(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 8 月 23 日(23.08.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/111714 A1

(51) 国際特許分類:
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2012/053547

(22) 国際出願日: 2012 年 2 月 15 日(15.02.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2011-030813 2011 年 2 月 16 日(16.02.2011) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 吉田 琢也 (YOSHIDA, Takuya) [JP/JP]. 岡田 光司 (OKADA, Koji) [JP/JP].

(74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門１丁目１２番９号 鈴榮特許綜合事務所内 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW,

[続葉有]

(54) **Title**: FILE SERVER DEVICE AND FILE SERVER SYSTEM

(54) 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

[図1]

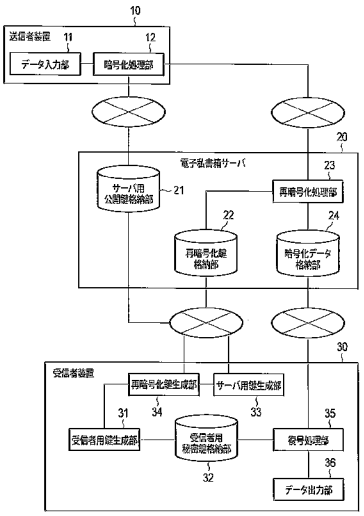


FIG. 1:
10 TRANSMITTER DEVICE
11 DATA INPUT UNIT
12 ENCRYPTION PROCESSING UNIT
20 ELECTRONIC PRIVATE MAILBOX SERVER
21 SERVER-USE PUBLIC KEY STORAGE UNIT
22 RE-ENCRYPTION KEY STORAGE UNIT
23 RE-ENCRYPTION PROCESSING UNIT
24 ENCRYPTED DATA STORAGE UNIT
30 RECEIVER DEVICE
31 RECEIVER-USE KEY GENERATING UNIT
32 RECEIVER-USE PRIVATE KEY STORAGE UNIT
33 SERVER-USE KEY GENERATING UNIT
34 RE-ENCRYPTION KEY GENERATING UNIT
35 DECODING PROCESSING UNIT
36 DATA OUTPUT UNIT

(57) **Abstract**: From a transmission device, a receiving means receives server-use encrypted data obtained by encrypting data using a server-use public key. A re-encryption key storage means stores a re-encryption key used for re-encrypting server-use encrypted data into receiver-use encrypted data obtained by encrypting the data using a receiver-use public key different from the server-use public key. A re-encryption means uses the re-encryption key stored in the re-encryption key storage means to re-encrypt the received server-use encrypted data into receiver-use encrypted data. A transmission means transmits the re-encrypted receiver-use encrypted data to the receiver device.

(57) 要約: 受信手段は、サーバ用公開鍵を用いてデータを暗号化することによって得られるサーバ用暗号化データを送信者装置から受信する。再暗号化鍵格納手段は、サーバ用暗号化データを、サーバ用公開鍵とは異なる受信者用公開鍵を用いてデータを暗号化す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。再暗号化手段は、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、受信されたサーバ用暗号化データを受信者用暗号化データに再暗号化する。送信手段は、再暗号化された受信者用暗号化データを受信者装置に送信する。

WO 2012/111714 A1

MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

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できることが望ましい。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）→（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）→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）→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$rk_{A\to B}$を出力する。つまり、ＲｅＫｅｙＧｅｎ（pk_A，sk_A，pk_B，sk_B）→$rk_{A\to B}$である。

[0077] プロシキ再暗号化における再暗号アルゴリズムＲｅＥｎｃは、再暗号化鍵$rk_{A\to B}$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（$rk_{A\to B}$，C_A）→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が異なる場合、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sk_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$rk_{A\to B}$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$rk_{A\to B}$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用暗号機密データC_Bを相互に再暗号化することができるｂｉｄｉｒｅｃｄｔｉｏｎａｌ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$rk_{A\to B}$を$rk_{A\Leftrightarrow B}$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ｐｋ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（pk_{RCV}）および受信者用秘密鍵（sk_{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３２に格納する（ステップＳ１２）。なお、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３２に格納されている場合は、上記ステップＳ１１およびステップＳ１２は実行されない。

[0087] 次に、サーバ用鍵生成部３３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Ｓ１３）。

[0088] 再暗号化鍵生成部３４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Ｓ１４）。つまり、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。

[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３４によって再暗号化鍵が生成されると、サーバ用鍵生成部３３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３０（に含まれるサーバ用鍵生成部３３および再暗号化鍵生成部３４）は、当該サーバ用鍵生成部３３によって生成されたサーバ用公開鍵および当該再暗号化鍵生成部３４によって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（ステップＳ１５）。

[0092] 電子私書箱サーバ２０は、受信者装置３０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２０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（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。

[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（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。

[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Ｓ５１）。

[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（$rk_{BOX \rightarrow RCV}$）を取得し（ステップＳ５２）、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、

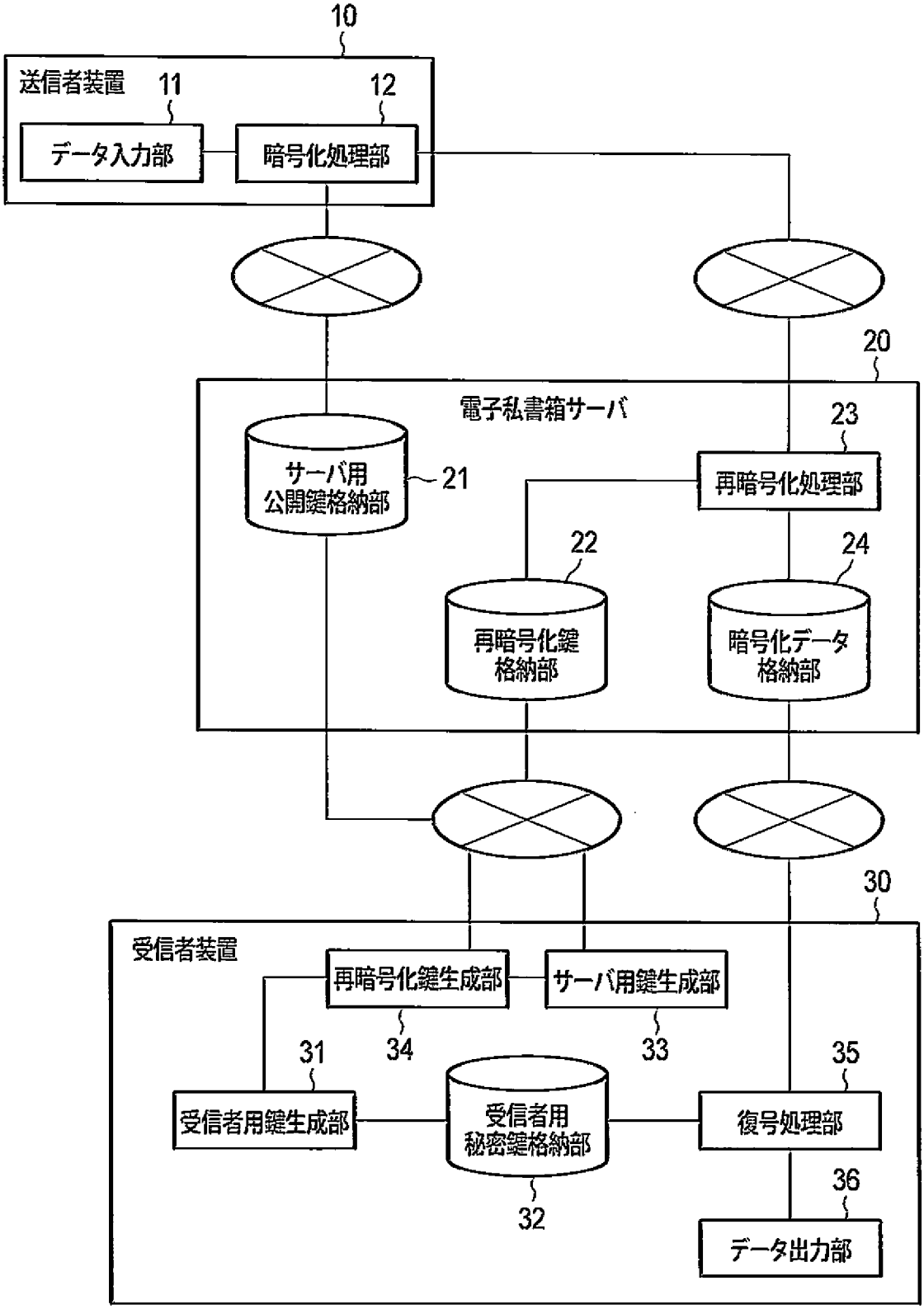
前記再暗号化鍵生成手段によって生成された再暗号化鍵を前記再暗号化鍵格納手段に格納する再暗号化鍵格納処理手段と

を更に含み、

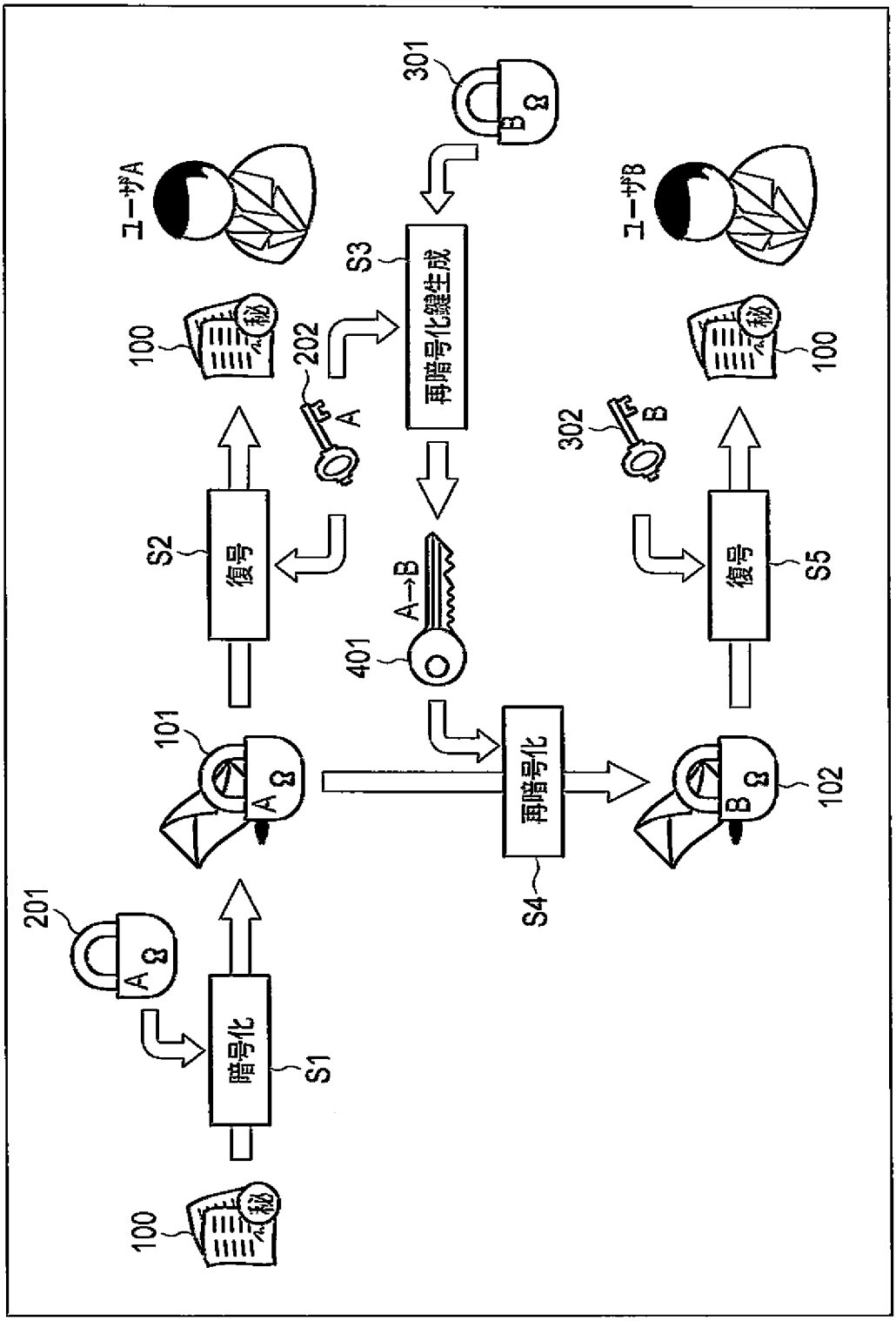
前記送信者装置に含まれる暗号化手段は、前記ファイルサーバ装置に含まれるサーバ用公開鍵格納手段に格納されたサーバ用公開鍵を用いて前記入力されたデータを暗号化する

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。

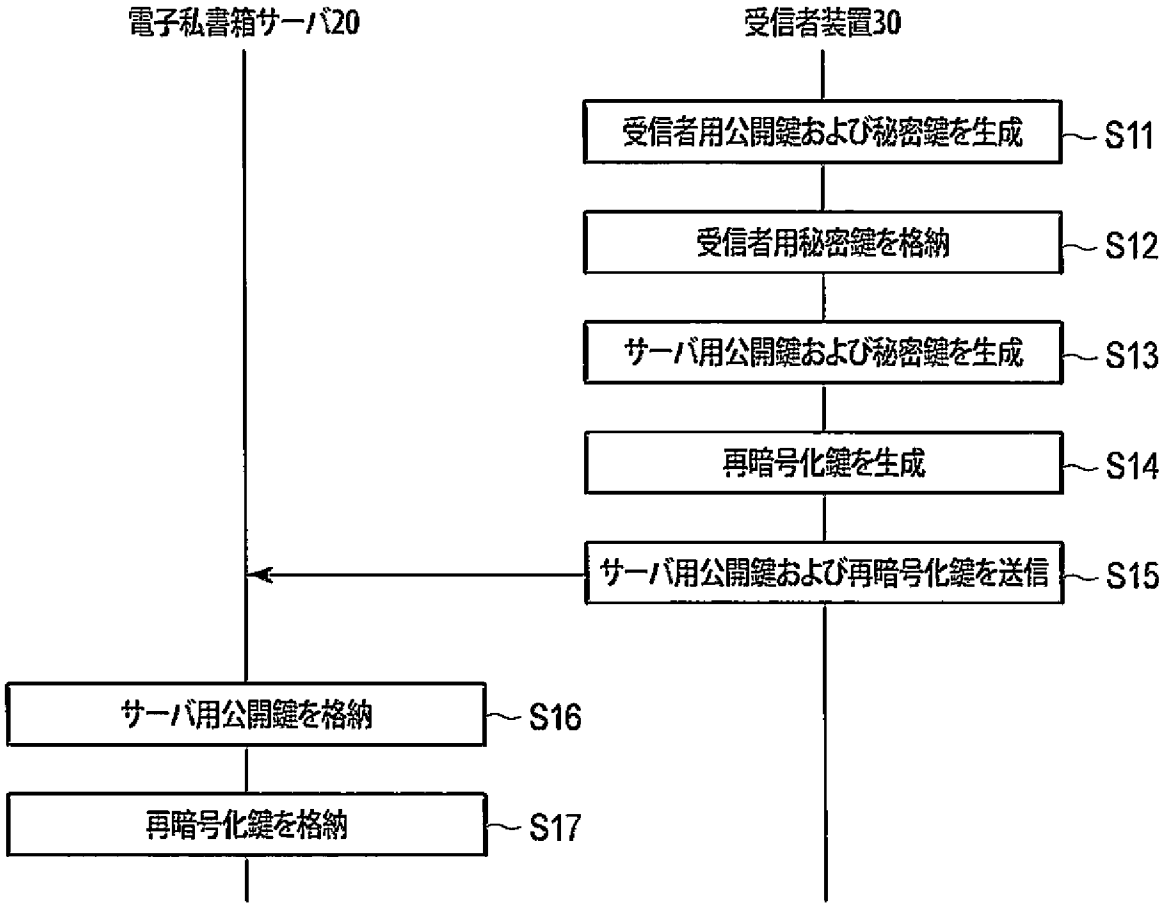
[図1]


10
送信者装置
11
12
データ入力部
暗号化処理部
20
電子私書箱サーバ
23
サーバ用
公開鍵格納部
21
再暗号化処理部
22
24
再暗号化鍵
格納部
暗号化データ
格納部
30
受信者装置
再暗号化鍵生成部
サーバ用鍵生成部
34
33
31
35
受信者用鍵生成部
受信者用
秘密鍵格納部
復号処理部
32
36
データ出力部

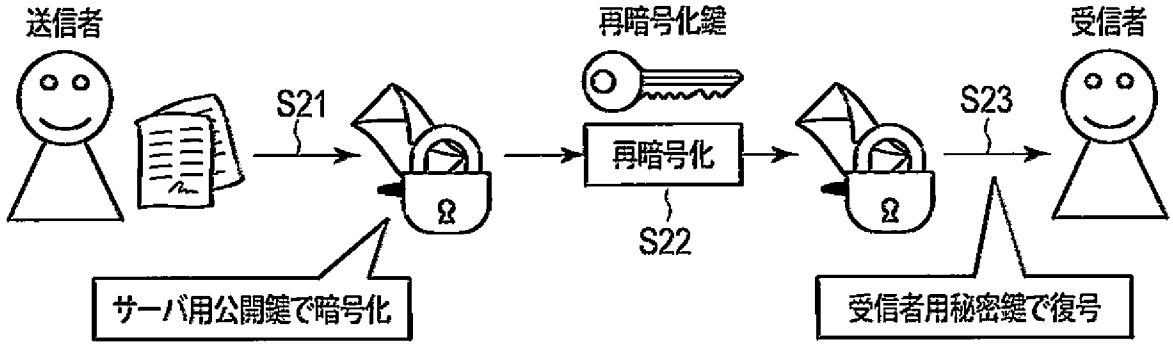
[図2]


301
B
ユーザA
ユーザB
S3
再暗号化鍵生成
100
秘
202
A
302
B
S2
復号
S5
復号
A→B
401
101
A
再暗号化
B
102
S4
201
A
暗号化
S1
100
秘

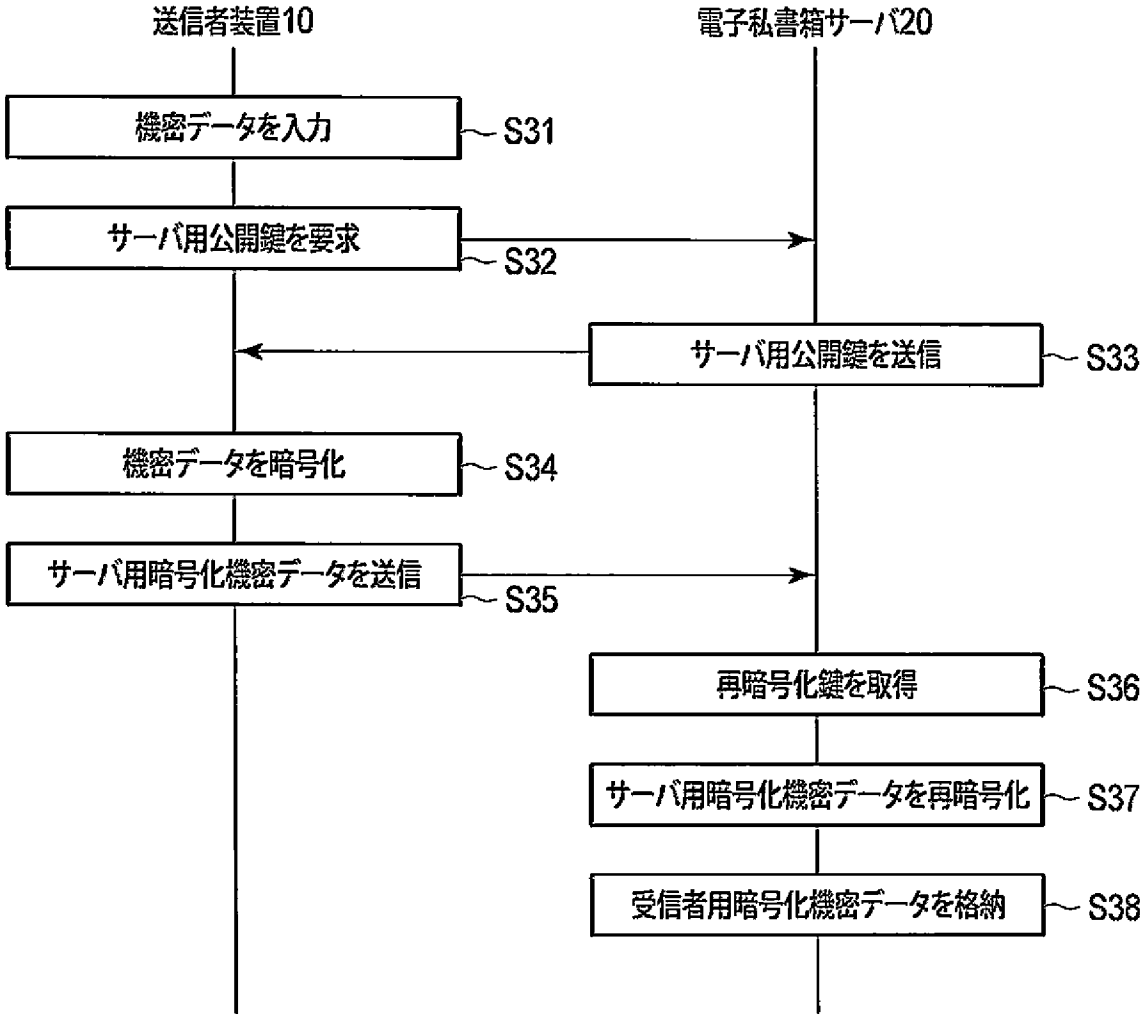
[図3]


電子私書箱サーバ20
受信者装置30
受信者用公開鍵および秘密鍵を生成
S11
受信者用秘密鍵を格納
S12
サーバ用公開鍵および秘密鍵を生成
S13
再暗号化鍵を生成
S14
サーバ用公開鍵および再暗号化鍵を送信
S15
サーバ用公開鍵を格納
S16
再暗号化鍵を格納
S17

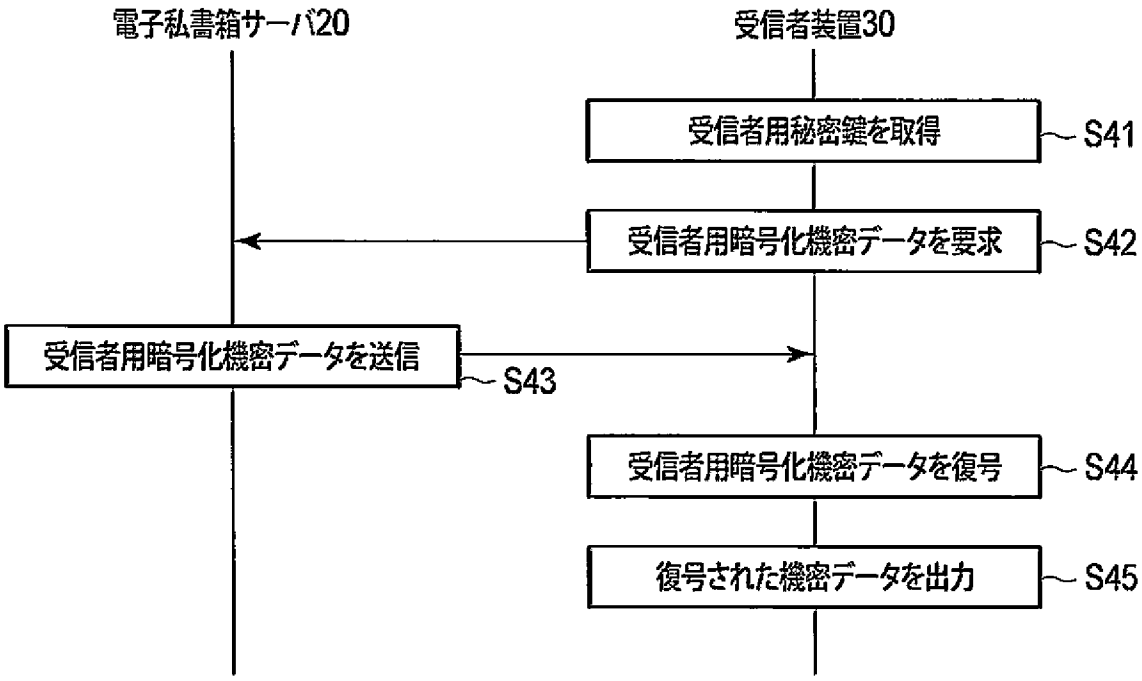
[図4]


送信者
S21
サーバ用公開鍵で暗号化
再暗号化鍵
再暗号化
S22
S23
受信者
受信者用秘密鍵で復号

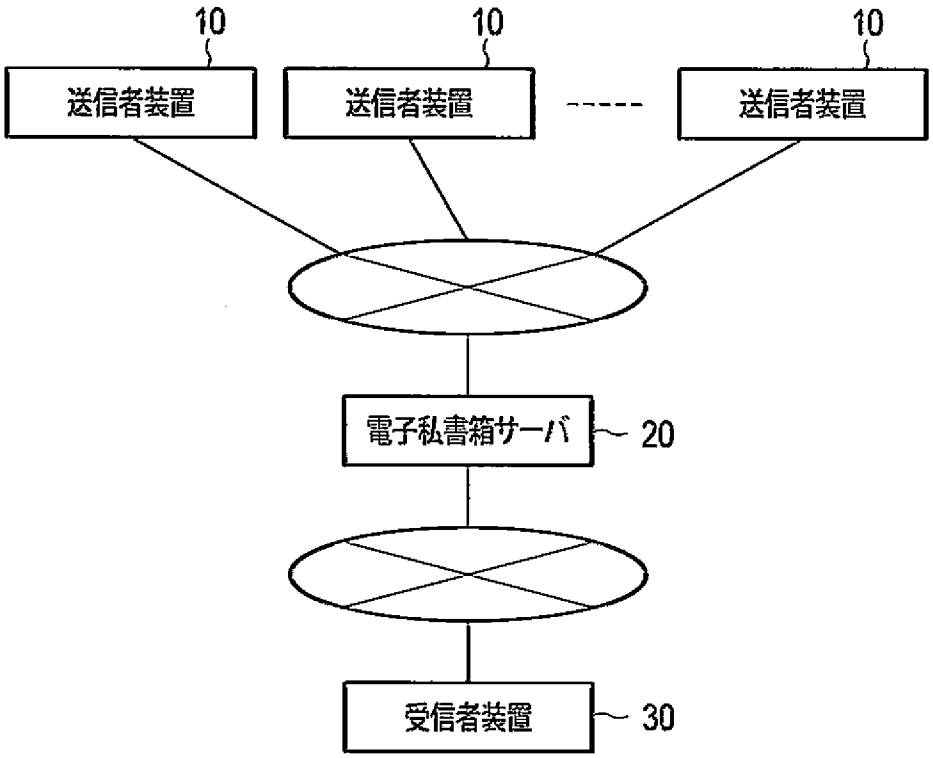
[図5]


送信者装置10
電子私書箱サーバ20
機密データを入力
S31
サーバ用公開鍵を要求
S32
サーバ用公開鍵を送信
S33
機密データを暗号化
S34
サーバ用暗号化機密データを送信
S35
再暗号化鍵を取得
S36
サーバ用暗号化機密データを再暗号化
S37
受信者用暗号化機密データを格納
S38

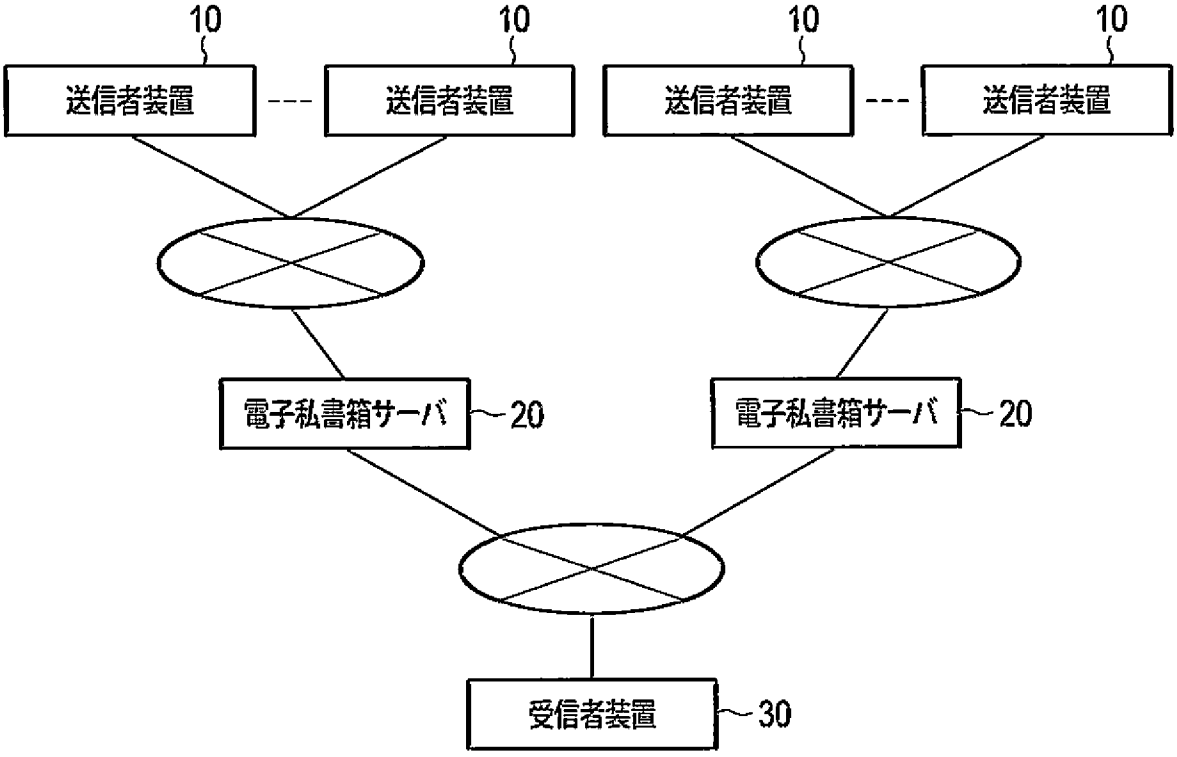
[図6]


電子私書箱サーバ20
受信者装置30
受信者用秘密鍵を取得
S41
受信者用暗号化機密データを要求
S42
受信者用暗号化機密データを送信
S43
受信者用暗号化機密データを復号
S44
復号された機密データを出力
S45

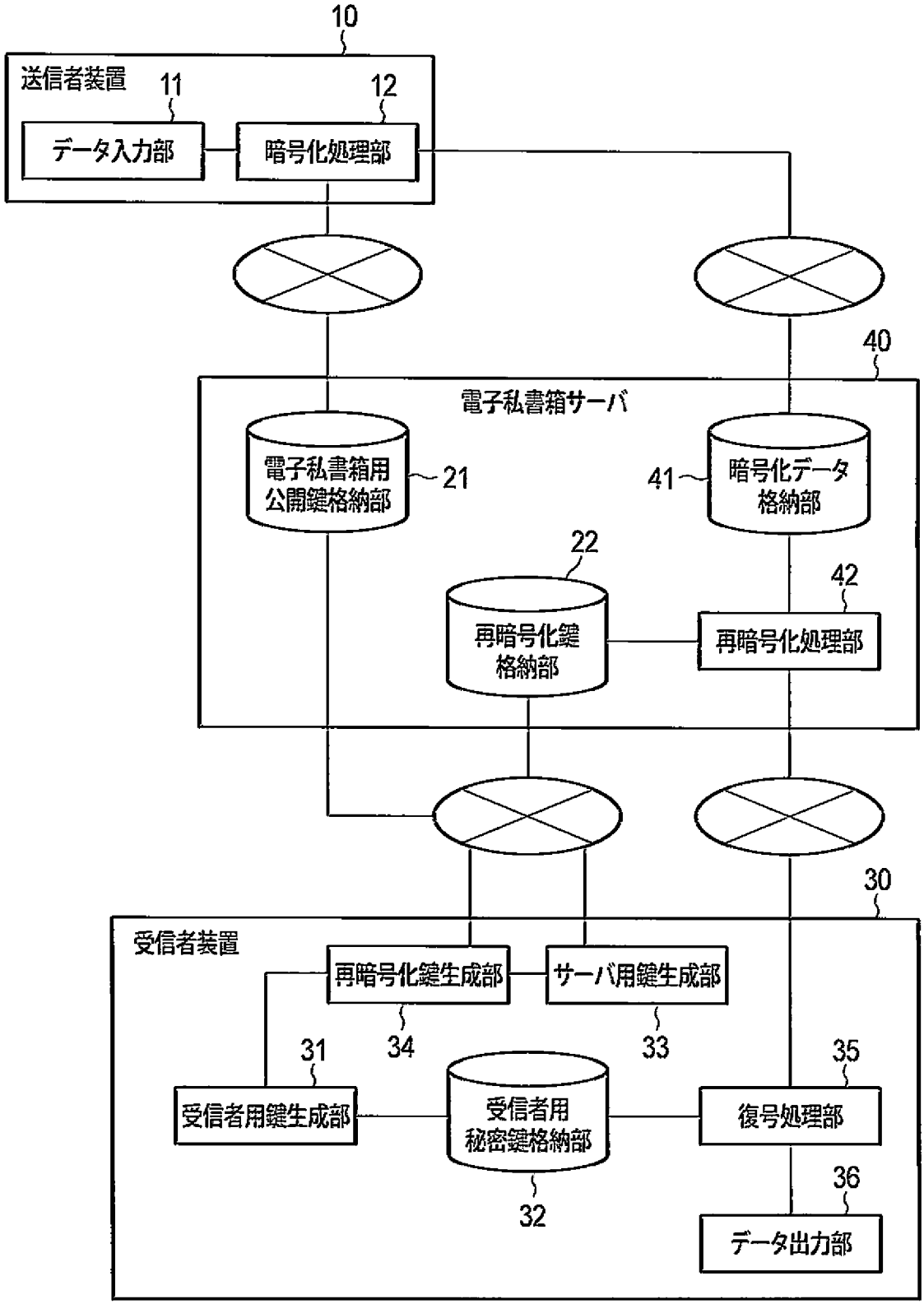
[図7]


10
10
10
送信者装置
送信者装置
送信者装置
電子私書箱サーバ
20
受信者装置
30

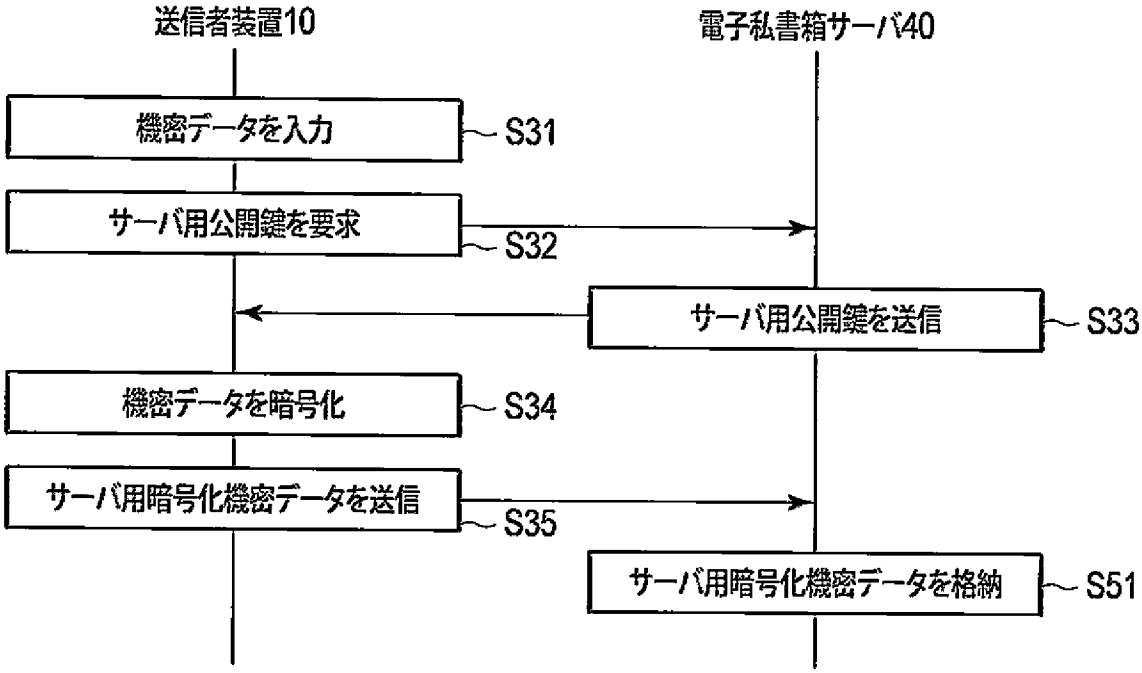
[図8]


10
10
10
10
送信者装置
送信者装置
送信者装置
送信者装置
電子私書箱サーバ
20
電子私書箱サーバ
20
受信者装置
30

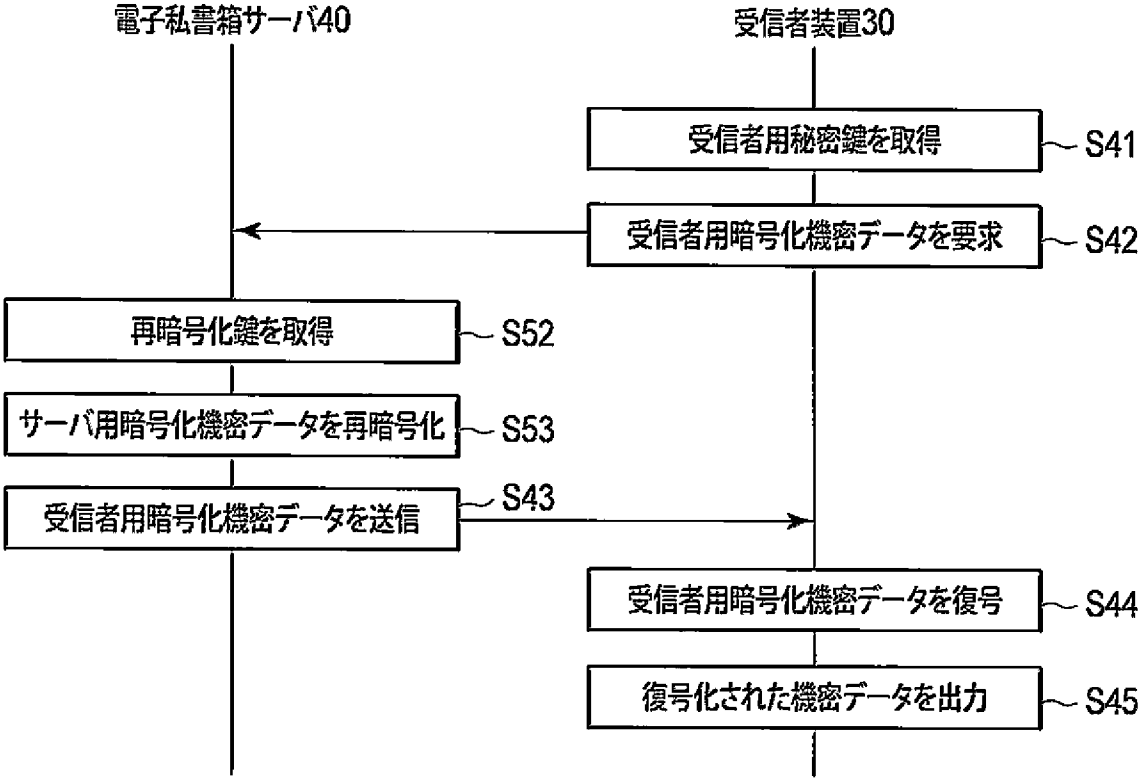
[図9]


10
送信者装置
11
12
データ入力部
暗号化処理部
40
電子私書箱サーバ
電子私書箱用
公開鍵格納部
21
41
暗号化データ
格納部
22
42
再暗号化鍵
格納部
再暗号化処理部
30
受信者装置
再暗号化鍵生成部
サーバ用鍵生成部
34
33
31
35
受信者用鍵生成部
受信者用
秘密鍵格納部
復号処理部
32
36
データ出力部

[図10]


送信者装置10
電子私書箱サーバ40
機密データを入力
S31
サーバ用公開鍵を要求
S32
サーバ用公開鍵を送信
S33
機密データを暗号化
S34
サーバ用暗号化機密データを送信
S35
サーバ用暗号化機密データを格納
S51

[図11]


電子私書箱サーバ40
受信者装置30
受信者用秘密鍵を取得
S41
受信者用暗号化機密データを要求
S42
再暗号化鍵を取得
S52
サーバ用暗号化機密データを再暗号化
S53
受信者用暗号化機密データを送信
S43
受信者用暗号化機密データを復号
S44
復号化された機密データを出力
S45

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/053547

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i, *G09C1/00*(2006.01)i, *H04L9/14*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08, G09C1/00, H04L9/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2009-33402 A (Mitsubishi Electric Corp.), 12 February 2009 (12.02.2009), paragraphs [0076] to [0090]; fig. 18 to 22 (Family: none)	1-4 5
Y A	Matthew Green et al, Identity-Based Proxy Re-encryption, [online], 15 December 2006 (15.12.2006), [retrieval date 15 March 2012 (15.03.2012)], Internet <URL:http://eprint. iacr.org/2006/473>	1-4 5
Y A	JP 2001-352320 A (Junko SUGINAKA), 21 December 2001 (21.12.2001), paragraphs [0066] to [0072], [0080]; fig. 7 (Family: none)	1-4 5

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 March, 2012 (15.03.12)	27 March, 2012 (27.03.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/053547

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/0059787 A1 (Susan R. Hohenberger), 06 March 2008 (06.03.2008), paragraphs [0044], [0047] (Family: none)	1-5
A	Giuseppe Ateniese et al, Improved proxy re-encryption schemes with applications to secure distributed storage, [online], 2005, [retrieval date 15 March 2012 (15.03.2012)], Internet <URL:http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.7790>	1-5
A	Junru Hu et al, Toward constant size CCA-secure multi-hop proxy re-encryption, Proceedings of the 2010 2nd International Conference on Signal Proceeding Systems, 2010.07, Volume 3, V1-603 - V1-605	1-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０５３５４７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i, G09C1/00(2006.01)i, H04L9/14(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08, G09C1/00, H04L9/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２０１２年
日本国実用新案登録公報　１９９６－２０１２年
日本国登録実用新案公報　１９９４－２０１２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus/JMEDPlus/JST7580(JDreamII), IEEE Xplore

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2009-33402 A（三菱電機株式会社）2009.02.12, 段落【００７６】－【００９０】,【図１８】－【図２２】（ファミリーなし）	１－４ ５
Y A	Matthew Green et al, Identity-Based Proxy Re-encryption, [online], 2006.12.15, [平成２４年３月１５日検索], インターネット＜URL:http://eprint.iacr.org/2006/473＞	１－４ ５

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１５．０３．２０１２	２７．０３．２０１２

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　３１４６
松平　英
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2001-352320 A (杉中　順子) 2001.12.21, 段落【００６６】－【００７２】,【００８０】,【図７】（ファミリーなし）	１－４ ５
A	US 2008/0059787 A1 (Susan R. Hohenberger) 2008.03.06, 段落［００４４］,［００４７］（ファミリーなし）	１－５
A	Giuseppe Ateniese et al, Improved proxy re-encryption schemes with applications to secure distributed storage, [online], 2005, [平成２４年３月１５日検索], インターネット <URL:http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.7790>	１－５
A	Junru Hu et al, Toward constant size CCA-secure multi-hop proxy re-encryption, Proceedings of the 2010 2nd International Conference on Signal Proceeding Systems, 2010.07, Volume 3, V1-603～V1-605	１－５