

明 細 書

発明の名称：ファイルサーバ装置およびファイルサーバシステム 技術分野

[0001] 本発明の実施形態は、ファイルサーバ装置およびファイルサーバシステムに関する。

背景技術

[0002] 一般的に、例えばネットワーク上でデータを共有するために用いられるシステムとして、ファイルサーバシステムが知られている。このファイルサーバシステムの一例としては、いわゆる電子私書箱システムが挙げられる。電子私書箱システムは、例えばネットワーク上で電子データをやりとりするための私書箱に相当する。

[0003] この電子私書箱システムによれば、例えば他人に見られては困るような電子データ（以下、機密データと表記）の受け取りを代行するサービス（電子私書箱サービス）が利用者に対して提供される。

[0004] 電子私書箱システムは、電子私書箱サービスを提供する電子私書箱サーバと、当該電子私書箱サーバに対して機密データを送信する送信者によって利用される送信者装置と、当該電子私書箱サーバから機密データを受信する受信者によって利用される受信者装置とから構成される。

[0005] なお、電子私書箱システムでは、上記したように機密データを取り扱うことが考えられるため、当該機密データを暗号化して扱う必要がある。この機密データを暗号化する方式としては、一般的に、暗号化および復号に共通の鍵（共通鍵）を用いる共通鍵暗号（方式）と、暗号化および復号に別個の鍵（公開鍵および秘密鍵）を用いる公開鍵暗号（方式）とが知られている。

[0006] ところで、電子私書箱システムにおいては、一般的に不特定多数の人が送信者になると考えられる。このため、電子私書箱システムにおいて共通鍵暗号が用いられる場合には、受信者と不特定多数の送信者とが事前に共通鍵を共有していなければならない。

- [0007] また、電子私書箱システムを利用する利用者は、用途に応じて使い分けるために複数の電子私書箱（サービス）を利用する（または複数の電子私書箱サーバから電子私書箱サービスの提供を受ける）場合がある。このため、電子私書箱システムにおいて共通鍵暗号が用いられる場合には、利用者は、利用する電子私書箱（サービス）毎の鍵（共通鍵）を管理しなければならず、利用者が扱う鍵の総数が多くなる。
- [0008] したがって、電子私書箱システムにおいて機密データを暗号化する場合には、事前の鍵の共有が不要であり、利用者が扱う鍵の総数が少ない公開鍵暗号を利用することが望ましい。
- [0009] また、電子私書箱システムは、公開鍵暗号を利用した上で、更に以下の第1～第3の要件を満たすことが望ましい。
- [0010] 第1の要件は、電子私書箱システムにおいて専用の公開鍵が利用できることである。電子私書箱システムは、受信者のプライバシーを守るために利用されることが想定される。このため、電子私書箱システムには、受信者（利用者）の匿名性も必要とされる。そこで、電子私書箱システムを利用する受信者のプライバシーを確保するためには、公開鍵から当該受信者を特定できないように当該電子私書箱専用の公開鍵を利用することが望ましい。更に、同一の受信者が複数の電子私書箱サービスを利用する場合には、当該電子私書箱サービスにおいて用いられる複数の公開鍵から同一の受信者が利用する公開鍵であることを特定できないという非結合性を満たしていることが望ましい。
- [0011] 第2の要件は、電子私書箱システムを利用する受信者が管理する鍵の数が少ないことである。例えば受信者が管理する鍵の数が多くなると、鍵の管理が煩雑になり、利便性が損なわれる。特に、受信者（利用者）が多数の電子私書箱サービスを利用する場合にも管理する鍵の数が少ないことが望ましい。つまり、利用する電子私書箱サービスの数にかかわらず受信者が管理する鍵は1つであることが理想的である。
- [0012] 第3の要件は、電子私書箱サーバおよび当該サーバの管理者（以下、単に

管理者と表記) に対しても機密データの内容を秘匿できることである。電子私書箱サーバおよび管理者を信頼でき、機密データの内容を知られてもいいようなモデルでは、電子私書箱サービスの用途は限定的となる。そのため、一般的には電子私書箱サーバおよび管理者に対しても機密データの内容を秘匿できることが望ましい。また、このような電子私書箱サーバおよび管理者に対して機密データの内容を秘匿できるような仕組みがあれば、例えば当該電子私書箱サーバが攻撃を受けるまたは当該管理者が不正を働くというような事態が生じた場合であっても、その影響を小さくできるという利点がある。

[0013] ここで、上記した第1～第3の要件を満たすために、公開鍵暗号(技術)を利用した第1～第3の方式が考えられる。以下、この第1～第3の方式の各々について説明する。

[0014] なお、以下の説明においては、電子私書箱システムを利用する受信者に紐づけられた公開鍵暗号における公開鍵および秘密鍵を受信者用公開鍵および受信者用秘密鍵と称する。一方、電子私書箱(サーバ)に紐づけられた公開鍵暗号における公開鍵および秘密鍵を電子私書箱用公開鍵および電子私書箱用秘密鍵と称する。また、受信者用公開鍵および受信者用秘密鍵のペアを受信者用鍵ペア、電子私書箱用公開鍵および電子私書箱用秘密鍵のペアを電子私書箱用鍵ペアと称する。

[0015] 第1の方式は、電子私書箱システムにおいて受信者用公開鍵をそのまま電子私書箱用公開鍵として利用する、という方式である。

[0016] 第1の方式における鍵の生成および管理について説明する。第1の方式によれば、受信者装置において受信者用鍵ペアが生成され、当該受信者用鍵ペアのうちの受信者用秘密鍵は当該受信者装置において安全に管理される。一方、受信者装置において生成された受信者用鍵ペアのうちの受信者用公開鍵は、電子私書箱用公開鍵として用いるために電子私書箱サーバに登録される。

[0017] 更に、第1の方式における暗号化および復号処理(処理シーケンス)につ

いて説明する。第１の方式によれば、機密データは、電子私書箱用公開鍵（＝受信者用公開鍵）を用いて送信者装置で暗号化される。暗号化された機密データ（暗号化機密データ）は、送信者装置から電子私書箱サーバに送信される。送信者装置から電子私書箱サーバに送信された暗号化機密データは、変換等の処理が実行されることなく、当該電子私書箱サーバにおいてそのまま保持される。電子私書箱サーバにおいて保持された暗号化機密データは、当該電子私書箱サーバから受信者装置に対して送信され、受信者用秘密鍵を用いて受信者装置で復号される。

[0018] 上記したように第１の方式によれば、受信者装置（受信者）は、受信者用秘密鍵のみを安全に管理すればよい。したがって、第１の方式は、上記した第２の要件を満たす。また、第１の方式によれば、暗号化機密データは受信者用秘密鍵がなければ復号できないため、受信者本人以外は機密データの内容を知ることができない。したがって、第１の方式は、上記した第３の要件を満たす。

[0019] 第２の方式は、受信者装置（受信者）が電子私書箱用鍵ペアを生成し、当該電子私書箱用鍵ペアのうちの電子私書箱用秘密鍵を受信者装置で管理する、という方式である。

[0020] 第２の方式における鍵の生成および管理について説明する。第２の方式によれば、受信者装置において電子私書箱用鍵ペアが生成され、当該電子私書箱用鍵ペアのうちの電子私書箱用秘密鍵が当該受信者装置において安全に管理される。一方、受信者装置において生成された電子私書箱用鍵ペアのうちの電子私書箱用公開鍵は、電子私書箱サーバに登録される。なお、第２の方式において、電子私書箱用鍵ペアは、受信者用鍵ペアまたは他の電子私書箱用の鍵ペア（つまり、公開鍵および秘密鍵のペア）とは独立に生成される。また、電子私書箱用鍵ペアを１組のみ生成し、複数の電子私書箱において共通に利用する方式も考えられるが、当該方式では本質的に上記した第１の方式と同様となる。

[0021] 更に、第２の方式における暗号化および復号処理について説明する。第２

の方式によれば、機密データは、電子私書箱用公開鍵を用いて送信者装置で暗号化される。暗号化機密データは、送信者装置から電子私書箱サーバに送信される。送信者装置から電子私書箱サーバに送信された暗号化機密データは、変換等の処理が実行されることなく、当該電子私書箱サーバにおいてそのまま保持される。電子私書箱サーバにおいて保持された暗号化機密データは、当該電子私書箱サーバから受信者装置に対して送信され、電子私書箱用秘密鍵を用いて当該受信者装置で復号される。

[0022] 上記したように第2の方式によれば、電子私書箱用鍵ペアは受信者用鍵ペアとは独立に生成される。つまり、第2の方式においては、受信者用鍵ペアとは独立に生成された電子私書箱用鍵ペア（の電子私書箱用公開鍵）からは受信者を特定することができない。したがって、第2の方式は、上記した第1の要件を満たす。また、第2の方式によれば、暗号化機密データは電子私書箱用秘密鍵がなければ復号できないため、受信者本人以外は機密データの内容を知ることができない。したがって、第2の方式は、上記した第3の要件を満たすことができる。

[0023] 第3の方式は、受信者装置（受信者）が電子私書箱用鍵ペアを生成し、当該電子私書箱用鍵ペアのうちの電子私書箱用秘密鍵を電子私書箱サーバで管理する、という方式である。

[0024] 第3の方式における鍵の生成および管理について説明する。第3の方式によれば、受信者装置において電子私書箱用鍵ペアが生成される。受信者装置において生成された電子私書箱用鍵ペアは、電子私書箱サーバに送信される。受信者装置から電子私書箱サーバに送信された電子私書箱用鍵ペアのうちの電子私書箱用秘密鍵は、当該電子私書箱サーバにおいて安全に管理される。一方、受信者装置から電子私書箱サーバに送信された電子私書箱用鍵ペアのうちの電子私書箱用公開鍵は公開される。これにより、受信者装置において電子私書箱用公開鍵および電子私書箱用秘密鍵を管理する必要はない。なお、第3の方式において、電子私書箱用鍵ペアは、受信者用鍵ペアまたは他の電子私書箱用の鍵ペアとは独立に生成される。また、受信者用公開鍵は、

電子私書箱サーバに登録される。なお、ここでは電子私書箱用鍵ペアが受信者装置において生成されるものとして説明したが、当該電子私書箱用鍵ペアは、電子私書箱サーバにおいて生成されてもよい。

[0025] 更に、第3の方式における暗号化および復号処理について説明する。第3の方式によれば、機密データは、電子私書箱用公開鍵を用いて送信者装置で暗号化される。暗号化機密データは、送信者装置から電子私書箱サーバに送信される。送信者装置から電子私書箱サーバに送信された暗号化データは、電子私書箱用秘密鍵を用いて当該電子私書箱サーバで復号される。また、復号によって得られた機密データは、受信者用公開鍵を用いて電子私書箱サーバで暗号化される。これによって、電子私書箱サーバは、暗号化機密データを作り直す（再生成する）。作り直された暗号化機密データは、電子私書箱サーバから受信者装置に送信され、受信者用秘密鍵を用いて受信者装置で復号される。

[0026] 上記したように第3の方式によれば、電子私書箱用鍵ペアは受信者用鍵ペアとは独立に生成される。つまり、第3の方式においては、受信者用鍵ペアとは独立に生成された電子私書箱用鍵ペア（の電子私書箱用公開鍵）からは受信者を特定することができない。したがって、第3の方式は、上記した第1の要件を満たす。また、第3の方式によれば、受信者装置（受信者）は、受信者用秘密鍵のみを安全に管理すればよい。したがって、第3の方式は、上記した第2の要件を満たす。

先行技術文献

特許文献

[0027] 特許文献1：特許第4010766号公報

非特許文献

[0028] 非特許文献1：M. Blaze, G. Bleumer, M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. In Eurocrypt' 98, LNCS 1403, pp. 127-144, 1998

発明の概要

発明が解決しようとする課題

[0029] 上記したように第1の方式は、第2および第3の要件を満たす。しかしながら、第1の方式においては、受信者用公開鍵がそのまま電子私書箱用公開鍵として利用されるため、当該受信者用公開鍵から受信者が特定される可能性がある。したがって、第1の方式は、上記した第1の要件を満たさない。

[0030] また、第2の方式によれば、第1および第3の要件を満たす。しかしながら、第2の方式においては、受信者が利用する電子私書箱サービスの数の秘密鍵（電子私書箱用秘密鍵）を受信者装置で安全に管理しなければならない。したがって、第2の方式は、上記した第2の要件を満たさない。

[0031] また、第3の方式によれば、第1および第2の要件を満たす。しかしながら、第3の方式においては、電子私書箱サーバが電子私書箱用秘密鍵を保持しており、暗号化機密データが当該電子私書箱用秘密鍵を用いて電子私書箱サーバで復号される。つまり、第3の方式では、電子私書箱サーバおよび管理者に対して機密データの内容を秘匿することができない。したがって、第3の方式は、上記した第3の要件を満たさない。

[0032] つまり、上記した第1～第3の要件の全てを満たす方式は、知られていない。

[0033] そこで、本発明が解決しようとする課題は、専用の公開鍵を利用することができ、利用者が管理する鍵を少なくすることができ、機密データの内容を秘匿することができるファイルサーバ装置およびファイルサーバシステムを提供することにある。

課題を解決するための手段

[0034] 実施形態によれば、データを送信する送信者によって利用される送信者装置および当該データを受信する受信者によって利用される受信者装置と接続されたファイルサーバ装置が提供される。

[0035] 本実施形態に係るファイルサーバ装置は、受信手段と、再暗号化鍵格納手段と、再暗号化手段と、送信手段とを具備する。

- [0036] 受信手段は、サーバ用公開鍵を用いて前記データが暗号化されることによって得られるサーバ用暗号化データを前記送信者装置から受信する。
- [0037] 再暗号化鍵格納手段は、前記サーバ用公開鍵を用いて前記データが暗号化されることによって得られるサーバ用暗号化データを、前記サーバ用公開鍵とは異なる受信者用公開鍵であって前記受信者装置において管理される受信者用秘密鍵と対となる受信者用公開鍵を用いて前記データが暗号化されることによって得られる受信者用暗号化データに再暗号化するために用いられる再暗号化鍵を格納する。
- [0038] 再暗号化手段は、前記再暗号化鍵格納手段に格納されている再暗号化鍵を用いて、前記受信されたサーバ用暗号化データを前記受信者用暗号化データに再暗号化する。
- [0039] 送信手段は、前記再暗号化された受信者用暗号化データを前記受信者装置に送信する。

図面の簡単な説明

- [0040] [図1]第1の実施形態に係る電子私書箱システムの主として機能構成を示すブロック図。
- [図2]本実施形態に係る電子私書箱システムにおいて用いられるプロキシ再暗号化技術の概念について説明するための図。
- [図3]本実施形態に係る電子私書箱システムにおいて実行される鍵生成処理の処理手順を示すフローチャート。
- [図4]本実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理および機密データ復号処理を概念的に説明するための図。
- [図5]第1の実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理の処理手順を示すフローチャート。
- [図6]第1の実施形態に係る電子私書箱システムにおいて実行される機密データ復号処理の処理手順を示すフローチャート。
- [図7]受信者が複数の電子私書箱を利用する場合について説明するための図。
- [図8]受信者が複数の電子私書箱サーバ20を利用する場合について説明する

ための図。

[図9]第2の実施形態に係る電子私書箱システムの主として機能構成を示すブロック図。

[図10]第2の実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理の処理手順を示すフローチャート。

[図11]第2の実施形態に係る電子私書箱システムにおいて実行される機密データ復号処理の処理手順を示すフローチャート。

発明を実施するための形態

[0041] 以下、図面を参照して、各実施形態について説明する。

[0042] (第1の実施形態)

図1を参照して、第1の実施形態に係るファイルサーバシステムの構成について説明する。本実施形態に係るファイルサーバシステムは、例えばネットワーク上で電子データをやりとりするための私書箱に相当するいわゆる電子私書箱システムを想定している。以下の説明においては、本実施形態に係るファイルサーバシステムは電子私書箱システムであるものとして説明する。以下の実施形態についても同様である。

[0043] 図1は、本実施形態に係る電子私書箱システムの主として機能構成を示すブロック図である。

[0044] 図1に示すように、電子私書箱システムは、送信者装置10、電子私書箱サーバ（ファイルサーバ装置）20および受信者装置30を備える。なお、送信者装置10、電子私書箱サーバ20および受信者装置30は、それぞれ装置の各機能を実現するためのハードウェア構成、またはハードウェアとソフトウェアとの組み合わせ構成として実現されている。ソフトウェアは、予め記憶媒体またはネットワークからインストールされ、各装置10、20および30にその機能を実現させるためのプログラムからなる。

[0045] 送信者装置10は、例えば他人に見られては困るような電子データである機密データを送信する送信者によって利用される。電子私書箱サーバ20は、送信者装置10からの機密データの受け取りを代行し、受信者装置30に

転送するサービス（電子私書箱サービス）を提供する。なお、電子私書箱サーバ２０は、ネットワークを介して送信者装置１０および受信者装置３０と接続されている。受信者装置３０は、機密データを受信する受信者によって利用される。

[0046] 送信者装置１０は、データ入力部１１および暗号化処理部１２を含む。データ入力部１１は、送信者装置１０を利用する送信者の操作（要求）に応じて、機密データを入力する。

[0047] 暗号化処理部１２は、サーバ用公開鍵（電子私書箱用公開鍵）を用いてデータ入力部１１によって入力された機密データ（以下、単に機密データと表記）を暗号化する。暗号化処理部１２によって用いられるサーバ用公開鍵は、電子私書箱サーバ２０から取得される。暗号化処理部１２は、サーバ用公開鍵を用いて機密データが暗号化されることによって得られる暗号化機密データ（つまり、暗号化された機密データ）を電子私書箱サーバ２０に対して送信する。以下、サーバ用公開鍵を用いて機密データが暗号化されることによって得られる暗号化機密データをサーバ用暗号化機密データと称する。

[0048] 電子私書箱サーバ２０は、サーバ用公開鍵格納部２１、再暗号化鍵格納部２２、再暗号化処理部２３および暗号化データ格納部２４を含む。

[0049] サーバ用公開鍵格納部２１には、サーバ用公開鍵が格納される。このサーバ用公開鍵は、上記した送信者装置１０に含まれる暗号化処理部１２によって用いられる。

[0050] 再暗号化鍵格納部２２には、再暗号化鍵が格納される。再暗号化鍵格納部２２に格納されている再暗号化鍵は、サーバ用公開鍵格納部２１に格納されているサーバ用公開鍵を用いて機密データが暗号化されることによって得られる暗号化機密データ（つまり、サーバ用暗号化機密データ）を、当該サーバ用公開鍵とは異なる受信者用公開鍵を用いて当該機密データが暗号化されることによって得られる暗号化機密データ（以下、受信者用暗号化機密データと表記）に再暗号化するために用いられる。なお、受信者用公開鍵とは、後述するように受信者装置３０で管理されている受信者用秘密鍵と対となる

公開鍵である。

- [0051] 再暗号化処理部 23 は、送信者装置 10 に含まれる暗号化処理部 12 によって送信されたサーバ用暗号化機密データを受信する。
- [0052] 再暗号化処理部 23 は、再暗号化鍵格納部 22 に格納されている再暗号化鍵を用いて、受信されたサーバ用暗号化機密データを受信者用暗号化機密データに再暗号化する。
- [0053] 暗号化データ格納部 24 には、再暗号化処理部 23 によって再暗号化された受信者用暗号化機密データ（つまり、再暗号化鍵を用いてサーバ用暗号化機密データが再暗号化されることによって得られる受信者用暗号化機密データ）が格納される。なお、暗号化データ格納部 24 に格納された受信者用暗号化機密データは、例えば受信者装置 30（を利用する受信者）からの要求に応じて電子私書箱サーバ 20 から受信者装置 30 に対して送信される。
- [0054] 受信者装置 30 は、受信者用鍵生成部 31、受信者用秘密鍵格納部 32、サーバ用鍵生成部 33、再暗号化鍵生成部 34、復号処理部 35 およびデータ出力部 36 を含む。
- [0055] 受信者用鍵生成部 31 は、受信者用公開鍵および当該受信者用公開鍵と対となる受信者用秘密鍵を生成する。
- [0056] 受信者用秘密鍵格納部 32 には、受信者用鍵生成部 31 によって生成された受信者用秘密鍵が格納される。
- [0057] サーバ用鍵生成部 33 は、上記したサーバ用公開鍵および当該サーバ用公開鍵と対となるサーバ用秘密鍵を生成する。サーバ用鍵生成部 33 は、生成されたサーバ用公開鍵を電子私書箱サーバ 20 に対して送信する。なお、サーバ用鍵生成部 33 によって送信されたサーバ用公開鍵は、上記した電子私書箱サーバ 20 に含まれるサーバ用公開鍵格納部 21 に格納される。
- [0058] 再暗号化鍵生成部 34 は、受信者用鍵生成部 31 によって生成された受信者用公開鍵および受信者用秘密鍵と、サーバ用鍵生成部 33 によって生成されたサーバ用公開鍵およびサーバ用秘密鍵とを用いて、再暗号化鍵を生成する。この再暗号化鍵生成部 34 によって生成される再暗号化鍵は、上記した

サーバ用暗号化機密データを受信者用暗号化機密データに再暗号化するために用いられる鍵である。

[0059] 再暗号化鍵生成部 34 は、生成された再暗号化鍵を電子私書箱サーバ 20 に対して送信する。再暗号化鍵生成部 34 によって送信された再暗号化鍵は、電子私書箱サーバ 20 に含まれる再暗号化鍵格納部 22 に格納される。

[0060] 復号処理部 35 は、電子私書箱サーバ 20 に含まれる暗号化データ格納部 24 に格納された受信者暗号化機密データ（電子私書箱サーバ 20 から送信された受信者暗号化機密データ）を取得する。復号処理部 35 は、受信者用秘密鍵格納部 32 に格納された受信者用秘密鍵を用いて、取得された受信者用暗号化機密データを復号する。

[0061] データ出力部 36 は、復号処理部 35 によって復号された機密データ（つまり、受信者用暗号化機密データを復号することによって得られる機密データ）を出力する。

[0062] 次に、図 2 を参照して、本実施形態に係る電子私書箱システムにおいて用いられるプロキシ再暗号化技術（Proxy Re-Encryption）の概念について説明する。

[0063] ここでは、機密データ（メッセージ）100 を暗号化することによって保護しながら当該機密データ 100 をユーザ A および B が復号する場合について説明する。

[0064] まず、機密データ 100 は、ユーザ A 用公開鍵 201 を用いて暗号化される（ステップ S1）。これによって、ユーザ A 用暗号化機密データ 101 が得られる。なお、ユーザ A 用公開鍵は、ユーザ A に紐づけられた公開鍵であり、機密データ 100 を暗号化するための鍵である。ユーザ A 用公開鍵 201 は公開情報であり、当該ユーザ A 用公開鍵 201 を利用して誰でもデータを暗号化することができる。

[0065] 次に、ユーザ A は、ユーザ A 用秘密鍵 202 を用いてユーザ A 用暗号化機密データ 101 を復号する（ステップ S2）。これによって、ユーザ A は、機密データ 100 を得ることができる。なお、ユーザ A 用秘密鍵 202 は、

ユーザAに紐づけられたユーザA用公開鍵201と対となる鍵であって、当該ユーザA用公開鍵201を用いて暗号化されることによって得られる暗号化機密データを復号するための鍵である。ユーザA用秘密鍵202は秘密情報であり、当該ユーザA用秘密鍵202を知っている者のみがデータを復号することができる。

[0066] また、例えばユーザA用秘密鍵202およびユーザB用公開鍵301等を用いて、再暗号化鍵401が生成される（ステップS3）。再暗号化鍵401は、ユーザA用暗号化機密データ101をユーザB用暗号化機密データ102に再暗号化（変換）するための鍵である。ユーザB用暗号化機密データ102は、ユーザBに紐づけられた公開鍵（ユーザB用公開鍵301）を用いてデータ100が暗号化されることによって得られる暗号化機密データである。なお、再暗号化鍵401の生成には、ユーザA用秘密鍵202を利用するため、ユーザAの承認が必要である。

[0067] なお、ここではユーザA用秘密鍵202およびユーザB用公開鍵301を用いて再暗号化鍵401が生成されるものとして説明したが、これらの鍵202および301に加えてユーザA用公開鍵201およびユーザB用秘密鍵301を用いて再暗号化鍵401が生成される場合もある。

[0068] 次に、ユーザA用暗号化機密データ101は、再暗号化鍵401を用いて再暗号化される（ステップS4）。これによって、ユーザA用暗号化機密データ101は、ユーザB用暗号化機密データ102に再暗号化される。なお、再暗号化鍵401を用いたとしてもユーザA用暗号化機密データを復号することはできない。

[0069] ユーザBは、ユーザB用秘密鍵302を用いてユーザB用暗号化機密データ102を復号する（ステップS5）。これによって、ユーザBは、機密データ100を得ることができる。

[0070] 上記したように、プロキシ再暗号化技術によれば、例えばユーザA用暗号化機密データ101が復号されることなく、当該ユーザA用暗号化機密データ101をユーザB用暗号化機密データ102に再暗号化することが可能と

なる。

[0071] ここで、上記したプロキシ再暗号化で利用する記号について説明する。

[0072] このプロキシ再暗号化は、公開鍵暗号系に関する概念であり、基本的なモデルは鍵生成、暗号化、復号、再暗号化鍵生成、再暗号化の5つの関数からなる。なお、鍵生成、暗号化、復号については通常の公開鍵暗号と同様である。

[0073] プロキシ再暗号化における鍵生成アルゴリズム $KeyGen$ は、セキュリティパラメータ 1^k を入力とし、公開鍵 pk と秘密鍵 sk の組 (pk, sk) を出力する。つまり、 $KeyGen(1^k) \rightarrow (pk, sk)$ である。

[0074] プロキシ再暗号化における暗号化アルゴリズム Enc は、対象 A （例えば、ユーザ A ）の公開鍵 pk_A と機密データ（平文） m を入力とし、当該ユーザ A 用暗号化機密データ（暗号文） C_A を出力する。つまり、 $Enc(pk_A, m) \rightarrow C_A$ である。

[0075] プロキシ再暗号化における復号アルゴリズム Dec は、ユーザ A 用秘密鍵 sk_A およびユーザ A 用暗号化機密データ C_A を入力とし、機密データ m を出力する。つまり、 $Dec(sk_A, C_A) \rightarrow m$ である。

[0076] プロキシ再暗号化における再暗号化鍵生成アルゴリズム $ReKeyGen$ は、例えばユーザ A 用公開鍵 pk_A 、ユーザ A 用秘密 sk_A 、ユーザ B 用公開鍵 pk_B 、ユーザ B 用秘密 sk_B を入力とし、再暗号化鍵 $rk_{A \rightarrow B}$ を出力する。つまり、 $ReKeyGen(pk_A, sk_A, pk_B, sk_B) \rightarrow rk_{A \rightarrow B}$ である。

[0077] プロキシ再暗号化における再暗号アルゴリズム $ReEnc$ は、再暗号化鍵 $rk_{A \rightarrow B}$ およびユーザ A 用暗号化機密データ C_A を入力とし、ユーザ B 用暗号化機密データ（暗号文） C_B を出力する。つまり、 $ReEnc(rk_{A \rightarrow B}, C_A) \rightarrow C_B$ である。

[0078] 上記した鍵生成、暗号化、復号、再暗号化鍵生成および再暗号化が基本的なモデルであるが、実現方式によっては関数への入力異なる場合、または上記以外の関数または鍵を含む場合がある。

[0079] 具体的には、再暗号化鍵生成アルゴリズムの入力に $s k_B$ を必要としない *non-interactive* と呼ばれるモデル等がある。

[0080] 更に、再暗号化鍵 $r k_{A \rightarrow B}$ を用いてユーザ A 用暗号化機密データ C_A からユーザ B 用暗号化機密データ C_B の再暗号化を行うことができる一方で、その逆のユーザ B 用暗号化機密データ C_B からユーザ A 用暗号化機密データ C_A の再暗号化を行うことができない *unidirectional* と呼ばれるモデル、および当該再暗号化鍵 $r k_{A \rightarrow B}$ を用いてユーザ A 用暗号化機密データ C_A およびユーザ B 用暗号化機密データ C_B を相互に再暗号化することができる *bidirectional* と呼ばれるモデルもある。なお、*bidirectional* モデルにおいては、再暗号化鍵 $r k_{A \rightarrow B}$ を $r k_{A \leftrightarrow B}$ と表される場合がある。

[0081] 更に、公開鍵暗号の中でも ID ベース暗号に基づく方式がある。この場合、マスター鍵生成のための関数 *Setup* が増え、鍵生成 *KeyGen* の入力にマスター鍵および ID が追加される。なお、ID ベース暗号において、公開鍵 $p k$ は ID そのものである。

[0082] 以下、本実施形態に係る電子私書箱システムの動作について説明する。本実施形態に係る電子私書箱システムにおいては、鍵生成処理、機密データ暗号化処理および機密データ復号処理の 3 つの処理が実行される。以下、鍵生成処理、機密データ暗号化処理および機密データ復号処理の各々について説明する。

[0083] まず、図 3 のフローチャートを参照して、本実施形態に係る電子私書箱システムにおいて実行される鍵生成処理の処理手順について説明する。この鍵生成処理は、後述する機密データ暗号化処理および機密データ復号処理の前処理として実行される。

[0084] 受信者装置 30 に含まれる受信者用鍵生成部 31 は、上記した *KeyGen* (1^k) を実行し、受信者用公開鍵 ($p k_{RCV}$) および受信者用秘密鍵 ($s k_{RCV}$) を生成する (ステップ S11)。

[0085] 受信者用鍵生成部 31 は、生成された受信者用秘密鍵を受信者用秘密鍵格

納部 3 2 に格納する（ステップ S 1 2）。なお、受信者用鍵生成部 3 1 によって生成された受信者用公開鍵は公開される。

[0086] なお、既に受信者用公開鍵および受信者用秘密鍵が生成されており、受信者用秘密鍵が受信者用秘密鍵格納部 3 2 に格納されている場合は、上記ステップ S 1 1 およびステップ S 1 2 は実行されない。

[0087] 次に、サーバ用鍵生成部 3 3 は、上記した $KeyGen(1^k)$ を実行し、サーバ用公開鍵 (pk_{BOX}) およびサーバ用秘密鍵 (sk_{BOX}) を生成する（ステップ S 1 3）。

[0088] 再暗号化鍵生成部 3 4 は、上記した $ReKeyGen(pk_{BOX}, sk_{BOX}, pk_{RCV}, sk_{RCV})$ を実行し、再暗号化鍵 ($rk_{BOX \rightarrow RCV}$) を生成する（ステップ S 1 4）。つまり、再暗号化鍵生成部 3 4 は、受信者用鍵生成部 3 1 によって生成された受信者用公開鍵および受信者用秘密鍵とサーバ用鍵生成部 3 3 によって生成されたサーバ用公開鍵およびサーバ用秘密鍵とを用いて再暗号化鍵を生成する。

[0089] 再暗号化鍵は、サーバ用公開鍵を用いて暗号化された暗号化機密データ（サーバ用暗号化機密データ）を、受信者用公開鍵を用いて暗号化された暗号化機密データ（受信者用暗号化機密データ）に再暗号化するために用いられる。

[0090] なお、再暗号化鍵生成部 3 4 によって再暗号化鍵が生成されると、サーバ用鍵生成部 3 3 によって生成されたサーバ用秘密鍵 (sk_{BOX}) は削除されてもよい。

[0091] 次に、受信者装置 3 0（に含まれるサーバ用鍵生成部 3 3 および再暗号化鍵生成部 3 4）は、当該サーバ用鍵生成部 3 3 によって生成されたサーバ用公開鍵および当該再暗号化鍵生成部 3 4 によって生成された再暗号化鍵を電子私書箱サーバ 2 0 に対して送信する（ステップ S 1 5）。

[0092] 電子私書箱サーバ 2 0 は、受信者装置 3 0 によって送信されたサーバ用公開鍵および再暗号化鍵を受信する。

[0093] 電子私書箱サーバ 2 0 によって受信されたサーバ用公開鍵は、当該電子私

書箱サーバ２０に含まれるサーバ用公開鍵格納部２１に格納される（ステップＳ１６）。

[0094] また、電子私書箱サーバ２０によって受信された再暗号化鍵は、当該電子私書箱サーバ２０に含まれる再暗号化鍵格納部２２に格納される（ステップＳ１７）。ステップＳ１７の処理が実行されると、鍵生成処理は終了される。

[0095] 次に、図４を参照して、本実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理および機密データ復号処理を概念的に説明する。

[0096] まず、機密データ暗号化処理では、サーバ用公開鍵を用いることによって機密データが暗号化される（ステップＳ２１）。これによって、サーバ用暗号化機密データが得られる。

[0097] 次に、再暗号化鍵を用いることによってサーバ用暗号化機密データが受信者用暗号化機密データに再暗号化（変換）される（ステップＳ２２）。

[0098] また、機密データ復号処理では、受信者用暗号化機密データが受信者用秘密鍵を用いて復号される。

[0099] このように機密データ暗号化処理および機密データ復号処理が実行されることによって、本実施形態に係る電子私書箱システムにおいてはデータの機密性および受信者のプライバシーを保ちつつ、受信者が管理する鍵を減らすことができる。

[0100] 以下、本実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理および機密データ復号処理について詳細に説明する。

[0101] 図５のフローチャートを参照して、本実施形態に係る電子私書箱システムにおいて実行される機密データ暗号化処理の処理手順について説明する。

[0102] まず、送信者装置１０に含まれるデータ入力部１１は、当該送信者装置１０を利用する送信者の要求（操作）に応じて、機密データを入力する（ステップＳ３１）。

[0103] 暗号化処理部１２は、電子私書箱サーバ２０に含まれるサーバ用公開鍵格

納部 21 に格納されているサーバ用公開鍵 (pk_{BOX}) の取得要求を出し (ステップ S32)、電子私書箱サーバ 20 が送信するサーバ用公開鍵を受信する (ステップ S33)。

[0104] 暗号化処理部 12 は、取得されたサーバ用公開鍵を用いてデータ入力部 11 によって入力された機密データを暗号化する (ステップ S34)。これによって、暗号化処理部 12 は、サーバ用公開鍵を用いて暗号化された機密データ (つまり、サーバ用暗号化機密データ) を取得する。つまり、暗号化処理部 12 は、上記した $Enc(pk_{BOX}, m)$ を実行し、その出力としてサーバ用暗号化機密データ (C_{BOX}) を取得する。

[0105] 暗号化処理部 12 は、取得されたサーバ用暗号化機密データを電子私書箱サーバ 20 に送信する (ステップ S35)。

[0106] 電子私書箱サーバ 20 に含まれる再暗号化処理部 23 は、送信者装置 10 に含まれる暗号化処理部 12 によって送信されたサーバ用暗号化機密データを受信する。再暗号化処理部 23 は、サーバ用暗号化機密データが受信されると、再暗号化鍵格納部 22 に格納されている再暗号化鍵 ($rk_{BOX \rightarrow RCV}$) を取得する (ステップ S36)。

[0107] 次に、再暗号化処理部 23 は、取得された再暗号化鍵を用いて、受信されたサーバ用暗号化機密データを受信者用暗号化機密データに再暗号化する (ステップ S37)。これによって、再暗号化処理部 23 は、受信者用暗号化機密データを取得する。つまり、再暗号化処理部 23 は、上記した $ReEnc(rk_{BOX \rightarrow RCV}, C_{BOX})$ を実行し、その出力として受信者用暗号化機密データ (C_{RCV}) を取得する。

[0108] なお、再暗号化鍵を用いて再暗号化処理が実行された場合であっても、サーバ用暗号化機密データおよび受信者用暗号化機密データは復号されることはない。

[0109] 再暗号化処理部 23 は、取得された受信者用暗号化機密データを暗号化データ格納部 24 に格納する (ステップ S38)。ステップ S38 の処理が実行されると、機密データ暗号化処理は終了される。

[0110] 次に、図6のフローチャートを参照して、機密データ復号処理の処理手順について説明する。この機密データ復号処理は、例えば受信者装置30を利用する受信者からの要求に応じて実行される。

[0111] まず、受信者装置30の復号処理部35は、受信者用秘密鍵格納部32に格納されている受信者用秘密鍵 (sk_{RCV}) を取得する (ステップS41)。

[0112] 復号処理部35は、電子私書箱サーバ20に含まれる暗号化データ格納部24に格納されている受信者用暗号化機密データ (C_{RCV}) の取得要求を出し (ステップS42)、電子私書箱サーバ20が送信する受信者用暗号化機密データを受信する (ステップS43)。暗号化データ格納部24に格納されている受信者用暗号化機密データは、例えば受信者からの要求に応じて電子私書箱サーバ20から送信される。これによって、復号処理部35は、受信者用暗号化機密データを取得する。

[0113] 次に、復号処理部35は、ステップS41において取得された受信者用秘密鍵を用いて、ステップS43において取得された受信者用暗号化機密データを復号する (ステップS44)。つまり、復号処理部35は、上記した $Dec(sk_{RCV}, C_{RCV})$ を実行し、その出力として復号された機密データ (m) を取得する。

[0114] データ出力部36は、復号処理部35によって取得された機密データ (復号された機密データ) を出力する (ステップS45)。ステップS45の処理が実行されると、機密データ復号処理は終了される。

[0115] 上記したように本実施形態においては、送信者装置においてサーバ用公開鍵を用いて機密データが暗号化され、ファイルサーバ装置 (電子私書箱サーバ) 20においてサーバ用暗号化機密データが再暗号化鍵を用いて受信者用暗号化機密データに再暗号化され、受信者装置において受信者用暗号化データが受信者用秘密鍵を用いて復号され、当該復号されることによって得られた機密データが出力される。

[0116] これにより、本実施形態においては、送信者装置10においては受信者用公開鍵ではなくサーバ用公開鍵が用いられるため、当該受信者用公開鍵から

受信者が特定されることがなく受信者のプライバシーを確保することができる。

[0117] また、本実施形態においては、受信者装置 30 において管理すべき鍵は受信者用秘密鍵のみであるため、受信者が管理する鍵の数が少なく利便性が高い。

[0118] 更に、本実施形態においては、電子私書箱サーバ（ファイルサーバ装置）20 においてサーバ用暗号化機密データが再暗号化鍵を用いて受信者用暗号化機密データに再暗号化されるだけであり、当該サーバ用暗号化機密データおよび受信者用暗号化機密データは復号されることはないため、当該ファイルサーバ装置 20 およびその管理者に対しても機密データの内容を秘匿できる。

[0119] また、本実施形態においては、暗号化データ格納部 24 に、受信者用暗号化機密データが保存されているため、受信者装置 30 からの受信者用暗号化機密データ取得要求に対する応答が速いという特長がある。

[0120] したがって、本実施形態においては、受信者用公開鍵でなく専用の公開鍵（つまり、サーバ用公開鍵）を利用することができ、受信者（利用者）が管理する鍵を少なくすることができ、更には、ファイルサーバ装置 20 およびその管理者に対しても機密データの内容を秘匿することができる。

[0121] なお、本実施形態においては、受信者装置 30 を利用する受信者（および送信者装置 10 を利用する送信者）が 1 つの電子私書箱（サービス）を利用するものとして説明したが、受信者は、1 つの電子私書箱サーバ 20 において複数の電子私書箱を利用しても構わない。この場合、図 7 に示すように、複数の送信者装置 10 の各々を利用する送信者は、1 つの電子私書箱サーバ 20 における複数の電子私書箱に対してデータを送信することができる。

[0122] 更に、図 8 に示すように、受信者が複数の電子私書箱サーバ 20 を利用する構成であっても構わない。また、複数の電子私書箱サーバ 20 が複数の電子私書箱（サービス）を提供しても構わない。

[0123] また、本実施形態においては、受信者用公開鍵（ $p k_{RCV}$ ）は公開されるも

のとして説明したが、当該受信者用公開鍵を公開せず、当該受信者用公開鍵および受信者用秘密鍵 ($p k_{RCV}$, $s k_{RCV}$) の組 (ペア) を受信者装置 30 において管理する構成であってもよい。

[0124] また、本実施形態においては、機密データ暗号化処理において送信者装置 10 (に含まれる暗号化処理部 12) が電子私書箱サーバ 20 (に含まれるサーバ用公開鍵格納部 21) からサーバ用公開鍵を取得するものとして説明したが、送信者装置 10 は、例えばサーバ用公開鍵を必要なときにオンラインで取得してもよいし、サーバ用公開鍵を事前に取得しておいてローカルに保存しておいても構わない。

[0125] また、本実施形態においては、機密データ復号処理において受信者からの要求に応じて受信者用暗号化機密データが取得されるものとして説明したが、当該受信者用暗号化機密データを取得する方法は、受信者装置 30 が当該受信者からの要求に応じて受信者用暗号化機密データを取得するプル型であってもよいし、例えば電子私書箱サーバ 20 が再暗号化処理後に受信者用暗号化機密データを受信者装置 30 に送信するプッシュ型であっても構わない。

[0126] また、本実施形態においては、再暗号化処理部 23 によって再暗号化された受信者用暗号化機密データが暗号化データ格納部 24 に格納されるものとして説明したが、当該受信者用暗号化機密データが暗号化データ格納部 24 に格納されることなく受信者装置 30 に転送 (送信) される構成であっても構わない。

[0127] また、本実施形態においては、サーバ用公開鍵およびサーバ用秘密鍵 ($p k_{BOX}$, $s k_{BOX}$) は受信者装置 30 (に含まれるサーバ用鍵生成部 33) によって生成されるものとして説明したが、当該サーバ用公開鍵およびサーバ用秘密鍵は電子私書箱サーバ 20 側で生成されても構わない。この場合には、受信者装置 30 において再暗号化鍵を生成するために、電子私書箱サーバ 20 において生成されたサーバ用公開鍵およびサーバ用秘密鍵は受信者装置 30 に対して送信される。なお、上述した *non-interactive*

と呼ばれるモデルのプロキシ再暗号化を利用すれば、受信者装置 30 が受信者用公開鍵 ($p k_{RCV}$) を電子私書箱サーバ 20 に対して送信し、電子私書箱サーバ 20 において再暗号化鍵を生成することもできる。

[0128] また、本実施形態において利用されるプロキシ再暗号化は、ID ベースではない方式が利用されてもよいし、ID ベースの方式が利用されてもよい。

[0129] (第 2 の実施形態)

次に、図 9 乃至図 11 を参照して、第 2 の実施形態に係る電子私書箱システム (ファイルサーバシステム) の構成について説明する。なお、前述した図 1、図 5 および図 6 と同様の部分には同一参照符号を付してその詳しい説明を省略する。ここでは、図 9 乃至図 11 がそれぞれ図 1、図 5 および図 6 と異なる部分について主に述べる。

[0130] 本実施形態においては、電子私書箱システムに備えられる電子私書箱サーバにおいてサーバ用暗号化機密データが格納される点が前述した第 1 の実施形態とは異なる。

[0131] 図 9 に示すように、本実施形態に係る電子私書箱システムは、電子私書箱サーバ (ファイルサーバ装置) 40 を備える。

[0132] 電子私書箱サーバ 40 は、暗号化データ格納部 41 および再暗号化処理部 42 を含む。図 10 に示すように、図 5 と異なり暗号化データ格納部 41 には、送信者装置 10 に含まれる暗号化処理部 12 によって送信されたサーバ用暗号化機密データが格納される (ステップ S 51)。

[0133] 図 11 に示すように、図 6 と異なり再暗号化処理部 42 は、例えば受信者装置 30 (を利用する受信者) からの要求に応じて、再暗号化鍵格納部 22 に格納されている再暗号化鍵 ($r k_{BOX \rightarrow RCV}$) を取得し (ステップ S 52)、暗号化データ格納部 41 に格納されているサーバ用暗号化機密データを受信者用暗号化機密データに再暗号化する (ステップ S 53)。なお、再暗号化処理部 42 は、前述した第 1 の実施形態と同様に、再暗号化鍵格納部 22 に格納されている再暗号化鍵を用いて再暗号化処理を実行する。

[0134] 再暗号化処理部 42 によって再暗号化された受信者用暗号化機密データは

、前述した第1の実施形態と同様に、受信者装置30に含まれる復号処理部35によって復号される。

[0135] 上記したように本実施形態においては、電子私書箱サーバ40に含まれる暗号化データ格納部41にサーバ用暗号化機密データが格納され、受信者からの要求に応じて当該暗号化データ格納部41に格納されたサーバ用暗号化機密データが受信者用暗号化機密データに再暗号化される。

[0136] これにより、本実施形態においては、前述した第1の実施形態と同様に、受信者用公開鍵でなく専用の公開鍵を利用することができ、受信者が管理する鍵を少なくすることができ、更には、電子私書箱サーバ（ファイルサーバ装置）20およびその管理者に対しても機密データの内容を秘匿することができる。

[0137] また、本実施形態においては、暗号化データ格納部24に、サーバ用暗号化機密データが保存されているため、受信者用公開鍵および受信者用秘密鍵が変わった場合にも、暗号化データ格納部24に格納されているデータを更新する必要がないという特長がある。

[0138] なお、本実施形態においても第1の実施形態と同様に、受信者装置30を利用する受信者（および送信者装置10を利用する送信者）が1つの電子私書箱（サービス）を利用するものとして説明したが、受信者は、1つの電子私書箱サーバ20において複数の電子私書箱を利用しても構わない。この場合も、図7に示すように、複数の送信者装置10の各々を利用する送信者は、1つの電子私書箱サーバ20における複数の電子私書箱に対してデータを送信することができる。

[0139] 更に、図8に示すように、受信者が複数の電子私書箱サーバ20を利用する構成であっても構わない。また、複数の電子私書箱サーバ20が複数の電子私書箱（サービス）を提供しても構わない。

[0140] また、本実施形態においても第1の実施形態と同様に、受信者用公開鍵（ pk_{RCV} ）は公開されるものとして説明したが、当該受信者用公開鍵を公開せず、当該受信者用公開鍵および受信者用秘密鍵（ pk_{RCV} , sk_{RCV} ）の組（

ペア)を受信者装置30において管理する構成であってもよい。

[0141] また、本実施形態においても第1の実施形態と同様に、機密データ暗号化処理において送信者装置10(に含まれる暗号化処理部12)が電子私書箱サーバ20(に含まれるサーバ用公開鍵格納部21)からサーバ用公開鍵を取得するものとして説明したが、送信者装置10は、例えばサーバ用公開鍵を必要なときにオンラインで取得してもよいし、サーバ用公開鍵を事前に取得しておいてローカルに保存しておいても構わない。

[0142] また、本実施形態においても第1の実施形態と同様に、機密データ復号処理において受信者からの要求に応じて受信者用暗号化機密データが取得されるものとして説明したが、当該受信者用暗号化機密データを取得する方法は、受信者装置30が当該受信者からの要求に応じて受信者用暗号化機密データを取得するプル型であってもよいし、例えば電子私書箱サーバ20が再暗号化処理後に受信者用暗号化機密データを受信者装置30に送信するプッシュ型であっても構わない。

[0143] また、本実施形態においても第1の実施形態と同様に、再暗号化処理部23によって再暗号化された受信者用暗号化機密データが暗号化データ格納部24に格納されるものとして説明したが、当該受信者用暗号化機密データが暗号化データ格納部24に格納されることなく受信者装置30に転送(送信)される構成であっても構わない。

[0144] また、本実施形態においても第1の実施形態と同様に、サーバ用公開鍵およびサーバ用秘密鍵(pk_{BOX} , sk_{BOX})は受信者装置30(に含まれるサーバ用鍵生成部33)によって生成されるものとして説明したが、当該サーバ用公開鍵およびサーバ用秘密鍵は電子私書箱サーバ20側で生成されても構わない。この場合には、受信者装置30において再暗号化鍵を生成するために、電子私書箱サーバ20において生成されたサーバ用公開鍵およびサーバ用秘密鍵は受信者装置30に対して送信される。なお、上述した *non-interactive* と呼ばれるモデルのプロキシ再暗号化を利用すれば、受信者装置30が受信者用公開鍵(pk_{RCV})を電子私書箱サーバ20に対

して送信し、電子私書箱サーバ20において再暗号化鍵を生成することもできる。

[0145] また、本実施形態において利用されるプロキシ再暗号化も第1の実施形態と同様に、IDベースではない方式が利用されてもよいし、IDベースの方式が利用されてもよい。

[0146] 以上で説明した少なくとも1つの実施形態によれば、専用の公開鍵を利用することができ、利用者が管理する鍵を少なくすることができ、機密データの内容を秘匿することができるファイルサーバ装置（電子私書箱サーバ）およびファイルサーバシステム（電子私書箱システム）を提供することができる。

[0147] なお、本願発明は、上記の各実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記各実施形態に開示されている複数の構成要素の適宜な組合せにより種々の発明を形成できる。例えば、各実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組合せてもよい。

符号の説明

[0148] 10…送信者装置、11…データ入力部、12…暗号化処理部、20…電子私書箱サーバ（ファイルサーバ装置）、21…サーバ用公開鍵格納部、22…再暗号化鍵格納部、23…再暗号化処理部、24…暗号化データ格納部、30…受信者装置、31…受信者用鍵生成部、32…受信者用秘密鍵格納部、34…再暗号化鍵生成部、35…復号処理部、36…データ出力部。

請求の範囲

[請求項1] データを送信する送信者によって利用される送信者装置および当該データを受信する受信者によって利用される受信者装置と接続されたファイルサーバ装置において、

サーバ用公開鍵を用いて前記データが暗号化されることによって得られるサーバ用暗号化データを前記送信者装置から受信する受信手段と、

前記サーバ用公開鍵を用いて前記データが暗号化されることによって得られるサーバ用暗号化データを、前記サーバ用公開鍵とは異なる受信者用公開鍵であって前記受信者装置において管理される受信者用秘密鍵と対となる受信者用公開鍵を用いて前記データが暗号化されることによって得られる受信者用暗号化データに再暗号化するために用いられる再暗号化鍵を格納する再暗号化鍵格納手段と、

前記再暗号化鍵格納手段に格納されている再暗号化鍵を用いて、前記受信されたサーバ用暗号化データを前記受信者用暗号化データに再暗号化する再暗号化手段と、

前記再暗号化された受信者用暗号化データを前記受信者装置に送信する送信手段と

を具備することを特徴とするファイルサーバ装置。

[請求項2] 前記再暗号化された受信者用暗号化データを格納する暗号化データ格納手段を更に具備し、

前記送信手段は、前記受信者の要求に応じて前記暗号化データ格納手段に格納された受信者用暗号化データを前記受信者装置に送信することを特徴とする請求項1記載のファイルサーバ装置。

[請求項3] 前記受信されたサーバ用暗号化データを格納する暗号化データ格納手段を更に具備し、前記再暗号化手段は、前記受信者の要求に応じて、前記再暗号化鍵格納手段に格納されている再暗号化鍵を用いて前記暗号化データ格納手段に格納されたサーバ用暗号化データを前記受

信者用暗号化データに再暗号化する

ことを特徴とする請求項 1 記載のファイルサーバ装置。

[請求項4]

データを送信する送信者によって利用される送信者装置と、当該データを受信する受信者によって利用される受信者装置と、当該送信者装置および当該受信者装置と接続されるファイルサーバ装置を具備し、

前記送信者装置は、

前記送信者の操作に応じて前記データを入力する入力手段と、

サーバ用公開鍵を用いて前記入力されたデータを暗号化することによってサーバ用暗号化データを取得する暗号化手段と

を含み、

前記ファイルサーバ装置は、

前記サーバ用公開鍵を用いて前記データが暗号化されることによって得られるサーバ用暗号化データを、前記サーバ用公開鍵とは異なる受信者用公開鍵を用いて当該データが暗号化されることによって得られる受信者用暗号化データに再暗号化するために用いられる再暗号化鍵を格納する再暗号化鍵格納手段と、

前記再暗号化鍵格納手段に格納されている再暗号化鍵を用いて、前記暗号化手段によって取得されたサーバ用暗号化データを前記受信者用暗号化データに再暗号化する再暗号化手段と

を含み、

前記受信者装置は、

前記受信者用公開鍵と対となる受信者用秘密鍵を格納する秘密鍵格納手段と、

前記秘密鍵格納手段に格納されている受信者用秘密鍵を用いて、前記再暗号化された受信者用暗号化データを復号する復号手段と、

前記受信者用暗号化データが復号されることによって得られるデータを出力する出力手段と

を含む

ことを特徴とするファイルサーバシステム。

[請求項5]

前記受信者装置は、

前記受信者用公開鍵および当該受信者用公開鍵と対となる受信者用秘密鍵を生成する受信者用鍵生成手段と、

前記生成された受信者用秘密鍵を前記秘密鍵格納手段に格納する受信者用秘密鍵格納処理手段と、

前記サーバ用公開鍵および当該サーバ用公開鍵と対となるサーバ用秘密鍵を生成するサーバ用鍵生成手段と、

前記受信者用鍵生成手段によって生成された受信者用公開鍵および受信者用秘密鍵と前記サーバ用鍵生成手段によって生成されたサーバ用公開鍵およびサーバ用秘密鍵とを用いて、前記再暗号化鍵を生成する再暗号化鍵生成手段と

を更に含み、

前記ファイルサーバ装置は、

前記サーバ用鍵生成手段によって生成されたサーバ用公開鍵を格納するサーバ用公開鍵格納手段と、

前記再暗号化鍵生成手段によって生成された再暗号化鍵を前記再暗号化鍵格納手段に格納する再暗号化鍵格納処理手段と

を更に含み、

前記送信者装置に含まれる暗号化手段は、前記ファイルサーバ装置に含まれるサーバ用公開鍵格納手段に格納されたサーバ用公開鍵を用いて前記入力されたデータを暗号化する

ことを特徴とする請求項4記載のファイルサーバシステム。