウントの属性値として格納するための機能部である。アカウント管理部25は、例えば、図8に示すように、管理番号、ユーザID、生体参照情報証明書及び有効フラグを互いに関連付けて保存可能となっている。但し、管理番号及び有効フラグは、適宜、省略してもよい。
- [0083] すなわち、アカウント管理部25は、例えば、以下の機能(f25-1)～(f25-2)をもっている。
- [0084] (f25-1) 認証対象者のユーザID及び生体参照情報証明書RCを互いに関連付けて記憶するためのアカウント記憶機能。アカウント記憶機能は、例えば、ユーザID及び生体参照情報証明書RCを互いに関連付けて記述するアカウントデータテーブルを記憶する記憶領域として実施可能となっている。

また、アカウント記憶機能は、予めユーザIDをアカウントデータテーブルに書込む機能を含んでいてもよい。但し、予めユーザIDをアカウントデータテーブルに書込む機能は、例えば制御部22が有していてもよい。

[0085] (f25-2) 生成された生体参照情報証明書を、認証対象者のユーザIDに関連付けて前記アカウント記憶機能に書き込む証明書書込機能。

[0086] このアカウント管理部25は、生体参照情報証明書生成装置20に閉じてもよく、任意のID管理 (Identity Management) システムと連携してもよい。また、認証対象者のアカウントを特定する手段に関しては、各実施形態の範囲外であり、従来からあるユーザID/パスワードによる認証など任意の手段を取ればよい。

[0087] 次に、以上のように構成された生体参照情報登録装置の動作について図9及び図10のシーケンス図を用いて説明する。

[0088] 生体参照情報格納装置10は、図9に示すように、例えば認証対象者による入出力部の操作により、登録開始要求を生体参照情報証明書生成装置20に送信する(ST1)。なお、生体参照情報格納装置10に代えて、生体参照情報証明書生成装置20が登録処理開始要求を生体参照情報格納装置10に送信する構成としてもよい。また、認証対象者の特定は、ステップST1の前又はステップST1の登録開始要求により実行されることを前提とする。ここでいう認証対象者の特定は、例えば、認証対象者のユーザIDを予めアカウント管理部25に書き込む処理と、認証対象者の生体参照情報格納装置10の第1公開鍵を生体認証コンテキスト検証部23が取得する処理とを含んでいる。但し、第1公開鍵を取得する処理は、この時点に限らず、ステップST11における第1デジタル署名の検証処理までに実行すればよい。

[0089] 始めに、生体参照情報証明書生成装置20は、ステップST1の登録開始要求を受けると、生体認証コンテキスト検証部23が、生体認証コンテキストCの生成に必要なチャレンジ情報 (ランダム値) を生成し (ST2)、当該チャレンジ情報を生体参照情報格納装置10に通知する (ST3)。また、チャレンジ情報に限らず、生体認証コンテキストCの生成に必要な情報は

、ステップS T 1～S T 3において交換すればよい。

[0090] 生体参照情報格納装置 10 は、チャレンジ情報を受けると、生体情報採取部 13 により、認証対象者の生体情報を採取する（S T 4）。

[0091] 生体参照情報生成部 14 は、ステップS T 4 で採取した生体情報から生体参照情報を生成し（S T 5）、この生体参照情報を有効化情報一時保存部 17 に一時的に保存する（S T 6）。

[0092] 生体認証コンテキスト生成部 15 は、ステップS T 5 で生成した生体参照情報のハッシュ値を生成し（S T 7）、当該ハッシュ値を有効化情報一時保存部 17 に一時的に保存する。但し、当該ハッシュ値は、有効化情報一時保存部 17 内の生体参照情報から生成できるため、保存しなくてもよい。

[0093] 生体認証コンテキスト生成部 15 は、ステップS T 3 により通知されたチャレンジ情報と、ステップS T 7 により生成した生体参照情報のハッシュ値とに対して、自装置 10 の第 1 秘密鍵に基づいて第 1 デジタル署名を生成する。しかる後、生体認証コンテキスト生成部 15 は、チャレンジ情報と、生体参照情報のハッシュ値と、第 1 デジタル署名とを含む生体認証コンテキストCを生成し（S T 8）、この生体認証コンテキストCを有効化情報一時保存部 17 に一時的に保存する（S T 9）。

[0094] しかる後、生体参照情報格納装置 10 は、ステップS T 7～S T 8 により生成された生体参照情報のハッシュ値及び生体認証コンテキストCを生体参照情報証明書生成装置 20 に送信する（S T 10）。

[0095] 生体参照情報証明書生成装置 20 は、生体参照情報のハッシュ値及び生体認証コンテキストCを受信すると、生体認証コンテキスト検証部 23 が、生体参照情報格納装置 10 の秘密鍵に対応する公開鍵と、ステップS T 2 で通知したチャレンジ情報とに基づいて、当該生体認証コンテキストCの正当性を検証する（S T 11）。具体的には、生体認証コンテキスト検証部 23 は、生体認証コンテキストCから抽出したチャレンジ情報を、ステップS T 2 で送信したチャレンジ情報に基づいて検証する。また、生体認証コンテキスト検証部 23 は、受信した生体認証コンテキスト内の第 1 デジタル署名を、

生体参照情報格納装置 10 の第 1 秘密鍵に対応する第 1 公開鍵に基づいて検証する。

[0096] ストップ ST 11 の検証結果が正当性を示す場合、証明書生成部 24 は、

自装置の第 2 秘密鍵に基づいて、受信した生体参照情報のハッシュ値及び生体認証コンテキストに対する第 2 デジタル署名を生成する。また、証明書生成部 24 は、生体参照情報のハッシュ値、生体認証コンテキスト及び第 2 デジタル署名を含む生体参照情報証明書 RC を生成する (ST 12)。なお、ストップ ST 11 の検証の結果、正当でない場合には、処理全体を終了する。このとき、生体参照情報証明書生成装置 20 は、検証失敗により処理を終了した旨を生体参照情報格納装置 10 に通知してもよい。

[0097] ストップ ST 12 の後、アカウント管理部 25 は、生成した生体参照情報証明書 RC を、認証対象者のアカウントの属性の値として格納する (ST 13)。どのような属性を利用するかは、認証対象者のアカウント構造に依存するため、本実施形態では具体的な属性については特に要求しないが、生体参照情報証明書 RC を表現可能な属性であることが望ましい。また、本ストップ ST 13 を省略し、ストップ ST 21 の成功応答の確認の後に、生体参照情報証明書 RC を認証対象者のアカウントの属性の値として格納するように変形してもよい。この変形例の場合、アカウント管理部 25 又は証明書生成部 24 は、生体参照情報証明書 RC を一時的な任意の保存領域に格納しておけばよい。

[0098] いずれにしても、生体参照情報証明書生成装置 20 の出力部 21 は、ストップ ST 12 で生成した生体参照情報証明書 RC を生体参照情報格納装置 10 に送信する (ST 14)。

[0099] 生体参照情報格納装置 10 は、図 10 に示すように、この生体参照情報証明書 RC を受信すると (ST 15)、有効化判定部 16 が、この生体参照情報証明書 RC から生体参照情報のハッシュ値と生体認証コンテキストとを抽出する (ST 16)。

[0100] 有効化判定部 16 は、抽出した生体参照情報のハッシュ値と、有効化情報

一時保存部 17 内の生体参照情報のハッシュ値とを比較検証する (ST 17)。スナップ ST 17 の比較検証の結果、両者が不一致の場合には、処理全体を終了する。このとき、生体参照情報格納装置 10 は、検証失敗により処理を終了した旨を生体参照情報証明書生成装置 20 に通知してもよい。また、有効化情報一時保存部 17 に生体参照情報のみを一時保存する場合には、本スナップで有効化判定部 16 が生体参照情報のハッシュ値を生成すればよい。

[0101] スナップ ST 17 の比較検証の結果、両者が一致した場合、有効化判定部 16 は、スナップ ST 16 で抽出した生体認証コンテキストと、有効化情報一時保存部 17 内の生体認証コンテキストとを比較検証する (ST 18)。スナップ ST 18 の比較検証の結果、両者が不一致の場合には、処理全体を終了する。このとき、生体参照情報格納装置 10 は、検証失敗により処理を終了した旨を生体参照情報証明書生成装置 20 に通知してもよい。また、スナップ ST 17、ST 18 は、逆の順序で実行してもよい。

[0102] スナップ ST 18 の比較検証の結果、両者が一致した場合、有効化判定部 16 は、有効化情報一時保存部 17 内の生体参照情報と、スナップ ST 15 で受信した生体参照情報証明書 R C とを情報格納部 18 に格納する (ST 19)。また、有効化判定部 16 は、生体参照情報証明書 R C を有効化情報一時保存部 17 に保存することにより、生体参照情報証明書 R C を有効化する (ST 20)。

[0103] しかる後、生体参照情報格納装置 10 は、全ての処理の成功を示す成功応答を生体参照情報証明書生成装置 20 に通知する (ST 21)。なお、成功応答は、例えば、アカウント管理部 25 内の有効フラグに関連付けられた情報 (例、ユーザ ID、生体参照情報証明書 R C) の少なくとも 1 つを含んでいてもよい。

[0104] 生体参照情報証明書生成装置 20 は、成功応答を受けると、アカウント管理部 25 が、例えば、成功応答内の情報に関連付けられた有効フラグを true に更新する。

[0105] 上述したように本実施形態によれば、生体参照情報証明書生成装置 20 はチャレンジ情報を生体参照情報格納装置 10 に送信する。生体参照情報格納装置 10 は、当該チャレンジ情報、生体参照情報のハッシュ値及び第 1 デジタル署名を含む生体認証コンテキスト C と生体参照情報のハッシュ値とを生体参照情報証明書生成装置 20 に送信する。生体参照情報証明書生成装置 20 は、チャレンジ情報を検証し、且つ第 1 デジタル署名を第 1 公開鍵で検証した後、当該生体認証コンテキスト、当該生体参照情報のハッシュ値及び第 2 デジタル署名を含む生体参照情報証明書 RC を生体参照情報格納装置 10 に送信する。生体参照情報格納装置 10 は、生体参照情報のハッシュ値及び生体認証コンテキスト C を検証した後、生体参照情報及び生体参照情報証明書 RC を格納する。

[0106] このように、共有の秘密情報を用いず、チャレンジアンドレスポンス認証、公開鍵による認証、ハッシュ値による認証などを用いた構成により、デバイス（生体参照情報格納装置 10）と生体認証システムとの間で予め秘密情報を共有せずに、ネットワーク Nw を介して生体参照情報を保証及び格納することができる。

[0107] 例えば、認証対象者が選択したデバイスを用いて、認証対象者が選択した生体認証システムに対して、オンラインを介して生体参照情報を保証し、デバイスに生体参照情報を格納することができる。これにより、生体認証システムにおける生体参照情報を登録または更新するときの、利用者の利便性向上が期待できる。

[0108] また、デバイスと生体認証システムとの間で予め秘密情報を共有する必要がないので、利用者は、生体認証システム毎に対応するデバイスを保有する必要が無く、デバイス保有の負担を削減することができる。

[0109] <第 2 の実施形態>

図 11 は第 2 の実施形態に係る生体参照情報登録システムの構成例を示す模式図であり、図 12 及び図 13 は同システムにおける各装置の構成例を示す模式図であって、前述した図面と略同一部分には同一符号を付してその詳

しい説明を省略し、ここでは異なる部分について主に述べる。

[0110] 第1の実施形態では、単一の生体参照情報格納装置10が生体参照情報を生成する構成を説明したが、これに限らず、生体情報採取部13又は生体参照情報生成部14の何れかを含む装置として分離する構成としてもよく、生体情報採取部13及び生体参照情報生成部14の両方を含む装置として分離する構成としてもよい。図11乃至図13は、生体情報採取部13を含む生体情報採取装置10aと、生体参照情報生成部14を含む生体参照情報格納装置10とを分離した構成例を示している。

[0111] この場合、分離したそれぞれの装置10a、10にも生体認証コンテキスト生成部15a、15を配備し、第1の実施形態に述べた動作と同様に各生体認証コンテキストC1、C2を生成する。生成された各生体認証コンテキストC1、C2は、生体参照情報格納装置10の有効化情報一時保存部17でまとめて管理すればよい。

[0112] なお、第1生体認証コンテキストC1は、生体情報採取装置10aにより生成され、図14に示すように、チャレンジ情報、生体情報のハッシュ値及び第0デジタル署名を含んでいる。第0デジタル署名は、生体情報採取装置10aの第0秘密鍵に基づいて、チャレンジ情報及び生体情報のハッシュ値に対する署名処理により生成される。

[0113] 第2生体認証コンテキストC2は、生体参照情報格納装置10により生成され、図15に示すように、チャレンジ情報、生体情報のハッシュ値、生体参照情報のハッシュ値及び第1デジタル署名を含んでいる。生体情報のハッシュ値は、生体参照情報格納装置10の入力として与えられる生体情報のハッシュ値である。第1デジタル署名は、生体参照情報格納装置10の第1秘密鍵に基づいて、チャレンジ情報及び生体参照情報のハッシュ値に対する署名処理により生成される。

[0114] 生体参照情報証明書RCは、生体参照情報証明書生成装置20により生成され、図16に示すように、第1生体認証コンテキストC1、第2生体認証コンテキストC2、生体参照情報のハッシュ値、及び第2デジタル署名を含

んでいる。第2デジタル署名は、生体参照情報証明書生成装置20の第2秘密鍵に基づいて、第1生体認証コンテキストC1、第2生体認証コンテキストC2、及び生体参照情報のハッシュ値に対する署名処理により生成される。

[0115] また、図4及び図5に示した有効化情報一時保存部17における生体認証コンテキストの記憶領域にも、2つの生体認証コンテキストC1、C2が記憶される。

[0116] 次に、以上のように構成された生体参照情報登録システムの動作を図17のシーケンス図を用いて説明する。

[0117] いま、前述同様に、ステップST1～ST3が実行されたとする。

[0118] 生体参照情報格納装置10は、生体参照情報証明書生成装置20からチャレンジ情報を受けると、チャレンジ情報及び生体情報採取要求を生体情報採取装置10aに送信する(ST4-1)。

[0119] 生体情報採取装置10aは、入出力部11aがチャレンジ情報及び生体情報採取要求を受信すると、制御部12aがチャレンジ情報を生体認証コンテキスト生成部15aに送出すると共に、生体情報採取部13を起動する。生体情報採取部13は、認証対象者の生体情報を採取する(ST4-2)。生体情報は、制御部12aを介して生体認証コンテキスト生成部15aに送出される。但し、制御部12aを省略し、各部11a、13、15aが直接的に情報を転送してもよい。

[0120] 生体情報採取装置10aの生体認証コンテキスト生成部15aは、ステップST4-2で生成した生体参照情報のハッシュ値を生成する。

[0121] 生体認証コンテキスト生成部15aは、ステップST4-1により受信したチャレンジ情報と、当該生成した生体参照情報のハッシュ値とに対して、自装置10aの第0秘密鍵に基づいて第0デジタル署名を生成する。また、生体認証コンテキスト生成部15aは、チャレンジ情報と、生体参照情報のハッシュ値と、第0デジタル署名とを含む第1生体認証コンテキストC1を生成する(ST4-1)。

- [0122] しかる後、生体認証コンテキスト生成部 15 a は、この第 1 生体認証コンテキスト C 1 と、ステップ S T 4 - 2 で採取した生体情報とを生体参照情報格納装置 10 に送信する (S T 4 - 4)。
- [0123] 生体参照情報生成部 14 は、ステップ S T 4 - 4 で採取した生体情報から生体参照情報を生成し (S T 5)、この生体参照情報を有効化情報一時保存部 17 に一時的に保存する (S T 6)。また、生体参照情報生成部 14 は、ステップ S T 4 - 4 で採取した第 1 生体認証コンテキスト C 1 を有効化情報一時保存部 17 に一時的に保存する。
- [0124] 以下、前述したステップ S T 7 以降と同様の処理が各装置 10, 20 により実行される。但し、2 つの生体認証コンテキスト C 1, C 2 を用いる点が若干、異なっている。
- [0125] 例えば、ステップ S T 8 ~ S T 9 では、生体認証コンテキスト生成部 15 は、チャレンジ情報と、生体参照情報のハッシュ値と、第 1 デジタル署名とを含む第 2 生体認証コンテキスト C 2 を生成し、この第 2 生体認証コンテキスト C を有効化情報一時保存部 17 に一時的に保存する。
- [0126] ステップ S T 8 ~ S T 9 では、生体参照情報格納装置 10 は、生体参照情報のハッシュ値、第 1 及び第 2 生体認証コンテキスト C 1, C 2 を生体参照情報証明書生成装置 20 に送信する。
- [0127] ステップ S T 11 では、生体認証コンテキスト検証部 23 が、生体情報採取装置 10 a の第 0 秘密鍵に対応する第 0 公開鍵と、生体参照情報格納装置 10 の第 1 秘密鍵に対応する第 1 公開鍵と、ステップ S T 2 で通知したチャレンジ情報とに基づいて、各生体認証コンテキスト C 1, C 2 の正当性を検証する。
- [0128] 具体的には、生体認証コンテキスト検証部 23 は、各生体認証コンテキスト C 1, C 2 から抽出したチャレンジ情報を、ステップ S T 2 で送信したチャレンジ情報に基づいて検証する。また、生体認証コンテキスト検証部 23 は、受信した第 1 生体認証コンテキスト C 1 内の第 0 デジタル署名を、生体情報採取装置 10 a の第 0 秘密鍵に対応する第 0 公開鍵に基づいて検証する。

。同様に、生体認証コンテナスタ検証部23は、受信した第2生体認証コンテナスタC2内の第1デジタル署名を、生体参照情報格納装置10の第1秘密鍵に対応する第1公開鍵に基づいて検証する。

[0129] ステップST12では、ステップST11の検証結果が正当性を示す場合、証明書生成部24は、自装置の第2秘密鍵に基づいて、受信した生体参照情報のハッシュ値及び各生体認証コンテナスタC1、C2に対する第2デジタル署名を生成する。また、証明書生成部24は、生体参照情報のハッシュ値、各生体認証コンテナスタC1、C2及び第2デジタル署名を含む生体参照情報証明書RCを生成する。

[0130] ステップST16では、有効化判定部16が、この生体参照情報証明書RCから生体参照情報のハッシュ値と各生体認証コンテナスタC1、C2とを抽出する。

[0131] ステップST18では、有効化判定部16は、ステップST16で抽出した第1生体認証コンテナスタC1と、有効化情報一時保存部17内の第1生体認証コンテナスタC1とを比較検証する。同様に、有効化判定部16は、ステップST16で抽出した第2生体認証コンテナスタC2と、有効化情報一時保存部17内の第2生体認証コンテナスタC2とを比較検証する。

[0132] 以下、ステップST19以降の処理が前述同様に実行される。

[0133] 上述したように本実施形態によれば、第1の実施形態の生体参照情報格納装置10から生体情報採取部13を分離した構成としても、第1の実施形態と同様の効果を得ることができる。

[0134] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることができるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0135] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても

良い。

[0136] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0137] さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0138] また、記憶媒体は1つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0139] なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0140] また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0141] なお、本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

[請求項1]

ネットワークを介して互いに通信可能な生体参照情報格納装置（10）と生体参照情報証明書生成装置（20）とを備え、認証対象者の生体参照情報を前記生体参照情報格納装置に登録する生体参照情報登録システムであって、

前記生体参照情報格納装置は、

自装置の第1秘密鍵を記憶する第1秘密鍵記憶手段（15）と、

前記生体参照情報証明書生成装置からチャレンジ情報を受信するチャレンジ情報受信手段（11）と、

前記認証対象者から採取した生体情報に基づいて生体参照情報を生成する生体参照情報生成手段（14）と、

前記生体参照情報のハッシュ値を生成するハッシュ値生成手段（15）と、

前記第1秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第1デジタル署名を生成する第1署名生成手段（15）と、

前記チャレンジ情報、前記生体参照情報のハッシュ値、及び前記第1デジタル署名を含む生体認証コンテキスト（C）を生成する生体認証コンテキスト生成手段（15）と、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信する生体認証コンテキスト送信手段（11）と、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストと、当該生体参照情報のハッシュ値及び前記生体認証コンテキストに対する第2デジタル署名とを含む生体参照情報証明書を前記生体参照情報証明書生成装置から受信する証明書受信手段（11）と、

前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出する第1抽出手段（16）と、

前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証するハッシュ値検証手段（１６）と、

前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証する生体認証コンテキスト検証手段（１６）と、

前記生体参照情報及び前記生体参照情報証明書を格納するための格納手段（１８）と、

前記ハッシュ値検証手段及び前記生体認証コンテキスト検証手段による検証結果がそれぞれ正当性を示す場合、前記生体参照情報及び前記生体参照情報証明書を前記格納手段に書込む書込手段（１６）と、

を備え、

前記生体参照情報証明書生成装置は、

前記認証対象者のユーザＩＤ及び前記生体参照情報証明書を互いに関連付けて記憶するためのアカウント記憶手段（２５）と、

自装置の第２秘密鍵を記憶した第２秘密鍵記憶手段（２４）と、

前記チャレンジ情報を生成して当該チャレンジ情報を前記生体参照情報格納装置に送信するチャレンジ情報送信手段（２３）と、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信する生体認証コンテキスト受信手段（２１）と、

前記受信した生体認証コンテキストからチャレンジ情報を抽出する第２抽出手段（２３）と、

前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証するチャレンジ情報検証手段（２３）と、

前記受信した生体認証コンテキスト内の第１デジタル署名を前記第１秘密鍵に対応する第１公開鍵に基づいて検証する署名検証手段（２３）と、

前記チャレンジ情報検証手段及び前記署名検証手段による検証結果

がそれぞれ正当性を示す場合、前記第2秘密鍵に基づいて、前記受信した前記生体参照情報のハッシュ値及び前記生体認証コンテキストに対する前記第2デジタル署名を生成する第2署名生成手段（24）と、

前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第2デジタル署名を含む前記生体参照情報証明書を生成する証明書生成手段（24）と、

前記生成された生体参照情報証明書を、前記認証対象者のユーザIDに関連付けて前記アカウント記憶手段に書き込む証明書書込手段（25）と、

前記生成された生体参照情報証明書を前記生体参照情報格納装置に送信する証明書送信手段（21）と、

を備えたことを特徴とする生体参照情報登録システム。

[請求項2]

ネットワークを介して生体参照情報証明書生成装置（20）に通信可能な生体参照情報格納装置（10）であって、

自装置の第1秘密鍵を記憶する第1秘密鍵記憶手段（15）と、

前記生体参照情報証明書生成装置からチャレンジ情報を受信するチャレンジ情報受信手段（11）と、

認証対象者から採取した生体情報に基づいて生体参照情報を生成する生体参照情報生成手段（14）と、

前記生体参照情報のハッシュ値を生成するハッシュ値生成手段（15）と、

前記第1秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第1デジタル署名を生成する第1署名生成手段（15）と、

前記チャレンジ情報、前記生体参照情報のハッシュ値、及び前記第1デジタル署名を含む生体認証コンテキスト（C）を生成する生体認証コンテキスト生成手段（15）と、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信する生体認証コンテキスト送信手段（１１）と、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストと、当該生体参照情報のハッシュ値及び前記生体認証コンテキストに対する第２デジタル署名とを含む生体参照情報証明書を前記生体参照情報証明書生成装置から受信する証明書受信手段（１１）と、

前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出する第１抽出手段（１６）と、

前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証するハッシュ値検証手段（１６）と、

前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証する生体認証コンテキスト検証手段（１６）と、

前記生体参照情報及び前記生体参照情報証明書を格納するための格納手段（１８）と、

前記ハッシュ値検証手段及び前記生体認証コンテキスト検証手段による検証結果がそれぞれ正当性を示す場合、前記生体参照情報及び前記生体参照情報証明書を前記格納手段に書込む書込手段（１６）と、
を備え、

前記生体参照情報証明書生成装置は、前記チャレンジ情報を前記生体参照情報格納装置に送信し、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信し、前記生体認証コンテキストからチャレンジ情報を抽出し、前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証し、前記生体認証コンテキスト内の第１デジタル署名を前記第１秘密鍵に対応する第１公開鍵に基づいて検証し、検証結果がそれぞれ正当性を示す場合、自装置の第２秘密鍵に基づいて前記第２デジタル署名を生

成し、前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第2デジタル署名を含む前記生体参照情報証明書を生成し、前記生体参照情報証明書を前記生体参照情報格納装置に送信する

ことを特徴とする生体参照情報格納装置。

[請求項3]

ネットワークを介して生体参照情報格納装置（10）に通信可能な生体参照情報証明書生成装置（20）であって、

認証対象者のユーザID及び生体参照情報証明書を互いに関連付けて記憶するためのアカウント記憶手段（25）と、

自装置の第2秘密鍵を記憶した第2秘密鍵記憶手段（24）と、

チャレンジ情報を生成して当該チャレンジ情報を前記生体参照情報格納装置に送信するチャレンジ情報送信手段（23）と、

前記生体参照情報格納装置が、前記認証対象者から採取した生体情報に基づいて生体参照情報を生成し、前記生体参照情報のハッシュ値を生成し、自装置の第1秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第1デジタル署名を生成し、前記チャレンジ情報、前記生体参照情報のハッシュ値及び前記第1デジタル署名を含む生体認証コンテキストを生成し、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信した場合、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信する生体認証コンテキスト受信手段（21）と、

前記受信した生体認証コンテキストからチャレンジ情報を抽出する第2抽出手段（23）と、

前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証するチャレンジ情報検証手段（23）と、

前記受信した生体認証コンテキスト内の第1デジタル署名を前記第1秘密鍵に対応する第1公開鍵に基づいて検証する署名検証手段（23）と、

前記チャレンジ情報検証手段及び前記署名検証手段による検証結果がそれぞれ正当性を示す場合、前記第2秘密鍵に基づいて、前記受信した前記生体参照情報のハッシュ値及び前記生体認証コンテキストに対する前記第2デジタル署名を生成する第2署名生成手段（24）と、

前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第2デジタル署名を含む前記生体参照情報証明書を生成する証明書生成手段（24）と、

前記生成された生体参照情報証明書を、前記認証対象者のユーザIDに関連付けて前記アカウント記憶手段に書き込む証明書書込手段（25）と、

前記生成された生体参照情報証明書を前記生体参照情報格納装置に送信する証明書送信手段（21）と、

を備え、

前記生体参照情報格納装置は、前記生体参照情報証明書を前記生体参照情報証明書生成装置から受信し、前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出し、前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証し、前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証し、検証結果がそれぞれ正当性を示す場合、前記生体参照情報及び前記生体参照情報証明書を格納手段に書込む

ことを特徴とする生体参照情報証明書生成装置。

[請求項4]

ネットワークを介して生体参照情報証明書生成装置（20）に通信可能であり、第1秘密鍵記憶手段及び格納手段を備えた生体参照情報格納装置（10）に用いられるプログラムであって、

前記生体参照情報格納装置（10）を、

自装置の第1秘密鍵を前記第1秘密鍵記憶手段（15）に書込む手

段、

前記生体参照情報証明書生成装置からチャレンジ情報を受信する手段（１１）、

認証対象者から採取した生体情報に基づいて生体参照情報を生成する手段（１４）、

前記生体参照情報のハッシュ値を生成する手段（１５）、

前記第１秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第１デジタル署名を生成する手段（１５）

、

前記チャレンジ情報、前記生体参照情報のハッシュ値、及び前記第１デジタル署名を含む生体認証コンテキスト（Ｃ）を生成する手段（１５）、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信する手段（１１）、

前記生体参照情報のハッシュ値及び前記生体認証コンテキストと、当該生体参照情報のハッシュ値及び前記生体認証コンテキストに対する第２デジタル署名とを含む生体参照情報証明書を前記生体参照情報証明書生成装置から受信する手段（１１）、

前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出する手段（１６）、

前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証する手段（１６）、

前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証する手段（１６）、

前記検証した結果がそれぞれ正当性を示す場合、前記生体参照情報及び前記生体参照情報証明書を前記格納手段（１８）に書込む手段（１６）、

として機能させ、

前記生体参照情報証明書生成装置は、前記チャレンジ情報を前記生体参照情報格納装置に送信し、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信し、前記生体認証コンテキストからチャレンジ情報を抽出し、前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証し、前記生体認証コンテキスト内の第1デジタル署名を前記第1秘密鍵に対応する第1公開鍵に基づいて検証し、当該検証結果がそれぞれ正当性を示す場合、自装置の第2秘密鍵に基づいて前記第2デジタル署名を生成し、前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第2デジタル署名を含む前記生体参照情報証明書を生成し、前記生体参照情報証明書を前記生体参照情報格納装置に送信することを特徴とするプログラム。

[請求項5]

ネットワークを介して生体参照情報格納装置（10）に通信可能であり、アカウント記憶手段及び第2秘密鍵記憶手段を備えた生体参照情報証明書生成装置（20）に用いられるプログラムであって、

前記生体参照情報証明書生成装置を、

認証対象者のユーザIDを前記アカウント記憶手段（25）に書込む手段、

自装置の第2秘密鍵を前記第2秘密鍵記憶手段（24）に書込む手段、

チャレンジ情報を生成して当該チャレンジ情報を前記生体参照情報格納装置に送信する手段（23）、

前記生体参照情報格納装置が、前記認証対象者から採取した生体情報に基づいて生体参照情報を生成し、前記生体参照情報のハッシュ値を生成し、自装置の第1秘密鍵に基づいて、前記チャレンジ情報及び前記生体参照情報のハッシュ値に対する第1デジタル署名を生成し、前記チャレンジ情報、前記生体参照情報のハッシュ値及び前記第1デジタル署名を含む生体認証コンテキストを生成し、前記生体参照情報

のハッシュ値及び前記生体認証コンテキストを前記生体参照情報証明書生成装置に送信した場合、前記生体参照情報のハッシュ値及び前記生体認証コンテキストを前記生体参照情報格納装置から受信する手段（２１）、

前記受信した生体認証コンテキストからチャレンジ情報を抽出する手段（２３）、

前記抽出したチャレンジ情報を、前記送信したチャレンジ情報に基づいて検証する手段（２３）、

前記受信した生体認証コンテキスト内の第１デジタル署名を前記第１秘密鍵に対応する第１公開鍵に基づいて検証する手段（２３）、

前記チャレンジ情報検証手段及び前記署名検証手段による検証結果がそれぞれ正当性を示す場合、前記第２秘密鍵に基づいて、前記受信した前記生体参照情報のハッシュ値及び前記生体認証コンテキストに対する前記第２デジタル署名を生成する手段（２４）、

前記生体参照情報のハッシュ値、前記生体認証コンテキスト及び前記第２デジタル署名を含む前記生体参照情報証明書を生成する手段（２４）、

前記生成された生体参照情報証明書を、前記認証対象者のユーザＩＤに関連付けて前記アカウント記憶手段に書き込む手段（２５）、

前記生成された生体参照情報証明書を前記生体参照情報格納装置に送信する手段（２１）、

として機能させ、

前記生体参照情報格納装置は、前記生体参照情報証明書を前記生体参照情報証明書生成装置から受信し、前記生体参照情報証明書から前記生体参照情報のハッシュ値及び前記生体認証コンテキストを抽出し、前記抽出したハッシュ値を、前記生成したハッシュ値に基づいて検証し、前記抽出した生体認証コンテキストを、前記生成した生体認証コンテキストに基づいて検証し、検証結果がそれぞれ正当性を示す場

合、前記生体参照情報及び前記生体参照情報証明書を格納手段に書込む

ことを特徴とするプログラム。