(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-42372
(P2020-42372A)
(43)公開日　令和2年3月19日(2020.3.19)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/62	(2013.01)	G06F 21/62	318	
G06F 21/32	(2013.01)	G06F 21/32		

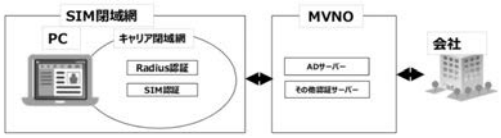
審査請求 未請求　請求項の数 5　ＯＬ　（全 12 頁）

(21)出願番号　特願2018-167399 (P2018-167399)
(22)出願日　平成30年9月6日 (2018.9.6)

(71)出願人　518319964
株式会社ペンライズ・アンド・カンパニー
東京都杉並区和泉３丁目５９－２４
(74)代理人　100140408
弁理士　鈴木　康介
(72)発明者　友村　清
東京都府中市新町１丁目６８番９号
(72)発明者　嶋村　俊彦
東京都府中市新町１丁目６８番９号

(54)【発明の名称】認証システム

(57)【要約】
【課題】生体認証を用いたより安全な認証システムを提供する。
【解決手段】生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を登録する際、前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、前記コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップと、秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスにそれぞれ記憶する記憶ステップとを備える認証システムを備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を登録する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップと、
秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスにそれぞれ記憶する記憶ステップとを備える認証システム。
【請求項２】
生体認証機能を有する第一のデバイスと、第二のデバイスと、第三のデバイスとを備える認証システムにおいて生体情報を登録する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップと、
秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスと、第三のデバイスにそれぞれ記憶する記憶ステップとを備える認証システム。
【請求項３】
請求項１、または請求項２に記載の認証システムにおいて、
各認証キーが復号可能か確認する確認ステップとを備える認証システム。
【請求項４】
生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を認証する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップと、
前記第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップと、
取得した前記第一の認証キーと前記第二の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップと、
前記コード化された生体情報と、認証情報とを照合するステップとを備える認証システム。
【請求項５】
生体認証機能を有する第一のデバイスと、第二のデバイスと第三のデバイスを備える認証システムにおいて生体情報を認証する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップと、
前記第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップと、
前記第三のデバイスに記憶されている第三の認証キーを取得する第三認証キー取得ステップと、

取得した前記第一の認証キーと前記第二の認証キーと前記第三の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップと、
前記コード化された生体情報と、認証情報とを照合するステップとを備える認証システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、認証システムに関する。
【背景技術】
【０００２】
国が推進している働き方変革として、自宅や出張先など社外でいつものような仕事を行えるようなテレワークがキーポイントとなって来ている。このテレワークを促進するためには、自宅や出張先な社外で会社へアクセスするためのテレワーク環境が安心・安全にかつ快適に利用できる必要がある。
【０００３】
しかしながら、現在のテレワーク環境には、第一に、「利用するネットワークが正しいものか？」。第二に、「利用しているＰＣ等のデバイスが正しいものか？」。第三に、「利用者が本人であるか？」という三つの課題がある。
【０００４】
第一の課題である「利用するネットワークが正しいものか？」に対しては、ＳＩＭ等のネットワーク認証を行うことにより解決することが必要である。このネットワーク認証は、ＬＴＥ５Ｇによる高速かつセキュア・ネットワークなＳＩＭ閉域網を利用することで、ネットワーク認証としてＳＩＭ認証を取れ、ＶＰＮが不要なネットワーク環境を得ることができる。
【０００５】
第二の課題である「利用しているＰＣ等のデバイスが正しいものか？」に対しては、ＰＣ等のデバイスの個体認証を行う必要がある。第三の課題である「利用者が本人であるか？」については、確実な本人認証を行う必要がある。
【０００６】
テレワークを行う上で重要なネットワーク環境モバイル・ネットワークは、ＬＴＥ５Ｇなどの高速ネットワークの発展により、利用者に快適な利用環境を提供できるようになる。さらに、ＳＩＭ閉域網とＭＶＮＯによるネットワーク環境によって、ＶＰＮを必要としないネットワーク環境を構築できるようになるとともに、この新しいネットワーク環境のテレワークへの利用によって、現在のテレワークの課題のうち第一の課題と第二の課題の２つを解決することが可能になる。
【０００７】
第一の課題である「利用するネットワークが正しいものか？」については、ＰＣ等のモバイルのためのネットワーク認証（ＳＩＭ認証）により、ネットワークへのアクセスの正当性を確認できる。また、第二の課題である「利用しているＰＣ等のデバイスが正しいものか？」については、ＰＣ等のデバイスの個体認証（Ｒａｄｉｕｓ認証）により、デバイスの正当性を確認できる。
【０００８】
このように、テレワーク環境を利用して、社外から会社へアクセスする場合、ＳＩＭ閉域網によるモバイル・ネットワークを利用することで、ＰＣ等のデバイス認証及びネットワークのＳＩＭ認証により、利用するデバイスとネットワークの正当性を確認できる（課題１、２）。
【０００９】
しかし、このように、正しいネットワークや、正しいことデバイスであったとしても、実際の利用者が正当な利用者であるかどうかが確かめられていない。例えば、ＳＩＭカー

ド付きのＰＣ等のモバイルが窃盗され、このモバイルを用いてネットワークにアクセスされた場合、アクセスを防止することができない。このため、本人認証としては、指紋、光彩、静脈等の生体情報を利用した生体認証が有効である（特許文献１）。
【先行技術文献】
【特許文献】
【００１０】
【特許文献１】特開２０１８－１２０４８３
【発明の概要】
【発明が解決しようとする課題】
【００１１】
しかしながら、デバイスに生体情報を全て記憶した場合、デバイスが盗難され、デバイス内の生体情報を利用して不正アクセスされてしまう恐れがある。また、サーバに全ての生体情報を記録した場合、サーバから生体情報が持ち出されると、その情報を利用して不正アクセスされる恐れがある。このため、テレワークを可能とするためにより安全な認証システムが求められている。
【００１２】
本発明は、上述した課題を解決するために、生体認証を用いたより安全な認証システム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】
【００１３】
（１）　生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を登録する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップと、
秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスにそれぞれ記憶する記憶ステップとを備える認証システム。
【００１４】
（２）　生体認証機能を有する第一のデバイスと、第二のデバイスと、第三のデバイスとを備える認証システムにおいて生体情報を登録する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップと、
秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスと、第三のデバイスにそれぞれ記憶する記憶ステップとを備える認証システム。
【００１５】
（３）　（１）、または（２）に記載の認証システムにおいて、
各認証キーが復号可能か確認する確認ステップとを備える認証システム。
【００１６】
（４）　生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を認証する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップと、

前記第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップと、
取得した前記第一の認証キーと前記第二の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップと、
前記コード化された生体情報と、認証情報とを照合するステップとを備える認証システム。
【００１７】
（５） 生体認証機能を有する第一のデバイスと、第二のデバイスと第三のデバイスを備える認証システムにおいて生体情報を認証する際、
前記第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップと、
前記情報入手ステップで入手した前記ユーザの生体情報をコード化するコードステップと、
前記第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップと、
前記第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップと、
前記第三のデバイスに記憶されている第三の認証キーを取得する第三認証キー取得ステップと、
取得した前記第一の認証キーと前記第二の認証キーと前記第三の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップと、
前記コード化された生体情報と、認証情報とを照合するステップとを備える認証システム。
【図面の簡単な説明】
【００１８】
【図１】テレワークにおける課題の解決方法の一例を説明する概念図である。
【図２】本発明にかかる認証システムの一例を説明する概念図である。
【図３】本発明にかかる認証システムの一例を説明する概念図である。
【図４】本発明にかかる認証システムの一例を説明する概念図である。
【図５】本発明にかかる認証システムの一例を説明するフローチャートである。
【図６】本発明にかかる認証システムの一例を説明するフローチャートである。
【図７】本発明にかかる認証システムの一例を説明するフローチャートである。
【図８】本発明にかかる認証システムの一例を説明するフローチャートである。
【図９】本発明にかかる認証システムの一例を説明する概念図である。
【図１０】本発明にかかる認証システムの一例を説明する概念図である。
【発明を実施するための最良の形態】
【００１９】
図１は、課題１と課題２の解決策を示す一例である。テレワークを行う上で重要なネットワーク環境モバイル・ネットワークは、ＬＴＥ５Ｇなどの高速ネットワークの発展により、利用者に快適な利用環境を提供できる。
【００２０】
さらに、図１に示すように、ＳＩＭ閉域網とＭＶＮＯによるネットワーク環境によって、ＶＰＮを必要としないネットワーク環境を構築できるようになるとともに、この新しいネットワーク環境のテレワークへの利用によって、現在のテレワークの課題のうち下記の２つを解決できる。
【００２１】
課題１「利用するネットワークが正しいものか？」については、ＰＣ等のモバイルのためのネットワーク認証（ＳＩＭ認証）を利用することにより、ネットワークへのアクセスの正当性を認可できる。
【００２２】
課題２「利用しているＰＣ等のデバイスが正しいものか？」については、ＰＣ等のデバ

イスの個体認証（Ｒａｄｉｕｓ認証）を利用することにより、デバイスの正当性を認可できる。

【００２３】

図２は、本発明の概要を示す説明図である。テレワーク環境を利用して、社外から会社へアクセスする場合、ＳＩＭ閉域網によるモバイル・ネットワークを利用することで、ＰＣ等のデバイス認証及びネットワークのＳＩＭ認証により、利用するデバイスとネットワークの正当性は確保できる（課題１、２）。しかし、実際の利用者が正当な利用者であるかどうかが確かめられていない。本人認証としては、指紋、光彩、静脈等の生体情報を利用した生体認証が有効である。

【００２４】

そこで図２に示すように、本発明では、ＰＣなどモバイルデバイスやスマートフォンに付属している指紋読取装置による指紋認証やスマートフォンの顔認証などから得られる生体情報に対して秘密分散処理を行い、分散片１（分割したデータ片の一部、後に認証キーとも表記する）をＭＶＮＯの管理する認証サーバに、分散片２（分割したデータ片の一部、後に認証キーとも表記する）をスマートフォン等の外部デバイスに保存することで、ＰＣに依存しないＩＤ／パスワードを不要とする本人認証が可能とする。

【００２５】

図３はモバイルデバイスを用いた本人認証の手順の一例である。図４に示すように、秘密分散技術を利用して、認証サーバとスマートフォンに生体情報を分散保管する。認証時に認証サーバとスマートフォンの分散データを復号し、生体情報と照会することで本人かどうか判断できる。

【００２６】

図３に示すように、モバイルデバイスの電源を入れると、キャリア閉域網へＳＩＭ接続される（ＳＩＭ認証によってネットワークが正しいか判別できる）。さらに、モバイルデバイスなどのデバイス認証が行われる（Ｒａｄｉｕｓ認証によって、正しいデバイスか判別できる）。その後、認証サーバから送信される生体情報の分散片１とスマートフォンから送信される生体情報の分散片２とをモバイルデバイス内で復号し、読み取った生体情報と比較し、本人かどうか判断する。正しい使用者の場合にはモバイルデバイスのディスプレイにおいてデスクトップ画面を表示する。

【００２７】

図４は、本発明にかかる登録時と、認証時の概念図である。図４に示すように、登録時は、読取装置で取得した生体情報を秘密分散処理で、分散片１と分散片２に分割し、別々の場所に保管する。認証時は、分散片１と分散片２から復号化された生体情報とパターンマッチング照合して本人かどうか判断する。このように、生体情報を秘密分散処理して、分散情報を分散管理することで、多要素認証による新しい本人認証を実現できる。

【００２８】

図５は、認証キーが２つの場合の登録時の処理フローである。ステップＳ５０２において、モバイルデバイス１００は、登録プログラムを起動する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ５０４に処理を移す。

【００２９】

ステップＳ５０４において、モバイルデバイス１００は、モバイルデバイス１００に接続された生体認証デバイス１２０を起動し、生体認証デバイス１２０を用いてユーザの生体情報（例えば、指紋や顔や虹彩など）を読み取る。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ５０６に処理を移す。このように、本処理は、第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップの一例である。

【００３０】

ステップＳ５０６において、モバイルデバイス１００は、読み取った生体情報をコード化し、生体情報コードを作成する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ５０８に処理を移す。このように、本処理は、情報入手ステップで入手したユーザの生体情報をコード化するコードステップの一例である。

【００３１】
ステップＳ５０８において、モバイルデバイス１００は、ステップＳ５０６で作成された生体情報コードを秘密分散処理し、認証キーＫ１と認証キーＫ２という２つの認証キーを作成する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ５１０に処理を移す。このように、本処理は、コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップの一例である。
【００３２】
ステップＳ５１０において、モバイルデバイス１００は、分散片（認証キー）を各デバイスに分散し、保管する処理を行う。具体的には、モバイルデバイス１００は、スマートフォン２００に認証キーＫ１を送信し、認証サーバ３００に認証キーＫ２を送信する。なお、本実施形態においてモバイルデバイス１００は、認証サーバ３００に認証キーを送信しているが本発明はこれに限定されず、モバイルデバイス１００内において、認証キーＫ２を保存しても良い。このように、これらの処理は、秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスにそれぞれ記憶する記憶ステップの一例である。
【００３３】
ステップＳ５１２において、スマートフォン２００は、モバイルデバイス１００から送信された認証キーＫ１を記憶する。さらに、スマートフォン２００は、記憶された認証キーＫ１をモバイルデバイス１００に送信する。
【００３４】
ステップＳ５１４において、認証サーバ３００は、モバイルデバイス１００から送信された認証キーＫ２を記憶する。さらに、認証サーバ３００は、記憶された認証キーＫ２をモバイルデバイス１００に送信する。
【００３５】
ステップＳ５１６において、モバイルデバイス１００は、スマートフォン２００から受信した認証キーＫ１と認証サーバ３００から送信された認証キーＫ２とから生体情報コードを復号する。この処理が終了した場合には、ステップＳ５１８に処理を移す。
【００３６】
ステップＳ５１８において、モバイルデバイス１００は、ステップＳ５１６で認証キーＫ１と認証キーＫ２とから生体情報コードが復号できた場合には、ステップＳ５２２に処理を移し、登録プログラムを終了する。復号できなかった場合には、ステップＳ５０４に処理を移す。このように、本処理は、各認証キーが復号可能か確認する確認ステップの一例である。また、このように、これらの一連の処理は、生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を登録する際の一例である。
【００３７】
図６は、認証キーが２つの場合の認証時の処理フローである。ステップＳ６０２において、モバイルデバイス１００は、認証プログラムを起動する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ６０４に処理を移す。
【００３８】
ステップＳ６０４において、モバイルデバイス１００は、モバイルデバイス１００に接続された生体認証デバイス１２０を起動し、生体認証デバイス１２０を用いてユーザの生体情報（例えば、指紋や顔や虹彩）を読み取る。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ６０６に処理を移す。このように、本処理は、第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップの一例である。
【００３９】
ステップＳ６０６において、モバイルデバイス１００は、読み取った生体情報をコード化し、生体情報コードを作成する。このように、本処理は、情報入手ステップで入手したユーザの生体情報をコード化するコードステップの一例である。
【００４０】

ステップＳ６０８において、スマートフォン２００は、記憶された認証キーＫ１をモバイルデバイス１００に送信する。このように、本処理は、第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップの一例である。

【００４１】

ステップＳ６１０において、認証サーバ３００は、記憶された認証キーＫ２をモバイルデバイス１００に送信する。このように、本処理は、第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップの一例である。

【００４２】

ステップＳ６１２において、モバイルデバイス１００は、スマートフォン２００から受信した認証キーＫ１と認証サーバ３００から送信された認証キーＫ２とから認証情報コードを復号する。この処理が終了した場合には、ステップＳ６１４に処理を移す。このように、本処理は、取得した第一の認証キーと第二の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップの一例である。

【００４３】

ステップＳ６１４において、モバイルデバイス１００は、複合した認証情報コードと生体情報コードを照合する処理を行う。この処理が終了した場合には、ステップＳ６１６に処理を移す。このように、本処理は、コード化された生体情報と、認証情報とを照合するステップの一例である。

【００４４】

ステップＳ６１６で認証情報コードと生体情報コードとの照合結果が正常だった場合には、ステップＳ６１８に処理を移し、認証プログラムを終了する。正常ではない場合には、ステップＳ６０４に処理を移す。このように、これらの一連の処理は、生体認証機能を有する第一のデバイスと、第二のデバイスを備える認証システムにおいて生体情報を認証する処理の一例である。

【００４５】

図７は、認証キーが３つの場合の登録時の処理フローである。ステップＳ７０２において、モバイルデバイス１００は、登録プログラムを起動する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ７０４に処理を移す。

【００４６】

ステップＳ７０４において、モバイルデバイス１００は、モバイルデバイス１００に接続された生体認証デバイス１２０を起動し、生体認証デバイス１２０を用いてユーザの生体情報（例えば、指紋や顔や虹彩など）を読み取る。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ７０６に処理を移す。このように、本処理は、第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップの一例である。

【００４７】

ステップＳ７０６において、モバイルデバイス１００は、読み取った生体情報をコード化し、生体情報コードを作成する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ７０８に処理を移す。このように、本処理は、情報入手ステップで入手したユーザの生体情報をコード化するコードステップの一例である。

【００４８】

ステップＳ７０８において、モバイルデバイス１００は、ステップＳ７０６で作成された生体情報コードを秘密分散処理し、認証キーＫ１と認証キーＫ２と認証キーＫ３という３つの認証キーを作成する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ７１０に処理を移す。このように、本処理は、コードステップにおいて、コード化したコード化後生体情報を秘密分散処理し、認証キーを複数生成する秘密分散処理ステップの一例である。

【００４９】

ステップＳ７１０において、モバイルデバイス１００は、分散片（認証キー）を各デバイスに分散し、保管する処理を行う。具体的には、モバイルデバイス１００は、スマートフォン２００に認証キーＫ１を送信し、モバイルデバイス１００内で認証キーＫ２を記憶

（ステップＳ７１３）し、認証サーバ３００に認証キーＫ３を送信する。

【００５０】

ステップＳ７１２において、スマートフォン２００は、モバイルデバイス１００から送信された認証キーＫ１を記憶する。さらに、スマートフォン２００は、記憶された認証キーＫ１をモバイルデバイス１００に送信する。

【００５１】

ステップＳ７１４において、認証サーバ３００は、モバイルデバイス１００から送信された認証キーＫ３を記憶する。さらに、認証サーバ３００は、記憶された認証キーＫ３をモバイルデバイス１００に送信する。このように、これらの処理は、秘密分散処理した各認証キーを第一のデバイスと、第二のデバイスと、第三のデバイスにそれぞれ記憶する記憶ステップの一例である。

【００５２】

ステップＳ７１６において、モバイルデバイス１００は、スマートフォン２００から受信した認証キーＫ１と、モバイルデバイス１００に記憶された認証キーＫ２と、認証サーバ３００から送信された認証キーＫ３とから生体情報コードを復号する。この処理が終了した場合には、ステップＳ７１８に処理を移す。

【００５３】

ステップＳ７１８において、モバイルデバイス１００は、ステップＳ７１６で認証キーＫ１と認証キーＫ２と認証キーＫ３とから生体情報コードが復号できた場合には、ステップＳ７２２に処理を移し、登録プログラムを終了する。復号できなかった場合には、ステップＳ７０４に処理を移す。このように、本処理は、各認証キーが復号可能か確認する確認ステップの一例である。また、このように、これらの一連の処理は、生体認証機能を有する第一のデバイスと、第二のデバイスと、第三のデバイスとを備える認証システムにおいて生体情報を登録する際の処理の一例である。

【００５４】

図８は、認証キーが３つの場合の認証時の処理フローである。ステップＳ８０２において、モバイルデバイス１００は、認証プログラムを起動する。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ８０４に処理を移す。

【００５５】

ステップＳ８０４において、モバイルデバイス１００は、モバイルデバイス１００に接続された生体認証デバイス１２０を起動し、生体認証デバイス１２０を用いてユーザの生体情報（例えば、指紋や顔や虹彩）を読み取る。この処理が終了した場合には、モバイルデバイス１００は、ステップＳ８０６に処理を移す。このように、本処理は、第一のデバイスにおいて、ユーザから生体情報を入手する情報入手ステップの一例である。

【００５６】

ステップＳ８０６において、モバイルデバイス１００は、読み取った生体情報をコード化し、生体情報コードを作成する。このように、本処理は、情報入手ステップで入手したユーザの生体情報をコード化するコードステップの一例である。

【００５７】

ステップＳ８０８において、スマートフォン２００は、記憶された認証キーＫ１をモバイルデバイス１００に送信する。このように、本処理は、第一のデバイスに記録されている第一の認証キーを取得する第一認証キー取得ステップの一例である。

【００５８】

ステップＳ８１１において、モバイルデバイス１００は、記憶された認証キーＫ２を呼び出す。このように、本処理は、第二のデバイスに記憶されている第二の認証キーを取得する第二認証キー取得ステップの一例である。

【００５９】

ステップＳ８１０において、認証サーバ３００は、記憶された認証キーＫ３をモバイルデバイス１００に送信する。このように、本処理は、第三のデバイスに記憶されている第三の認証キーを取得する第三認証キー取得ステップの一例である。

【００６０】
ステップＳ８１２において、モバイルデバイス１００は、スマートフォン２００から受信した認証キーＫ１と、モバイルデバイス１００に記憶されていた認証キーＫ２と、認証サーバ３００から送信された認証キーＫ３とから認証情報コードを復号する。この処理が終了した場合には、ステップＳ８１４に処理を移す。このように、本処理は、取得した第一の認証キーと第二の認証キーと第三の認証キーから認証キーを復号処理し、認証情報を取得する認証情報取得ステップの一例である。
【００６１】
ステップＳ８１４において、モバイルデバイス１００は、複合した認証情報コードと生体情報コードを照合する処理を行う。この処理が終了した場合には、ステップＳ８１６に処理を移す。このように、本処理は、コード化された生体情報と、認証情報とを照合するステップの一例である。
【００６２】
ステップＳ８１６で認証情報コードと生体情報コードとの照合結果が正常だった場合には、ステップＳ８１８に処理を移し、認証プログラムを終了する。正常ではない場合には、ステップＳ８０４に処理を移すこのように、これらの一連の流れは、生体認証機能を有する第一のデバイスと、第二のデバイスと第三のデバイスを備える認証システムにおいて生体情報を認証する処理の一例である。
【００６３】
図９は、スマートフォンを利用した認証システムの一例である。スマートフォン２００は、分散片１（認証キーＫ１、秘密鍵）を記憶している。モバイルデバイス１００は、分散片２（認証キーＫ２、公開鍵）を記憶している。認証サービスサーバ３００は、分散片３（認証キーＫ３）を記憶している。
【００６４】
認証時、スマートフォン２００がモバイルデバイス１００に認証キーＫ１を送信する。次に、モバイルデバイス１００は、分散片２をサービス事業者のサーバ４００に送信する。サービス事業者のサーバ４００は、認証サービスサーバ３００に分散片３を要求する。
【００６５】
認証サービスサーバ３００は、モバイルデバイス１００に対して、サービス事業者のサーバ４００からの分散片３の要求に応じて良いかという確認の問い合わせを送る。ユーザがこの問い合わせに対して承認する場合、認証サービスサーバ３００に対して要求の承認を送信する。
【００６６】
ユーザの承認に応じて、認証サーバ３００は、分散片３をサービス事業者のサーバ４００に送信する。サービス事業者のサーバ４００は、分散片２と分散片３とを復号化して、本人認証を実施する。
【００６７】
図１０は、スマートフォンを利用したＷｅｂサービスへの応用の一例である。前提条件として、本人情報は、モバイルデバイス１００上で、登録時に秘密分散化して、認証キーＫ１と、認証キーＫ２に分散化されている（図５参照）。また、認証キーＫ１はスマートフォン２００に認証キーＫ２はサーバに送信され、データベースサーバに保存されている。
【００６８】
認証キーＫ１をスマートフォン２００からモバイルデバイス１００に送信する。認証キーＫ１をサーバから送られてきた真性乱数と排他的論理和を行い、統合認証キーを生成する。
（認証キーＫ１　ＸＯＲ　真正乱数　＝＞　統合認証キー）
【００６９】
モバイルデバイス１００は、統合認証キーをＷｅｂサーバに送信する。Ｗｅｂサーバは、統合認証キーと真性乱数とを排他的論理和を行って、認証キーＫ１を復元する。

（認証キーＫ１　ＸＯＲ　真正乱数　）ＸＯＲ　真正乱数　＝＞認証キーＫ１

【００７０】

Ｗｅｂサーバは、データベースサーバに認証キーＫ２を要求する。データベースサーバは、Ｗｅｂサーバに認証キーＫ２を送信する。Ｗｅｂサーバは、認証キーＫ１と認証キーＫ２を復元し、本人認証要求をＡＤ／ＬＤＡＰサーバに要求する。ＡＤ／ＬＤＡＰサーバは、本人認証確認結果をＷｅｂサーバに送信する。Ｗｅｂサーバは、本人認証確認の結果が正しい場合には、初期画面をモバイルデバイス１００に送信する。

【００７１】

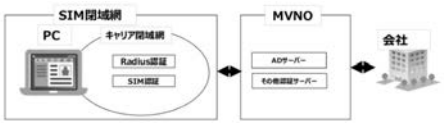
現在、全てのＰＣに生体認証デバイスもしくは機能があるわけではない。このため、本発明利用して、身近な携帯電話を生体機能デバイスとして利用できることで、ＩＤ／パスワードが不要の仕組みが確立できる。本発明にかかるシステムでは、秘密分散技術によって、ＰＣと携帯電話に生体情報を含め認証情報を分散することで、個体認証を行い、パスワードだけでなく、ＩＤも不要にすることが可能になる。

【符号の説明】

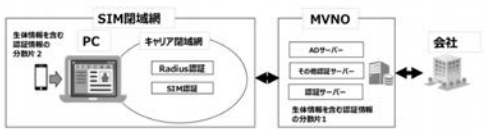
【００７２】

１００　モバイルデバイス
２００　スマートフォン
３００　認証サービスサーバ
４００　サービス事業者のサーバ

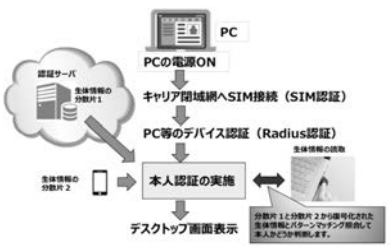
【図１】



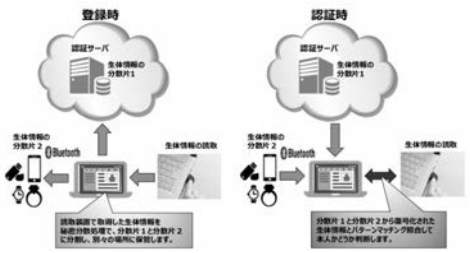
【図２】



【図３】



【図４】

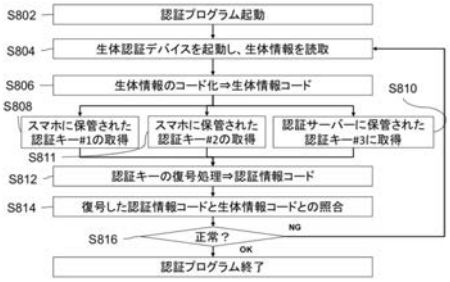


【図５】

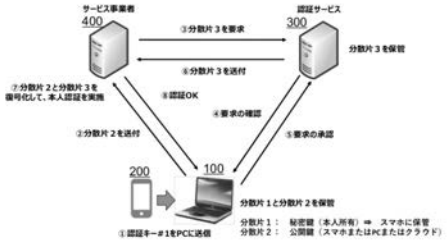
【図６】

【図７】

【図８】



【図９】



【図１０】