

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5454960号
(P5454960)

(45) 発行日 平成26年3月26日 (2014. 3. 26)

(24) 登録日 平成26年1月17日 (2014. 1. 17)

(51) Int. Cl. F I
HO4L 9/14 (2006.01) HO4L 9/00 641
GO9C 1/00 (2006.01) GO9C 1/00 660D

請求項の数 6 (全 29 頁)

(21) 出願番号	特願2011-245618 (P2011-245618)	(73) 特許権者	000003078
(22) 出願日	平成23年11月9日 (2011. 11. 9)		株式会社東芝
(65) 公開番号	特開2013-101260 (P2013-101260A)		東京都港区芝浦一丁目1番1号
(43) 公開日	平成25年5月23日 (2013. 5. 23)	(73) 特許権者	301063496
審査請求日	平成24年3月30日 (2012. 3. 30)		東芝ソリューション株式会社
			東京都港区芝浦一丁目1番1号
		(74) 代理人	100108855
			弁理士 蔵田 昌俊
		(74) 代理人	100159651
			弁理士 高倉 成男
		(74) 代理人	100088683
			弁理士 中村 誠
		(74) 代理人	100109830
			弁理士 福原 淑弘

最終頁に続く

(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

(57) 【特許請求の範囲】

【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暗号化データ送信処理と並行して、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前記暗号化データ送信処理に並行して受けると、当該暗号化データ送信処理の後に当該第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とを備え、

10

20

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と

10

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、前記データを得ることを特徴とする再暗号化システム。

【請求項2】

請求項1に記載の再暗号化システムにおいて、

前記ファイル共有装置における前記暗号化ファイルを取得する手段、前記分離する手段、前記再暗号化要求を前記再暗号化装置に送信する手段、及び前記第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は、所定の処理を追加するフィルタ機能を用いて構成されていることを特徴とする再暗号化システム。

20

【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に通信可能なファイル共有装置であって、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を含む暗号化ファイルをファイル記憶手段に記憶し、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ファイル記憶手段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暗号化データ送信処理と並行して、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再暗号化装置に送信し、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前記暗号化データ送信処理に並行して受けると、当該暗号化データ送信処理の後に当該第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、

30

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と

40

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、前記データを得ることを特徴とする再暗号化装置。

50

【請求項 4】

請求項 3 に記載の再暗号化装置において、

前記ファイル共有装置における、前記暗号化ファイルを取得し、前記分離し、前記暗号化データ部分を前記クライアント装置に送信し、前記再暗号化要求を前記再暗号化装置に送信し、前記第 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処理は、所定の処理を追加するフィルタ機能を用いて行われることを特徴とする再暗号化装置。

【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に通信可能なファイル共有装置であって、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ファイル記憶手段に記憶し、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ファイル記憶手段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暗号化データ送信処理と並行して、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再暗号化装置に送信し、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前記暗号化データ送信処理に並行して受けると、当該暗号化データ送信処理の後に当該第 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に用いられるプログラムであって、

前記再暗号化鍵装置を、

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再暗号化鍵記憶手段に書込む手段、

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、

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、

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、

として機能させ、

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、前記データを得るようにしたことを特徴とするプログラム。

【請求項 6】

請求項 5 に記載のプログラムにおいて、

前記ファイル共有装置における、前記暗号化ファイルを取得し、前記分離し、前記暗号化データ部分を前記クライアント装置に送信し、前記再暗号化要求を前記再暗号化装置に送信し、前記第 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処理は、所定の処理を追加するフィルタ機能を用いて行われることを特徴とするプログラム。

【発明の詳細な説明】

【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

10

20

30

40

50

イング（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。特にパブリッククラウドについては、セキュリティの不安感からクラウドの利用に踏み切れない企業が多い。

【0003】

その反面、複数のメンバからなるグループが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く、このニーズはクラウドの用途の上位にも上げられている。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を利用して、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ダウンロードして利用することになる。

10

【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は暗号化されていない。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、全てクラウドサービスの信頼性に依存してしまう。例えばクラウドストレージ1は多くの企業・ユーザに利用されているが、設定ミスにより他テナントのデータが見えてしまう心配や、認証処理が適切に行われない心配がある。また、サーバ管理者による内部犯行により、預けているデータが漏えいしてしまう心配もある。

【0006】

20

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っている。

【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】

30

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、どちらの方法(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のトレードオフとなる。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 $e_{k_{Gr1}}$ /復号化鍵 $d_{k_{Gr1}}$ を共有し、公開鍵暗号を用いて暗号化する場合、暗号化鍵 $e_{k_{Gr1}}$ /復号鍵 $d_{k_{Gr1}}$ は1つの組なので、アップロードするメンバ、ダウンロードするメンバともに管理は容易であり、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。

40

【0010】

上記(i)の方法のデメリットとしては、復号鍵 $d_{k_{Gr1}}$ をメンバ間で共有する必要がある点と、復号鍵 $d_{k_{Gr1}}$ 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 $d_{k_{Gr1}}$ を共有することから、メンバが増加するほど復号鍵 $d_{k_{Gr1}}$ の漏洩リスクが増えてしまう。仮に復号鍵 $d_{k_{Gr1}}$ を漏えいした場合、漏洩した復号鍵 $d_{k_{Gr1}}$ の利用を防ぐ趣旨で、グループで共有する復号鍵 $d_{k_{Gr1}}$ 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

50

による復号を防ぐ趣旨で、他のメンバの復号鍵 $d k_{Gr1}$ を更新する必要性が生じるため、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。

【 0 0 1 1 】

このように、上記 (i) のグループで鍵を共有する方法においては、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。

【 0 0 1 2 】

(i i) メンバそれぞれの鍵で暗号化する方法

上記 (i i) 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 1 5 に示すように、メンバ A , ... 毎に公開鍵 $p k_A$ / 秘密鍵 $s k_A$, ... 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 $E (p k_A , D)$, ... 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 $s k_A$, ... 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 $s k_I$ を漏えいさせたとしても、他のメンバが秘密鍵 $s k_I$ を更新する必要はない。

【 0 0 1 3 】

上記 (i i) 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 $p k_A$, ... 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 $p k_H$ でデータ D を暗号しなおす必要がある点が挙げられる。例えば、データ D を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 $p k_H$ でデータ D を暗号化してクラウドストレージ 1 に保管する必要性が生じるため、利便性を低下させてしまう。

【 0 0 1 4 】

このように従来暗号化技術では、利便性とセキュリティが二律背反の関係にある。

【 0 0 1 5 】

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 J a v a (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】

【 0 0 1 6 】

【特許文献 1】特許第 4 0 6 1 2 8 8 号公報

【非特許文献】

【 0 0 1 7 】

【非特許文献 1】ハイブリッド暗号方式 - - - 共通鍵暗号と公開鍵暗号を組み合わせる - 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/servlet/jsp/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】

【 0 0 1 8 】

以上説明したように、従来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。

【 0 0 1 9 】

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。

10

【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。

20

【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。

30

【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。

40

【図面の簡単な説明】

【0032】

【図1】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】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】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】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】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】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

50

トである。

【図 7】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】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】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】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】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】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】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。

10

【図 14】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】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 16】一般的な再暗号化技術を従来の暗号化技術と比較して示す模式図である。

【図 17】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】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】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】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。

20

【図 21】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】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】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】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。

30

【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】

再暗号化とは、図 16 (a) 及び図 16 (b) に従来の暗号化技術と比較して示すように、あるメンバの公開鍵 $p k_{Gr1}$ で暗号化したデータ $E(p k_{Gr1}, D)$ を、復号することなく、別のメンバ A の公開鍵 $p k_A$ で暗号化したデータ $E(p k_A, D)$ に変換できる、つまり鍵を付け替えることができる技術である。

【0036】

40

このような再暗号化処理を行うには再暗号化鍵 $r k_{Gr1_A}$ が必要である。再暗号化鍵 $r k_{Gr1_A}$ は、図 17 に示すように、付け替える前の秘密鍵 $s k_{Gr1}$ と、付け替える後の公開鍵 $p k_A$ から作成される。再暗号化鍵 $r k_{Gr1_A}$ 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】

すなわち、アップロードするメンバは、グループの公開鍵 $p k_{Gr1}$ でデータ D を暗号化し、暗号化データ $E(p k_{Gr1}, D)$ をクラウドストレージ 1 に保管する。これにより、グループ内の各メンバの鍵管理が不要になった。

50

【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 ($p k_{Gr1}, D$)を当該メンバA向けの再暗号化鍵 $r k_{Gr1_A}$ により再暗号化し、得られた再暗号化データE ($p k_A, D$)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 $s k_A, \dots$ を共有する必要がない。

10

【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 $r k_{Gr1_A}, \dots$ 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 $p k_C$ を取得する。グループ管理者は、グループの秘密鍵 $s k_{Gr1}$ と取得した公開鍵 $p k_C$ から再暗号化鍵 $r k_{Gr1_C}$ を作成し、作成した再暗号化鍵 $r k_{Gr1_C}$ 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 ($p k_{Gr1}, D$)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としては、特に見当たらない。

20

【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 $p k$ で暗号化して暗号化鍵E ($p k, k$)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。

30

【0045】

なお、ハイブリッド方式を使用するか否かは別にして、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。

40

【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と呼んでいたものに相当する装置)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

50

装置 3 と連携する処理（例、フィルタ 4）のみである。

【 0 0 5 0 】

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。

【 0 0 5 1 】

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 $E(p k_{Gr1}, D)$ を再暗号化するため、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。

10

【 0 0 5 2 】

そこで、図 2 2 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 2 1 に示した暗号化データ $E(p k_{Gr1}, D)$ に代えて、図 2 3 に示すように、（公開鍵 $p k_{Gr1}$ で暗号化された）共通鍵 k からなる暗号化共通鍵 $E(p k_{Gr1}, k)$ 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 $E(p k_{Gr1}, k)$ 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 $E(p k_{Gr1}, k)$ 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。

20

【 0 0 5 3 】

また、図 2 4 に示すように、再暗号化装置 3 に暗号化共通鍵 $E(p k_{Gr1}, k)$ 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。

【 0 0 5 4 】

以上のように、データの配布処理を改善した形態は、図 2 2 乃至図 2 4 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 $E(p k_{Gr1}, k)$ 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 2 1 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。

30

【 0 0 5 5 】

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。

【 0 0 5 6 】

< 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 2 0 に通信可能なファイル共有装置 1 0 及び再暗号化装置 3 0 を備えている。なお、ファイル共有装置 1 0 及び再暗号化装置 3 0 はサーバ装置であり、各装置 1 0, 2 0, 3 0 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 1 0, 2 0, 3 0 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、予めネットワーク又は記憶媒体から対応する装置のコンピュータにインストールされ、対応する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。

40

50

【 0 0 5 7 】

ここで、ファイル共有装置 1 0 は、制御部 1 1、通信部 1 2、挿入処理部 1 3、ファイル共有部 1 4、ファイル記憶部 1 5、グループ情報記憶部 1 6、公開鍵取得部 1 7、再暗号化鍵登録部 1 8 及びグループ管理部 1 9 を備えている。

【 0 0 5 8 】

制御部 1 1、通信部 1 2、挿入処理部 1 3、ファイル共有部 1 4、公開鍵取得部 1 7、再暗号化鍵登録部 1 8 及びグループ管理部 1 9 は、例えば図示しない C P U が、後述するファイル共有装置 1 0 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 1 2 は、他の装置 2 0、3 0 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 2 0、3 0 との間のデータの送受信に通信部 1 2 を介する旨の記載を省略している。

10

【 0 0 5 9 】

また、例えば再暗号化装置 3 0 に連携する挿入処理部 1 3、公開鍵取得部 1 7 及び再暗号化鍵登録部 1 8 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、J a v a のフィルタ機能を利用して実現してもよい。

【 0 0 6 0 】

ファイル記憶部 1 5 は、図示しない C P U 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。

20

【 0 0 6 1 】

グループ情報記憶部 1 6 は、図示しない C P U 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 I D と、当該グループに属するメンバを識別するメンバ I D とを関連付けて記憶する。

【 0 0 6 2 】

一方、クライアント装置 2 0 は、制御部 2 1、通信部 2 2、ファイル記憶部 2 3、秘密鍵記憶部 2 4、暗号処理部 2 5、共通鍵生成部 2 6 及び再暗号化鍵作成部 2 7 を備えている。

30

【 0 0 6 3 】

制御部 2 1、通信部 2 2、暗号処理部 2 5、共通鍵生成部 2 6 及び再暗号化鍵作成部 2 7 は、例えば図示しない C P U が、後述するクライアント装置 2 0 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 2 2 は、他の装置 1 0、3 0 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 1 0、3 0 との間のデータの送受信に通信部 2 2 を介する旨の記載を省略している。

【 0 0 6 4 】

ファイル記憶部 2 3 は、図示しない C P U 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。

40

【 0 0 6 5 】

秘密鍵記憶部 2 4 は、図示しない C P U 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 2 4 は、更に、グループの公開鍵に対応する秘密鍵を記憶する。

【 0 0 6 6 】

他方、再暗号化装置 3 0 は、制御部 3 1、通信部 3 2、再暗号化処理部 3 3、公開鍵記憶部 3 4 及び再暗号化鍵記憶部 3 5 を備えている。

【 0 0 6 7 】

制御部 3 1、通信部 3 2 及び再暗号化処理部 3 3 は、例えば図示しない C P U が、後述

50

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】

10

20

30

40

50

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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ で暗号化し、得られた第 1 暗号化共通鍵部分 ($E(p k_{Gr1}, k)$) を制御部 21 に渡す (ST5)。

10

【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 ($E(p k_{Gr1}, k)$) 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)。

20

【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。

30

【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。

40

【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】

50

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] (ST 12 - 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 ($E(p k_{Gr1}, k)$) と暗号化データ部分 ($E(k, D)$) に分離する (ST 13)。

【 0096 】

ステップ ST 14 ' 及び ST 14 は、並列に実行される。ステップ ST 14 ' では、以下のステップ ST 14 ' - 1 ~ ST 14 ' - 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 ST 14 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 (ST 14 ' - 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 (ST 14 ' - 2)。

【 0099 】

ステップ ST 14 では、以下のステップ ST 14 - 1 ~ ST 14 - 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 ($E(p k_{Gr1}, k)$) 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 (ST 14 - 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 $r k_{Gr1_A}$ を取得し、当該取得した再暗号化鍵 $r k_{Gr1_A}$ に基づいて、再暗号化要求内の第 1 暗号化共通鍵部分 ($E(p k_{Gr1}, k)$) を第 2 暗号化共通鍵部分 ($E(p k_A, k)$) 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 ($E(p k_{Gr1}, k)$) 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 $r k_{Gr1_A}$ を取得し、第 1 暗号化共通鍵部分 ($E(p k_{Gr1}, k)$) を第 2 暗号化共通鍵部分 ($E(p k_A, k)$) に再暗号化し、得られた第 2 暗号化共通鍵部分 ($E(p k_A, k)$) を制御部 31 に渡す (ST 14 - 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 ($E(p k_A, k)$) をファイル共有装置 10 に送信する (ST 14 - 3)。

【 0104 】

ファイル共有装置 10 では、挿入処理部 13 が、ステップ ST 14 ' - 2 の送信処理が終わっていないならば終わるまで待って、制御部 11 に第 2 暗号化共通鍵部分 ($E(p k_A, k)$) を渡す。ステップ ST 14 ' - 2 の送信処理が終わってればすぐ渡す (ST 14 - 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 ($E(p k_A, k)$) をクライアント装置 20 に送信する [挿入した処理の終了] (ST 14 - 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 ST 14 - 5 とステップ ST 14 ' - 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。

10

20

30

40

50

【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($E(p k_A, k)$)をメンバの公開鍵 $p k_A$ に対応する秘密鍵 $s k_A$ 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 $s k_A$ を取得し、秘密鍵 $s k_A$ と第2暗号化共通鍵部分($E(p k_A, k)$)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($E(p k_A, k)$)を秘密鍵 $s k_A$ で復号し、得られた共通鍵 k を制御部21に渡す(ST15)。

10

【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。

20

【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 $p k_C$ を要求する(ST23)。

30

【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 $p k_C$ 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 $p k_C$ 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 $p k_C$ 及びメンバID(C)も渡す)[挿入した処理の終了](ST26)。

40

【0118】

ファイル共有装置10では、制御部11が、メンバの公開鍵 $p k_C$ 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 $s k_{G1}$ を読み込む(ST28)。

【0121】

50

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_C} を作成し、メンバの再暗号化鍵 rk_{Gr1_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_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_C} 及びメンバ ID (C) とグループ ID (Gr1) を渡す (ST31)。

10

【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_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_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_C} を登録した旨をファイル共有装置 10 に通知する (ST34)。

20

【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。

30

【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_C} を登録した旨を制御部 11 に通知する (ST38)。

40

【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_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】

50

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 $r_{k_{Gr1}}_C$ 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 $r_{k_{Gr1}}_C$ 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

10

20

30

40

50

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、再暗号化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。

10

【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、クライアント端末で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。

20

【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。

30

【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。

40

【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

50

、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)~(f10-1)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($rk_{Gr1_A}, rk_{Gr1_B}, \dots$)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

10

20

30

40

50

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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ 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 $p k_{Gr1}$ で暗号化し、得られた第1暗号化ファイル $E(p k_{Gr1}, D)$ 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 $E(p k_{Gr1}, D)$ 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 $E(p k_{Gr1}, D)$ 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 $E(p k_{Gr1}, D)$ 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。

10

20

30

40

50

【 0 1 8 3 】

続いて、ファイルダウンロードの処理の流れを説明する。

【 0 1 8 4 】

クライアント装置 2 0 では、制御部 2 1 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 1 0 に送信する。

【 0 1 8 5 】

ファイル共有装置 1 0 では、制御部 1 1 が、ファイル要求をクライアント装置 2 0 から受けると、ファイル共有部 1 4 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 1 5 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 1 1 は、クライアント装置 2 0 から受けたファイル要求をファイル共有部 1 4 に送出する。ファイル共有部 1 4 は、ファイル記憶部 1 5 から第 1 暗号化ファイル E (pk_{Gr1}, D) を取得し、制御部 1 1 に渡す。

10

【 0 1 8 6 】

ファイル共有装置 1 0 では、制御部 1 1 が、取得した第 1 暗号化ファイル E (pk_{Gr1}, D) を挿入処理部 1 3 に渡す [処理の挿入]。

【 0 1 8 7 】

ファイル共有装置 1 0 では、処理挿入部 1 3 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 3 0 に送信する。

20

【 0 1 8 8 】

再暗号化装置 3 0 では、再暗号化要求をファイル共有装置 1 0 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 3 5 から再暗号化鍵 rk_{Gr1_A} を取得し、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。

【 0 1 8 9 】

具体的には、制御部 3 1 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 3 3 に渡す。再暗号化処理部 3 3 は、このメンバ ID に基づいて再暗号化鍵記憶部 3 4 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 3 1 に渡す。

30

【 0 1 9 0 】

再暗号化装置 3 0 では、制御部 3 1 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 1 0 に送信する。

【 0 1 9 1 】

ファイル共有装置 1 0 では、挿入処理部 1 3 が、制御部 1 1 に第 2 暗号化ファイル E (pk_A, D) を渡す。

【 0 1 9 2 】

ファイル共有装置 1 0 では、制御部 1 1 が、第 2 暗号化ファイル E (pk_A, D) をクライアント装置 2 0 に送信する [挿入した処理の終了]。

40

【 0 1 9 3 】

クライアント装置 2 0 は、ファイル共有装置 1 0 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。

【 0 1 9 4 】

具体的には、クライアント装置 2 0 では、制御部 2 1 が、秘密鍵記憶部 2 4 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 2 5 に渡す。暗号処理部 2 5 は、第 2 暗号化ファイル E (pk_A, D) を秘密鍵 sk_A で復号し、

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

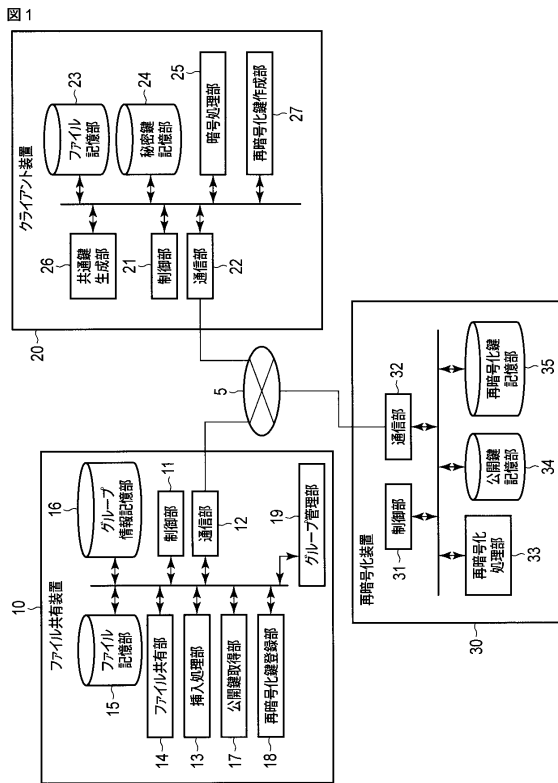
まれる。

【符号の説明】

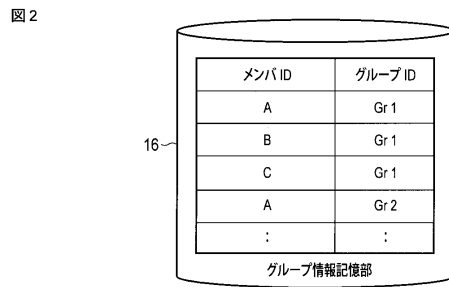
【0206】

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

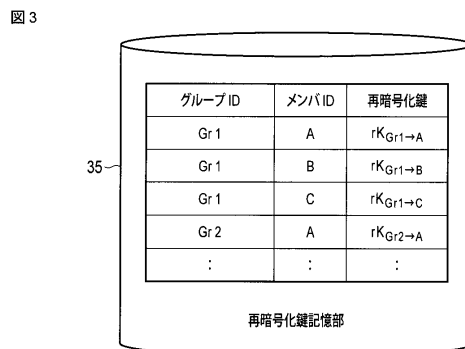
【図1】



【図2】

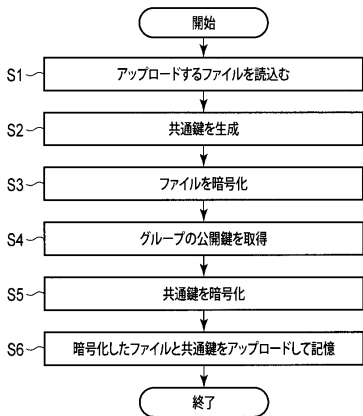


【図3】



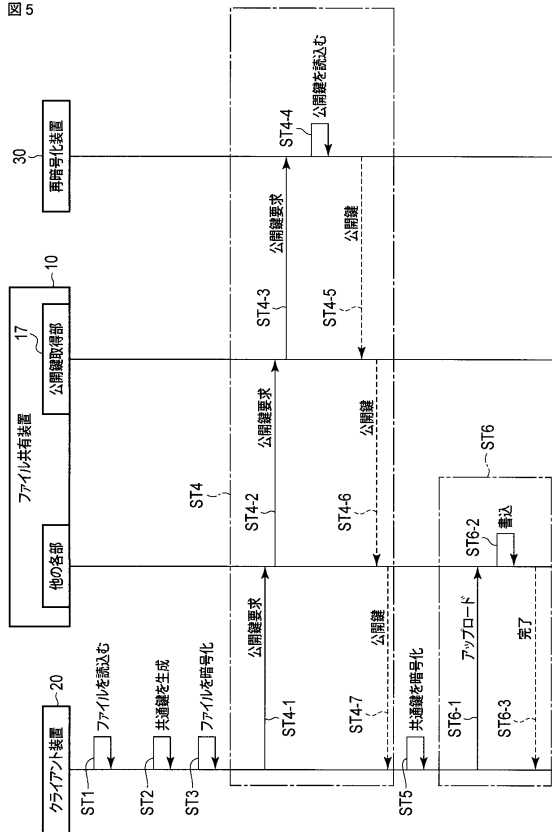
【 図 4 】

図 4



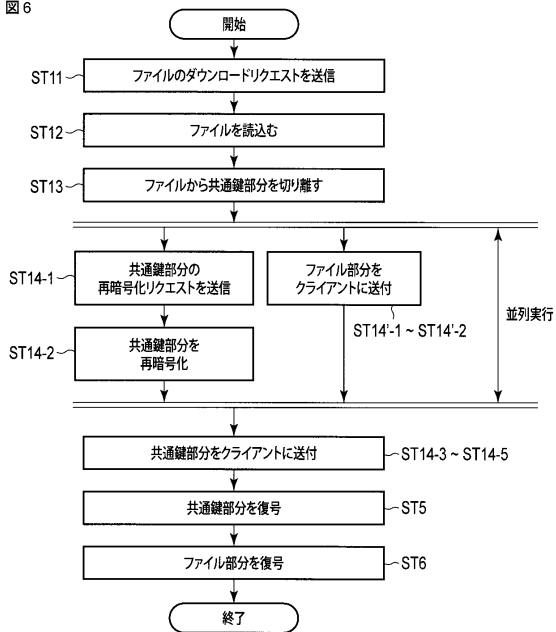
【 図 5 】

図 5



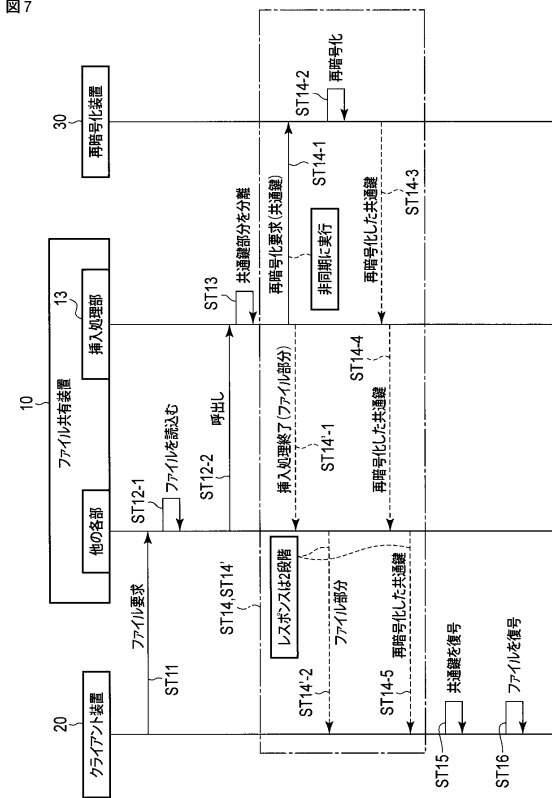
【 図 6 】

図 6

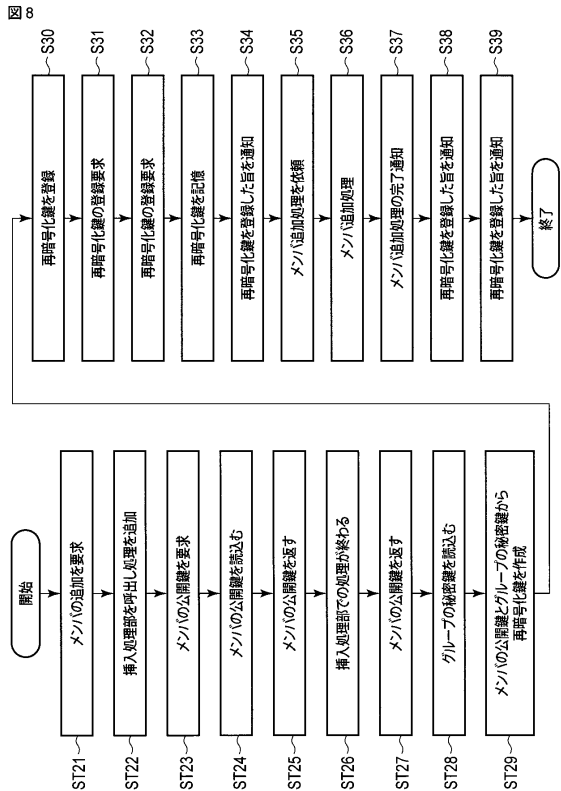


【 図 7 】

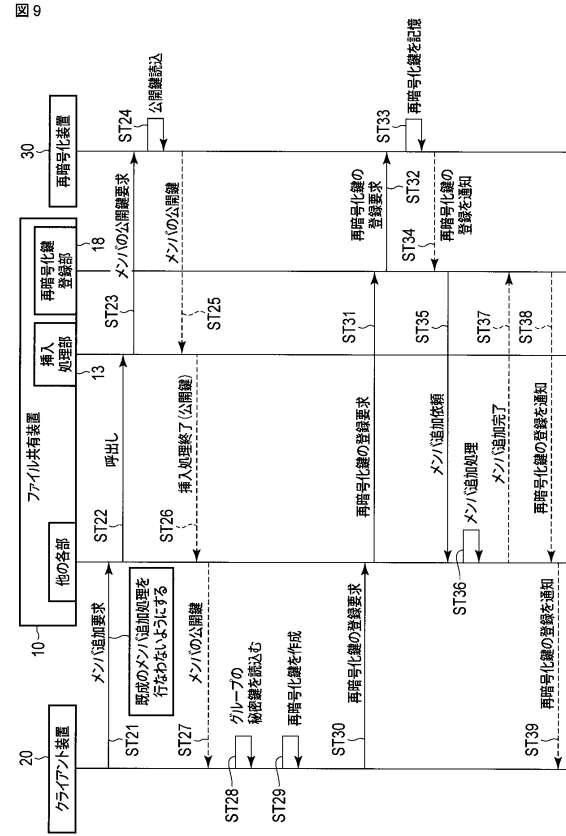
図 7



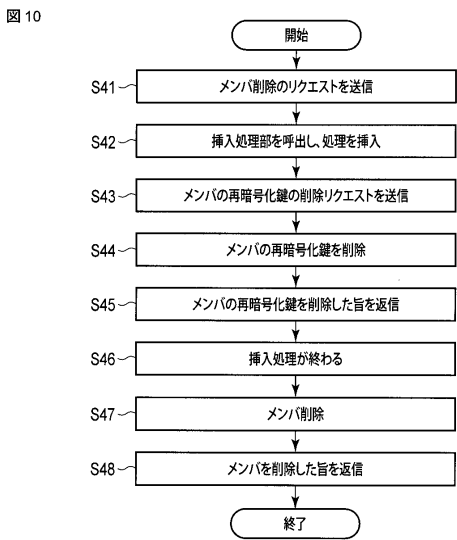
【 図 8 】



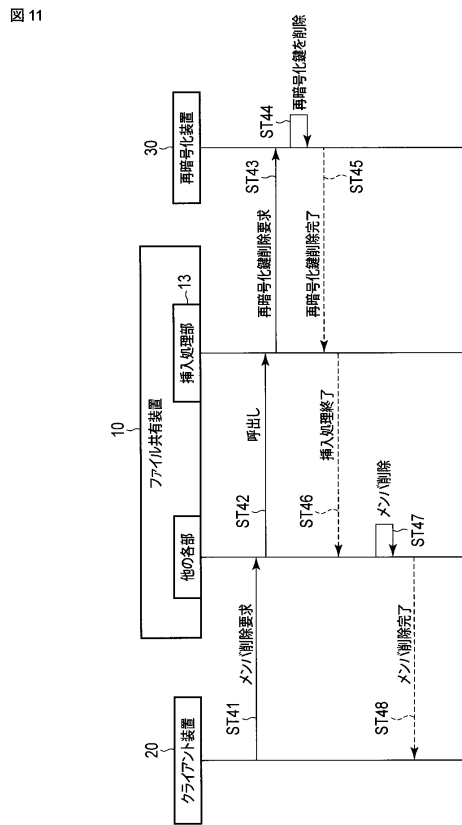
【 図 9 】



【 図 10 】

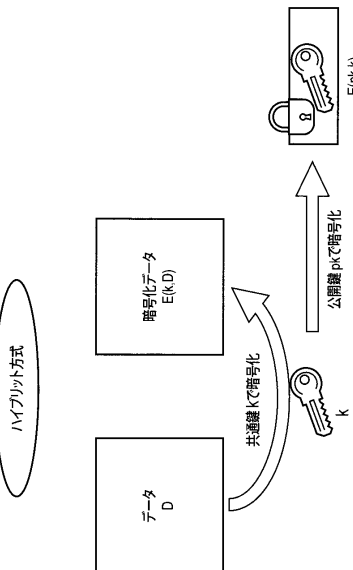


【 図 11 】



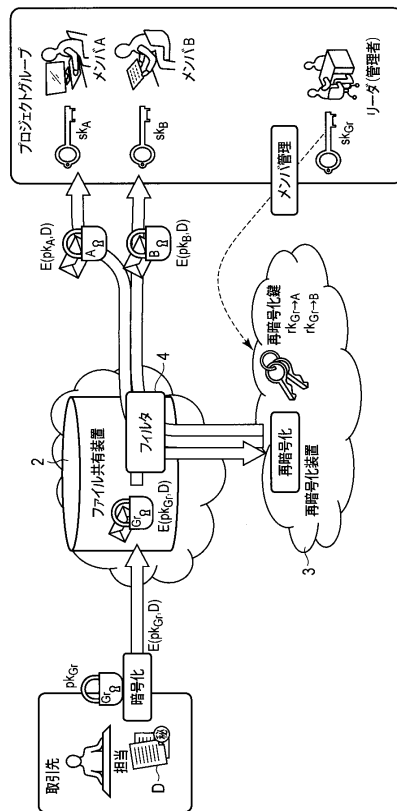
【図 20】

図 20



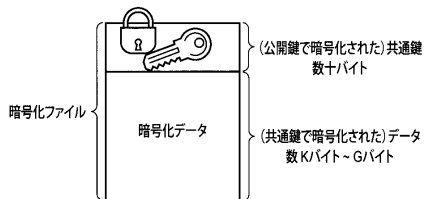
【図 21】

図 21



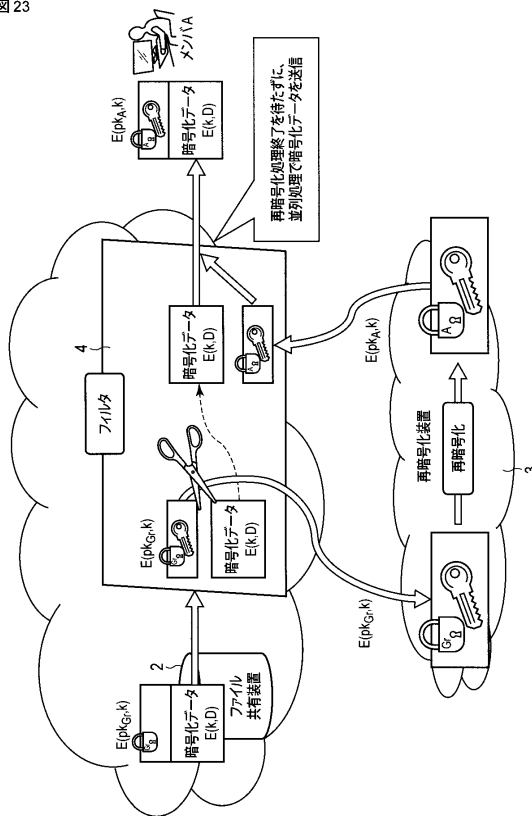
【図 22】

図 22



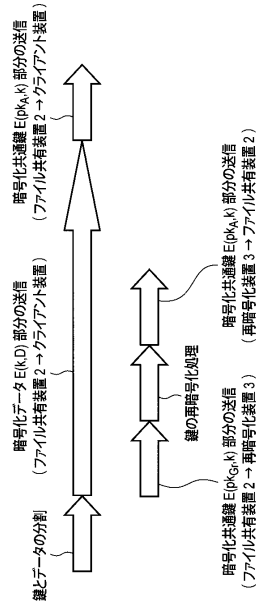
【図 23】

図 23



【 図 24 】

図 24



フロントページの続き

- (74)代理人 100075672
弁理士 峰 隆司
- (74)代理人 100095441
弁理士 白根 俊郎
- (74)代理人 100103034
弁理士 野河 信久
- (74)代理人 100119976
弁理士 幸長 保次郎
- (74)代理人 100153051
弁理士 河野 直樹
- (74)代理人 100140176
弁理士 砂川 克
- (74)代理人 100158805
弁理士 井関 守三
- (74)代理人 100124394
弁理士 佐藤 立志
- (74)代理人 100112807
弁理士 岡田 貴志
- (74)代理人 100111073
弁理士 堀内 美保子
- (74)代理人 100134290
弁理士 竹内 将訓
- (72)発明者 総田 佑樹
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内
- (72)発明者 吉田 琢也
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内
- (72)発明者 藤井 吉弘
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内
- (72)発明者 阿部 真吾
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内
- (72)発明者 山田 正隆
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内

審査官 松平 英

- (56)参考文献 特開2007-080145(JP,A)
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,株式会社東芝,2011年11月1日,第66巻 第11号,p.18~22

(58)調査した分野(Int.Cl.,DB名)

G09C 1/00
H04L 9/00
G06F 21/20
G06F 21/24
H04L 12/00
H04L 29/00
H04W 4/00