(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7632477号
(P7632477)

(45)発行日　令和7年2月19日(2025.2.19)

(24)登録日　令和7年2月10日(2025.2.10)

(51)国際特許分類

Ｇ０６Ｆ　21/32　(2013.01)	Ｇ０６Ｆ	21/32	
Ｇ０６Ｆ　21/45　(2013.01)	Ｇ０６Ｆ	21/45	
Ｇ０６Ｆ　21/60　(2013.01)	Ｇ０６Ｆ	21/60	３２０

ＦＩ

請求項の数　9　（全29頁）

(21)出願番号　特願2022-569389(P2022-569389)
(86)(22)出願日　令和2年12月16日(2020.12.16)
(86)国際出願番号　PCT/JP2020/046917
(87)国際公開番号　WO2022/130528
(87)国際公開日　令和4年6月23日(2022.6.23)
審査請求日　令和5年6月12日(2023.6.12)

(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　田宮 寛人

最終頁に続く

(54)【発明の名称】　回復用検証システム、照合システム、回復用検証方法およびプログラム

(57)【特許請求の範囲】

【請求項１】

被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶するテンプレート記憶手段と、

クライアントの要求に応じて、乱数を生成する乱数生成手段と、

前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成手段と、

判定手段と、

登録用入力情報ごとに固有の固有鍵を記憶する鍵記憶手段と、

を備え、

前記判定手段は、

登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得し、

前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行い、

前記乱数生成手段は、

前記クライアントの前記要求に応じて、第１乱数を発生する第１乱数生成手段と、

前記クライアントの前記要求に応じて、第２乱数を発生する第２乱数生成手段と

を有し、
前記秘匿化テンプレート生成手段は、前記第１乱数と、前記第２乱数を用いて前記固有鍵を秘匿化した秘匿化固有鍵と、を用いて、前記秘匿化テンプレートを生成し、
前記判定手段は、前記公開鍵、前記第１乱数および前記固有鍵を用いて、前記秘匿化指標を復号した指標を生成する
回復用検証システム。
【請求項２】
前記判定手段は、生成された前記指標が所定範囲内の値を示す場合、前記照合情報についての認証を受理する
請求項１に記載の回復用検証システム。
【請求項３】
前記照合情報ごとにチャレンジ信号を生成して前記クライアントに送信するチャレンジ生成手段をさらに有し、
前記クライアントにおいて、前記チャレンジ信号に対応するレスポンスとして前記秘匿化指標を算出するように構成されている
請求項１または２に記載の回復用検証システム。
【請求項４】
前記登録用入力情報および前記照合情報は、何れもベクトルによって表される、
請求項１から３のいずれか一項に記載の回復用検証システム。
【請求項５】
前記秘匿化指標は、前記照合情報と、前記秘匿化テンプレートと、の内積に基づいて定められる
請求項１から４のいずれか一項に記載の回復用検証システム。
【請求項６】
クライアントと、
被登録者の通常登録用入力情報の照合のために入力される通常照合情報、についての認証を行う通常検証システムと、
前記被登録者の前記通常登録用入力情報に関連するアカウントを回復するための回復用検証システムと
を備える照合システムであって、
前記回復用検証システムは、
前記被登録者の生体情報である回復用の登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶するテンプレート記憶手段と、
前記クライアントの要求に応じて、乱数を生成する乱数生成手段と、
前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成手段と、
判定手段と、
登録用入力情報ごとに固有の固有鍵を記憶する鍵記憶手段と、
を備え、
前記判定手段は、
回復用の登録用入力情報と、被認証者の生体情報である回復用照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記回復用照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得し、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記回復用照合情報についての認証を行い、
前記乱数生成手段は、
前記クライアントの前記要求に応じて、第１乱数を発生する第１乱数生成手段と、
前記クライアントの前記要求に応じて、第２乱数を発生する第２乱数生成手段と
を有し、

前記秘匿化テンプレート生成手段は、前記第１乱数と、前記第２乱数を用いて前記固有鍵を秘匿化した秘匿化固有鍵と、を用いて、前記秘匿化テンプレートを生成し、
前記判定手段は、前記公開鍵、前記第１乱数および前記固有鍵を用いて、前記秘匿化指標を復号した指標を生成する
照合システム。
【請求項７】
前記クライアントは、
前記秘密鍵と前記公開鍵とを生成する鍵生成手段と、
前記秘密鍵を用いて前記テンプレートを生成するテンプレート生成手段と
を有し、
前記鍵生成手段は、前記公開鍵を前記回復用検証システムに送信する
請求項６に記載の照合システム。
【請求項８】
クライアントの要求に応じて、乱数を生成する乱数生成段階と、
前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成段階であって、前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである、秘匿化テンプレート生成段階と、
登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する取得段階と、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う認証段階と、をコンピュータが実行し、
前記乱数生成段階は、前記クライアントの前記要求に応じて、第１乱数を発生し、前記クライアントの前記要求に応じて、第２乱数を発生する段階を含み、
前記秘匿化テンプレート生成段階は、前記第１乱数と、前記第２乱数を用いて登録用入力情報ごとに固有の固有鍵を秘匿化した秘匿化固有鍵と、を用いて、前記秘匿化テンプレートを生成する段階を含み、
前記認証段階は、前記公開鍵、前記第１乱数および前記固有鍵を用いて、前記秘匿化指標を復号した指標を生成する段階を含む
回復用検証方法。
【請求項９】
クライアントの要求に応じて、乱数を生成する乱数生成処理と、
前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成処理であって、前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである、秘匿化テンプレート生成処理と、
登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する取得処理と、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う認証処理と、をコンピュータに実行させ、
前記乱数生成処理は、前記クライアントの前記要求に応じて、第１乱数を発生し、前記クライアントの前記要求に応じて、第２乱数を発生する処理を含み、
前記秘匿化テンプレート生成処理は、前記第１乱数と、前記第２乱数を用いて登録用入力情報ごとに固有の固有鍵を秘匿化した秘匿化固有鍵と、を用いて、前記秘匿化テンプレートを生成する処理を含み、
前記認証処理は、前記公開鍵、前記第１乱数および前記固有鍵を用いて、前記秘匿化指

標を復号した指標を生成する処理を含む
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、回復用検証システム、照合システム、回復用検証方法および非一時的なコンピュータ可読媒体に関する。
【背景技術】
【０００２】
クライアントがサーバシステムにログインする場合、予め登録されているクライアントのユーザの登録情報（秘密情報）と、ユーザから入力される情報とを照合する認証処理が行われる（特許文献１、２、３および４参照）。
【０００３】
そしてこのようなシステムにおいて、ユーザが認証に用いる秘密情報を失った場合に、アクセス権限を回復する処理（アカウントリカバリ）が行われている。ここでＦＩＤＯ（Fast ID entity Online）アライアンスが発行した非特許文献１では、複数のクライアントやＩＣカード等にテンプレートを登録しておくことが推奨されている。これにより、ユーザが認証に用いる秘密情報を完全に失いにくくし、アカウントリカバリが実施される回数を削減することができる。
【０００４】
さらに、非特許文献１では、ユーザが全てのテンプレートを失った際のアカウントリカバリ方法として２つの方法が挙げられている。第１の方法は、テンプレート登録時と同様の身元確認を行う方法であり、第２の方法は、アカウントリカバリ用の認証情報を予めサーバに登録しておき、それを用いて身元確認を行う方法である。第１の方法としては、例えば運転免許証等の身分証明書の確認を行う方法が挙げられる。また、第２の方法としては、予め登録しておいた電話番号やメールアドレスにリカバリーコードを送信し、リカバリーコードを確認する方法が挙げられる。
【先行技術文献】
【特許文献】
【０００５】
【文献】特開２０１１－２１１５９３号公報
【文献】特開２００９－１２９２９２号公報
【文献】国際公開第２０１８／１１０６０８号
【文献】国際公開第２０２０／１２１４６１号
【非特許文献】
【０００６】
【文献】五味 英仁, Bill Leddy, Dean H. Saxe著, 「Recommended Account Recovery Practices for FIDO Relying Parties」, FIDO Alliance, ２０１９年
【発明の概要】
【発明が解決しようとする課題】
【０００７】
アカウントリカバリとして、身分証明書で身元確認を行う方法は一般に利便性が低く、リカバリーコードで身元確認を行う方法は一般に安全性が低い。
【０００８】
利便性と安全性を両立させるために、アカウントリカバリに生体認証を用いることが提案されている。しかし一般にアカウントリカバリに生体認証を用いる場合、アカウントリカバリ時の検証サーバに、テンプレートとして個人情報である生体特徴量を保管しておく必要がある。したがって、マルウェア等によるサイバー攻撃や管理者の不正等により、テンプレートが漏えいしてしまった場合、生涯不変の生体特徴量が漏洩してしまうというリスクが存在する。したがって、アカウントリカバリ時の認証においても、生体認証に用い

るテンプレートを厳重に保護する必要があるという課題があった。

【０００９】

本開示は、このような課題を解決するためになされたものであり、利便性および安全性が高い回復用検証システム、照合システム、回復用検証方法および非一時的なコンピュータ可読媒体を提供することを目的とする。

【課題を解決するための手段】

【００１０】

本開示の一態様にかかる回復用検証システムは、テンプレート記憶手段と、乱数生成手段と、秘匿化テンプレート生成手段と、判定手段とを備える。前記テンプレート記憶手段は、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶する。前記乱数生成手段は、クライアントの要求に応じて、乱数を生成する。前記秘匿化テンプレート生成手段は、前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記秘匿化テンプレートを前記クライアントに送信する。前記判定手段は、登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する。そして前記判定手段は、前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う。

【００１１】

本開示の一態様にかかる照合システムは、クライアントと、通常検証システムと、回復用検証システムとを備える。前記通常検証システムは、被登録者の通常登録用入力情報の照合のために入力される通常照合情報、についての認証を行う。前記回復用検証システムは、前記被登録者の前記通常登録用入力情報に関連するアカウントを回復するためのシステムである。前記回復用検証システムは、回復用検証システムは、テンプレート記憶手段と、乱数生成手段と、秘匿化テンプレート生成手段と、判定手段とを備える。前記テンプレート記憶手段は、被登録者の生体情報である回復用の登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶する。前記乱数生成手段は、クライアントの要求に応じて、乱数を生成する。前記秘匿化テンプレート生成手段は、前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記秘匿化テンプレートを前記クライアントに送信する。前記判定手段は、回復用の登録用入力情報と、被認証者の生体情報である回復用照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記回復用照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する。そして前記判定手段は、前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記回復用照合情報についての認証を行う。

【００１２】

本開示の一態様にかかる回復用検証方法は、乱数生成段階と、秘匿化テンプレート生成段階と、取得段階と、認証段階とを備える。前記乱数生成段階は、クライアントの要求に応じて、乱数を生成する段階である。前記秘匿化テンプレート生成段階は、前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する段階である。前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである。前記取得段階は、秘匿化指標の情報を、前記クライアントから取得する段階である。前記秘匿化指標は、登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出されたものである。前記認証段階は、前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う段階である。

【００１３】
本開示の一態様にかかる非一時的なコンピュータ可読媒体は、コンピュータに、乱数生成処理と、秘匿化テンプレート生成処理と、取得処理と、認証処理とを実行させる。前記乱数生成処理は、クライアントの要求に応じて、乱数を生成する処理である。前記秘匿化テンプレート生成処理は、前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する処理である。前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである。前記取得処理は、秘匿化指標の情報を、前記クライアントから取得する処理である。前記秘匿化指標は、登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出されたものである。前記認証処理は、前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う処理である。
【発明の効果】
【００１４】
本開示により、生体認証を基礎としつつテンプレートを保護したまま照合を行うため、利便性および安全性が高い回復用検証システム、照合システム、回復用検証方法および非一時的なコンピュータ可読媒体を提供できる。
【図面の簡単な説明】
【００１５】
【図１】実施形態１にかかる回復用検証システムの機能構成を示すブロック図である。
【図２】回復用検証システムが適用されることができる照合システムの概略構成図である。
【図３】実施形態２にかかる通常照合システムの概略構成図である。
【図４】実施形態２にかかる回復用照合システムの概略構成図である。
【図５】実施形態２にかかる通常照合システムの登録処理の手順を示すシーケンス図である。
【図６】実施形態２にかかる通常照合システムの認証処理の手順を示すシーケンス図である。
【図７】実施形態２にかかる回復用照合システムの回復用登録処理の手順を示すシーケンス図である。
【図８】実施形態２にかかる回復用照合システムの回復用認証処理の手順を示すシーケンス図である。
【図９】本実施形態やその具体例におけるクライアントやサーバに係るコンピュータの構成例を示す概略ブロック図である。
【発明を実施するための形態】
【００１６】
以下、実施形態を通じて本開示を説明するが、請求の範囲にかかる発明を以下の実施形態に限定するものではない。また、実施形態で説明する構成の全てが課題を解決するための手段として必須であるとは限らない。説明の明確化のため、以下の記載および図面は、適宜、省略、および簡略化がなされている。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いる。
【００１７】
＜実施形態の課題＞
ここで、本実施形態が解決しようとする課題について改めて説明する。
認証の一例として、生体認証がある。「生体認証」とは、被登録者の生体情報と、被認証者の生体情報と、を照合することにより、被登録者と被認証者とが一致するか否かを確認する個人認証の手法である。また、「生体情報」とは、身体や行動に関する一部の特徴から抽出されたデータ、または、その抽出されたデータを変換することによって生成されたデータである。このデータは、特徴量と称されることもある。ここで、被登録者の生体情報（以下では登録情報と称す。）によって生成されたデータを含む、生体認証のために

予め保存されるデータは、テンプレートと呼ばれる。

【００１８】

クライアント・サーバシステムによって生体認証を行う場合、テンプレートをクライアントに保存する態様と、テンプレートをサーバに保存する態様と、がある。

【００１９】

上述の特許文献１および特許文献２には、暗号化された登録情報をテンプレートとしてサーバに保存することにより、登録情報が漏えいしない認証装置および認証方法の一例が記載されている。また、上述の特許文献３には、二値のベクトルに関して安全性を高める照合システムが記載されている。

【００２０】

クライアントにテンプレートを保存する態様の例としては、ＦＩＤＯ（Fast ID entity Online）認証方式が挙げられる。ＦＩＤＯ認証方式では、クライアントに予めテンプレートが保存される。そして、そのクライアントを現在使用しているユーザ（被認証者）の生体情報がクライアントに入力されると、クライアントは、入力された生体情報と、テンプレートとによって、被認証者が被登録者に該当するか否かを判定する。そして、被認証者が被登録者に該当するとクライアントが判定した場合、サーバは、クライアントが署名鍵（秘密鍵）によって生成したデジタル署名に基づいて、クライアントが有する署名鍵と、サーバが有する検証鍵（公開鍵）とが対をなす鍵であるか否かを判定する。すなわち、ＦＩＤＯ認証方式では、クライアントにおいて生体認証に成功し、サーバにおいてクライアントの署名の検証に成功した場合に、最終的に、ユーザ（被認証者）の認証に成功したと判定される。

【００２１】

また、ＦＩＤＯ認証方式では、被登録者の生体情報を暗号化した情報を含むデータが、テンプレートとして予めクライアントに保存される。そして、その暗号化された情報を復号するための鍵もクライアントに保存される。被認証者の生体情報がクライアントに入力されると、クライアントは、その鍵を用いてテンプレートに含まれる生体情報の暗号文を復号し、復号された生体情報と、入力された生体情報を用いて、被認証者が被登録者に該当するか否かを判定する。

【００２２】

特許文献４には、クライアントにテンプレートが保存されており、クライアントがテンプレートと照合情報との近さを示す指標を秘匿化した秘匿化指標を算出し、サーバが秘匿化指標に基づいて認証を行う照合システムが開示されている。

【００２３】

また、IC（Integrated Circuit）カードのＩＣチップに、暗号化された生体情報を保存しておく場合もある。

【００２４】

ところで認証システムにおいて、ユーザが認証に用いる秘密情報を失った場合には、アクセス権限を回復するアカウントリカバリが必要となる。ＦＩＤＯアライアンスが発行した非特許文献１では、ユーザが全てのテンプレートを失った場合のアカウントリカバリ方法として、２つの方法が挙げられている。しかし上述の通り、利便性または安全性の面で課題があった。

【００２５】

利便性と安全性を両立させるために、アカウントリカバリに生体認証を用いることが提案されているが、上述の通り、テンプレートの漏えいリスクを低減するために安全性の向上が求められている。

【００２６】

以上のように、アカウントリカバリには、利便性および安全性の両立という課題が存在する。本開示は、このような課題を解決するためになされたものであり、以下に実施形態を説明する。

【００２７】

＜実施形態１＞
まず図１を用いて、本開示の実施形態１について説明する。図１は、実施形態１にかかる回復用検証システム１０の機能構成を示すブロック図である。回復用検証システム１０は、アカウントリカバリのための認証を行うコンピュータシステムである。回復用検証システム１０は、クライアント２０に通信可能に接続されている。クライアント２０は、被認証者が認証のために使用するコンピュータ装置またはコンピュータシステムである。
【００２８】
回復用検証システム１０は、テンプレート記憶部１５１と、乱数生成部１５３と、秘匿化テンプレート生成部１５２と、判定部１７５とを備える。
【００２９】
テンプレート記憶部１５１は、テンプレートを記憶する。テンプレートは、登録用入力情報を、秘密鍵を用いて暗号化した情報である。登録用入力情報は、アカウント回復用のユーザ登録のために、被登録者が入力した、被登録者の生体情報である。
【００３０】
乱数生成部１５３は、クライアント２０のアカウント回復要求に応じて、乱数を生成する。
【００３１】
秘匿化テンプレート生成部１５２は、乱数生成部１５３が生成した乱数を用いて、テンプレート記憶部１５１に格納されているテンプレートを秘匿化し、その結果として秘匿化テンプレートを生成する。そして秘匿化テンプレート生成部１５２は、生成した秘匿化テンプレートをクライアント２０に送信する。
【００３２】
判定部１７５は、秘匿化指標の情報を、クライアント２０から取得する。そして秘匿化指標は、登録用入力情報と、照合情報と、の間の近似度を秘匿化した指標である。照合情報は、アカウント回復用のユーザ認証のために、被認証者が入力した被認証者の生体情報である。秘匿化指標は、クライアント２０において、照合情報と秘匿化テンプレートとに基づいて算出される。
【００３３】
次に判定部１７５は、秘密鍵に対応する公開鍵と、乱数生成部１５３が生成した乱数とを用いて、秘匿化指標を復号した指標を生成する。そして判定部１７５は、生成された（復号した）指標が所定範囲内の値を示すか否かに基づいて、照合情報についての認証を行う。例えば判定部１７５は、生成された指標が所定範囲内の値を示す場合、照合情報についての認証を受理する。
【００３４】
このように実施形態１によれば、回復用検証システム１０は、生体認証を基礎としているため、生体認証と同程度の利便性を有している。また回復用検証システム１０は、テンプレートを保護したまま照合処理を行う。このとき回復用検証システム１０は、クライアントの要求に応じて発生させた乱数、すなわち要求毎に異なる乱数、で保護したテンプレートをクライアントに提供するため、生体情報の漏洩リスクが小さく、安全性が高い。このような利便性かつ安全性の高いシステムをアカウントリカバリに採用することで、アカウントリカバリのための管理コストを低減できる。
【００３５】
＜実施形態２＞
次に図２～８を用いて、本開示の実施形態２について説明する。図２は、回復用検証システムが適用されることができる照合システム１の概略構成図である。照合システム１は、サーバ側システム１０ａと、クライアント側システム２０ａとを備える。
【００３６】
サーバ側システム１０ａは、サーバ側のコンピュータシステムである。サーバ側システム１０ａは、認証情報検証装置１３０と、回復用登録情報記憶装置１５０と、回復用認証情報検証装置１７０とを有する。

【００３７】
クライアント側システム２０ａは、クライアント側のコンピュータシステムであり、実施形態１にかかるクライアント２０に対応する。クライアント側システム２０ａは、登録情報生成装置１１０と、認証情報生成装置１２０と、回復用登録情報生成装置１４０と、回復用認証情報生成装置１６０とを有する。
【００３８】
登録情報生成装置１１０、認証情報生成装置１２０および認証情報検証装置１３０は、通常照合システム２を構成するコンピュータ装置である。通常照合システム２は、通常登録処理および通常認証処理を行う照合システムである。通常照合システム２内の各装置は、互いに通信可能に接続される。
【００３９】
登録情報生成装置１１０は、通常認証処理に用いる被登録者の通常登録情報を生成し、通常登録情報を登録する。すなわち登録情報生成装置１１０は、通常登録処理を実行する。ここで通常登録情報は、被登録者の秘密情報を暗号化した情報、いわゆる通常のテンプレートである。例えば秘密情報は、パスワード等のテキストデータまたは被登録者の生体情報であってよいが、これらに限らない。また被登録者は、クライアント側システム２０ａのユーザであってよい。
【００４０】
認証情報生成装置１２０は、被登録者の通常登録情報と、被認証者の通常照合情報とを用いて、通常認証情報を生成する。ここで通常照合情報は、被認証者によって、被登録者の通常登録情報の照合のために入力される情報である。また通常認証情報は、通常認証を受理するか否かを判定するための材料となる情報であり、例えば通常登録情報と、通常照合情報との近似度を示す情報である。
【００４１】
認証情報検証装置１３０は、通常認証情報を検証し、その結果として通常照合情報についての認証を行う。なお認証情報検証装置１３０は、通常検証システムとも呼ばれる。
【００４２】
回復用登録情報生成装置１４０、回復用登録情報記憶装置１５０、回復用認証情報生成装置１６０および回復用認証情報検証装置１７０は、回復用照合システム３を構成するコンピュータ装置である。回復用照合システム３は、被登録者の通常登録情報に関連するアカウントを回復するための回復用登録処理および回復用認証処理を行う照合システムである。
【００４３】
回復用登録情報生成装置１４０は、秘密鍵を用いて、回復用認証処理に用いる被登録者の回復用登録情報を生成する。回復用登録情報は、被登録者の生体情報である回復用の登録用入力情報（回復登録用入力情報）を秘密鍵で暗号化した情報である。つまり回復用登録情報は、実施形態１のテンプレートに対応する。回復用登録情報生成装置１４０は、回復用登録情報記憶装置１５０および回復用認証情報検証装置１７０に通信可能に接続される。回復用登録情報生成装置１４０は、回復用登録情報を回復用登録情報記憶装置１５０に、秘密鍵に対応する公開鍵を回復用認証情報検証装置１７０に送信する。
【００４４】
回復用登録情報記憶装置１５０は、回復用登録情報を記憶する。回復用登録情報記憶装置１５０は、回復用認証情報生成装置１６０の要求に応じて乱数を発生させて乱数マスクを生成する。回復用登録情報記憶装置１５０は、回復用登録情報および生成した乱数マスクを用いて、回復情報を生成する。回復情報は、実施形態１の秘匿化テンプレートに対応する。回復用登録情報記憶装置１５０は、回復情報を回復用認証情報生成装置１６０に送信する。
【００４５】
回復用認証情報生成装置１６０は、回復情報と、被認証者が入力した被認証者の生体情報である回復用照合情報とを用いて、回復用認証情報を生成する。回復用照合情報は、実

施形態１の照合情報に対応する。また回復用認証情報は、回復登録用入力情報と、回復用照合情報と、の間の近似度を秘匿化した秘匿化指標の情報を含む。回復用認証情報生成装置１６０は、回復用認証情報を回復用認証情報検証装置１７０に送信する。

【００４６】

回復用認証情報検証装置１７０は、被登録者の通常登録情報に関連するアカウントを回復するために、公開鍵および乱数マスクを用いて回復用認証情報を検証し、その結果として回復用照合情報の認証を行う。

【００４７】

また回復用登録情報記憶装置１５０および回復用認証情報検証装置１７０は、実施形態１の回復用検証システム１０に対応する。

【００４８】

サーバ側システム１０ａを構成する認証情報検証装置１３０、回復用登録情報記憶装置１５０、および回復用認証情報検証装置１７０の各種機能は、単一の装置に実装されてもよく、複数の装置に実装されてもよい。クライアント側システム２０ａを構成する登録情報生成装置１１０、認証情報生成装置１２０、回復用登録情報生成装置１４０、および回復用認証情報生成装置１６０の各種機能についても、同様である。なお登録情報生成装置１１０については、クライアント側システム２０ａに代えてサーバ側システム１０ａに含まれていてもよい。

【００４９】

次に、通常照合システム２および回復用照合システム３の詳細について説明するが、以下では、通常照合システム２で行われる処理および該処理に用いられる情報を指す場合、「通常」を省略することがある。なお、本実施形態２では、回復用登録情報および回復用照合情報が、共通の次元のベクトルで表されている場合を例にして説明する。また、本実施形態２において、生体情報は、指紋、虹彩、網膜、顔、血管（静脈）、掌紋、声紋、またはこれらの組み合わせから抽出されてもよい。生体情報は、上述した例以外の、生体を識別可能な他の情報から抽出されてもよい。

【００５０】

図３は、実施形態２にかかる通常照合システム２の概略構成図である。前述の通り、通常照合システム２は、登録情報生成装置１１０、認証情報生成装置１２０および認証情報検証装置１３０を有する。

【００５１】

（登録情報生成装置１１０）

登録情報生成装置１１０は、秘密情報入力部１１１と、登録情報生成部１１２とを備える。

【００５２】

秘密情報入力部１１１は、被登録者の秘密情報の入力を受け付ける。

【００５３】

登録情報生成部１１２は、秘密情報入力部１１１に入力された被登録者の秘密情報から登録情報と検証情報とを生成する。例えば、登録情報は、秘密情報を、秘密鍵を用いて暗号化した情報であり、検証情報は、通常用の秘密鍵に対応する公開鍵（検証鍵）であってよい。また例えば、登録情報は、秘密情報のナンス値のデータであり、検証情報は、秘密情報および登録情報に基づいて算出されるハッシュ値のデータであってもよい。

【００５４】

そして登録情報生成部１１２は、登録情報を、後述する認証情報生成装置１２０の登録情報受信部１２１に送信し、検証情報を後述する認証情報検証装置１３０の検証情報受信部１３１に送信する。

【００５５】

秘密情報入力部１１１と登録情報生成部１１２は、例えば、クライアント用プログラム、または、サーバ用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュー

タのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラム、または、サーバ用プログラムを読み込む。そしてＣＰＵが、そのプログラムに従って、通信インターフェースを用いて、秘密情報入力部１１１、登録情報生成部１１２として動作すればよい。

【００５６】

（認証情報生成装置１２０）

認証情報生成装置１２０は、登録情報受信部１２１と、登録情報記憶部１２２と、照合情報入力部１２３と、認証情報生成部１２４と、出力部１２５とを有する。

【００５７】

登録情報受信部１２１は、登録情報生成装置１１０から送信される登録情報と、認証情報検証装置１３０から送信されるＩＤとを受信し、登録情報記憶部１２２に記憶させる。

【００５８】

登録情報記憶部１２２は、登録情報とＩＤとを関連付けて記憶する装置である。

【００５９】

照合情報入力部１２３は、被認証者からの照合情報の入力を受け付ける。

【００６０】

認証情報生成部１２４は、登録情報と照合情報とから、検証に用いる認証情報を算出する。なお、本実施形態２の通常照合システム２には、クライアント側システム２０ａとサーバ側システム１０ａとの間の通信を盗聴する攻撃者によるクライアントへのなりすましが防止されるように、チャレンジ・レスポンス方式を導入している。したがって認証情報生成部１２４は、チャレンジ信号に対応するレスポンスとして、認証情報を算出する。しかし、通常照合システム２は、チャレンジ・レスポンス方式を導入していなくてもよい。

【００６１】

出力部１２５は、認証情報検証装置１３０から送信された、認証の結果を示す認証結果情報を受信する。また、出力部１２５は、受信された認証結果情報を、認証情報生成装置１２０の外部に出力する。

【００６２】

登録情報受信部１２１、照合情報入力部１２３、認証情報生成部１２４、出力部１２５は、例えば、クライアント用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラムを読み込む。そしてＣＰＵが、そのプログラムに従って、通信インターフェースを用いて、登録情報受信部１２１、照合情報入力部１２３、認証情報生成部１２４、出力部１２５として動作すればよい。

【００６３】

登録情報記憶部１２２は、例えば、コンピュータが備える記憶装置によって実現される。

【００６４】

（認証情報検証装置１３０）

認証情報検証装置１３０は、検証情報受信部１３１と、ＩＤ発行部１３２と、検証情報記憶部１３３と、判定部１３４と、チャレンジ生成部１３５とを有する。

【００６５】

検証情報受信部１３１は、登録情報生成装置１１０によって生成され、登録情報生成装置１１０から送信される検証情報を受信し、検証情報記憶部１３３に記憶させる。

【００６６】

ＩＤ発行部１３２は、被登録者ごとに識別番号（ＩＤ）を発行し、ＩＤを検証情報記憶部１３３に記憶させる。

【００６７】

検証情報記憶部１３３は、検証情報とＩＤとを関連付けて記憶する装置である。

【００６８】

判定部１３４は、認証情報生成装置１２０から受信した認証情報と、検証情報記憶部１

３３に記憶されている検証情報と、から、被登録者と被認証者とが一致するか否かを判定する。判定部１３４は、被登録者と被認証者とが一致する場合、「受理」という認証結果情報を、認証情報生成装置１２０に送信する。被登録者と被認証者が一致しない場合、「拒否」という認証結果情報を、認証情報生成装置１２０に送信する。

【００６９】

認証情報生成装置１２０は、「受理」という認証結果情報を受け取った場合、認証に成功したものとして、ＩＤに対応する認証後の処理を実行する。ただし、認証後の処理を実行する装置は、認証情報生成装置１２０に限定されず、「受理」という認証結果情報を得られたことを条件に、認証情報生成装置１２０以外の装置がＩＤに対応する認証後の処理を実行してもよい。

【００７０】

チャレンジ生成部１３５は、判定部１３４が認証情報を認証情報生成装置１２０から受け取る前に、チャレンジ信号を生成し、生成したチャレンジ信号を認証情報生成装置１２０に送信する。なお、チャレンジ・レスポンスは行われなくてもよく、この場合、認証情報検証装置１３０にチャレンジ生成部１３５が備えられていなくてもよいものとする。

【００７１】

検証情報受信部１３１、ＩＤ発行部１３２、判定部１３４、チャレンジ生成部１３５は、例えば、サーバ用プログラムに従って動作するコンピュータのＣＰＵ（Central Processing Unit）、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からサーバ用プログラムを読み込む。そしてＣＰＵが、そのプログラムに従って、通信インターフェースを用いて、検証情報受信部１３１、ＩＤ発行部１３２、判定部１３４、チャレンジ生成部１３５として動作すればよい。

【００７２】

検証情報記憶部１３３は、例えば、コンピュータが備える記憶装置によって実現される。

【００７３】

図４は、実施形態２にかかる回復用照合システム３の概略構成図である。前述の通り、回復用照合システム３は、回復用登録情報生成装置１４０と、回復用登録情報記憶装置１５０と、回復用認証情報生成装置１６０と、回復用認証情報検証装置１７０とを有する。

【００７４】

（回復用登録情報生成装置１４０）

回復用登録情報生成装置１４０は、回復用情報入力部１４１と、回復用ＩＤ入力部１４２と、鍵生成部１４３と、秘匿化部１４４とを備える。

【００７５】

回復用情報入力部１４１は、回復登録用入力情報に応じた入力デバイスであればよい。回復用情報入力部１４１は、生体情報から回復登録用入力情報となるベクトルを抽出し、そのベクトルを入力として受け付ける入力デバイスであってもよい。また、回復用情報入力部１４１は、回復登録用入力情報となるベクトルが直接入力される入力デバイスであってもよい。以下では、回復用情報入力部１４１に入力される被登録者の生体情報に該当するベクトルをＸと記す。

【００７６】

回復用ＩＤ入力部１４２は、被登録者の回復用ＩＤを取得する。

【００７７】

鍵生成部１４３は、秘密鍵ｓｋと、秘密鍵ｓｋに対応する公開鍵ｐｋとを生成する。鍵生成部１４３は、公開鍵ｐｋと回復用ＩＤを回復用認証情報検証装置１７０の鍵受信部１７１に送信する。

【００７８】

秘匿化部１４４は、生体情報Ｘと秘密鍵ｓｋとを用いて回復用登録情報を生成する。すなわち、秘匿化部１４４は、テンプレート生成手段として機能する。そして秘匿化部１４４は、回復用登録情報と回復用ＩＤを回復用登録情報記憶装置１５０の回復用登録情報記

憶部１５１ａに送信する。
【００７９】
回復用情報入力部１４１、回復用ＩＤ入力部１４２、鍵生成部１４３、秘匿化部１４４は、例えば、クライアント用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラムを読み込む。そして、ＣＰＵが、そのプログラムに従って、通信インターフェースを用いて、回復用情報入力部１４１、回復用ＩＤ入力部１４２、鍵生成部１４３、秘匿化部１４４として動作すればよい。
【００８０】
（回復用登録情報記憶装置１５０）
回復用登録情報記憶装置１５０は、回復用登録情報記憶部１５１ａと、回復情報生成部１５２ａと、マスク生成部１５３ａとを備える。
【００８１】
回復用登録情報記憶部１５１ａは、回復用登録情報生成装置１４０から回復用登録情報と回復用ＩＤとを受信し、これらを記憶する。つまり、回復用登録情報記憶部１５１ａは、実施形態１のテンプレート記憶部１５１に対応する。
【００８２】
回復情報生成部１５２ａは、回復用認証情報生成装置１６０から回復用ＩＤを受信し、回復用登録情報記憶部１５１ａから回復用ＩＤに対応する回復用登録情報を取得する。そして回復情報生成部１５２ａは、回復用登録情報と、マスク生成部１５３ａで生成した乱数マスクＲ＿Ｍと、から回復情報を生成し、回復情報を回復用認証情報生成装置１６０の回復情報受信部１６３に送信する。つまり、回復情報生成部１５２ａは、実施形態１の秘匿化テンプレート生成部１５２に対応する。
【００８３】
マスク生成部１５３ａは、乱数マスクＲ＿Ｍを生成する。マスク生成部１５３ａは、実施形態１の乱数生成部１５３に対応する。
【００８４】
回復用登録情報記憶部１５１ａ、回復情報生成部１５２ａ、マスク生成部１５３ａは、例えば、サーバ用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からサーバ用プログラムを読み込。そしてＣＰＵは、そのプログラムに従って、通信インターフェースを用いて、回復用登録情報記憶部１５１ａ、回復情報生成部１５２ａ、マスク生成部１５３ａとして動作すればよい。
【００８５】
回復用登録情報記憶部１５１ａは、例えば、コンピュータが備える記憶装置によって実現される。
【００８６】
（回復用認証情報生成装置１６０）
回復用認証情報生成装置１６０は、回復用照合情報入力部１６１と、回復用ＩＤ入力部１６２と、回復情報受信部１６３と、回復用認証情報生成部１６４と、出力部１６５とを備える。
【００８７】
回復用照合情報入力部１６１は、回復用照合情報に応じた入力デバイスであればよい。また、回復用照合情報入力部１６１は、回復用照合情報となるベクトルが直接、入力される入力デバイスであってもよい。回復用照合情報入力部１６１に入力される被認証者の生体情報に該当するベクトルをＹと記す。
【００８８】
回復用ＩＤ入力部１６２は、回復用ＩＤを取得し、回復用ＩＤを回復用登録情報記憶装置１５０の回復情報生成部１５２ａに送信する。

【００８９】
回復情報受信部１６３は、回復用登録情報記憶装置１５０から回復情報を受信する。
【００９０】
回復用認証情報生成部１６４は、被認証者の生体情報Ｙと、回復情報とから、生体情報Ｘと生体情報Ｙとの近似度を示す値である指標、を秘匿化したデータ（以下、回復用認証情報と記す。）を生成する。回復用認証情報は、回復用照合情報と、回復用登録情報と、の内積に基づいて定められてよい。なお回復情報は、被登録者の生体情報Ｘを秘匿化することで得られた回復用登録情報に乱数マスクＲ＿Ｍを加えた値である。回復用認証情報生成部１６４は、回復情報の秘匿化の解除をすることなく、回復用認証情報を生成する。
【００９１】
ここで、本実施形態２の回復用照合システム３には、クライアント側システム２０ａとサーバ側システム１０ａとの間の通信を盗聴する攻撃者によるクライアントへのなりすましが防止されるように、チャレンジ・レスポンス方式が導入されている。具体的には、回復用認証情報検証装置１７０が認証ごとに毎回異なるチャレンジ信号を回復用認証情報生成装置１６０に送信する。そして回復用認証情報生成装置１６０は、チャレンジ信号に対応し、かつ、回復情報と回復用照合情報との近似度を含むレスポンスを計算させることによって、レスポンスの値が認証ごとに変更される。これにより、攻撃者が盗聴によりレスポンスの値を取得したとしても、盗聴された値は次の回復用認証において使用不能であり、攻撃者は別のチャレンジに対応するレスポンスを生成できないため、クライアントへのなりすましが防止される。
【００９２】
したがって回復用認証情報生成部１６４は、生体情報Ｙおよび回復情報に加えて、回復用認証情報検証装置１７０から受け取るチャレンジ信号に基づいて、チャレンジ信号に対応するレスポンスとして、回復用認証情報を生成する。
【００９３】
出力部１６５は、回復用認証情報検証装置１７０から送信された、生体認証の結果を示す認証結果情報を受信する。また、出力部１６５は、受信された認証結果情報を回復用認証情報生成装置１６０の外部に出力する。
【００９４】
回復情報受信部１６３、回復用認証情報生成部１６４、出力部１６５は、クライアント用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラムを読み込む。そしてＣＰＵは、そのプログラムに従って、通信インターフェースを用いて、回復情報受信部１６３、回復用認証情報生成部１６４、出力部１６５として動作すればよい。
【００９５】
回復用照合情報入力部１６１は、クライアント用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータのインターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラムを読み込み、そのプログラムに従って、インターフェースを用いて、回復用照合情報入力部１６１として動作すればよい。
【００９６】
回復用ＩＤ入力部１６２は、クライアント用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータのインターフェースと通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からクライアント用プログラムを読み込む。そしてＣＰＵは、そのプログラムに従って、インターフェースと通信インターフェースを用いて、回復用ＩＤ入力部１６２として動作すればよい。
【００９７】
（回復用認証情報検証装置１７０）

回復用認証情報検証装置１７０は、鍵受信部１７１と、鍵記憶部１７２と、回復用鍵生成部１７３と、受理範囲記憶部１７４と、判定部１７５ａと、チャレンジ生成部１７６とを有する。

【００９８】

鍵受信部１７１は、回復用登録情報生成装置１４０から公開鍵ｐｋと回復用ＩＤとを受信する。

【００９９】

鍵記憶部１７２は、公開鍵ｐｋと、回復用ＩＤとを関連付けて記憶する。

【０１００】

回復用鍵生成部１７３は、回復用認証情報生成装置１６０から受信した回復用ＩＤに対応する公開鍵ｐｋと回復用登録情報記憶装置１５０から受信した乱数マスクＲ＿Ｍとを用いて、回復用検証鍵ｐｋ’を生成する。

【０１０１】

判定部１７５ａは、回復用認証情報生成装置１６０から受信した回復用認証情報が、予め定められた受理範囲内の値であるか否かを、回復用検証鍵ｐｋ’を用いて判定することによって、被登録者と被認証者とが一致するか否かを判定する。なお、予め定められた受理範囲は、受理範囲記憶部１７４に記憶されている。

【０１０２】

すなわち、判定部１７５ａは、回復用認証情報が、受理範囲内の値であるならば、被登録者と被認証者とが一致すると判定する。被登録者と被認証者とが一致することは、回復用照合情報と回復用登録情報とが対応することに相当する。また、判定部１７５ａは、回復用認証情報が、受理範囲内の値でないならば、被登録者と被認証者とが一致しないと判定する。つまり、判定部１７５ａは、実施形態１の判定部１７５に対応する。

【０１０３】

判定部１７５ａは、被登録者と被認証者が一致する場合、「受理」という認証結果情報を、回復用認証情報生成装置１６０に送信する。被登録者と被認証者が一致しない場合、「拒否」という認証結果情報を、回復用認証情報生成装置１６０に送信する。

回復用認証情報生成装置１６０は、「受理」という認証結果情報を受け取った場合に、認証に成功したものとして、回復用ＩＤに対応する認証後の処理を実行する。ただし、認証後の処理を実行する装置は、回復用認証情報生成装置１６０に限定されず、「受理」という認証結果情報を得られたことを条件に、回復用認証情報生成装置１６０以外の装置が回復用ＩＤに対応する認証後の処理を実行してもよい。

【０１０４】

チャレンジ生成部１７６は、認証ごとに、すなわち回復用照合情報ごとに、チャレンジ信号を生成する。チャレンジ生成部１７６は、判定部１７５ａが回復用認証情報を回復用認証情報生成装置１６０から受け取る前に、生成したチャレンジ信号を回復用認証情報生成装置１６０に送信する。

【０１０５】

鍵受信部１７１、回復用鍵生成部１７３、判定部１７５ａ、チャレンジ生成部１７６は、例えば、サーバ用プログラムに従って動作するコンピュータのＣＰＵ、および、そのコンピュータの通信インターフェースによって実現される。例えば、ＣＰＵが、コンピュータのプログラム記憶装置等のプログラム記録媒体からサーバ用プログラムを読み込む。そして、ＣＰＵは、そのプログラムに従って、通信インターフェースを用いて、鍵受信部１７１、回復用鍵生成部１７３、判定部１７５ａ、チャレンジ生成部１７６として動作すればよい。

【０１０６】

鍵記憶部１７２、受理範囲記憶部１７４は、例えば、コンピュータが備える記憶装置によって実現される。

【０１０７】

次に、図５～６を用いて、通常照合システム２の処理について説明する。

図５は、実施形態２にかかる通常照合システム２の登録処理の手順を示すシーケンス図である。なお、すでに説明した事項については、詳細な説明を省略する。

【０１０８】

まず、登録情報生成装置１１０の秘密情報入力部１１１は、被登録者による秘密情報の入力を受け付け、秘密情報を取得する（ステップＳ１０）。次いで、登録情報生成装置１１０の登録情報生成部１１２は、秘密情報から登録情報と検証情報とを生成する（ステップＳ１２）。次いで、登録情報生成装置１１０の登録情報生成部１１２は、検証情報を認証情報検証装置１３０に送信する（ステップＳ１３）。

【０１０９】

認証情報検証装置１３０の検証情報受信部１３１は、検証情報を受信したことに応じて、検証情報を検証情報記憶部１３３に格納する（ステップＳ１４）。

【０１１０】

また、登録情報生成装置１１０の登録情報生成部１１２は、登録情報を認証情報生成装置１２０の登録情報受信部１２１に送信する。（ステップＳ１６）。

【０１１１】

認証情報生成装置１２０の登録情報受信部１２１は、登録情報を受信したことに応じて、登録情報を登録情報記憶部１２２に格納する（ステップＳ１６）。

【０１１２】

次いで、認証情報検証装置１３０のＩＤ発行部１３２は、ＩＤを発行する（ステップＳ１７）。そして、ＩＤ発行部１３２は、ＩＤを認証情報生成装置１２０の登録情報受信部１２１に送信する（ステップＳ１８）。

【０１１３】

次いで、認証情報生成装置１２０の登録情報受信部１２１はＩＤを受信したことに応じて、登録情報記憶部１２２にＩＤを登録情報と関連付けて格納する（ステップＳ１９）。

【０１１４】

また、認証情報検証装置１３０の検証情報記憶部１３３は、ＩＤを登録情報と関連付けて記憶する（ステップＳ２０）。

【０１１５】

図６は、実施形態２にかかる通常照合システム２の認証処理の手順を示すシーケンス図である。

【０１１６】

まず、認証情報生成装置１２０の照合情報入力部１２３は、被認証者による照合情報の入力を受け付け、照合情報を取得する（ステップＳ３０）。次いで、認証情報生成装置１２０は、登録情報記憶部１２２に記憶されているＩＤを、認証情報検証装置１３０の判定部１３４に送信する（ステップＳ３１）。

【０１１７】

認証情報検証装置１３０の判定部１３４は、ＩＤを受信したことに応じて、ＩＤに対応する検証情報を、検証情報記憶部１３３から取得する（ステップＳ３２）。次いで、認証情報検証装置１３０のチャレンジ生成部１３５は、チャレンジを生成する（ステップＳ３３）。次いで、チャレンジ生成部１３５は、チャレンジを認証情報生成装置１２０に送信する（ステップＳ３４）。

【０１１８】

チャレンジを受信した認証情報生成装置１２０の認証情報生成部１２４は、登録情報記憶部１２２から登録情報を取得する（ステップＳ３５）。次いで、認証情報生成部１２４は、レスポンスとして認証情報を生成する（ステップＳ３６）。次いで、認証情報生成部１２４は、認証情報を認証情報検証装置１３０に送信する（ステップＳ３７）。

【０１１９】

認証情報検証装置１３０の判定部１３４は、認証情報を受信したことに応じて、認証情報と検証情報とから照合判定を行う（ステップＳ３８）。次いで、判定部１３４は、照合結果を示す認証結果情報を、認証情報生成装置１２０に送信する（ステップＳ３９）。

【０１２０】
認証情報生成装置１２０の出力部１２５は、認証結果情報を受信したことに応じて、認証結果を出力する（ステップＳ４０）。
【０１２１】
次に、図７～８を用いて、回復用照合システム３の処理について説明する。
図７は、実施形態２にかかる回復用照合システム３の回復用登録処理の手順を示すシーケンス図である。
【０１２２】
まず、回復用登録情報生成装置１４０の回復用情報入力部１４１は、被登録者による被登録者の生体情報Ｘの入力を受け付け、生体情報Ｘを取得する（ステップＳ５０）。次いで、回復用登録情報生成装置１４０の回復用ＩＤ入力部１４２は、被登録者による回復用ＩＤの入力を受け付け、回復用ＩＤを取得する（ステップＳ５１）。回復用登録情報生成装置１４０は、回復用ＩＤを、回復用登録情報記憶装置１５０の回復用登録情報記憶部１５１ａおよび回復用認証情報検証装置１７０の鍵受信部１７１に送信する（ステップＳ５２）。
【０１２３】
回復用登録情報記憶装置１５０および回復用認証情報検証装置１７０はそれぞれ、回復用ＩＤを受信したことに応じて、回復用登録情報記憶部１５１ａおよび鍵記憶部１７２に回復用ＩＤを格納する（ステップＳ５３）。
【０１２４】
一方、回復用登録情報生成装置１４０の鍵生成部１４３は、乱数を生成する（ステップＳ５４）。そして鍵生成部１４３は、乱数に基づいて、秘密鍵ｓｋと公開鍵ｐｋとを生成する（ステップＳ５５）。次いで、回復用登録情報生成装置１４０の秘匿化部１４４は、生体情報Ｘおよび秘密鍵ｓｋから回復用登録情報を生成する（ステップＳ５６）。回復用登録情報は、テンプレートとも呼ばれる。鍵生成部１４３は、公開鍵ｐｋを回復用認証情報検証装置１７０の鍵受信部１７１に送信する（ステップＳ５７）。
【０１２５】
回復用認証情報検証装置１７０の鍵受信部１７１は、公開鍵ｐｋを受信したことに応じて、公開鍵ｐｋを鍵記憶部１７２に格納する（ステップＳ５８）。
【０１２６】
一方、回復用登録情報生成装置１４０の秘匿化部１４４は、回復用登録情報を回復用登録情報記憶装置１５０に送信する（ステップＳ５９）。
【０１２７】
回復用登録情報記憶装置１５０は、回復用登録情報を受信したことに応じて、回復用登録情報記憶部１５１ａに回復用登録情報を格納する（ステップＳ６０）。
【０１２８】
図８は、実施形態２にかかる回復用照合システム３の回復用認証処理の手順を示すシーケンス図である。
【０１２９】
まず、回復用認証情報生成装置１６０の回復用ＩＤ入力部１６２は、被認証者による回復用ＩＤの入力を受け付け、回復用ＩＤを取得する（ステップＳ７０）。次いで、回復用認証情報生成装置１６０の回復用照合情報入力部１６１は、被認証者による被認証者の生体情報Ｙの入力を受け付け、生体情報Ｙを取得する（ステップＳ７１）。次いで、回復用ＩＤ入力部１６２は、回復用ＩＤを回復用登録情報記憶装置１５０に送信する（ステップＳ７２）。
【０１３０】
回復用登録情報記憶装置１５０の回復情報生成部１５２ａは、回復用ＩＤを受信したことに応じて、回復用ＩＤに対応する回復用登録情報を、回復用登録情報記憶部１５１ａから取得する（ステップＳ７３）。次いで、回復用登録情報記憶装置１５０のマスク生成部１５３ａは、乱数マスクを生成する（ステップＳ７４）。マスク生成部１５３ａは、回復

用ＩＤと乱数マスクとを、回復用認証情報検証装置１７０に送信する（ステップＳ７５、７６）。これにより、回復用認証情報検証装置１７０の回復用鍵生成部１７３は、回復用ＩＤと乱数マスクとを受信する。

【０１３１】

次いで、回復用登録情報記憶装置１５０の回復情報生成部１５２ａは、回復用登録情報および乱数マスクから回復情報を生成する（ステップＳ７７）。回復情報は、秘匿化テンプレートとも呼ばれる。回復情報生成部１５２ａは、回復情報を回復用認証情報生成装置１６０に送信する（ステップＳ７８）。これにより回復用認証情報生成装置１６０の回復情報受信部１６３は、回復情報を受信する。

【０１３２】

次いで、回復用認証情報検証装置１７０の回復用鍵生成部１７３は、鍵記憶部１７２から回復用ＩＤに対応する公開鍵ｐｋを取得する（ステップＳ７９）。次いで、回復用鍵生成部１７３は、公開鍵ｐｋと乱数マスクＲ＿Ｍとを用いて、回復用検証鍵ｐｋ’を生成する（ステップＳ８０）。次いで、回復用認証情報検証装置１７０のチャレンジ生成部１７６は、チャレンジを生成し（ステップＳ８１）、チャレンジを回復用認証情報生成装置１６０の回復用認証情報生成部１６４に送信する（ステップＳ８２）。

【０１３３】

回復用認証情報生成装置１６０の回復用認証情報生成部１６４は、チャレンジを受信したことに応じて、生体情報Ｙ、回復情報およびチャレンジから、回復用認証情報を生成する（ステップＳ８３）。次いで、回復用認証情報生成部１６４は、回復用認証情報を回復用認証情報検証装置１７０の判定部１７５ａに送信する（ステップＳ８４）。

【０１３４】

回復用認証情報検証装置１７０の判定部１７５ａは、回復用認証情報を受信したことに応じて、回復用認証情報の中に受理範囲に含まれている指標があるか否かの照合を、回復用検証鍵ｐｋ’とチャレンジとを用いて行う（ステップＳ８５）。また、判定部１７５ａは、照合結果を示す認証結果情報を、回復用認証情報生成装置１６０の出力部１６５に送信する（ステップＳ８６）。

【０１３５】

次いで、回復用認証情報生成装置１６０の出力部１６５は、認証結果情報を受信したことに応じて、認証結果を出力する（ステップＳ８７）。その後、認証（照合）に成功していた場合、登録情報を回復させる処理が実行される。

【０１３６】

以下、本実施形態２の回復用照合システム３の処理の具体例について説明する。以下の説明では、生体情報Ｘおよび生体情報Ｙは、いずれもｎ次元のベクトルであるものとする。そして、Ｘの各要素は、Ｘ＝（ｘ＿１，ｘ＿２，…，ｘ＿ｎ）と表され、Ｙの各要素は、Ｙ＝（ｙ＿１，ｙ＿２，…，ｙ＿ｎ）と表されるものとする。また、記号ｉで１，２，…，ｎを表すものとする。例えば、｛ｕ＿ｉ｝＝ｕ＿１，ｕ＿２，…，ｕ＿ｎである。

【０１３７】

（具体例）

本具体例では、Ｓｃｈｎｏｒｒ署名が使用される場合の具体的な回復用登録処理および回復用認証処理を説明する。本具体例では、生体情報Ｘと生体情報Ｙとの近さを示す指標が、生体情報Ｘと生体情報Ｙとの内積である場合を考える。生体情報Ｘと生体情報Ｙとの内積＜Ｘ，Ｙ＞は、Σ（ｘ＿ｉ・ｙ＿ｉ）である。以下では、指標が内積である場合の処理の一例を示す。

【０１３８】

また、本具体例では、Ｓｃｈｎｏｒｒ署名が用いられる。Ｓｃｈｎｏｒｒ署名では、秘密鍵ｓｋと公開鍵ｐｋ＝ｇ＾ｓｋとの組が生成される。なお、ｓｋ∈Ｚ＿ｑ（Ｚ＿ｑ＝｛０，１，…，ｑ－１｝、ｑは素数）である（Ｚは整数全体の集合を表す記号）。また、ｇは、位数ｑの群Ｇの生成元である。すなわち、Ｇ＝｛ｇ＿０，ｇ＿１，…，ｇ＿ｑ－１｝である。Ｚ＿ｑ、ｇ、およびＧは、全ての装置との間で共有されている。

【０１３９】
さらに、回復用認証情報検証装置１７０には、受理範囲Θ＝｛θ＿１，…，θ＿ｍ｝が与えられている。回復用認証情報検証装置１７０の受理範囲記憶部１７４は、Θ’＝｛ｇ＾(θ＿１)，…，ｇ＾(θ＿ｍ)｝を記憶している。なお、Θ’は、Θの各値を指数とするｇのべき乗の集合である。
【０１４０】
なお、本具体例の通常照合システム２による登録処理と認証処理には、ＩＤ・パスワード認証等、一般的な認証が行われているものとし、説明を省略する。
以下、Ｓｃｈｎｏｒｒ署名が使用される場合の回復用照合システム３による具体的な回復用登録処理を説明する。
【０１４１】
最初に、被登録者の生体情報Ｘが、回復用情報入力部１４１に入力される。次いで、回復用ＩＤが回復用ＩＤ入力部１４２に入力される。次いで、鍵生成部１４３は、以下の式（１）～（４）のように乱数を生成する。
【０１４２】
Ｒ＿１←＾ＲＺ＿ｑ　・・・（１）
Ｒ＿２←＾ＲＺ＿ｑ　・・・（２）
Ｒ＿３←＾ＲＺ＿ｑ　・・・（３）
（ｒ＿１，ｒ＿２，…，ｒ＿ｎ）←＾ＲＺ＿ｑ　・・・（４）
【０１４３】
鍵生成部１４３は、Ｒ＿３を秘密鍵とみなし、秘密鍵に基づいて、公開鍵ｇ＾（Ｒ＿３）を生成する。また、鍵生成部１４３は、｛ｒ＿ｉ｝と，乱数Ｒ＿１，Ｒ＿２とを、秘匿化鍵とみなす。秘匿化鍵は、被登録者ごと、すなわち生体情報Ｘごとに固有の固有鍵である。
【０１４４】
鍵生成部１４３は、秘密鍵Ｒ＿３と秘匿化鍵｛ｒ＿ｉ｝，Ｒ＿１，Ｒ＿２とを、秘匿化部１４４に入力する。また、鍵生成部１４３は、回復用ＩＤと、公開鍵ｇ＾（Ｒ＿３）と、秘匿化鍵Ｒ＿１，Ｒ＿２とを、回復用認証情報検証装置１７０の鍵受信部１７１に送信する。
【０１４５】
次いで、鍵記憶部１７２は、受信した回復用ＩＤと、公開鍵と、秘匿化鍵のＲ＿１，Ｒ＿２とを関連付けて記憶する。
【０１４６】
次いで、回復用登録情報生成装置１４０の秘匿化部１４４は、入力された秘密鍵および秘匿化鍵と、生体情報Ｘとを基に、ｉ＝１，２，…，ｎに対して、Ｒ＿１・ｘ＿ｉ＋Ｒ＿２・ｒ＿ｉ＋Ｒ＿３と、ｇ＾（ｒ＿ｉ）とを生成する。以下、テンプレートを｛Ｒ＿１・ｘ＿ｉ＋Ｒ＿２・ｒ＿ｉ＋Ｒ３｝、｛ｇ＾（ｒ＿ｉ)｝とする。
【０１４７】
秘匿化部１４４は、回復用ＩＤおよびテンプレートを、回復用登録情報記憶装置１５０の回復用登録情報記憶部１５１ａに送信する。そして、回復用登録情報記憶部１５１ａは、回復用ＩＤとテンプレートを記憶し、回復用登録処理を終了する。
【０１４８】
なおテンプレートを保持する回復用登録情報記憶装置１５０は、セキュリティリスク軽減のため、秘匿化鍵および公開鍵を保持していない。
【０１４９】
次に、Ｓｃｈｎｏｒｒ署名が使用される場合の回復用照合システム３による具体的な回復用認証処理を説明する。
【０１５０】
最初に、回復用認証情報生成装置１６０は、回復用ＩＤを回復用登録情報記憶装置１５０に送信する。

【０１５１】
次いで、回復情報生成部１５２ａは、回復用登録情報記憶部１５１ａから回復用ＩＤに対応するテンプレートを取得する。
【０１５２】
ここで回復情報生成部１５２ａは、｛ｇ＾ｒ＿ｉ｝を秘匿化するために、｛ｇ＾ｒ＿ｉ｝を回復用認証情報検証装置１７０に送信する。
【０１５３】
次いで、回復用認証情報検証装置１７０は、以下の式（５）のように乱数を生成する。
【０１５４】
（ｒ’＿１，ｒ’＿２，・・・，ｒ’＿ｎ）←＾ＲＺ＿ｑ　・・・（５）
【０１５５】
次いで、回復用認証情報検証装置１７０は｛ｇ＾（ｒ＿ｉ＋ｒ’＿ｉ）｝と｛ｒ’＿ｉ・Ｒ＿２｝とを計算し、回復用登録情報記憶装置１５０に送信する。
【０１５６】
次いで、回復用登録情報記憶装置１５０の回復情報生成部１５２ａは、｛ｇ＾（ｒ＿ｉ＋ｒ’＿ｉ）｝と｛ｒ’＿ｉ・Ｒ＿２｝とを受信する。
【０１５７】
次いで、マスク生成部１５３ａは、以下の式（６）～（８）のように乱数を生成する。
【０１５８】
Ｒ’＿１←＾ＲＺ＿ｑ　・・・（６）
Ｒ’＿２←＾ＲＺ＿ｑ　・・・（７）
Ｒ’＿３←＾ＲＺ＿ｑ　・・・（８）
【０１５９】
次いで、回復情報生成部１５２ａは、回復情報として、｛Ｒ’＿１・Ｒ＿１・ｘ＿ｉ＋Ｒ’＿１・Ｒ＿２・（ｒ＿ｉ＋ｒ’＿ｉ）＋Ｒ’＿１・Ｒ＿３＋Ｒ’＿３｝と、｛ｇ＾（ｒ＿ｉ＋ｒ’＿ｉ）・（１／Ｒ’＿２）｝とを生成する。
【０１６０】
次いで、マスク生成部１５３ａは、マスクＲ’＿１、Ｒ’＿２、Ｒ’＿３を、回復用認証情報検証装置１７０の回復用鍵生成部１７３に送信する。これにより、回復用鍵生成部１７３は、マスクＲ’＿１、Ｒ’＿２、Ｒ’＿３を受信する。
【０１６１】
次いで、回復用登録情報記憶装置１５０の回復情報生成部１５２ａは、回復情報を回復用認証情報生成装置１６０の回復情報受信部１６３に送信する。これにより、回復用認証情報生成装置１６０の回復情報受信部１６３は、回復情報を受信する。
【０１６２】
次いで、被認証者の生体情報Ｙが、回復用照合情報入力部１６１に入力される。回復用認証情報生成部１６４は、回復用照合情報入力部１６１から生体情報Ｙを取得する。
【０１６３】
次いで、回復用認証情報生成部１６４は、σ＿１＝ｇ＾（Σ（ｒ＿ｉ＋ｒ’＿ｉ）・ｙ＿ｉ）・（１／Ｒ’＿２）を計算する。その後、回復用認証情報生成部１６４は、回復用ＩＤとσ＿１とを、回復用認証情報検証装置１７０の判定部１７５ａに送信する。
【０１６４】
次いで、回復用ＩＤおよびσ＿１を受信した回復用認証情報検証装置１７０は、チャレンジ生成部１７６において、Ｍ，Ｒ←＾ＲＺ＿ｑを生成する。そして回復用認証情報検証装置１７０は、鍵記憶部１７２に記憶されている公開鍵ｇ＾（Ｒ＿３）とマスクＲ’＿１、Ｒ’＿３とを用いて、ｇ＾（Ｒ・（Ｒ’＿１・Ｒ＿３＋Ｒ’＿３））を計算する。その後、チャレンジとしてＭ，ｇ＾（Ｒ・（Ｒ’＿１・Ｒ＿３＋Ｒ’＿３））を回復用認証情報生成装置１６０の回復用認証情報生成部１６４に送信する。
【０１６５】
次いで、回復用認証情報生成部１６４は、Ｓ＝Ｈ（Ｍ，ｇ＾ｒ）を算出する。なお、Ｈ

は暗号学的ハッシュ関数である。次いで、回復用認証情報生成部１６４は、入力された生体情報Ｙとテンプレートとを基に、以下の各値を、式（９）～（１１）から算出する。

【０１６６】

Ａ＝Σ＿ｉ（Ｒ’＿１・Ｒ＿１・ｘ＿ｉ＋Ｒ’＿１・Ｒ＿２・（ｒ＿ｉ＋ｒ’＿ｉ）＋Ｒ’＿１・Ｒ３＋Ｒ’＿３）・ｙ＿ｉ　・・・（９）

σ＿２＝ｒ－Ａ・Ｓ　・・・（１０）

σ＿３＝ｇ＾（Ｒ・（Ｒ’＿１・Ｒ＿３＋Ｒ’＿３）・ｙ＿ｉ）　・・・（１１）

【０１６７】

各値を算出した後、回復用認証情報生成部１６４は、生体情報Ｘと生体情報Ｙとの内積を含むレスポンスとして、（Ｓ，σ＿２，σ＿３）を回復用認証情報検証装置１７０の判定部１７５ａに送信する。（Ｓ，σ＿２，σ＿３）は、Ａを秘密鍵とするＳｃｈｎｏｒｒ署名に相当する。

【０１６８】

判定部１７５ａは、回復用認証情報生成部１６４からレスポンスを受信する。判定部１７５ａは、鍵記憶部１７２に回復用ＩＤとともに記憶されている公開鍵ｇ＾（Ｒ＿３）と、秘匿化鍵Ｒ＿１，Ｒ＿２とマスクＲ’＿１，Ｒ’＿２を用いて、デジタル署名Ｓ，σ＿２，σ＿３を検証する。具体的には、以下の式（１２）を計算する。

【０１６９】

ｖ＝［｛ｇ＾（σ＿２）｝・｛（σ＿３）＾（Ｓ・Ｒ）｝・｛（σ＿１）＾（Ｓ・Ｒ’＿１・Ｒ＿２・Ｒ’＿２）｝・（ｇ＾（－ｒ））］＾（－１／Ｒ＿１・Ｒ’＿１）　・・・（１２）

【０１７０】

判定部１７５ａは、計算されたｖがΘ’に含まれるか否かを確認する。判定部１７５ａは、Θ’に含まれない場合、「認証失敗」を示す認証結果情報を生成する。また、判定部１７５ａは、Θ’に含まれる場合、「認証成功」を示す認証結果情報を生成する。

【０１７１】

次いで、判定部１７５ａは、生成された認証結果情報を回復用認証情報生成装置１６０の出力部１６５に送信する。次いで、認証結果情報を受信した出力部１６５は、認証結果情報を出力する。認証成功した場合、被認証者のＩＤへのアクセス権限を回復し、被認証者は、通常登録処理を実行する。

【０１７２】

なお、本具体例では、本具体例ではＳｃｈｎｏｒｒ署名が用いられているが、ＤＳＡ署名等の他の暗号学的に安全なデジタル署名方式が用いられてもよい。

【０１７３】

このように、本具体例では、回復用認証情報検証装置１７０の鍵記憶部１７２は、生体情報Ｘごとに固有の秘匿化鍵と公開鍵とを記憶する。そして回復用登録情報記憶装置１５０のマスク生成部１５３ａは、クライアントの要求に応じて、第１乱数を発生する第１乱数生成手段として機能する。また回復用認証情報検証装置１７０は、クライアントの要求に応じて、第２乱数を発生する第２乱数生成手段として機能し、第２乱数を用いて秘匿化鍵をさらに秘匿化した鍵（秘匿化固有鍵）を生成する。回復用登録情報記憶装置１５０の回復情報生成部１５２ａは、第１乱数と、秘匿化固有鍵とを用いて、テンプレートを秘匿化した回復情報を生成する。そして回復用認証情報検証装置１７０の判定部１７５ａは、公開鍵、第１乱数および固有鍵を回復用検証鍵として用いて、レスポンスに含まれる秘匿化指標を復号する。

【０１７４】

このような構成をとることにより、秘匿化鍵の記憶場所とテンプレートの記憶場所とを、別々に分けて管理できる。したがって、セキュリティリスクが軽減される。

【０１７５】

本実施形態２およびその具体例において、照合システム１は、テンプレートを保護したまま照合できる生体認証をアカウントリカバリに用いている。本実施形態２による生体認

証は、身分証明書で身元確認を行う方法よりも利便性が高く、リカバリーコードで身元確認を行う方法よりも安全性が高い。そのため照合システム１は、アカウントリカバリ時も含めて、サーバ側システム１０ａの管理コスト低減や、生体情報の漏洩リスクが小さいシステムとなる。

【０１７６】

なお、照合システム１は、回復用登録処理および回復用認証処理のみを実行してもよい。例えば、回復用登録情報生成装置１４０と、回復用登録情報記憶装置１５０と、回復用認証情報生成装置１６０と、回復用認証情報検証装置１７０とから、照合システム１が構成されてもよい。

【０１７７】

図９は、上記の実施形態やその具体例におけるクライアントやサーバに係るコンピュータの構成例を示す概略ブロック図である。以下、図９を参照して説明するが、クライアントとして用いられるコンピュータと、サーバとして用いられるコンピュータとは、別々のコンピュータである。

【０１７８】

コンピュータ１０００は、ＣＰＵ１００１と、主記憶装置１００２と、補助記憶装置１００３と、インターフェース１００４と、通信インターフェース１００５とを備える。

【０１７９】

クライアントを実現するコンピュータ１０００の動作は、クライアント用プログラムの形式で補助記憶装置１００３に記憶されている。ＣＰＵ１００１は、そのクライアント用プログラムを補助記憶装置１００３から読み出して主記憶装置１００２に展開し、そのクライアント用プログラムに従って、上記の実施形態やその具体例で説明したクライアントの動作を実行する。

【０１８０】

サーバを実現するコンピュータ１０００の動作は、サーバ用プログラムの形式で補助記憶装置１００３に記憶されている。ＣＰＵ１００１は、そのサーバ用プログラムを補助記憶装置１００３から読み出して主記憶装置１００２に展開し、そのサーバ用プログラムに従って、上記の実施形態やその具体例で説明したサーバの動作を実行する。

【０１８１】

補助記憶装置１００３は、一時的でない有形の媒体の例である。一時的でない有形の媒体の他の例として、インターフェース１００４を介して接続される磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ（Compact Disk Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disk Read Only Memory）、半導体メモリ等が挙げられる。また、プログラムが通信回線によってコンピュータ１０００に配信される場合、配信を受けたコンピュータ１０００がそのプログラムを主記憶装置１００２に展開し、そのプログラムに従って動作してもよい。

【０１８２】

また、クライアントの各構成要素の一部または全部は、汎用または専用の回路（circuitry）、プロセッサ等やこれらの組み合わせによって実現されてもよい。これらは、単一のチップによって構成されてもよいし、バスを介して接続される複数のチップによって構成されてもよい。各構成要素の一部または全部は、上述した回路等とプログラムとの組み合わせによって実現されてもよい。この点は、サーバに関しても同様である。

【０１８３】

上記の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うるが、以下には限られない。

（付記１）

被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶するテンプレート記憶手段と、

クライアントの要求に応じて、乱数を生成する乱数生成手段と、

前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記

秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成手段と、
判定手段と
を備え、
前記判定手段は、
登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得し、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う
回復用検証システム。
（付記２）
前記判定手段は、生成された前記指標が所定範囲内の値を示す場合、前記照合情報についての認証を受理する
付記１に記載の回復用検証システム。
（付記３）
前記照合情報ごとにチャレンジ信号を生成して前記クライアントに送信するチャレンジ生成手段をさらに有し、
前記クライアントにおいて、前記チャレンジ信号に対応するレスポンスとして前記秘匿化指標を算出するように構成されている
付記１または２に記載の回復用検証システム。
（付記４）
前記登録用入力情報および前記照合情報は、何れもベクトルによって表される、
付記１から３のいずれか一項に記載の回復用検証システム。
（付記５）
前記秘匿化指標は、前記照合情報と、前記秘匿化テンプレートと、の内積に基づいて定められる
付記１から４のいずれか一項に記載の回復用検証システム。
（付記６）
登録用入力情報ごとに固有の固有鍵を記憶する鍵記憶手段を備え、
前記乱数生成手段は、
前記クライアントの前記要求に応じて、第１乱数を発生する第１乱数生成手段と、
前記クライアントの前記要求に応じて、第２乱数を発生する第２乱数生成手段と
を有し、
前記秘匿化テンプレート生成手段は、前記第１乱数と、前記第２乱数を用いて前記固有鍵を秘匿化した秘匿化固有鍵と、を用いて、前記秘匿化テンプレートを生成し、
前記判定部は、前記公開鍵、前記第１乱数および前記固有鍵を用いて、前記秘匿化指標を復号した指標を生成する
付記１から５のいずれか一項に記載の回復用検証システム。
（付記７）
クライアントと、
被登録者の通常登録用入力情報の照合のために入力される通常照合情報、についての認証を行う通常検証システムと、
前記被登録者の前記通常登録用入力情報に関連するアカウントを回復するための回復用検証システムと
を備える照合システムであって、
前記回復用検証システムは、
前記被登録者の生体情報である回復用の登録用入力情報を、秘密鍵を用いて暗号化したテンプレート、を記憶するテンプレート記憶手段と、
前記クライアントの要求に応じて、乱数を生成する乱数生成手段と、

前記乱数を用いて前記テンプレートを秘匿化した秘匿化テンプレート、を生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成手段と、
判定手段と
を備え、
前記判定手段は、
回復用の登録用入力情報と、被認証者の生体情報である回復用照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記回復用照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得し、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記回復用照合情報についての認証を行う
照合システム。
（付記８）
前記クライアントは、
前記秘密鍵と前記公開鍵とを生成する鍵生成手段と、
前記秘密鍵を用いて前記テンプレートを生成するテンプレート生成手段と
を有し、
前記鍵生成手段は、前記公開鍵を前記回復用検証システムに送信する
付記７に記載の照合システム。
（付記９）
クライアントの要求に応じて、乱数を生成する乱数生成段階と、
前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成段階であって、前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである、秘匿化テンプレート生成段階と、
登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する段階と、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う認証段階と
を備える
回復用検証方法。
（付記１０）
クライアントの要求に応じて、乱数を生成する乱数生成処理と、
前記乱数を用いてテンプレートを秘匿化した秘匿化テンプレートを生成し、前記秘匿化テンプレートを前記クライアントに送信する秘匿化テンプレート生成処理であって、前記テンプレートは、被登録者の生体情報である登録用入力情報を、秘密鍵を用いて暗号化したものである、秘匿化テンプレート生成処理と、
登録用入力情報と、被認証者の生体情報である照合情報と、の間の近似度を秘匿化した指標である秘匿化指標であって、前記照合情報と前記秘匿化テンプレートとに基づいて算出された秘匿化指標、の情報を、前記クライアントから取得する処理と、
前記秘密鍵に対応する公開鍵と、前記乱数とを用いて、前記秘匿化指標を復号した指標を生成し、生成された前記指標が所定範囲内の値を示すか否かに基づいて、前記照合情報についての認証を行う認証処理と
をコンピュータに実行させるためのプログラムが格納された非一時的なコンピュータ可読媒体。
【０１８４】
以上、実施形態を参照して本開示を説明したが、本開示は上記によって限定されるものではない。本開示の構成や詳細には、発明のスコープ内で当業者が理解し得る様々な変更

をすることができる。
【産業上の利用可能性】
【０１８５】
本開示は、クライアントとサーバを用いる生体認証を行う照合システムに好適に適用される。
【符号の説明】
【０１８６】
１　照合システム
２　通常照合システム
３　回復用照合システム
１０　回復用検証システム
１０ａ　サーバ側システム
２０　クライアント
２０ａ　クライアント側システム
１１０　登録情報生成装置
１１１　秘密情報入力部
１１２　登録情報生成部
１２０　認証情報生成装置
１２１　登録情報受信部
１２２　登録情報記憶部
１２３　照合情報入力部
１２４　認証情報生成部
１２５，１６５　出力部
１３０　認証情報検証装置
１３１　検証情報受信部
１３２　ＩＤ発行部
１３３　検証情報記憶部
１３４，１７５，１７５ａ　判定部
１３５，１７６　チャレンジ生成部
１７４　受理範囲記憶部
１４０　回復用登録情報生成装置
１４１　回復用情報入力部
１４２　回復用ＩＤ入力部
１４３　鍵生成部
１４４　秘匿化部
１５０　回復用登録情報記憶装置
１５１　テンプレート記憶部
１５１ａ　回復用登録情報記憶部
１５３　乱数生成部
１５３ａ　マスク生成部
１５２　秘匿化テンプレート生成部
１５２ａ　回復情報生成部
１６０　回復用認証情報生成装置
１６１　回復用照合情報入力部
１６２　回復用ＩＤ入力部
１６３　回復情報受信部
１６４　回復用認証情報生成部
１７０　回復用認証情報検証装置
１７１　鍵受信部
１７２　鍵記憶部

１７３　回復用鍵生成部
１０００　コンピュータ
１００１　ＣＰＵ
１００２　主記憶装置
１００３　補助記憶装置
１００４　インターフェース
１００５　通信インターフェース

【図面】

【図１】

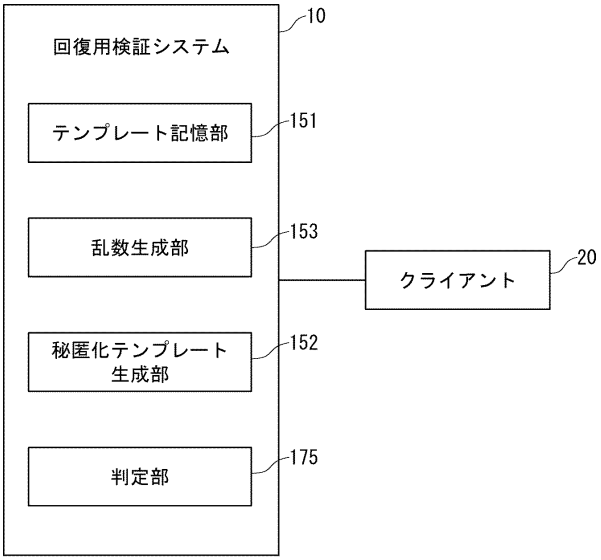

Fig. 1

【図２】

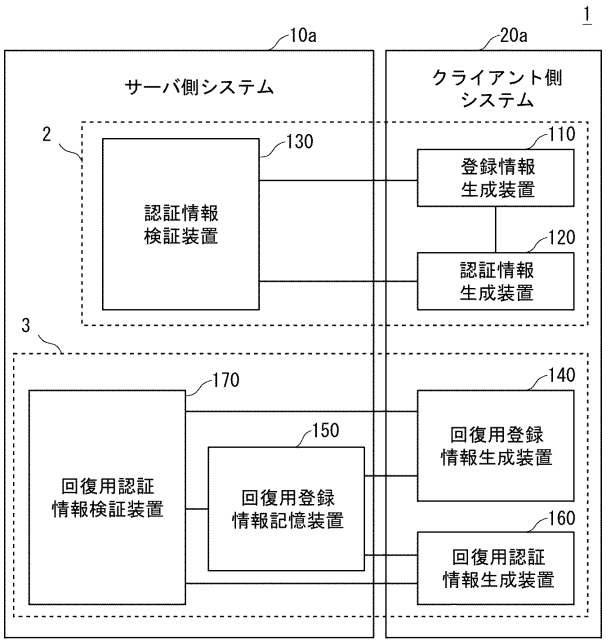

Fig. 2

【図３】

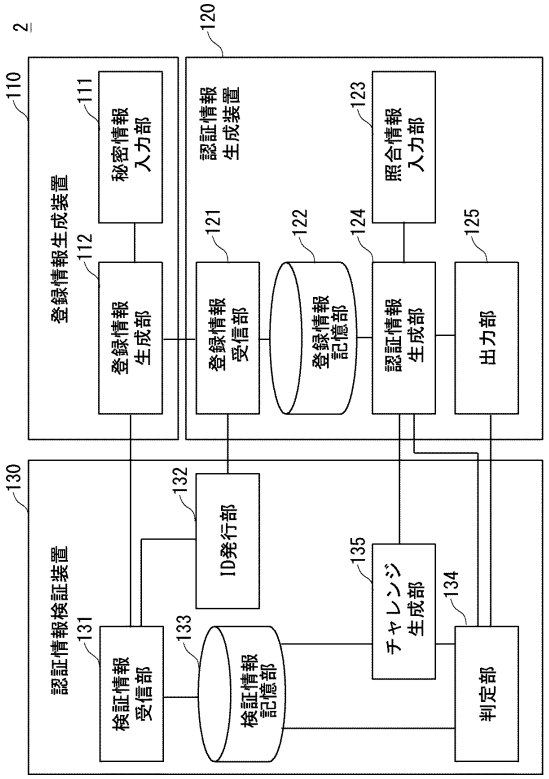

Fig. 3

【図４】

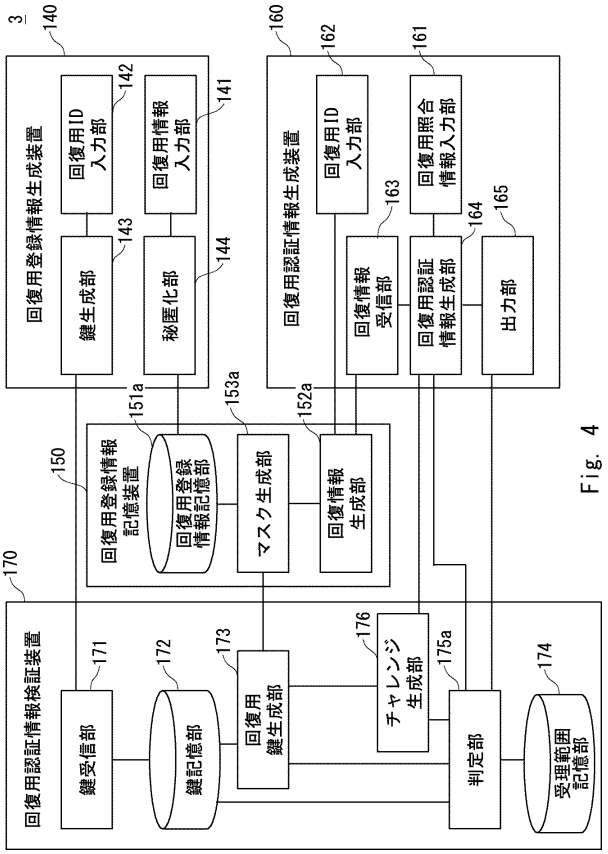

Fig. 4

【図５】

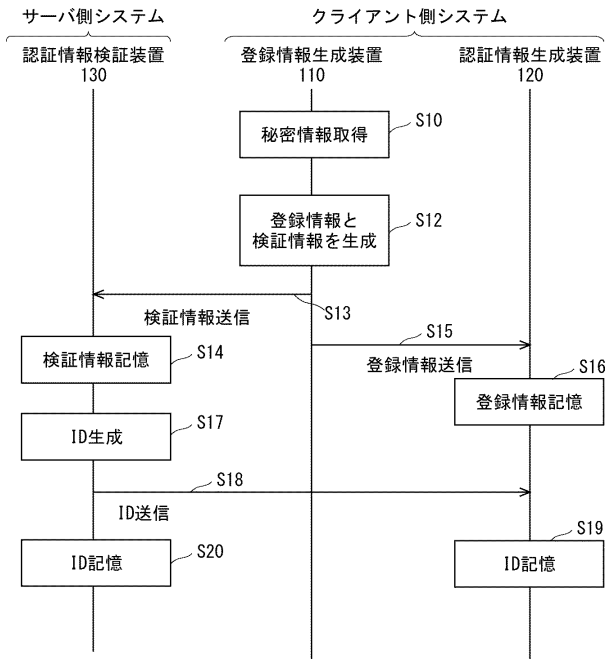

Fig. 5

【図６】

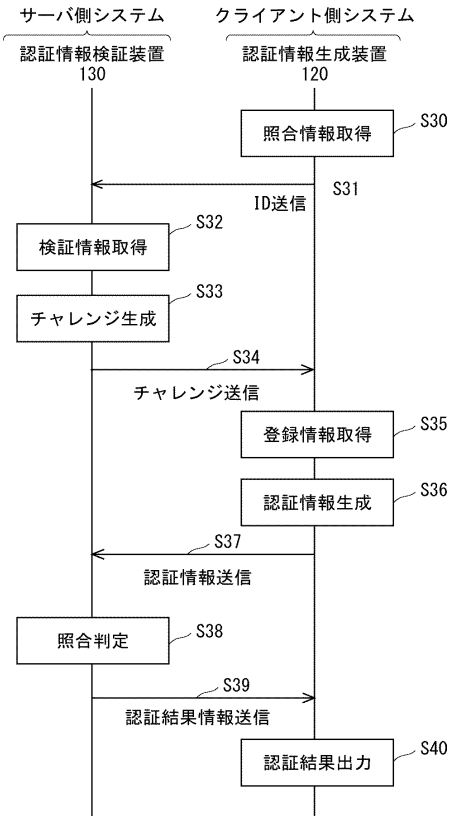

Fig. 6

【図７】

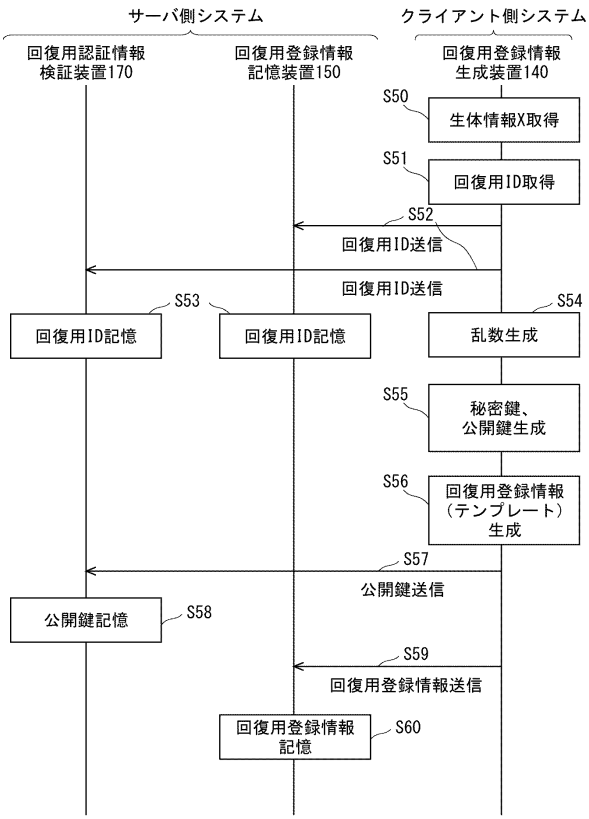

Fig. 7

【図８】

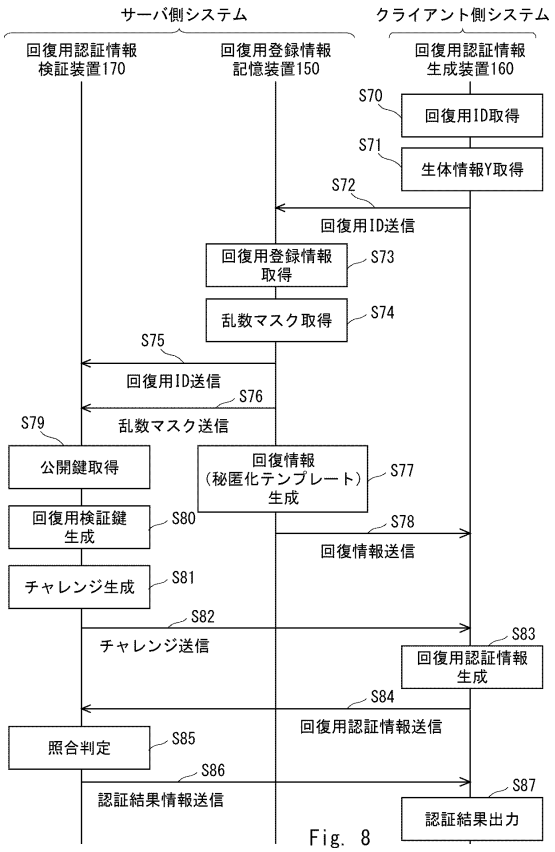

Fig. 8

【図９】

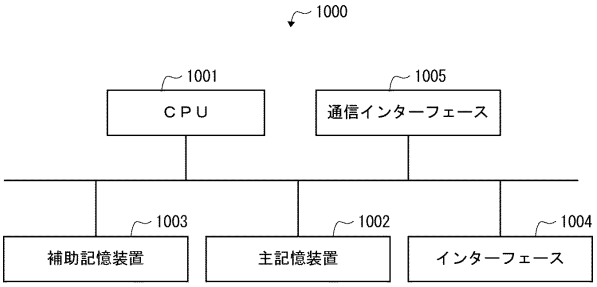

Fig. 9

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

審査官　高橋 克

(56)参考文献　国際公開第２０２０／２４５９３９（WO，Ａ１）
国際公開第２０１８／１７４０６３（WO，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３２
Ｇ０６Ｆ　２１／４５
Ｇ０６Ｆ　２１／６０