(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4719950号
(P4719950)
(45)発行日　平成23年7月6日(2011.7.6)　(24)登録日　平成23年4月15日(2011.4.15)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 673D
H04L 9/00 673A

請求項の数 10　(全 23 頁)

(21)出願番号　特願平11-320895
(22)出願日　平成11年11月11日(1999.11.11)
(65)公開番号　特開2001-144748(P2001-144748A)
(43)公開日　平成13年5月25日(2001.5.25)
審査請求日　平成18年3月13日(2006.3.13)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　水谷　陽一
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　渡邊　浩一郎
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法、並びにプログラム提供媒体

(57)【特許請求の範囲】
【請求項１】
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、
パスワードを入力するパスワード入力手段と、
前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、
前記中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、
を有することを特徴とする暗号鍵生成装置。
【請求項２】
前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、ＤＮＡパターンのいずれか、または指紋、眼底像、声紋、ＤＮＡパターンの２以上の生体情報の組み合せであることを特徴とする請求項１に記載の暗号鍵生成装置。
【請求項３】
前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、
前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項１に記載

の暗号鍵生成装置。
【請求項４】
前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする請求項１に記載の暗号鍵生成装置。
【請求項５】
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、
パスワードを入力するパスワード入力手段と、
前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、
前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、
暗号化すべきデータを入力するデータ入力手段と、
前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、
前記暗号化手段において暗号化したデータを出力する出力手段と、
を有することを特徴とする暗号化装置。
【請求項６】
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、
パスワードを入力するパスワード入力手段と、
前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、
前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、
復号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの復号化処理を実行する復号化手段と、
前記復号化手段において復号化したデータを出力する出力手段と、
を有することを特徴とする復号化装置。
【請求項７】
暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、
生体情報読み取り手段によって、生体情報を取得して該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワード入力手段によって、パスワードの入力を受け付けるパスワード入力ステップと、
中間コード生成手段によって、前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
を有することを特徴とする暗号鍵生成方法。
【請求項８】
生体情報読み取り手段によって、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワード入力手段によって、パスワードの入力を行うパスワード入力ステップと、
中間コード生成手段によって、前記生体情報読み取りステップで読み取られた生体コー

ドと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
データ入力手段によって、暗号化すべきデータの入力を行うデータ入力ステップと、
暗号化手段によって、前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化ステップと、
データ出力手段によって、前記暗号化ステップにおいて暗号化したデータを出力する出力ステップと、
を有することを特徴とする暗号化方法。
【請求項９】
生体情報読み取り手段によって、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワード入力手段によって、パスワードの入力を行うパスワード入力ステップと、
中間コード生成手段によって、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
データ入力手段によって、復号化すべきデータの入力を行うデータ入力ステップと、
復号化手段によって、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの復号化処理を実行する復号化ステップと、
データ出力手段によって、前記復号化ステップにおいて復号化したデータを出力する出力ステップと、
を有することを特徴とする復号化方法。
【請求項１０】
暗号鍵生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを記録したプログラム提供媒体であって、
前記コンピュータ・プログラムは、
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワードを入力するパスワード入力ステップと、
前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
を有することを特徴とするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術的分野】
本発明は、暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法、並びにプログラム提供媒体に関する。さらに詳細には、指紋等、個人固有の生体情報とパスワードとを組み合わせたデータに基づいて暗号化鍵、復号化鍵を生成する暗号鍵生成装置および方法に関するものであり、さらに、機密保持の要請される文書データ、音声データ、画像データ、各種プログラム等、様々な情報の暗号化処理、復号化処理を生体情報とパスワードとを組み合わせたデータに基づく暗号化鍵、復号化鍵を用いて行なう暗号化・復号化装置および暗号化・復号化方法に関するものである。
【０００２】
【従来の技術】

近年、インターネット等の各種ネットワークシステムを介した情報転送が盛んになり、ネットワーク上での電子決済や電子マネーの使用が急激に増大している。さらに多くの企業、あるいは個人において機密文書をハードディスク、光ディスク等、様々な記憶媒体を利用して保存することも頻繁に行われている。このようなネットワークを介する転送データ、あるいは様々な記憶媒体に格納されるデータのセキュリティをいかに確保するかが重要な課題となっている。

【０００３】

セキュリティ確保の方法には様々な手法があるが、その一つがコンピュータの利用を正規の利用者に限定する方法である。この方法の代表的なものは、予め正規利用者に対してパスワードを与え、正しいパスワードの入力を行なった者のみがデータへのアクセスを可能とする構成である。さらに、セキュリティを高めるためのデータ自体に対する処理としてデータの暗号化処理がある。ネットワークを介して転送する文書を暗号化し、また、記憶媒体に格納する情報を暗号化処理することにより、転送情報および蓄積情報の安全性を高めることができる。

【０００４】

暗号化データは、所定の手続きによる復号化によって解読可能な文書（平文）に戻すことができる。情報の暗号化処理に暗号化鍵を用い、復号化に復号化鍵を用いるデータ暗号化、復号化方法が従来から知られている。

【０００５】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類あるが、その１つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にＤＥＳ（データ暗号標準：Ｄｅｔａ　ｅｎｃｒｙｐｔｉｏｎ　ｓｔａｎｄａｒｄ）がある。

【０００６】

また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号がある。

【０００７】

前述の共通鍵暗号化方式は、想定される通信相手数が多くなると鍵の数が膨大となり、不特定多数の通信には向かない。また、公開鍵暗号化方式は、管理する鍵の数は少なくてすむという利点がある。しかし、公開鍵暗号化方式は暗号化処理、復号化が煩雑になるという欠点がある。

【０００８】

上述の共通鍵暗号化方式と、公開鍵暗号化方式とを融合させた方式としてハイブリッド暗号化方式がある。ハイブリッド暗号化方式は、情報の暗号化には共通鍵を用い、暗号化に用いた共通鍵を公開鍵暗号化方式で暗号化するものである。このハイブリッド暗号化方式によれば、処理の早い共通鍵暗号化方式をデータ量の多い文書に適用し、処理の遅い公開鍵暗号化方式をデータ量の少ない共通鍵の暗号化にのみ使用するので、両者の利点を有効に利用できる。

【０００９】

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等

に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザＩＤ等のパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるユーザＩＤ等のパスワードを求めることは実質上不可能である。

【００１０】

上述の観点から、暗号化鍵、復号化鍵を用いる構成においては、パスワード管理がセキュリティ管理上、非常に重要な問題となる。しかしながら、ユーザＩＤ等のパスワードを個人で管理することには様々な問題があるのが現状である。セキュリティを高めるためには複雑なパスワードを持つことが有利と考えられるが、複雑なパスワードを人間が記憶することは困難である。人間の記憶を補うために例えばハードディスク等何らかの記憶装置にパスワードを記憶させて保存することも可能であるが、このような記憶装置にパスワードを格納した場合、第三者が記憶装置からパスワードを盗むという可能性もあり、安全性に関して問題がある。

【００１１】

パスワード管理の問題点を解決するための一つの手法として、個人の生体情報、例えば眼底像、指紋等を用いて、正規ユーザであるか否かの照合を行なう方法がある。個人の生体情報を用いたセキュリティ管理システム例として、特開平１１－２１５１１９号公報に開示の個人情報管理装置および方法がある。

【００１２】

特開平１１－２１５１１９号公報に記載のシステムは、正規ユーザ個人の生体情報、例えば眼底像から得られるコード情報を予めシステムに登録して保存する構成を持つ。本システムは、文書の暗号化処理を行なおうとするユーザが、まず自分の眼底情報等、生体情報の読み取りをシステムに実行させる。次に、システムは、ユーザが正規の登録済みユーザであるか否かについて、ユーザから読み取った生体情報と登録した生体情報とを比較照合して確認する。この照合処理によってユーザの正当性が確認された場合にのみ、生体情報に基づく鍵によって暗号化処理に移行する構成としたものである。この方法によれば、個人固有の生体情報に基づく秘密鍵を用いて暗号化処理が実行されるので、他人による秘密鍵の複製、悪用が防止されるという効果がある。

【００１３】

【発明が解決しようとする課題】

しかしながら、このような生体情報を用いた個人の正当性確認処理を実現するためには、新たに読み取った個人の眼底像、指紋等の生体情報と比較対象となる照合情報をシステム中の記憶装置中に格納しておく必要がある。すなわち正規ユーザである各個人の眼底像、指紋等を予め電子撮影して得られた画像情報、あるいは、この画像情報から得られるコード列を予め記憶装置に記憶することが必要となる。特開平１１－２１５１１９号では生体情報から得られるコードを変換処理した２次コードを保存することにより安全性を高めてはいるが、このようなシステムでは、記憶情報が盗用されてしまった場合に、盗用された情報に基づいて暗号鍵が複製される可能性があり、システムの信頼性が必ずしも十分ではない。

【００１４】

さらに、従来の生体情報のみに頼るコード生成手法では、異なる個人の指紋等から読み取られる生体情報コードが同一になってしまうと、その同一コードに基づいて同一の暗号鍵が生成される可能性がある。このような可能性を排除するため、スキャナ等の生体情報読み取り手段のパターン読み取り精度を極めて高精度にして各個人の生体情報コードを確実に異なるものとしなければならなかった。しかし、現実には、そのような高精度な読み取りを実現させることは困難であり、また高精度な読み取りを実現させようとすると、たとえ同一人であっても読み取り毎に異なるコードが生成されるなどの不具合が発生する可能性があり、現実として使用に耐えるシステムを実現するのは困難である。

【００１５】
さらに、従来のシステム構成では、正規ユーザの眼底像等、生体情報を予め電子撮影した画像情報、あるいは、それらの画像情報から得られるコード列を記憶した記憶装置を持たないシステムにおいては照合処理が不可能である。従って、ネットワークを介した暗号情報配信システム等に上記構成を適用した場合は、照合情報を蓄積したメモリを搭載した装置のみが通信に参加することができ、照合情報を蓄積していない装置は通信に参加できないことになる。従って、上記構成は極めて限定されたシステムにおいてのみ有効な構成であって拡張性に劣るという欠点がある。
【００１６】
さらに、特開平１１－２１５１１９号公報に開示の個人情報管理装置および方法のように、眼底像情報に基づいて暗号化鍵を生成しようとする場合、個人から得られる眼底像情報は、左右の目を使用した場合でも２つであり、眼底像情報から得られるコード列は極めて少ない種類となるので暗号化鍵の種類を増やすことは困難となる。さらに異なる暗号鍵を作成しようとした場合、他の生体情報、例えば指紋を使用することが考えられるが１０本の指を使用した場合でも、最大１０種類のコードが得られるのみであるので、生体情報のみを使用した暗号化鍵生成方法において生成される暗号鍵は極めて限定された有限数に限られてしまうという問題がある。
【００１７】
本発明の、暗号化・復号化装置および暗号化・復号化方法、並びにプログラム提供媒体は、上述のような従来技術における問題点に鑑みてなされたものである。
【００１８】
本発明は、生体情報のみではなく、任意のパスワードを生体情報に組み合わせた合成コードに基づいて暗号鍵を生成する構成とすることにより、異なる個人において生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードの一致する可能性をなくし、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単な構成とすることを可能とした暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法を提供することを目的とする。
【００１９】
さらに、本発明の、暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法は、生体情報を用いた暗号化鍵または復号化鍵生成手法を用いたシステムは、記憶装置等に予め正規ユーザの生体情報を登録する必要性を排除してシステムの拡張性を確保したシステムを提供することを目的とする。
【００２０】
さらに、本発明は、生体情報にパスワードを組み合わせたコード列に基づいて暗号化鍵、または復号化鍵を生成する構成とすることにより、無限数の異なる暗号化鍵または復号化鍵の生成を可能とした暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法を提供することを目的とする。
【００２１】
【課題を解決するための手段】
本発明の第１の側面は、
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、
パスワードを入力するパスワード入力手段と、
前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、
前記中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、
を有することを特徴とする暗号鍵生成装置にある。
【００２２】

さらに、本発明の暗号鍵生成装置において、前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、ＤＮＡパターンのいずれか、または指紋、眼底像、声紋、ＤＮＡパターンの２以上の生体情報の組み合せであることを特徴とする。

【００２３】

さらに、本発明の暗号鍵生成装置において、前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする。

【００２６】

さらに、本発明の暗号鍵生成装置において、前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする。

【００２７】

さらに、本発明の第２の側面は、

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

暗号化すべきデータを入力するデータ入力手段と、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、

前記暗号化手段において暗号化したデータを出力する出力手段と、

を有することを特徴とする暗号化装置にある。

【００３２】

さらに、本発明の第３の側面は、

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、

前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成手段と、

前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、

復号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの復号化処理を実行する復号化手段と、

前記復号化手段において復号化したデータを出力する出力手段と、

を有することを特徴とする復号化装置にある。

【００３７】

さらに、本発明の第４の側面は、

暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、

生体情報読み取り手段によって、生体情報を取得して該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、

パスワード入力手段によって、パスワードの入力を行うパスワード入力ステップと、

中間コード生成手段によって、前記生体情報読み取りステップにおいて読み取られた生

体コードと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
を有することを特徴とする暗号鍵生成方法にある。

【００４２】

さらに、本発明の第５の側面は、
生体情報読み取り手段によって、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワード入力手段によって、パスワードの入力を行うパスワード入力ステップと、
中間コード生成手段によって、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
データ入力手段によって、暗号化すべきデータの入力を行うデータ入力ステップと、
暗号化手段によって、前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化ステップと、
データ出力手段によって、前記暗号化ステップにおいて暗号化したデータを出力する出力ステップと、
を有することを特徴とする暗号化方法にある。

【００４３】

さらに、本発明の第６の側面は、
生体情報読み取り手段によって、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワード入力手段によって、パスワードの入力を行うパスワード入力ステップと、
中間コード生成手段によって、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
暗号鍵生成手段によって、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、
データ入力手段によって、復号化すべきデータの入力を行うデータ入力ステップと、
復号化手段によって、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの復号化処理を実行する復号化ステップと、
データ出力手段によって、前記復号化ステップにおいて復号化したデータを出力する出力ステップと、
を有することを特徴とする復号化方法にある。

【００４４】

さらに、本発明の第７の側面は、
暗号鍵生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを記録したプログラム提供媒体であって、
前記コンピュータ・プログラムは、
生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、
パスワードを入力するパスワード入力ステップと、
前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードをアドレスとするテーブル検索によって中間コードを生成する中間コード生成ステップと、
前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、

を有することを特徴とするプログラム提供媒体にある。

【００４５】

本発明の第７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００４６】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００４７】

【作用】

本発明の構成によれば、指紋コードのような各種の生体情報とパスワードとを組み合わせた合成コードを生成し、この合成コードに基づいて暗号鍵を生成する構成であるので、パスワードによる合成コードのユニーク性を高めることが可能となり、異なる個人間において読み取り生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードは異なるものとすることが可能となり、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単なコードとすることが可能となり、高精度の読み取り装置を必要としない暗号化・復号化装置構成が実現される。

【００４８】

また、本発明の構成によれば、パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置にパスワードを記憶して管理することができ、従って暗号鍵の生成および機密管理が容易となる。ここで、共有の暗号鍵（共有鍵）とは、ユーザ間で共有したい鍵をいい、鍵自体は共通鍵、公開鍵を問わない。すなわち、ＤＥＳ暗号などの共通鍵方式のときは共通鍵を、ＲＳＡ暗号などの公開鍵方式のときは秘密鍵（秘密の復号化鍵、認証の場合には、秘密の通信文検査鍵）を意味する。なお、公開鍵方式において、暗号化鍵、通信文生成鍵は公開ファイルによってすでに共有されているといえる。

【００４９】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５０】

【発明の実施の形態】

以下、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法の実施の形態について、図面を参照しながら、詳細に説明する。

【００５１】

【実施例】

図１に本発明の暗号化装置、図２に復号化装置、図３に暗号化／復号化装置の各構成を示すブロック図を示す。さらに、図４に各構成におけるハードウェア構成例を示す。以下、各図に従って、順次説明する。

【００５２】

図１は、本発明の暗号化・復号化装置の一実施例に係る暗号化装置を構成するブロック図を示したものである。

【００５３】

暗号化装置は図１に示すように、指紋読み取り手段１０１、パスワード入力手段１０２、暗号鍵生成手段１０３、データ入力手段１０４、暗号化手段１０５、データ出力手段１０６を有する。なお、以下の実施例の説明においては、図１の暗号化装置に示すように、生体情報として指紋を使用する例を中心として説明する。しかしながら、本発明の暗号化・

復号化装置および暗号化・復号化方法で使用する生体情報は、指紋に限らず、眼底像、声紋、ＤＮＡパターン、その他、個人特有の生体に関する情報、あるいはこれらの組み合わせであれば使用可能であり、実施例に示す構成に限定されない。眼底像、声紋、ＤＮＡパターンを使用する場合は、それぞれの生体情報に対する読み取り装置、分析装置を使用する。例えば眼底像をしようする場合は眼底カメラ、声紋を使用する場合は音声認識装置、ＤＮＡパターンを使用する場合はＤＮＡ分析装置等を用いて生体情報を読み取る。ただし、以下では、説明の複雑化をさけるため、生体情報として指紋を使用した例について説明する。

【００５４】

図１の暗号化装置における指紋読み取り手段１０１は、利用者（ユーザ）の指が押し当てられたときに、指紋パターンを読み取り、その特徴抽出を行い、抽出された特徴データに基づいて指紋コードを出力し、暗号鍵生成手段１０３に出力する。指紋パターンの読み取りは光学的に指紋を読み取るスキャナ、あるいは指を押し当てることによって発生する圧力を微少部分毎に検出して凹凸パターンを読み取る圧力センサ等、各種の読み取り構成によって実現可能である。

【００５５】

パスワード入力手段１０２は、例えばキーボードのようなユーザがパスワードを入力する手段である。パスワード入力手段１０２から入力されたパスワードは暗号鍵生成手段１０３に出力される。

【００５６】

暗号鍵生成手段１０３は、指紋読み取り手段１０１から読み取られた指紋コードとパスワード入力手段１０２から入力されたパスワードの組み合わせに応じて、暗号鍵を生成し、暗号化手段１０５へ出力する。この暗号鍵生成手段１０３で生成する暗号鍵には、暗号化するための暗号化鍵と、復号化するための復号化鍵を含むものであり、前述した共通鍵暗号化方式、公開鍵暗号化方式、ハイブリッド暗号化方式等、各種の暗号化方式のいずれを適用するかによって、生成する鍵の種類が決定されることになる。本発明は、いずれの暗号化方式においても適用可能なものであり、生成する鍵は、データの暗号化処理または復号化処理、あるいは前述のハイブリッド方式を適用する場合には、鍵自体の暗号化処理または復号化処理においても用いられる。この図１では、データの暗号化処理に用いる暗号化鍵を生成したものとして、以下説明する。なお、暗号鍵生成手段の具体例については、後段で説明する。

【００５７】

データ入力手段１０４は、暗号化すべきデータを入力するたとえばハードディスク、ネットワークインタフェース等によって構成されるデータ入力手段であり、暗号化すべきデータを暗号化手段１０５へ出力する。暗号化手段１０５は、データ入力手段１０４から入力された暗号化すべきデータを、暗号鍵生成手段１０３で生成された暗号化鍵で暗号化し、データ出力手段１０６へ出力する。

【００５８】

データ出力手段１０６は、ネットワークインタフェース、あるいはハードディスク等の記憶手段等によって構成され、暗号化手段１０５で暗号化されたデータを出力する。

【００５９】

図１に示す暗号化装置では、指紋読み取り手段１０１において指紋から取得される特徴コードと、パスワード入力手段１０２から入力されるパスワードの組み合わせに応じて、暗号鍵生成手段１０３が暗号化鍵を生成し、この暗号化鍵により、データ入力手段１０４から入力したデータを暗号化してデータ出力手段１０６に出力することが可能であり、指紋読み取り手段１０１によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列にパスワード入力手段１０２から入力する任意のパスワードを組み合わせて暗号化鍵生成用コードとすることができるので、パスワードを変更することにより無数の異なるコード列を生成することができ、異なる暗号化鍵を無限に生成することが可能となる。

【００６０】
さらに、図１に示す暗号化装置では、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。
【００６１】
次に、図２を用いて本発明による復号化装置の構成を説明する。図２は、本発明に係る復号化装置の構成を示したブロック図である。図２に示すように復号化装置は、指紋読み取り手段２０１、パスワード入力手段２０２、暗号鍵生成手段２０３、データ入力手段２０４、復号化手段２０５、データ出力手段２０６を有する。
【００６２】
指紋読み取り手段２０１、パスワード入力手段２０２、暗号鍵生成手段２０３、データ入力手段２０４、データ出力手段２０６の基本構成は、前述の図１で説明した暗号化装置における各手段と同様であるので、同一構成についての説明は省略し、異なる部分を中心として説明する。
【００６３】
図２に示す復号化装置において、暗号鍵生成手段２０３は、指紋読み取り手段２０１から読み取られた指紋コードとパスワード入力手段２０２から入力されたパスワードの組み合わせに応じて、暗号鍵、この場合は暗号データの復号化に用いる復号化鍵を生成し、復号化手段２０５へ出力する。
【００６４】
データ入力手段２０４は、復号化すべき暗号化データを入力し、復号化手段２０５へ出力する。復号化手段２０５は、データ入力手段２０４から入力された復号化すべき暗号データを、暗号鍵生成手段２０３で生成された復号化鍵で復号し、データ出力手段２０６へ出力する。データ出力手段２０６は、復号化手段２０５で、復号化されたデータを出力する。
【００６５】
この図２に示す復号化装置を用いれば、指紋から取得される特徴コードとパスワードの組み合わせに応じて生成される復号化鍵により、暗号データを復号化して出力することが可能であり、指紋読み取り手段によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列に任意のパスワードを組み合わせて復号化鍵の元データとすることができ、パスワードを変更することにより無数の異なるコード列を生成することができるので、異なる無数の復号化鍵を生成することが可能となる。
【００６６】
また、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。
【００６７】
次に、図３を用いて本発明による暗号化・復号化装置の構成を説明する。図３は、本発明による暗号化・復号化装置の構成を示したブロック図である。図３に示すように暗号化・復号化装置は、指紋読み取り手段３０１、パスワード入力手段３０２、暗号鍵生成手段３０３、データ入力手段３０４、暗号化・復号化手段３０５、データ出力手段３０６を有する。
【００６８】
指紋読み取り手段３０１、パスワード入力手段３０２、暗号鍵生成手段３０３、データ入力手段３０４、データ出力手段３０６の基本構成は、前述の図１、２で説明した暗号化装置、復号化装置における各手段と同様であるので、同一構成についての説明は省略し、異なる部分を中心として説明する。
【００６９】
図３に示す暗号化・復号化装置において、暗号鍵生成手段３０３は、指紋読み取り手段３０１から読み取られた指紋コードとパスワード入力手段３０２から入力されたパスワード

の組み合わせに応じて、暗号鍵、この場合はデータの暗号化に用いる暗号化鍵、または暗号データの復号化に用いる復号化鍵を生成し、暗号化・復号化手段３０５へ出力する。

【００７０】

データ入力手段３０４は、暗号化すべきデータ、または復号化すべき暗号化データを入力し、暗号化・復号化手段３０５へ出力する。暗号化・復号化手段３０５は、データ入力手段３０４から入力された暗号化すべきデータ、または復号化すべき暗号データを、暗号鍵生成手段３０３で生成された暗号化鍵で暗号化処理、または復号化鍵で復号し、データ出力手段３０６へ出力する。データ出力手段３０６は、暗号化手段３０５で暗号化されたデータ、または、復号されたデータを出力する。

【００７１】

この図３に示す暗号化・復号化装置においても、前述の暗号化装置、または復号化装置と同様に、指紋から取得される特徴コードとパスワードの組み合わせに応じて生成される暗号化鍵、または復号化鍵により、データの暗号化処理または復号化が可能となり、指紋読み取り手段によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列に任意のパスワードを組み合わせて暗号化鍵、復号化鍵の元データとすることができるので、パスワードを変更することにより無数の異なるコード列を生成することができ、異なる無数の暗号化鍵および復号化鍵を生成することが可能となる。

【００７２】

また、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。

【００７３】

次に、図４を用いて、上述の暗号化装置、復号化装置、および暗号化・復号化装置のハードウェア構成について説明する

【００７４】

図４は、図１～３において説明した暗号化装置、復号化装置、および暗号化・復号化装置に関するハードウェア構成の一例を示すブロック図である。

【００７５】

指紋読み取り手段４００は、光学的な指紋パターン読み取り手段としてのスキャナ４０２、マイクロコンピュータ＃１：４０３を含む。マイクロコンピュータ＃１：４０３は、バス４０４にＣＰＵ４０５、ＲＯＭ４０６、ＲＡＭ４０７、インプット・アウトプット・インタフェース（Ｉ／Ｏ）４０８を接続した構成を持つ。

【００７６】

マイクロコンピュータ＃１：４０３を構成するＲＯＭ４０６は、マイクロコンピュータ＃１：４０３を起動しオペレーティングシステム（ＯＳ）等を立ち上げるための基本プログラム等を格納し、ＲＡＭ４０７は、主記憶用メモリとして使用され、ＣＰＵ４０５によるコード生成処理等、各種処理のための作業領域を備えている。各種プログラム、例えば、指紋コード生成プログラムは図示しないフロッピーディスクやハードディスク等の記憶媒体に格納され、実行時にＲＡＭ４０７にロードされるようにしてもよい。

【００７７】

スキャナ４０２において読み取られた指紋画像データは、Ｉ／Ｏ４０８を介してマイクロコンピュータ＃１：４０３に入力され指紋コードを生成する処理が実行される。

【００７８】

指紋読み取り手段４００における処理、すなわちスキャナ４０２によって読み取られた指紋画像データから指紋コードを生成する処理について図５を用いて説明する。

【００７９】

なお、本発明の暗号化・復号化装置および暗号化・復号化方法においては、暗号鍵の生成元となるコードは、指紋等の生体情報コードと入力パスワードの双方に基づいて形成される。従って、入力パスワードを変更することによって合成して生成されるコードをいかにでも複雑化することが可能であるので、指紋等の生体情報コード自体は複雑なコードとす

ることが要請されない。生体情報から得られるコードを単純な短いデータ列としても、パスワードと組み合わせたコード列において同一コードが生成される可能性はほとんどない。従って、指紋読み取り精度を高くすることなく、高度なスキャン装置が必要とされない。

【００８０】

従来の生体情報のみに頼るコード生成手法では、異なる個人の指紋等から読み取られる生体情報コードが同一になってしまうと、その同一コードに基づいて同一の暗号鍵が生成される可能性がある。このような可能性を排除するため、スキャナの読み取り精度を極めて高精度にして各個人の生体情報コードを確実に異なるものとすることが要請されていた。しかし、現実には、高精度な読み取りを実行させると、同一人であっても読み取り時毎に異なる指紋コードが生成されるなどの不具合も発生し、使用に耐えるシステムは実現されていないのが現状である。

【００８１】

本発明の暗号化・復号化装置および暗号化・復号化方法においては、上述のような従来システムとは異なり、生体情報のみではなく、任意のパスワードを組み合わせたコードに基づいて暗号鍵を生成する構成であるので、異なる個人において生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードが一致する可能性はまずない。従って、指紋パターン等の生体情報の読み取りによって取得するコードは極めて簡単な構成とすることが可能である。本発明の暗号化・復号化装置において適用可能な指紋パターン読み取りおよびコード生成の一例を図５を用いて説明する。

【００８２】

指紋パターンからコードを生成するために、まず、図５（ａ）に示すように、スキャナに指を触れたときに形成される指紋像を複数領域に分割する。指の中心部を直交する線により、画像を領域１～４の４つの領域に分割し、分割各領域においてコードを生成する。

【００８３】

図５（ｂ）は、指紋の隆線方向（指紋の線の流れ）を４つのパターンに分類し、それぞれに対するコードを付与したものである。水平方向の隆線を０（００）、右上がりの隆線を１（０１）、垂直方向の隆線を２（１０）、右下がりの隆線を３（１１）としてコードを対応付けている。

【００８４】

図５（ｃ）は、図５（ａ）の指紋パターンの各領域における隆線パターン、すなわち各領域の指紋の隆線方向（指紋の線の流れ）を平均化して、図５（ｂ）の各パターン中、最も類似するパターン選択して指紋パターンと選択パターンを併せて示した図である。

【００８５】

図５（ｃ）の各領域において指紋パターンともっとも類似する選択パターンの持つコードを領域１～４の順に並べて生成されるデータを指紋コードとした。すなわち、図５の例では、図５（ｄ）に示すように１１０１１１０１（２進数）、あるいはｄｄ（１６進数）を指紋パターンに基づくコード、すなわち指紋コードとして出力される。

【００８６】

なお、図５で示すコード生成例は、生体情報からコードを生成する１つの例にすぎない。図５では領域分割数を４（図５（ａ）参照）とし、またコードを対応付けたコード対応パターンについても４種類（図５（ｂ）参照）とした例であるが、領域分割数を４以上の８、あるいは１６等に増やしてもよく、また、コード対応パターンについても、さらに方向を細かく区切ってコードを増加させることで、各指紋パターンに応じた細かな分類づけ、コード生成処理が可能である。

【００８７】

図６に図４に示す指紋読み取り手段４００における処理である読み取り指紋画像データから指紋コードを生成する処理フローを示す。図６は、具体的には、図４の指紋読み取り手段４００におけるマイクロコンピュータ＃１：４０３の指紋コード読み取りの処理アルゴリズムを示すフローチャートである。

【００８８】
ステップ６０１は、図４に示すスキャナ４０２において読み取られた指紋データを２次元のイメージデータへ展開し、方向の修正、ノイズ処理等の前処理を実行するステップである。
【００８９】
ステップ６０２は、ステップ６０１において前処理されたイメージデータを、ｎ個の領域へ分割する処理を実行するステップである。分割された各領域を（Ｉ１，Ｉ２，…，Ｉｎ）とする。
【００９０】
ステップ６０３は、ステップ６０２において分割された領域毎に、そのイメージデータの特徴抽出を行い、その特徴量をコード化するステップである。各領域Ｉ１，Ｉ２，…，Ｉｎ）から出力されるコード列を、（Ｃ１，Ｃ２，…，Ｃｎ）とする。
【００９１】
ステップ６０４では、各領域から出力されたコードを合成し、１つのコードへと合成する。その合成方法の一例は、単純に各領域のコードをつなげる、すなわち連接する方法である。合成コードをＡとすると、
Ａ＝Ｃ１Ｃ２…Ｃｎ
として示される。
【００９２】
ステップ６０５は、上記のステップ６０４において求めたコードＡを指紋コードとして出力する。
【００９３】
指紋読み取り手段４００は、このような手順を実行することにより、暗号鍵生成のために必要となる指紋コードを生成する。
【００９４】
このようにして生成された指紋パターンから得られるコードは、図４の暗号鍵生成手段４２０に出力される。
【００９５】
暗号鍵生成手段４２０は、マイクロコンピュータ＃２：４２３を含む。マイクロコンピュータ＃２：４２３は、バス４２４にＣＰＵ４２５、ＲＯＭ４２６、ＲＡＭ４２７、インプット・アウトプット・インタフェース（Ｉ／Ｏ）４２８を接続した構成を持つ。
【００９６】
マイクロコンピュータ＃２：４２３を構成するＲＯＭ４２６は、マイクロコンピュータ＃２：４２３を起動しオペレーティングシステム（ＯＳ）等を立ち上げるための基本プログラム等を格納し、ＲＡＭ４２７は、主記憶用メモリとして使用され、ＣＰＵ４２５による暗号鍵生成処理等、各種処理のための作業領域を備えている。各種プログラム、例えば、暗号鍵生成プログラムは図示しないフロッピーディスクやハードディスク等の記憶媒体に格納され、実行時にＲＡＭ４２７にロードされるようにしてもよい。
【００９７】
指紋読み取り手段４００において読み取られ、生成されたコードは、Ｉ／Ｏ４２８を介してマイクロコンピュータ＃２：４２３に入力され、暗号鍵生成処理が実行される。
【００９８】
暗号鍵生成手段４２０は、指紋読み取り手段４００において読み取られ、生成されたコードを入力するとともに、パスワード入力手段４１０から入力されるパスワードを入力する。パスワード入力手段４１０は、文字入力するためのキーボード４１１を備え、ユーザは任意のパスワードを入力できる。
【００９９】
暗号鍵生成手段４２０は、指紋読み取り手段４００において読み取られ生成されたコードと、パスワード入力手段４１０から入力されるパスワードに基づいて暗号鍵を生成する。
【０１００】

暗号鍵生成手段４２０は、例えば図７に示す機能構成を持つ。図７は、図４に示すマイクロコンピュータ＃２：４２３において実行される処理を、暗号鍵生成のアルゴリズムに従って機能構成に分割して示した機能ブロック図である。図７に示すように、暗号鍵生成手段７０１は、その処理機能として中間コード生成部７１１、暗号鍵生成部７１２を有する。

【０１０１】

中間コード生成部７１１は、指紋読み取り手段から読み取られた指紋コードとパスワード入力手段から入力されたパスワードの組み合わせに応じて、中間コードを生成し暗号生成部７１２に出力する。

【０１０２】

暗号鍵生成部７１２は、中間コード生成部７１１から出力された中間コードに所定の関数を施すことにより暗号鍵を生成し、暗号化・復号化手段に出力する。暗号鍵生成部７１２が生成する鍵は、システムが使用している暗号化方式が例えばＤＥＳ暗号などの共通鍵方式のときは共通鍵であり、またＲＳＡ暗号などの公開鍵方式を使用している場合は、秘密鍵、公開鍵となる。

【０１０３】

中間コード生成部７１１は、前述の図５、図６を用いて説明したような手法で指紋読み取り手段で読み取られた指紋パターンに基づいて生成された指紋コードと、パスワード入力手段から入力されたパスワードを結合して中間コードを生成する。

【０１０４】

中間コード生成部７１１において実行される中間コードの生成例を図８に示す。指紋読み取り手段において読み取られた指紋コードが、例えば、１６ビットで、

ＦＥ２６（指紋コード）…（１）

であり、

また、パスワード入力手段から入力されたパスワードが、例えば、１６ビットで、

３５ＢＡ（パスワード）…（２）

であったと仮定する。

【０１０５】

中間コード生成部６１１は、上記（１）の指紋コードと、（２）のパスワードを合成して、

ＦＥ２６３５ＢＡ…（３）

の３２ビットの中間コードを生成する。

【０１０６】

図７に示す中間コード生成部７１１において生成された中間コードは、暗号鍵生成部７１２へ出力される。

【０１０７】

なお、図８に示す中間コードの生成例は、１つの例であり、中間コードは指紋読み取り手段において生成される指紋コードと、パスワード入力手段によって入力されるパスワードに基づいて生成されるデータであれば許容されるものであり、図８に示すようなコード連接処理に限らず、指紋コードとパスワードに基づく新たなコードを生成すればよいものである。例えば、指紋コードとパスワードに対して関数を適用して中間コードを得る構成としてもよく、また、指紋コードとパスワードをアドレスとするテーブル検索による処理等によって新たなコードを生成してもよい。

【０１０８】

中間コード生成部７１１において生成された中間コードは、暗号鍵生成部７１２に出力され、暗号鍵生成部７１２は中間コードに基づいて暗号鍵を生成する。暗号鍵の生成手法は、ＲＳＡ方式、ＤＥＳ方式等、システムの採用している方式に従って処理が行なわれることになる。

【０１０９】

図９に図９（ａ）として共通鍵暗号化方式の場合の暗号鍵生成処理に用いる機能ブロック

構成、図９（ｂ）として公開鍵暗号化方式の場合の暗号鍵生成処理に用いる機能ブロック構成をそれぞれ示す。

【０１１０】

図９（ａ）の共通鍵暗号化方式について、まず説明する。先に説明したように共通鍵暗号化方式は、暗号化するときに使用する鍵と、復号化するときに使用する鍵とを共通化した暗号化方式である。

【０１１１】

図９（ａ）に示す共通鍵暗号化方式における暗号鍵生成部９０１は、関数Ｆを適用する関数処理手段９０２を有し、中間コード生成部から受領する中間コードに関数Ｆを適用して暗号化鍵、復号化鍵を生成して暗号化・復号化手段に出力する。関数Ｆの例としては、例えばＭＤ４ハッシュ関数、またはＭＤ５ハッシュ関数等の一方向関数がある。先に説明したように、生成された暗号鍵に基づいて、元のデータ、この場合は中間コードを導くことは困難である。

【０１１２】

共通鍵暗号化方式を採用している場合は、このようにして生成された暗号化鍵、または復号化鍵を用いて、データの暗号化処理または復号化処理が実行されることになる。

【０１１３】

次に図９（ｂ）の公開鍵暗号化方式について説明する。図９（ｂ）を用いてＲＳＡ方式を採用している場合の暗号鍵生成処理について説明する。図９（ｂ）に示すように暗号鍵生成部９０３は、中間コード分割部９０４、素数生成器９０５、公開鍵・秘密鍵生成部９０６を有する。

【０１１４】

ＲＳＡ方式において公開鍵と、秘密鍵を生成するためには、２個の素数ｐ，ｑが必要となる。中間コード分割部９０４では、中間コード生成部から入力される中間コードを２つのコードに分割する。例えば中間コードを途中で区切り、上位ビットと下位ビットの２つのコードを生成する。

【０１１５】

中間コード分割部９０４で生成された２つのコードは素数生成器９０５に出力される。素数生成器８０５は乱数発生器を有する。中間コード分割部９０４で生成された２つのコードのそれぞれが素数生成器８０５の有する乱数発生器に対する種として使用され、乱数発生器で発生された乱数をもとに素数判定し、素数が２つ抽出される。抽出された２つの素数が、暗号鍵生成用の素数ｐ、ｑとして公開鍵・秘密鍵生成部９０６に対して出力される。

【０１１６】

公開鍵・秘密鍵生成部９０６は、素数ｐ，ｑに基づいて公開鍵、秘密鍵を生成する。ｐ，ｑは、素数生成器９０５が生体情報コードとパスワードに基づく分割中間コードに基づいて出力した２つの素数ｐ，ｑであり、十分に大きな素数（例えば５１２～２０４８ビット）である。

【０１１７】

公開鍵・秘密鍵生成部９０６における暗号鍵の生成処理は、例えば以下の手順で行なわれる。まず、ｆ＝（ｐ－１）（ｑ－１）とし、このｆに互いに素（最大公約数が１）である値、ｅを求める。すなわちｇｃｄ（ｅ，（ｐ－１），（ｑ－１））＝１を満足する値、ｅを求める。なお、ｇｃｄは最大公約数を意味する。さらに、ｅｄ＝１　ｍｏｄｆとする値、ｄを求め、これら各値に基づいて公開鍵をｎ、ｅとし、秘密鍵をｐ、ｑ、ｄとして決定する。

【０１１８】

公開鍵・秘密鍵生成部９０６の生成した公開鍵、秘密鍵は、素数ｐ，ｑを知っていればｄをユークリッドの互除法で求めることができるが、ｐ，ｑを知らないものは、ｄを求めるためにはｎを因数分解することが必要となり、これは膨大な計算量となるため、実質的に値ｄを求めることは不可能である。公開鍵・秘密鍵生成部９０６は、このような手順に従

って、公開鍵・秘密鍵を生成する。なお、システムが適用している暗号化方式が異なれば鍵の生成方法も異なってくる。

【０１１９】

図４に戻って、本発明の暗号化・復号化装置の構成について説明を続ける。暗号鍵生成手段４２０では、上述した手法に従って各種の暗号鍵を生成する。

【０１２０】

暗号鍵生成手段４２０の生成した暗号鍵は、暗号化・復号化手段４３０に送られる。図４に示す例では、暗号化・復号化手段４３０として暗号化処理、復号化処理のいずれでも実行可能な構成、すなわち、図３に対応する暗号化・復号化装置の構成として示してあるが、図１または図２に示すように暗号化処理装置、または復号化処理装置である場合は、暗号化処理、または復号化処理のいずれか一方を実行する構成となる。

【０１２１】

暗号化・復号化手段４３０は、図４に示すように、マイクロコンピュータ＃３：４３３を含む。マイクロコンピュータ＃３：４３３は、バス４３４にＣＰＵ４３５、ＲＯＭ４３６、ＲＡＭ４３７、インプット・アウトプット・インタフェース（Ｉ／Ｏ）４３８を接続した構成を持つ。

【０１２２】

マイクロコンピュータ＃３：４３３を構成するＲＯＭ４３６は、マイクロコンピュータ＃３：４３３を起動しオペレーティングシステム（ＯＳ）等を立ち上げるための基本プログラム等を格納し、ＲＡＭ４３７は、主記憶用メモリとして使用され、ＣＰＵ４３５による暗号化処理、復号化処理等、各種処理のための作業領域を備えている。各種プログラム、例えば、暗号化処理プログラム、または復号化プログラムは図示しないフロッピーディスクやハードディスク等の記憶媒体に格納され、実行時にＲＡＭ４３７にロードされるようにしてもよい。

【０１２３】

暗号鍵生成手段４２０において生成された暗号鍵は、Ｉ／Ｏ４３８を介してマイクロコンピュータ＃３：４３３に入力され、暗号化処理、または復号化処理が実行される。

【０１２４】

暗号化・復号化手段４３０は、データ入力手段４４０から暗号化の対象となるデータ、または復号対象となる暗号化データを入力する。データ入力手段４４０は、図４の例では、記憶装置としてのハードディスク４４１を備え、ハードディスク中に処理対象のデータが格納されたものを想定しているが、データ入力は、例えばネットワークを介して転送されてくるデータであってもよい。

【０１２５】

暗号化・復号化手段４３０において、暗号化処理、または復号化が実行されたデータは、データ出力手段４５０に出力される。図４ではデータ出力手段４５０としてネットワークインタフェース４５１を記載しているが、このようにネットワークインタフェース４５１を介して外部に出力する構成、あるいはハードディスク、光ディスク、その他の記憶媒体に処理データを格納する構成としてもよい。

【０１２６】

暗号化・復号化手段４３０において実行される暗号化処理、または復号化処理は、前述の共通鍵暗号化方式、公開鍵暗号化方式等に基づいて、例えばＲＳＡ方式、ＤＥＳ方式等が適用されて処理が実行され、暗号化情報の生成、または暗号データからの復号データの生成が実行される。

【０１２７】

以上の説明から明らかなように、本発明の暗号化・復号化装置および暗号化・復号化方法においては、共通鍵暗号化方式、公開鍵暗号化方式いずれの暗号化方式においても、指紋読み取り手段４００による指紋情報から生成される個人特有の生体情報コードと、パスワード入力手段４１０から入力されるパスワードとに基づいて暗号鍵生成手段４２０において暗号鍵が生成され、この暗号鍵に基づいてデータの暗号化処理、または復号化が実行さ

れることになるので、個人固有の鍵生成が可能となり、また、様々なパスワードを組み合わせることで多様な鍵を無数に生成することが可能となる。

【０１２８】

さらに、本発明の構成によれば、暗号鍵の生成元データの一部を構成するパスワードを例えばハードディスク等の記憶装置に記憶し、暗号化処理、復号処理を行なう場合にのみ生体情報と合成して中間コードを生成して暗号鍵を生成する構成としてもよい。パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置からパスワードが盗まれてもデータの復号処理には適用できない。従って、複雑なパスワードを使用したい場合は、これを記憶媒体に記憶して管理することができ機密管理が容易となる。

【０１２９】

なお、図４に示すハードウェア構成例では指紋読み取り手段４００、暗号鍵生成手段４２０、暗号化・復号化手段４３０をそれぞれ個別のマイクロコンピュータとして示してあるが、指紋読み取り、暗号鍵生成、暗号化・復号化処理は、１つのコンピュータによって順次処理することも可能であり、図４に示すように複数のコンピュータによる構成のみならず、様々な構成が可能である。

【０１３０】

また、上述の実施例では、生体情報として指紋情報を用いた例を説明したが、先にも延べたように、指紋以外にも、「その人固有の情報」、たとえば、声紋や、眼底パターン、ＤＮＡパターンなどに基づいて、生体コードを生成し、このコードとパスワードとを組み合わせた合成コードに基づいて暗号化、復号化する構成としてもよい。さらに、生体コード自体を指紋コードと声紋コードとの合成コード、指紋コードと眼底パターンとの合成コードとし、これらにさらにパスワードを組み合わせて暗号鍵生成用のコードとしてもよい。

【０１３１】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１３２】

【発明の効果】

以上、説明したように、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法によれば、指紋コードのような各種の生体情報とパスワードとを組み合わせた合成コードを生成し、この合成コードに基づいて暗号鍵を生成する構成とした。従って、パスワードによる合成コードのユニーク性を高め、固有のものとすることが可能となり、異なる個人間において読み取り生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードは異なるものとすることが可能であるので、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単なコードとすることが可能となり、高精度の読み取り装置を必要としない暗号化・復号化装置構成が実現される。

【０１３３】

さらに本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、記憶装置等に予め正規ユーザの生体情報を登録して照合処理を実行する構成ではないので、利用可能な装置が照合データを持つシステムに限られず、拡張性の高い構成が実現される。

【０１３４】

さらに、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、生体情報にパスワードを組み合わせたコード列に基づいて暗号化鍵、または復号化鍵を生成する構成としたので、パスワードを変更することにより無限数の異なる暗号化鍵または復号化鍵の生成が可能となる。

【０１３５】

さらに、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置にパスワードを記憶して管理することができ機密管理が容易となる。

【図面の簡単な説明】

【図１】本発明に係る暗号化装置の構成を示すブロック図である。

【図２】本発明に係る復号化装置の構成を示すブロック図である。

【図３】本発明に係る暗号化・復号化装置の構成を示すブロック図である。

【図４】本発明に係る暗号化装置、復号化装置、暗号化・復号化装置のハードウェア構成を示すブロック図である。

【図５】本発明の暗号化・復号化装置における指紋パターンからコードを生成する処理例を説明する図である。

【図６】本発明の暗号化・復号化装置における指紋パターンからコードを生成する処理フローを示す図である。

【図７】本発明の暗号化・復号化装置における暗号鍵生成手段の処理ブロック図を示す図である。

【図８】本発明の暗号化・復号化装置における暗号鍵生成手段の指紋コード、パスワード、および中間コードの例を示す図である。

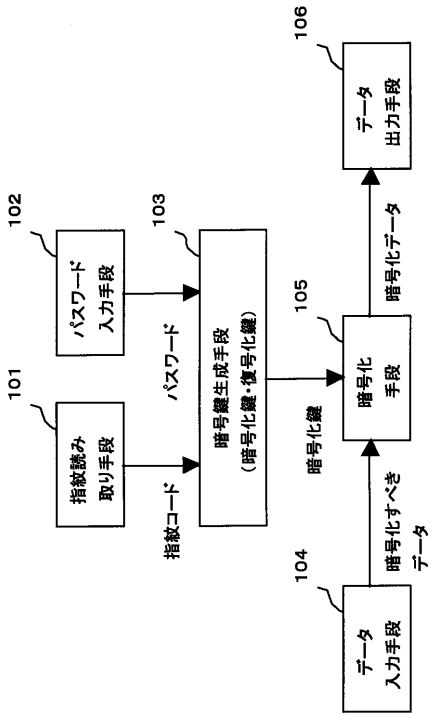
【図９】本発明の暗号化・復号化装置における暗号鍵生成手段の共通鍵暗号化方式と公開鍵暗号化方式における構成を示すブロック図である。

【符号の説明】

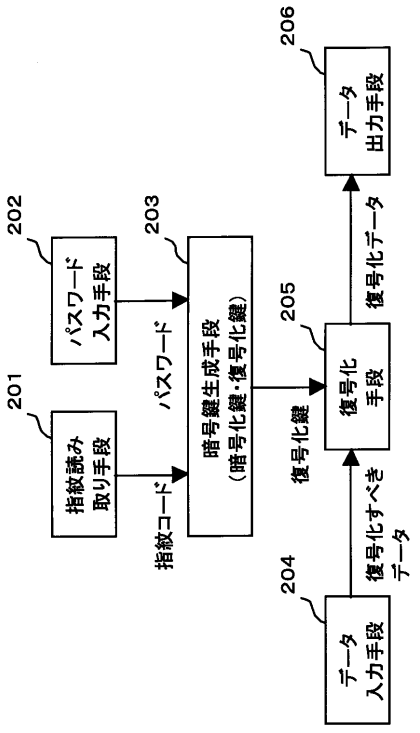
１０１，２０１，３０１　指紋読み取り手段
１０２，２０２，３０２　パスワード入力手段
１０３．２０３，３０３　暗号鍵生成手段
１０４，２０４，３０４　データ入力手段
１０５　暗号化手段
１０６，２０６，３０６　出力手段
２０５　復号化手段
３０５　暗号化・復号化手段
４００　指紋読み取り手段
４０２　スキャナ
４０３，４２３，４３３　マイクロコンピュータ
４０４，４２４，４３４　バス
４０５，４２５，４３５　ＣＰＵ
４０６，４２６，４３６　ＲＯＭ
４０７，４２７，４３７　ＲＡＭ
４１０　パスワード入力手段
４１１　キーボード
４２０　暗号鍵生成手段
４３０　暗号化（復号化）手段
４４０　データ入力手段
４４１　ハードディスク
４５０　データ出力手段
４５１　ネットワークインタフェース
７０１　暗号鍵生成手段
７１１　中間コード生成部
７１２　暗号鍵生成部
９０１　暗号鍵生成手段
９０２　関数処理手段
９０３　暗号鍵生成手段
９０４　中間コード分割部

９０５　素数生成器
９０６　公開鍵・秘密鍵生成部

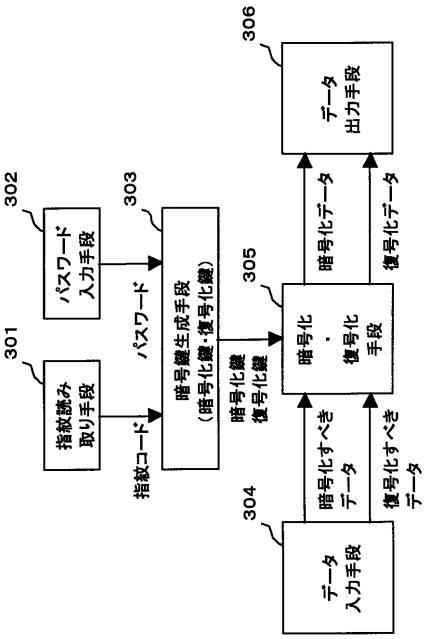
【図１】



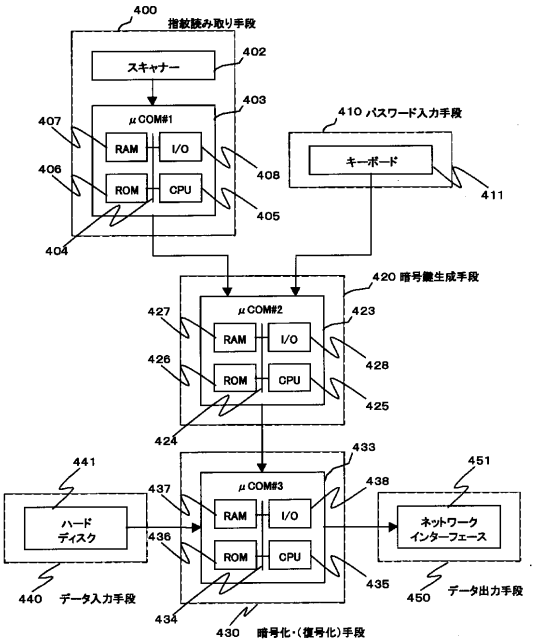
【図２】



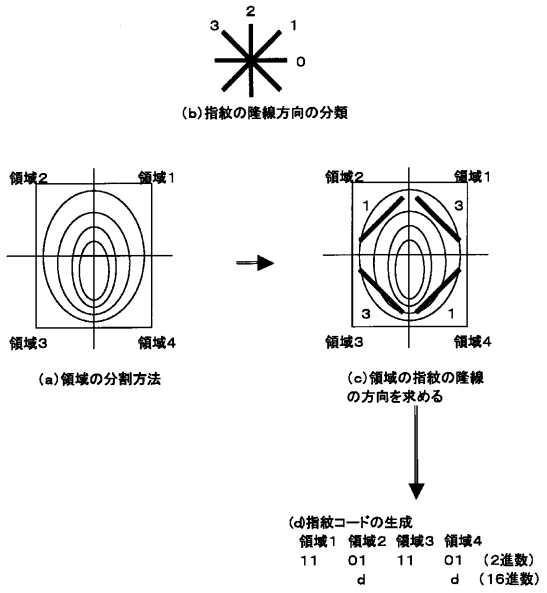
【図３】


306
データ出力手段
302
パスワード入力手段
303
暗号鍵生成手段（暗号化鍵・復号化鍵）
パスワード
暗号化データ
復号化データ
305
暗号化・復号化手段
301
指紋読み取り手段
指紋コード
暗号化鍵
復号化鍵
暗号化すべきデータ
復号化すべきデータ
304
データ入力手段

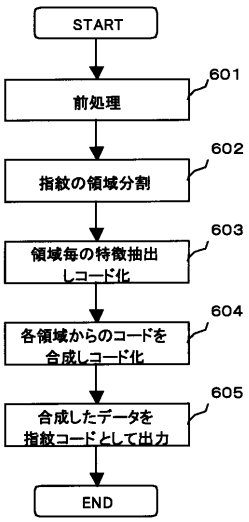
【図４】


400
指紋読み取り手段
スキャナー
402
403
μCOM#1
RAM
I/O
ROM
CPU
407
406
408
405
404
410 パスワード入力手段
キーボード
411
420 暗号鍵生成手段
μCOM#2
427
423
426
428
425
424
433
μCOM#3
441
437
438
451
ハードディスク
436
ネットワークインターフェース
435
440 データ入力手段
450 データ出力手段
434
430 暗号化・(復号化)手段

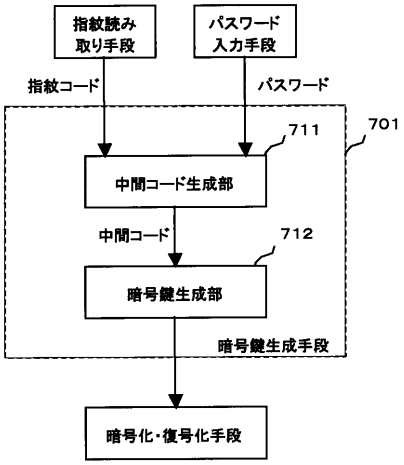
【図５】


3
2
1
0
(b)指紋の隆線方向の分類
領域2
領域1
領域3
領域4
(a)領域の分割方法
1
3
(c)領域の指紋の隆線の方向を求める
(d)指紋コードの生成
領域1 領域2 領域3 領域4
11 01 11 01 (2進数)
d d (16進数)

【図６】


START
601
前処理
602
指紋の領域分割
603
領域毎の特徴抽出しコード化
604
各領域からのコードを合成しコード化
605
合成したデータを指紋コードとして出力
END

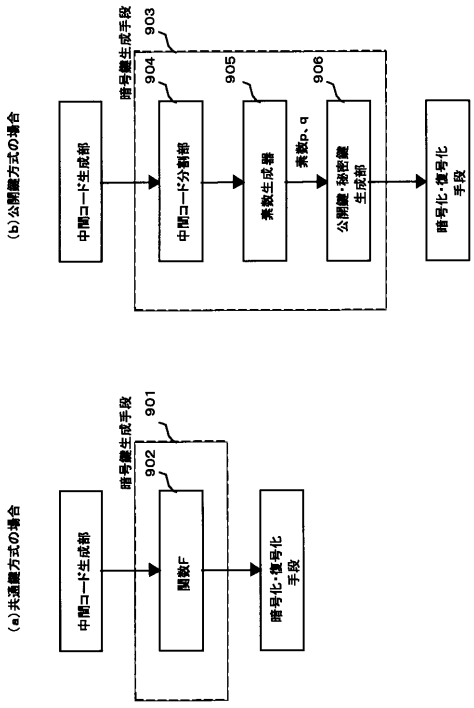
【図７】



【図８】

指紋コード	パスワード	中間コード
FE26	35BE	FE2635BE

【図９】



フロントページの続き

審査官　新田　亮

(56)参考文献　特開平１１－２６１５５０（ＪＰ，Ａ）
国際公開第９８／００１９７５（WO，Ａ１）
特開平０９－２７４４３１（ＪＰ，Ａ）
特開平０４－０５２９７５（ＪＰ，Ａ）
特開平０６－０９８１７９（ＪＰ，Ａ）
国際公開第９９／０３５７８６（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/32