

明 細 書

発明の名称： 情報送受信システム

技術分野

[0001] 本発明の実施形態は、情報送受信システムに関する。

背景技術

[0002] 従来、機密情報などを電子メールで送信する場合、パスワードを設定した機密情報を含む電子データとしてのファイルを電子メールに添付する形で送信することが多い。このような場合、送信者は、電子メールに添付したファイルに設定したパスワードを当該電子メールとは別の送信方法で送信先の相手（受信者）に通知する。

[0003] しかしながら、電子メールに添付されたファイルに設定されたパスワードは、当該電子メールとは別の送信方法で受信者に通知されるため、喪失してしまうことがある。当然ながら、パスワードを喪失すると、パスワードが設定されファイルは、開くことができなくなる。このため、電子メールに添付するファイルなどの電子データを安全に送受信でき、かつ、受信者が確実にデータを開くことができるシステムが要望されている。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開2013-152511号公報

発明の概要

発明が解決しようとする課題

[0005] 上記した課題を解決するために、安全に電子データを送受信でき、受信者が確実に電子データを取得できる情報送受信システムを提供する。

課題を解決するための手段

[0006] 実施形態によれば、情報送受信システムは、送信装置と受信装置とを有する。受信装置は、第1の通信部とインターフェースと記憶部と第1のプロセッサとを有する。送信装置は、第2の通信部と第2のプロセッサとを有する

。第1の通信部は、送信装置と通信する。インターフェースは、受信者の生体認証を行う生体認証装置に接続する。記憶部は、生体認証装置によって生体認証が成功した受信者の第1鍵と第1鍵に対応する第2鍵とを記憶する。第1のプロセッサは、送信装置が受信者の第2鍵で施錠した電子データを保存し、生体認証装置によって生体認証が成功した受信者の第1鍵を用いて受信者の第2鍵で施錠された電子データを解錠する。第2の通信部は、受信装置と通信する。第2のプロセッサは、受信者の第2鍵で施錠した電子データを受信装置へ送信する。

図面の簡単な説明

[0007] [図1] 図1は、実施形態に係る情報送受信システムの構成例を概略的に示す図である。

[図2] 図2は、実施形態に係る情報送受信システムにおける送信装置の構成例を示すブロック図である。

[図3] 図3は、実施形態に係る情報送受信システムにおける受信装置の構成例を示すブロック図である。

[図4] 図4は、実施形態に係る情報送受信システムにおける第1動作例を概略的に説明するための図である。

[図5] 図5は、実施形態に係る情報送受信システムにおける第1動作例を説明するためのシーケンスである。

[図6] 図6は、実施形態に係る情報送受信システムにおける第2動作例を概略的に説明するための図である。

[図7] 図7は、実施形態に係る情報送受信システムにおける第2動作例を説明するためのシーケンスである。

[図8] 図8は、実施形態に係る情報送受信システムにおける第3動作例を概略的に説明するための図である。

[図9] 図9は、実施形態に係る情報送受信システムにおける第3動作例を説明するためのシーケンスである。

[図10] 図10は、実施形態に係る情報送受信システムにおける第4動作例を

概略的に説明するための図である。

[図11]図 1 1 は、実施形態に係る情報送受信システムにおける第 4 動作例を説明するためのシーケンスである。

[図12]図 1 2 は、実施形態に係る情報送受信システムにおける第 5 動作例を概略的に説明するための図である。

[図13]図 1 3 は、実施形態に係る情報送受信システムにおける第 5 動作例を説明するためのシーケンスである。

[図14]図 1 4 は、実施形態に係る情報送受信システムにおける第 5 動作例を説明するためのシーケンスである。

実施形態

[0008] 以下、実施形態について、図面を参照しつつ説明する。

まず、実施形態に係る情報送受信システムに用いる認証デバイスの発行（登録）手続きについて説明する。

図 1 は、実施形態に係る情報送受信システムの構成例を概略的に示す図である。

図 1 に示す構成例において、情報送受信システム 1 は、送信装置 1 1、および、受信装置 1 2 を有する。送信装置 1 1 と受信装置 1 2 とは、メールサーバ 1 3、1 4 およびネットワーク 1 5 を介して保護対象とする電子データとしてのファイルを添付した電子メールの送受信を行う。また、情報送受信システム 1 において、送信装置 1 1 と受信装置 1 2 とは、メールサーバ 1 3、1 4 を介さずに保護対象とする電子データを送受信するようにしても良い。

[0009] 送信装置 1 1 は、電子メールを送信する送信者が使用する端末装置である。受信装置 1 2 は、電子メールを受信する受信者が使用する端末装置である。送信装置 1 1 および受信装置 1 2 は、電子データを送受信する機能を有する電子装置である。例えば、送信装置 1 1 および受信装置 1 2 は、電子メールを送受信するためのアプリケーションプログラムがインストールされたパーソナルコンピュータ（PC）、スマートフォン、通信装置などである。

[0010] 送信装置 1 1 および受信装置 1 2 は、生体情報によってユーザ認証を行う生体認証を実行する生体認証装置を接続するインターフェースを備える。また、送信装置 1 1 および受信装置 1 2 は、生体情報によってユーザ認証を行う生体認証を実行する生体認証部を備える構成であっても良い。なお、送信者の生体認証が不要な運用として実施される情報送受信システム 1 であれば、送信装置 1 1 は、生体認証装置を接続しなくても良い。

[0011] 次に、実施形態に係る情報送受信システム 1 における送信装置 1 1 の構成について説明する。

図 2 は、実施形態に係る情報送受信システム 1 における送信装置 1 1 の構成例を示すブロック図である。

図 2 に示すように、送信装置 1 1 は、プロセッサ 2 1、ROM 2 2、RAM 2 3、記憶部 2 4、通信部 2 5、操作部 2 7、表示部 2 8 およびインターフェース 2 9 を有する。

[0012] プロセッサ 2 1 は、プログラムを実行することにより各種の処理を実行する。プロセッサ 2 1 は、例えば、CPU (Central Processing Unit) である。プロセッサ 2 1 は、システムバスを介して送信装置 1 1 内の各部と接続され、各部との間でデータを送受信する。プロセッサ 2 1 は、ROM 2 2 および RAM 2 3 と協働して送信装置 1 1 における制御およびデータ処理などの動作を実行する。

[0013] ROM (Read Only Memory) 2 2 は、送信装置 1 1 の基本的な動作を実行するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

RAM (Random Access Memory) 2 3 は、データを一時的に記憶する揮発性のメモリである。RAM 2 3 は、プロセッサ 2 1 がプログラムを実行する場合にワーキングメモリとして機能する。

[0014] 記憶部 2 4 は、各種のデータを記憶するメモリである。記憶部 2 4 は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、記憶部 2 4 は、OS プログラム、アプリケーションプログラム、動作設定情報などを

記憶する。本実施形態において、記憶部 24 は、電子メールを送受信するためのプログラム、鍵情報を用いたデータ処理を実行するためのプログラム、および、後述する各種の処理を実行するためのプログラムなどが記憶されるものとする。

[0015] また、記憶部 24 は、セキュアな記憶領域を有し、送信者が保持しておくべき鍵情報（例えば、送信者の公開鍵および秘密鍵）などの情報をセキュアに記憶するものとする。また、記憶部 34 は、当該送信装置 11 を使用するユーザである登録者（送信者）の生体情報（生体認証に用いる生体情報）を記憶するようにしても良いし、送信者が保持しておくべき鍵情報（例えば、送信者の第 1 鍵および第 2 鍵）などをセキュアな記憶領域に保持するようにしても良い。

[0016] 通信部 25 は、外部装置と通信するための通信インターフェースである。通信部 25 は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。本実施形態において、通信部 25 は、メールサーバ 13 およびネットワーク 15 を介して受信装置 12 宛の電子メールを送信する。

[0017] 操作部 27 は、ユーザ（送信者）が操作指示を入力する入力デバイスである。操作部 27 は、例えば、キーボード、タッチパネル、マウスなどで構成される。表示部 28 は、情報を表示するディスプレイである。例えば、表示部 28 は、電子メールにファイルを添付して送信する場合に、送信先、添付するファイル、あるいは、ファイルに不可する条件情報などを指示するための設定画面などを表示する。また、操作部 27 および表示部 28 は、タッチパネル付きの表示装置によって構成しても良い。

[0018] インターフェース 29 は、外部装置を接続する。インターフェース 29 は、後述する受信装置 12 に接続される生体認証装置 40 と同様な構成で、送信装置 11 を操作するユーザである送信者に対する生体認証を実行する。また、送信装置 11 は、送信者に対する生体認証を実行する生体認証部を備える構成としても良い。

[0019] 次に、実施形態に係る情報送受信システム 1 における受信装置 12 の構成

について説明する。

図3は、実施形態に係る情報送受信システム1における受信装置12の構成例を示すブロック図である。

図3に示すように、受信装置12は、プロセッサ31、ROM32、RAM33、記憶部34、通信部35、インターフェース36、操作部37および表示部38を有する。

[0020] プロセッサ31は、プログラムを実行することにより各種の処理を実行する。プロセッサ31は、例えば、CPU (Central Processing Unit) である。プロセッサ31は、システムバスを介して受信装置12内の各部と接続され、各部との間でデータを送受信する。プロセッサ31は、ROM32およびRAM33と協働して受信装置12における制御およびデータ処理などの動作を実行する。

[0021] ROM (Read Only Memory) 32は、受信装置12の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

RAM (Random Access Memory) 33は、データを一時的に記憶する揮発性のメモリである。RAM33は、プロセッサ31がプログラムを実行する場合にワーキングメモリとして機能する。

[0022] 記憶部34は、各種のデータを記憶するメモリである。記憶部34は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、記憶部34は、OSプログラム、アプリケーションプログラム、動作設定情報などを記憶する。本実施形態において、記憶部24は、電子メールを送受信するためのプログラム、鍵情報を用いたデータ処理を実行するためのプログラム、および、後述する各種の処理を実行するためのプログラムなどが記憶されるものとする。また、記憶部24は、セキュアな記憶領域を有し、受信者が保持しておくべき鍵情報（例えば、受信者の第1鍵および第2鍵）などがセキュアな記憶領域に記憶されるものとする。また、記憶部34は、当該受信装置を使用するユーザである登録者（受信者）の生体情報を記憶するようにし

ても良い。

[0023] 通信部 35 は、外部装置と通信するための通信インターフェースである。通信部 35 は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。本実施形態において、通信部 35 は、インターネットなどの広域のネットワーク 15 を介して、送信装置 11 と通信する。

[0024] インターフェース 36 は、外部装置を接続する。図 3 に示す例において、インターフェース 36 は、生体認証装置 40 を接続する。生体認証装置 40 は、生体センサ 41 を備える。生体認証装置 40 は、生体センサ 41 が取得する生体情報に基づく人物認証（生体認証）を実行する。生体センサ 41 は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。生体認証装置 40 は、生体センサ 41 が読み取る生体情報と予め登録されている登録者であるユーザ（受信者）の生体情報と照合することにより、生体センサ 41 が生体情報を読み取った人物が予め登録されているユーザ（受信者）であることを認証する。

[0025] 生体センサ 41 は、例えば、利用者の指紋情報（指紋画像）を読み取る指紋センサである。生体センサ 41 は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、顔画像、掌紋、静脈、虹彩等）を取得するセンサであっても良い。生体認証装置 40 は、生体センサ 41 が取得する生体情報に対応した生体認証を実行する機能（例えば、指紋照合、顔照合、掌紋照合、静脈照合、虹彩照合等を実行する IC チップ）を備える。

[0026] なお、生体認証装置 40 は、生体センサ 41 が取得する生体情報をプロセッサ 31 へ供給するものとし、生体センサ 41 が取得する生体情報に基づく生体認証をプロセッサ 31 が実行する構成としても良い。

また、受信装置 12 は、生体認証装置 40 と同等の生体認証を実行する生体認証部を備える構成であっても良い。また、受信装置 12 は、生体認証に用いる登録者であるユーザ（受信者）の生体情報を記憶部 34 に登録するようにしても良いし、生体認証装置 40 に設けたメモリに登録するようにしても良い。

[0027] 操作部 37 は、ユーザが操作指示を入力する入力デバイスである。操作部 37 は、例えば、キーボード、タッチパネル、マウスなどである。表示部 38 は、情報を表示するディスプレイである。例えば、表示部 38 は、施錠されていたファイルを鍵データで開錠した場合にファイル内のデータを表示する。また、操作部 37 および表示部 38 は、タッチパネル付きの表示装置によって構成しても良い。

[0028] なお、情報送受信システム 1 は、受信装置 12 が受信する電子メールあるいは電子メールに添付されたファイルをファイルサーバなどの外部装置に保存する構成としても良い。この場合、受信装置 12 は、受信した電子メールあるいは電子メールに添付されたファイルを保存するための外部装置としてのファイルサーバにアクセスするためのインターフェースを備えるようにしても良い。

[0029] 次に、本実施形態に係る情報送受信システム 1 によるファイル（電子データ）の送受信処理について説明する。

まず、本実施形態に係る情報送受信システム 1 によるファイルの送受信処理の第 1 動作例について説明する。

図 4 は、実施形態に係る情報送受信システム 1 によるファイルの送受信処理の第 1 動作例を概略的に説明するための図である。

図 4 に示すように、第 1 動作例では、送信者 O が 1 人の受信者 A にファイルを送信する場合を想定して説明する。送信装置 11 は、送信者 O の公開鍵（公開鍵 O）と秘密鍵（秘密鍵 O）とを保持しているものとする。また、受信装置 12（12A）は、受信者 A の生体情報が登録され、受信者 A に対する生体認証が実行できるようになっているものとする。

[0030] まず、送信装置 11 は、ファイルを送信する前に、送信者 O の公開鍵 O を受信者 A の受信装置 12A に供給する。受信装置 12A は、送信者 O の公開鍵 O を取得すると、受信者 A であることを認証するための生体認証を実行する。生体認証が成功すると（受信者 A であることが確認されると）、受信装置 12A は、受信者 A の第 1 鍵 A と第 1 鍵 A に関する第 2 鍵 A とを生成する

。受信装置 1 2 A は、第 1 鍵および第 2 鍵 A を生成すると、第 2 鍵 A を公開鍵 O で暗号化したデータを送信装置 1 1 へ送信する。

[0031] 送信装置 1 1 は、受信装置 1 2 A から公開鍵 O で第 2 鍵 A を暗号化したデータを取得すると、公開鍵 O に対応する秘密鍵を用いて暗号化された第 2 鍵 A を復号化（解錠）することにより第 2 鍵 A を取得する。送信装置 1 1 は、第 2 鍵 A を取得すると、受信者 A へ送信すべきファイルを第 2 鍵 A で施錠（暗号化）する。送信装置 1 1 は、第 2 鍵 A で施錠したファイルを受信者 A の受信装置 1 2 A へ送信する。

[0032] 受信装置 1 2 A は、送信者 O から受信した第 2 鍵 A で施錠されたファイルを保存する。受信者 A は、第 2 鍵 A で施錠されたファイル（送信装置 1 1 から受信したファイル）を閲覧する場合、受信装置 1 2 A で生体認証を実行する。受信装置 1 2 A は、受信者 A による操作に応じて受信者 A の生体情報を取得して生体認証を実行する。生体認証により受信者 A であることが確認されると、受信装置 1 2 A は、受信者 A の第 1 鍵 A を取得し、受信者 A の第 1 鍵 A を用いて第 2 鍵 A で施錠されたファイルを解錠する。これにより、受信装置 1 2 A は、送信者 O から受信した第 2 鍵 A で施錠されたファイルを閲覧可能とする。

[0033] 次に、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 1 動作例における送信装置 1 1 および受信装置 1 2（1 2 A）の動作について説明する。

図 5 は、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 1 動作例における送信装置 1 1 と受信装置 1 2 A との動作例を説明するためのシーケンスである。

例えば、送信者 O は、送信装置 1 1 の操作部 2 7 により受信者 A にセキュリティ設定を施したファイル（保護対象となる電子データ）の送信を指示する。送信装置 1 1 のプロセッサ 2 1 は、送信者 O による操作指示に応じて送信先（受信者）および送信するファイルなどを設定する（S T 1 1）。

[0034] 送信装置 1 1 のプロセッサ 2 1 は、送信先として受信者 A を設定すると、

通信部 25 により受信者 A に対して送信者 O の公開鍵 O を送信（開示）し、受信者 A の受信装置 12 A が生体認証に紐づけて生成する第 2 鍵を要求する（ST 12）。例えば、プロセッサ 21 は、公開鍵 O を含む第 2 鍵 A の要求を受信者 A 宛の電子メールによって送信しても良い。第 2 鍵 A は、受信者 A の生体認証が成功した場合に生成される第 1 鍵 A に対応する鍵データであり、例えば、第 1 鍵 A から所定のアルゴリズムによって生成される。

[0035] 受信者 A の受信装置 12 A は、通信部 35 により送信者 O から受信者 A 宛の第 2 鍵の要求と公開鍵 O とを受信する。受信装置 12 A のプロセッサ 31 は、送信者 O からの第 2 鍵の要求を受信すると、インターフェース 36 に接続した生体認証装置 40 によって受信者 A の生体認証を実行する（ST 13）。プロセッサ 31 は、受信者 A に対する生体認証が成功すると、生体認証が成功した受信者 A の第 1 鍵 A を生成する（ST 13）。プロセッサ 31 は、第 1 鍵 A を生成すると、第 1 鍵 A と対になる第 2 鍵 A を生成する（ST 14）。すなわち、プロセッサ 31 は、受信者 A に対する生体認証の成功に応じて受信者 A 用の鍵のペアとして第 1 鍵 A と第 2 鍵 A とを生成する。例えば、プロセッサ 31 は、受信者 A に対する生体認証が成功した場合に読み出せるように第 1 鍵 A と第 2 鍵 A とを記憶部 34 に保存する。

[0036] 第 1 鍵 A は、例えば、受信者 A の生体情報などから特定のアルゴリズムによって生成される。また、第 1 鍵 A は、所定のアルゴリズムを用いることにより受信者 A の生体情報から再現できるようにしても良い。この場合、受信装置などの不具合によって第 1 鍵 A を喪失しても受信者 A の生体情報から第 1 鍵 A を取得することができる。また、第 2 鍵 A は、第 1 鍵 A から特定のアルゴリズムで生成される。例えば、第 2 鍵 A は、所定のアルゴリズムを用いることにより第 1 鍵 A から再現できるようにしても良い。この場合、受信装置などの不具合によって第 2 鍵 A を喪失しても第 1 鍵 A から第 2 鍵 A を取得することができる。

[0037] また、第 1 鍵 A は、受信者 A 以外はアクセスできないように秘匿した状態で保管され、受信者 A の生体認証が成功した場合にアクセスできるように保

存される。例えば、第1鍵A（又は、第1鍵Aおよび第2鍵A）は、受信装置12Aの記憶部34に保存されるものに限定されるものではなく、生体認証装置40内のメモリ又は外部記憶装置にセキュアに保管するようにしても良い。

[0038] 受信装置12Aのプロセッサ31は、第2鍵Aを生成すると、生成した第2鍵Aを公開鍵Oで暗号化（施錠）する（ST16）。プロセッサ31は、第2鍵Aを公開鍵Oで暗号化すると、通信部35により公開鍵Oで暗号化した第2鍵Aのデータを送信者Oの送信装置11へ送信する（ST17）。

[0039] 送信者Oの送信装置11は、通信部25により受信者Aの受信装置12Aが公開鍵Oで暗号化した第2鍵Aのデータを受信する。送信装置11のプロセッサ21は、公開鍵Oで暗号された第2鍵Aを受信すると、公開鍵Oに対応する秘密鍵Oにより公開鍵Oで暗号化（施錠）された第2鍵Aのデータを復号化（解錠）する（ST18）。プロセッサ21は、秘密鍵Oで復号化（解錠）したデータとして第2鍵Aを取得する（ST19）。

[0040] 送信装置11のプロセッサ21は、第2鍵Aを取得すると、取得した第2鍵Aに受信者Aに送信すべきファイルを暗号化（施錠）する（ST20）。プロセッサ21は、第2鍵Aでファイルを暗号化（施錠）すると、第2鍵Aで施錠したファイルを添付した電子メールを作成する。ここで、プロセッサ21は、送信者Oが受信者A宛の電子メールの本文を作成するようにしても良い。

[0041] また、プロセッサ21は、電子メールに添付する第2鍵Aで施錠したファイルに解錠条件（閲覧可能とする条件）を付加しても良い。例えば、プロセッサ21は、送信者Oが操作部27を用いて指定する解錠条件を第2鍵Aで施錠したファイルに対して設定する。解錠条件としては、第2鍵Aで施錠したファイルに対する解錠（閲覧）を可能とする期限であっても良いし、解錠を可能とする装置であっても良い。前者の場合、プロセッサ21は、例えば、送信者Oが操作部27を用いて指定する任意の期限を解錠期限（解錠条件）として設定するようにしても良い。また、後者の場合、プロセッサ21は

、例えば、公開鍵Oで暗号化した第2鍵Aの送信（生成）元である受信装置12を解錠可能な装置として設定するようにしても良い。

[0042] 送信装置11のプロセッサ21は、第2鍵Aで施錠したファイルを添付した受信者A宛の電子メールを作成すると、作成した受信者A宛の電子メールを通信部25によりメールサーバ13へ送信する（ST21）。メールサーバ13は、ネットワーク15を介してメールサーバ14へ受信者A宛の電子メールを送信する。メールサーバ14は、受信者A宛の電子メールを受信者Aの受信装置12へ送信する。

[0043] 受信装置12Aは、通信部35により第2鍵Aで施錠されたファイルが添付された受信者A宛の電子メールを受信する。受信装置12Aのプロセッサ31は、受信した電子メールに添付された第2鍵Aが施錠されたファイルを記憶部34に保存する（ST22）。プロセッサ31は、第2鍵Aで施錠されたファイルを添付された電子メールとともに保存しても良いし、第2鍵Aで施錠されたファイルを保存しても良い。また、プロセッサ31は、第2鍵Aで施錠されたファイルをファイルサーバなどの外部装置に保存するようにしても良い。

[0044] 受信装置12Aのプロセッサ31は、操作部37を操作する受信者Aによる保存した第2鍵Aで施錠されたファイルに対する解錠要求を受け付ける。ここで、プロセッサ31は、第2鍵Aで施錠されたファイルに解錠条件が設定されていれば、解錠要求を受けた場合に解錠条件を満たしているか否かによりファイルの解錠を受け付けるか否かを判断するようにしても良い。

[0045] 受信装置12Aのプロセッサ31は、解錠要求に応じてファイルの解錠を実行する場合（ST23、YES）、インターフェース36に接続した生体認証装置40による受信者Aの生体認証を実行する（ST24）。プロセッサ31は、受信者Aに対する生体認証が成功すると、生体認証が成功した受信者Aの第1鍵Aを取得する（ST25）。ここでは、公開鍵Oを受信した場合に実行した受信者Aの生体認証の成功に応じて生成した第2鍵Aと対になる第1鍵Aが記憶部34のセキュアな記憶領域に保存されているものとす

る。

[0046] 受信装置 12A のプロセッサ 21 は、第 1 鍵 A を取得すると、取得した第 1 鍵 A を用いて第 2 鍵 A で施錠されたファイルを解錠する (ST26)。プロセッサ 31 は、第 1 鍵 A を用いてファイルを解錠すると、解錠したファイルを開いて閲覧可能な状態とする (ST27)。例えば、プロセッサ 31 は、第 1 鍵 A で解錠したファイルのデータを表示部 38 に表示することによりファイルの内容を受信者 A に開示する。

[0047] 以上のような第 1 動作例によれば、実施形態に係る情報送受信システムは、送信者から受信者の生体認証で取得できる鍵で施錠されたファイルを受信でき、鍵で保護された状態のファイルを保存しておくことができる。受信者 A は、生体認証によって取得できる鍵によって任意のタイミングで保護されたファイルを取得することできる。この結果、実施形態に係る情報送受信システムによれば、パスワードなどを紛失でファイルが閲覧不可能となることがなく、閲覧権限のある人（生体認証を成功させることができる人）なら任意のタイミングで確実に閲覧可能とすることができる。

[0048] また、第 1 動作例として説明したように、実施形態に係る情報送受信システムでは、鍵で保護するファイルに解錠（閲覧）期限などの解錠条件を付加することもできる。例えば、送信者が閲覧期限を 1 年に指定した場合、鍵で保護するファイルには閲覧を 1 年間とする解錠条件を付加することができる。このように、実施形態に係る情報送受信システムによれば、閲覧権限のある受信者（生体認証を成功させることができる人）に対しても解錠条件によって閲覧を制限することも可能となる。

[0049] 次に、本実施形態に係る情報送受信システム 1 によるファイルの送受信処理の第 2 動作例について説明する。

[0050] 図 6 は、実施形態に係る情報送受信システム 1 によるファイルの送受信処理の第 2 動作例を概略的に説明するための図である。

図 6 に示すように、第 2 動作例では、送信者 O が複数の受信者 A、B、C にファイルを送信する場合を想定して説明する。すなわち、第 2 動作例に係

る情報送受信システム 1 は、送信装置 1 1 と複数の受信装置 1 2 (1 2 A、1 2 B、1 2 C) とを含むものとする。また、送信装置 1 1 は、送信者 O の公開鍵 (公開鍵 O) と秘密鍵とを保持しているものとする。また、受信者 A の受信装置 1 2 (1 2 A)、受信者 B の受信装置 1 2 (1 2 B)、受信者 C の受信装置 1 2 (1 2 C) は、それぞれ受信者 A、B、C の生体情報が登録され、受信者 A、B、C に対する生体認証が実行できるようになっているものとする。

[0051] まず、送信装置 1 1 は、ファイルを送信する前に、送信者 O の公開鍵 O を受信者 A、B、C の受信装置 1 2 にそれぞれ供給する。

各受信者 A、B、C の受信装置 1 2 は、送信者 O の公開鍵 O を取得すると、それぞれ受信者 A、B、C であることを認証するための生体認証を実行する。受信者 A の生体認証が成功した受信装置 1 2 は、受信者 A の第 1 鍵 A と第 1 鍵 A と対になる第 2 鍵 A とを生成する。受信者 B の生体認証が成功した受信装置 1 2 は、受信者 B の第 1 鍵 B と第 1 鍵 B と対になる第 2 鍵 B とを生成する。受信者 C の生体認証が成功した受信装置 1 2 は、受信者 C の第 1 鍵 C と第 1 鍵 C と対になる第 2 鍵 C とを生成する。受信者 A、B、C の各受信装置 1 2 A、1 2 B、1 2 C は、それぞれ生成した第 2 鍵 A、B、C を公開鍵 O で暗号化したデータを送信装置 1 1 へ送信する。

[0052] 送信装置 1 1 は、受信装置 1 2 A、1 2 B、1 2 C から公開鍵 O で暗号化された第 2 鍵 A、B、C を取得し、公開鍵 O に対応する秘密鍵 O を用いて暗号化された第 2 鍵 A、B、C をそれぞれ復号化 (解錠) することにより第 2 鍵 A、B、C を取得する。送信装置 1 1 は、全ての受信者 A、B、C の第 2 鍵 A、B、C を取得すると、受信者 A、B、C へ送信すべきファイルを第 2 鍵 A、B、C で施錠 (暗号化) する。ここで、送信装置 1 1 が第 2 鍵 A、B、C で施錠 (暗号化) したファイルは、第 2 鍵 A、B、C に対応する第 1 鍵 A、第 1 鍵 B 又は第 1 鍵 C で解錠できるものとする。送信装置 1 1 は、第 2 鍵 A、B、C で施錠したファイルを受信者 A の受信装置 1 2 へ送信する。

[0053] 受信者 A の受信装置 1 2 は、送信者 O から受信した第 2 鍵 A、B、C で施

錠されたファイルを保存する。受信者Aは、第2鍵A、B、Cで施錠されたファイルを閲覧する場合、受信装置12で生体認証を実行する。受信者Aの生体認証が成功した受信装置12Aは、受信者Aの第1鍵Aを用いて第2鍵A、B、Cで施錠されたファイルを解錠する。これにより、受信者Aは、送信者Oから受信したファイルが閲覧可能となる。

[0054] 同様に、受信者Bの受信装置12Bは、受信者Bの生体認証が成功した場合に受信者Bの第1鍵Bを用いて送信者Oから受信した第2鍵A、B、Cで施錠されたファイルを解錠する。これにより、受信者Bも、送信者Oから受信したファイルが閲覧可能となる。また、受信者Cの受信装置12Cは、受信者Cの生体認証が成功した場合に受信者Cの第1鍵Cを用いて送信者Oから受信した第2鍵A、B、Cで施錠されたファイルを解錠する。これにより、受信者Cも、送信者Oから受信したファイルが閲覧可能となる。

[0055] 次に、実施形態に係る情報送受信システム1によるファイル送受信処理の第2動作例を実行する場合の送信装置11および受信装置12（12A、12B、12C）の動作について説明する。

[0056] 図7は、実施形態に係る情報送受信システム1によるファイル送受信処理の第1動作例における送信装置11と受信装置12（12A、12B、12C）との動作例を説明するためのシーケンスである。

例えば、送信者Oは、送信装置11の操作部27により複数の送信先（受信者A、B、C）にセキュリティ設定を施したファイル（保護対象となる電子データ）を送信することを指示する。送信装置11のプロセッサ21は、送信者Oによる操作指示に応じて各受信者A、B、Cと各受信者A、B、Cへ送信するファイルなどを設定する（ST31）。

[0057] プロセッサ21は、送信先として受信者A、B、Cを設定すると、通信部25により受信者A、B、Cに対して送信者Oの公開鍵Oを送信（開示）し、各受信者A、B、Cの受信装置12A、12B、12Cに生体認証に紐づけて生成する第2鍵A、B、Cを要求する（ST32）。例えば、プロセッサ21は、第2鍵Aの要求と公開鍵Oとを受信者A宛の電子メールで送信し

、第2鍵Bの要求と公開鍵Oとを受信者B宛の電子メールで送信し、第2鍵Cの要求と公開鍵Oとを受信者C宛の電子メールで送信しても良い。

[0058] 各受信者A、B、Cの各受信装置12A、12B、12Cのプロセッサ31は、送信者Oからの第2鍵の要求を受信すると、それぞれインターフェース36に接続した生体認証装置40による受信者A、B、Cの生体認証を実行する(ST33)。プロセッサ31は、受信者A(B、C)に対する生体認証が成功すると、生体認証が成功した受信者A(B、C)の第1鍵A(B、C)を生成する(ST34)。プロセッサ31は、第1鍵A(B、C)を生成すると、第1鍵A(B、C)と対になる第2鍵A(B、C)を生成する(ST35)。各受信装置12A、12B、12Cが生成する第1鍵A、B、Cおよび第2鍵A、B、Cは、第1動作例で説明したものと同様のものでも良い。

[0059] 受信装置12A(12B、12C)のプロセッサ31は、第2鍵A(B、C)を生成すると、生成した第2鍵A(B、C)を公開鍵Oで暗号化(施錠)する(ST36)。プロセッサ31は、第2鍵A(B、C)を公開鍵Oで暗号化すると、通信部35により公開鍵Oで暗号化した第2鍵A(B、C)のデータを送信者Oの送信装置11へ送信する(ST37)。公開鍵Oで暗号化した第2鍵A、公開鍵Oで暗号化した第2鍵Bおよび公開鍵Oで暗号化した第2鍵Cは、それぞれの受信装置12A、12B、12Cが送信装置11へ送信するものとする。ただし、公開鍵Oで暗号化した第2鍵A、公開鍵Oで暗号化した第2鍵Bおよび公開鍵Oで暗号化した第2鍵Cは、何れかの受信装置12A、12B、12Cなどがまとめて送信するようにしても良い。

[0060] 送信者Oの送信装置11は、通信部35により各受信者A、B、Cの各受信装置12A、12B、12Cから公開鍵Oで暗号化された第2鍵A、B、Cのデータを受信する。送信装置11のプロセッサ21は、公開鍵Oで暗号された第2鍵A(B、C)を受信するごとに、公開鍵Oに対応する秘密鍵を用いて公開鍵Oで暗号化(施錠)された第2鍵A(B、C)のデータを復号

化（解錠）する（ST38）。これにより、プロセッサ21は、受信装置12A（12B、12C）からのデータを秘密鍵で復号化（解錠）したデータとして第2鍵A（B、C）を取得する（ST39）。

[0061] プロセッサ21は、受信者A、B、Cの受信装置12A、12B、12Cの何れかから第2鍵を取得するごとに、ファイルの送信先である全ての受信者A、B、Cからの第2鍵A、B、Cを取得したか否かを判断する（ST40）。

[0062] プロセッサ21は、ファイルの送信先である全ての受信者A、B、Cから第2鍵A、B、Cを取得した場合（ST40、YES）、取得した全ての第2鍵A、B、Cで各受信者A、B、Cに送信すべきファイルを暗号化（施錠）する（ST41）。ここで、プロセッサ21は、第1鍵A、第1鍵B又は第1鍵Cの何れかで解錠できるように、第2鍵A、B、Cでファイルを施錠（暗号化）する。

[0063] プロセッサ21は、第2鍵A、B、Cでファイルを暗号化（施錠）すると、第2鍵A、B、Cで施錠したファイルを添付した電子メールを作成する。ここで、プロセッサ21は、送信者Oの操作によってファイルを添付する電子メールの本文を作成するようにしても良い。さらに、プロセッサ21は、電子メールに添付する第2鍵A、B、Cで施錠したファイルに、第1動作例で説明したような解錠条件を付加しても良い。

[0064] プロセッサ21は、第2鍵A、B、Cで施錠したファイルを添付した電子メールを作成すると、作成した電子メールを各受信者A、B、C宛の電子メールとして通信部35によりメールサーバ13へ送信する（ST42）。メールサーバ13は、ネットワーク15を介してメールサーバ14へ受信者A、B、C宛の電子メールを送信する。メールサーバ14は、各受信者A、B、C宛に電子メールを送信する。

[0065] 各受信装置12A、12B、12Cは、それぞれ通信部25により第2鍵A、B、Cで施錠されたファイルが添付された各受信者A、B、C宛の電子メールを受信する。受信装置12A（12B、12C）のプロセッサ31は

、受信した電子メールに添付された第2鍵A、B、Cで施錠されたファイルを記憶部34に保存する(ST43)。ここで、プロセッサ31は、第2鍵A、B、Cで施錠されたファイルをファイルサーバなどの外部装置に保存するようにしても良い。

[0066] 例えば、受信装置12A(12B、12C)のプロセッサ31は、操作部37を操作する受信者Aによる保存した第2鍵A、B、Cで施錠されたファイルに対する解錠要求を受け付ける。ここで、プロセッサ31は、第2鍵A、B、Cで施錠されたファイルに解錠条件が設定されていれば、解錠要求を受けた場合に解錠条件を満たしているか否かによりファイルの解錠を受け付けるか否かを判断するようにしても良い。

[0067] 解錠要求に応じてファイルの解錠を実行する場合(ST44、YES)、受信装置12A(12B、12C)のプロセッサ31は、インターフェース36に接続した生体認証装置40による受信者A(B、C)の生体認証を実行する(ST45)。プロセッサ31は、受信者A(B、C)に対する生体認証が成功すると、生体認証が成功した受信者A(B、C)の第1鍵A(B、C)を取得する(ST46)。ここで、公開鍵Oを受信した場合に実行した受信者A(B、C)の生体認証の成功に応じて生成した第2鍵A(B、C)と対になる第1鍵A(B、C)が受信装置12A(12B、12C)の記憶部34のセキュアな記憶領域に保存されているものとする。この場合、プロセッサ31は、記憶部34から当該受信者A(B、C)の第1鍵A(B、C)を取得する。

[0068] 受信装置12A(12B、12C)のプロセッサ31は、第1鍵A(B、C)を取得すると、取得した第1鍵A(B、C)を用いて第2鍵A、B、Cで施錠されたファイルを解錠する(ST47)。受信装置12A(12B、12C)のプロセッサ31は、第1鍵A(B、C)を用いてファイルを解錠すると、解錠したファイルを開いて閲覧可能な状態とする(ST48)。例えば、プロセッサ31は、第1鍵A(B、C)で開錠したファイルのデータを表示部38に表示することにより受信者Aに開示する。

[0069] 以上のような第2動作例によれば、送信者Oから複数の受信者にファイルを送信する場合であっても、複数の受信者がそれぞれの生体認証で取得する複数の鍵で施錠されたファイルを送信装置から複数の受信装置へ安全に送信でき、各受信装置では鍵で保護された状態のファイルを保存しておくことができる。各受信者は、自身の生体認証によって取得できる鍵を用いて任意のタイミングで保護されたファイルを開くことができる。この結果、複数の受信者が、パスワードなどを紛失でファイルを開覧できなくなることがなく、閲覧権限のある人（生体認証を成功させることができる人）であれば誰でも任意のタイミングで確実に閲覧可能とすることができる。

[0070] また、第2動作例においても、鍵で保護するファイルに解錠（閲覧）期限などの解錠条件を付加することが可能となる。これにより、複数の受信者にファイルを配信する場合であっても、閲覧権限のある各受信者（生体認証を成功させることができる人）に対して解錠条件によって閲覧を制限することも可能なる。

[0071] 次に、本実施形態に係る情報送受信システム1によるファイルの送受信処理の第3動作例について説明する。

[0072] 図8は、実施形態に係る情報送受信システム1によるファイルの送受信処理の第3動作例を概略的に説明するための図である。

図8に示すように、第3動作例では、上述した第2動作例によって送信者Oが複数の受信者A、B、Cに第2鍵A、B、Cで施錠したファイルを送信した後、さらに、別の受信者Dを当該ファイルの受信者に追加する場合を想定して説明する。ここでは、第2動作例で説明した前提条件に加えて、受信者Dの受信装置12（12D）は、受信者Dの生体情報が登録され、受信者Dに対する生体認証が実行できるようになっているものとする。

[0073] また、第3動作例の説明として、図8に示すように、送信装置11は、ファイルを送付済みの受信者ABCの第2鍵A、B、Cを保持し、受信装置12A（B、C）は、送信装置11が第2鍵A、B、Cで施錠したファイルと第1鍵A（B、C）と第2鍵A（B、C）とを保持しているものとする。こ

の状態において、受信者Dをファイルの受信者として追加する処理を実行する。

[0074] まず、送信装置11は、送信者Oの公開鍵Oを受信者Dの受信装置12Dに供給する。受信者Dの受信装置12Dは、送信者Oの公開鍵Oを取得すると、受信者Dであることを認証するための生体認証を実行する。受信者Dの生体認証が成功した受信装置12Dは、受信者Dの第1鍵Dと第1鍵Dと対になる第2鍵Dとを生成する。受信装置12Dは、生体した第2鍵Dを公開鍵Oで暗号化したデータを送信装置11へ送信する。

[0075] 送信装置11は、受信装置12Dから公開鍵Oで暗号化された第2鍵Dを取得し、公開鍵Oに対応する秘密鍵Oを用いて暗号化された第2鍵Dを復号化（解錠）することにより第2鍵Dを取得する。送信装置11は、受信者Dの第2鍵Dを取得すると、新たに取得した受信者Dの第2鍵Dを加えた4つの第2鍵A、B、C、Dでファイルを施錠（暗号化）する。ここで、送信装置11が第2鍵A、B、C、Dで施錠（暗号化）したファイルは、第1鍵Dで解錠できるものとする。

[0076] 送信装置11は、第2鍵A、B、C、Dで施錠したファイルを受信者Dの受信装置12Dへ送信する。受信者Dの受信装置12Dは、送信者Oから受信した第2鍵A、B、C、Dで施錠されたファイルを保存する。受信装置12Dは、送信者Oから受信した第2鍵A、B、C、Dで施錠されたファイルを保存した後、受信者Dの生体認証が成功した場合に受信者Dの第1鍵Dを用いて第2鍵A、B、C、Dで施錠されたファイルを解錠することにより、追加受信者である受信者Dも当該ファイルが閲覧可能となる。

[0077] また、送信装置11は、第2鍵A、B、C、Dで施錠したファイルを受信者A、B、Cの受信装置12A、12B、12Cにも送信するようにして良い。受信装置12A、12B、12Cは、送信者Oから受信した第2鍵A、B、C、Dで施錠されたファイルを保存し、受信者A、B、Cの生体認証が成功した場合に受信者A、B、Cの第1鍵A、B、Cを用いて第2鍵A、B、C、Dで施錠されたファイルを解錠できる。

[0078] 次に、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 3 動作例のける送信装置 1 1 および受信装置 1 2 の動作について説明する。

図 9 は、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 3 動作例における送信装置 1 1 と受信装置 1 2 (1 2 A、1 2 B、1 2 C) との動作例を説明するためのシーケンスである。

ここで、図 9 に示す処理は、図 8 に示すように、受信装置 1 2 A (B、C) が送信装置 1 1 から受信済みの第 2 鍵 A、B、C で施錠されたファイルを保持しているものとする。この状態において、図 9 に示す処理が開始されるものとする。

[0079] 例えば、送信者 O は、送信装置 1 1 の操作部 2 7 により受信者 D にセキュリティ設定を施したファイル (保護対象となる電子データ) の送信先に追加することを指示する。送信装置 1 1 のプロセッサ 2 1 は、送信者 O による操作指示に応じて受信者 D をファイルの追加送信先 (追加受信者) に設定する (S T 5 1)。

[0080] プロセッサ 2 1 は、追加送信先として受信者 D を設定すると、通信部 2 5 により受信者 D に対して送信者 O の公開鍵 O を送信 (開示) し、受信者 D の受信装置 1 2 D に生体認証に紐づけて生成する第 2 鍵 D を要求する (S T 5 2)。例えば、プロセッサ 2 1 は、第 2 鍵 D の要求と公開鍵 O とを受信者 D 宛の電子メールで送信するようにしても良い。

[0081] 受信者 D の受信装置 1 2 D のプロセッサ 3 1 は、送信者 O からの第 2 鍵 D の要求を受信すると、インターフェース 3 6 に接続した生体認証装置 4 0 による受信者 D の生体認証を実行する (S T 5 3)。プロセッサ 3 1 は、受信者 D に対する生体認証が成功すると、生体認証が成功した受信者 D の第 1 鍵 D を生成する (S T 5 4)。プロセッサ 3 1 は、第 1 鍵 D を生成すると、第 1 鍵 D と対になる第 2 鍵 D を生成する (S T 5 5)。受信装置 1 2 D が生成する第 1 鍵 D および第 2 鍵 D は、第 1 動作例で説明したものと同様の手順で生成されるもので良い。

- [0082] 受信装置 1 2 D のプロセッサ 3 1 は、第 2 鍵 D を生成すると、生成した第 2 鍵 D を公開鍵 O で暗号化（施錠）する（S T 5 6）。プロセッサ 3 1 は、第 2 鍵 D を公開鍵 O で暗号化すると、通信部 3 5 により公開鍵 O で暗号化した第 2 鍵 D のデータを送信者 O の送信装置 1 1 へ送信する（S T 5 7）。
- [0083] 送信者 O の送信装置 1 1 は、通信部 3 5 により受信者 D の受信装置 1 2 D から公開鍵 O で暗号化された第 2 鍵 D のデータを受信する。送信装置 1 1 のプロセッサ 2 1 は、公開鍵 O で暗号された第 2 鍵 D を受信すると、公開鍵 O に対応する秘密鍵 O により公開鍵 O で暗号化（施錠）された第 2 鍵 D のデータを復号化（解錠）する（S T 5 8）。これにより、プロセッサ 2 1 は、秘密鍵 O で復号化（解錠）したデータとして第 2 鍵 D を取得する（S T 5 9）。
- [0084] 送信装置 1 1 のプロセッサ 2 1 は、追加する受信者である受信者 D の受信装置 1 2 D から第 2 鍵 D を取得すると、追加受信者である受信者 D を含むファイル（保護対象とする電子データ）の全ての送信先である受信者 A、B、C、D の第 2 鍵 A、B、C、D でファイルを暗号化（施錠）する（S T 6 0）。ここで、プロセッサ 2 1 は、第 2 鍵 D に対応する第 1 鍵 D で施錠できるようにファイルを第 2 鍵 A、B、C、D で施錠（暗号化）する。
- [0085] プロセッサ 2 1 は、第 2 鍵 A、B、C、D でファイルを暗号化（施錠）すると、第 2 鍵 A、B、C、D で施錠したファイルを添付した電子メールを作成する。ここで、プロセッサ 2 1 は、送信者 O が第 2 鍵 A、B、C、D で施錠したファイルを添付する電子メールの本文を作成するようにしても良い。また、プロセッサ 2 1 は、電子メールに添付する第 2 鍵 A、B、C、D で施錠したファイルに対して、第 1 動作例で説明したような解錠条件を付加しても良い。プロセッサ 2 1 は、第 2 鍵 A、B、C、D で施錠したファイルを添付した電子メールを作成すると、作成した電子メールを受信者 D 宛に送信する（S T 6 1）。
- [0086] 追加受信者である受信者 D の受信装置 1 2 D は、通信部 3 5 により第 2 鍵 A、B、C、D で施錠されたファイルが添付された電子メールを受信する。

受信装置 1 2 D のプロセッサ 3 1 は、受信した電子メールに添付された第 2 鍵 A、B、C、D で施錠されたファイルを記憶部 3 4 に保存する（S T 6 2）。

[0087] 第 2 鍵 A、B、C、D で施錠されたファイルを保存した後、受信装置 1 2 D のプロセッサ 3 1 は、第 2 鍵 A、B、C、D で施錠されたファイルに対する解錠要求を受け付ける。プロセッサ 3 1 は、第 2 鍵 A、B、C、D で施錠されたファイルに解錠条件が設定されていれば、解錠要求を受けた場合に解錠条件を満たしているか否かによりファイルの解錠を受け付けるか否かを判断する。

[0088] 受信装置 1 2 D のプロセッサ 3 1 は、解錠要求に応じてファイルの解錠を実行する場合（S T 6 3、YES）、インターフェース 3 6 に接続した生体認証装置 4 0 による受信者 D の生体認証を実行する（S T 6 4）。プロセッサ 3 1 は、受信者 D に対する生体認証が成功すると、生体認証が成功した受信者 D の第 1 鍵 D を取得する（S T 6 5）。プロセッサ 3 1 は、第 1 鍵 D を用いて第 2 鍵 A、B、C、D で施錠されたファイルを解錠し（S T 6 6）、解錠したファイルを開放して閲覧可能な状態とする（S T 6 7）。

[0089] また、送信装置 1 1 のプロセッサ 2 1 は、第 2 鍵 A、B、C、D で施錠したファイルを添付した電子メールを受信者 A、B、C 宛にも送信するようにしても良い。この場合、受信者 A、B、C の各受信装置 1 2 A、1 2 B、1 2 C は、それぞれ通信部 3 5 により第 2 鍵 A、B、C、D で施錠されたファイルが添付された電子メールを受信する。

[0090] 各受信装置 1 2 A、1 2 B、1 2 C のプロセッサ 3 1 は、第 2 鍵 A、B、C で施錠されたファイルを新たに受信した電子メールに添付されている第 2 鍵 A、B、C、D で施錠されたファイルに更新するようにしても良い。各受信装置 1 2 A、1 2 B、1 2 C のプロセッサ 3 1 は、第 2 鍵 A、B、C、D で施錠されたファイルを保存した場合、受信者 A、B、C の生体認証によって取得する第 1 鍵 A、B、C を用いて第 2 鍵 A、B、C、D で施錠されたファイルを解錠するようにすれば良い。

[0091] 以上のような第3動作例によれば、送信者から既に受信者にファイルが送信された後であっても、既存の受信者以外に当該ファイルを閲覧可能な新たな受信者を追加できる。送信装置は、追加受信者の生体認証で取得する鍵と送信済み受信者の鍵とを含む複数の鍵で施錠されたファイルを送信装置から複数の受信装置へ安全に送信でき、各受信装置では鍵で保護された状態のファイルを保存しておくことができる。

[0092] この結果、追加受信者を含む複数の受信者は、自身の生体認証によって取得できる鍵を用いて任意のタイミングで保護されたファイルを開くことができる。また、追加可能な複数の受信者が、パスワードなどを紛失でファイルを閲覧できなくなることがなく、閲覧権限のある人（生体認証を成功させることができる人）であれば誰でも任意のタイミングで確実に閲覧可能とすることができる。

[0093] 次に、本実施形態に係る情報送受信システム1によるファイルの送受信処理の第4動作例について説明する。

図10は、実施形態に係る情報送受信システム1によるファイルの送受信処理の第4動作例を概略的に説明するための図である。

図10に示すように、第4動作例では、上述した第2動作例によって送信者Oが複数の受信者A、B、Cに第2鍵A、B、Cで施錠したファイルを送信した後、当該ファイルを既に受信している受信者Aが別の受信者Dをファイルの受信者に追加する場合を想定して説明する。ここで、受信者Dの受信装置12（12D）は、第3動作例で説明した前提条件と同様に、受信者Dの生体情報が登録され、受信者Dに対する生体認証が実行できるようになっているものとする。

[0094] 第4動作例の説明として、図10に示すように、送信装置11は、第2鍵A、B、Cで施錠したファイルに対して受信者Aにファイル受信者の追加を許可する権限（追加工権）を付与することを示す追加工権情報を付加し、追加工権情報を付加したファイルを受信者Aへ送信するものとする。受信者Aの受信装置12Aは、送信装置11から受信する追加工権情報が付与された

ファイルを保存するものとする。

[0095] この状態において、ファイルを閲覧する追加受信者として受信者Dを追加するものとする。追加特権情報によって受信者を追加する権限が与えられた受信者Aの受信装置12Aは、受信者A（追加権限者A）の公開鍵Aを受信者Dの受信装置12Dに供給する。受信者Dの受信装置12Dは、受信者（追加権限者）Aの公開鍵Aを取得すると、受信者D自身であることを認証するための生体認証を実行する。受信者Dの生体認証が成功した受信装置12Dは、受信者Dの第1鍵Dと第1鍵Dと対になる第2鍵Dとを生成する。受信装置12Dは、生成した第2鍵Dを公開鍵Aで暗号化（施錠）したデータを受信装置12Aへ送信する。

[0096] 受信装置12Aは、受信装置12Dから公開鍵Aで暗号化された第2鍵Dを取得し、公開鍵Aに対応する秘密鍵Aを用いて暗号化された第2鍵Dを復号化（解錠）することにより第2鍵Dを取得する。受信装置12Aは、受信者Dの第2鍵Dを取得すると、新たに取得した受信者Dの第2鍵Dを加えた4つの第2鍵A、B、C、Dでファイルを施錠（暗号化）する。ここで、受信装置12Aが第2鍵A、B、C、Dで施錠（暗号化）したファイルは、第1鍵Dで解錠できるものとする。

[0097] 受信装置12Aは、第2鍵A、B、C、Dで施錠したファイルを受信者Dの受信装置12Dへ送信する。受信者Dの受信装置12Dは、送信者Oから受信した第2鍵A、B、C、Dで施錠されたファイルを保存する。受信装置12Dは、送信者Oから受信した第2鍵A、B、C、Dで施錠されたファイルを保存した後、受信者Dの生体認証が成功した場合に受信者Dの第1鍵Dを用いて第2鍵A、B、C、Dで施錠されたファイルを解錠することにより当該ファイルが閲覧可能となる。

[0098] また、受信装置12Aは、第2鍵A、B、C、Dで施錠したファイルを保存するとともに、第2鍵A、B、C、Dで施錠したファイルを受信者B、Cの受信装置12B、12Cに送信するようにしても良い。この場合、受信装置12B、12Cは、受信者Aから受信した第2鍵A、B、C、Dで施錠さ

れたファイルを保存する。これにより、第2鍵A、B、C、Dで施錠されたファイルを保存した受信装置12A、12B、12Cは、受信者A、B、Cの生体認証が成功した場合に第1鍵A、B、Cで第2鍵A、B、C、Dで施錠されたファイルが解錠できるようになる。

[0099] 次に、実施形態に係る情報送受信システム1によるファイル送受信処理の第4動作例のける送信装置11および各受信装置12の動作について説明する。

図11は、実施形態に係る情報送受信システム1によるファイル送受信処理の第4動作例における送信装置11と受信装置12（12A、12D）との動作例を説明するためのシーケンスである。

[0100] まず、送信装置11のプロセッサ21は、第2鍵A、B、Cで施錠したファイルに対して、受信者Aにファイル受信者の追加を許可する権限を付与することを示す追加特権情報（以下、追加特権Aと称する）を設定する（ST71）。例えば、プロセッサ21は、第2鍵A、B、Cで施錠したファイルに対する属性情報として追加特権Aを付加するようにしても良い。

[0101] 送信装置11のプロセッサ21は、追加特権Aを付加した第2鍵A、B、Cで施錠したファイルを受信者A宛に送信する（ST72）。例えば、プロセッサ21は、図7におけるST42の処理として各受信者A、B、Cへ第2鍵A、B、Cで施錠したファイルを電子メールに添付して送信する前に第2鍵A、B、Cで施錠したファイルに追加特権Aを付加する。また、送信装置11のプロセッサ21は、図7に示す処理とは別の処理として、追加特権Aを付加した第2鍵A、B、Cで施錠したファイルを受信者Aに送信するようにしても良い。

[0102] 受信者Aの受信装置12Aは、送信装置11から追加特権Aが付加された第2鍵A、B、Cで施錠したファイルを受信する。受信装置12Aのプロセッサ31は、送信装置11から受信した追加特権A付きの第2鍵A、B、Cで施錠したファイルを記憶部34などに保存する（ST81）。

[0103] この状態において、ファイルの受信者（ファイルの閲覧が許可される者）

を追加する権限を与えられた受信者Aが追加受信者として受信者Dを追加するものとする。例えば、受信者Aは、受信装置12Aの操作部37により受信者Dにファイル（保護対象となる電子データ）の送信先（受信者）に追加することを指示する。受信装置12Aのプロセッサ31は、受信者Aによる操作指示に応じて受信者Dをファイルの追加送信先に設定する（ST82）。

- [0104] プロセッサ31は、ファイルの追加受信者として受信者Dを設定すると、通信部35により受信者Dに対して受信者Aの公開鍵Aを送信（開示）し、受信装置12Dが受信者Dの生体認証に紐づけて生成する第2鍵Dを要求する（ST83）。例えば、受信装置12Aのプロセッサ31は、第2鍵Dの要求と公開鍵Aとを受信者D宛の電子メールで送信するようにしても良い。
- [0105] 受信者Dの受信装置12Dのプロセッサ31は、受信者（追加権限者）Aからの第2鍵Dの要求を受信すると、インターフェース36に接続した生体認証装置40による受信者Dの生体認証を実行する（ST84）。受信装置12Dのプロセッサ31は、受信者Dに対する生体認証が成功すると、生体認証が成功した受信者Dの第1鍵Dを生成する（ST85）。受信装置12Dのプロセッサ31は、第1鍵Dを生成すると、第1鍵Dと対になる第2鍵Dを生成する（ST86）。受信装置12Dが生成する第1鍵Dおよび第2鍵Dは、第1動作例で説明したものと同様のものであっても良い。
- [0106] 受信装置12Dのプロセッサ31は、第2鍵Dを生成すると、生成した第2鍵Dを公開鍵Aで暗号化（施錠）する（ST87）。受信装置12Dのプロセッサ31は、第2鍵Dを公開鍵Aで暗号化すると、通信部35により公開鍵Aで暗号化した第2鍵Dのデータを受信者Aの受信装置12Aへ送信する（ST88）。
- [0107] 受信者Aの受信装置12Aは、通信部35により受信者Dの受信装置12Dから公開鍵Aで暗号化された第2鍵Dのデータを受信する。受信装置12Aのプロセッサ31は、公開鍵Aで暗号された第2鍵Dを受信すると、公開鍵Aに対応する秘密鍵Aにより公開鍵Aで暗号化（施錠）された第2鍵Dの

データを復号化（解錠）する（ST89）。これにより、受信装置12Aのプロセッサ31は、秘密鍵Aで復号化（解錠）したデータとして第2鍵Dを取得する（ST90）。

[0108] 受信装置12Aのプロセッサ31は、追加する受信者である受信者Dの受信装置12Dから第2鍵Dを取得すると、第2鍵A、B、Cで施錠されているファイルに追加受信者である受信者Dの第2鍵Dを追加する（ST91）。ここで、受信装置12Aのプロセッサ31は、第2鍵Dに対応する第1鍵Dでファイルを解錠できるように第2鍵Dを用いてファイルを施錠（暗号化）する。

[0109] 受信装置12Aのプロセッサ31は、第2鍵A、B、C、Dでファイルを暗号化（施錠）すると、第2鍵A、B、C、Dで施錠したファイルを添付した電子メールを作成する。ここで、受信装置12Aのプロセッサ31は、受信者D宛の電子メールの本文を作成するようにしても良い。受信装置12Aのプロセッサ31は、第2鍵A、B、C、Dで施錠したファイルを添付した電子メールを受信者D宛として通信部35により送信する（ST92）。

[0110] 追加受信者である受信者Dの受信装置12Dは、通信部35により第2鍵A、B、C、Dで施錠されたファイルが添付された電子メールを受信する。受信装置12Dのプロセッサ31は、受信した電子メールに添付された第2鍵A、B、C、Dで施錠されたファイルを記憶部34に保存する（ST93）。

[0111] 受信装置12Dのプロセッサ31は、第2鍵A、B、C、Dで施錠されたファイルを保存した後、第2鍵A、B、C、Dで施錠されたファイルに対する解錠要求を受け付ける。受信装置12Dのプロセッサ31は、第2鍵A、B、C、Dで施錠されたファイルに解錠条件が設定されていれば、解錠要求を受けた場合に解錠条件を満たしているか否かによりファイルの解錠を受け付けるか否かを判断する。

[0112] 解錠要求に応じてファイルの解錠を実行する場合（ST94、YES）、受信装置12Dのプロセッサ31は、インターフェース36に接続した生体

認証装置40による受信者Dの生体認証を実行する(ST95)。プロセッサ31は、受信者Dに対する生体認証が成功すると、生体認証が成功した受信者Dの第1鍵Dを取得する(ST96)。プロセッサ31は、第1鍵Dを用いて第2鍵A、B、C、Dで施錠されたファイルを解錠し(ST97)、解錠したファイルを開放して閲覧可能な状態とする(ST98)。

[0113] また、受信装置12Aのプロセッサ31は、第2鍵A、B、C、Dで施錠したファイルを添付した電子メールを受信者B、C宛にも送信するようにしても良い。この場合、受信者B、Cの各受信装置12B、12Cは、それぞれ第2鍵A、B、C、Dで施錠されたファイルが添付された電子メールを受信し、第2鍵A、B、C、Dで施錠されたファイルを保存する。

[0114] 各受信装置12B、12Cのプロセッサ31は、第2鍵A、B、Cで施錠されたファイルを新たに受信した電子メールに添付されている第2鍵A、B、C、Dで施錠されたファイルに更新するようにしても良い。各受信装置12B、12Cのプロセッサ31は、第2鍵A、B、C、Dで施錠されたファイルを保存した場合、受信者B、Cの生体認証によって取得する第1鍵B、Cを用いて第2鍵A、B、C、Dで施錠されたファイルを解錠するようにすれば良い。

[0115] 以上のような第4動作例によれば、送信者から既に受信者にファイルが送信された後であっても、受信者を追加する権限が与えられた追加権限者が既存の受信者以外に当該ファイルを閲覧可能な新たな受信者を追加できる。追加権限者の受信装置は、追加受信者の生体認証で取得する鍵と送信済み受信者の鍵とを含む複数の鍵で施錠したファイルを追加受信者の受信装置へ安全に送信でき、受信装置では各受信者の鍵で保護されたファイルを保存しておくことができる。

[0116] この結果、追加受信者を含む各受信者は、自身の生体認証によって取得できる鍵を用いて任意のタイミングで保護されたファイルを開くことができる。また、追加可能な複数の受信者が、パスワードなどを紛失でファイルを閲覧できなくなることがなく、閲覧権限のある人(生体認証を成功させることが

できる人)であれば誰でも任意のタイミングで確実に閲覧可能とすることができる。

[0117] 次に、本実施形態に係る情報送受信システム1によるファイルの送受信処理の第5動作例について説明する。

図12は、実施形態に係る情報送受信システム1によるファイルの送受信処理の第5動作例を概略的に説明するための図である。

第5動作例では、ファイルの改ざん防止を実施する。第5動作例で説明するファイルの改ざん防止は、上述した第1、第2、第3および第4動作例に適用可能である。ここでは、第5動作例として、上述した第1動作例に改ざん防止を適用する場合の動作例について説明するものとする。第5動作例では、ファイルの送信者が作成する電子証明書(以下、証明書とも称する)によって受信者へ送信されるファイルの正当性を確認する。

[0118] 第5動作例に係る情報送受信システム1では、送信装置11が送信者Oであることを確認するための生体認証を実行する機能を備えるものとする。例えば、送信装置11は、生体認証部を備えるものとしても良いし、生体認証を実行する生体認証装置を接続するインターフェースを備えるものとする。ここでは、送信装置11が生体認証部を備えることを想定して説明するものとする。

[0119] 図12に示す例において、第5動作例では、上述した図4に示すような第1動作例に加えて、送信者の送信装置11が生体認証を伴う証明書の作成を実行し、受信者の受信装置12が受信したファイルの添付される証明書の確認を実行する。また、図12に示す例において、送信装置11は、送信者Oの生体情報が登録され、送信者Oに対する生体認証が実行できるようになっているものとする。受信装置12Aは、受信者Aの公開鍵(公開鍵A)と秘密鍵とを保持しているものとする。

[0120] 送信装置11は、受信者Aが確認可能な証明書を作成する場合、受信者Aの公開鍵Aを受信者Aの受信装置12Aから取得する。送信装置11は、受信者Aの公開鍵Aを取得すると、操作者が送信者Oであることを認証するた

めの生体認証を実行する。生体認証が成功すると（送信者Oであることが確認すると）、送信装置11は、送信者Oの第1鍵Oと第1鍵Oに対応する第2鍵Oとを生成する。送信装置11は、第1鍵Oに対応する第2鍵Oを生成すると、第2鍵Oを公開鍵Aで暗号化したデータを受信装置12Aへ送信する。

[0121] 受信装置12Aは、送信装置11から公開鍵Aで暗号化（施錠）された第2鍵Oを受信する。受信装置12Aは、公開鍵Aに対応する秘密鍵を用いて送信装置11から受信した暗号化された第2鍵Aを復号化（解錠）することにより第2鍵Oを取得し、取得した第2鍵を保持する。

[0122] また、送信装置11は、送信者Oの生体認証に伴って第1鍵Oを生成すると、第1鍵Oを用いて証明書を作成する。例えば、送信装置11は、受信者Aへ送信するファイルのハッシュ値を算出し、算出したハッシュ値を第1鍵Oで暗号化する。ファイルのハッシュ値を第1鍵Oで暗号化する証明書は、送信者Oの第1鍵と対になる第2鍵Oで確認可能なデータとなる。送信装置11は、第2鍵Oでチェック可能な証明書を作成すると、受信者Aへ送信する証明書付きのファイルを作成する。

[0123] また、送信装置11は、上述した第1動作例と同様な流れの処理によって、受信者Aの第2鍵Aを取得する。送信装置11は、第2鍵Aを取得すると、受信者Aの第2鍵Aを用いて証明書付きのファイルを施錠（暗号化）し、施錠したファイルを受信者Aの受信装置12Aへ送信する。

[0124] 受信装置12は、送信者Oから第2鍵Aで施錠された証明書付きのファイルを受信して保存する。受信者Aは、第2鍵Aで施錠されたファイルを閲覧する場合、受信装置12で生体認証を実行する。受信装置12は、生体認証により受信者Aであることが確認されると、受信者Aの第1鍵Aを用いて第2鍵Aで施錠されたファイルを解錠する。

[0125] 受信装置12Aは、第2鍵Aでファイルを解錠すると、さらに、ファイルに添付されている証明書を送信者Oから取得した第2鍵Oを用いてチェックする。例えば、受信装置12Aは、第2鍵Aで解錠したファイルのハッシュ

値を算出するとともに、上述した手続きで送信装置 11 から取得した送信者 O の第 1 鍵 O で証明書を復号化する。

[0126] 受信装置 12 A は、ファイルから算出したハッシュ値と第 1 鍵で復号化した証明書のデータとが一致するか否かを判定する。例えば、受信装置 12 A は、ファイルのハッシュ値と証明書のデータとが一致する場合、ファイルが改ざんのない正当なデータであると判定して、当該ファイルを閲覧可能とする。また、受信装置 12 A は、ファイルのハッシュ値と証明書のデータとが一致しない場合、改ざんの疑いがあるため、当該ファイルの閲覧を不可とする。

[0127] 次に、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 5 動作例における送信装置 11 および受信装置 12 の動作について説明する。

[0128] 図 13 および図 14 は、実施形態に係る情報送受信システム 1 によるファイル送受信処理の第 5 動作例における送信装置 11 と受信装置 12 との動作例を説明するためのシーケンスである。

送信者 O は、送信装置 11 の操作部 27 により証明書付きでファイル（保護対象となる電子データ）の受信者 A へ送信することを指示する。送信装置 11 のプロセッサ 21 は、送信者 O による操作指示に応じて送信先（受信者）および送信するファイルなどを設定する（ST110）。

[0129] 送信装置 11 のプロセッサ 21 は、送信先として受信者 A を設定すると、受信者 A の公開鍵 O を取得する（ST111）。送信装置 11 のプロセッサ 21 は、受信者 A の公開鍵を取得すると、生体認証部による送信者 O の生体認証を実行する（ST112）。プロセッサ 21 は、送信者 O の生体認証が成功すると、生体認証が成功した送信者 O の第 1 鍵 O を生成する（ST113）。プロセッサ 21 は、第 1 鍵 O を生成すると、第 1 鍵 O と対になる第 2 鍵 O を生成する（ST114）。すなわち、プロセッサ 21 は、送信者 O に対する生体認証の成功に応じて送信者 O 用の鍵のペアを生成する。送信装置 11 のプロセッサ 21 による第 1 鍵 O および第 2 鍵 O を生成する処理は、第

1 動作例として説明した受信装置 1 2 による第 1 鍵 A および第 2 鍵 A を生成する処理と同様な処理によって実現可能である。

[0130] 送信装置 1 1 のプロセッサ 2 1 は、第 2 鍵 O を生成すると、生成した第 2 鍵 O を公開鍵 A で暗号化（施錠）する（S T 1 1 5）。プロセッサ 2 1 は、第 2 鍵 O を公開鍵 A で暗号化すると、通信部 3 5 により公開鍵 A で暗号化した第 2 鍵 O のデータを受信者 A の受信装置 1 2 A へ送信する（S T 1 1 6）。

[0131] 受信者 A の受信装置 1 2 A は、通信部 3 5 により送信装置 1 1 が公開鍵 A で暗号化した第 2 鍵 O のデータを受信する。受信装置 1 2 A のプロセッサ 2 1 は、公開鍵 A で暗号された第 2 鍵 O を受信すると、公開鍵 A に対応する秘密鍵により公開鍵 A で暗号化（施錠）された第 2 鍵 O を復号化（解錠）する（S T 1 1 7）。これにより、受信装置 1 2 A のプロセッサ 3 1 は、第 2 鍵 A を取得し（S T 1 1 8）、取得した第 2 鍵 A を保持する。

[0132] また、送信装置 1 1 のプロセッサ 2 1 は、第 1 鍵 O を生成した後、第 1 鍵 O を用いて受信者 A へ送信するファイルに対する証明書を作成する（S T 1 2 0）。プロセッサ 2 1 は、受信者 A へ送信するファイルのハッシュ値を算出し（S T 1 2 0 a）、算出したハッシュ値を第 1 鍵 O で暗号化する（S T 1 2 0 b）。プロセッサ 2 1 は、ファイルのハッシュ値を第 1 鍵 O で暗号化したデータをファイルの送信者（所有者）が送信者 O であることを証明書とする。

[0133] また、送信装置 1 1 のプロセッサ 2 1 は、受信者 A へ送信するファイルを施錠するために、上述した第 1 動作例と同様な流れで受信者 A の第 2 鍵を取得する処理を実行する。すなわち、送信装置 1 1 のプロセッサ 2 1 は、受信者 A に対して送信者 O の公開鍵 O を送信（開示）し（S T 1 2 1）、受信者 A の第 2 鍵を要求する。

[0134] 受信者 A の受信装置 1 2 A のプロセッサ 3 1 は、送信者 O からの第 2 鍵 A の要求を受信すると、インターフェース 3 6 に接続した生体認証装置 4 0 による受信者 A の生体認証を実行する（S T 1 2 2）。受信装置 1 2 A のプロセッサ 3 1 は、受信者 A に対する生体認証が成功すると、生体認証が成功し

た受信者Aの第1鍵Aを生成する(ST123)。プロセッサ31は、第1鍵Aを生成すると、第1鍵Aと対になる第2鍵Aを生成する(ST124)。プロセッサ31は、生成した第2鍵Aを公開鍵Oで暗号化(施錠)し(ST125)、公開鍵Oで暗号化した第2鍵Aのデータを送信者Oの送信装置11へ送信する(ST126)。

[0135] 送信者Oの送信装置11のプロセッサ21は、受信装置12Aから公開鍵Oで暗号された第2鍵Aを受信すると、公開鍵Oに対応する秘密鍵により公開鍵Oで暗号化(施錠)された第2鍵Aのデータを復号化(解錠)し(ST128)、秘密鍵で復号化(解錠)したデータとして第2鍵Aを取得する(ST129)。

[0136] 送信装置11のプロセッサ21は、第2鍵Aを取得すると、第2鍵Aを用いて受信者Aに送信するファイルと証明書とを暗号化(施錠)する(ST130)。送信装置11のプロセッサ21は、第2鍵Aで施錠した証明書付きのファイルを添付した電子メールを作成する。ここで、プロセッサ21は、電子メールに添付する第2鍵Aで施錠したファイルには解錠条件を付加しても良い。

[0137] 送信装置11のプロセッサ21は、第2鍵Aで施錠した証明書付きのファイルを添付した電子メールを受信者Aへ送信する(ST131)。これにより、受信者Aの受信装置12Aは、通信部35により第2鍵Aで施錠されたファイルが添付された受信者A宛の電子メールを受信する。受信装置12Aのプロセッサ31は、受信した電子メールに添付された第2鍵Aが施錠された証明書付きのファイルを記憶部34に保存する(ST132)。プロセッサ31は、第2鍵Aで施錠されたファイルを添付された電子メールとともに保存しても良いし、第2鍵Aで施錠されたファイルを保存しても良い。また、プロセッサ31は、第2鍵Aで施錠されたファイルをファイルサーバなどの外部装置に保存するようにしても良い。

[0138] 送信装置11のプロセッサ31は、受信者Aからの解錠要求に応じてファイルの解錠を実行する場合(ST133、YES)、インターフェース36

に接続した生体認証装置40による受信者Aの生体認証を実行する(ST134)。プロセッサ31は、受信者Aに対する生体認証が成功すると、生体認証が成功した受信者Aの第1鍵Aを取得する(ST25)。プロセッサ31は、第1鍵Aを取得すると、取得した第1鍵Aを用いて第2鍵Aで施錠された証明書付きのファイルを解錠する(ST136)。

[0139] 受信装置12Aのプロセッサ31は、第2鍵Aで施錠された証明書付きのファイルを解錠すると、解錠したファイルの付いていた証明書のチェックを実行する(ST136)。受信装置12Aのプロセッサ31は、証明書のチェックとして、第2鍵Aで解錠したファイルのハッシュ値を算出する(ST137a)。プロセッサ31は、ファイルのハッシュ値を算出すると、ST118で取得した送信者Oの第1鍵Oで証明書としてのデータを復号化する(ST137b)。プロセッサ31は、ファイルから算出したハッシュ値と第1鍵Oで復号化した証明書のデータとを照合することにより証明書の正当性をチェックする(ST137c)。受信装置12Aのプロセッサ31は、ファイルのハッシュ値と第1鍵Oで復号化した証明書とが一致した場合、第2鍵Aで解錠したファイルが正常であるものとする。

[0140] 受信装置12Aのプロセッサ31は、ファイルのハッシュ値と第1鍵Oで復号化した証明書とが一致した場合、つまり、証明書によってファイルの正当性が確認された場合、解錠したファイルを閲覧可能とする(ST138)。また、受信装置12Aのプロセッサ31は、ファイルのハッシュ値と第1鍵Oで復号化した証明書のデータとが一致しない場合、当該ファイルに改ざんの疑いがあるため、当該ファイルの閲覧を不可とする。

[0141] なお、上述した第5動作例は、図13および図14に示す手順で実施されるものに限定されない。例えば、ST111-ST113、ST120の処理は、ST130の前であればどの手順で実行しても良い。また、ST115-ST118の処理は、ST137の前であればどの手順で実行しても良い。

[0142] また、図13および図14を参照して説明した上述の動作例では、第5動

作例を第1動作例に組み合わせて実施した場合について説明したが、第5動作例は、第1動作例だけでなく、第2、第3又は第4動作例とを組み合わせて実施するようにしても良い。

[0143] 以上のような第5動作例によれば、実施形態に係る情報送受信システムは、受信者の生体認証で取得できる鍵で施錠されたファイル（電子データ）に証明書をつけて送受信できる。これにより、受信者は、鍵で保護され、証明書で改ざんがないことを確認できる状態のファイルを保存しておくことができる。この結果、受信者は、生体認証によって取得できる鍵によって任意のタイミングで保護されたファイルを取得でき、取得したファイルに改ざんがないことも確認できる。

[0144] すなわち、第5動作例によれば、実施形態に係る情報送受信システムは、パスワードなどを紛失でファイルが閲覧不可能となることがなく、閲覧権限のある人（生体認証を成功させることができる人）が任意のタイミングで改ざんがないことが確認されたファイルを閲覧することができる。

[0145] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] 送信装置と受信装置とを有する情報送受信システムであって、
前記受信装置は、
前記送信装置と通信する第1の通信部と、
受信者の生体認証を行う生体認証装置に接続するインターフェースと、
前記生体認証装置によって生体認証が成功した受信者の第1鍵と前記第1鍵に対応する第2鍵とを記憶する記憶部と、
前記送信装置が前記受信者の第2鍵で施錠した電子データを保存し、
前記生体認証装置によって生体認証が成功した受信者の第1鍵を用いて前記受信者の第2鍵で施錠された電子データを解錠する第1のプロセッサと、を有し、
前記送信装置は、
前記受信装置と通信する第2の通信部と、
前記受信者の第2鍵で施錠した電子データを前記受信装置へ送信する第2のプロセッサと、を有する、
情報送受信システム。
- [請求項2] 前記受信装置において、
前記第1のプロセッサは、前記電子データを送信する送信者の公開鍵で施錠した前記受信者の第2鍵を前記送信装置へ送信し、
前記送信装置において、
前記第2のプロセッサは、前記受信装置が前記送信者の公開鍵で施錠した受信者の第2鍵を解錠する、
請求項1に記載の情報送受信システム。
- [請求項3] 前記受信装置は、複数であり、
各受信装置において、
前記インターフェースは、それぞれが受信者の生体認証を行う生体認証装置に接続し、
前記記憶部は、それぞれが前記インターフェー

スに接続する前記生体認証装置によって生体認証が成功した受信者の第 1 鍵と前記第 1 鍵に対応する第 2 鍵とを記憶し、

前記第 2 のプロセッサは、前記送信装置が前記電子データの解錠を許可する複数の受信者の第 2 鍵で施錠した前記電子データを前記生体認証装置による生体認証が成功した受信者の第 1 鍵を用いて解錠し、
前記送信装置において、

前記第 2 の通信部は、前記複数の受信装置と通信し、

前記第 2 のプロセッサは、前記電子データの解錠を許可する複数の受信者の第 2 鍵で施錠した前記電子データを前記複数の受信者へ送信する、

請求項 1 に記載の情報送受信システム。

[請求項 4]

各受信装置において、

前記第 1 のプロセッサは、前記電子データを送信する送信者の公開鍵で施錠した前記受信者の第 2 鍵を前記送信装置へ送信し、

前記送信装置において、

前記第 2 のプロセッサは、前記電子データの送信先とする各受信者の受信装置が前記送信者の公開鍵で施錠した各受信者の第 2 鍵を解錠する、

請求項 3 に記載の情報送受信システム。

[請求項 5]

前記送信装置において、

前記第 2 のプロセッサは、前記電子データの解錠を許可した受信者の第 2 鍵で施錠した電子データを送信した後、前記電子データの解錠を許可する受信者を追加する場合、さらに追加する受信者の第 2 鍵で施錠した電子データを前記追加する受信者へ送信する、

請求項 3 に記載の情報送受信システム。

[請求項 6]

前記複数の受信装置のうち前記電子データの解錠を許可する受信者を追加する権限が与えられた追加権限者の受信装置において、

前記第 1 のプロセッサは、さらに前記追加権限者が前記電子データ

の解錠を許可する追加受信者の第2鍵で施錠した電子データを前記追加受信者へ送信する、

請求項3に記載の情報送受信システム。

[請求項7]

前記追加受信者の受信装置における前記第1のプロセッサは、前記追加権限者の公開鍵で施錠した前記追加受信者の第2鍵を前記追加権限者の受信装置へ送信し、

前記追加権限者の受信装置における前記第1のプロセッサは、前記追加受信者の受信装置によって前記追加権限者の公開鍵で施錠された前記追加受信者の第2鍵を解錠する、

請求項6に記載の情報送受信システム。

[請求項8]

前記送信装置において、

前記第2のプロセッサは、前記電子データを閲覧可能とする解錠条件を設定し、前記受信者の第2鍵で施錠した前記解錠条件付きの電子データを前記受信装置へ送信する、

前記受信装置において、

前記第1のプロセッサは、前記送信装置が前記受信者の第2鍵で施錠した解錠条件付きの電子データを保存し、前記生体認証装置によって生体認証が成功した場合に前記解錠条件を満たす場合には前記受信者の第1鍵を用いて前記第2鍵で施錠された前記電子データを解錠し、

請求項1乃至7の何れか1項に記載の情報送受信システム。

[請求項9]

前記送信装置において、

前記第2のプロセッサは、前記受信装置が前記電子データの正当性を示す電子証明書を作成し、前記受信者の第2鍵で施錠した電子データに前記電子証明書を添えて前記受信装置へ送信し、

前記受信装置において、

前記第1のプロセッサは、前記生体認証装置によって生体認証が成功した受信者の第1鍵を用いて施錠した電子メールに添付された前記

電子証明書を用いて前記電子データの正当性が確認された場合に前記電子データを閲覧可能とする、

請求項 1 乃至 8 の何れか 1 項に記載の情報送受信システム。

[請求項10]

前記送信装置において、

さらに、送信者の生体認証を行う生体認証装置に接続する第 2 のインターフェースを有し、

前記第 2 のプロセッサは、前記第 2 のインターフェースに接続する生体認証装置による生体認証が成功した場合に前記電子データの正当性を示す電子証明書を作成する、

請求項 9 に記載の情報送受信システム。

[請求項11]

前記送信装置において、

前記第 2 のプロセッサは、前記第 2 のインターフェースに接続する生体認証装置による生体認証が成功した送信者の第 1 鍵と前記第 1 鍵に対応する第 2 鍵とを生成し、前記電子データのハッシュ値を前記送信者の第 1 鍵で暗号化した電子証明書を作成し、

前記受信装置において、

前記第 1 のプロセッサは、前記受信者の第 2 鍵で解錠した電子データのハッシュ値と前記電子証明書を前記送信者の第 2 鍵で復号化した結果とが一致する場合に前記電子データを閲覧可能とする、

請求項 10 に記載の情報送受信システム。

[請求項12]

前記送信装置において、

前記第 2 のプロセッサは、前記受信者の公開鍵で施錠した前記送信者の第 2 鍵を前記受信装置へ送信し、

前記受信装置において、

前記第 1 のプロセッサは、前記送信装置が前記受信者の公開鍵で施錠した送信者の第 2 鍵を解錠する、

請求項 11 に記載の情報送受信システム。