(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2008-217300
(P2008-217300A)
(43)公開日　平成20年9月18日(2008.9.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	530D	5B017
H04L 9/32	(2006.01)	G06F	12/14	540A	5J104
G09C 1/00	(2006.01)	G06F	12/14	540P	
		G06F	12/14	560B	
		H04L	9/00	673D	

審査請求 未請求　請求項の数 7　OL　（全 19 頁）　最終頁に続く

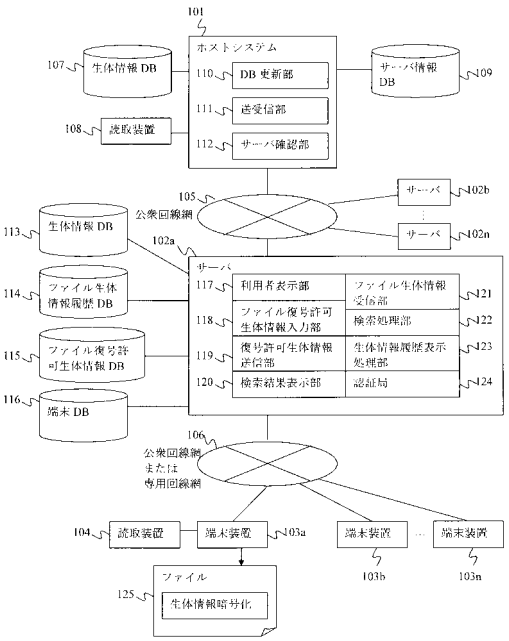
(21)出願番号　特願2007-52406(P2007-52406)
(22)出願日　平成19年3月2日(2007.3.2)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
東京都品川区東品川四丁目１２番７号
(74)代理人　100096954
弁理士　矢島　保夫
(72)発明者　遠藤　亨
東京都品川区東品川４丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Fターム(参考)　5B017 AA03　BA05　BA07　CA16
5J104 AA07　KA01　KA16　PA07　PA14

(54)【発明の名称】生体情報付きファイル暗号化システム及び復号化システム、並びにその方法

(57)【要約】
【課題】ファイルにアクセスすることのできる利用者の生体情報をファイル自身に設定することで、ファイルが仮に高セキュリティエリアから持ち出されても、アクセスすることができないような、生体情報付きファイル暗号化及び復号化の技術を提供することを目的とする。
【解決手段】端末に生体情報の読取装置を取付け、ファイル単位に使用できる利用者の生体情報を設定し、設定した利用者以外はファイルにアクセスできないようにする。ファイルを開くときには、設定された利用者であるかを判定する。利用者の生体情報とファイルの情報は端末に格納され、操作履歴はサーバに送信される。それらの情報を検索することで、ファイルの操作履歴を把握できる。ファイル単位に復号可能な生体情報を設定するため、物理的な高セキュリティエリアからファイルが持ち出されても、第三者がアクセスすることができない強固なセキュリティが実現できる。
【選択図】図１



【特許請求の範囲】
【請求項１】
ファイルを暗号化する生体情報付きファイル暗号化システムであって、
暗号化されていないファイルデータ本体を所定のファイル暗号化鍵で暗号化し、暗号化ファイルデータ本体を生成する手段と、
前記暗号化ファイルデータ本体に、当該ファイルの復号を許可する全ての利用者の生体情報を有するファイル復号許可生体情報データを付加する手段と、
前記ファイル復号許可生体情報データが付加された暗号化ファイルデータ本体を、所定の暗号化鍵で暗号化して、生体情報付き暗号化ファイルを作成する手段と
を備えることを特徴とする生体情報付きファイル暗号化システム。
【請求項２】
請求項１に記載の生体情報付き暗号化システムにより暗号化された生体情報付き暗号化ファイルを復号する生体情報付きファイル復号化システムであって、
前記暗号化鍵に対応する復号化鍵を取得する手段と、
取得した復号化鍵を用いて前記生体情報付き暗号化ファイルを復号し、前記ファイル復号許可生体情報データと暗号化ファイルデータ本体とを取得する手段と、
利用者の生体情報を取得する手段と、
前記取得した生体情報が前記ファイル復号許可生体情報データ内に含まれているか否かを判定する手段と、
前記取得した生体情報が前記ファイル復号許可生体情報データ内に含まれている場合のみ、前記暗号化ファイルデータ本体を復号するためのファイル復号化鍵を取得し、該ファイル復号化鍵を用いて、前記暗号化ファイルデータ本体を復号する手段と
を備えることを特徴とする生体情報付きファイル復号化システム。
【請求項３】
ファイルを暗号化する生体情報付きファイル暗号化システムであって、
ネットワークに接続されたサーバと端末装置とを備え、
前記サーバは、
前記端末装置からの要求に応じて暗号化鍵を送信する手段
を備え、
前記端末装置は、
前記サーバから暗号化鍵を取得する手段と、
ファイルの復号を許可する利用者の指定を受け付ける手段と、
指定された利用者全ての生体情報を有するファイル復号許可生体情報データを生成する手段と、
前記サーバから取得した暗号化鍵と前記ファイル復号許可生体情報データからファイル暗号化鍵を生成する手段と、
暗号化されていないファイルデータ本体を前記ファイル暗号化鍵で暗号化し、暗号化ファイルデータ本体を生成する手段と、
前記暗号化ファイルデータ本体に前記ファイル復号許可生体情報データを付加する手段と、
前記ファイル復号許可生体情報データが付加された暗号化ファイルデータ本体を、前記サーバから取得した暗号化鍵で暗号化して、生体情報付き暗号化ファイルを作成する手段と
を備えることを特徴とする生体情報付きファイル暗号化システム。
【請求項４】
請求項３に記載の生体情報付きファイル暗号化システムにより暗号化された生体情報付き暗号化ファイルを復号する生体情報付きファイル復号化システムであって、
ネットワークに接続されたサーバと端末装置とを備え、
前記サーバは、
前記端末装置からの要求に応じて、前記暗号化に使用した暗号化鍵に対応する復号化

鍵を送信する手段
を備え、
前記端末装置は、
前記サーバから前記復号化鍵を取得する手段と、
取得した復号化鍵を用いて前記生体情報付き暗号化ファイルを復号し、前記ファイル復号許可生体情報データと暗号化ファイルデータ本体とを取得する手段と、
利用者の生体情報を取得する手段と、
前記利用者の生体情報が前記ファイル復号許可生体情報データ内に含まれているか否かを判定する手段と、
前記利用者の生体情報が前記ファイル復号許可生体情報データ内に含まれている場合のみ、前記サーバから取得した復号化鍵と前記ファイル復号許可生体情報データから、前記暗号化ファイルデータ本体を復号するためのファイル復号鍵を生成する手段と、
生成したファイル復号鍵を用いて、前記暗号化ファイルデータ本体を復号する手段と
を備えることを特徴とする生体情報付きファイル復号化システム。
【請求項５】
請求項４に記載の生体情報付きファイル復号化システムにおいて、
前記端末装置は、前記生体情報付き暗号化ファイルを対象として行われた操作履歴、及び該操作が行われたときの利用者の生体情報を、前記サーバに送信する手段を備え、
前記サーバは、前記端末装置から送信される操作履歴及び前記利用者の生体情報を、ファイル生体情報履歴データベースに格納する手段を備えることを特徴とする生体情報付きファイル復号化システム。
【請求項６】
ファイルを暗号化する生体情報付きファイル暗号化方法であって、
ネットワークにサーバと端末装置とを接続するとともに、
前記端末装置から前記サーバに暗号化鍵の取得要求を送信する工程と、
前記暗号化鍵の取得要求に応じて、前記サーバが暗号化鍵を送信する工程と、
前記サーバから送信される暗号化鍵を前記端末装置で受信する工程と、
前記端末装置が、ファイルの復号を許可する利用者の指定を受け付ける工程と、
前記端末装置が、前記指定された利用者全ての生体情報を有するファイル復号許可生体情報データを生成する工程と、
前記端末装置が、前記サーバから取得した暗号化鍵と前記ファイル復号許可生体情報データから、ファイル暗号化鍵を生成する工程と、
前記端末装置が、暗号化されていないファイルデータ本体を前記ファイル暗号化鍵で暗号化する工程と、
前記端末装置が、前記暗号化ファイルデータ本体に前記ファイル復号許可生体情報データを付加する工程と、
前記端末装置が、前記ファイル復号許可生体情報データが付加された暗号化ファイルデータ本体を、前記サーバから取得した暗号化鍵で暗号化して、生体情報付き暗号化ファイルを作成する工程と
を備えることを特徴とする生体情報付きファイル暗号化方法。
【請求項７】
請求項６に記載の生体情報付きファイル暗号化方法により暗号化された生体情報付き暗号化ファイルを復号する生体情報付きファイル復号化方法であって、
前記生体情報付き暗号化ファイルの復号を希望する端末装置が、前記サーバに、復号化鍵の取得要求を送信する工程と、
前記復号化鍵の取得要求に応じて、前記サーバが、前記暗号化鍵に対応する復号化鍵を送信する工程と、
前記サーバから送信される復号化鍵を前記端末装置で受信する工程と、
前記端末装置が、前記復号化鍵を用いて前記生体情報付き暗号化ファイルを復号し、前記ファイル復号許可生体情報データと暗号化ファイルデータ本体とを取得する工程と、

前記端末装置が、利用者の生体情報を取得する工程と、
前記端末装置が、前記利用者の生体情報が前記ファイル復号許可生体情報データ内に含まれているか否かを判定する工程と、
前記端末装置が、利用者の生体情報が前記ファイル復号許可生体情報データ内に含まれている場合のみ、前記サーバから取得した復号化鍵と前記ファイル復号許可生体情報データから、前記暗号化ファイルデータ本体部分を復号するためのファイル復号化鍵を生成する工程と、
前記端末装置が、生成したファイル復号化鍵を用いて、前記暗号化ファイルデータ本体を復号する工程と
を備えることを特徴とする生体情報付きファイル復号化方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、固定型あるいは移動型の端末装置のフォルダやファイルに対する生体情報付きファイル暗号化及び復号化の技術に関するものである。
【背景技術】
【０００２】
端末装置の小型化と大容量化、及びネットワーク技術の進歩に伴い、ファイルの複製や移動が容易にできるようになっている。例えば、端末本体に対して着脱可能な携帯型の記憶媒体にファイルを格納して携帯し、自宅にて作業を行ったり、或いは、ネットワーク回線を使用して最新のファイルをダウンロードしたりするなどの様々な応用が可能になってきている。
【０００３】
その一方で、近年、機密データの持ち出しや盗難による顧客データの漏洩等による深刻な被害が後を絶たない。このような、機密データのアクセス管理については、従来から様々な提案がなされている。例えば、機密データへアクセスできる端末を予め特定し、その端末を生体認証などが必要な物理的な高セキュリティエリアに配置する方式や、ファイルに対して利用者単位に詳細なアクセス権を設定してアクセスさせる方式などである。
【０００４】
なお、生体情報を利用したファイル暗号化については下記特許文献１に記載のような技術が知られている。これはファイルの暗号化に生体情報を利用するが、そのファイル自体に生体情報を埋め込むものではない。
【特許文献１】特開２００６－１２６８９１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ところで、生体認証を使用した高セキュリティエリア内の特定の端末装置内で、かつ詳細なアクセス権が設定されたファイルであったとしても、一度持ち出されてしまったファイルに関しては、不特定多数の利用者がアクセスすることが可能となり、データの漏洩が発生する。このため、ファイルに対するアクセス履歴を管理することによって、高セキュリティエリアに入る人のモラルを向上させたり、高セキュリティエリアに入るときに複数人で入り、持ち出しを抑制するような運用が実施されたりしている。しかし、それにもかかわらず、高セキュリティエリアに入ることができる人によって、顧客データなどが持ち出され、刑事事件まで発生するケースが生じている。
【０００６】
また、ファイルに対して、利用者単位にアクセス権を設定してアクセスさせる方式は、予め利用者単位で設定されたパスワードで端末にログイン認証することが前提である。しかし、パスワードは忘却によって、本人でも認証できなくなったり、第三者にパスワードが盗難され認証される恐れがある。
【０００７】

本発明の目的は、ファイルにアクセスすることのできる利用者の生体情報をファイル自身に設定することで、ファイルが仮に高セキュリティエリアから持ち出されても、アクセスすることができないような、生体情報付きファイル暗号化及び復号化の技術を提供することにある。

【課題を解決するための手段】

【０００８】

上記目的を達成するため、本発明は、ファイルデータ本体を所定のファイル暗号鍵で暗号化し、前記暗号化ファイルデータ本体に、当該ファイルの復号を許可する全ての利用者の生体情報を有するファイル復号許可生体情報データを付加し、前記ファイル復号許可生体情報データが付加された暗号化ファイルデータ本体を所定の暗号化鍵で暗号化して、生体情報付き暗号化ファイルを作成することを特徴とする。

【０００９】

また、本発明は、そのような生体情報付き暗号化ファイルを復号する際、前記暗号化鍵に対応する復号化鍵を取得し、取得した復号化鍵を用いて前記生体情報付き暗号化ファイルを復号し、前記ファイル復号許可生体情報データと暗号化ファイルデータ本体とを取得し、利用者の生体情報を取得し、前記利用者が、前記ファイル復号許可生体情報が示すファイルの復号を許可する利用者に含まれているか否かを判定し、含まれている場合のみ、前記暗号化ファイルデータ本体を復号するためのファイル復号鍵を取得し、該ファイル復号鍵を用いて、前記暗号化ファイルデータ本体を復号することを特徴とする。

【００１０】

また、本発明は、ネットワークにサーバと端末装置とを接続したシステムで、前記端末装置から前記サーバに暗号化鍵の取得要求を送信し、前記暗号化鍵の取得要求に応じて、前記サーバが暗号化鍵を送信し、前記サーバから送信される暗号化鍵を前記端末装置で受信し、前記端末装置で、ファイルの復号を許可する利用者を示すファイル復号許可生体情報を入力し、前記サーバから取得した暗号化鍵と前記ファイル復号許可生体情報から、ファイル暗号化鍵を生成し、暗号化されていないファイルデータ本体を前記ファイル暗号鍵で暗号化し、前記暗号化ファイルデータ本体に、当該ファイルの復号を許可する利用者を示すファイル復号許可生体情報を付加し、前記ファイル復号許可生体情報が付加された暗号化ファイルデータ本体を、前記サーバから取得した暗号化鍵で暗号化して、生体情報付き暗号化ファイルを作成することを特徴とする。

【００１１】

また、本発明は、前記生体情報付き暗号化ファイルを復号する際、前記端末装置から前記サーバに復号化鍵の取得要求を送信し、前記復号化鍵の取得要求に応じて、前記サーバが前記暗号化鍵に対応する復号化鍵を送信し、前記サーバから送信される復号化鍵を前記端末装置で受信し、前記端末装置で、前記復号化鍵を用いて前記生体情報付き暗号化ファイルを復号し、前記ファイル復号許可生体情報と暗号化ファイルデータ本体とを取得し、利用者の生体情報を取得し、前記利用者が前記ファイル復号許可生体情報が示すファイルの復号を許可する利用者に含まれているか否かを判定し、利用者が前記復号を許可する利用者に含まれている場合のみ、前記サーバから取得した復号化鍵と前記ファイル復号許可生体情報から、前記暗号化ファイルデータ本体部分を復号するためのファイル復号化鍵を生成し、生成したファイル復号化鍵を用いて、前記暗号化ファイルデータ本体を復号することを特徴とする。

【００１２】

さらに、前記端末装置は、前記生体情報付き暗号化ファイルを対象として行われた操作履歴、及び該操作が行われたときの該利用者の生体情報を、前記サーバに送信し、前記サーバは、前記端末装置から送信される操作履歴及び前記利用者の生体情報を、ファイル生体情報履歴データベースに格納するようにしてもよい。

【発明の効果】

【００１３】

本発明によれば、次のような効果がある。

（１）高セキュリティエリア外へファイルが持ち出されても、第三者によるファイルへのアクセスを防止することができる。
（２）利用者を認証する手段が生体情報のため、パスワードの盗難等による第三者への情報漏えいを防止することができる。
（３）持ち出されたファイルのファイル名を変更したり、コピーされた場合であってもファイルのアクセス権は維持できる。
（４）持ち出されたファイルの操作履歴を調べることができる。
（５）ファイルに設定する生体情報は、ホストシステムから随時受信できる。
（６）ホストシステムにて、サーバの契約情報を保持しているため、契約者以外からの最新の生体情報要求を排除することができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明を適用した生体情報付きファイル暗号化及び複合化システムの一実施の形態について説明する。

【００１５】

図１は、本発明の一実施形態を示すシステム構成図である。この実施形態の生体情報付き暗号化及び複合化システムは、生体情報データベース107を備えたホストシステム101と、このホストシステム101から生体情報を受信する複数のサーバ102a、102b、…、及び102nと、生体情報を取得する為の読取装置104を備えた複数のクライアント端末装置103a、103b、…、及び103nを備えている。サーバ102a、102b、…、及び102nの台数は任意である。任意の１台のサーバを指すときは「サーバ102」と呼ぶものとする。端末装置103a、103b、…、及び103nの台数も任意である。任意の１台の端末装置を指すときは「端末装置103」と呼ぶものとする。

【００１６】

図１のホストシステム101には、生体情報データベース107の他に、生体情報を取得する為の読取装置108と、生体情報暗号化契約者のサーバ情報を格納するサーバ情報データベース109とが接続されている。ホストシステム101の生体情報データベース107には、例えば、生体情報ＩＤ、生体情報、及び利用者名などを含む生体情報データが登録されている。生体情報は、例えば読取装置108によりすべての利用者から取得し、生体情報ＩＤなどと対応づけて生体情報データベース107へ登録する。サーバ情報データベース109には、生体情報暗号化契約者の契約情報が登録される。生体情報暗号化契約者の契約情報は、契約者の情報、サーバの情報、接続可能な端末装置数、及び契約期間などを含んでおり、これらの情報はサーバ102に生体情報を送信するときなどに使用される。なお、読取装置108は、利用者の便宜のために、複数箇所に設けられ、ネットワーク経由でホストシステム101に送信される等の構成となっていてもよい。

【００１７】

また、ホストシステム101は、生体情報データベース107やサーバ情報データベース109の更新処理を行うデータベース更新部110と、サーバ102から送られる主に生体情報データの更新要求の処理などを行う送受信部111と、サーバ情報データベース109に生体情報暗号化契約者を登録し、生体情報データの更新要求をするサーバがその契約者かどうか確認するサーバ確認部112とを備えている。

【００１８】

サーバ102aには、ホストシステム101から配信された生体情報データとその最新登録更新日時などを格納する生体情報データベース113と、端末装置103のファイルの生体情報履歴データを保存するファイル生体情報履歴データベース114と、ファイル単位のファイル復号許可生体情報を格納するファイル復号許可生体情報データベース115と、契約された端末台数を管理し、生体情報データを送信するための端末情報を格納する端末データベース116とが接続されている。

【００１９】

生体情報データベース113には、ホストシステム101から受信した生体情報データとその

生体情報データの登録更新日時などが登録されている。サーバ102aに設定された時間間隔（その時間間隔は、管理者が任意に設定できる）で、サーバ102aは、ホストシステム101に接続し、前回取得した生体情報から更新された部分の生体情報を受信し、生体情報データベース113を定期的に更新する。

【００２０】

ファイル生体情報履歴データベース114には、複数の端末装置103a、103b、…、及び103nの生体情報付き暗号化ファイルの生体情報履歴データが登録されている。ファイル生体情報履歴データベース114に格納されるデータは、本システムで管理する対象となる生体情報付き暗号化ファイルに対するアクセス履歴のデータである。この生体情報履歴データは、端末装置103から、ある特定のタイミングでサーバ102aに送信され、ファイル生体情報履歴データベース114に格納される。そのため、このファイル生体情報履歴データベース114を参照することで、どのファイルがいつどこの端末で誰にアクセスされたのか参照が可能となる。

【００２１】

ファイル復号許可生体情報データベース115には、端末装置103a、103b、…、及び103nで作成された生体情報付き暗号化ファイルの復号を許可する利用者の生体情報が登録されている。本データベース115に登録されるファイル復号許可生体情報は、サーバ102の管理者や端末装置103の利用者が、特定のファイルを指定して、当該ファイルの復号を許可する利用者を設定する為のデータである。例えば、端末装置103aのシステムファイルに対してファイル復号許可利用者を設定すると、端末装置103aのシステムファイルが暗号化されるため、端末装置103aを使用することのできる利用者を管理者側から設定することが可能になる。

【００２２】

端末データベース116には、複数の端末装置103a、103b、…、及び103nの固有の情報が登録されており、これによりサーバ102aは、契約した台数の端末装置（本サーバ102aの管理下にある端末装置）に対してのみ、生体情報付き暗号化及び復号化サービスを提供することができるようになっている。

【００２３】

また、サーバ102aは、生体情報データベース113に生体情報が登録されている利用者の一覧を表示するための利用者表示部117と、管理者により指定された復号を許可する利用者の生体情報を生体情報データベース113から読み出し、読み出した生体情報からファイル復号許可生体情報データを生成し、ファイル復号許可生体情報データベース115にそのファイル復号許可生体情報データを格納するファイル復号許可生体情報入力部118と、ファイル復号許可生体情報データベース115と端末データベース116からファイルの復号を許可する生体情報（利用者）を取得し、端末装置103に送信する復号許可生体情報送信部119と、複数の端末装置103a、103b、…、及び103nからファイルの生体情報履歴データを受信するファイル生体情報受信部121と、生体情報データベース113、ファイル生体情報履歴データベース114、ファイル復号許可生体情報データベース115、及び端末データベース116の内容を検索する検索処理部122と、その検索結果を表示する検索結果表示部120と、ファイル生体情報履歴データベース114からファイルの生体情報の履歴を読み出して表示する生体情報履歴表示処理部123と、端末装置103に暗号化鍵及び復号化鍵を発行する認証局124とを備えている。なお、任意台数の他のサーバ102b～102nも同様の構成である。

【００２４】

図１の端末装置103aには、サーバ102の認証局124から送信された暗号化鍵と生体情報により暗号化された複数の生体情報付き暗号化ファイル125と、端末装置103aで利用者の生体情報を取得するための読取装置104が設けられている。端末装置103a内のファイル125は、サーバ102の認証局124にて発行された暗号化鍵を使用して、特定の利用者でのみ復号し使用することができるように暗号化されている。ファイル125の暗号化は、端末装置103aの利用者からの指令により行うこともできるし、サーバ102の管理者からの指令により行うこともできる。なお、任意台数の他の端末装置103b～103nも同様の構成である。

【００２５】
図１のネットワーク105には、ホストシステム101と生体情報暗号化を契約した複数のサーバ102a、102b、…、及び102nとが接続され、必要に応じて、サーバ102上の生体情報情報を更新できるように構成されている。ネットワーク106には、サーバ102と契約した接続可能端末装置台数以内の端末装置103a、103b、…、及び103nが接続され、端末内の生体情報暗号化ファイルの履歴などがサーバ102に送信でき、サーバ102上の生体情報データやファイル復号許可生体情報や認証局から発行された暗号鍵や復号鍵などが端末装置103に送信できるように構成されている。
【００２６】
なお、ホストシステム101は、本発明に係る生体情報付きファイル暗号化及び復号化技術を利用したサービスを提供するサービス提供会社のものを想定している。このサービスを受けたい会社等は、当該サービス提供会社にサービスの提供を申し込むことにより生体情報暗号化契約者となる。サーバ102は、当該生体情報暗号化契約者が保有するもの、或いはサービス提供会社から当該生体情報暗号化契約者に提供されたものを想定している。端末装置103の各利用者は、生体情報暗号化契約者となった会社等の例えば社員である。
【００２７】
図２は、図１の端末装置103の詳細な構成図である。端末装置201は、サーバ102から送られた生体情報データを格納するための生体情報データベース202と、生体情報によって暗号化されたファイルのアクセス履歴を格納するためのファイル生体情報履歴データベース203と、利用者の生体情報を取得する為の読取装置204（図１の104）と、サーバ102の認証局124にて発行された暗号化鍵を使用して、生体情報によって暗号化されたファイル205（図１の125）とを備えている。
【００２８】
さらに、端末装置201は、生体情報データベース202に生体情報が格納されている利用者の一覧を表示するための利用者表示部206と、読取装置204から利用者の生体情報を取得する生体情報取得部207と、生体情報を使用してファイルを暗号化処理する暗号化部209及び復号化処理する復号化部210を備えたファイル処理部208と、サーバ102に対してファイルの生体情報履歴を送信するための生体情報履歴送信部211と、ファイルの復号許可生体情報などを入力する入力部212とを備えている。
【００２９】
図２の生体情報データベース202には、図１のサーバ102から受信した生体情報データとその生体情報データの登録更新日時などが格納されている。端末装置201またはサーバ102に設定された時間間隔（その時間間隔は、サーバ102の管理者または端末201の利用者が任意に設定できる）で、端末装置201は、サーバ102に接続し、生体情報データの更新された部分を受信し、生体情報データベース202を定期的に更新する。
【００３０】
図３は、図１のホストシステム101の生体情報データベース107に格納される生体情報及び生体情報関連情報のデータテーブルである。生体情報データベース107は、生体情報ID301、利用者名302、生体情報303、登録日時304、及び区分305の各フィールドを持つ。生体情報303は、利用者から読み取った生体情報そのものであり、例えば指紋、静脈、虹彩のパターン情報などである。生体情報ID301は当該生体情報を一意に特定するＩＤであり、利用者名302はその利用者の名称である。登録日時304には、当該生体情報を登録または更新した日時が格納される。区分305は、当該レコードが生体情報を格納したレコードであることを示すために”生体情報”が格納される。
【００３１】
なお、サーバ102に接続される生体情報データベース113及び端末装置201（103）に接続される生体情報データベース202も図３に示したのと同じデータ形式である。本実施形態では、初めに、生体情報暗号化契約者である会社等に属する全利用者の生体情報をホストシステム101の読取装置108で読み取り、生体情報データベース107に格納することを前提としている。ホストシステム101の生体情報データベース107に全利用者の生体情報が格納

された状態で、生体情報暗号化契約者に係るサーバ102を追加するとき、後述する図８のステップ804で、当該サーバ102に対応する生体情報暗号化契約者である会社等の管理下にある全利用者の生体情報をホストの生体情報データベース107から読み出して、サーバ102の生体情報データベース113に格納する。また、サーバ102に接続する端末装置103を追加するとき、後述する図９のステップ906におけるインストール処理で、当該サーバ102の生体情報データベース107に格納されている生体情報を全て、追加した端末装置103の生体情報データベース202にコピーする。端末装置103の生体情報データベース202やサーバ102の生体情報データベース107は、ファイルの暗号化を行う場合に、そのファイルの復号を許可する利用者の生体情報をファイルに付加する際に参照するものである。

【００３２】

図４は、ホストシステム101のサーバ情報データベース109に格納される生体情報暗号化契約者の契約情報の構成例を示す。生体情報暗号化契約者の契約情報は、契約者ID401、契約者名402、代表契約者住所403、契約形態404、契約期日405、プロダクトキー406、及び接続端末台数407で構成され、それぞれ、契約者ごとの一意のID、契約者名あるいは法人名、代表契約者の住所、契約の形態、生体情報データと生体情報関連情報を送信する契約の期間、サーバを一意に指定するプロダクトキー、及びサーバに接続する端末装置台数が登録される。

【００３３】

契約形態404は、サーバ102の構成方法による契約形態を示す。この契約形態は、例えば、サーバのパフォーマンス向上やサーバの故障発生時の対処の為に、複数のサーバで１つのサービスを提供するフォールトトレランスを取るサーバの構成や、サーバ1台のみでサービスを提供するサーバの構成など、クライアントのサーバ構成に対応するために使用される。

【００３４】

図５は、図１のサーバ102のファイル生体情報履歴データベース114に格納されるファイル生体情報履歴データの構成例を示す。ファイル生体情報履歴データは、ファイル識別子501、年月日502、生体情報データ503、ファイル名称504、利用者操作505、及び利用者名506で構成され、それぞれ、全てのシステムにおいて一意なファイルを特定するための識別子、端末装置から当該ファイル生体情報履歴データの送られた年月日と時間、端末で読み取った利用者の生体情報、拡張子付のファイル名称、本ファイル生体情報履歴データを送るきっかけとなった利用者の操作内容、及びその利用者名が登録される。

【００３５】

このファイル生体情報履歴データは、端末装置103において生体情報付き暗号化ファイルに対して何らかの利用者操作が行われたときに、該端末装置103からサーバ102に送信されファイル生体情報履歴データベース114に格納される。端末装置103からサーバ102にファイル生体情報履歴データを送るきっかけとなる利用者操作としては、生体情報付き暗号化ファイルに対する「データ読み取り」、「データ書き込み」、「ファイル削除」、「ファイル名変更」、及び「ファイルコピー」などの操作がある。また、この利用者操作としては、「定期送信」（厳密には利用者操作ではないが）や「ネットワーク接続開始時」も含むものとする。「定期送信」とは、定期的（その周期は利用者が設定できる）に端末装置103の全生体情報付き暗号化ファイルについてのファイル情報をサーバ102に送る場合のことである。「ネットワーク接続開始時」とは、端末装置103がネットワーク106に接続開始したときに該端末装置103の全生体情報付き暗号化ファイルについてのファイル情報をサーバ102に送る場合のことである。これらの利用者操作があった場合、端末装置103は、その操作に係る図５で説明したファイル生体情報履歴データ（利用者操作505には、契機となった利用者操作を記載する）をサーバ102に送信する。サーバ102は、送られてきたファイル生体情報履歴データをファイル生体情報履歴データベース114に格納する。

【００３６】

ファイル識別子501は、端末装置の「ＭＡＣアドレス」、「システム時間」、及び「ファイル名称」の各データを使用して作成される。生体情報付き暗号化ファイルがコピーさ

れた場合は、コピー先の生体情報付き暗号化ファイルに対応するファイル生体情報履歴データが作成されるが、「コピー先のファイル識別子」は「コピー元のファイル識別子」を使用して作成され、「コピー先のファイル識別子」を見れば「コピー元のファイル識別子」が分るようになっている。従って、ファイルがコピーされた場合であっても、コピー元ファイルの場所を特定することが可能となる。「ＭＡＣアドレス」は端末単位に一意であり、「システム時間」もまた刻々と変化するため、全てのシステムを通じて同一のファイル識別子は存在しなくなる。

【００３７】

また、ファイル識別子501は、ファイル名称を変更した場合は変更されない。例えば、ファイル名称504が「生体情報暗号化基本設計書.txt」である生体情報付き暗号化ファイルを「20050804_生体情報暗号化基本設計書.txt」と名称変更した場合であっても、同一のファイル識別子のままとなる。

【００３８】

図６に、サーバ102のファイル復号許可生体情報データベース115に格納されるファイル復号許可生体情報の構成例を示す。ファイル復号許可生体情報は、ファイル識別子601、ファイルパス602、生体情報データ603、及び暗号化フラグ604で構成され、それぞれ、ファイルを特定するための識別子、生体情報による暗号化を行うファイルのパス、ファイルの復号を許可する利用者の生体情報の配列、及びファイルが暗号化されているか否かを示すフラグ情報が登録される。

【００３９】

ファイル識別子601は、生体情報による暗号化を行うファイルのパスが設定されたときに、端末データベース116にアクセスし、該当する端末装置の「ＭＡＣアドレス」、「システム時間」、及び「ファイル名称」等を使用して生成する。

【００４０】

ファイル復号許可生体情報データベース115は、サーバ102の管理者または端末装置103の利用者が特定のファイルを指定してアクセス権を設定するときに使用するものである。例えば、端末装置103aのシステムファイルに対して、特定の利用者でのみ復号可能なアクセス権を設定することで、端末装置103aを使用することのできる利用者を設定することが可能になる。

【００４１】

なお、サーバ102の管理者が端末装置103の特定のファイルを指定しそのファイル復号許可生体情報を設定して暗号化する場合、まずサーバ102の管理者は、サーバ102にて端末装置103と該端末装置103のどのファイルを暗号化するのかを指定する。これにより、ファイル復号許可生体情報データベース115に、指定されたファイルのファイル復号許可生体情報が設定される。この時点で、ファイル識別子601とファイルパス602には、指定されたファイルのファイル識別子とファイルパスが設定される。次に、管理者は、利用者表示部117を使用して、生体情報データベース113に登録されている利用者の一覧から当該ファイルの復号を許可する利用者を全て指定する。サーバ102は、指定された利用者の生体情報を生体情報データベース113から読み出し、配列としてまとめ、生体情報データ603として設定する。また、この時点で、暗号化フラグ604は「暗号化未実施」と設定する。その後、適当なタイミングでサーバ102と当該ファイルを持つ端末装置103とが通信可能なときに、サーバ102から当該端末装置103に当該ファイルの暗号化指令を送信する。この暗号化指令は、上記ファイル復号許可生体情報データ603を含むものである。端末装置103は、該暗号化指令を受信すると、後述する図１１の処理を行って（ただし、ファイルの復号を許可する利用者は、既に管理者が指定してあり、そのファイル復号許可生体情報データ603は暗号化指令に含めてあるので、ステップ1103ではそのファイル復号許可生体情報データ603が利用される）、当該ファイルを暗号化し、生体情報付き暗号化ファイルとする。暗号化の処理が終わったら、端末装置103がその旨をサーバ102に通知する。サーバ102は、該通知を受けて、当該ファイルに関するファイル復号許可生体情報の暗号化フラグ604を「暗号化実施済み」と設定する。

【００４２】
また、端末装置103の利用者が自ら自端末装置内のファイルを指定して暗号化する場合、まず該利用者は、端末装置103にて、どのファイルを暗号化するのかを指定する。この指定が為されると、後述する図１１の処理が実行され、当該ファイルが生体情報付き暗号化ファイルとされる。その後、端末装置103は、暗号化したファイルのファイル識別子、ファイルパス、及び復号を許可する利用者を示す生体情報データを、サーバ102に通知する。サーバ102は、該通知を受けて、当該ファイルに関するファイル復号許可生体情報をファイル復号許可生体情報データベース115に登録する。その際、暗号化フラグ604は「暗号化実施済み」とする。
【００４３】
図７に、サーバ102の端末データベース116に格納される端末装置の情報の構成例を示す。端末装置の情報は、端末装置識別子701、端末名702、及びＭＡＣアドレス703で構成され、それぞれ、サーバによって払い出される端末装置に格納されている端末装置識別子の値、端末名、及びＭＡＣアドレスが登録される。端末装置識別子701の値は、端末装置103に本生体情報暗号化システムに係るソフトウェアをインストールしたときに、サーバ102から当該端末装置103に払い出された値であり、インストールが完了したタイミングでサーバ102の端末データベース116に格納される。
【００４４】
以下、以上のように構成された生体情報暗号化及び復号化システムの動作を説明する。
【００４５】
図８は、ホストシステム101におけるサーバ情報追加処理の概要を示すフローチャートである。この処理は、新たなサーバ102を追加するとき（すなわち、新たな生体情報暗号化契約者を登録するとき）に実行される。
【００４６】
まず、ホストシステム101のサーバ情報データベース109（図４）に新規レコードを追加し、該レコードに、該契約者の「契約者ID」、「契約者名」、「代表契約者住所」、「契約形態」、「契約期日」、及び「接続端末台数」を登録する（ステップ801）。これらの情報は、ホストシステム101において入力された情報を登録すればよいが、その契約者が以前に契約をしていて「契約者名」及び「代表契約者住所」などが分っている場合は、それらの情報を用いてもよい。サーバ情報データベース109への登録が終了したら、ホストシステム101は、登録された情報に従って「プロダクトキー」を生成し払い出す（ステップ802）。払い出された「プロダクトキー」は、サーバ情報データベース109の当該レコードに登録するとともに、ネットワーク105経由で当該契約者のサーバ102にインストール指令とともに送信される。サーバ102は、このインストール指令に応じて、ホストシステム101によって払い出されたプロダクトキーを使用して、生体情報付きファイル暗号化システムをインストールする（ステップ803）。このインストールにより、図１に示したサーバ102と該サーバ102に接続された各ＤＢの構成が実装される。サーバ102は、生体情報付きファイル暗号化システムのインストールが終了した後、ホストシステム101に、当該プロダクトキーを送信する。
【００４７】
ホストシステム101は、サーバ102から送信されたプロダクトキーの情報と、サーバ情報データベース109に登録したプロダクトキーとを、サーバ確認部112にて比較する。一致したならば、当該サーバが適正に追加されたということであるから、契約形態に従って、送受信部111により、生体情報データベース107の生体情報データをサーバ102に送信する。サーバ102はその生体情報データを受信し、生体情報データベース113に生体情報データとデータ登録日などを格納する（ステップ804）。以上でサーバ情報の追加処理を終える。なお、ホストシステム101からサーバ102に送信される生体情報データは、当該サーバ102に対応する生体情報暗号化契約者の管理下にある利用者（端末装置103）の生体情報のみである。
【００４８】

図９は、端末装置追加処理の概要を示すフローチャートである。この処理は、追加する端末装置103からサーバ102に接続し、生体情報付きファイル暗号化システムをインストールするためのプログラムを取得し、当該端末装置103上で実行することにより開始する。

【００４９】

生体情報付きファイル暗号化システムをインストールするためのプログラムは、まず、本端末装置103のMACアドレスと端末装置名をネットワーク106経由でサーバ102に送信する(ステップ901)。サーバ102では、受け取った端末装置のMACアドレスと端末データベース116（図７）に既に登録されているMACアドレスデータとを比較し、同じMACアドレスがあれば、生体情報付きファイル暗号化システムを既にインストール済みと判定し、なければインストール未実施と判定する（ステップ902）。

【００５０】

インストール未実施であれば、新規端末である為、端末データベース116に登録されている端末装置の数が契約で当該サーバに許されている接続端末台数（図４の407）以上か判定する（ステップ903）。端末データベース116に登録されている端末装置の数が契約端末台数以上である場合は、既に契約台数分の端末に対して生体情報付きファイル暗号化システムがインストールされていると判定されるので、端末の新規追加は不可となり、インストールは失敗として終了する（ステップ905）。端末データベース116に登録されている端末装置の数が契約端末台数以上でない場合は、サーバ102にて端末装置識別子を生成し、端末データベース116（図７）に当該端末の端末装置情報を追加する（ステップ904）。ステップ904の後、またはステップ902で当該端末103が生体情報付きファイル暗号化システムをインストール済みの場合は、サーバ102から当該端末103に対して生体情報付きファイル暗号化システムのプログラムと生体情報データを送信し、当該端末103に生体情報付きファイル暗号化システム（端末版）をインストールする（ステップ906）。このインストールにより、図２に示した端末装置201と該端末装置201に接続された各ＤＢの構成が実装される。なお、ステップ902からステップ906に進む場合は、再インストールを行うことになる。

【００５１】

図１０は、サーバ102の生体情報データベース113上の生体情報データの更新処理を示すフローチャートである。

【００５２】

まず、システム日付（現在時）とサーバ102の生体情報データベース113の最新登録更新日とを比較し、サーバ102に前もって設定してある生体情報の更新期間が経過したか判定する（ステップ1001）。サーバ102に前もって設定してある生体情報の更新期間が経過していた場合、サーバ102は、ホストシステム101に接続し、プロダクトキー（図８のステップ802で当該サーバ102に払い出されているもの）を送信する。ホストシステム101は、サーバ確認部112で、サーバ情報データベース109（図４）に格納されている当該サーバ102の契約期間が切れていないか判定する（ステップ1002）。

【００５３】

契約期間が切れていない場合、当該サーバ102の最新の生体情報データベース更新日をホストシステム101に送信し、ホストシステム101の生体情報データベース107（図３）にサーバ102の最新の生体情報データベース登録更新日よりも新しい生体情報データがあるか判定する（ステップ1003）。ホストシステム101の生体情報データベース107にサーバ102の最新の生体情報データベース登録更新日よりも新しい生体情報データがある場合、ホストシステム101から最新の生体情報データを取得し、サーバ102の生体情報データベース113を更新する（ステップ1004）。

【００５４】

なお、サーバがフォールトトレランス構成の場合は、1台のメインサーバがホストシステムに接続し、他のサーバはメインサーバに接続して、生体情報データを更新することもできる。

【００５５】

図１１は、端末装置201（図１の103）の暗号化処理部209にて実行するファイルの暗号化処理を示すフローチャートである。まず、端末装置103が、サーバ102より、有効なファイルの暗号化鍵を取得済みか判定する（ステップ1101）。端末装置103が、サーバ102より有効な暗号化鍵を取得していない場合は、サーバ102に接続し、有効期限の切れていない暗号化鍵を取得する（ステップ1102）。端末装置103を使用してファイルを暗号化する利用者は、端末装置の利用者表示部206を使用して、暗号化するファイルの復号を許可する利用者を指定する（ステップ1103）。利用者表示部206は、生体情報データベース206に格納されている利用者名の一覧を表示するので、その一覧から、復号を許可する利用者（複数でも良い）を指定すればよい。端末装置103は、指定された利用者の生体情報を生体情報データベース206から全て読み出し、読み出した生体情報の配列を作ってファイル復号許可生体情報データ（図６の603に相当するデータ）を生成する。次に、端末装置103は、ファイルデータを暗号化するファイル暗号化鍵を、サーバ102から取得した暗号化鍵と前記ファイル復号許可生体情報データとを使用して作成する（ステップ1104）。すなわち、ファイルデータを暗号化する鍵は、ファイルを復号許可する生体情報を使用して随時作成される。ステップ1104で作成されたファイル暗号化鍵と、サーバから送信された暗号化鍵を使用して、ファイルを暗号化する（ステップ1105，1106）。

【００５６】

なお、図１１のステップ1102で端末装置103から暗号化鍵の取得要求を受けたサーバ102は、図７の端末データベース116を参照して、当該端末装置103が正式に登録されている端末であるか否かをチェックし、正式に登録されている端末であるときは、その端末装置103で暗号化に使用する暗号化鍵を生成して送信する。サーバ102は、その暗号化鍵を、端末装置103と対応させて、所定のデータベース（図７の端末データベース116でもよい）に記憶し管理する。

【００５７】

図１２は、端末装置103の暗号化処理部209にて実行されるステップ1105及び1106の生体情報暗号化処理で、ファイルデータが暗号化されていく様子を示す。図１２(a)のファイルデータ部1201は、暗号化する対象のファイルデータを示す。このファイルデータ部1201は、サーバ102から送信された暗号化鍵とファイルの復号を許可する利用者の生体情報から作成したファイル復号許可生体情報データとから生成されたファイル暗号化鍵によって暗号化される。図１２(b)の1202が、暗号化されたファイルデータ部を示す。次に、図１２(c)に示すように、暗号化されたファイルデータ部1202に、前記ファイル復号許可生体情報データ1203を付加する。この暗号化されたファイルデータ部1202とファイル復号許可生体情報データ部1203を、サーバ102から送信された暗号化鍵を使用して暗号化し、生体情報付き暗号化ファイル1204を作成する（図１２(d)）。

【００５８】

図１３は、端末装置201（103）の復号化処理部210にて実行される生体情報付き暗号化ファイルの復号化処理を示すフローチャートである。まず、端末装置103が、サーバ102より、有効なファイルの復号化鍵を取得済みか判定する（ステップ1301）。サーバ102から有効な復号化鍵を取得していない場合は、サーバ102に接続して、復号化鍵を取得する（ステップ1302）。

【００５９】

次に、端末装置103で利用者の生体情報を取得するため、端末装置の生体情報取得部207にて、読取装置204に接続し、利用者の生体情報を取得する（ステップ1303）。復号対象の生体情報付き暗号化ファイルをサーバ102から送信された復号化鍵を使用して復号化し、ファイルの復号許可生体情報（図１２(c)のファイル復号許可生体情報部1203）と暗号化されたファイルデータ部（図１２(c)のファイルデータ部1202）を取得する。読取装置204から取得した利用者の生体情報が当該ファイルの復号許可生体情報内にあるか判定する（ステップ1304）。利用者の生体情報がファイルの復号許可生体情報内にない場合は、復号を許可せず、ステップ1301に戻る。利用者の生体情報が当該ファイルの復号許可生体情報内にある場合は、サーバ102から取得した復号化鍵とファイルの復号許可生体情報とを

使用して、ファイル復号鍵を作成する（ステップ1305）。対象のファイルデータをファイル復号鍵を使用して復号する（ステップ1306）。

【００６０】

なお、図１３のステップ1302で端末装置103から復号化鍵の取得要求を受けたサーバ102は、図７の端末データベース116を参照して、当該端末装置103が正式に登録されている端末であるか否かをチェックし、正式に登録されている端末であるときは、その端末装置103で復号化に使用する復号化鍵を送信する。この復号化鍵は、図１１のステップ1102でサーバ102から当該端末装置103に送られた暗号化鍵に対応する復号化鍵である。

【００６１】

以上のように、本実施形態の生体情報暗号化システムによれば次のような効果がある。

（１）高セキュリティエリア外へファイルが持ち出されても、第三者によるファイルへのアクセスを防止することができる。

（２）利用者を認証する手段が生体情報のため、パスワードの盗難等による第三者への情報漏えいを防止することができる。

（３）持ち出されたファイルのファイル名を変更したり、コピーされた場合であってもファイルのアクセス権は維持できる。

（４）持ち出されたファイルの操作履歴を調べることができる。

（５）ファイルに設定する生体情報は、ホストシステムから随時受信できる。

（６）ホストシステムにて、サーバの契約情報を保持しているため、契約者以外からの最新の生体情報要求を排除することができる。

【００６２】

なお、上記実施の形態ではファイルを暗号化する例を説明したが、ファイルの代りにフォルダを指定し、そのフォルダ内の全ファイルを同様に暗号化するようにしてもよい。また、上記実施形態では、端末装置がサーバと通信して暗号化や復号化を行っているが、ネットワークに接続されていない端末装置に対して本発明を適用することもできる。暗号化や復号化を行う前に、サーバから暗号化鍵や復号化鍵を取得しておき、暗号化では図１１のステップ1101からステップ1102をスキップしてステップ1103移行の処理を行い、復号化では図１３のステップ1301からステップ1302をスキップしてステップ1303移行の処理を行えば良い。また、ネットワークに接続されていない端末装置で、生体情報付き暗号化ファイルを操作した場合は、その履歴を端末装置内に記憶しておき、あとでネットワークに接続されたときに、記憶されている履歴情報をサーバに送り図５のファイル生体情報履歴データベース114に格納するようにしても良い。

【００６３】

さらに、上記実施形態では、サーバから取得した暗号化鍵とファイル復号許可生体情報データとからファイル暗号化鍵を生成しているが、この方式に限らず、別の方式でファイル暗号化鍵を生成しても良い。

【００６４】

上記実施形態では、生体情報暗号化契約者である会社等に属する全利用者の生体情報をホストシステム101の読取装置108で読み取り、生体情報データベース107に格納することを前提としているが、例えば、本サービスを提供するサービス提供会社の担当者が生体情報暗号化契約者である会社等に出向いて、全利用者の生体情報を収集し、持ち帰ってホストシステム101の生体情報データベース107に格納するようにしてもよい。また、各利用者が端末からホストシステム101にネットワーク経由で接続し、生体情報を登録更新できるようにしてもよい。

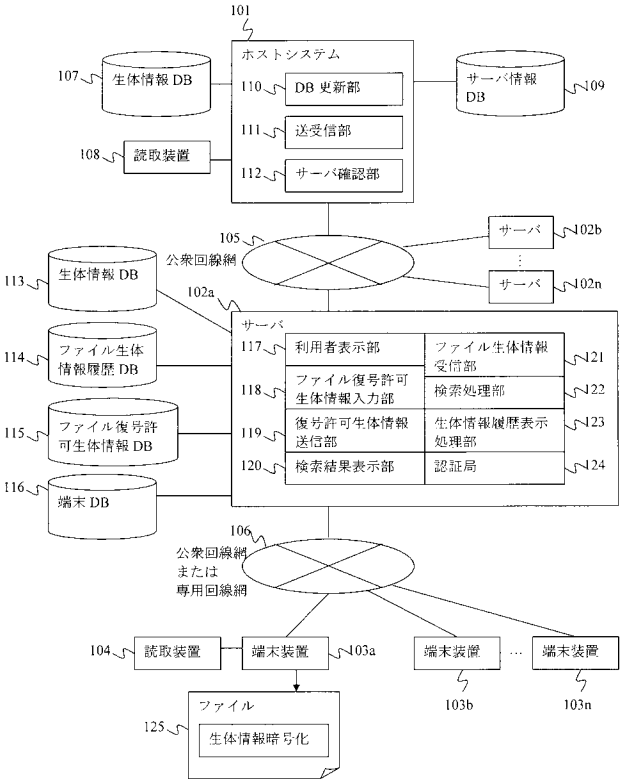
【００６５】

上記実施形態では、各端末103に生体情報データベース202を設けているが、該データベース202を設ける代わりに、端末103から生体情報にアクセスしたい場合には、ネットワーク経由でサーバ102に接続されている生体情報データベース113のデータを使用するようにしても良い。

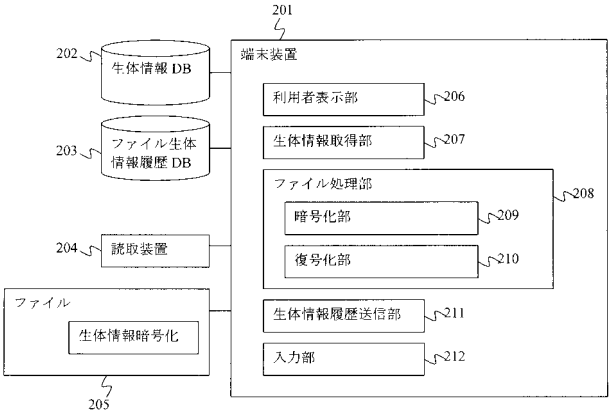
【図面の簡単な説明】

【００６６】
【図１】本発明の一実施形態例を示すシステム構成図である。
【図２】端末装置の構成図である。
【図３】ホストシステムの生体情報データベースに格納される生体情報データ及び生体情報関連情報のデータテーブルである。
【図４】ホストシステムのサーバ情報データベースに格納される生体情報暗号化契約者の契約情報データの構成図である。
【図５】サーバのファイル生体情報履歴データベースに格納されるファイル生体情報履歴情報データの構成図である。
【図６】サーバのファイル復号許可生体情報データベースに格納されるファイルの復号許可生体情報の構成図である。
【図７】サーバの端末データベースに格納される端末装置の情報データの構成図である。
【図８】サーバ情報追加処理の概要を示すフローチャートである。
【図９】端末装置追加処理の概要を示すフローチャートである。
【図１０】サーバの生体情報情報データの更新処理を示すフローチャートである。
【図１１】端末装置の暗号化処理部にて実行されるファイルの暗号化処理を示すフローチャートである。
【図１２】端末装置の暗号化処理部にて実行されるファイルの暗号化処理の様子を示す概要図である。
【図１３】端末装置の復号化処理部にて実行されるファイルの位置復号化処理を示すフローチャートである。
【符号の説明】
【００６７】
101…ホストシステム、107…生体情報データベース、108…更新部分生体情報データベース、109…サーバ情報データベース、110…データベース更新部、111…送受信部、112…サーバ確認部、105,106…ネットワーク、102a、102b、及び102n…サーバ、103a、103b、及び103n…端末装置。

【図１】



【図２】



【図３】

301	生体情報 ID	0010030031122333398
302	利用者名	Abcdefg001
303	生体情報	(生体情報)
304	登録日時	2006 年 8 月 31 日 00 時 00 分 00 秒
305	区分	生体情報

【図４】

401	契約者 ID	0000000000001
402	契約者名	○○○　○○○
403	代表契約者住所	神奈川県横浜市保土ヶ谷区
404	契約形態	A
405	契約期日	2006 年 9 月 1 日～2006 年 8 月 31 日
406	プロダクトキー	QKA4 - 1FAJF - 5RIFE - 34BQBF
407	接続端末台数	10000

【図５】

501	ファイル識別子	{fjla13-32jib-hmci-lapkn-09322-kbabx}
502	年月日	2005 年 8 月 4 日 9:17:18
503	生体情報データ	(端末で読み取った生体情報)
504	ファイル名称	生体情報暗号化基本設計書.txt
505	利用者操作	読み取り
506	利用者名	Abcdefg001

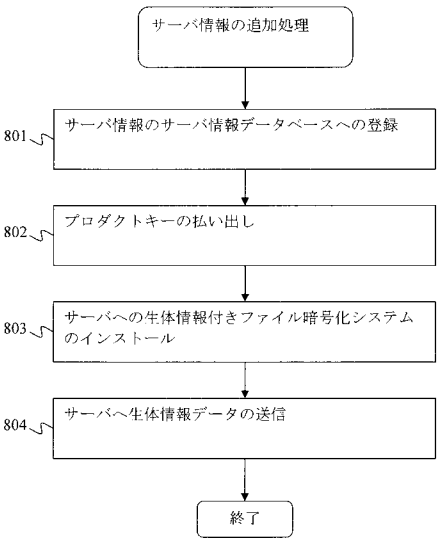
【図６】

601	ファイル識別子	{fjla13-32jib-hmci-lapkn-09322-kbabx}
602	ファイルパス	¥¥abcded¥c$¥ c$¥WINDOWS¥system32¥ bootcfg.e
603	生体情報データ	(許可する生体情報の配列)
604	暗号化フラグ	暗号化未実施

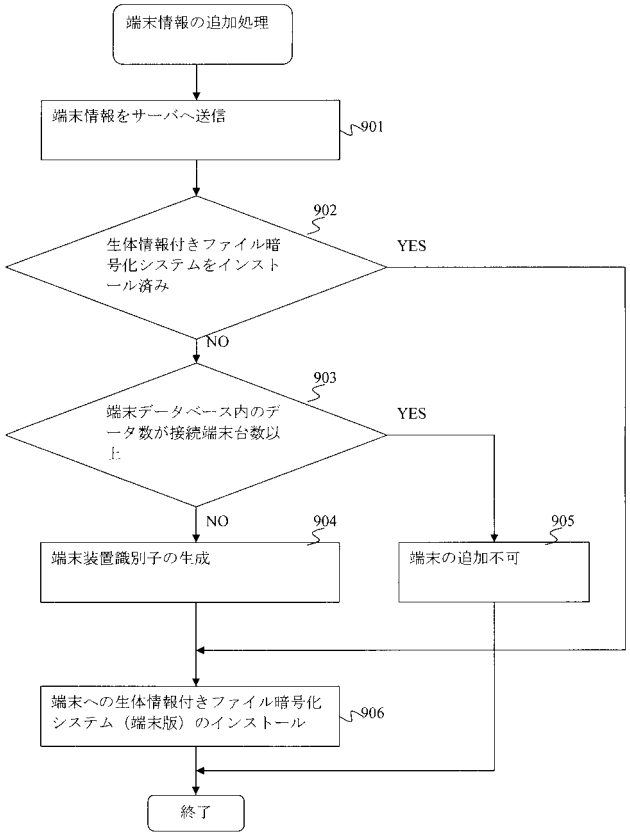
【図７】

701	端末装置識別子	{lcbe9-bi3kn-ckso0-76ma }
702	端末名	AABC-DDEE01
703	MAC アドレス	00-00-E2-93-CB-CC

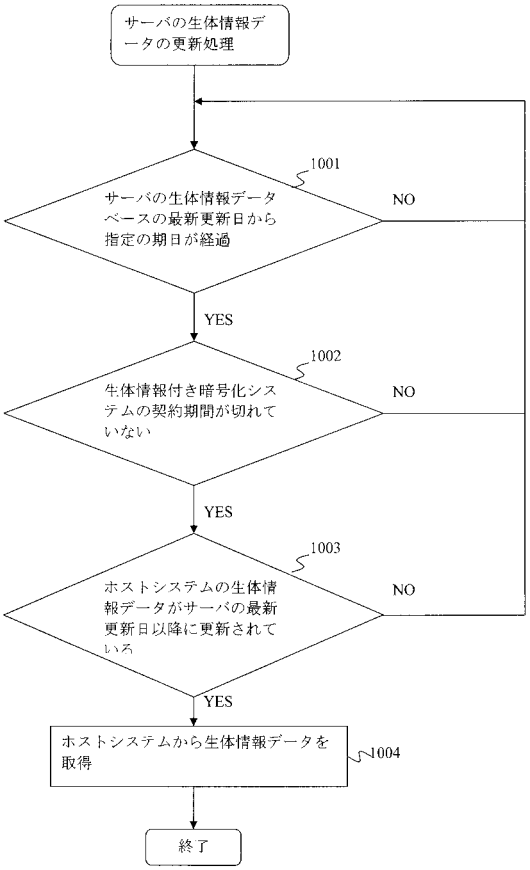
【図８】


サーバ情報の追加処理
801
サーバ情報のサーバ情報データベースへの登録
802
プロダクトキーの払い出し
803
サーバへの生体情報付きファイル暗号化システムのインストール
804
サーバへ生体情報データの送信
終了

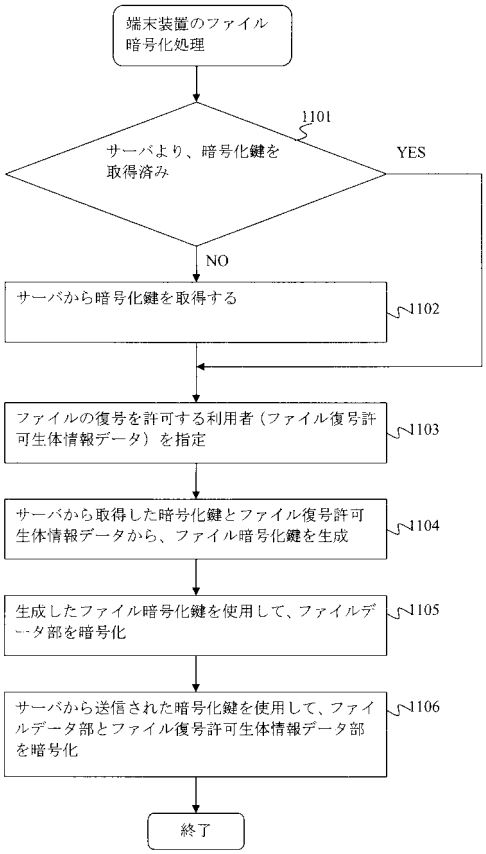
【図９】


端末情報の追加処理
端末情報をサーバへ送信
901
902
生体情報付きファイル暗号化システムをインストール済み
YES
NO
903
端末データベース内のデータ数が接続端末台数以上
YES
NO
904
端末装置識別子の生成
905
端末の追加不可
端末への生体情報付きファイル暗号化システム（端末版）のインストール
906
終了

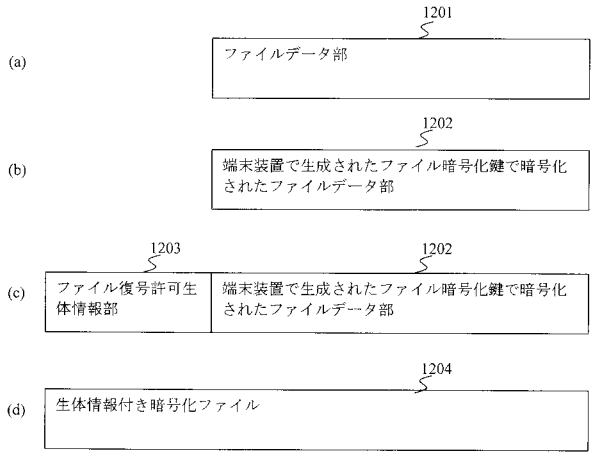
【図１０】


サーバの生体情報データの更新処理
1001
サーバの生体情報データベースの最新更新日から指定の期日が経過
NO
YES
1002
生体情報付き暗号化システムの契約期間が切れていない
NO
YES
1003
ホストシステムの生体情報データがサーバの最新更新日以降に更新されている
NO
YES
ホストシステムから生体情報データを取得
1004
終了

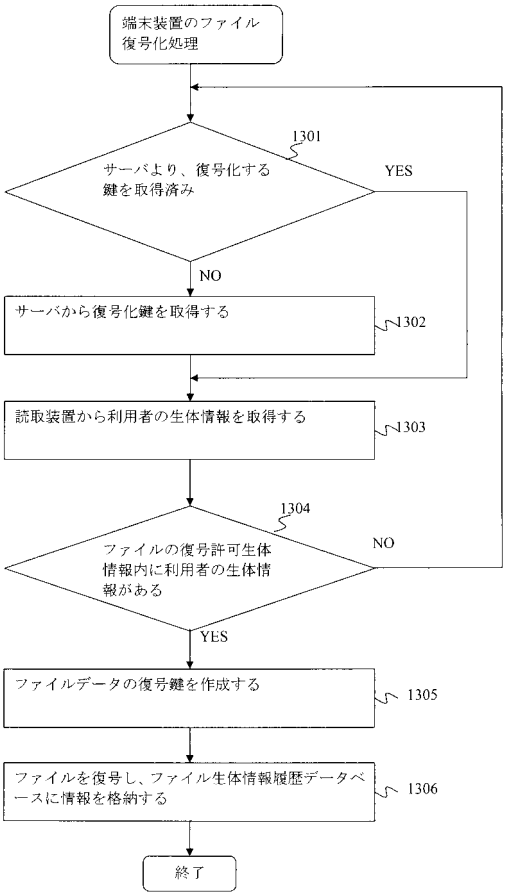
【図１１】


端末装置のファイル暗号化処理
1101
サーバより、暗号化鍵を取得済み
YES
NO
サーバから暗号化鍵を取得する
1102
ファイルの復号を許可する利用者（ファイル復号許可生体情報データ）を指定
1103
サーバから取得した暗号化鍵とファイル復号許可生体情報データから、ファイル暗号化鍵を生成
1104
生成したファイル暗号化鍵を使用して、ファイルデータ部を暗号化
1105
サーバから送信された暗号化鍵を使用して、ファイルデータ部とファイル復号許可生体情報データ部を暗号化
1106
終了

【図１２】


(a)
1201
ファイルデータ部
(b)
1202
端末装置で生成されたファイル暗号化鍵で暗号化されたファイルデータ部
(c)
1203
ファイル復号許可生体情報部
1202
端末装置で生成されたファイル暗号化鍵で暗号化されたファイルデータ部
(d)
1204
生体情報付き暗号化ファイル

【図１３】


端末装置のファイル復号化処理
1301
サーバより、復号化する鍵を取得済み
YES
NO
サーバから復号化鍵を取得する
1302
読取装置から利用者の生体情報を取得する
1303
1304
ファイルの復号許可生体情報内に利用者の生体情報がある
NO
YES
ファイルデータの復号鍵を作成する
1305
ファイルを復号し、ファイル生体情報履歴データベースに情報を格納する
1306
終了

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	G09C 1/00 660D	