(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
2013 年 5 月 16 日(16.05.2013)

WIPO | PCT

(10) 国際公開番号
WO 2013/069505 A1

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

(21) 国際出願番号: PCT/JP2012/078028

(22) 国際出願日: 2012 年 10 月 30 日(30.10.2012)

(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 2011-245618 2011 年 11 月 9 日(09.11.2011) JP

(71) 出願人: 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: 綛田 佑樹 (KASEDA, Yuki); 〒1056691 東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 吉田 琢也 (YOSHIDA, Takuya); 〒1056691 東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 藤井 吉弘 (FUJII, Yoshihiro); 〒1056691 東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 阿部 真吾 (ABE, Shingo); 〒1056691 東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 山田 正隆 (YAMADA, Masataka); 〒1056691 東京都港区芝浦一丁目１番１号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (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).

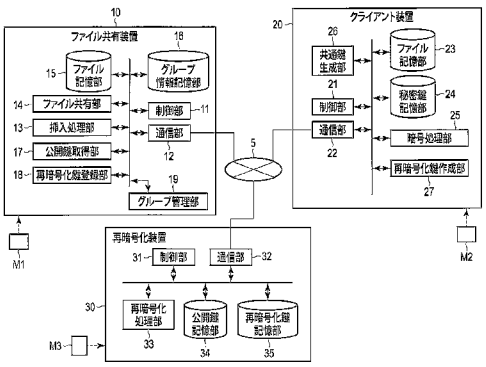
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG,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

[続葉有]

(54) **Title**: RE-ENCRYPTION SYSTEM, RE-ENCRYPTION DEVICE, AND PROGRAM

(54) 発明の名称 : 再暗号化システム、再暗号化装置及びプログラム

[図1]



10... FILE-SHARING DEVICE
11, 21, 31... CONTROL UNIT
12, 22, 32... COMMUNICATION UNIT
13... INSERTION PROCESSING UNIT
14... FILE-SHARING UNIT
15, 23... FILE STORAGE UNIT
16... GROUP INFORMATION STORAGE UNIT
17... PUBLIC KEY ACQUISITION UNIT
18... RE-ENCRYPTION KEY REGISTRATION UNIT
19... GROUP MANAGEMENT UNIT
20... CLIENT DEVICE
24... PRIVATE KEY STORAGE UNIT
25... CRYPTOGRAPHIC PROCESSING UNIT
26... PUBLIC KEY GENERATION UNIT
27... RE-ENCRYPTION KEY GENERATION UNIT
30... RE-ENCRYPTION DEVICE
33... RE-ENCRYPTION PROCESSING UNIT
34... PUBLIC KEY STORAGE UNIT
35... RE-ENCRYPTION KEY STORAGE UNIT

(57) **Abstract**: An embodiment of this re-encryption system is equipped with a file-sharing device and a re-encryption device. Upon receiving a file request from a client device, the file-sharing device obtains a first encrypted file on the basis of a file name contained in the file request, and transmits a re-encryption request, which includes the first encrypted file, to the re-encryption device. The re-encryption device re-encrypts the first encrypted file in the re-encryption request into a second encrypted file on the basis of a re-encryption key, and transmits the second encrypted file to the file-sharing device. The file-sharing device transmits the second encrypted file to the client device. The client device decrypts the second encrypted file received from the file-sharing device on the basis of a private key that corresponds to a public key of the member in order to obtain the file.

(57) 要約: 実施形態の再暗号化システムは、ファイル共有装置及び再暗号化装置を備えている。前記ファイル共有装置は、ファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて第１暗号化ファイルを取得し、前記第１暗号化ファイルを含む再暗号化要求を前記再暗号化装置に送信する。前記再暗号化装置は、前記再暗号化鍵に基づいて前記再暗号化要求内の第１暗号化ファイルを前記第２暗号化ファイルに再暗号化し、前記第２暗号化ファイルを前記ファイル共有装置に送信する。前記ファイル共有装置は、当該第２暗号化ファイルを前記クライアント装置に送信する。前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得る。

WO 2013/069505 A1

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, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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 ： 再暗号化システム、再暗号化装置及びプログラム

技術分野

[0001] 本発明の実施形態は、再暗号化システム、再暗号化装置及びプログラムに関する。

背景技術

[0002] 近年、情報技術基盤（ＩＴインフラ）や運用管理のコストを削減し得ると同時に、サービスの柔軟性や拡張性を確保して利便性にも優れていることから、クラウドコンピューティング（以下、クラウドという）が急速に普及してきている。一方、既存のクラウドのセキュリティは不十分である。セキュリティの不安感から、特にパブリッククラウドの導入に踏み切れない企業が多数ある。

[0003] その反面、複数のメンバからなるグループは、データをクラウドストレージ内に共有したいニーズが高い。このニーズはクラウドの用途の上位にも挙げられている。しかし、既存のクラウドを利用してデータを共有すると、次のような課題が考えられる。

[0004] 既存のクラウドサービスにおいては、データをグループ間で共有する場合、あるユーザがデータをクラウドストレージ上にアップロードし、グループのメンバがデータをダウンロードして利用する。

[0005] しかしながら、アップロードの際に、図１２に示すように、通信路上のデータＤはＳＳＬ／ＴＬＳにより保護されるが、クラウドストレージ１内のデータＤは暗号化されない。このため、クラウドストレージ１内のデータＤのセキュリティは、クラウドサービスの信頼性に依存する。例えばクラウドストレージ１は多くの企業・ユーザに利用されるため、設定ミスにより他テナントからデータが見られる心配や、不適切な認証処理が実行される心配がある。また、クラウドストレージ１内のデータは、サーバ管理者の内部犯行により、漏えいする心配もある。

[0006] これに対し、既存のクラウドサービスにおいて、図１３に示すように、サーバ内でデータＤを共通鍵暗号方式の共通鍵ｋによって暗号化し、暗号化データＥ（ｋ，Ｄ）をクラウドストレージ１に保管する場合がある。この場合、クラウドストレージ１内の暗号化データＥ（ｋ，Ｄ）は保護される。しかしながら、暗号化前のデータＤの受け取り（アップロード）時と、復号したデータＤの配布（ダウンロード）時には暗号化されていない状態であることや、サーバの管理者が暗号化データＥ（ｋ，Ｄ）を復号できることから、セキュリティ上の課題が残る。

[0007] 以上のような課題から、既存クラウドの導入に踏み切れない企業が多数ある。

[0008] これら課題を解決する１つの方法として、アップロード前にデータを暗号化することが考えられるが、利便性が低下する問題がある。例えば、従来の暗号化技術を用いてデータを暗号化しグループで共有する場合、大きく２つの方法（ｉ）（ｉｉ）が考えられる。但し、いずれの方法（ｉ）（ｉｉ）にもメリットとデメリットがあり、利便性とセキュリティが二律背反（trade-off）の関係にある。これら（ｉ）（ｉｉ）の方法について以下に説明する。

[0009] （ｉ）グループの鍵を共有する方法

上記（ｉ）の方法のメリットとしては、クラウド上でデータを常に暗号化した状態で保管できる点と、暗号化鍵の管理が容易である点が挙げられる。例えば、図１４に示すように、グループで暗号化鍵ek_{Gr1}／復号鍵dk_{Gr1}を共有し、公開鍵暗号を用いて暗号化する場合、暗号化鍵ek_{Gr1}／復号鍵dk_{Gr1}は１つの組である。このため、アップロードするメンバと、ダウンロードするメンバとのいずれも鍵を容易に管理できる。また、クラウド上では常に暗号化した状態でデータを保管できるため、セキュリティの不安を払拭できる。

[0010] 上記（ｉ）の方法のデメリットとしては、復号鍵dk_{Gr1}をメンバ間で共有する必要がある点と、復号鍵dk_{Gr1}の配布・共有を安全に行う方法が必要な点が挙げられる。例えば、各メンバが復号鍵dk_{Gr1}を共有するため、メンバの増加に応じて復号鍵dk_{Gr1}の漏洩リスクが増えてしまう。仮に復号鍵dk_{Gr1}を漏え

いした場合、漏洩した復号鍵dk_{Gr1}の利用を防ぐ趣旨で、グループで共有する復号鍵dk_{Gr1}を更新する必要が生じるため、利便性を低下させてしまう。また、グループからメンバが抜けた場合、抜けたメンバによる復号を防ぐ趣旨で、他のメンバの復号鍵dk_{Gr1}を更新する必要が生じるため、メンバ追加・削除時の手続きにより利便性を低下させてしまう。

[0011] このように、上記（ｉ）の方法では、鍵の管理が容易となる一方、鍵の共有方法などに課題が残る。

[0012] （ｉｉ）メンバそれぞれの鍵で暗号化する方法

上記（ｉｉ）の方法のメリットとしては、クラウド上で常に暗号化したデータを保管できる点と、メンバ間で鍵を共有しない点が挙げられる。例えば、図１５に示すように、メンバＡ，…毎に公開鍵pk_A／秘密鍵sk_A，…を作成し、公開鍵暗号を用いてデータＤを暗号化し、暗号化データＥ（pk_A，Ｄ），…をクラウドストレージ１に保管する場合、他のメンバと秘密鍵sk_A，…を共有しないため、鍵を配布・共有する必要がない。このため、あるメンバＩが秘密鍵sk_Iを漏えいさせたとしても、他のメンバが秘密鍵sk_Iを更新する必要はない。

[0013] 上記（ｉｉ）の方法のデメリットとしては、暗号化するメンバが各メンバの公開鍵pk_A，…を管理する必要がある点と、あるメンバＨをグループに追加した場合、追加したメンバＨの公開鍵pk_HでデータＤを暗号化しなおす必要がある点が挙げられる。例えば、暗号化するメンバに関しては、各メンバの鍵管理が煩雑になり、利便性を低下させてしまう。また、追加メンバＨが生じた場合、暗号化するメンバに関しては、追加メンバＨの公開鍵pk_HでデータＤを暗号化してクラウドストレージ１に保管する必要があるため、利便性を低下させてしまう。

[0014] このように従来の暗号化技術では、利便性とセキュリティが二律背反の関係にある。

[0015] なお、以下は実施形態に関連する先行技術文献を示している。このうち、特にハイブリッド暗号方式やＪａｖａ（登録商標）に関する非特許文献１，

２については、同様の技術を示す他の文献があると推測される。

先行技術文献

特許文献

[0016] 特許文献1：特許第４０６１２８８号公報

非特許文献

[0017] 非特許文献1：ハイブリッド暗号方式ーーー共通鍵暗号と公開鍵暗号を組み合わせるー情報セキュリティ入門：ITpro、http://itpro.nikkeibp.co.jp/article/COLUMN/20060620/241303/

非特許文献2：Javaの道：Servlet（10.フィルタ）、http://www.javaroad.jp/servletjsp/sj_servlet10.htm

非特許文献3：B. Libert and D. Vergnaud, ”Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption,” Proc. PKC 2008, LNCS 4939, pp.360-379, Springer, 2008.

発明の概要

発明が解決しようとする課題

[0018] 以上説明したように、従来の暗号化技術を用いて暗号化データを保管する場合、利便性とセキュリティが二律背反の関係にある。

[0019] 本発明が解決しようとする課題は、利便性とセキュリティを両立し得る再暗号化システム、再暗号化装置及びプログラムを提供することである。

課題を解決するための手段

[0020] 実施形態の再暗号化システムは、グループに属するメンバに操作されるクライアント装置に通信可能なファイル共有装置及び再暗号化装置を備えている。

[0021] 前記ファイル共有装置は、ファイル記憶手段を備えている。

[0022] 前記ファイル記憶手段は、前記グループの公開鍵に基づいてファイルが暗号化されてなる第１暗号化ファイルを記憶する。

[0023] 前記ファイル共有装置は、前記メンバを識別するメンバＩＤ及び前記第１

暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記ファイル記憶手段から前記第１暗号化ファイルを取得する。

[0024] 前記ファイル共有装置は、前記取得した第１暗号化ファイル及び前記ファイル要求内のメンバＩＤを含む再暗号化要求を前記再暗号化装置に送信する。

[0025] 前記ファイル共有装置は、前記メンバＩＤの公開鍵に基づいて前記ファイルが暗号化されてなる第２暗号化ファイルを前記再暗号化装置から受けると、当該第２暗号化ファイルを前記クライアント装置に送信する。

[0026] 前記再暗号化装置は、再暗号化鍵記憶手段を備えている。

[0027] 前記再暗号化鍵記憶手段は、前記メンバを識別するメンバＩＤと、前記第１暗号化ファイルを復号せずに前記第２暗号化ファイルに再暗号化するための再暗号化鍵とを関連付けて記憶する。

[0028] 前記再暗号化装置は、前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する。

[0029] 前記再暗号化装置は、前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化ファイルを前記第２暗号化ファイルに再暗号化する。

[0030] 前記再暗号化装置は、前記再暗号化により得られた第２暗号化ファイルを前記ファイル共有装置に送信する。

[0031] 前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得る。

図面の簡単な説明

[0032] [図1]図１は、第１の実施形態に係る再暗号化システムの構成を示す模式図である。

[図2]図２は、同実施形態におけるグループ情報記憶部を説明するための模式図である。

[図3]図３は、同実施形態における再暗号化鍵記憶部を説明するための模式図である。

[図4]図４は、同実施形態におけるファイルアップロードの処理を説明するためのフローチャートである。

[図5]図５は、同実施形態におけるファイルアップロードの処理を説明するためのシーケンス図である。

[図6]図６は、同実施形態におけるファイルダウンロードの処理を説明するためのフローチャートである。

[図7]図７は、同実施形態におけるファイルダウンロードの処理を説明するためのシーケンス図である。

[図8]図８は、同実施形態におけるメンバ追加の処理を説明するためのフローチャートである。

[図9]図９は、同実施形態におけるメンバ追加の処理を説明するためのシーケンス図である。

[図10]図１０は、同実施形態におけるメンバ削除の処理を説明するためのフローチャートである。

[図11]図１１は、同実施形態におけるメンバ削除の処理を説明するためのシーケンス図である。

[図12]図１２は、従来のクラウドストレージの課題を説明するための模式図である。

[図13]図１３は、従来の共通鍵で暗号化する場合の課題を説明するための模式図である。

[図14]図１４は、従来のグループの公開鍵で暗号化する場合の課題を説明するための模式図である。

[図15]図１５は、従来のメンバ毎の公開鍵で暗号化する場合の課題を説明するための模式図である。

[図16A]図１６Ａは、従来の暗号化技術を示す模式図である。

[図16B]図１６Ｂは、一般的な再暗号化技術を示す模式図である。

[図17]図１７は、一般的な再暗号化鍵の作成過程を説明するための模式図である。

[図18]図１８は、各実施形態の概要に係る再暗号化システムを説明するための模式図である。

[図19]図１９は、各実施形態の概要における再暗号化システムによるメンバ追加を説明するための模式図である。

[図20]図２０は、一般的なハイブリッド方式を説明するための模式図である。

[図21]図２１は、各実施形態の概要における再暗号化システムにフィルタ機能を適用した場合の利点を説明するための模式図である。

[図22]図２２は、ハイブリッド方式におけるファイルのフォーマットを示す模式図である。

[図23]図２３は、ハイブリッド方式を適用した再暗号化システムを説明するための模式図である。

[図24]図２４は、ハイブリッド方式を適用した再暗号化システムの処理時間を説明するための模式図である。

発明を実施するための形態

[0033] 以下、各実施形態について図面を用いて説明するが、その前に各実施形態の前提となる再暗号化技術、ハイブリッド方式及び各実施形態の概要を述べる。

[0034] 利便性とセキュリティを両立させる方法として、再暗号化技術（非特許文献３参照。）が知られている。

[0035] 従来の暗号化技術を図１６Ａに示し、再暗号化技術を図１６Ｂに示す。再暗号化技術では、図１６Ｂに示すように、あるメンバの公開鍵pk_{Gr1}で暗号化したデータＥ（pk_{Gr1}，Ｄ）を、復号することなく、別のメンバＡの公開鍵pk_{A}で暗号化したデータＥ（pk_{A}，Ｄ）に変換できる。つまり、再暗号化とは、暗号化データを復号せずに、鍵を付け替えることができる技術である。

[0036] このような再暗号化処理を行うには再暗号化鍵$rk_{Gr1\rightarrow A}$が必要である。再暗

号化鍵$rk_{Gr1\to A}$は、図１７に示すように、付け替える前の秘密鍵sk_{Gr1}と、付け替える後の公開鍵pk_Aから作成される。再暗号化鍵$rk_{Gr1\to A}$は公開しても問題ない。

[0037] 再暗号化技術を用いた場合、図１８に示すように、データＤとしてのファイルが、暗号化された状態でクラウドストレージ１にアップロード・ダウンロードされる。

[0038] このとき、アップロードするメンバは、グループの公開鍵pk_{Gr1}でデータＤを暗号化し、暗号化データＥ（pk_{Gr1}，Ｄ）をクラウドストレージ１に保管する。このため、グループ内の各メンバの鍵管理が不要である。

[0039] グループのメンバＡがデータＤをダウンロードするとき、サーバ上で暗号化データＥ（pk_{Gr1}，Ｄ）を当該メンバＡ向けの再暗号化鍵$rk_{Gr1\to A}$により再暗号化し、得られた再暗号化データＥ（pk_A，Ｄ）をダウンロードする。

[0040] このような再暗号化システムのメリットとしては、クラウド上でデータを常に暗号化した状態で保管できる点と、暗号化鍵の管理が容易な点と、メンバ間で鍵を共有しない点が挙げられる。例えば、再暗号化処理はデータＤを暗号化した状態で実行できるので、クラウドストレージ１上でデータＤが復号されない。また、各メンバは他のメンバと秘密鍵sk_A，…を共有する必要がない。

[0041] なお、再暗号化技術を利用したグループのメンバ管理は、図１９に示すように、クラウドストレージ１上に再暗号化鍵$rk_{Gr1\to A}$，…の追加・削除を行うことになる。追加の場合、グループ管理者が追加するメンバＣの公開鍵pk_Cを取得する。グループ管理者は、グループの秘密鍵sk_{Gr1}と取得した公開鍵pk_Cから再暗号化鍵$rk_{Gr1\to C}$を作成し、作成した再暗号化鍵$rk_{Gr1\to C}$をクラウドストレージ１に配置する。このようなメンバ変更がある場合でも、従来とは異なり、暗号化データＥ（pk_{Gr1}，Ｄ）をクラウドストレージ１上で暗号化しなおす必要が無いので、利便性が低下しない。

[0042] 一方、再暗号化システムのデメリットは、特に見当たらない。

[0043] なお、公開鍵暗号を用いてデータを暗号化する場合、一般的に、暗号・復

号処理が速い共通鍵暗号技術と組み合わせたハイブリッド暗号と呼ばれる方式（以下、ハイブリッド方式という）を用いて高速化が図られている（非特許文献１参照。）。ハイブリッド方式では、図２０に示すように、保護対象のデータＤを共通鍵暗号方式の共通鍵ｋで高速に暗号化して暗号化データＥ（ｋ，Ｄ）を作成し、この共通鍵ｋを公開鍵暗号方式の公開鍵ｐｋで暗号化して暗号化鍵Ｅ（ｐｋ，ｋ）を作成する。

[0044] ハイブリッド方式を用いることで、鍵の配布・管理が容易な公開鍵暗号方式のメリットと、処理が高速な共通鍵暗号方式のメリットの両方を活かすことができる。

[0045] なお、ハイブリッド方式を用いるか否かによらず、再暗号化技術を用いる構成であれば、クラウドストレージ上で、メンバ間で安全にデータを共有することが可能になる。

[0046] この再暗号化技術を用いた再暗号化システムを構築する場合、新たに構築するケースと、既存のファイル共有システムに対して再暗号化機能を追加して構築するケースが考えられる。

[0047] 後者のケースの場合、既存のファイル共有システムに対し、再暗号化機能を組み込んで構築する場合、大きな手間とコストが必要になる。

[0048] 既存のファイル共有システムの処理を大きく改修することなく、新たに別の機能と連携する一つの方法として、Ｊａｖａのフィルタ（非特許文献２参照。）を利用する方法が考えられる。フィルタ機能を利用することで、ファイル共有装置（クラウドストレージ１に相当する装置）とそのクライアント間のリクエスト・レスポンス処理に、処理を追加することができる。このフィルタ処理で再暗号化処理を行うことで、既存のファイル共有システムを大きく修正することなく、また再暗号化機能を組み込むことなく、少ない改修で再暗号化機能を追加できる。

[0049] すなわち、図２１に示すように、ファイル共有装置２に追加する構成要素は、再暗号化装置３と連携する処理（例、フィルタ４）のみである。

[0050] なお、上述した再暗号化システムは、そのまま実施してもよいが、本発明

者の検討によれば、データの配布処理を改善した形態の方がより好ましい。そこで、第１の実施形態では、データの配布処理を改善した形態について述べている。

[0051] 補足すると、再暗号化システムにおいて、単純に再暗号化装置３と連携した場合、ファイル共有装置２に保管している暗号化データＥ（pk_{Gr1}，Ｄ）を再暗号化する必要があるため、メンバに配布するためには必ず再暗号化処理を待たなければならない。再暗号化処理は既存の公開鍵暗号方式と比べて複雑なため、処理時間がかかる。

[0052] そこで、図２２に示すように、ハイブリッド方式におけるファイルのフォーマットに注目する。このフォーマットによれば、ファイル共有装置２内の暗号化ファイルのうち、再暗号化処理を行う部分は、（公開鍵で暗号化された）共通鍵部分だけになる。そこで、図２１に示した暗号化データＥ（pk_{Gr1}，Ｄ）に代えて、図２３に示すように、（公開鍵pk_{Gr1}で暗号化された）共通鍵ｋからなる暗号化共通鍵Ｅ（pk_{Gr1}，ｋ）部分と、共通鍵ｋで暗号化されたデータＤからなる暗号化データＥ（ｋ，Ｄ）部分とからなる暗号化ファイルをファイル共有装置２に保管し、暗号化共通鍵Ｅ（pk_{Gr1}，ｋ）部分のみ再暗号化装置３に送付する。暗号化データＥ（ｋ，Ｄ）部分が、データの大きさに依存するが、暗号化共通鍵Ｅ（pk_{Gr1}，ｋ）部分と比べて大幅にサイズが大きいことを考えると、ファイル共有装置２と再暗号化装置３の間での通信処理を軽減することができる。

[0053] また、図２４に示すように、再暗号化装置３に暗号化共通鍵Ｅ（pk_{Gr1}，ｋ）部分を送信する処理に並行して、暗号化データＥ（ｋ，Ｄ）部分をメンバ（クライアント）に送信する。暗号化データＥ（ｋ，Ｄ）部分の大きさやネットワークの速さに依存するが、一般的にダウンロード処理の方が再暗号化処理よりも時間がかかるため、ダウンロード処理の実行中に再暗号化処理が終わる。このため、再暗号化処理によるサーバ処理時間は、クライアント装置へ暗号化データＥ（ｋ，Ｄ）部分を送信している間に完了することが期待できる。

[0054] 以上のように、データの配布処理を改善した形態は、図２２乃至図２４に示したように、ハイブリッド方式のデータフォーマットに着目し、暗号化共通鍵Ｅ（ｐｋ$_{Gr1}$，ｋ）部分の再暗号化処理と暗号化データＥ（ｋ，Ｄ）部分の送信を並行して行なうことから、図２１に示した形態に比べ、ダウンロード処理全体の時間を短縮できる点で好ましい。

[0055] 以上がデータの配布処理を改善した形態についての補足説明である。続いて、各実施形態について具体的に説明する。なお、第１の実施形態は、データの配布処理を改善した応用形態であり、第２の実施形態は、データの配布処理を改善していない基本形態である。

[0056] ＜第１の実施形態＞

図１は第１の実施形態に係る再暗号化システムの構成を示す模式図である。この再暗号化システムは、クライアント／サーバ構成であり、グループに属するメンバに操作されるクライアント装置２０に通信可能なファイル共有装置１０及び再暗号化装置３０を備えている。なお、ファイル共有装置１０及び再暗号化装置３０はサーバ装置であり、各装置１０，２０，３０は、互いにインターネット５を介して通信可能となっている。また、各装置１０，２０，３０は、それぞれハードウェア構成、又はハードウェア資源とソフトウェアとの組合せ構成のいずれでも実施可能となっている。組合せ構成のソフトウェアとしては、図１に示す如き、予めネットワーク又は非一時的なコンピュータ読取可能な記憶媒体（non-transitory computer-readable storage medium）Ｍ１～Ｍ３から各コンピュータにインストールされ、当該各コンピュータのプロセッサに実行されることにより、当該各コンピュータに各装置の機能を実現させるためのプログラムが用いられる。これらのことは、後述する変形例でも同様である。

[0057] ここで、ファイル共有装置１０は、制御部１１、通信部１２、挿入処理部１３、ファイル共有部１４、ファイル記憶部１５、グループ情報記憶部１６、公開鍵取得部１７、再暗号化鍵登録部１８及びグループ管理部１９を備えている。

[0058] 制御部１１、通信部１２、挿入処理部１３、ファイル共有部１４、公開鍵取得部１７、再暗号化鍵登録部１８及びグループ管理部１９は、例えば図示しないＣＰＵが、後述するファイル共有装置１０内の各ステップを含むプログラムを実行することにより実現される機能ブロックとなっている。また、通信部１２は、他の装置２０，３０との間の通信インターフェースである。但し、以下の説明中では、説明の簡単化の観点から、他の装置２０，３０との間のデータの送受信に通信部１２を介する旨の記載を省略している。

[0059] また、例えば再暗号化装置３０に連携する挿入処理部１３、公開鍵取得部１７及び再暗号化鍵登録部１８については、既存のファイル共有システムを大きく修正せずに再暗号化システムを構築したい観点から、Ｊａｖａのフィルタ機能を利用して実現してもよい。

[0060] ファイル記憶部１５は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、グループの公開鍵に基づいて共通鍵が暗号化されてなる第１暗号化共通鍵部分と、当該共通鍵に基づいてデータが暗号化されてなる暗号化データ部分とを含む暗号化ファイルを記憶する。なお、「第１暗号化共通鍵部分」は、「第１暗号化共通鍵」又は「暗号化共通鍵」と読み替えてもよい。また、「暗号化データ部分」は、「暗号化データ」と読み替えてもよい。

[0061] グループ情報記憶部１６は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、図２に示すように、グループを識別するグループＩＤと、当該グループに属するメンバを識別するメンバＩＤとを関連付けて記憶する。

[0062] 一方、クライアント装置２０は、制御部２１、通信部２２、ファイル記憶部２３、秘密鍵記憶部２４、暗号処理部２５、共通鍵生成部２６及び再暗号化鍵作成部２７を備えている。

[0063] 制御部２１、通信部２２、暗号処理部２５、共通鍵生成部２６及び再暗号化鍵作成部２７は、例えば図示しないＣＰＵが、後述するクライアント装置２０内の各ステップを含むプログラムを実行することにより実現される機能

ブロックとなっている。また、通信部２２は、他の装置１０，３０との間の通信インターフェースである。但し、以下の説明中では、説明の簡単化の観点から、他の装置１０，３０との間のデータの送受信に通信部２２を介する旨の記載を省略している。

[0064] ファイル記憶部２３は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、例えば、アップロード対象のファイルを記憶する。

[0065] 秘密鍵記憶部２４は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、例えば、メンバの公開鍵に対応する秘密鍵を記憶する。また、メンバがグループ管理者の場合、秘密鍵記憶部２４は、更に、グループの公開鍵に対応する秘密鍵を記憶する。

[0066] 他方、再暗号化装置３０は、制御部３１、通信部３２、再暗号化処理部３３、公開鍵記憶部３４及び再暗号化鍵記憶部３５を備えている。

[0067] 制御部３１、通信部３２及び再暗号化処理部３３は、例えば図示しないＣＰＵが、後述する再暗号化装置３０内の各ステップを含むプログラムを実行することにより実現される機能ブロックとなっている。また、通信部３２は、他の装置１０，２０との間の通信インターフェースである。但し、以下の説明中では、説明の簡単化の観点から、他の装置１０，２０との間のデータの送受信に通信部３２を介する旨の記載を省略している。

[0068] 公開鍵記憶部３４は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、グループを識別するグループＩＤと、当該グループの公開鍵と、メンバを識別するメンバＩＤと、当該メンバの公開鍵とを関連付けて記憶する。

[0069] 再暗号化鍵記憶部３５は、図示しないＣＰＵから読出／書込可能な記憶装置として実現可能となっており、図３に示すように、メンバを識別するメンバＩＤと、第１暗号化共通鍵部分を復号せずに第２暗号化共通鍵部分に再暗号化するための再暗号化鍵とを関連付けて記憶する。なお、「第２暗号化共通鍵部分」は、「第２暗号化共通鍵」又は「再暗号化共通鍵」と読み替えて

もよい。

[0070] 次に、以上のように構成された再暗号化システムの動作を図４乃至図１１を用いて説明する。なお、以下の説明は、ファイルアップロードの処理（図４及び図５）、ファイルダウンロードの処理（図６及び図７）、メンバ追加の処理（図８及び図９）及びメンバ追加の処理（図１０及び図１１）の順に行う。

[0071] 始めに、ファイルアップロードの処理の流れを図４及び図５に示す。

[0072] クライアント装置２０では、制御部２１がファイル記憶部２３からアップロードするファイルを読み込む（ＳＴ１）。

[0073] クライアント装置２０では、制御部２１が共通鍵生成部２６により共通鍵ｋを生成する。制御部２１は、この共通鍵ｋとステップＳＴ１で読み込んだファイルを暗号処理部２５に渡す（ＳＴ２）。

[0074] クライアント装置２０では、暗号処理部２５が、ファイルのデータＤを共通鍵ｋで暗号化し、得られた暗号化データ部分（Ｅ（ｋ，Ｄ））を制御部２１に渡す（ＳＴ３）。

[0075] ステップＳＴ４では、以下のステップＳＴ４－１～ＳＴ４－７が実行される。

[0076] クライアント装置２０では、制御部２１が、アップロードするファイルを公開するグループの公開鍵pk_{Gr1}をファイル共有装置１０に要求する（ＳＴ４－１）。具体的には、グループを識別するグループＩＤを含む公開鍵要求をファイル共有装置１０に送信する。

[0077] ファイル共有装置１０では、制御部１１が、この公開鍵要求を公開鍵取得部１７に送出する（ＳＴ４－２）。

[0078] ファイル共有装置１０では、公開鍵取得部１７が、この公開鍵要求を再暗号化装置３０に送信する（ＳＴ４－３）。

[0079] 再暗号化装置３０では、制御部３１が、公開鍵要求内のグループＩＤに基づいて、公開鍵記憶部３４からグループの公開鍵pk_{Gr1}を取り出す（ＳＴ４－４）。

[0080] 再暗号化装置３０では、制御部３１がグループの公開鍵pk_{Gr1}をファイル共有装置１０に送信する（ＳＴ４－５）。

[0081] ファイル共有装置１０では、公開鍵取得部１７が、制御部１１にグループの公開鍵pk_{Gr1}を渡す（ＳＴ４－６）。

[0082] ファイル共有装置１０では、制御部１１が、グループの公開鍵pk_{Gr1}をクライアント装置２０に送信する（ＳＴ４－７）。

[0083] クライアント装置２０では、制御部２１が、受信したグループの公開鍵pk_{Gr1}と、ステップＳＴ２で生成した共通鍵ｋを暗号処理部２５に渡す。暗号処理部２５は、共通鍵ｋをグループの公開鍵pk_{Gr1}で暗号化し、得られた第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））を制御部２１に渡す（ＳＴ５）。

[0084] ステップＳＴ６では、以下のステップＳＴ６－１～ＳＴ６－３が実行される。

[0085] クライアント装置２０では、制御部２１が、ステップＳＴ２で渡された暗号化データ部分（Ｅ（ｋ，Ｄ））と、ステップＳＴ５で得られた第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））とを１つのファイル（暗号化ファイル）に纏め、纏めた暗号化ファイルをファイル共有装置１０に送信する（ＳＴ６－１）。

[0086] ファイル共有装置１０では、制御部１１が、暗号化ファイルをファイル共有部１４に渡す。ファイル共有部１４は、暗号化ファイルをファイル記憶部１５に書込む（ＳＴ６－２）。

[0087] ファイル共有装置１０では、制御部１１が、ファイルアップロードが完了した旨をクライアント装置２０に通知する（ＳＴ６－３）。

[0088] クライアント装置２０では、制御部２１が、この通知を表示部（図示せず）に表示する。

[0089] 以上により、ファイルアップロードの処理が完了する。

[0090] 続いて、ファイルダウンロードの処理の流れを図６及び図７に示す。

[0091] クライアント装置２０では、制御部２１が、メンバを識別するメンバＩＤ及びグループを識別するグループＩＤ（フォルダ内のファイルをグループで

共有する場合は、フォルダ名をグループＩＤとしてもよい）と、暗号化ファイルのファイル名を含むファイル要求をファイル共有装置１０に送信する（ＳＴ１１）。なお、メンバＩＤについては、クライアント装置２０から送付するのがメンバＩＤではなくてセッションＩＤである場合、ファイル共有装置１０の制御部１１でセッションＩＤとメンバＩＤとを結び付けて管理し、その管理しているメンバＩＤを利用して、セッションＩＤから逆算してメンバＩＤを導くようにしてもよい。

[0092] ステップＳＴ１２では、以下のステップＳＴ１２－１～ＳＴ１２－２が実行される。

[0093] ファイル共有装置１０では、制御部１１が、メンバを識別するメンバＩＤ及び暗号化ファイルのファイル名を含むファイル要求をクライアント装置２０から受けると、ファイル共有部１４を介して、ファイル要求内のファイル名に基づいてファイル記憶部１５から暗号化ファイルを取得する。具体的には、制御部１１は、クライアント装置２０から受けたファイル要求をファイル共有部１４に送出する。ファイル共有部１４は、ファイル記憶部１５から暗号化ファイルを取得し、制御部１１に渡す（ＳＴ１２－１）。

[0094] ファイル共有装置１０では、制御部１１が、取得した暗号化ファイルを挿入処理部１３に渡す［処理の挿入］（ＳＴ１２－２）。

[0095] ファイル共有装置１０では、処理挿入部１３が、渡された暗号化ファイルを、第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））と暗号化データ部分（Ｅ（ｋ，Ｄ））に分離する（ＳＴ１３）。

[0096] ステップＳＴ１４’及びＳＴ１４は、並列に実行される。ステップＳＴ１４’では、以下のステップＳＴ１４’－１～ＳＴ１４’－２が実行される。

[0097] ファイル共有装置１０では、挿入処理部１３が、ステップＳＴ１４の処理と並行して、暗号化データ部分（Ｅ（ｋ，Ｄ））を制御部１１に渡す（ＳＴ１４’－１）。

[0098] ファイル共有装置１０では、制御部１１が、クライアント装置２０に暗号化データ部分（Ｅ（ｋ，Ｄ））を送信する（ＳＴ１４’－２）。

[0099] ステップＳＴ１４では、以下のステップＳＴ１４－１～ＳＴ１４－５が実行される。

[0100] ファイル共有装置１０では、処理挿入部１３が、分離された暗号化データ部分（Ｅ（ｋ，Ｄ））をクライアント装置２０に送信する処理と並行して、第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））及びファイル要求内のメンバＩＤ及びグループＩＤを含む再暗号化要求を再暗号化装置３０に送信する（ＳＴ１４－１）。

[0101] 再暗号化装置３０では、再暗号化要求をファイル共有装置１０から受けると、当該再暗号化要求内のメンバＩＤ（例、Ａ）とグループＩＤ（例、Ｇｒ１）に基づいて再暗号化鍵記憶部３５から再暗号化鍵$rk_{Gr1\rightarrow A}$を取得し、当該取得した再暗号化鍵$rk_{Gr1\rightarrow A}$に基づいて、再暗号化要求内の第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））を第２暗号化共通鍵部分（Ｅ（pk_{A}，ｋ））に再暗号化する。

[0102] 具体的には、制御部３１は、再暗号化要求内の第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ）及びメンバＩＤ（例、Ａ）及びグループＩＤ（例、Ｇｒ１）を再暗号化処理部３３に渡す。再暗号化処理部３３は、このメンバＩＤとグループＩＤに基づいて再暗号化鍵記憶部３５から再暗号化鍵$rk_{Gr1\rightarrow A}$を取得し、第１暗号化共通鍵部分（Ｅ（pk_{Gr1}，ｋ））を第２暗号化共通鍵部分（Ｅ（pk_{A}，ｋ）に再暗号化し、得られた第２暗号化共通鍵部分（Ｅ（pk_{A}，ｋ））を制御部３１に渡す（ＳＴ１４－２）。

[0103] 再暗号化装置３０では、制御部３１が、再暗号化により得られた第２暗号化共通鍵部分（Ｅ（pk_{A}，ｋ））をファイル共有装置１０に送信する（ＳＴ１４－３）。

[0104] ファイル共有装置１０では、挿入処理部１３が、ステップＳＴ１４’－２の送信処理が終わっていなければ終わるまで待って、制御部１１に第２暗号化共通鍵部分（Ｅ（pk_{A}，ｋ））を渡す。ステップＳＴ１４’－２の送信処理が終わっていればすぐ渡す（ＳＴ１４－４）。

[0105] ファイル共有装置１０では、制御部１１が、第２暗号化共通鍵部分（Ｅ（

pk_A，ｋ））をクライアント装置２０に送信する［挿入した処理の終了］（ＳＴ１４－５）。

[0106] ファイル共有装置１０からクライアント装置２０へのレスポンスはステップＳＴ１４－５とステップＳＴ１４’－２との２回送信しているが、これは１つの通信のレスポンスとして２段階でデータを送付している。

[0107] クライアント装置２０は、ファイル共有装置１０から受けた第２暗号化共通鍵部分（Ｅ（pk_A，ｋ））をメンバの公開鍵pk_Aに対応する秘密鍵sk_Aに基づいて復号することによって共通鍵ｋを得ることと、ファイル共有装置１０から受けた暗号化データ部分（Ｅ（ｋ，Ｄ））を、当該得られた共通鍵ｋに基づいて復号することとにより、ファイルのデータＤを得る。

[0108] 具体的には、クライアント装置２０では、制御部２１が、秘密鍵記憶部２４から秘密鍵sk_Aを取得し、秘密鍵sk_Aと第２暗号化共通鍵部分（Ｅ（pk_A，ｋ））を暗号処理部２５に渡す。暗号処理部２５は、第２暗号化共通鍵部分（Ｅ（pk_A，ｋ））を秘密鍵sk_Aで復号し、得られた共通鍵ｋを制御部２１に渡す（ＳＴ１５）。

[0109] クライアント装置２０では、制御部２１が、ステップＳＴ１４’で受信した第２暗号化データ部分（Ｅ（ｋ，Ｄ））とステップＳＴ１５で得た共通鍵ｋを暗号処理部２５に渡す。暗号処理部２５は、第２暗号化データ部分を共通鍵ｋで復号し、ファイルの平文のデータＤを得る。データＤのファイルを制御部２１に渡す（ＳＴ１６）。

[0110] 以上により、ファイルダウンロードの処理が完了する。

[0111] 次に、グループにメンバを追加する処理の流れを図８及び図９に示す。ただし、ここでクライアント装置２０は、グループ管理者が利用しているものとする。

[0112] クライアント装置２０では、制御部２１が、追加したいメンバを識別するメンバＩＤ（例、Ｃ）を含むメンバ追加リクエストをファイル共有装置１０に送信する（ＳＴ２１）。

[0113] ファイル共有装置１０では、制御部１１が、メンバ追加リクエストを受け

ると、挿入処理部１３を呼出す［処理の挿入］（ＳＴ２２）。

[0114] ファイル共有装置１０では、挿入処理部１３が、メンバ追加リクエスト内のメンバＩＤ（Ｃ）に基づいて、再暗号化装置３０にメンバの公開鍵pk_Cを要求する（ＳＴ２３）。

[0115] 再暗号化装置３０では、制御部３１が、要求されたメンバＩＤ（Ｃ）に関連付けられた公開鍵pk_Cを公開鍵記憶部３４から読み込む（ＳＴ２４）。

[0116] 再暗号化装置３０では、制御部３１が、ファイル共有装置１０の挿入処理部１３にメンバの公開鍵pk_C及びメンバＩＤ（Ｃ）を返す（ＳＴ２５）。

[0117] ファイル共有装置１０では、挿入処理部１３が、制御部１１に処理を戻す（取得したメンバの公開鍵pk_C及びメンバＩＤ（Ｃ）も渡す）［挿入した処理の終了］（ＳＴ２６）。

[0118] ファイル共有装置１０では、制御部１１が、メンバの公開鍵pk_C及びメンバＩＤ（Ｃ）をクライアント装置２０に送信する（ＳＴ２７）。

[0119] 本来、既成の機能部は、メンバ追加リクエストの受信時にステップＳＴ３６のメンバ追加処理を行うが、挿入処理部１３の機能により行わないようにする。

[0120] クライアント装置２０では、制御部２１が、秘密鍵記憶部２４からグループの秘密鍵sk_{Gr1}を読み込む（ＳＴ２８）。

[0121] クライアント装置２０では、制御部２１が、メンバの公開鍵pk_Cとグループの秘密鍵sk_{Gr1}を再暗号化鍵作成部２７に渡す。再暗号化鍵作成部２７は、メンバの公開鍵pk_Cとグループの秘密鍵sk_{Gr1}から、メンバの再暗号化鍵$rk_{Gr1\to C}$を作成し、メンバの再暗号化鍵$rk_{Gr1\to C}$及びメンバＩＤ（Ｃ）を制御部２１に渡す（ＳＴ２９）。

[0122] クライアント装置２０では、制御部２１が、メンバの再暗号化鍵$rk_{Gr1\to C}$及びメンバＩＤ（Ｃ）及びグループＩＤ（Ｇｒ１）をファイル共有装置１０に送信する（ＳＴ３０）。

[0123] ファイル共有装置１０では、制御部１１が、再暗号化鍵登録部１８にメンバの再暗号化鍵$rk_{Gr1\to C}$及びメンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）を渡

す（ＳＴ３１）。

[0124] ファイル共有装置１０では、処理挿入部１３が、再暗号化装置３０に再暗号化鍵$rk_{Gr1\to C}$及びメンバＩＤ（Ｃ）を渡す（ＳＴ３２）。

[0125] 再暗号化装置３０では、制御部３１が、再暗号化鍵記憶部３５に再暗号化鍵$rk_{Gr1\to C}$及びメンバＩＤ（Ｃ）を関連付けて書込む（ＳＴ３３）。

[0126] 再暗号化装置３０では、制御部３１が、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）に関連付けて再暗号化鍵$rk_{Gr1\to C}$を登録した旨をファイル共有装置１０に通知する（ＳＴ３４）。

[0127] ファイル共有装置１０では、再暗号化鍵登録部１８が、この通知を受けると、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）を含むメンバ追加依頼をグループ管理部１９に送出する（ＳＴ３５）。

[0128] ファイル共有装置１０では、グループ管理部１９が、メンバ追加依頼を受けると、グループ情報記憶部１６のグループ情報にメンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）を追加する（ＳＴ３６）。

[0129] なお、再暗号化鍵の登録リクエストでメンバ追加処理を行う理由は、ファイル共有装置１０のグループ情報記憶部１６と、再暗号化装置３０の再暗号化鍵記憶部３５との間に不整合が起こらないようにするためである。

[0130] ファイル共有装置１０では、ファイル共有部１４が、メンバ追加処理が完了した旨を再暗号化鍵登録部１８に通知する（ＳＴ３７）。

[0131] ファイル共有装置１０では、暗号化鍵登録部１８が、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）に対応する再暗号化鍵$rk_{Gr1\to C}$を登録した旨を制御部１１に通知する（ＳＴ３８）。

[0132] ファイル共有装置１０では、制御部１１が、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）に対応する再暗号化鍵$rk_{Gr1\to C}$を登録した旨をクライアント装置２０に通知する（ＳＴ３９）。

[0133] クライアント装置２０では、制御部２１が、この通知を表示部（図示せず）に表示する。

[0134] 以上により、メンバ追加の処理が完了する。

[0135] 続いて、グループにメンバを削除する処理の流れを図１０及び図１１に示す。ただし、ここでクライアント装置２０はグループ管理者が利用しているものとする。

[0136] クライアント装置２０では、制御部２１が、削除したいメンバを識別するメンバＩＤ（例、Ｃ）及びそのメンバを削除するグループを識別するグループＩＤ（例、Ｇｒ１）を含むメンバ削除リクエストをファイル共有装置１０に送信する（ＳＴ４１）。

[0137] ファイル共有装置１０では、制御部１１が、メンバ削除リクエストを受けると、処理挿入部１３を呼出す［処理の挿入］（ＳＴ４２）。

[0138] ファイル共有装置１０では、処理挿入部１３が、メンバ削除リクエスト内のメンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）を含む再暗号化鍵削除リクエストを再暗号化装置３０に送信する（ＳＴ４３）。

[0139] 再暗号化装置３０では、制御部３１が、再暗号化鍵削除リクエスト内のメンバＩＤ（Ｃ）に基づいて、当該メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）に関連付けられた再暗号化鍵$rk_{Gr1\to C}$を再暗号化鍵記憶部３５から削除する（ＳＴ４４）。

[0140] 再暗号化装置３０では、制御部３１が、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）に関連付けられた再暗号化鍵$rk_{Gr1\to C}$を削除した旨をファイル共有装置１０に通知する（ＳＴ４５）。

[0141] ファイル共有装置１０では、処理挿入部１３が、この通知を受けると、制御部１１に処理を戻す［処理の挿入終了］（ＳＴ４６）。

[0142] ファイル共有装置１０では、制御部１１が、この通知に基づいて、メンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）を含むメンバ削除依頼をグループ管理部１９に送出する。グループ管理部１９は、メンバ削除依頼を受けると、グループ情報記憶部１６のグループ情報からメンバＩＤ（Ｃ）とグループＩＤ（Ｇｒ１）が関連付けられている行を削除する（ＳＴ４７）。

[0143] ファイル共有装置１０では、制御部１１が、メンバ削除処理が完了した旨をクライアント装置２０に通知する（ＳＴ４８）。

[0144] クライアント装置２０では、制御部２１が、この通知を表示部（図示せず）に表示する。

[0145] 以上により、メンバ削除の処理が完了する。

[0146] 上述したように本実施形態によれば、ファイル共有装置１０が、クライアント装置２０から受けたファイル要求に基づいてファイル記憶部１５から暗号化ファイルを取得し、当該暗号化ファイルを第１暗号化共通鍵部分と暗号化データ部分に分離し、当該暗号化データ部分をクライアント装置２０に送信する処理と並行して、当該第１暗号化共通鍵部分及びメンバＩＤを含む再暗号化要求を再暗号化装置３０に送信し、再暗号化装置３０が、再暗号化要求に基づいて再暗号化鍵記憶部３５から再暗号化鍵を取得し、当該再暗号化鍵に基づいて再暗号化要求内の第１暗号化共通鍵部分を第２暗号化共通鍵部分に再暗号化し、当該第２暗号化共通鍵部分をファイル共有装置１０を介してクライアント装置２０に送信する構成により、クライアント装置２０が、第２暗号化共通鍵部分をメンバの公開鍵に対応する秘密鍵に基づいて復号することによって共通鍵を得ると共に、暗号化データ部分を、当該得られた共通鍵に基づいて復号することにより、データを得るようにしたので、利便性とセキュリティを両立させることができる。

[0147] また、本実施形態によれば、ファイル共有装置１０においては、既存のファイル共有システムの機能を提供している部分を変更せずに、フィルタ機能で再暗号化装置３０と連携することができるため、改修コストを削減することができる。

[0148] また、ファイル共有装置１０がハイブリッド暗号のデータを切り離して鍵部分だけを再暗号化装置に送付することで、通信時間を短縮することができる。データ部分の送信と並行して再暗号化処理を行うことによって、再暗号処理による処理時間の増大を軽減することができる。別途、再暗号化装置３０を用意しているので、既存のファイル共有装置にＣＰＵ負荷をかけずに再暗号化処理を追加することができる。

[0149] 続いて、本実施形態と特許文献１との相違について補足的に説明する。

[0150] 本実施形態では、図２３に示したようにハイブリッド方式での共通鍵部分とデータ部分を切り離し、データ部分をクライアント装置に送付する間に、共通鍵部分の再暗号化処理を行うことで、再暗号化処理に費やす時間によるサービスレベル低下の軽減を図っている。

[0151] これに対し、特許文献１記載の技術は、クライアント端末でＳＯＡＰメッセージに対して暗号化処理を行う際に、ボディ部とヘッダ部に分割し、ボディ部をゲートウェイに送信すると共にボディ部に対して暗号化処理を行い、ヘッダ部を作成する。そして、特許文献１記載の技術は、ボディ部の送信後にヘッダ部をゲートウェイに送信し、ゲートウェイで本来のＳＯＡＰメッセージを作成するものである。ここで、特許文献１記載の技術は、クライアント端末の処理のみに注目するとデータの送信と暗号化処理を並行して行っていることから、本実施形態に似た内容にも見えるが、以下の点で本実施形態とは構成・機能が異なっている。

[0152] （１）特許文献１記載の技術においては、ボディ部とヘッダ部が揃わないとゲートウェイから本来のサーバへ送信できないため、クライアント端末での暗号化処理とデータ送信を並列に行うことでクライアント端末全体での処理を軽減している。しかしながら、特許文献１記載の技術では、ゲートウェイからサーバに送るデータ送信時間が削減できていない点と、ＳＯＡＰメッセージ構築の時間が削減できていない点と、ゲートウェイ装置を別途発明の内容で構築しなければならない点が異なる。また、特許文献１記載の技術でシステム全体の負荷が軽減できるか否かは、暗号化処理を実行するクライアント端末の性能に依存する。

[0153] （２）特許文献１記載の技術においては、暗号化処理をクライアント端末でしか実行できず、ゲートウェイに委託することができない。そのため、特許文献１記載の技術は、クライアント端末での暗号化処理の負荷を軽減できない。

[0154] 上記（１）（２）に対し、本実施形態では、メッセージ構築に該当する処理が存在しないこと、そのためゲートウェイの機能に該当する処理が不要な

こと、および暗号化処理を外部に委託することが可能になる点と、システム全体の負荷が軽減できる点で優れている。また、本実施形態は、メッセージ構築が不要な点や暗号化処理の委託ができることから、特許文献１記載の技術とは構成・機能が異なっている。

[0155] ＜第２の実施形態＞

次に、第２の実施形態に係る再暗号化システムについて図１を参照して説明する。

第２の実施形態は、図１８に示した如き、ハイブリッド方式を用いない基本形態であり、ファイル全体を暗号化及び再暗号化する構成となっている。

[0156] この再暗号化システムは、図１を参照して示すように、前述同様に、クライアント／サーバ構成であり、グループに属するメンバに操作されるクライアント装置２０に通信可能なファイル共有装置１０及び再暗号化装置３０を備えている。但し、共通鍵ｋを用いないため、クライアント装置２０の共通鍵生成部２６は省略される。クライアント装置２０の他の構成は、以下の動作説明中に示す通りである。

[0157] ここで、ファイル共有装置１０のファイル記憶部１５は、グループの公開鍵pk_{Gr1}に基づいてファイル（Ｄ）が暗号化されてなる第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を記憶する。また、ファイル共有装置１０は、例えばファイルダウンロードに関し、以下の各機能(f10-1)～(f10-3)をもっている。

[0158] (f10-1) 制御部１１及び通信部１２により、メンバを識別するメンバＩＤ（例、Ａ）及びグループＩＤ（例、Ｇｒ１）と、第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）のファイル名を含むファイル要求をクライアント装置２０から受けると、制御部１１及びファイル共有部１４により、当該ファイル要求内のファイル名に基づいてファイル記憶部１５から第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を取得する機能。

[0159] (f10-2) 制御部１１、通信部１２及び挿入処理部１３により、当該取得した第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）及び当該ファイル要求内のメンバＩＤ（Ａ）とグループＩＤ（Ｇｒ１）を含む再暗号化要求を再暗号化装置３０に

送信する機能。

[0160] (f10-3) 制御部１１、通信部１２及び挿入処理部１３により、メンバＩＤ（Ａ）とグループＩＤ（Ｇｒ１）の公開鍵$ｐｋ_A$に基づいてファイルが暗号化されてなる第２暗号化ファイルＥ（$ｐｋ_A$，Ｄ）を再暗号化装置３０から受けると、制御部１１及び通信部１２により、当該第２暗号化ファイルＥ（$ｐｋ_A$，Ｄ）をクライアント装置に送信する。

[0161] ファイル共有装置１０の他の構成（ファイルアップロード・メンバ追加処理・メンバ削除処理に関する構成）は、以下の動作説明中に示す通りである。

[0162] また、再暗号化装置３０の再暗号化鍵記憶部３５は、メンバを識別するメンバＩＤ（Ａ，Ｂ，…）及びグループを識別するグループＩＤ（Ｇｒ１，Ｇｒ２，…）と、第１暗号化ファイルを復号せずに第２暗号化ファイルに再暗号化するための再暗号化鍵（$ｒｋ_{Gr1→A}$，$ｒｋ_{Gr1→B}$，…）とを関連付けて記憶する。また、再暗号化装置３０は、例えばファイルダウンロードに関し、以下の各機能(f30-1)～(f30-3)をもっている。

[0163] (f30-1) 制御部３１及び通信部３２により、再暗号化要求をファイル共有装置１０から受けると、制御部３１及び再暗号化処理部３３により、当該再暗号化要求内のメンバＩＤ（例、Ａ）とグループＩＤ（例、Ｇｒ１）に基づいて再暗号化鍵記憶部３５から再暗号化鍵$ｒｋ_{Gr1→A}$を取得する機能。

[0164] (f30-2) 再暗号化処理部３３により、当該取得した再暗号化鍵$ｒｋ_{Gr1→A}$に基づいて、再暗号化要求内の第１暗号化ファイルＥ（$ｐｋ_{Gr1}$，Ｄ）を第２暗号化ファイルＥ（$ｐｋ_A$，Ｄ）に再暗号化する機能。

[0165] (f30-3) 制御部３１及び通信部３２により、当該再暗号化により得られた第２暗号化ファイルＥ（$ｐｋ_A$，Ｄ）をファイル共有装置１０に送信する機能。

[0166] 再暗号化装置３０の他の構成（ファイルアップロード・メンバ追加処理・メンバ削除処理に関する構成）は、以下の動作説明中に示す通りである。

[0167] 次に、以上のように構成された再暗号化システムの動作について説明する

。

[0168] 始めに、ファイルアップロードの処理の流れを述べる。

[0169] クライアント装置２０では、制御部２１がファイル記憶部２３からアップロードするファイル（Ｄ）を読み込む。

[0170] クライアント装置２０では、制御部２１が、アップロードするファイルを公開するグループの公開鍵pk_{Gr1}をファイル共有装置１０に要求する。具体的には、グループを識別するグループＩＤ（例、Ｇｒ１）を含む公開鍵要求をファイル共有装置１０に送信する。

[0171] ファイル共有装置１０では、制御部１１が、この公開鍵要求を公開鍵取得部１７に送出する。

[0172] ファイル共有装置１０では、公開鍵取得部１７が、この公開鍵要求を再暗号化装置３０に送信する。

[0173] 再暗号化装置３０では、制御部３１が、公開鍵要求内のグループＩＤ（例、Ｇｒ１）に基づいて、公開鍵記憶部３４からグループの公開鍵pk_{Gr1}を取り出す。

[0174] 再暗号化装置３０では、制御部３１がグループの公開鍵pk_{Gr1}をファイル共有装置１０に送信する。

[0175] ファイル共有装置１０では、公開鍵取得部１７が、制御部１１にグループの公開鍵pk_{Gr1}を渡す。

[0176] ファイル共有装置１０では、制御部１１が、グループの公開鍵pk_{Gr1}をクライアント装置２０に送信する。

[0177] クライアント装置２０では、制御部２１が、受信したグループの公開鍵pk_{Gr1}と、アップロードするファイルとを暗号処理部２５に渡す。暗号処理部２５は、ファイル（Ｄ）をグループの公開鍵pk_{Gr1}で暗号化し、得られた第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を制御部２１に渡す。

[0178] クライアント装置２０では、制御部２１が、第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）をファイル共有装置１０に送信する。

[0179] ファイル共有装置１０では、制御部１１が、第１暗号化ファイルＥ（pk_{Gr1}

，Ｄ）をファイル共有部１４に渡す。ファイル共有部１４は、第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）をファイル記憶部１５に書込む。

[0180] ファイル共有装置１０では、制御部１１が、ファイルアップロードが完了した旨をクライアント装置２０に通知する。

[0181] クライアント装置２０では、制御部２１が、この通知を表示部（図示せず）に表示する。

[0182] 以上により、ファイルアップロードの処理が完了する。

[0183] 続いて、ファイルダウンロードの処理の流れを説明する。

[0184] クライアント装置２０では、制御部２１が、メンバを識別するメンバＩＤ（例、Ａ）及びグループを識別するグループＩＤ（例、Ｇｒ１）と、第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）のファイル名を含むファイル要求をファイル共有装置１０に送信する。

[0185] ファイル共有装置１０では、制御部１１が、ファイル要求をクライアント装置２０から受けると、ファイル共有部１４を介して、ファイル要求内のファイル名に基づいてファイル記憶部１５から第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を取得する。具体的には、制御部１１は、クライアント装置２０から受けたファイル要求をファイル共有部１４に送出する。ファイル共有部１４は、ファイル記憶部１５から第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を取得し、制御部１１に渡す。

[0186] ファイル共有装置１０では、制御部１１が、取得した第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）を挿入処理部１３に渡す［処理の挿入］。

[0187] ファイル共有装置１０では、処理挿入部１３が、渡された第１暗号化ファイルＥ（pk_{Gr1}，Ｄ）及びファイル要求内のメンバＩＤを含む再暗号化要求を再暗号化装置３０に送信する。

[0188] 再暗号化装置３０では、再暗号化要求をファイル共有装置１０から受けると、当該再暗号化要求内のメンバＩＤ（例、Ａ）とグループＩＤ（例、Ｇｒ１）に基づいて再暗号化鍵記憶部３５から再暗号化鍵$rk_{Gr1\rightarrow A}$を取得し、当該取得した再暗号化鍵$rk_{Gr1\rightarrow A}$に基づいて、再暗号化要求内の第１暗号化ファイ

ル（Ｅ（ｐｋ$_{Gr1}$，Ｄ）を第２暗号化ファイル（Ｅ（ｐｋ$_{A}$，Ｄ）に再暗号化する。

[0189] 具体的には、制御部３１は、再暗号化要求内の第１暗号化ファイルＥ（ｐｋ$_{Gr1}$，Ｄ）及びメンバＩＤ（例、Ａ）とグループＩＤ（例、Ｇｒ１）を再暗号化処理部３３に渡す。再暗号化処理部３３は、このメンバＩＤに基づいて再暗号化鍵記憶部３４から再暗号化鍵ｒｋ$_{Gr1→A}$を取得し、第１暗号化ファイルＥ（ｐｋ$_{Gr1}$，Ｄ）を第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）に再暗号化し、得られた第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）を制御部３１に渡す。

[0190] 再暗号化装置３０では、制御部３１が、再暗号化により得られた第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）をファイル共有装置１０に送信する。

[0191] ファイル共有装置１０では、挿入処理部１３が、制御部１１に第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）を渡す。

[0192] ファイル共有装置１０では、制御部１１が、第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）をクライアント装置２０に送信する［挿入した処理の終了］。

[0193] クライアント装置２０は、ファイル共有装置１０から受けた第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）をメンバの公開鍵ｐｋ$_{A}$に対応する秘密鍵ｓｋ$_{A}$に基づいて復号することにより、ファイル（Ｄ）を得る。

[0194] 具体的には、クライアント装置２０では、制御部２１が、秘密鍵記憶部２４から秘密鍵ｓｋ$_{A}$を取得し、秘密鍵ｓｋ$_{A}$と第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）を暗号処理部２５に渡す。暗号処理部２５は、第２暗号化ファイルＥ（ｐｋ$_{A}$，Ｄ）を秘密鍵ｓｋ$_{A}$で復号し、得られたファイル（Ｄ）を制御部２１に渡す。

[0195] 以上により、ファイルダウンロードの処理が完了する。

[0196] なお、メンバ追加処理及びメンバ削除処理は、第１の実施形態と同様である。

[0197] 上述したように本実施形態によれば、ファイル共有装置１０が、クライアント装置２０から受けたファイル要求に基づいてファイル記憶部１５から第１暗号化ファイルを取得し、当該第１暗号化ファイルを含む再暗号化要求を

再暗号化装置３０に送信し、再暗号化装置３０が、再暗号化鍵に基づいて再暗号化鍵記憶部３５から再暗号化鍵を取得し、当該再暗号化鍵に基づいて再暗号化要求内の第１暗号化ファイルを第２暗号化ファイルに再暗号化し、当該第２暗号化ファイルをファイル共有装置１０を介してクライアント装置２０に送信し、クライアント装置２０が、第２暗号化ファイルをメンバの公開鍵に対応する秘密鍵に基づいて復号することによってファイルを得る構成により、第１暗号化ファイル全体を再暗号化することから、第１の実施形態に比べて処理時間がかかる点を除き、第１の実施形態と同様の効果を得ることができる。

[0198] なお、上記の各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

[0199] また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

[0200] また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が上記実施形態を実現するための各処理の一部を実行しても良い。

[0201] さらに、各実施形態における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

[0202] また、記憶媒体は１つに限らず、複数の媒体から上記の各実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

[0203] なお、各実施形態におけるコンピュータは、記憶媒体に記憶されたプログ

ラムに基づき、上記の各実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

[0204] また、各実施形態におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

[0205] なお、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］ グループに属するメンバに操作されるクライアント装置（２０）に通信可能なファイル共有装置（１０）及び再暗号化装置（３０）を備えた再暗号化システムであって、

前記ファイル共有装置は、

前記グループの公開鍵に基づいてファイルが暗号化されてなる第１暗号化ファイルを記憶するファイル記憶手段（１５）と、

前記メンバを識別するメンバＩＤ及び前記第１暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記ファイル記憶手段から前記第１暗号化ファイルを取得する手段（１１）と、

前記取得した第１暗号化ファイル及び前記ファイル要求内のメンバＩＤを含む再暗号化要求を前記再暗号化装置に送信する手段（１３）と、

前記メンバＩＤの公開鍵に基づいて前記ファイルが暗号化されてなる第２暗号化ファイルを前記再暗号化装置から受けると、当該第２暗号化ファイルを前記クライアント装置に送信する手段（１１）と

を備え、

前記再暗号化装置は、

前記メンバを識別するメンバＩＤと、前記第１暗号化ファイルを復号せずに前記第２暗号化ファイルに再暗号化するための再暗号化鍵とを関連付けて記憶する再暗号化鍵記憶手段（３５）と、

前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する手段（３３）と、

前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化ファイルを前記第２暗号化ファイルに再暗号化する手段（３３）と、

前記再暗号化により得られた第２暗号化ファイルを前記ファイル共有装置に送信する手段（３１）と

を備え、

前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得る再暗号化システム。

［請求項2］ グループに属するメンバに操作されるクライアント装置（２０）に通信可能なファイル共有装置（１０）及び再暗号化装置（３０）を備えた再暗号化システムであって、

前記ファイル共有装置は、

前記グループの公開鍵に基づいて共通鍵が暗号化されてなる第１暗号化共通鍵部分と、前記共通鍵に基づいてデータが暗号化されてなる暗号化データ部分とを含む暗号化ファイルを記憶するファイル記憶手段（１５）と、

前記メンバを識別するメンバＩＤ及び前記暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記ファイル記憶手段から前記暗号化ファイルを取得する手段（１１）と、

前記取得した暗号化ファイルを前記第１暗号化共通鍵部分と前記暗号化データ部分に分離する手段（１３）と、

前記分離された暗号化データ部分を前記クライアント装置に送信する処理と並行して、前記第１暗号化共通鍵部分及び前記ファイル要求内のメンバＩＤを含む再暗号化要求を前記再暗号化装置に送信する手段（１３）と、

前記メンバＩＤの公開鍵に基づいて前記共通鍵が暗号化されてなる第２暗号化共通鍵部分を前記再暗号化装置から受けると、当該第２暗号化共通鍵部分を前記クライアント装置に送信する手段（１１）と

を備え、

前記再暗号化装置は、

前記メンバを識別するメンバＩＤと、前記第１暗号化共通鍵部分を復号せずに前記第２暗号化共通鍵部分に再暗号化するための再暗号化鍵とを関連付けて記憶する再暗号化鍵記憶手段（３５）と、

前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する手段（３３）と、

前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化共通鍵部分を前記第２暗号化共通鍵部分に再暗号化する手段（３３）と、

前記再暗号化により得られた第２暗号化共通鍵部分を前記ファイル共有装置に送信する手段（３１）と

を備え、

前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化共通鍵部分を前記メンバの公開鍵に対応する秘密鍵に基づいて復号することによって前記共通鍵を得ることと、前記ファイル共有装置から受けた暗号化データ部分を、当該得られた共通鍵に基づいて復号することとにより、前記データを得る再暗号化システム。

［請求項3］ グループに属するメンバに操作されるクライアント装置（２０）に通信可能なファイル共有装置（１０）であって、前記グループの公開鍵に基づいてファイルが暗号化されてなる第１暗号化ファイルをメモリに記憶し、前記メンバを識別するメンバＩＤ及び前記第１暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記メモリから前記第１暗号化ファイルを取得し、前記取得した第１暗号化ファイル及び前記ファイル要求内のメンバＩＤを含む再暗号化要求を再暗号化装置（３０）に送信し、前記メンバＩＤの公開鍵に基づいて前記ファイルが暗号化されてなる第２暗号化ファイルを前記再暗号化装置か

ら受けると、当該第２暗号化ファイルを前記クライアント装置に送信する前記ファイル共有装置に通信可能な前記再暗号化装置であって、

前記メンバを識別するメンバＩＤと、前記第１暗号化ファイルを復号せずに前記第２暗号化ファイルに再暗号化するための再暗号化鍵とを関連付けて記憶する再暗号化鍵記憶手段（３５）と、

前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する手段（３３）と、

前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化ファイルを前記第２暗号化ファイルに再暗号化する手段（３３）と、

前記再暗号化により得られた第２暗号化ファイルを前記ファイル共有装置に送信する手段（３１）と

を備えており、

前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得る再暗号化装置。

［請求項4］ グループに属するメンバに操作されるクライアント装置（２０）に通信可能なファイル共有装置（１０）であって、前記グループの公開鍵に基づいて共通鍵が暗号化されてなる第１暗号化共通鍵部分と、前記共通鍵に基づいてデータが暗号化されてなる暗号化データ部分とを含む暗号化ファイルをメモリに記憶し、前記メンバを識別するメンバＩＤ及び前記暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記メモリから前記暗号化ファイルを取得し、前記取得した暗号化ファイルを前記第１暗号化共通鍵部分と前記暗号化データ部分に分離し、前記分離した暗号化データ部分を前記クライアント装置に送信する処理と並行して、前記第１暗号化共通鍵部分及び前記ファイ

ル要求内のメンバＩＤを含む再暗号化要求を前記再暗号化装置（３０）に送信し、前記メンバＩＤの公開鍵に基づいて前記共通鍵が暗号化されてなる第２暗号化共通鍵部分を前記再暗号化装置から受けると、当該第２暗号化共通鍵部分を前記クライアント装置に送信する前記ファイル共有装置に通信可能な前記再暗号化装置であって、

前記メンバを識別するメンバＩＤと、前記第１暗号化共通鍵部分を復号せずに前記第２暗号化共通鍵部分に再暗号化するための再暗号化鍵とを関連付けて記憶する再暗号化鍵記憶手段（３５）と、

前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する手段（３３）と、

前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化共通鍵部分を前記第２暗号化共通鍵部分に再暗号化する手段（３３）と、

前記再暗号化により得られた第２暗号化共通鍵部分を前記ファイル共有装置に送信する手段（３１）と

を備えており、

前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化共通鍵部分を前記メンバの公開鍵に対応する秘密鍵に基づいて復号することによって前記共通鍵を得ることと、前記ファイル共有装置から受けた暗号化データ部分を、当該得られた共通鍵に基づいて復号することとにより、前記データを得る再暗号化装置。

［請求項5］ グループに属するメンバに操作されるクライアント装置（２０）に通信可能なファイル共有装置（１０）であって、前記グループの公開鍵に基づいてファイルが暗号化されてなる第１暗号化ファイルをメモリに記憶し、前記メンバを識別するメンバＩＤ及び前記第１暗号化ファイルのファイル名を含むファイル要求を前記クライアント装置から受けると、前記ファイル要求内のファイル名に基づいて前記メモリか

ら前記第１暗号化ファイルを取得し、前記取得した第１暗号化ファイル及び前記ファイル要求内のメンバＩＤを含む再暗号化要求を再暗号化装置（３０）に送信し、前記メンバＩＤの公開鍵に基づいて前記ファイルが暗号化されてなる第２暗号化ファイルを前記再暗号化装置から受けると、当該第２暗号化ファイルを前記クライアント装置に送信する前記ファイル共有装置に通信可能であり、且つ再暗号化鍵記憶手段を備えた前記再暗号化装置のプロセッサに実行され、非一時的なコンピュータ読取り可能な記憶媒体（Ｍ３）に記憶されたプログラムであって、

前記メンバを識別するメンバＩＤと、前記第１暗号化ファイルを復号せずに前記第２暗号化ファイルに再暗号化するための再暗号化鍵とを関連付けて前記再暗号化鍵記憶手段（３５）に書込む処理を前記プロセッサに実行させる第１プログラムコード、

前記再暗号化要求を前記ファイル共有装置から受けると、当該再暗号化要求内のメンバＩＤに基づいて前記再暗号化鍵記憶手段から前記再暗号化鍵を取得する処理を前記プロセッサに実行させる第２プログラムコード（３３）、

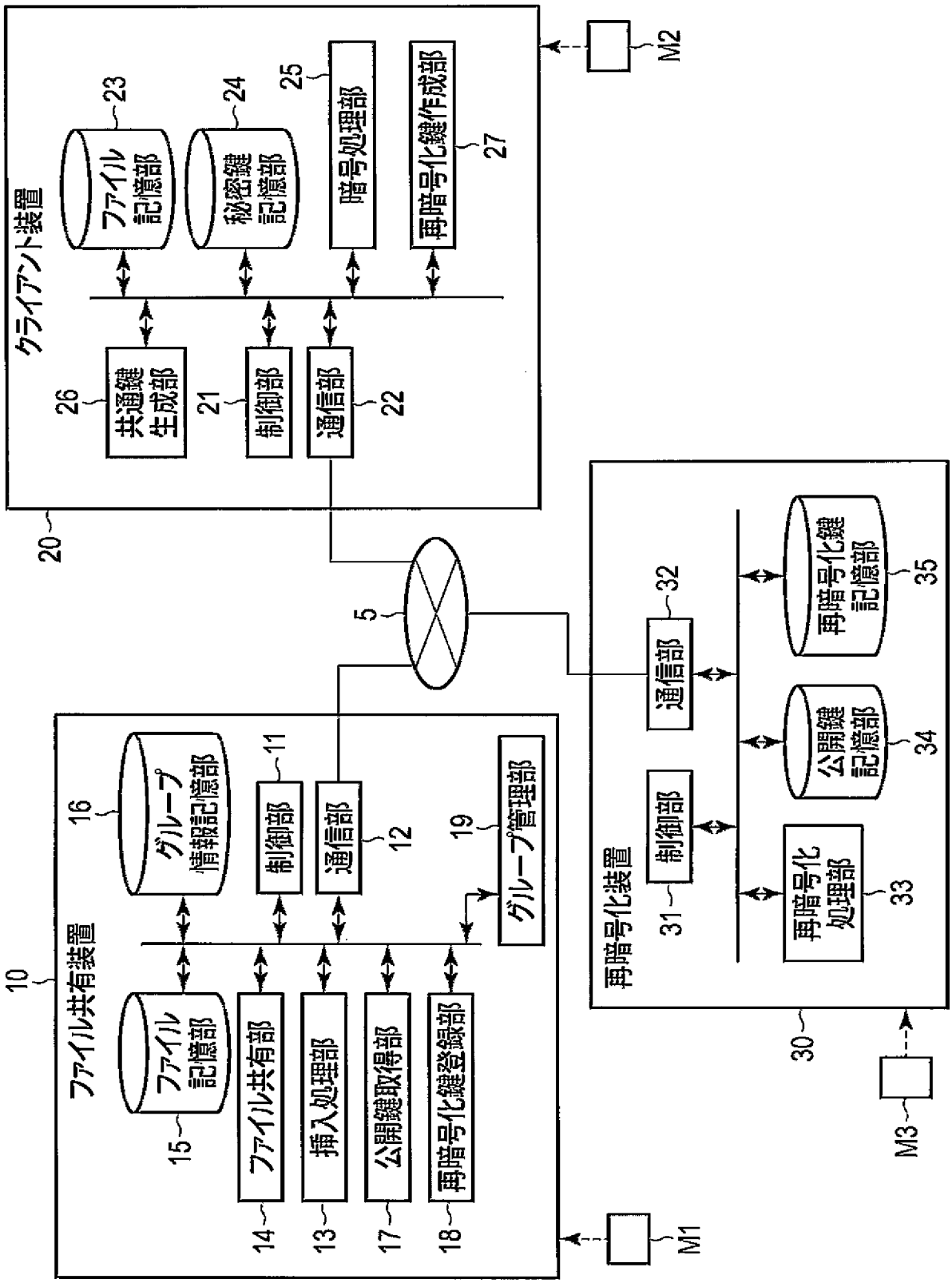
前記取得した再暗号化鍵に基づいて、前記再暗号化要求内の第１暗号化ファイルを前記第２暗号化ファイルに再暗号化する処理を前記プロセッサに実行させる第３プログラムコード（３３）、

前記再暗号化により得られた第２暗号化ファイルを前記ファイル共有装置に送信する処理を前記プロセッサに実行させる第４プログラムコード（３１）、

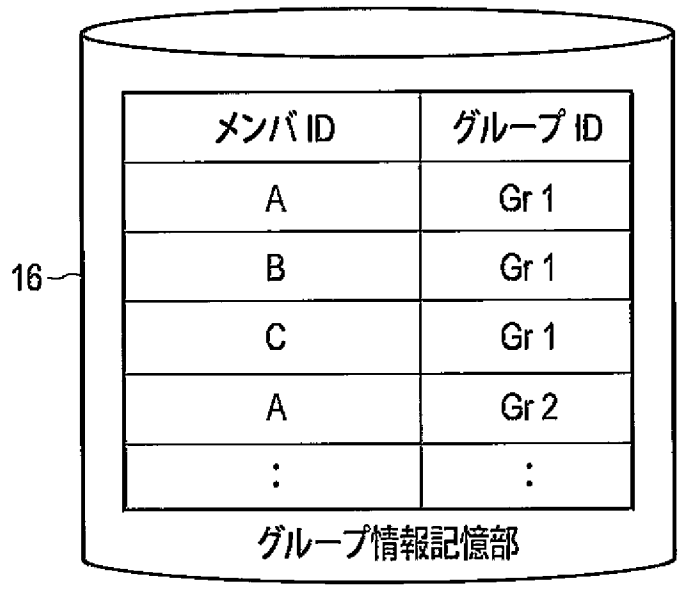
を備えており、

前記クライアント装置は、前記ファイル共有装置から受けた第２暗号化ファイルを前記メンバの公開鍵に対応する秘密鍵に基づいて復号することにより、前記ファイルを得るプログラム。

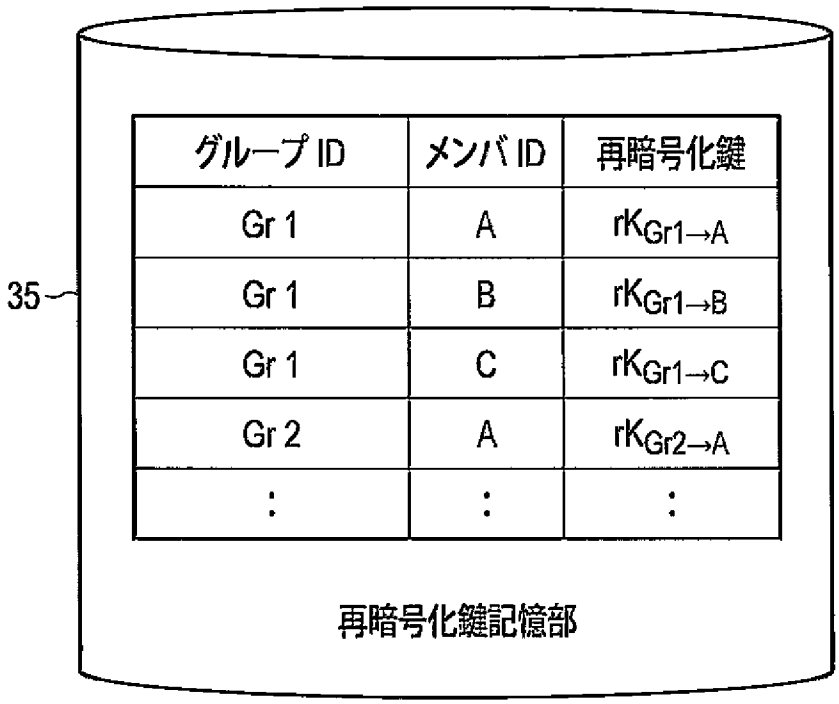
[図1]


クライアント装置
20
ファイル記憶部
23
秘密鍵記憶部
24
暗号処理部
25
再暗号化鍵作成部
27
共通鍵生成部
26
制御部
21
通信部
22
M2
5
ファイル共有装置
10
グループ情報記憶部
16
制御部
11
通信部
12
グループ管理部
19
ファイル記憶部
15
ファイル共有部
14
挿入処理部
13
公開鍵取得部
17
再暗号化鍵登録部
18
M1
再暗号化装置
30
通信部
32
制御部
31
再暗号化処理部
33
公開鍵記憶部
34
再暗号化鍵記憶部
35
M3

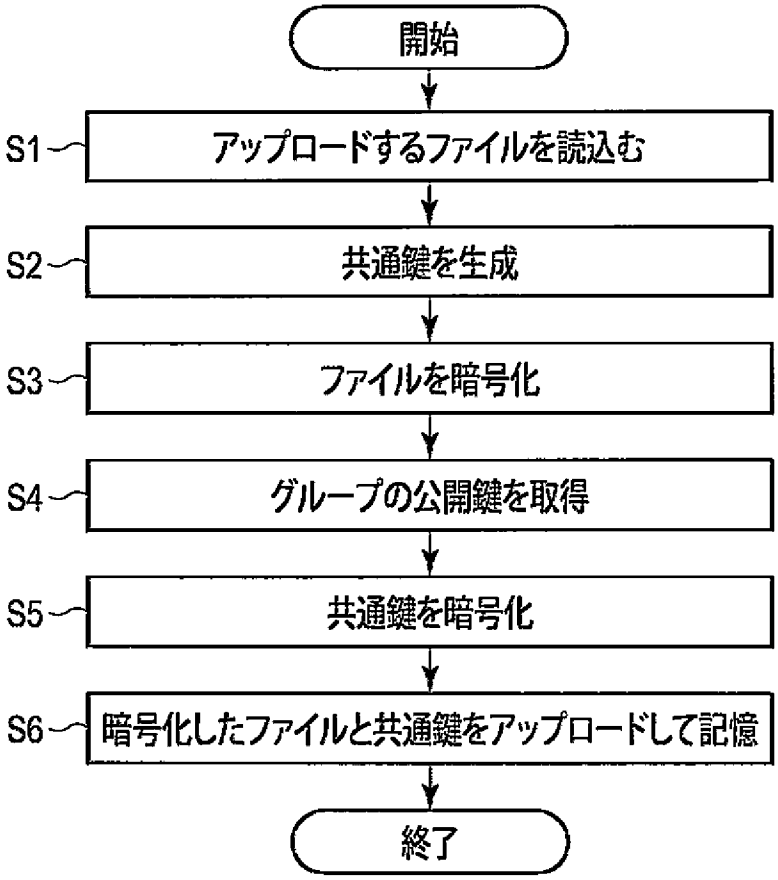
[図2]


16
メンバ ID
グループ ID
A
Gr 1
B
Gr 1
C
Gr 1
A
Gr 2
:
:
グループ情報記憶部

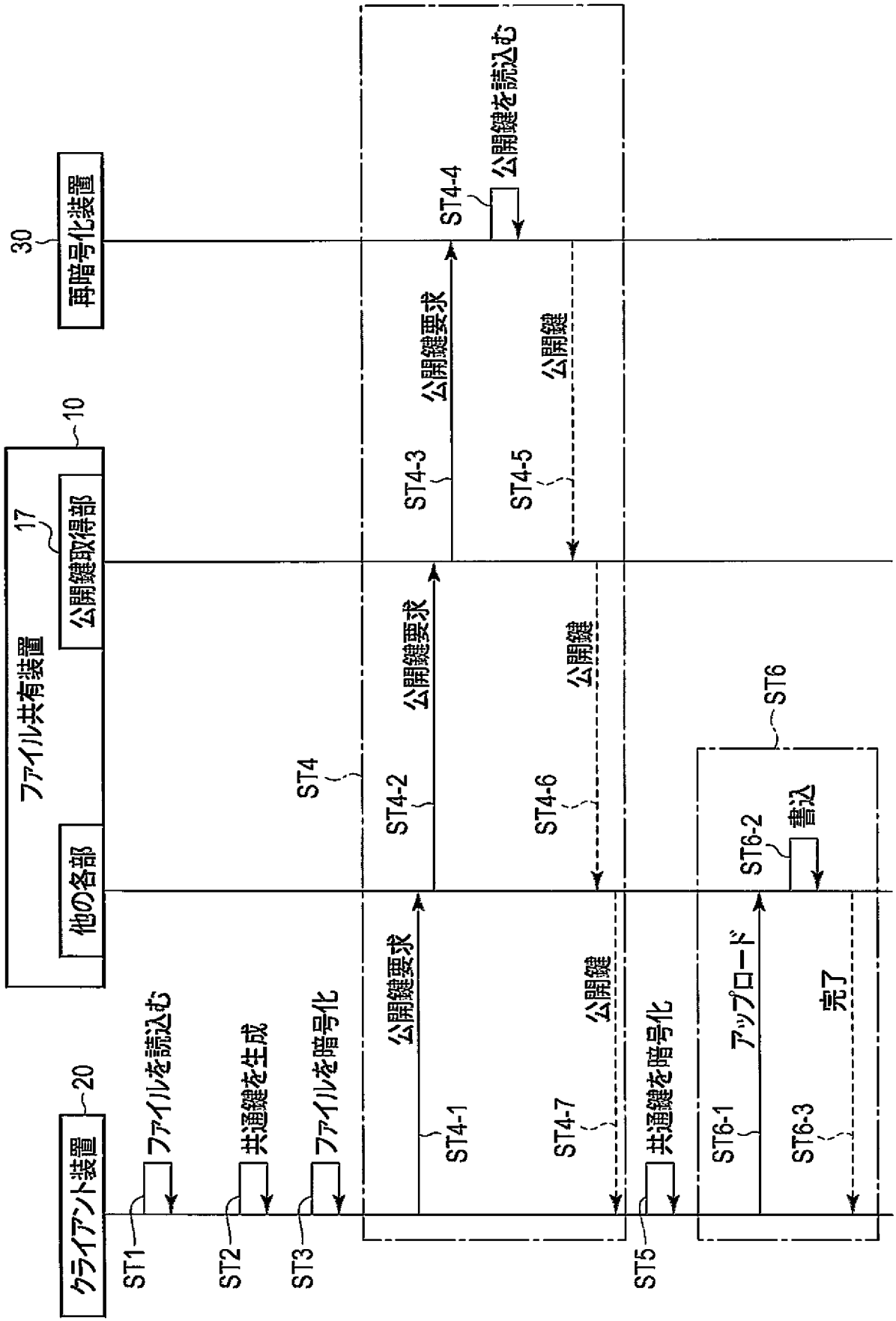
[図3]


35
グループ ID
メンバ ID
再暗号化鍵
Gr 1
A
$rK_{Gr1 \to A}$
Gr 1
B
$rK_{Gr1 \to B}$
Gr 1
C
$rK_{Gr1 \to C}$
Gr 2
A
$rK_{Gr2 \to A}$
:
:
:
再暗号化鍵記憶部

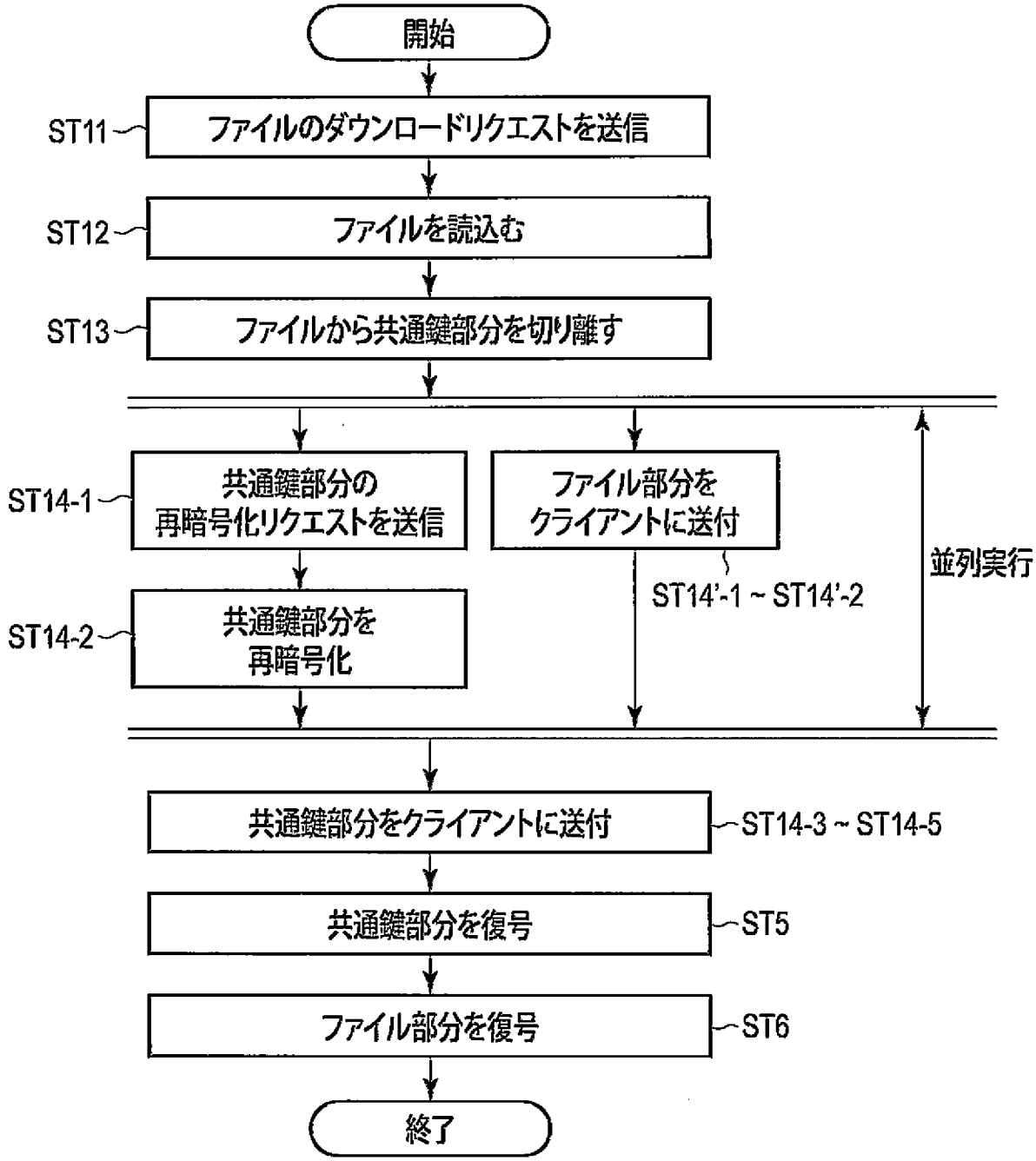
[図4]


開始
S1
アップロードするファイルを読込む
S2
共通鍵を生成
S3
ファイルを暗号化
S4
グループの公開鍵を取得
S5
共通鍵を暗号化
S6
暗号化したファイルと共通鍵をアップロードして記憶
終了

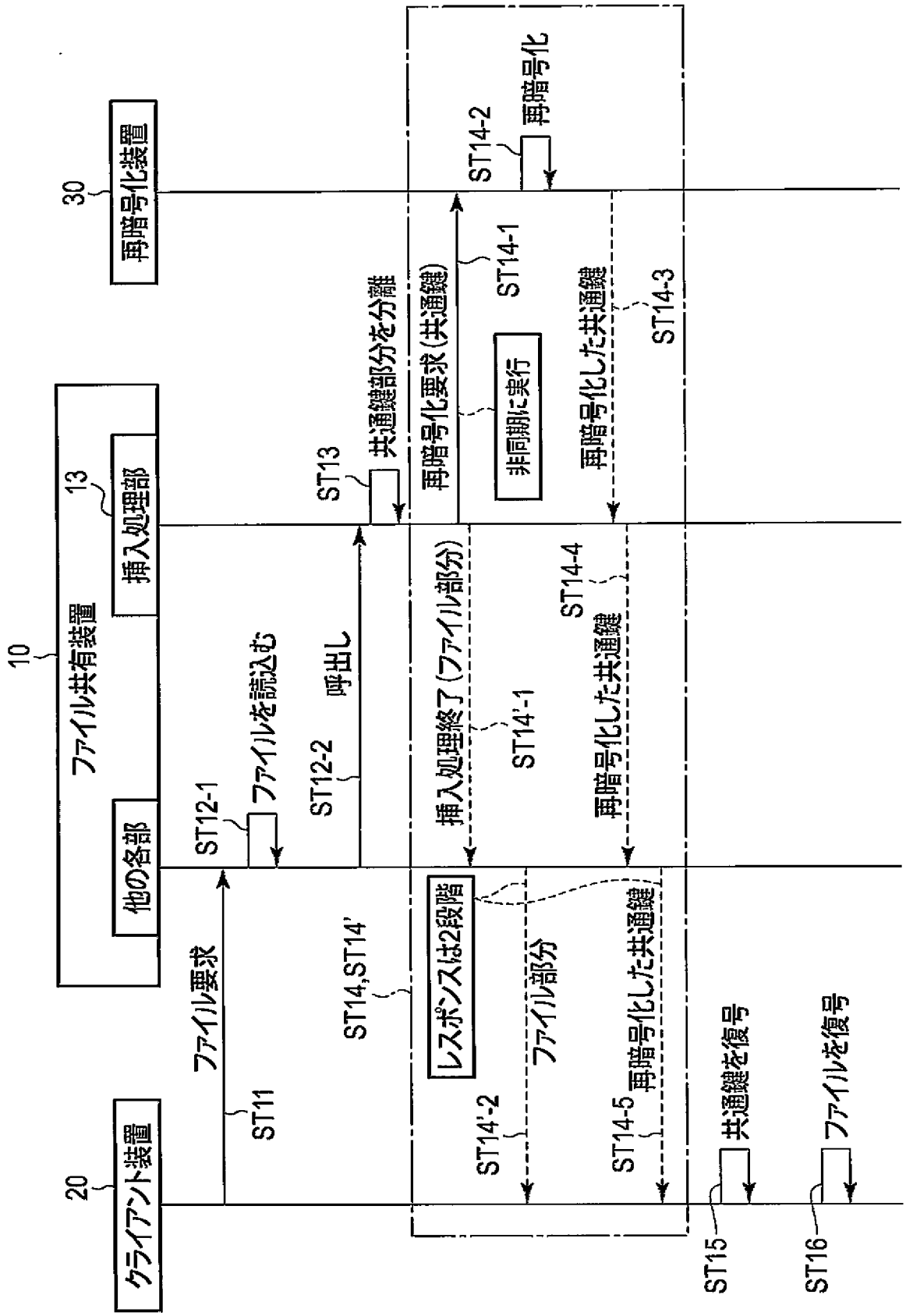
[図5]


クライアント装置
20
ファイル共有装置
10
他の各部
公開鍵取得部
17
再暗号化装置
30
ST1
ファイルを読込む
ST2
共通鍵を生成
ST3
ファイルを暗号化
ST4
ST4-1
公開鍵要求
ST4-2
公開鍵要求
ST4-3
公開鍵要求
ST4-4
公開鍵を読込む
ST4-5
公開鍵
ST4-6
公開鍵
ST4-7
公開鍵
ST5
共通鍵を暗号化
ST6
ST6-1
アップロード
ST6-2
書込
ST6-3
完了

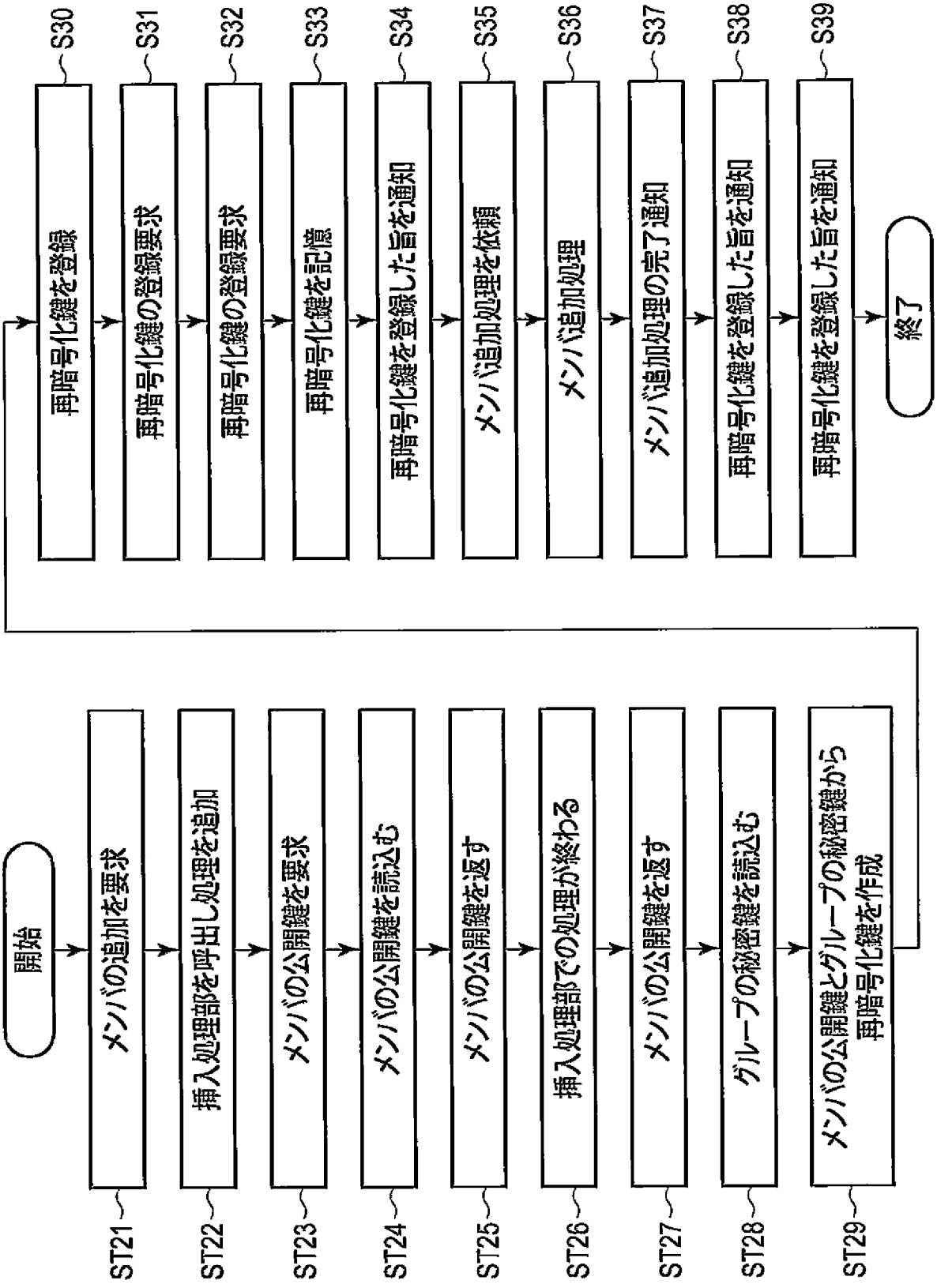
[図6]


開始
ST11
ファイルのダウンロードリクエストを送信
ST12
ファイルを読込む
ST13
ファイルから共通鍵部分を切り離す
ST14-1
共通鍵部分の
再暗号化リクエストを送信
ファイル部分を
クライアントに送付
ST14'-1 ~ ST14'-2
並列実行
ST14-2
共通鍵部分を
再暗号化
共通鍵部分をクライアントに送付
ST14-3 ~ ST14-5
共通鍵部分を復号
ST5
ファイル部分を復号
ST6
終了

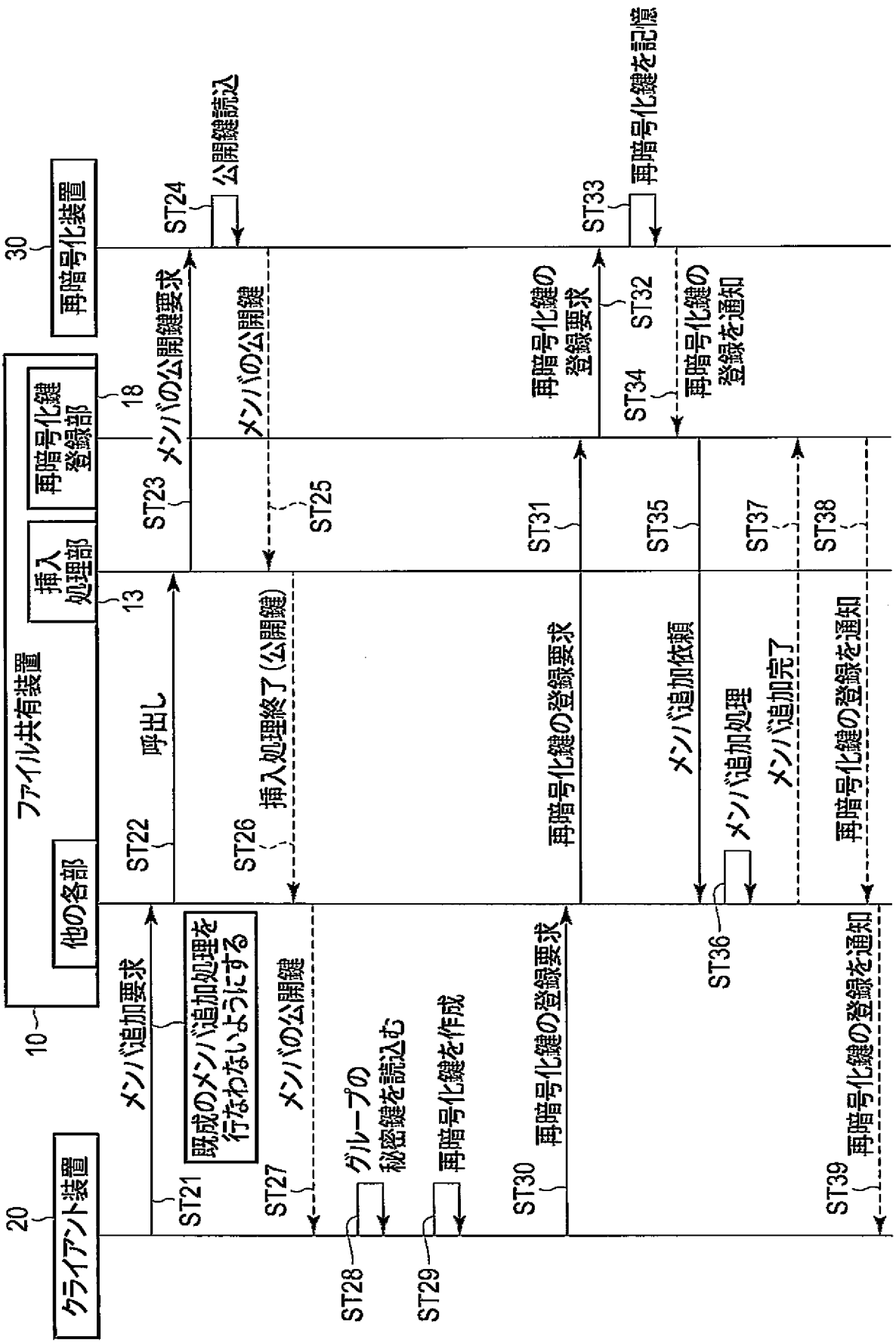
[図7]


10
ファイル共有装置
13
挿入処理部
他の各部
20
クライアント装置
30
再暗号化装置
ST11
ファイル要求
ST12-1
ファイルを読込む
ST12-2
呼出し
ST13
共通鍵部分を分離
ST14,ST14'
ST14-1
再暗号化要求(共通鍵)
非同期に実行
ST14-2
再暗号化
ST14-3
再暗号化した共通鍵
ST14'-1
挿入処理終了(ファイル部分)
ST14-4
再暗号化した共通鍵
レスポンスは2段階
ST14'-2
ファイル部分
ST14-5
再暗号化した共通鍵
ST15
共通鍵を復号
ST16
ファイルを復号

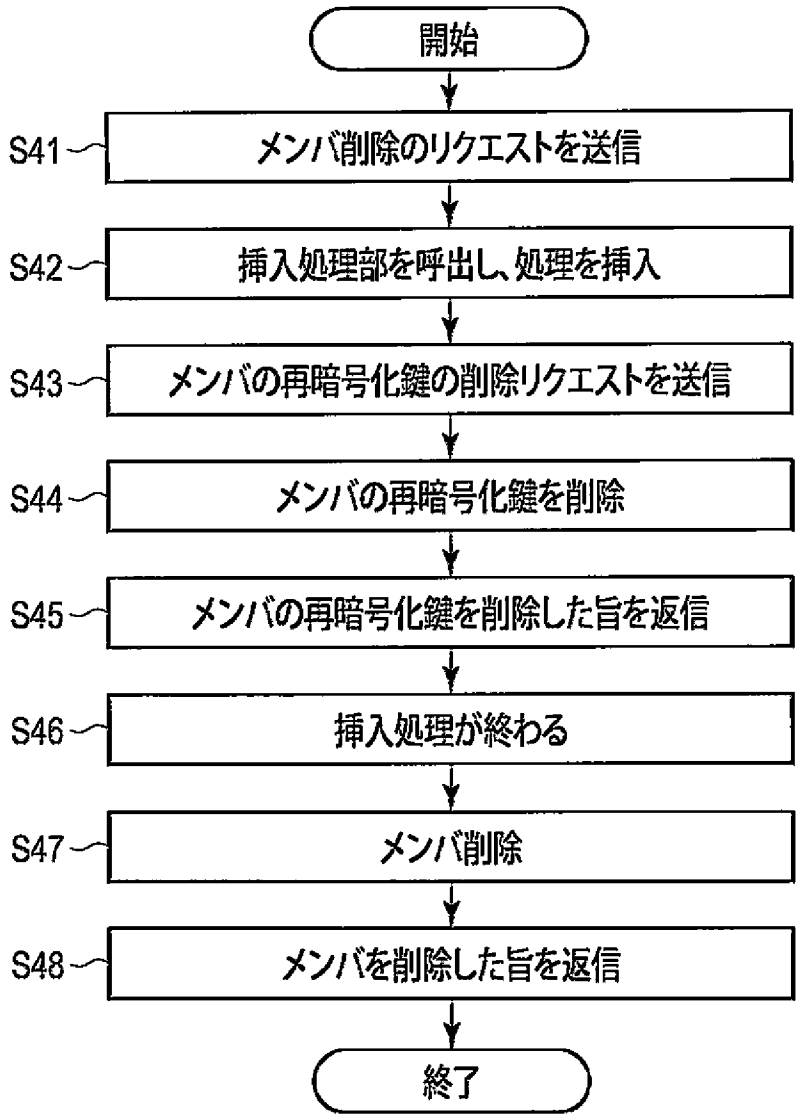
[図8]


開始
メンバの追加を要求
挿入処理部を呼出し処理を追加
メンバの公開鍵を要求
メンバの公開鍵を読込む
メンバの公開鍵を返す
挿入処理部での処理が終わる
メンバの公開鍵を返す
グループの秘密鍵を読込む
メンバの公開鍵とグループの秘密鍵から再暗号化鍵を作成
再暗号化鍵を登録
再暗号化鍵の登録要求
再暗号化鍵の登録要求
再暗号化鍵を記憶
再暗号化鍵を登録した旨を通知
メンバ追加処理を依頼
メンバ追加処理
メンバ追加処理の完了通知
再暗号化鍵を登録した旨を通知
再暗号化鍵を登録した旨を通知
終了
ST21
ST22
ST23
ST24
ST25
ST26
ST27
ST28
ST29
S30
S31
S32
S33
S34
S35
S36
S37
S38
S39

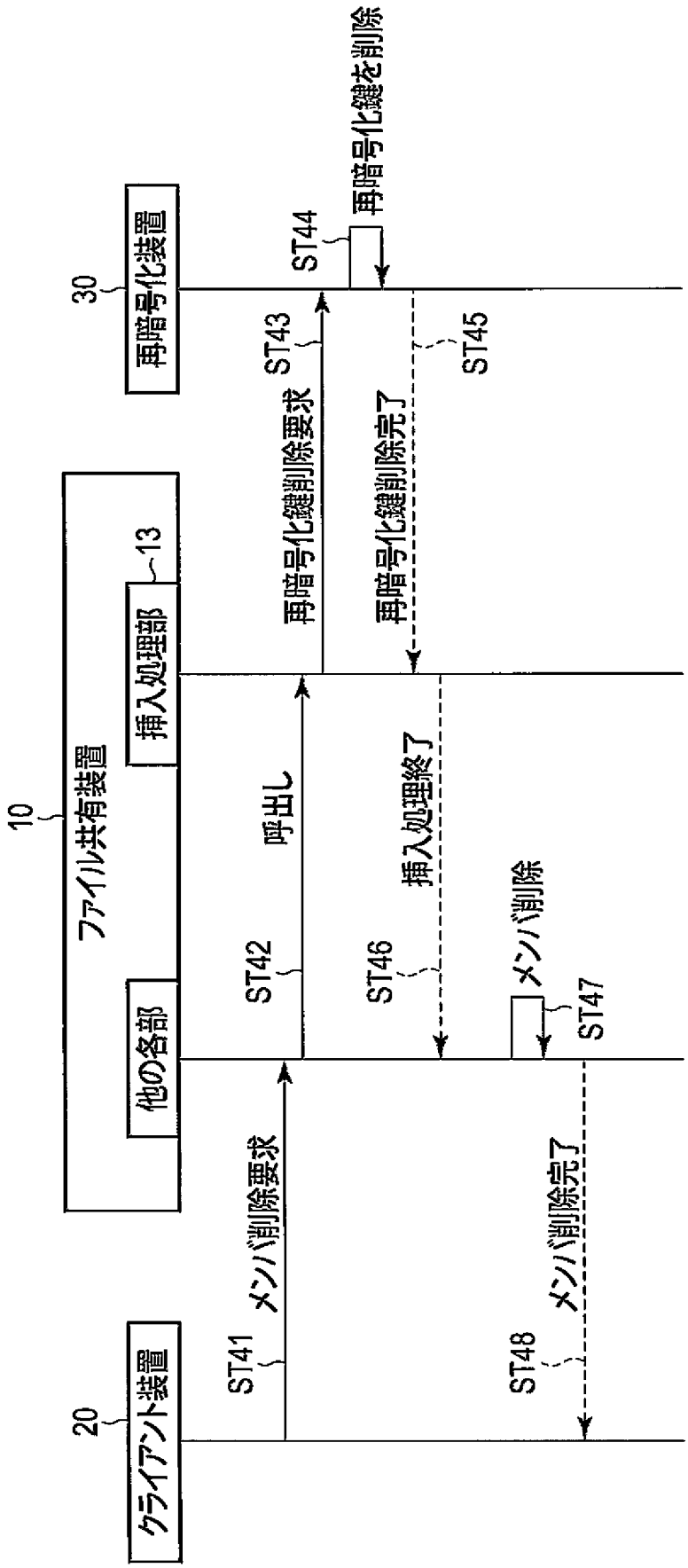
[図9]


ファイル共有装置
10
他の各部
挿入処理部
13
再暗号化鍵登録部
18
再暗号化装置
30
クライアント装置
20
メンバ追加要求
既成のメンバ追加処理を行なわないようにする
ST21
呼出し
ST22
挿入処理終了(公開鍵)
ST26
メンバの公開鍵
ST27
グループの秘密鍵を読込む
ST28
再暗号化鍵を作成
ST29
再暗号化鍵の登録要求
ST30
メンバの公開鍵要求
ST23
公開鍵読込
ST24
メンバの公開鍵
ST25
再暗号化鍵の登録要求
ST31
再暗号化鍵を記憶
ST33
再暗号化鍵の登録要求
ST32
再暗号化鍵の登録を通知
ST34
メンバ追加依頼
ST35
メンバ追加処理
ST36
メンバ追加完了
ST37
再暗号化鍵の登録を通知
ST38
再暗号化鍵の登録を通知
ST39

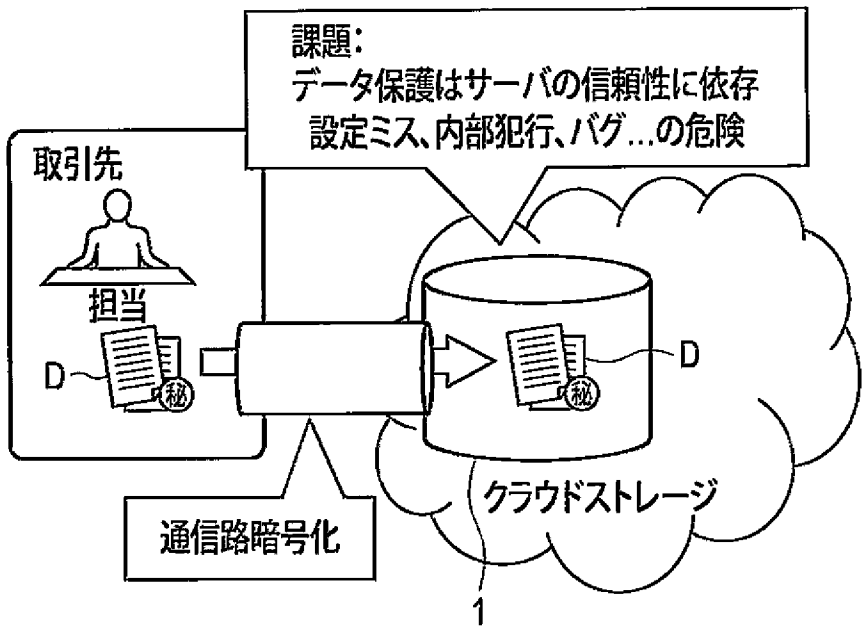
[図10]


開始
S41
メンバ削除のリクエストを送信
S42
挿入処理部を呼出し、処理を挿入
S43
メンバの再暗号化鍵の削除リクエストを送信
S44
メンバの再暗号化鍵を削除
S45
メンバの再暗号化鍵を削除した旨を返信
S46
挿入処理が終わる
S47
メンバ削除
S48
メンバを削除した旨を返信
終了

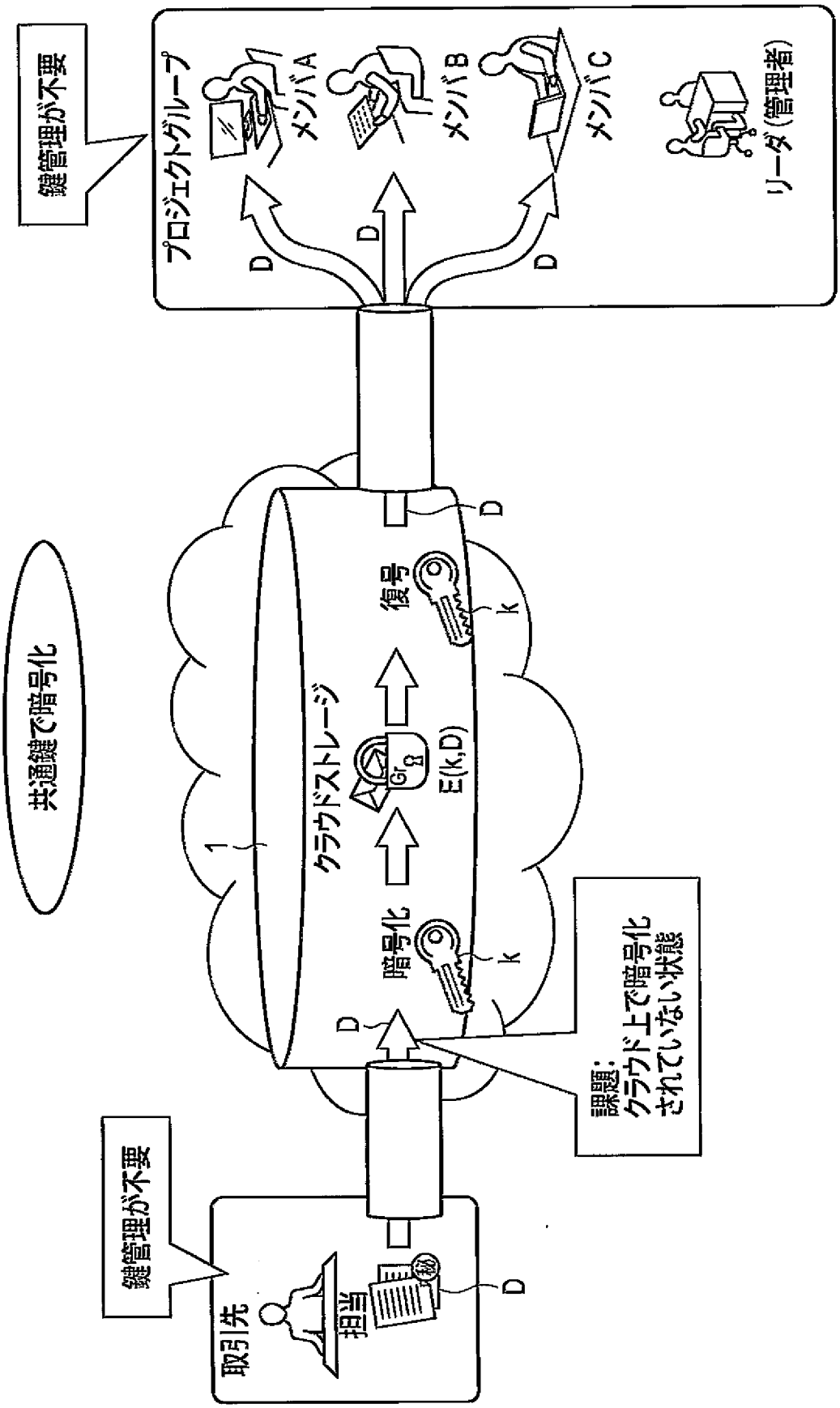
[図11]


10
ファイル共有装置
他の各部
挿入処理部
13
20
クライアント装置
30
再暗号化装置
ST41
メンバ削除要求
ST42
呼出し
ST43
再暗号化鍵削除要求
ST44
再暗号化鍵を削除
ST45
再暗号化鍵削除完了
ST46
挿入処理終了
メンバ削除
ST47
ST48
メンバ削除完了

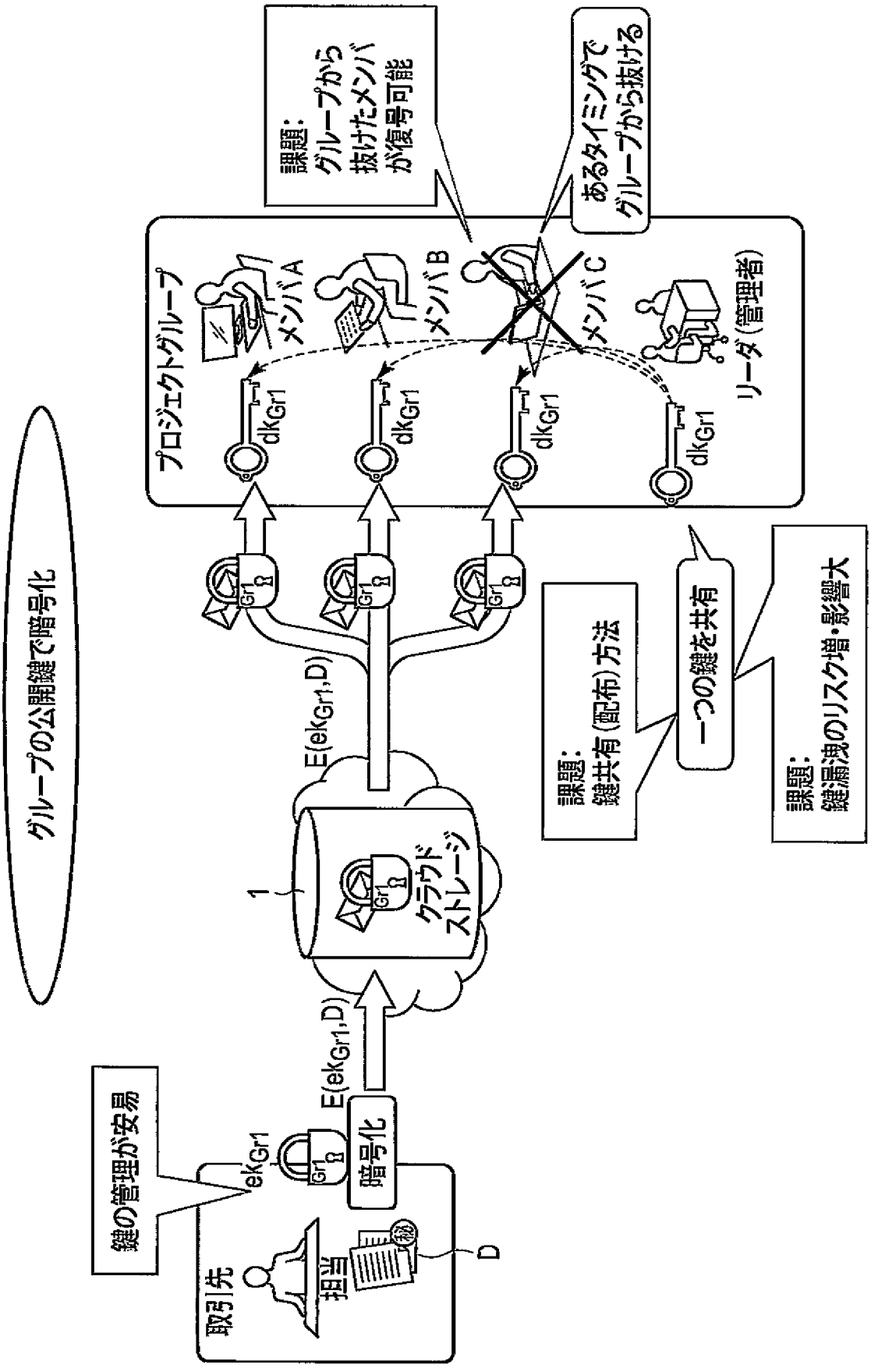
[図12]


課題:
データ保護はサーバの信頼性に依存
設定ミス、内部犯行、バグ...の危険
取引先
担当
D
秘
D
秘
クラウドストレージ
通信路暗号化
1

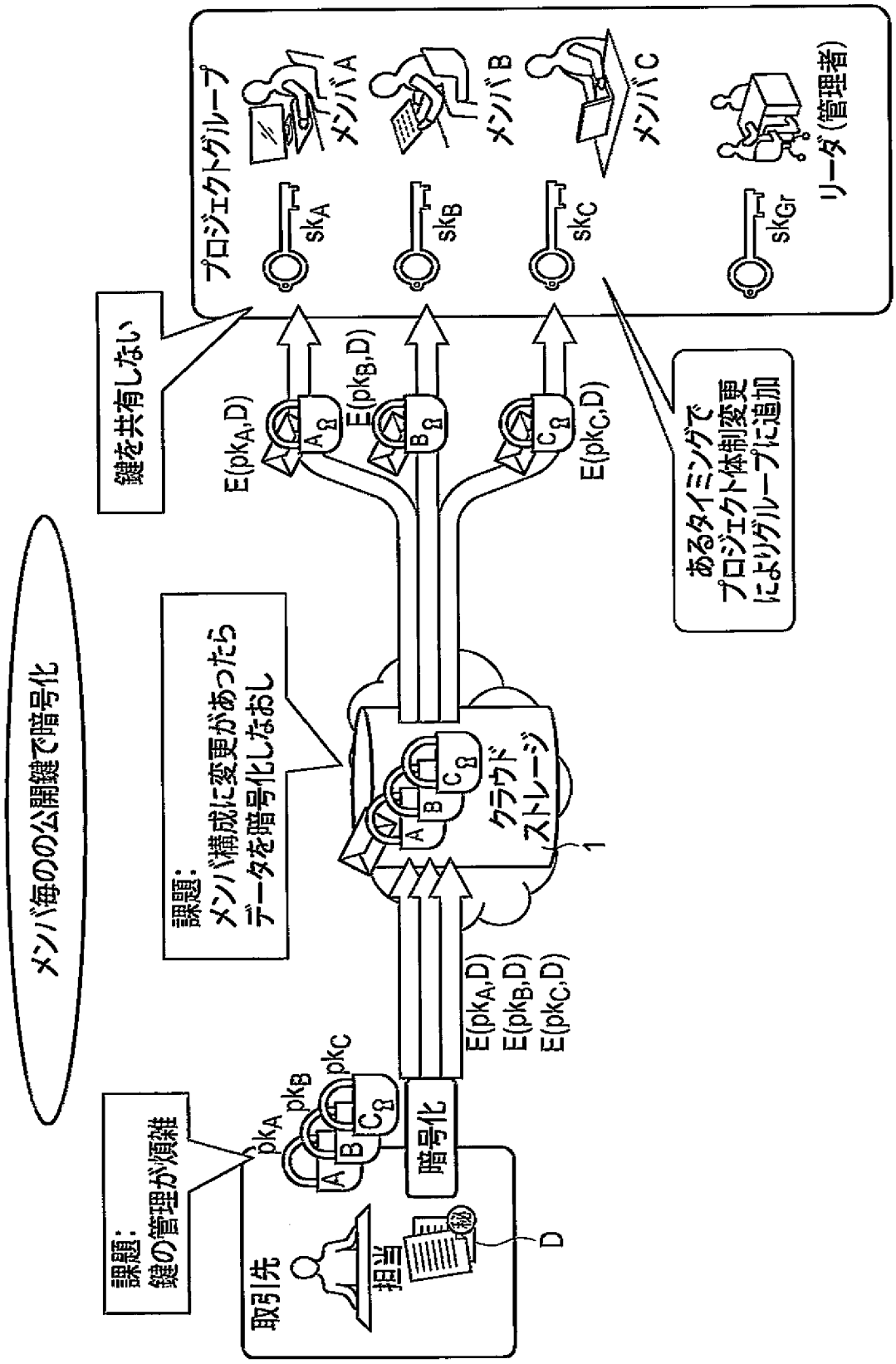
[図13]


鍵管理が不要
プロジェクトグループ
メンバA
メンバB
メンバC
リーダ(管理者)
D
D
D
共通鍵で暗号化
1
クラウドストレージ
暗号化
復号
E(k,D)
k
k
D
D
課題:
クラウド上で暗号化
されていない状態
鍵管理が不要
取引先
担当
秘
D

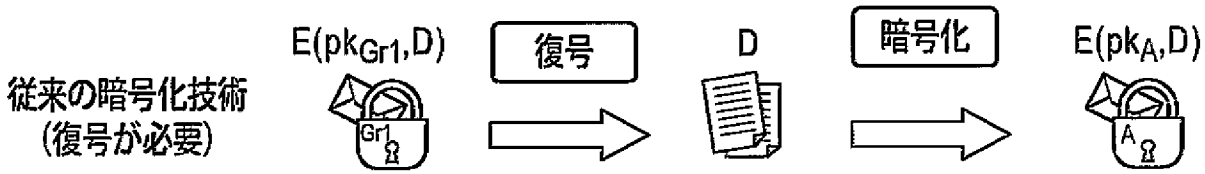
[図14]


グループの公開鍵で暗号化
プロジェクトグループ
メンバA
メンバB
メンバC
リーダ(管理者)
課題:
グループから
抜けたメンバ
が復号可能
あるタイミングで
グループから抜ける
一つの鍵を共有
課題:
鍵共有(配布)方法
課題:
鍵漏洩のリスク増・影響大
クラウド
ストレージ
1
E(ekGr1,D)
E(ekGr1,D)
暗号化
鍵の管理が安易
取引先
担当
秘
D

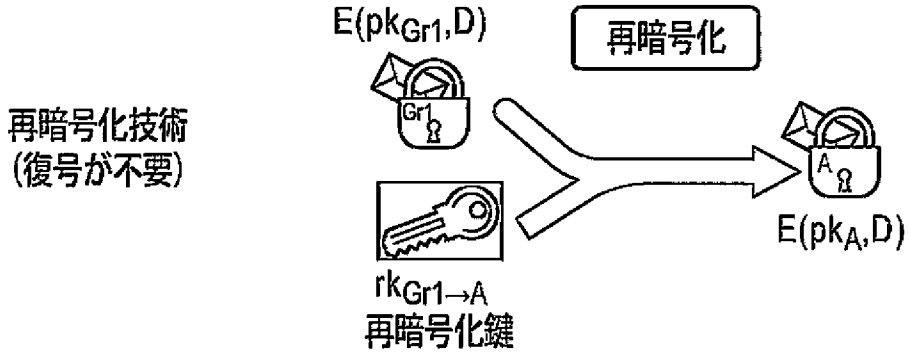
[図15]


プロジェクトグループ
メンバA
メンバB
メンバC
リーダ(管理者)
sk_A
sk_B
sk_C
sk_{Gr}
鍵を共有しない
$E(pk_A,D)$
$E(pk_B,D)$
$E(pk_C,D)$
あるタイミングで
プロジェクト体制変更
によりグループに追加
メンバ毎の公開鍵で暗号化
課題:
メンバ構成に変更があったら
データを暗号化しなおし
クラウド
ストレージ
1
課題:
鍵の管理が煩雑
pk_A
pk_B
pk_C
暗号化
取引先
担当
D

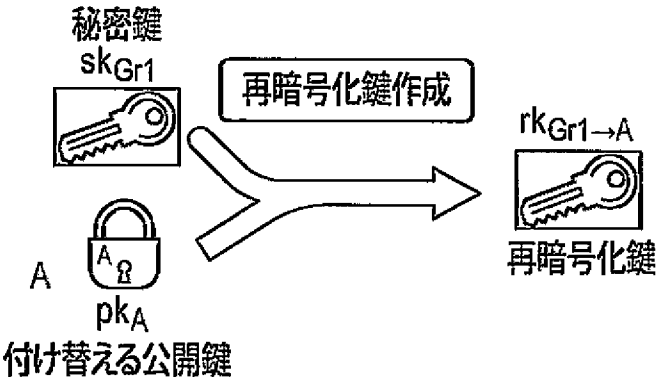
[図16A]


従来の暗号化技術
(復号が必要)
$E(pk_{Gr1},D)$
復号
D
暗号化
$E(pk_A,D)$

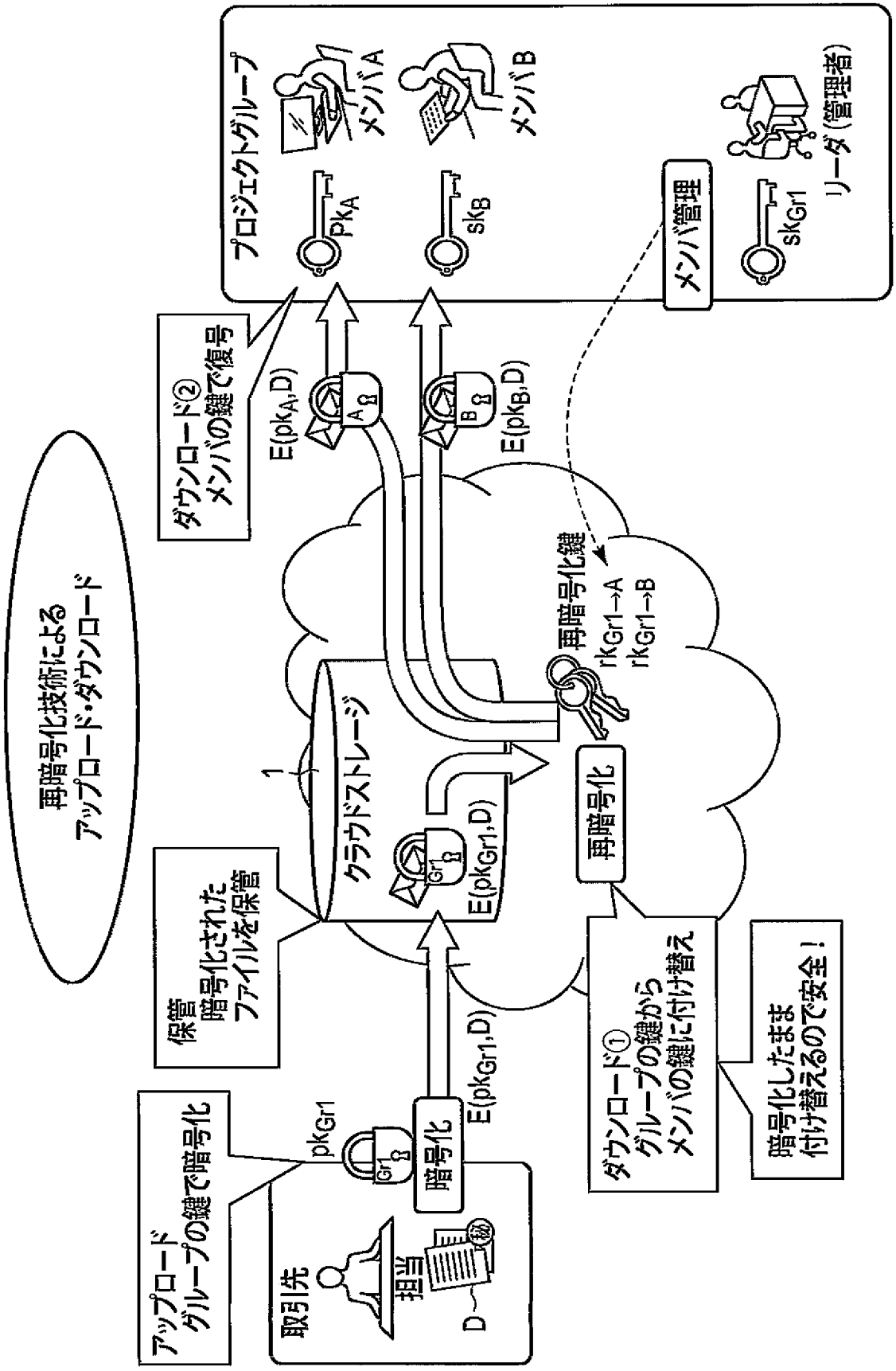
[図16B]


再暗号化技術
(復号が不要)
E(pkGr1,D)
Gr1
再暗号化
A
E(pkA,D)
rkGr1→A
再暗号化鍵

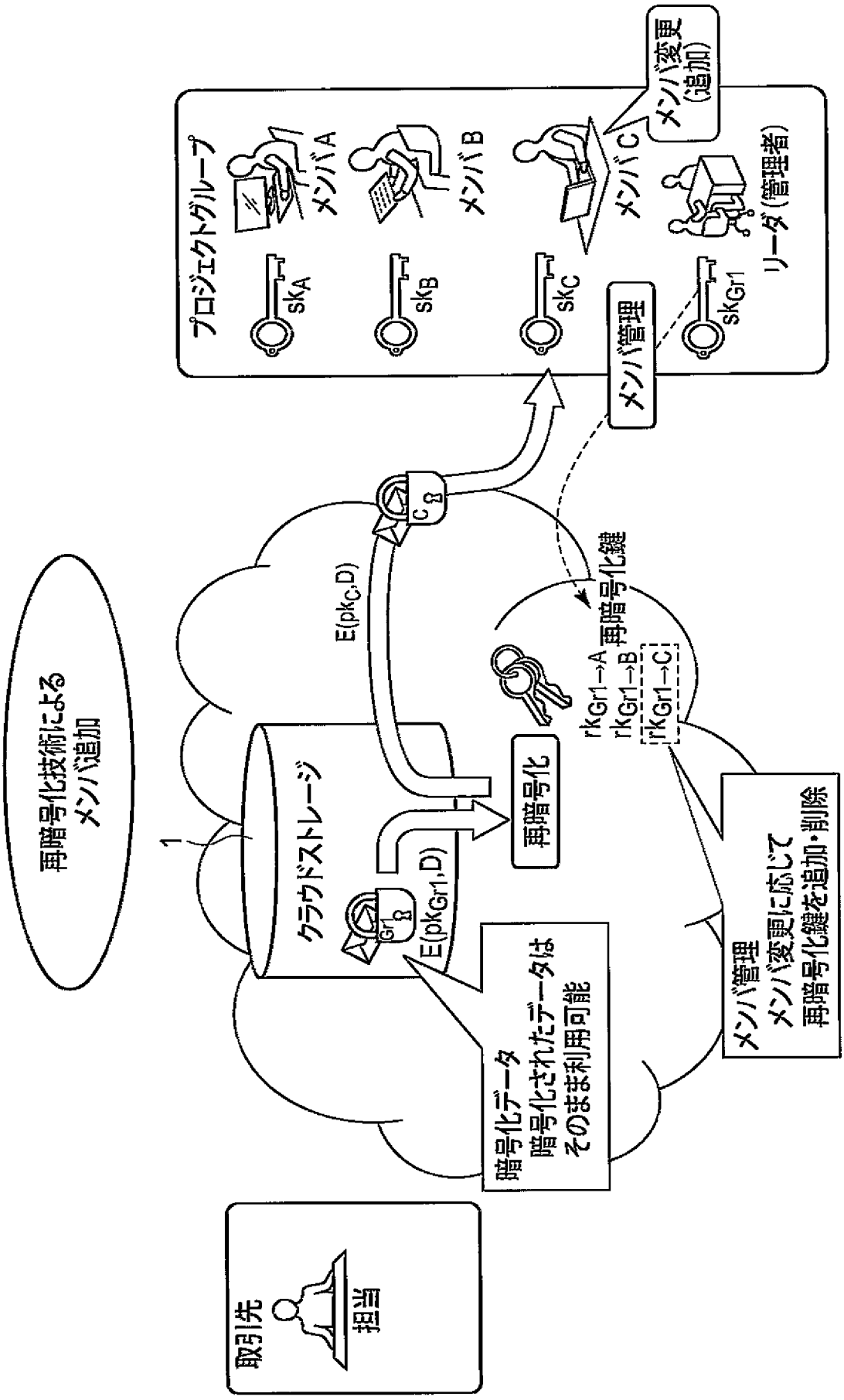
[図17]


秘密鍵
skGr1
再暗号化鍵作成
rkGr1→A
再暗号化鍵
A
pkA
付け替える公開鍵

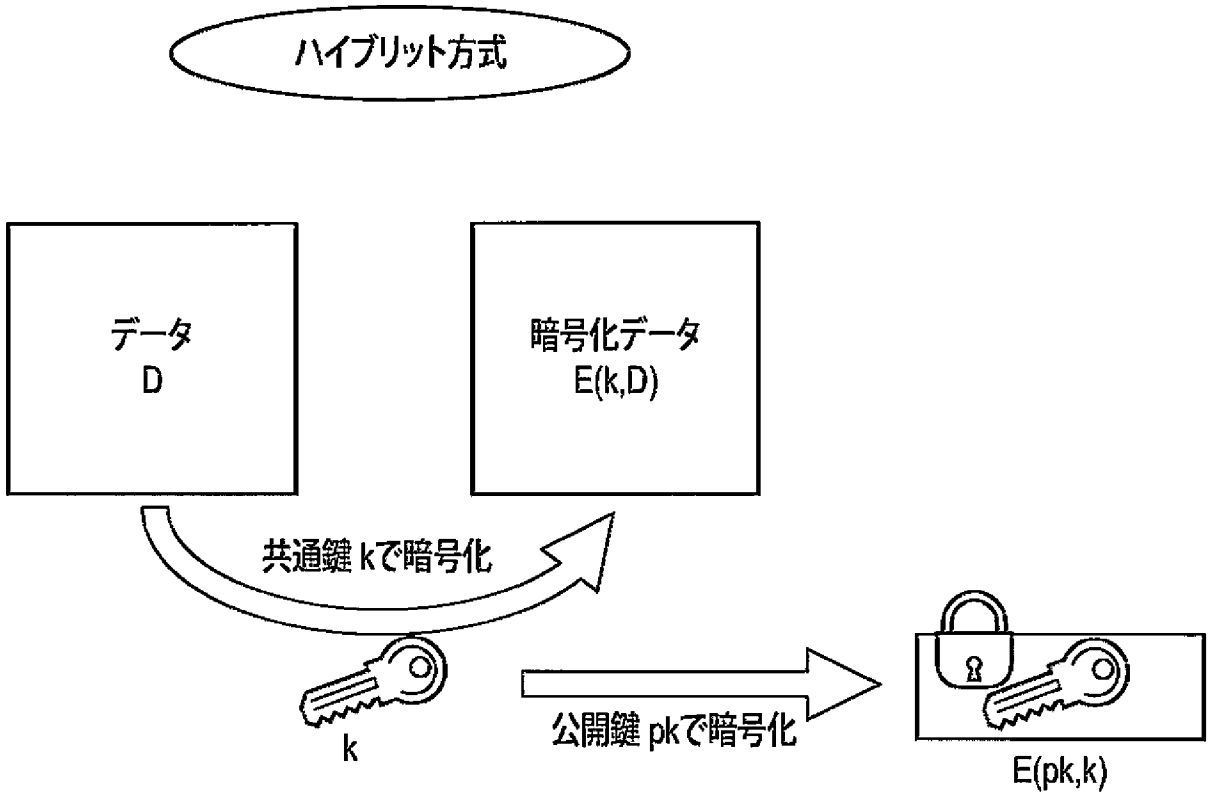
[図18]


再暗号化技術による
アップロード・ダウンロード
プロジェクトグループ
メンバA
メンバB
リーダ(管理者)
メンバ管理
ダウンロード②
メンバの鍵で復号
E(pkA,D)
E(pkB,D)
再暗号化鍵
rkGr1→A
rkGr1→B
クラウドストレージ
1
保管
暗号化された
ファイルを保管
E(pkGr1,D)
再暗号化
アップロード
グループの鍵で暗号化
pkGr1
暗号化
E(pkGr1,D)
取引先
担当
D
ダウンロード①
グループの鍵から
メンバの鍵に付け替え
暗号化したまま
付け替えるので安全！

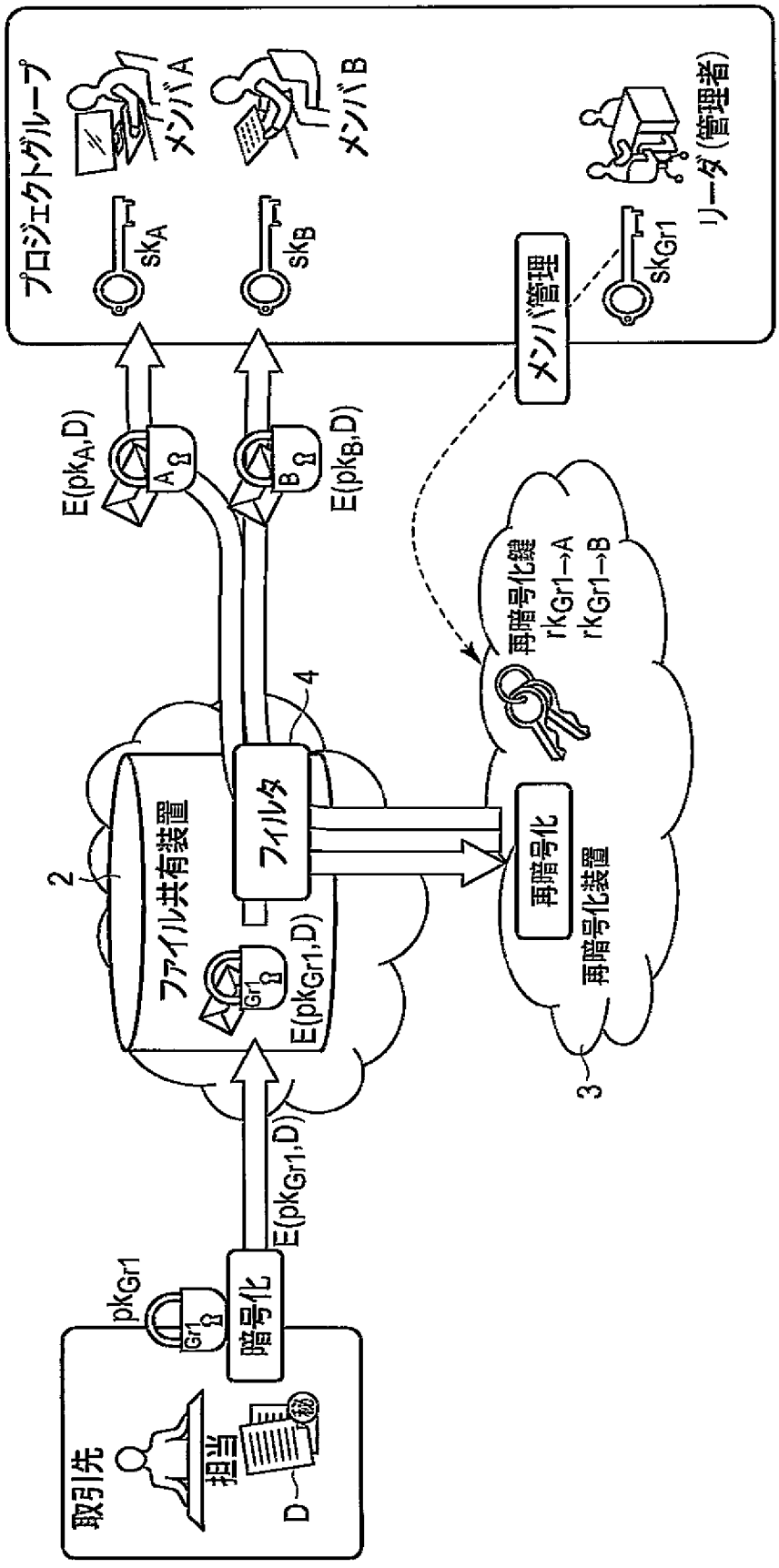
[図19]


再暗号化技術による
メンバ追加
1
クラウドストレージ
E(pkGr1,D)
E(pkC,D)
再暗号化
rkGr1→A 再暗号化鍵
rkGr1→B
rkGr1→C
暗号化データ
暗号化されたデータは
そのまま利用可能
メンバ管理
メンバ変更に応じて
再暗号化鍵を追加・削除
取引先
担当
プロジェクトグループ
メンバA
メンバB
メンバC
メンバ変更
(追加)
リーダ(管理者)
skA
skB
skC
skGr1
メンバ管理

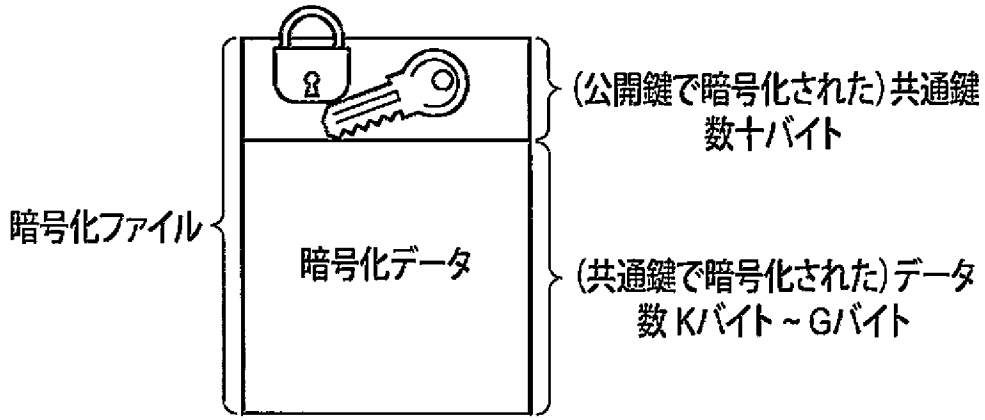
[図20]



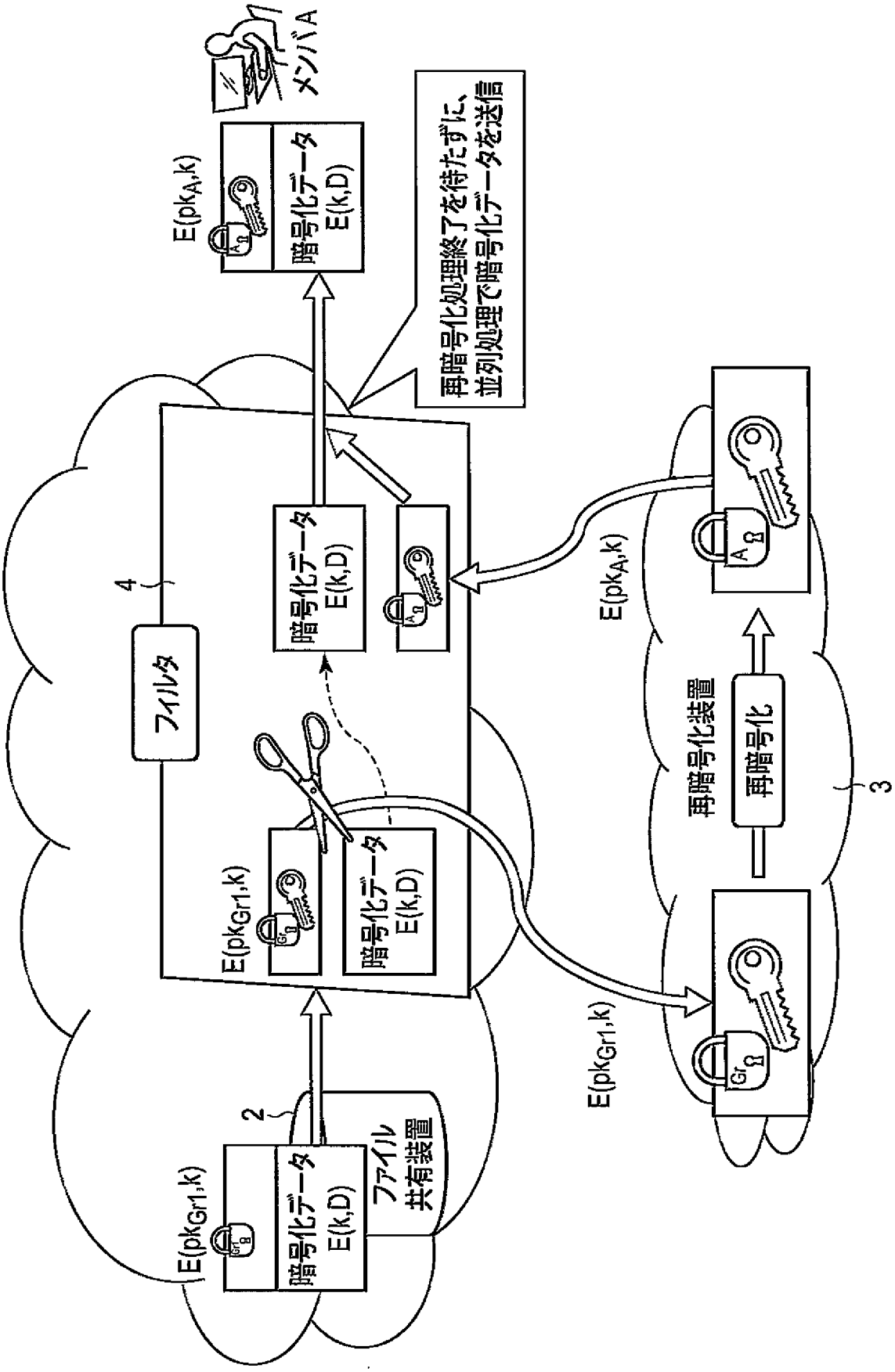
[図21]


プロジェクトグループ
メンバA
メンバB
リーダ(管理者)
sk_A
sk_B
sk_{Gr1}
メンバ管理
$E(pk_A,D)$
$E(pk_B,D)$
再暗号化鍵
$rk_{Gr1\to A}$
$rk_{Gr1\to B}$
4
2
ファイル共有装置
フィルタ
再暗号化
再暗号化装置
3
$E(pk_{Gr1},D)$
pk_{Gr1}
暗号化
取引先
担当
D

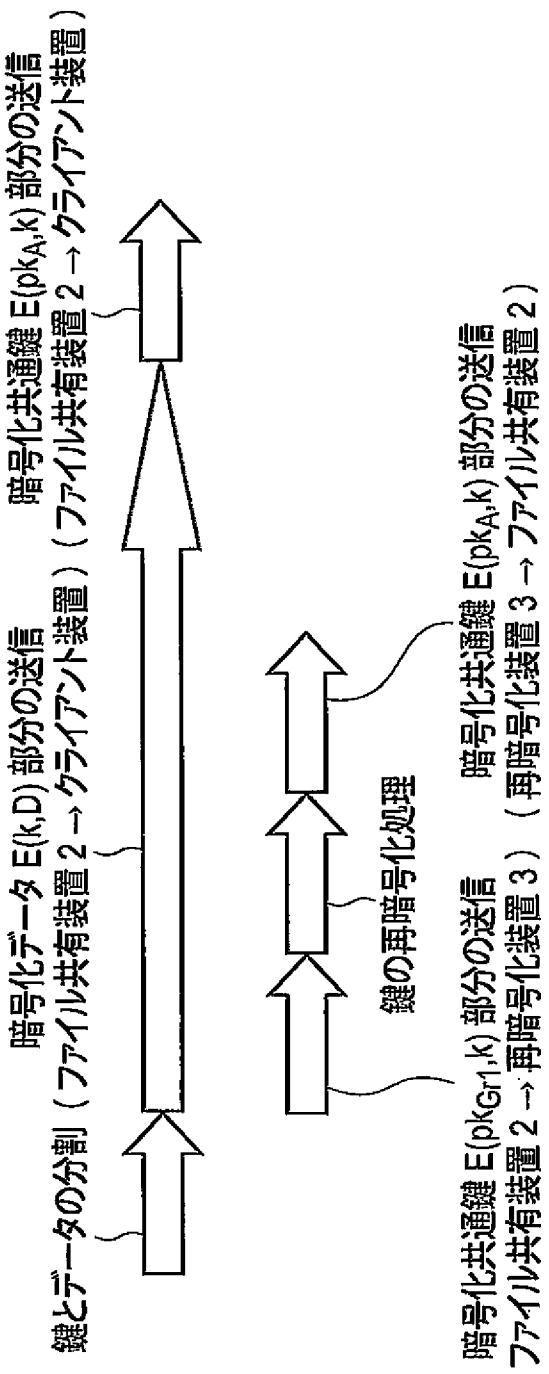
[図22]


暗号化ファイル
暗号化データ
(公開鍵で暗号化された)共通鍵
数十バイト
(共通鍵で暗号化された)データ
数Kバイト~Gバイト

[図23]


メンバA
E(pkA,k)
暗号化データ
E(k,D)
再暗号化処理終了を待たずに、
並列処理で暗号化データを送信
4
フィルタ
暗号化データ
E(k,D)
E(pkGr1,k)
暗号化データ
E(k,D)
E(pkA,k)
再暗号化装置
再暗号化
3
2
E(pkGr1,k)
暗号化データ
E(k,D)
ファイル
共有装置
E(pkGr1,k)

[図24]


暗号化データ E(k,D) 部分の送信
（ファイル共有装置 2 → クライアント装置）
暗号化共通鍵 E(pk$_A$,k) 部分の送信
（ファイル共有装置 2 → クライアント装置）
鍵とデータの分割
鍵の再暗号化処理
暗号化共通鍵 E(pk$_{Gr1}$,k) 部分の送信
（ファイル共有装置 2 → 再暗号化装置 3）
暗号化共通鍵 E(pk$_A$,k) 部分の送信
（再暗号化装置 3 → ファイル共有装置 2）

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/078028

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

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	Takuya YOSHIDA et al., "Proxy Re-encryption Scheme for Secure Data Sharing in Cloud Services", Toshiba Review, 01 November 2011 (01.11.2011), vol.66, no.11, pages 18 to 22	1-5
Y	JP 2007-80145 A (Ricoh Co., Ltd.), 29 March 2007 (29.03.2007), paragraphs [0019] to [0021]; fig. 1, 3 (Family: none)	1-5
P,A	Shingo ABE et al., "Proxy Sai Angoka Hoshiki o Riyo shita Anzen na Cloud Storage no Teian", 2012 Nen Symposium on Cryptography and Information Security Yokoshu CD-ROM, 30 January 2012 (30.01.2012), 2A1-5	1-5

☐ 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
26 November, 2012 (26.11.12)	04 December, 2012 (04.12.12)

Name and mailing address of the ISA/	Authorized officer
Japanese Patent Office	
Facsimile No.	Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０７８０２８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

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

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	吉田　琢也　他，クラウドサービス上でより安全なデータ共有を実現する再暗号化技術，東芝レビュー，2011.11.01，第６６巻　第１１号，p.18-22	１－５
Y	JP 2007-80145 A（株式会社リコー）2007.03.29，段落【００１９】－【００２１】，【図１】，【図３】（ファミリーなし）	１－５

☑　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
２６．１１．２０１２	０４．１２．２０１２

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
Ｐ，Ａ	阿部　真吾　他，プロキシ再暗号化方式を利用した安全なクラウドストレージの提案，2012 年 暗号と情報セキュリティシンポジウム予稿集　CD-ROM，2012.01.30，2A1-5	１－５