(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7563496号
(P7563496)

(45)発行日　令和6年10月8日(2024.10.8)

(24)登録日　令和6年9月30日(2024.9.30)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)		Ｈ０４Ｌ	9/32　１００Ｄ
Ｇ０６Ｆ　21/32　(2013.01)		Ｇ０６Ｆ	21/32

請求項の数　17　（全17頁）

(21)出願番号　特願2022-577957(P2022-577957)
(86)(22)出願日　令和3年1月29日(2021.1.29)
(86)国際出願番号　PCT/JP2021/003294
(87)国際公開番号　WO2022/162884
(87)国際公開日　令和4年8月4日(2022.8.4)
審査請求日　令和5年7月4日(2023.7.4)

(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　100103894
弁理士　家入 健
(72)発明者　奈良 成泰
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　岡村 利彦
東京都港区芝五丁目７番１号 日本電気株式会社内
(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
(72)発明者　森 健吾

最終頁に続く

(54)【発明の名称】　生体認証システム、そのテンプレート更新方法、テンプレート更新プログラム、生体認証クライアント装置及び生体認証サーバ装置

(57)【特許請求の範囲】

【請求項１】

更新値を生成する更新値生成部と、

生体情報から生成されるテンプレートを、前記更新値を用いて更新する第１の更新処理部と、

前記生体情報から前記テンプレートとともに生成される検証鍵を、前記更新値を用いて更新する第２の更新処理部と、

を有し、

Ｒａ、Ｒｂ、およびＲｃを乱数とし、ｇを素数ｑを位数とする群Ｇの生成元とすると、前記検証鍵は｛Ｒａ，Ｒｂ，g^{Rc}｝であり、

前記テンプレートは、｛ｔｅｍｐ１［ｉ］，ｔｅｍｐ２［ｉ］｝であり、

｛ｘ１，ｘ２，・・・，ｘｎ｝を前記生体情報とし、ｔｉを予め設定される係数とすると、ｔｅｍｐ１［ｉ］＝Ｒａ・ｘｉ＋Ｒｂ・ｔｉ＋Ｒｃであり、ｔｅｍｐ２［ｉ］＝g^{ti}であり、

Ｒａ、Ｒｂ、Ｒｃ、およびｔｉが、前記更新値に基づいて更新される

生体認証システム。

【請求項２】

前記生体情報から前記テンプレートと前記検証鍵の初期値を生成する秘匿情報生成部と、

前記テンプレートを格納するテンプレート格納部と、

前記検証鍵を格納する検証鍵格納部と、

を有する請求項１に記載の生体認証システム。
【請求項３】
前記第１の更新処理部は、前記テンプレート格納部に格納された前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、
前記第２の更新処理部は、検証鍵格納部に格納された前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する請求項２に記載の生体認証システム。
【請求項４】
前記更新値生成部は、乱数生成部を有し、当該乱数生成部により生成された乱数を前記更新値とする請求項１乃至３のいずれか１項に記載の生体認証システム。
【請求項５】
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成する秘匿認証情報生成装置と、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する秘匿認証情報検証装置と、
をさらに有する請求項１乃至４のいずれか１項に記載の生体認証システム。
【請求項６】
生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化された前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、を有する生体認証システムのテンプレート更新方法であって、
更新値を前記生体認証システム内で生成し、
前記更新値を用いて前記テンプレートを更新し、
前記更新値を用いて前記検証鍵を更新し、
Ｒａ、Ｒｂ、およびＲｃを乱数とし、ｇを素数ｑを位数とする群Ｇの生成元とすると、前記検証鍵は｛Ｒａ，Ｒｂ，g^{Rc}｝であり、
前記テンプレートは、｛ｔｅｍｐ１［ｉ］，ｔｅｍｐ２［ｉ］｝であり、
｛ｘ１，ｘ２，・・・，ｘｎ｝を前記生体情報とし、ｔｉを予め設定される係数とすると、ｔｅｍｐ１［ｉ］＝Ｒａ・ｘｉ＋Ｒｂ・ｔｉ＋Ｒｃであり、ｔｅｍｐ２［ｉ］＝g^{ti}であり、
Ｒａ、Ｒｂ、Ｒｃ、およびｔｉが、前記更新値に基づいて更新される
テンプレート更新方法。
【請求項７】
前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、
前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する請求項６に記載のテンプレート更新方法。
【請求項８】
前記生体認証システム内で生成される乱数を用いて前記更新値を生成する請求項６又は７に記載のテンプレート更新方法。
【請求項９】
前記更新値は、前記テンプレート格納部が設けられる生体認証クライアント装置と、前記検証鍵が設けられる生体認証サーバ装置とのいずれか一方で生成される請求項６乃至８のいずれか１項に記載のテンプレート更新方法。
【請求項１０】
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成し、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する請求項６乃至９のいずれか１項に記載のテンプレート更新方法。
【請求項１１】
生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化され

た前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、プログラムを実行する演算部と、を有する生体認証システムで実行されるテンプレート更新プログラムであって、
前記テンプレート更新プログラムは、
更新値を前記生体認証システム内で生成する更新値生成処理と、
前記更新値を用いて前記テンプレートを更新するテンプレート更新処理と、
前記更新値を用いて前記検証鍵を更新する検証鍵更新処理と、
を行い、
Ｒａ、Ｒｂ、およびＲｃを乱数とし、ｇを素数ｑを位数とする群Ｇの生成元とすると、前記検証鍵は｛Ｒａ，Ｒｂ，g^{Rc}｝であり、
前記テンプレートは、｛ｔｅｍｐ１［ｉ］，ｔｅｍｐ２［ｉ］｝であり、
｛ｘ１，ｘ２，・・・，ｘｎ｝を前記生体情報とし、ｔｉを予め設定される係数とすると、ｔｅｍｐ１［ｉ］＝Ｒａ・ｘｉ＋Ｒｂ・ｔｉ＋Ｒｃであり、ｔｅｍｐ２［ｉ］＝g^{ti}であり、
Ｒａ、Ｒｂ、Ｒｃ、およびｔｉが、前記更新値に基づいて更新される
テンプレート更新プログラム。
【請求項１２】
前記テンプレート更新処理では、前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、
前記検証鍵更新処理では、前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する請求項１１に記載のテンプレート更新プログラム。
【請求項１３】
前記更新値生成処理では、前記生体認証システム内で生成される乱数を用いて前記更新値を生成する請求項１１又は１２に記載のテンプレート更新プログラム。
【請求項１４】
前記テンプレート更新処理は、前記テンプレート格納部が設けられる生体認証クライアント装置内の第１の演算部で実行されるプログラムにより行われ、
前記検証鍵更新処理は、前記検証鍵が設けられる生体認証サーバ装置に設けられる第２の演算部で実行されプログラムにより行われ、
前記更新値生成処理は、前記第１の演算部と前記第２の演算部のいずれか一方で実行されるプログラムにより行われる請求項１１乃至１３のいずれか１項に記載のテンプレート更新プログラム。
【請求項１５】
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成する秘匿認証情報生成プログラムと、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する判定プログラムと、をさらに有する請求項１１乃至１４のいずれか１項に記載のテンプレート更新プログラム。
【請求項１６】
更新値を生成する更新値生成部と、
生体情報から生成されるテンプレートを、前記更新値を用いて更新するテンプレート更新処理部と、を有し、
前記更新値生成部は、前記生体情報から前記テンプレートとともに生成される検証鍵を有する生体認証サーバ装置に前記更新値を送信し、
Ｒａ、Ｒｂ、およびＲｃを乱数とし、ｇを素数ｑを位数とする群Ｇの生成元とすると、前記検証鍵は｛Ｒａ，Ｒｂ，g^{Rc}｝であり、
前記テンプレートは、｛ｔｅｍｐ１［ｉ］，ｔｅｍｐ２［ｉ］｝であり、
｛ｘ１，ｘ２，・・・，ｘｎ｝を前記生体情報とし、ｔｉを予め設定される係数とすると、ｔｅｍｐ１［ｉ］＝Ｒａ・ｘｉ＋Ｒｂ・ｔｉ＋Ｒｃであり、ｔｅｍｐ２［ｉ］＝g^{ti}であり、
Ｒａ、Ｒｂ、Ｒｃ、およびｔｉが、前記更新値に基づいて更新される

生体認証クライアント装置。
【請求項１７】
更新値を生成する更新値生成部と、
生体情報から生成されるテンプレートにより秘匿化された秘匿認証情報の正当性の検証に用いる検証鍵を前記更新値を用いて更新する検証鍵更新処理部と、を有し、
前記更新値生成部は、前記テンプレートを有する生体認証クライアント装置に前記更新値を送信し、
Ｒａ、Ｒｂ、およびＲｃを乱数とし、ｇを素数ｑを位数とする群Ｇの生成元とすると、前記検証鍵は｛Ｒａ，Ｒｂ，g^{Rc}｝であり、
前記テンプレートは、｛ｔｅｍｐ１［ｉ］，ｔｅｍｐ２［ｉ］｝であり、
｛ｘ１，ｘ２，・・・，ｘｎ｝を前記生体情報とし、ｔｉを予め設定される係数とすると、ｔｅｍｐ１［ｉ］＝Ｒａ・ｘｉ＋Ｒｂ・ｔｉ＋Ｒｃであり、ｔｅｍｐ２［ｉ］＝g^{ti}であり、
Ｒａ、Ｒｂ、Ｒｃ、およびｔｉが、前記更新値に基づいて更新される
生体認証サーバ装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は生体認証システム、そのテンプレート更新方法、テンプレート更新プログラム、生体認証クライアント装置及び生体認証サーバ装置に関し、特にテンプレートを用いて入力される生体情報を秘匿化した秘匿認証情報を検証鍵を用いて当該生体情報の正当性を判定する生体認証システム、そのテンプレート更新方法、テンプレート更新プログラム、生体認証クライアント装置及び生体認証サーバ装置に関する。
【背景技術】
【０００２】
個人認証の一方法に個人の生体情報を用いた生体認証がある。この生体認証では、認証に用いる生体情報を事前に登録しておく。このとき、生体情報は、そのまま保存した場合セキュリティ上、危険が大きい。そのため、この生体情報は、登録時に秘匿化鍵を用いて秘匿したテンプレートとして保存される。そして、この事前に登録していた生体情報(テンプレート)を秘匿しながら生体認証を行う技術を秘匿生体認証と呼ぶ。この秘匿生体認証では、認証時に検証鍵を用いて入力された生体情報の正当性を判断する。この秘匿生体認証に関する技術の一例が特許文献１に開示されている。
【０００３】
特許文献１に記載の生体認証システムは、利用者が入力した生体情報をもとに生成したテンプレートと、利用者の生体情報を表すテンプレートを暗号化して暗号化テンプレートとして記録媒体に記録した暗号化テンプレートを復号化して生成したテンプレートとを比較し、該比較結果をもとに利用者を認証する登録認証サーバを備え、登録認証サーバにより利用者の認証に成功したとき、前記記録媒体に記録した暗号化テンプレートを異なる暗号化キー用いた暗号化テンプレートに置換して記録する。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２００５－２９３４９０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
生体認証システムにおいてテンプレートが漏洩した場合には、テンプレートを更新しなければセキュリティ上のリスクが生じる。このテンプレートの更新の方法の1つは、生体情報を再度入力して新たなテンプレートを作成する方法がある。しかしながら、新たなテンプレートを作成するためには利用者に生体情報の再登録を依頼する必要があり、再登録

にかかる手間が膨大になる問題がある。
【課題を解決するための手段】
【０００６】
本発明にかかる生体認証システムの一態様は、更新値を生成する更新値生成部と、生体情報から生成されるテンプレートを、前記更新値を用いて更新する第１の更新処理部と、前記生体情報から前記テンプレートとともに生成される検証鍵を、前記更新値を用いて更新する第２の更新処理部と、を有する。
【０００７】
本発明にかかるテンプレート更新方法の一態様は、生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化された前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、を有する生体認証システムのテンプレート更新方法であって、更新値を前記生体認証システム内で生成し、前記更新値を用いて前記テンプレートを更新し、前記更新値を用いて前記検証鍵を更新する。
【０００８】
本発明にかかるテンプレート更新プログラムの一態様は、生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化された前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、プログラムを実行する演算部と、を有する生体認証システムで実行されるテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記テンプレート更新プログラムは、更新値を前記生体認証システム内で生成する更新値生成処理と、前記更新値を用いて前記テンプレートを更新するテンプレート更新処理と、前記更新値を用いて前記検証鍵を更新する検証鍵更新処理と、を行う。
【０００９】
本発明にかかる生体認証クライアント装置の一態様は、新値を生成する更新値生成部と、生体情報から生成されるテンプレートを、前記更新値を用いて更新するテンプレート更新処理部と、を有し、前記更新値生成部は、前記生体情報から前記テンプレートとともに生成される検証鍵を有する生体認証サーバ装置に前記更新値を送信する。
【００１０】
本発明にかかる生体認証サーバ装置の一態様は、更新値を生成する更新値生成部と、生体情報から生成されるテンプレートにより秘匿化された秘匿認証情報の正当性の検証に用いる検証鍵を前記更新値を用いて更新する検証鍵更新処理部と、を有し、前記更新値生成部は、前記テンプレートを有する生体認証クライアント装置に前記更新値を送信する。
【発明の効果】
【００１１】
本発明にかかる生体認証システム、そのテンプレート更新方法、テンプレート更新プログラム、生体認証クライアント装置及び生体認証サーバ装置によれば、生体認証システムにおけるテンプレートの更新を容易に行うことができる。
【図面の簡単な説明】
【００１２】
【図１】実施の形態１にかかる生体認証システムのブロック図である。
【図２】実施の形態１にかかる生体認証システムにおけるテンプレート更新処理の流れを説明するフローチャートである。
【図３】実施の形態２にかかる生体認証システムのブロック図である。
【図４】実施の形態２にかかる生体認証システムにおけるテンプレート更新処理の流れを説明するフローチャートである。
【図５】実施の形態３にかかる生体認証システムのブロック図である。
【図６】実施の形態にかかる生体認証システムのハードウェア構成の一例を説明するブロック図である。
【発明を実施するための形態】
【００１３】
説明の明確化のため、以下の記載及び図面は、適宜、省略、及び簡略化がなされている

。また、様々な処理を行う機能ブロックとして図面に記載される各要素は、ハードウェア的には、ＣＰＵ（Central Processing Unit）、メモリ、その他の回路で構成することができ、ソフトウェア的には、メモリにロードされたプログラムなどによって実現される。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは当業者には理解されるところであり、いずれかに限定されるものではない。なお、各図面において、同一の要素には同一の符号が付されており、必要に応じて重複説明は省略されている。

【００１４】

また、上述したプログラムは、様々なタイプの非一時的なコンピュータ可読媒体を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、ＣＤ－ＲＯＭ（Read Only Memory）、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリ（例えば、マスクＲＯＭ、ＰＲＯＭ（Programmable ROM）、ＥＰＲＯＭ（Erasable PROM）、フラッシュＲＯＭ、ＲＡＭ（Random Access Memory））を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

【００１５】

実施の形態にかかる生体認証システムは、生体認証サーバと利用者が接する生体認証クライアントの２つの装置が別々に設けられる例を説明する。しかしながら、生体認証システムとしては、生体認証サーバの機能と生体認証クライアントの機能とが１つの装置として実装されていても良い。

【００１６】

実施の形態１

図１に実施の形態１にかかる生体認証システム１のブロック図を示す。図１に示すように、実施の形態１にかかる生体認証システム１は、生体認証クライアント１０、生体認証サーバ２０を有する。生体認証クライアント１０と生体認証サーバ２０はネットワークにより相互にデータの送受信が可能なように接続される。

【００１７】

実施の形態１にかかる生体認証システム１は、基本的な機能として利用者の指紋、静脈、虹彩等の生体情報を用いた生体認証により、利用者が登録済みの利用者であるか否かを判定する生体認証処理を行う。そして、実施の形態１にかかる生体認証システム１は、生体認証処理に用いるテンプレートの更新を行う機能を有する。図１では、生体認証クライアント１０及び生体認証サーバ２０に関して、特徴の１つであるテンプレートと検証鍵の更新に関連する主なブロックのみを示すものである。つまり、生体認証クライアント１０、生体認証サーバ２０は、それぞれ図示しない他のブロックも有する。

【００１８】

図１では、生体認証クライアント１０は、第１の更新処理部（例えば、テンプレート更新部１１）、更新値生成部３０を有する。生体認証サーバ２０は、第２の更新処理部（例えば、検証鍵更新部２１）を有する。更新値生成部３０は、更新値ＵＤを生成する。テンプレート更新部１１は、生体情報から生成されるテンプレートを、更新値ＵＤを用いて更新する。なお、テンプレートは、生体認証クライアント１０内で生体情報に対して所定のルールを適用して秘匿化した情報である。また、テンプレートは、図示しないテンプレート格納部に保持されており、テンプレート更新部１１は、テンプレート格納部に格納されているテンプレートを更新して上書きする。

【００１９】

検証鍵更新部２１は、生体情報からテンプレートとともに生成される検証鍵を、更新値

ＵＤを用いて更新する。更新鍵は、例えば、テンプレートに対して乱数を適用した秘匿化処理が施されたものである。また、検証鍵は、図示しない検証鍵格納部に保持されており、検証鍵更新部２１は、検証鍵格納部に格納されている検証鍵を更新して上書きする。

【００２０】

続いて、実施の形態１にかかる生体認証システム１におけるテンプレート更新処理について説明する。図２に実施の形態１にかかる生体認証システムにおけるテンプレート更新処理の流れを説明するフローチャートを示す。なお、実施の形態１にかかる生体認証システム１では、テンプレートの更新に合わせて検証鍵も更新する。これにより、実施の形態１にかかる生体認証システム１では、テンプレートと検証鍵の整合性を維持する。そこで、図２ではテンプレートと検証鍵とを更新値ＵＤにより更新する例を示した。

【００２１】

図２に示すように、実施の形態１にかかる生体認証システム１では、まず、更新値生成部３０により更新値ＵＤを生成する（ステップＳ１）。続いて、更新値生成部３０は、更新値ＵＤを生体認証サーバ２０に送信する（ステップＳ２）。そして、テンプレート更新部１１により更新値ＵＤを用いたテンプレートを更新する（ステップＳ３）。また、検証鍵更新部２１により更新値ＵＤを用いた検証鍵の更新を行う（ステップＳ４）。

【００２２】

ここで、更新値ＵＤを用いたテンプレート及び検証鍵の更新処理の具体例の１つを説明する。ここでは、乱数Ｒａ”を更新値ＵＤとして、以下の生体情報、テンプレート、検証鍵を有する生体認証システム１において更新処理を行う例を説明する。

【００２３】

まず、生体情報は（１）式で示される生体特徴量ベクトルであり、テンプレートは（２）式、検証鍵は（３）式で示されるものが用いられる物とする。なお、以下の説明では、ｎは生体情報のベクトル要素数、ｉは０より大きくｎより小さいベクトル要素の番号を示す整数であり、ｔは予め設定される係数、Ｒは乱数である。また、ｇは、十分大きな素数ｑを位数とする群Ｇの生成元である。

【数１】

$$\{x1, x2, \cdots, xn\} \quad \cdots \quad (1)$$

【数２】

$$\{temp1[i], temp2[i]\} \quad \cdots \quad (2)$$

【数３】

$$\{Ra, Rb, g^{Rc}\} \quad \cdots \quad (3)$$

なお、テンプレート内のｔｅｍｐ１［ｉ］、ｔｅｍｐ２［ｉ］は（４）式及び（５）式出表わされる。

【数４】

$$temp1[i] = Ra \cdot xi + Rb \cdot ti + Rc \quad \cdots \quad (4)$$

【数５】

$$temp2[i] = g^{ti} \quad \cdots \quad (5)$$

【００２４】

そして、実施の形態１にかかる生体認証システム１では、更新値生成部３０において乱数Ｒａ”を補正値ＵＤとして生成する。そして、テンプレート更新部１１は、更新値ＵＤをテンプレートに適用して（６）式及び（７）式による計算を行い、（８）式の更新後のテンプレートを算出する。そして、テンプレート更新部１１は、（８）式のテンプレートによりテンプレート格納部のテンプレートを上書きする。

【数６】

$$temp1'[i] = temp1[i] \cdot Ra'' = Ra'' \cdot Ra \cdot xi + Ra'' \cdot Rb \cdot ti + Ra''Rc$$
$$= Ra' \cdot xi + Rb' \cdot ti + Rc' \quad \cdots \quad (6)$$

【数７】
$$temp2'[i] = temp2[i] \quad \cdots \quad (7)$$

【数８】
$$\{temp1'[i], temp2'[i]\} \quad \cdots \quad (8)$$

【００２５】
また、実施の形態１にかかる生体認証システム１では、更新値ＵＤとして乱数Ｒａ”を受信して、検証鍵更新部２１が（９）式～（１１）式を用いて（１２）式で示される更新後の検証鍵を算出する。

【数９】
$$Ra' = Ra'' \cdot Ra \quad \cdots \quad (9)$$

【数１０】
$$Rb' = Ra'' \cdot Rb \quad \cdots \quad (10)$$

【数１１】
$$g^{Rc'} = g^{Ra'' \cdot Rc} \quad \cdots \quad (11)$$

【数１２】
$$\{Ra', Rb', g^{Rc'}\} \quad \cdots \quad (12)$$

【００２６】
上記説明より、実施の形態１にかかる生体認証システム１では、更新値生成部３０で生成した補正値ＵＤを用いてテンプレート及び検証鍵を更新することで、生体情報を用いることなく新たなテンプレートを生成することができる。また、実施の形態１にかかる生体認証システム１では、テンプレートと同時に補正値ＵＤを用いて検証鍵を更新する。これにより、実施の形態１にかかる生体認証システム１では、テンプレートと検証鍵の整合性を容易に維持することができる。

【００２７】
また、実施の形態１にかかる生体認証システム１では、システム内の更新値生成部３０により更新値ＵＤを生成するため、更新処理に用いた情報が外部に漏洩するリスクが小さい。また、更新値ＵＤが乱数であることで、同じ更新値を生成することが困難であるため、生体認証システム１はセキュリティを高く維持することができる。

【００２８】
実施の形態２

実施の形態２では、実施の形態１にかかる生体認証システム１の別の形態となる生体認証システム２について説明する。そこで、図３に実施の形態２にかかる生体認証システムのブロック図を示す。図３に示すように、実施の形態２にかかる生体認証システム２では、更新値生成部３０が生体認証サーバ２０側に設けられる。

【００２９】
そのため、実施の形態２にかかる生体認証システム２では、テンプレート及び検証鍵の更新処理の流れのうち更新値ＵＤの受け渡し処理が実施の形態１と異なる。そこで、図４に実施の形態２にかかる生体認証システム２におけるテンプレート更新処理の流れを説明するフローチャートを示す。図４に示すように、実施の形態２にかかる生体認証システム２では、まず、更新値生成部３０により更新値ＵＤを生成する（ステップＳ１１）。続い

て、更新値生成部３０は、更新値ＵＤを生体認証クライアント１０に送信する（ステップＳ１２）。そして、テンプレート更新部１１により更新値ＵＤを用いたテンプレートの更新する（ステップＳ１３）。また、検証鍵更新部２１により更新値ＵＤを用いた検証鍵の更新を行う（ステップＳ１４）。

【００３０】

ここで、更新値ＵＤを用いたテンプレート及び検証鍵の更新処理の具体例について、実施の形態１とは異なる計算式を用いた方法を説明する。ここでは、乱数Ｒａ”、Ｒｂ”、Ｒｃ”の３つの乱数を更新値ＵＤとして、実施の形態１の（１）式～（３）式で示した生体情報、テンプレート、検証鍵を有する生体認証システム２において更新処理を行う例を説明する。

【００３１】

実施の形態２にかかる生体認証システム２では、更新値生成部３０で生成された更新値ＵＤを用いて、検証鍵更新部２１が（１３）式～（１５）式を用いて（１６）式で示される更新後の検証鍵を算出する。

【数１３】

$$Ra' = Ra'' \cdot Ra \quad \cdots \quad (13)$$

【数１４】

$$Rb' = Rb'' \cdot Rb \quad \cdots \quad (14)$$

【数１５】

$$g^{Rc\prime} = g^{Rc\prime\prime \cdot Rc} \quad \cdots \quad (15)$$

【数１６】

$$\{Ra', Rb', g^{Rc\prime}\} \quad \cdots \quad (16)$$

【００３２】

また、実施の形態２にかかる生体認証システム２では、更新値生成部３０が（１７）式で示す更新値ＵＤをテンプレート更新部１１に渡す。そして、テンプレート更新部１１は、（１８）式及び（１９）式を用いて（２０）式で示される更新後のテンプレートを算出する。

【数１７】

$$\left\{Ra'', \frac{1}{Rb''}, Rc''\right\} \quad \cdots \quad (17)$$

【数１８】

$$\begin{aligned} temp1'[i] = (temp1[i] \cdot Rc'') \cdot Rc'' &= Ra'' \cdot Ra \cdot xi + Ra'' \cdot Rb \cdot ti + Ra''(Rc + Rc'') \\ &= Ra'' \cdot Ra \cdot xi + Ra'' \cdot Rb'' \cdot \left(ti \cdot \frac{1}{Rb''}\right) + Ra''(Rc + Rc'') \\ &= Ra' \cdot xi + Rb' \cdot ti' + Rc' \quad \cdots \quad (18) \end{aligned}$$

【数１９】

$$temp2'^{[i]} = g^{ti\frac{1}{R2''}} = g^{ti\prime} \quad \cdots \quad (19)$$

【数２０】

$$\{temp1'[i], temp2'[i]\} \quad \cdots \quad (20)$$

【００３３】

上記説明より、更新値生成部３０は、生体認証クライアント１０と生体認証サーバ２０とのいずれに属していてもよく、更新値生成部３０により更新値ＵＤを生成することで、テンプレートの更新を容易に行うことが出来る。

【００３４】

また、更新値ＵＤとして生成する乱数は、生体認証システムの仕様に応じて任意に設定することができる。また、更新値ＵＤとしてどのような値を用いるかにより計算負荷を調整することもできる。

【００３５】

実施の形態３

実施の形態３にかかる生体認証システムは、実施の形態１、２で説明した生体認証システム１、２のより詳細な構成の一例を説明するものである。そこで、図５に実施の形態３にかかる生体認証システムのブロック図を示す。

【００３６】

図５に示す例では、生体認証クライアント１０がテンプレート更新部１１及び秘匿認証情報生成部１２を有する。また、生体認証サーバ２０が検証鍵更新部２１及び秘匿認証情報検証部２２を有する。また、図５では、更新値生成部３０及び登録情報秘匿部４０を示した。更新値生成部３０及び登録情報秘匿部４０は、生体認証クライアント１０と生体認証サーバ２０のいずれに装置内に配置されてもよく、また、生体認証クライアント１０及び生体認証サーバ２０とは異なる装置として独立して設けられていても良い。

【００３７】

テンプレート更新部１１は、個人認証に用いる生体情報から生成されるテンプレートを、更新値ＵＤを用いて更新する。テンプレート更新部１１は、更新値受信部１１１、テンプレート更新処理部１１２を有する。更新値受信部１１１は、更新値生成部３０から更新値ＵＤを受信し、テンプレート更新処理部１１２に渡すインタフェース回路である。テンプレート更新処理部１１２は、秘匿認証情報生成部１２内のテンプレート更新処理部１１２に格納されているテンプレートを更新する。テンプレート更新処理部１１２は、例えば、（６）式及び（７）式、或いは、（１８）式及び（１９）式を用いてテンプレートを更新する。

【００３８】

秘匿認証情報生成部１２は、利用者から取得する生体情報を秘匿化して認証に用いる秘匿認証情報を生成する。秘匿認証情報生成部１２は、テンプレート受信部１２１、テンプレート格納部１２２、秘匿認証情報生成処理部１２３、入力部１２４、出力部１２５を有する。テンプレート受信部１２１は、登録情報秘匿部４０で生成されたテンプレートを受信して、テンプレート格納部１２２に格納する。テンプレート格納部１２２は、テンプレートを格納する記憶部である。秘匿認証情報生成処理部１２３は、テンプレート格納部１２２に格納されているテンプレートと、生体認証サーバ２０から送信されるチャレンジ値と、を用いて入力部１２４から与えられた生体情報を秘匿化して秘匿認証情報を生成する。入力部１２４は、利用者の指紋等の生体情報を取得するスキャナ、カメラ等の入力機器である。出力部１２５は、生体認証サーバ２０により生体情報の判定結果に基づき生体認証クライアント１０内の図示していない機能部に認証結果を出力する。生体認証クライアント１０では、認証結果に基づき、機能ロック状態の解除、ゲートの解錠等の制限された機能の解除処理を行う。

【００３９】

生体認証サーバ２０は、生体認証クライアント１０から与えられる秘匿認証情報を用いて生体認証クライアント１０において取得した生体情報が登録済みの生体情報に対して正当な物と判定できるか否かを判定する認証処理を行う。生体認証サーバ２０は、検証鍵更新部２１、秘匿認証情報検証部２２を有する。

【００４０】

検証鍵更新部２１は、更新値受信部２１１、検証鍵更新処理部２１２を有する。更新値受信部２１１は、更新値生成部３０から更新値ＵＤを受信し、検証鍵更新処理部２１２に

渡すインタフェース回路である。検証鍵更新処理部２１２は、秘匿認証情報検証部２２内の検証鍵格納部２２２に格納されている検証鍵を更新する。検証鍵更新処理部２１２は、例えば、（９）式～（１１）式、或いは、（１３）式～（１５）式を用いて検証鍵を更新する。

【００４１】

秘匿認証情報検証部２２は、検証鍵受信部２２１、検証鍵格納部２２２、チャレンジ生成部２２３、判定部２２４、受理範囲記憶部２２５を有する。検証鍵受信部２２１は、登録情報秘匿部４０で生成される検証鍵を受信して、検証鍵格納部２２２に格納する。検証鍵格納部２２２は、検証鍵を格納する記憶部である。チャレンジ生成部２２３は、検証鍵格納部２２２に格納されている検証鍵を用いてチャレンジ値を生成して生体認証クライアント１０及び判定部２２４に与える。判定部２２４は、生体認証クライアント１０から与えられる秘匿認証情報をチャレンジ値、検証鍵を用いて解読し、解読結果を受理範囲記憶部２２５に格納されている受理範囲を参照して、入力部１２４により取得した生体情報が受理可能なものであるか否かを判定する。そして、判定部２２４は、判定結果を出力部１２５に出力する。受理範囲記憶部２２５は、受理範囲を示す情報を格納する記憶部である。受理範囲とは、１つの生体情報の揺らぎに対して受理可能と判定される範囲を示す情報である。

【００４２】

更新値生成部３０は、更新値ＵＤを生成する。図５に示す例では、更新値生成部３０は、乱数生成部３１及び更新値送信部３２を有する。乱数生成部３１は、更新値ＵＤとなる乱数を生成する。更新値送信部３２は、乱数生成部３１が生成した乱数を更新値ＵＤとしてテンプレート更新部１１及び検証鍵更新部２１に送信する。

【００４３】

登録情報秘匿部４０は、利用者の生体情報の生体認証システムへの登録処理を行う。登録情報秘匿部４０は、入力部４１、秘匿化部４２、乱数生成部４３、検証鍵生成部４４を有する。入力部４１は、例えば登録情報秘匿部４０が生体認証クライアント１０に組み込まれている場合、入力部１２４と同一の機器であってもよい。入力部４１は、利用者の生体情報を取得する機器である。秘匿化部４２は、入力部４１で取得された生体情報を所定のルールに基づき秘匿化してテンプレートを生成する。秘匿化部４２が生成したテンプレートは、テンプレート受信部１２１を介してテンプレート格納部１２２に格納される。乱数生成部４３は、乱数を生成する。検証鍵生成部４４は、秘匿化部４２が生成したテンプレートに乱数生成部４３で生成された乱数を適用して検証鍵を生成する。検証鍵生成部４４が生成した検証鍵は、検証鍵受信部２２１を介して検証鍵格納部２２２に格納される。

【００４４】

上記説明より、実施の形態３にかかる生体認証システムでは、テンプレートの更新処理以外に生体認証システムが有する認証機能を実現する処理ブロックを説明した。実施の形態３で説明した処理ブロックは、生体認証システムに実装される機能の一部であり、生体認証システムは他の処理機能を備えていても良い。

【００４５】

実施の形態４

実施の形態４では、生体認証システムを実現するハードウェア構成について説明する。そこで、図６に実施の形態にかかる生体認証システムのハードウェア構成の一例を説明するブロック図を示す。図６に示す例は、ハードウェア構成の一例であり、生体認証システム１を実現する他のハードウェア構成を除外するものではない。

【００４６】

図６に示す例では、生体認証システムは、１つの生体認証サーバ２０と複数の生体認証クライアント１０（例えば、生体認証クライアント１０ａ～１０ｅ）を有する。また、図６に示す例では、生体認証サーバ２０と生体認証クライアント１０a～１０ｅは相互にネットワークにより通信可能に接続される。

【００４７】

そして、生体認証クライアント１０ａ～１０ｅは同一のハードウェア構成で構成可能であるため、生体認証クライアント１０ａを例に生体認証クライアント１０ａ～１０ｅのハードウェア構成について説明する。

【００４８】

生体認証クライアント１０ａは、第１の演算部（例えば、演算部１００）、メモリ１０１、入力部１０２、通信インタフェース１０３を有する。演算部１００は、生体認証システムを実現するプログラムを実行する。このプログラムとしては、テンプレートの更新を行うテンプレート更新部１１を実現するテンプレート更新処理プログラムと、秘匿認証情報生成部１２の機能を実現する生体認証プログラムの一部がある。メモリ１０１は、テンプレート更新処理プログラム、生体認証プログラムが格納される記憶部である。また、メモリ１０１は、テンプレート格納部１２２となる記憶部である。入力部１０２は、入力部１２４を実現するハードウェアであり、指紋等の生体情報を取得するスキャナ或いはカメラである。通信インタフェース１０３は、演算部１００が生体認証サーバ２０と通信するためのインタフェース回路である。

【００４９】

生体認証サーバ２０は、第２の演算部（例えば、演算部２００）、メモリ２０１、通信インタフェース２０２を有する。演算部２００は、生体認証システムを実現するプログラムを実行する。このプログラムとしては、検証鍵更新部２１を実現する検証鍵更新プログラムと、秘匿認証情報検証部２２の機能を実現する生体認証プログラムの一部がある。メモリ２０１は、検証鍵更新プログラム、生体認証プログラムが格納される記憶部である。また、メモリ２０１は、検証鍵格納部２２２及び受理範囲記憶部２２５となる記憶部である、通信インタフェース２０２は、演算部２００が生体認証クライアント１０ａ～１０ｅと通信するためのインタフェース回路である。

【００５０】

このように、生体認証システムは、コンピュータと同等のハードウェア構成を有する装置においてプログラムを実行することで実現可能である。なお、生体認証システムは、上記で説明した機能を実現する専用のハードウェアを用いて構成することもできる。

【００５１】

なお、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。

【００５２】

（付記１）

更新値を生成する更新値生成部と、

生体情報から生成されるテンプレートを、前記更新値を用いて更新する第１の更新処理部と、

前記生体情報から前記テンプレートとともに生成される検証鍵を、前記更新値を用いて更新する第２の更新処理部と、

を有する生体認証システム。

（付記２）

前記生体情報から前記テンプレートと前記検証鍵の初期値を生成する秘匿情報生成部と、

前記テンプレートを格納するテンプレート格納部と、

前記検証鍵を格納する検証鍵格納部と、

を有する付記１に記載の生体認証システム。

（付記３）

前記第１の更新処理部は、前記テンプレート格納部に格納された前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、

前記第２の更新処理部は、検証鍵格納部に格納された前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する付記２に記載の生体認証システム。

（付記４）

前記更新値生成部は、乱数生成部を有し、当該乱数生成部により生成された乱数を前記

更新値とする付記１乃至３のいずれか１項に記載の生体認証システム。
（付記５）
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成する秘匿認証情報生成装置と、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する秘匿認証情報検証装置と、
をさらに有する付記１乃至４のいずれか１項に記載の生体認証システム。
（付記６）
生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化された前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、を有する生体認証システムのテンプレート更新方法であって、
更新値を前記生体認証システム内で生成し、
前記更新値を用いて前記テンプレートを更新し、
前記更新値を用いて前記検証鍵を更新するテンプレート更新方法。
（付記７）
前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、
前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する付記６に記載のテンプレート更新方法。
（付記８）
前記生体認証システム内で生成される乱数を用いて前記更新値を生成する付記６又は７に記載のテンプレート更新方法。
（付記９）
前記更新値は、前記テンプレート格納部が設けられる生体認証クライアント装置と、前記検証鍵が設けられる生体認証サーバ装置とのいずれか一方で生成される付記６乃至８のいずれか１項に記載のテンプレート更新方法。
（付記１０）
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成し、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する付記６乃至９のいずれか１項に記載のテンプレート更新方法。
（付記１１）
生体情報の秘匿化に用いるテンプレートを格納するテンプレート格納部と、秘匿化された前記生体情報の検証に用いる検証鍵を格納する検証鍵格納部と、プログラムを実行する演算部と、を有する生体認証システムで実行されるテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記テンプレート更新プログラムは、
更新値を前記生体認証システム内で生成する更新値生成処理と、
前記更新値を用いて前記テンプレートを更新するテンプレート更新処理と、
前記更新値を用いて前記検証鍵を更新する検証鍵更新処理と、
を行うテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体。
（付記１２）
前記テンプレート更新処理では、前記テンプレートに含まれる値に前記更新値を乗算することで前記テンプレートを更新し、
前記検証鍵更新処理では、前記検証鍵に含まれる値に前記更新値を乗算することで前記検証鍵を更新する付記１１に記載のテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体。
（付記１３）
前記更新値生成処理では、前記生体認証システム内で生成される乱数を用いて前記更新

値を生成する付記１１又は１２に記載のテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体。
（付記１４）
前記テンプレート更新処理は、前記テンプレート格納部が設けられる生体認証クライアント装置内の第１の演算部で実行されるプログラムにより行われ、
前記検証鍵更新処理は、前記検証鍵が設けられる生体認証サーバ装置に設けられる第２の演算部で実行されプログラムにより行われ、
前記更新値生成処理は、前記第１の演算部と前記第２の演算部のいずれか一方で実行されるプログラムにより行われる付記１１乃至１３のいずれか１項に記載のテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体。
（付記１５）
新たに入力される前記生体情報を前記テンプレートを用いて秘匿化して秘匿認証情報を生成する秘匿認証情報生成プログラムと、
前記秘匿認証情報に前記検証鍵を適用して、新たに入力された前記生体情報が受理可能なものであるか否かを判定する判定プログラムと、をさらに有する付記１１乃至１４のいずれか１項に記載のテンプレート更新プログラムを記録したコンピュータ読み取り可能な記録媒体。
（付記１６）
更新値を生成する更新値生成部と、
生体情報から生成されるテンプレートを、前記更新値を用いて更新するテンプレート更新処理部と、を有し、
前記更新値生成部は、前記生体情報から前記テンプレートとともに生成される検証鍵を有する生体認証サーバ装置に前記更新値を送信する生体認証クライアント装置。
（付記１７）
更新値を生成する更新値生成部と、
生体情報から生成されるテンプレートにより秘匿化された秘匿認証情報の正当性の検証に用いる検証鍵を前記更新値を用いて更新する検証鍵更新処理部と、を有し、
前記更新値生成部は、前記テンプレートを有する生体認証クライアント装置に前記更新値を送信する生体認証サーバ装置。
【符号の説明】
【００５３】
１　生体認証システム
２　生体認証システム
１０　生体認証クライアント
１１　テンプレート更新部
１２　秘匿認証情報生成部
２０　生体認証サーバ
２１　検証鍵更新部
２２　秘匿認証情報検証部
３０　更新値生成部
３１　乱数生成部
３２　更新値送信部
４０　登録情報秘匿部
４１　入力部
４２　秘匿化部
４３　乱数生成部
４４　検証鍵生成部
１１１　更新値受信部
１１２　テンプレート更新処理部
１２１　テンプレート受信部

１２２　テンプレート格納部
１２３　秘匿認証情報生成処理部
１２４　入力部
１２５　出力部
２１１　更新値受信部
２１２　検証鍵更新処理部
２２１　検証鍵受信部
２２２　検証鍵格納部
２２３　チャレンジ生成部
２２４　判定部
２２５　受理範囲記憶部
１００　演算部
１０１　メモリ
１０２　入力部
１０３　通信インタフェース
２００　演算部
２０１　メモリ
２０２　通信インタフェース
ＵＤ　更新値

【図面】

【図１】

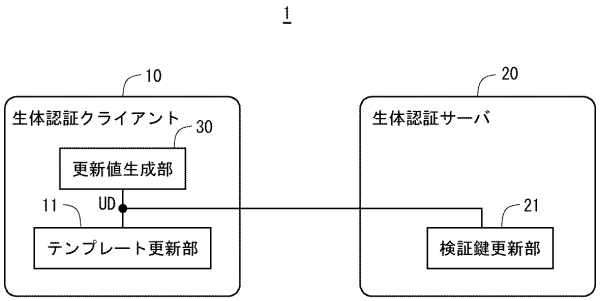

Fig. 1

【図２】

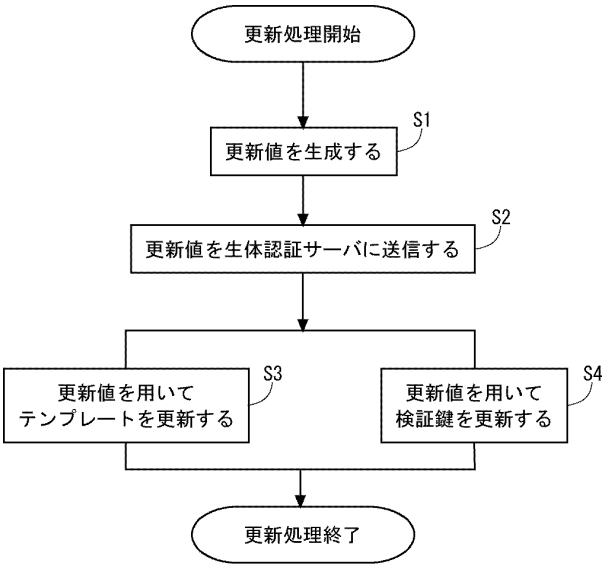

Fig. 2

【図３】

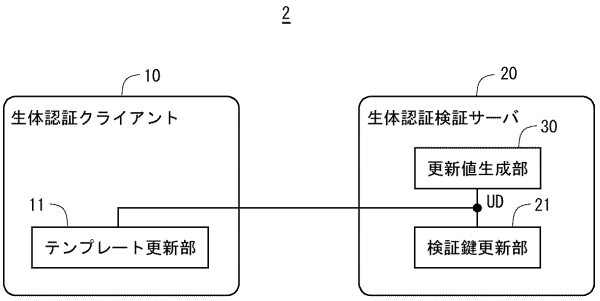

Fig. 3

【図４】

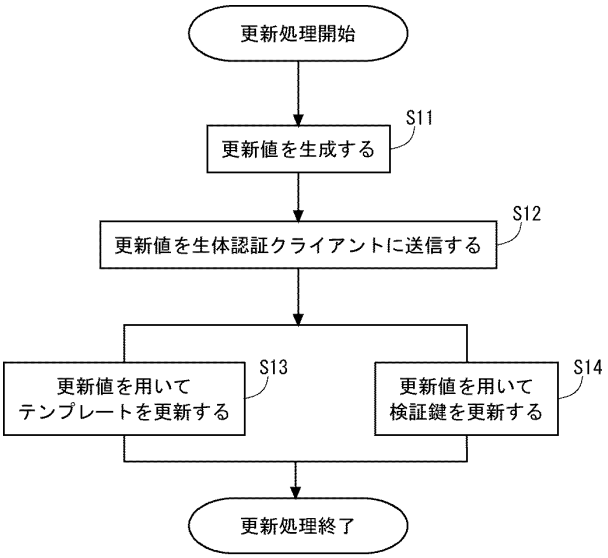

Fig. 4

【図５】

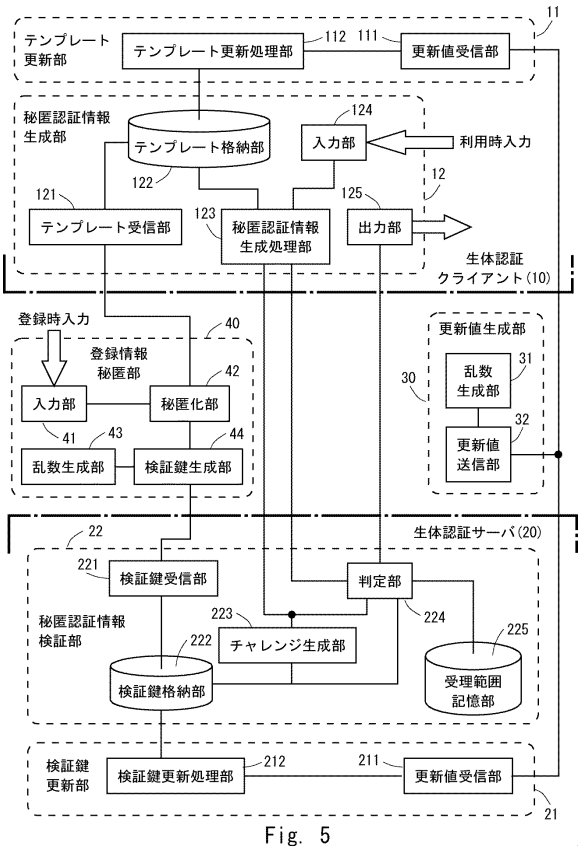

Fig. 5

【図６】

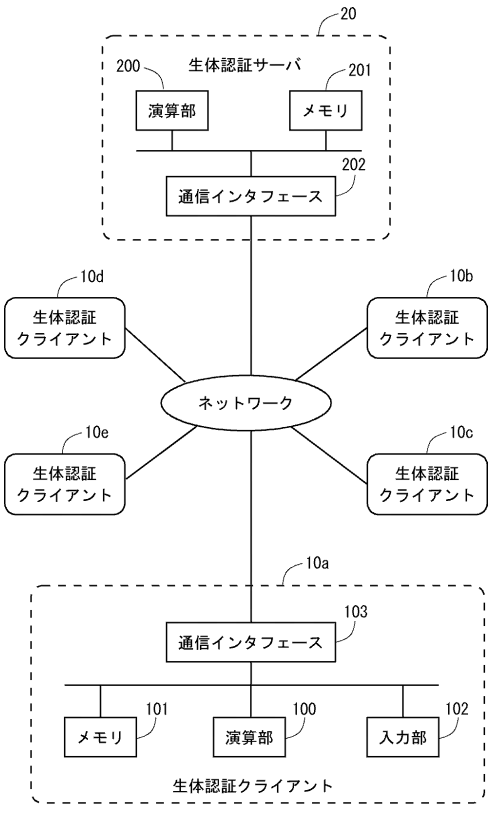

Fig. 6

フロントページの続き

東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者 田宮 寛人
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 辻 勇貴
(56)参考文献 国際公開第２０１３／０８０３２０（WO，Ａ１）
特開２０１８－２０７４３３（ＪＰ，Ａ）
国際公開第２０２０／２４５９３９（WO，Ａ１）
米国特許出願公開第２０２０／０１２７８２４（ＵＳ，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３２