

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6792191号
(P6792191)

(45) 発行日 令和2年11月25日 (2020. 11. 25)

(24) 登録日 令和2年11月10日 (2020. 11. 10)

(51) Int. Cl.	F I
H04L 9/08 (2006.01)	H04L 9/00 G01B
	H04L 9/00 G01E

請求項の数 12 (全 33 頁)

(21) 出願番号	特願2016-162116 (P2016-162116)	(73) 特許権者	000004237
(22) 出願日	平成28年8月22日 (2016. 8. 22)		日本電気株式会社
(65) 公開番号	特開2018-32908 (P2018-32908A)		東京都港区芝五丁目7番1号
(43) 公開日	平成30年3月1日 (2018. 3. 1)	(74) 代理人	100124811
審査請求日	令和1年7月4日 (2019. 7. 4)		弁理士 馬場 資博
		(74) 代理人	100088959
			弁理士 境 廣巳
		(72) 発明者	石井 真之
			東京都港区芝五丁目7番1号 日本電気株式会社社内
		審査官	児玉 崇晶

最終頁に続く

(54) 【発明の名称】 情報送信方法、情報処理方法、プログラム、復号方法、プログラム

(57) 【特許請求の範囲】

【請求項1】

送付側装置から管理サーバを介して受取側装置に対して情報を送信する情報送信方法であって、

前記管理サーバは、

第1の暗号鍵により暗号化された第1の暗号文を送付側装置から受信し、

前記受取側装置から当該受取側装置の状態を示す情報である状態情報を受信し、

受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信し、

前記送付側装置は、前記受取側装置に対して送信する情報を秘密分散により2つに分割し、一方を第1の暗号鍵により暗号化した後、第1の暗号文として前記管理サーバに送信し、他方を第1の暗号鍵により暗号化した後、第3の暗号文として前記受取側装置に送信し、

前記受取側装置は、前記管理サーバから受信した前記第2の暗号文と、前記送付側装置から受信した前記第3の暗号文と、に基づいて復号を行い、前記送付側装置が送信する情報を取得し、

前記受取側装置は、前記送付側装置が送信する情報を取得した後、当該取得した情報を秘密分散して2つに分割し、当該分割したうちの一方を前記第2の暗号鍵に基づいて暗号化した後、前記管理サーバに送信する情報送信方法。

10

20

【請求項 2】

請求項 1 に記載の情報送信方法であって、
前記管理サーバは、前記状態情報として、前記第 2 の暗号文の復号を行う装置を特定する情報である装置特定情報を受信する
情報送信方法。

【請求項 3】

請求項 1 又は 2 に記載の情報送信方法であって、
前記管理サーバは、前記状態情報として、前記第 2 の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する
情報送信方法。

10

【請求項 4】

請求項 1 乃至 3 のいずれかに記載の情報送信方法であって、
前記管理サーバは、前記状態情報として、前記受取側装置の操作者を特定する情報である操作者特定情報を受信する
情報送信方法。

【請求項 5】

請求項 1 乃至 4 のいずれかに記載の情報送信方法であって、
前記受取側装置は、前記第 3 の暗号文の復号を行う際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから前記第 2 の暗号文を受信する
情報送信方法。

20

【請求項 6】

請求項 1 乃至 5 のいずれかに記載の情報送信方法であって、
前記管理サーバは、
前記第 1 の暗号文を前記送付側装置から受信するとともに前記第 1 の暗号鍵を前記送付側装置から受信し、前記第 1 の暗号鍵に基づいて作成した第 3 の暗号鍵と前記第 1 の暗号文とに基づいて、前記第 1 の暗号文に基づく暗号文を作成して格納し、
前記受取側装置から前記状態情報を受信すると、前記第 2 の暗号鍵と、前記第 1 の暗号文に基づく暗号文と、に基づいて作成した前記第 2 の暗号文を前記受取側装置に対して送信する
情報送信方法。

30

【請求項 7】

受取側装置により行われる復号方法であって、
復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、
前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号し、
外部装置から暗号文を受信し、受信した当該暗号文を復号する際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから、前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、

前記管理サーバから受信した暗号文と、前記外部装置から受信した暗号文と、に基づいて復号を行い、

40

復号を行った後、当該復号により取得した情報を秘密分散して 2 つに分割し、当該分割したうちの一方を前記状態情報に基づいて作成される暗号鍵に基づいて暗号化した後、前記管理サーバに送信する

復号方法。

【請求項 8】

請求項 7 に記載の復号方法であって、
前記状態情報として、前記受取側装置を特定する情報である装置特定情報を送信する
復号方法。

【請求項 9】

50

請求項 7 又は 8 に記載の復号方法であって、
前記状態情報として、前記受取側装置の環境を特定する情報である環境特定情報を送信する
復号方法。

【請求項 10】

受取側装置に、
復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、
前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号し、
外部装置から暗号文を受信し、受信した当該暗号文を復号する際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから、前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、
前記管理サーバから受信した暗号文と、前記外部装置から受信した暗号文と、に基づいて復号を行い、
復号を行った後、当該復号により取得した情報を秘密分散して 2 つに分割し、当該分割したうちの一方を前記状態情報に基づいて作成される暗号鍵に基づいて暗号化した後、前記管理サーバに送信する

10

処理を実現するためのプログラム。

【請求項 11】

請求項 10 に記載のプログラムであって、
前記状態情報として、前記受取側装置を特定する情報である装置特定情報を送信するプログラム。

20

【請求項 12】

請求項 10 又は 11 に記載のプログラムであって、
前記状態情報として、前記受取側装置の環境を特定する情報である環境特定情報を送信する
プログラム。

【発明の詳細な説明】

【技術分野】

30

【0001】

本発明は、情報送信方法、情報処理方法、プログラム、復号方法、プログラムに関し、特に、外部のユーザと安全に情報を共有するための情報送信方法、情報処理方法、プログラム、復号方法、プログラムに関する。

【背景技術】

【0002】

外部のユーザと安全に情報を共有する手段の一つとして、ファイル・データを暗号化する方法が知られている。

【0003】

例えば、特許文献 1 には、データを秘密分散する方法の一例が記載されている。具体的には、特許文献 1 によると、データを 2 分割して一方のデータと他方のデータを生成する。そして、一方のデータに基づいて生成した複数の擬似乱数列を用いて他方のデータを多重に暗号化し、他方のデータに基づいて生成した複数の擬似乱数列を用いて一方のデータを多重に暗号化する。特許文献 1 によると、上記構成により、データを不等サイズに分割した際にも安全性の劣化を防止することが出来る。

40

【0004】

また、データの秘匿性・復元性を確保するためクライアント装置に格納されているデータをストレージ装置に格納する技術の 1 つとして、例えば、特許文献 2 がある。特許文献 2 には、秘密分散法によって原データ M を分割したうちの第 1 の分散情報を含む書込要求をストレージサーバへ送信して自身から第 1 の分散情報を削除する第 1 のステップと、第

50

2の分散情報を、公開鍵を用いて暗号化した第2の暗号化分散情報Epkを含むデータ書込要求をストレージサーバへ送信する第2のステップとを有するデータ保護方法が記載されている。特許文献2によると、上記構成により、データの秘匿性及び復元性を同時に提供することが出来る。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2009-288616号公報

【特許文献2】特開2008-097591号公報

【発明の概要】

10

【発明が解決しようとする課題】

【0006】

より強固にデータを秘匿するなどの目的のため、特許文献1に記載されているような方法で秘密分散した後さらに暗号化を行って、暗号化した後のデータをストレージ装置や相手先装置に送信することがある。ここで、特許文献2に記載されているような方法を用いて相手先にデータを送信しようとする場合、相手先でデータを復号するためには何らかの方法で復号するための鍵を入手することが必要となる。

【0007】

鍵の方法としては、例えば、認証サーバを介して認証が通った場合に復号するための鍵を配布する方法がある。しかしながら、この方法を用いる場合、事前にデータの共有相手を認証サーバに登録しておくことが必要となる。その結果、運用が煩雑となったり、認証サーバへの登録が出来ない相手と復号を要するデータの共有を行うことが難しくなったりなどの問題が生じることになる。一方、鍵をメールなどの方法により共有すると、メールの漏洩により第三者による復号が可能となり、また、復号されたことに気が付くことが出来ない、という問題が生じることになる。

20

【0008】

このように、暗号文を復号するための鍵を安全に相手方に渡すことは難しかった。その結果、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが難しい、という問題が生じていた。

【0009】

30

そこで、本発明の目的は、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが難しい、という問題を解決する情報送信方法、情報処理方法、プログラム、復号方法、プログラムを提供することにある。

【課題を解決するための手段】

【0010】

かかる目的を達成するため本発明の一形態である情報送信方法は、
送付側装置から管理サーバを介して受取側装置に対して情報を送信する情報送信方法であって、

前記管理サーバは、

40

第1の暗号鍵により暗号化された第1の暗号文を送付側装置から受信し、

前記受取側装置から当該受取側装置の状態を示す情報である状態情報を受信し、

受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する

という構成を採る。

【0011】

また、本発明の他の形態である情報処理方法は、

管理サーバにより行われる情報処理方法であって、

第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信し、

受取側装置の状態を示す状態情報を受信し、

50

受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信するという構成を採る。

【0012】

また、本発明の他の形態であるプログラムは、
管理サーバに、
第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信し、
受取側装置の状態を示す状態情報を受信し、
受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する
処理を実現するためのプログラムである。

10

【0013】

また、本発明の他の形態である復号方法は、
復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、
前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する
という構成を採る。

【0014】

また、本発明の他の形態であるプログラムは、
受取側装置に、
復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、
前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する
処理を実現させるためのプログラムである。

20

【発明の効果】

【0015】

本発明は、以上のように構成されることにより、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが難しい、という問題を解決する情報送信方法、情報処理方法、プログラム、復号方法、プログラムを提供することが可能となる。

30

【図面の簡単な説明】

【0016】

【図1】本発明の第1の実施形態における情報共有システムの構成の一例を示すブロック図である。

【図2】図1で示す送付側装置の構成の一例を示すブロック図である。

【図3】図1で示す管理サーバの構成の一例を示すブロック図である。

【図4】図3で示すコンテンツ情報格納部に格納されているコンテンツ情報の一例を示す図である。

40

【図5】図1で示す受取側装置の構成の一例を示すブロック図である。

【図6】情報共有システムの各構成が有する情報の一例を示す図である。

【図7】送付側装置がファイルMを秘密分散した後暗号化して、暗号化したファイルを管理サーバと受取側装置とに送信する際の処理の流れの一例を示す図である。

【図8】送付側装置から情報を受信した管理サーバにおける処理の流れの一例を示す図である。

【図9】受取側装置から管理サーバに対して送信される情報の一例を示す図である。

【図10】受取側装置から情報を受信した管理サーバにおける処理の流れの一例を示す図である。

【図11】受取側装置における復号処理の流れの一例を示す図である。

50

【図 1 2】管理サーバに格納されている情報の更新を行う際の処理の流れの一例を示す図である。

【図 1 3】本発明の第 1 の実施形態における情報共有システムの動作の一例（情報送信方法の流れの一例）を示すフローチャートである。

【図 1 4】本発明の第 1 の実施形態における情報共有システムの動作の一例を示すフローチャートである。

【図 1 5】本発明の第 1 の実施形態における情報共有システムの動作の一例を示すフローチャートである。

【図 1 6】秘密分散を行わない場合の処理の流れの一例を示す図である。

【図 1 7】秘密分散を行わない場合の処理の流れの一例を示す図である。

10

【図 1 8】本発明の第 2 の実施形態における情報共有システムの構成の一例を示すブロック図である。

【図 1 9】本発明の第 2 の実施形態における管理サーバの構成の一例を示すブロック図である。

【図 2 0】本発明の第 2 の実施形態における受取側装置の構成の一例を示すブロック図である。

【発明を実施するための形態】

【0017】

[第 1 の実施形態]

本発明の第 1 の実施形態を図 1 乃至図 1 7 を参照して説明する。図 1 は、情報共有システム 1 の構成の一例を示すブロック図である。図 2 は、送付側装置 1 1 の構成の一例を示すブロック図である。図 3 は、管理サーバ 1 2 の構成の一例を示すブロック図である。図 4 は、コンテンツ情報格納部 1 2 6 に格納されている情報であるコンテンツ情報 1 2 6 1 の一例を示す図である。図 5 は、受取側装置 1 3 の構成の一例を示すブロック図である。図 6 乃至図 1 2 は、情報共有システム 1 により行われる情報送信方法の流れの一例を説明するための図である。図 1 3 乃至図 1 5 は、情報共有システム 1 の動作の一例（つまり、情報送信方法の流れの一例）を示すフローチャートである。図 1 6、図 1 7 は、秘密分散を行わない場合の処理の流れの一例を示す図である。

20

【0018】

本発明の第 1 の実施形態では、送付側装置 1 1 から受取側装置 1 3 に対して安全に情報を送信することが出来る情報共有システム 1 について説明する。本実施形態における送付側装置 1 1 は、受取側装置 1 3 に対して送信しようとする情報であるファイル M をファイル M 1、ファイル M 2 に秘密分散した後、ファイル M 1 を暗号化して管理サーバ 1 2 に送信し、ファイル M 2 を暗号化して受取側装置 1 3 に送信する。後述するように、受取側装置 1 3 は、送付側装置 1 1 から受信したファイル M 2 の復号を試みる際に、受取側装置 1 3 の状態を示す情報である状態情報 (I m) を含む情報を管理サーバ 1 2 に送信する。そして、受取側装置 1 3 は、管理サーバ 1 2 から、状態情報 (I m) に基づいて作成された暗号鍵により暗号化したファイル M 1 を受信する。その後、受取側装置 1 3 は、送信元装置 1 1 から受信した暗号化したファイル M 2 と管理サーバ 1 2 から受信した暗号化したファイル M 1 とに基づいて、秘密分散する対象となった元データであるファイル M を復号する。

30

【0019】

図 1 は、本実施形態において説明する情報共有システム 1 の全体の構成の一例を示している。図 1 を参照すると、情報共有システム 1 は、送付側装置 1 1 と管理サーバ 1 2 と受取側装置 1 3 とを有している。

【0020】

図 1 で示すように、送付側装置 1 1 と管理サーバ 1 2 とは、ネットワーク 1 4 を介して互いに通信可能なよう接続されている。また、管理サーバ 1 2 と受取側装置 1 3 とは、ネットワーク 1 4 を介して互いに通信可能なよう接続されている。同様に、送付側装置 1 1 と受取側装置 1 3 とは、ネットワーク 1 4 を介して互いに通信可能なよう接続されている。

50

。

【0021】

送付側装置11は、例えば、パーソナルコンピュータやタブレット装置などの情報処理装置である。送付側装置11は、受取側装置13に対して送付する対象となる情報（例えば、ファイルM）を有しており、当該送付する対象となる情報であるファイルMを秘密分散した後暗号化して、当該秘密分散した後暗号化した情報を管理サーバ12や受取側装置13に送信する。また、送付側装置11は、後述する暗号鍵（K）を作成する際に用いるパスワード（Pw）や受取側装置13のメールアドレス（ML_b）を有している。

【0022】

図2は、送付側装置11の構成の一例である。図2を参照すると、送付側装置11は、送受信手段111と、分散処理手段112と、暗号鍵作成手段113と、暗号化手段114と、情報格納部115と、を有している。

10

【0023】

なお、送付側装置11は、図示しないCPU（Central Processing Unit）などの演算装置と記憶装置とを有している。送付側装置11は、例えば、記憶装置が備えるプログラムを演算装置が実行することで、上記各手段を実現する。

【0024】

送受信手段111は、管理サーバ12や受取側装置13と情報の送受信を行う。送受信手段111を介して管理サーバ12に対して送信される情報としては、例えば、暗号化した暗号鍵P_sv（K）や暗号化したファイルK（M1）、受取側装置13のメールアドレス（ML_b）などがある。また、送受信部111を介して管理サーバ12から受信する情報としては、例えば、公開鍵（P_sv）などがある。また、送受信部111を介して受取側装置13に対して送信される情報としては、例えば、暗号化したファイルK（M2）やパスワード（Pw）などがある。なお、送受信手段111が送受信する各種情報の詳細については、後述する。

20

【0025】

分散処理手段112（第2分散処理手段）は、送付する対象となる情報を秘密分散する。例えば、分散処理手段112は、ファイルMを秘密分散で2つに分割する（3つ以上に分割しても構わない）。つまり、分散処理手段112は、ファイルMを秘密分散してファイルM1とファイルM2を生成する。そして、分散処理手段112は、生成したファイルM1とファイルM2を暗号化手段114に送信する。なお、本実施形態においては、分散処理手段112により行われる秘密分散の具体的な方法については、特に限定しない。

30

【0026】

暗号鍵作成手段113は、パスワード（Pw）に基づいて、共通鍵である暗号鍵（K）を作成する。例えば、暗号鍵作成手段113は、情報格納部115を参照して情報格納部115からパスワード（Pw）を取得する。続いて、暗号鍵作成手段113は、取得したパスワード（Pw）に基づいて暗号鍵（K）を作成する（暗号鍵を作成する手段は、任意の手段を用いて構わない）。その後、暗号鍵作成手段113は、作成した暗号鍵（K）を暗号化手段114に送信する。なお、暗号鍵作成手段113は、パスワード（Pw）として送付側装置11が備えるキーボードなどの入力装置を介して入力されたものを用いても構わない。

40

【0027】

暗号化手段114（第2暗号化手段）は、暗号鍵作成手段113が作成した暗号鍵（K）や管理サーバ12から取得した公開鍵（P_sv）を用いて、秘密分散したファイルM1、ファイルM2や、暗号鍵（K）の暗号化を行う。

【0028】

例えば、暗号化手段114は、暗号鍵（K）を用いて、秘密分散したファイルM1、ファイルM2を暗号化する。つまり、暗号化手段114は、暗号鍵（K）によりファイルM1、ファイルM2を暗号化して、暗号化したファイルK（M1）、K（M2）を生成する。また、暗号化手段114は、暗号化したファイルK（M1）、K（M2）に対して、ユ

50

ニークなIDであるコンテンツID (C i d) を埋め込む。このように、暗号化したファイルK (M 1)、K (M 2) にコンテンツID (C i d) を埋め込むことで、暗号化したファイルK (M 1) と暗号化したファイルK (M 2) との対応関係を識別可能となる。暗号化手段114が暗号化した、暗号化したファイルK (M 1)、K (M 2) は、送受信手段111を介して、管理サーバ12や受取側装置13に送信されることになる。

【0029】

また、暗号化手段114は、管理サーバ12から送受信手段111を介して受信した公開鍵 (P__s v) を用いて、暗号鍵 (K) を暗号化する。つまり、暗号化手段114は、送受信手段111を介して、管理サーバ12から公開鍵 (P__s v) を取得する。続いて、暗号化手段114は、取得した公開鍵 (P__s v) により暗号鍵 (K) を暗号化して、暗号化した暗号鍵P__s v (K) を生成する。暗号化手段114が暗号化した暗号鍵P__s v (K) は、送受信手段111を介して、管理サーバ12に送信されることになる。

10

【0030】

情報格納部115は、メモリやディスク装置などの記憶装置である。情報格納部115には、パスワード (P w) や受取側装置13のメールアドレス (M L__b) などを格納することが出来る。

【0031】

管理サーバ12は、例えば、サーバ装置などの情報処理装置である。管理サーバ12は、送付側装置11から受信した、暗号化したファイルK (M 1) を平文化した後、暗号鍵 (K') により再度暗号化してコンテンツ情報格納部126に格納する。また、管理サーバ12は、受取側装置13からの要求に応じて、当該要求に対応するファイルを受取側装置13に送信する。後述するように、管理サーバ12は、受取側装置13にファイルを送信する際、受取側装置13から受信した状態情報 (I m) を用いて作成した暗号鍵 (K'') を用いて対応するファイルを暗号化し、当該暗号化したファイルを送信することになる。また、この際、管理サーバ12は、コンテンツ情報格納部126に格納する情報を、暗号鍵 (K'') を用いて暗号化したファイルに更新することになる。

20

【0032】

図3は、管理サーバ12の構成の一例である。図3を参照すると、管理サーバ12は、送受信手段121と、復号手段122と、暗号鍵作成手段123と、暗号化手段124と、コンテンツ情報管理手段125と、コンテンツ情報格納部126と、公開鍵・秘密鍵格納部127と、を有している。

30

【0033】

なお、管理サーバ12は、図示しないCPU (C e n t r a l P r o c e s s i n g U n i t) などの演算装置と記憶装置とを有している。管理サーバ12は、例えば、記憶装置が備えるプログラムを演算装置が実行することで、上記各手段を実現する。

【0034】

送受信手段121 (第1送受信手段) は、送付側装置11や受取側装置13と情報の送受信を行う。送受信手段121を介して送付側装置11から受信する情報としては、例えば、暗号化した暗号鍵P__s v (K) や暗号化したファイルK (M 1)、受取側装置13のメールアドレス (M L__b) などがある。また、送受信手段121を介して送付側装置11に対して送信する情報としては、例えば、公開鍵 (P__s v) などがある。また、送受信手段121を介して受取側装置13から受信する情報としては、例えば、パスワード (P w)、メールアドレス (M L__b)、状態情報 (I m)、コンテンツID (C i d)、暗号化したファイルK'' (M 1') などがある。また、送受信手段121を介して受取側装置13に対して送信する情報としては、例えば、暗号化したファイルK'' (M 1) などがある。なお、暗号化したファイルK'' (M 1') や暗号化したファイルK'' (M 1) の詳細については、後述する。

40

【0035】

復号手段122は、受信した暗号化した暗号鍵P__s v (K) の復号や暗号化したファイルK (M 1) の復号、暗号化したファイルK' (M 1) の復号を行う。

50

【0036】

例えば、復号手段122は、公開鍵・秘密鍵格納部127に格納されている秘密鍵（S__sv）を用いて、暗号化した暗号鍵P__sv（K）を復号する。つまり、復号手段122は、送受信手段121を介して、送付側装置11から暗号化した暗号鍵P__sv（K）を受信すると、公開鍵・秘密鍵格納部127を参照して、公開鍵・秘密鍵格納部127に格納されている秘密鍵（S__sv）を取得する。そして、復号手段122は、取得した秘密鍵（S__sv）を用いて暗号化した暗号鍵P__sv（K）を復号して、暗号鍵（K）を生成する。

【0037】

また、復号手段122は、暗号化した暗号鍵P__sv（K）を復号して暗号鍵（K）を生成した後、当該暗号鍵（K）を用いて、送受信手段121を介して送付側装置11から受信した暗号化したファイルK（M1）の復号を行う。つまり、復号手段122は、暗号鍵（K）により、暗号化したファイルK（M1）を復号して、ファイルM1を生成する。その後、復号手段122は、生成したファイルM1を暗号化手段124に送信する。

10

【0038】

また、復号手段122は、暗号鍵作成手段123から受信した暗号鍵（K'）を用いて、コンテンツ情報格納部126から取得した暗号化したファイルK'（M1）の復号を行う。つまり、復号手段122は、暗号鍵（K'）により、暗号化したファイルK'（M1）を復号して、ファイルM1を生成する。その後、復号手段122は、生成したファイルM1を暗号化手段124に送信する。なお、暗号鍵作成手段123や暗号鍵（K'）の詳細については、後述する。

20

【0039】

暗号鍵作成手段123（第1暗号鍵作成手段）は、パスワード（Pw）に基づいて、暗号鍵（K）を作成する。また、暗号鍵作成手段123は、共通鍵である暗号鍵（K'）の作成や、共通鍵である暗号鍵（K''）の作成を行う。

【0040】

例えば、暗号鍵作成手段123は、送受信手段121がパスワード（Pw）を受信すると、当該受信したパスワード（Pw）に基づいて暗号鍵（K）を作成する。

【0041】

また、暗号鍵作成手段123は、作成した暗号鍵（K）や復号手段122が復号することで生成した暗号鍵（K）と送受信手段121が受信した受取側装置13のメールアドレス（ML__b）とに基づいて、共通鍵である暗号鍵（K'）を作成する。そして、暗号鍵作成手段123は、作成した暗号鍵（K'）を暗号化手段124に送信する。

30

【0042】

また、暗号鍵作成手段123は、暗号鍵（K）と送受信手段121が受信した受取側装置13のメールアドレス（ML__b）と送受信手段121が受信した状態情報（Im）とに基づいて、共通鍵である暗号鍵（K''）を作成する。そして、暗号鍵作成手段123は、作成した暗号鍵（K''）を暗号化手段124に送信する。

【0043】

暗号化手段124（第1暗号化手段）は、暗号鍵作成手段123から受信した暗号鍵（K'）や暗号鍵（K''）を用いて、復号手段122から受信したファイルM1の暗号化を行う。

40

【0044】

例えば、暗号化手段124は、暗号鍵（K'）を用いて、ファイルM1を暗号化する。つまり、暗号化手段124は、暗号鍵（K'）によりファイルM1を暗号化して、暗号化したファイルK'（M1）を生成する。その後、暗号化手段124は、暗号化したファイルK'（M1）をコンテンツ情報管理手段125に送信する。

【0045】

また、暗号化手段124は、暗号鍵（K''）を用いて、ファイルM1を暗号化する。つまり、暗号化手段124は、暗号鍵（K''）によりファイルM1を暗号化して、暗号化し

50

たファイルK”(M1)を生成する。その後、暗号化手段124は、暗号化したファイルK”(M1)をコンテンツ情報管理手段125に送信するとともに、送受信手段121を介して受取側装置13に対して、暗号化したファイルK”(M1)を送信する。

【0046】

コンテンツ情報管理手段125は、コンテンツ情報格納部126に格納されているコンテンツ情報1261の作成、更新、削除、登録などの管理を行う。

【0047】

例えば、コンテンツ情報管理手段125は、暗号化したファイルK(M1)を送付側装置11より受信すると、暗号化したファイルK(M1)に埋め込まれているコンテンツID(Cid)を抽出して、コンテンツ情報格納部126内のコンテンツ情報1261に新たな登録を行う。つまり、コンテンツ情報管理手段125は、暗号化したファイルK(M1)を送付側装置11より受信すると、コンテンツ情報1261内に新たなレコードの作成を行い、暗号化したファイルK(M1)に埋め込まれているコンテンツID(Cid)を登録する。

【0048】

また、コンテンツ情報管理手段125は、暗号化手段124から受信した暗号化したファイルK'(M1)に基づいて、コンテンツID(Cid)に対応する箇所に、対応する受取側装置13のメールアドレス(ML_b)と、暗号化したファイルK'(M1)と、を登録する。

【0049】

また、コンテンツ情報管理手段125は、暗号化手段124から暗号化したファイルK”(M1)を受信すると、対応する箇所に格納されている情報を暗号化したファイルK”(M1)に更新する。つまり、コンテンツ情報管理手段125は、受取側装置13から受信した情報のうちのコンテンツID(Cid)及びメールアドレス(ML_b)を参照して、対応する情報が格納されている箇所を特定する。そして、コンテンツ情報管理手段125は、対応する箇所に格納されている情報を、暗号化したファイルK'(M1)から暗号化したファイルK”(M1)に更新する。換言すると、コンテンツ情報管理手段125は、暗号化手段124から暗号化したファイルK”(M1)を受信すると、対応する箇所に格納されている暗号化したファイルK'(M1)を削除する。また、コンテンツ情報管理手段125は、暗号化したファイルK'(M1)を削除した箇所に、新たに暗号化したファイルK”(M1)を登録する。

【0050】

また、コンテンツ情報管理手段125は、送受信手段121が暗号化したファイルK”(M1')を受信すると、対応する箇所に格納されている情報を暗号化したファイルK”(M1')に更新する。つまり、コンテンツ情報管理手段125は、受取側装置13から受信した情報のうちのコンテンツID(Cid)及びメールアドレス(ML_b)を参照して、対応する情報が格納されている箇所を特定する。そして、コンテンツ情報管理手段125は、対応する箇所に格納されている情報を、暗号化したファイルK”(M1)から暗号化したファイルK”(M1')に更新する。換言すると、コンテンツ情報管理手段125は、暗号化したファイルK”(M1')を受信すると、対応する箇所に格納されている暗号化したファイルK”(M1)を削除する。また、コンテンツ情報管理手段125は、暗号化したファイルK”(M1)を削除した箇所に、新たに暗号化したファイルK”(M1')を登録する。

【0051】

このように、コンテンツ情報管理手段125は、コンテンツ情報格納部126内のコンテンツ情報1261の管理を行う。

【0052】

コンテンツ情報格納部126は、メモリやディスク装置などの記憶装置である。コンテンツ情報格納部126には、暗号化したファイルK'(M1)や暗号化したファイルK”(M1)、暗号化したファイルK”(M1')などが格納されるコンテンツ情報1261

10

20

30

40

50

が格納されている。

【0053】

図4は、コンテンツ情報1261の一例である。図4を参照すると、コンテンツ情報1261には、コンテンツIDとメールアドレスとファイルとが含まれている。例えば、図4の1行目は、コンテンツID「A」と、メールアドレス「a」と、ファイル「α」と、を対応付けている。

【0054】

公開鍵・秘密鍵格納部127は、メモリやディスク装置などの記憶装置である。公開鍵・秘密鍵格納部127には、公開鍵(P__sv)と秘密鍵(S__sv)とが格納されている。

10

【0055】

受取側装置13は、例えば、パーソナルコンピュータやタブレット装置などの情報処理装置である。受取側装置13は、送付側装置11及び管理サーバ12から受信した暗号化したファイルを復号することで、送付側装置11が送信したような情報であるファイルMを取得する。受取側装置13は、状態情報(I m)や受取側装置13のメールアドレス(M L__b)を有している。

【0056】

なお、状態情報(I m)とは、受取側装置13の状態を示す情報のことをいう。状態情報(I m)としては、例えば、復号を可能とする装置を特定する装置特定情報や、復号を可能とする装置の環境を特定する環境特定情報などが考えられる。より具体的には、装置特定情報としては、例えば、情報共有システム1を利用するためのプログラムを受取側装置13にインストールする際に自動で生成されるユニークなID情報などのソフト特定情報や、受取側装置13のMAC名、受取側装置13のマシン名などの装置情報などが考えられる。また、環境特定情報としては、例えば、アクセスポイントやゲートウェイを識別するための接続箇所特定情報や、GPS情報などの位置情報などの受取側装置13を利用するエリアを特定するための利用エリア特定情報が考えられる。このように、状態情報(I m)としては、装置特定情報や環境特定情報などの様々な情報を採用することが出来る。

20

【0057】

なお、状態情報(I m)には、例えば、受取側装置13を操作する操作者の指紋に基づいて生成される値をハッシュ値化した情報や操作者の虹彩に基づいて作成される情報など、復号を可能とする装置の操作者を特定する操作者特定情報などを含んでいても構わない。換言すると、状態情報(I m)には、生体認証に用いる情報に基づいて作成される操作者特定情報を含めることが出来る。状態情報(I m)には、装置特定情報や環境特定情報、操作者特定情報のいずれか一つのみが含まれていても構わないし、複数の情報が含まれていても構わない。

30

【0058】

図5は、受取側装置13の構成の一例である。図5を参照すると、受取側装置13は、送受信手段131と、暗号鍵作成手段132と、復号手段133と、分散処理手段134と、暗号化手段135と、情報格納部136と、を有している。また、受取側装置13は、GPS測定手段や生体認証情報取得手段など、状態情報(I m)を取得するための構成を有することが出来る(図5には図示せず)。

40

【0059】

なお、受取側装置13は、図示しないCPU(Central Processing Unit)などの演算装置と記憶装置とを有している。受取側装置13は、例えば、記憶装置が備えるプログラムを演算装置が実行することで、上記各手段を実現する。

【0060】

送受信手段131は、送付側装置11や管理サーバ12と情報の送受信を行う。送受信手段131を介して送付側装置11から受信する情報としては、例えば、暗号化したファイルK(M2)やパスワード(Pw)などがある。また、送受信手段131を介して管理

50

サーバ12に対して送信する情報としては、例えば、パスワード(Pw)、受取側装置13のメールアドレス(ML_b)、状態情報(Im)、コンテンツID(Cid)や、暗号化したファイルK”(M1’)などがある。また、送受信手段131を介して管理サーバ12から受信する情報としては、例えば、暗号化したファイルK”(M1)などがある。

【0061】

暗号鍵作成手段132は、パスワード(Pw)に基づいて、暗号鍵(K)を作成する。また、暗号鍵作成手段132は、暗号鍵(K”)の作成を行う。暗号鍵作成手段132は、暗号鍵(K’)を作成するよう構成しても構わない。

【0062】

例えば、暗号鍵作成手段132は、送受信手段131が受信したパスワード(Pw)に基づいて暗号鍵(K)を作成する。また、暗号鍵作成手段132は、作成した暗号鍵(K)と受取側装置13のメールアドレス(ML_b)と状態情報(Im)とに基づいて、共通鍵である暗号鍵(K”)を作成する。そして、暗号鍵作成手段132は、作成した暗号鍵(K)や暗号鍵(K”)を復号手段133や暗号化手段135に送信する。

【0063】

復号手段133は、送付側装置11から受信した暗号化したファイルK(M2)をユーザが開こうとしてパスワード(Pw)を入力すると、送受信手段131を介して、入力されたパスワード(Pw)、受取側装置13のメールアドレス(ML_b)、状態情報(Im)、暗号化したファイルK(M2)に含まれるコンテンツID(Cid)、を管理サーバ12に送信する。その後、管理サーバ12から暗号化したファイルK”(M1)を受信すると、暗号鍵作成手段132から受信した暗号鍵(K)や暗号鍵(K”)を用いて、送付側装置11から受信した暗号化したファイルK(M2)と管理サーバ12から受信した暗号化したファイルK”(M1)の復号を行い、ファイルMを生成する。

【0064】

例えば、復号手段133は、暗号鍵(K)を用いて、暗号化したファイルK(M2)の復号を行う。つまり、復号手段133は、暗号鍵(K)により暗号化したファイルK(M2)を復号して、ファイルM2を生成する。また、復号手段133は、暗号鍵(K”)を用いて、暗号化したファイルK”(M1)の復号を行う。つまり、復号手段133は、暗号鍵(K”)により暗号化したファイルK”(M1)を復号して、ファイルM1を生成する。その後、復号手段133は、ファイルM1とファイルM2とからファイルMを生成する。復号手段133は、例えばこのようにして、送付側装置11及び管理サーバ12から受信した情報に基づいて復号を行い、ファイルMを生成する。

【0065】

分散処理手段134(第3分散処理手段)は、復号手段133が生成したファイルMを秘密分散する。例えば、分散処理手段134は、分散処理手段112とは異なる方法で(つまり、以前とは異なるファイルが生成されるように)ファイルMを2つに分割する。換言すると、分散処理手段134は、ファイルMを秘密分散して、ファイルM1、ファイルM2とは異なる、ファイルM1’とファイルM2’を生成する。そして、分散処理手段134は、生成したファイルM1’とファイルM2’を暗号化手段135に送信する。

【0066】

暗号化手段135(第3暗号化手段)は、暗号鍵(K)や暗号鍵(K”)を用いて、新たに秘密分散したファイルM1’、ファイルM2’を暗号化する。例えば、暗号化手段135は、暗号鍵(K)を用いてファイルM2’を暗号化する。つまり、暗号化手段135は、暗号鍵(K)によりファイルM2’を暗号化して、暗号化したファイルK(M2’)を生成する。また、暗号化手段135は、暗号鍵(K”)を用いてファイルM1’を暗号化する。つまり、暗号化手段135は、暗号鍵(K”)によりファイルM1’を暗号化して、暗号化したファイルK”(M1’)を生成する。そして、暗号化手段135は、暗号化したファイルK(M2’)や暗号化したファイルK”(M1’)に対して、対応するファイルK(M2)に埋め込まれていたコンテンツIDと同一のコンテンツID(Cid)

10

20

30

40

50

を埋め込む。なお、暗号化手段135は、利用履歴を示す利用履歴情報を暗号化したファイルK(M2')やファイルK"(M1')に埋め込むよう構成しても構わない。

【0067】

その後、暗号化手段135は、送受信手段131を介して、暗号化したファイルK"(M1')とコンテンツID(Cid)と受取側装置3のメールアドレス(ML__b)とを管理サーバ12に対して送信する。これにより、管理サーバ12側のコンテンツ情報1261の更新が行われることになる。なお、暗号化したファイルK(M2')は、例えば、受取側装置13が備える図示しない記憶装置に格納される。

【0068】

情報格納部136は、メモリやディスク装置などの記憶装置である。情報格納部136には、受取側装置13のメールアドレス(ML__b)が格納されている。情報格納部136には、状態情報(Im)が格納されていても構わない。

10

【0069】

以上が、情報共有システム1の構成の一例である。続いて、情報共有システム1により行われる情報送信方法の流れの一例について、図6乃至図15を参照して説明する。

【0070】

図6で示すように、送付側装置11は、ファイルMとパスワード(Pw)と受取側装置13のメールアドレス(ML__b)とを有している。また、管理サーバ12は、公開鍵(P__sv)と秘密鍵(S__sv)とを有している。また、受取側装置13は、状態情報(Im)と自身のメールアドレス(ML__b)とを有している。

20

【0071】

この状態において、送付側装置11の分散処理手段112は、図7、図13で示すように、ファイルMを秘密分散してファイルM1とファイルM2とを生成する(ステップS101)。そして、分散処理手段112は、秘密分散したファイルM1とファイルM2を暗号化手段114に送信する。

【0072】

また、送付側装置11の暗号鍵作成手段113は、パスワード(Pw)に基づいて暗号鍵(K)を作成する(ステップS102)。そして、暗号鍵作成手段113は、作成した暗号鍵(K)を暗号化手段114に送信する。

【0073】

30

暗号化手段114は、暗号鍵(K)を用いてファイルM1、ファイルM2を暗号化して、暗号化したファイルK(M1)、K(M2)を生成する。また、暗号化手段114は、一意に定まるコンテンツID(Cid)を、暗号化したファイルK(M1)、K(M2)に埋め込む(ステップS103)。

【0074】

また、暗号化手段114は、管理サーバ12から取得した公開鍵(P__sv)を用いて、暗号鍵(K)を暗号化して暗号化した暗号鍵P__sv(K)を生成する(ステップS104)。

【0075】

その後、送付側装置11は、暗号化したファイルK(M2)及びパスワード(Pw)を受取側装置13に送信する(ステップS105)。また、送付側装置11は、暗号化した暗号鍵P__sv(K)と暗号化したファイルK(M1)と受取側装置13のメールアドレス(ML__b)とを管理サーバ12に送信する(ステップS106)。

40

【0076】

続いて、図8、図13を参照すると、管理サーバ12は、送付側装置11が送信した、暗号化した暗号鍵P__sv(K)と暗号化したファイルK(M1)と受取側装置13のメールアドレス(ML__b)とを受信する。すると、管理サーバ12のコンテンツ情報管理手段125は、暗号化したファイルK(M1)からコンテンツID(Cid)を取り出して、コンテンツ情報1261のうちの新たに作成したレコードに、取り出したコンテンツID(Cid)を登録する(ステップS201)。

50

【0077】

また、管理サーバ12の復号手段122は、公開鍵・秘密鍵格納部127から取得した秘密鍵（S_{sv}）を用いて、暗号化した暗号鍵P_{sv}（K）を復号して暗号鍵（K）を取り出す（ステップS202）。そして、復号手段122は、取り出した暗号鍵（K）を用いて、暗号化したファイルK（M1）を復号してファイルM1を生成する（ステップS203）。その後、復号手段122は、生成したファイルM1を暗号化手段124に送信する。

【0078】

暗号鍵作成手段123は、復号手段122が取り出した暗号鍵（K）と、受信した受信側装置13のメールアドレス（ML_b）とに基づいて、暗号鍵（K'）を作成する（ステップS204）。そして、暗号鍵作成手段123は、作成した暗号鍵（K'）を暗号化手段124に送信する。

10

【0079】

暗号化手段124は、暗号鍵作成手段123から受信した暗号鍵（K'）を用いて、復号手段122から受信したファイルM1を暗号化して暗号化したファイルK'（M1）を生成する（ステップS205）。そして、暗号化手段124は、暗号化したファイルK'（M1）をコンテンツ情報管理手段125に送信する。

【0080】

コンテンツ情報管理手段125は、コンテンツ情報1261のうちの新たにコンテンツID（Cid）を登録した箇所と対応する箇所に、暗号化したファイルK'（M1）と受信側装置13のメールアドレス（ML_b）とを登録する（ステップS206）。その結果、図8で示すように、コンテンツ情報1261において、コンテンツID（Cid）とメールアドレス（ML_b）とファイルK'（M1）とが対応付けられることになる。

20

【0081】

図9、図14で示すように、送付側装置11から暗号化したファイルK（M2）及びパスワード（Pw）を受信した受取側装置13において、受取側装置13の利用者は、暗号化したファイルK（M2）を開こうとして、パスワード（Pw）を入力する。すると、受取側装置13は、入力されたパスワード（Pw）、自身のメールアドレス（ML_b）（例えば、情報共有システム1を利用する際に用いるプログラムに予め登録されている）、状態情報（Im）、開こうとしたファイル（暗号化したファイルK（M2））に埋め込まれているIDであるコンテンツID（Cid）を管理サーバ12に対して送信する（ステップS301）。

30

【0082】

上記情報を受取側装置13から受信すると、図10、図14で示すように、管理サーバ12の暗号鍵作成手段123は、受信したパスワード（Pw）に基づいて暗号鍵（K）を作成する（ステップS207）。また、暗号鍵作成手段123は、暗号鍵（K）と受信したメールアドレス（ML_b）とに基づいて、暗号鍵（K'）を作成する（ステップS208）。そして、暗号鍵作成手段123は、作成した暗号鍵（K'）を復号手段122に送信する。

【0083】

また、管理サーバ12のコンテンツ情報管理手段125は、受信したメールアドレス（ML_b）とコンテンツID（Cid）とに基づいて、コンテンツ情報1261に格納されているファイルを特定して取得する。つまり、コンテンツ情報管理手段125は、メールアドレス（ML_b）とコンテンツID（Cid）とに対応付けて格納されている、暗号化したファイルK'（M1）を取得する（ステップS209）。そして、コンテンツ情報管理手段125は、取得した暗号化したファイルK'（M1）を復号手段122に送信する。

40

【0084】

復号手段122は、暗号鍵作成手段123が作成した暗号鍵（K'）を用いて、暗号化したファイルK'（M1）を復号してファイルM1を生成する（ステップS210）。そ

50

して、復号手段122は、生成したファイルM1を暗号化手段124に送信する。

【0085】

また、暗号鍵作成手段123は、暗号鍵(K)とメールアドレス(ML__b)と状態情報(I m)とに基づいて、共通鍵である暗号鍵(K ")を作成する(ステップS211)。そして、暗号鍵作成手段123は、作成した暗号鍵(K ")を暗号化手段124に送信する。

【0086】

暗号化手段124は、暗号鍵作成手段123が作成した暗号鍵(K ")を用いて、復号手段122から受信したファイルM1を暗号化して暗号化したファイルK "(M1)を生成する(ステップS212)。

10

【0087】

その後、管理サーバ12は、送受信手段121を介して、受取側装置13に対して暗号化したファイルK "(M1)を送信する。また、管理サーバ12のコンテンツ情報管理手段125は、コンテンツ情報1261を更新する。つまり、コンテンツ情報1261においては、コンテンツID(C i d)とメールアドレス(ML__b)と暗号化したファイルK "(M1)とが対応付けられている状態となる。

【0088】

管理サーバ12から暗号化したファイルK "(M1)を受信すると、図11、図14で示すように、受取側装置13の暗号鍵作成手段132は、パスワード(P w)に基づいて暗号鍵(K)を作成し(ステップS302)、暗号鍵(K)、メールアドレス(ML__b)、状態情報(I m)から暗号鍵(K ")を作成する(ステップS303)。また、暗号鍵作成手段132は、暗号化鍵(K)と暗号鍵(K ")とを復号手段133に送信する。

20

【0089】

復号手段133は、受信した暗号鍵(K)を用いて、暗号化したファイルK (M2)の復号を行い、ファイルM2を生成する(ステップS304)。また、復号手段133は、受信した暗号鍵(K ")を用いて、暗号化したファイルK "(M1)の復号を行い、ファイルM1を生成する(ステップS305)。その後、復号手段133は、ファイルM1とファイルM2とからファイルMを生成する(ステップS306)。復号手段133は、例えばこのようにして、送付側装置11及び管理サーバ12から受信した情報に基づいて、ファイルMを生成する。

30

【0090】

その後、図12、図15で示すように、受取側装置13の分散処理手段134は、ファイルMを秘密分散してファイルM1'とファイルM2'を生成する(ステップS307)。そして、分散処理手段134は、生成したファイルM1'とファイルM2'を暗号化手段135に送信する。なお、ファイルMは生成後から秘密分散をする前に、ファイルの内容を更新されていても構わない。

【0091】

暗号化手段135は、暗号鍵(K)や暗号鍵(K ")を用いて、新たに秘密分散したファイルM1'、ファイルM2'を暗号化する。例えば、暗号化手段135は、暗号鍵(K)を用いてファイルM2'を暗号化して、暗号化したファイルK (M2')を生成する。また、暗号化手段135は、暗号鍵(K ")を用いてファイルM1'を暗号化して、暗号化したファイルK "(M1')を生成する。そして、暗号化手段135は、暗号化したファイルK (M2')や暗号化したファイルK "(M1')に対して、対応するファイルK (M2)に埋め込まれていたコンテンツIDと同一のコンテンツID(C i d)を埋め込む。なお、暗号化手段135は、利用履歴を示す利用履歴情報を暗号化したファイルK (M2')やファイルK "(M1')に埋め込むよう構成しても構わない(ステップS308)。

40

【0092】

その後、暗号化手段135は、暗号化したファイルK "(M1')とコンテンツID(C i d)と受取側装置3のメールアドレス(ML__b)とを管理サーバ12に対して送信

50

する（ステップS309）。上記情報を受信すると、管理サーバ12のコンテンツ情報管理手段125は、受信した情報に基づいてコンテンツ情報1261の更新を行う（ステップS214）。これにより、コンテンツ情報1261は、コンテンツID（Cid）とメールアドレス（ML_b）と暗号化したファイルK'（M1'）とを対応付けた状態となることになる。

【0093】

以上が、本実施形態における情報共有システム1により行われる情報送信方法の流れの一例である。

【0094】

このように、本実施形態における情報共有システム1の管理サーバ12は、暗号鍵作成手段123と暗号化手段124とを有している。このような構成により、管理サーバ12は、受取側装置13から受信した状態情報（Im）に基づいて暗号鍵（K'）を作成することが出来る。また、暗号化手段124は、送付側装置11から受信したファイルM1と、作成した暗号鍵（K'）とに基づいて、暗号化したファイルK'（M1）を作成することが出来る。これにより、管理サーバ12には、暗号化したファイルK'（M1）が格納されていることになる。その結果、仮に第三者にパスワード（Pw）が漏洩したとしても、当該パスワード（Pw）を取得した第三者による復号は行えないことになる。つまり、受取側装置13が利用した後では、第三者にパスワード（Pw）が流出したとしても、対応する状態情報（Im）を取得することが出来ないため、暗号化したファイルK'（M1）を復号することが出来なくなる。換言すると、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが可能となる。

【0095】

なお、仮に受取側装置13の利用前に第三者に利用された場合、受取側装置13の側から管理サーバ12に格納されている情報を復号することが出来なくなる。その結果、パスワード（Pw）などの情報の漏洩を早期に気づくことが可能となる。

【0096】

また、状態情報（Im）として環境特定情報を採用することで、正当な利用者であっても暗号化したファイルの利用場所などを特定することが可能となる。さらに、状態情報（Im）として操作者限定情報を採用することで、ファイルの復号を行う際の受取側装置13の操作者を特定することが可能となる。

【0097】

また、本実施形態における受取側装置13は、ファイルの復号を行った後、再度秘密分散して暗号化したファイルK'（M1'）を管理サーバ12に送信するよう構成されている。このような構成により、以前に秘密分散を行ったファイルに基づいて復号を行うことが出来なくなり、常に最新のファイルのみを利用可能とすることが可能となる。また、ファイルに利用履歴を埋め込むことで、ファイルの利用履歴をファイル内に管理することが可能となる。

【0098】

なお、本実施形態においては、送付側装置11は、秘密分散したファイルを管理サーバ12と受取側装置13とに送信するとした。しかしながら、送付側装置11は、秘密分散を行わずに、受取側装置13に送信したいファイルを管理サーバ12に送信するよう構成しても構わない。この場合、図16に示すように、暗号化したファイルK（M）が管理サーバ12に対して送信される一方、受取側装置13に対しては、パスワード（Pw）と対応するコンテンツID（Cid）とを含む所定の通知が送信されることになる。また、図17で示すように、当該通知を受けて受取側装置13から管理サーバ12に対して、パスワード（Pw）、メールアドレス（ML_b）、状態情報（Im）、コンテンツID（Cid）が送信される。すると、管理サーバ12の暗号鍵作成手段123は、受信したパスワード（Pw）に基づいて暗号鍵（K）を作成するとともに、暗号鍵（K）、メールアドレス（ML_b）、状態情報（Im）に基づいて暗号鍵（K'）を作成する。そして、復

号手段 1 2 2 により復号を行った後、暗号化手段 1 2 4 は、暗号鍵 (K ") を用いて、暗号化したファイル K " (M) を生成する。その結果、管理サーバ 1 2 には、暗号化したファイル K " (M) が格納されている状態となることになる。このような秘密分散しない構成であっても、本実施形態において説明した効果と同様の効果を得ることが出来る。なお、管理サーバ 1 2 としての機能を送付側装置 1 1 が有するよう構成しても構わない (送付側装置 1 1 と管理サーバ 1 2 とを一体的に構成しても構わない)。

【0099】

また、本実施形態においては、暗号鍵作成手段 1 2 3 や暗号鍵作成手段 1 3 2 は、暗号鍵 (K)、メールアドレス (ML__b)、状態情報 (Im) に基づいて暗号鍵 (K ") を作成するとした。しかしながら、暗号鍵作成手段 1 2 3 や暗号鍵作成手段 1 3 2 は、状態情報 (Im) を用いていれば、上記方法以外により暗号鍵 (K ") を作成しても構わない。例えば、暗号鍵作成手段 1 2 3 や暗号鍵作成手段 1 3 2 は、暗号鍵 (K ')、メールアドレス (ML__b)、状態情報 (Im) に基づいて暗号鍵 (K ") を作成するよう構成することが出来る。

10

【0100】

暗号文を復号するための鍵を安全にデータの共有相手に渡すために、鍵の配布ないし発行が可能な認証サーバにデータの共有相手を登録することも従来行われていた。本実施形態によれば、鍵配布の目的のために鍵配布ないし鍵発行が可能な認証サーバにデータの共有相手を登録することが不要となる効果が得られる。また、本実施形態によれば、鍵配布ないし鍵発行が可能な認証サーバを、暗号文を復号するための鍵を安全にデータの共有相手に渡す目的で設置することが不要となる効果が得られる。

20

【0101】

[第2の実施形態]

次に、図 1 8 乃至図 2 0 を参照して、本発明の第 2 の実施形態について説明する。第 2 の実施形態では、送付側装置 2 1 から管理サーバ 2 2 を介して受取側装置 2 3 に対して情報を送信する情報共有システム 2 や管理サーバ 3、受取側装置 4 の構成の概要について説明する。

【0102】

図 1 8 を参照すると、本実施形態における情報共有システム 2 は、送付側装置 2 1 と管理サーバ 2 2 と受取側装置 2 3 とを有している。図 1 8 で示すように、送付側装置 2 1 と管理サーバ 2 2 とは、互いに通信可能なよう接続されている。また、管理サーバ 2 2 と受取側装置 2 3 とは、互いに通信可能なよう接続されている。

30

【0103】

管理サーバ 2 2 は、第 1 送受信手段 2 2 1 と、第 1 暗号鍵作成手段 2 2 2 と、第 1 暗号化手段 2 2 3 と、を有している。管理サーバ 2 2 は、例えば、図示しない演算装置と記憶装置とを有しており、記憶装置が有するプログラムを演算装置が実行することで、上記各手段を実現する。

【0104】

第 1 送受信手段 2 2 1 は、第 1 の暗号鍵により暗号化された第 1 の暗号文を送付側装置 2 1 から受信するとともに、受取側装置 2 3 から受取側装置 2 3 の状態を示す情報である状態情報を受信する。

40

【0105】

第 1 暗号鍵作成手段 2 2 2 は、第 1 送受信手段 2 2 1 が受信した状態情報に基づいて、第 2 の暗号鍵を作成する。そして、第 1 暗号鍵作成手段 2 2 2 は、作成した第 2 の暗号鍵を第 1 暗号化手段 2 2 3 に送信する。

【0106】

第 1 暗号化手段 2 2 3 は、第 1 暗号鍵作成手段 2 2 2 が作成した第 2 の暗号鍵と、第 1 の暗号文と、に基づいて第 2 の暗号文を作成する。第 1 暗号化手段 2 2 3 が作成した第 2 の暗号文は、第 1 送受信手段 2 2 1 を介して受取側装置 2 3 に対して送信されることになる。

50

【0107】

このように、本実施形態における情報共有システム2は、送付側装置21と管理サーバ22と受取側装置23とを有している。また、管理サーバ22は、第1送受信手段221と第1暗号鍵作成手段222と第1暗号化手段223とを有している。このような構成により、管理サーバ22の第1暗号鍵作成手段222は、受取側装置23から受信した状態情報に基づいて第2の暗号鍵を作成することが出来る。また、第1暗号化手段223は、送付側装置21から受信した第1の暗号文と、作成した第2の暗号鍵とに基づいて、第2の暗号文を作成することが出来る。これにより、管理サーバ22には、第2の暗号文が格納されていることになる。その結果、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが可能となる。

10

【0108】

また、上述した情報共有システム2が作動することにより実行される情報送信方法は、送付側装置から管理サーバを介して受取側装置に対して情報を送信する情報送信方法であって、管理サーバは、第1の暗号鍵により暗号化された第1の暗号文を送付側装置から受信し、受取側装置から当該受取側装置の状態を示す情報である状態情報を受信し、受信した状態情報に基づいて作成した第2の暗号鍵と、第1の暗号文と、に基づいて作成した第2の暗号文を受取側装置に対して送信する、という方法である。

【0109】

上述した構成を有する情報送信方法の発明であっても、上記情報共有システム2と同様の作用を有するために、上述した本発明の目的を達成することが出来る。

20

【0110】

また、上記情報共有システム2と同様の目的を達成することの出来る管理サーバ3の構成の一例を図19に示す。図19を参照すると、管理サーバ3は、第1送受信手段31と第1暗号鍵作成手段32と第1暗号化手段33とを有している。管理サーバ3は、例えば、図示しない演算装置と記憶装置とを有しており、記憶装置が有するプログラムを演算装置が実行することで、上記各手段を実現する。なお、第1送受信手段31は上述した第1送受信手段221に対応し、第1暗号鍵作成手段32は第1暗号鍵作成手段222に対応し、第1暗号化手段33は第1暗号化手段223に対応する。そのため、各手段の説明は省略する。

【0111】

30

また、上記管理サーバ3は、当該管理サーバ3に所定のプログラムが組み込まれることで実現できる。具体的に、本発明の他の形態であるプログラムは、管理サーバに、第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信し、受取側装置の状態を示す状態情報を受信し、受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する、処理を実現するためのプログラムである。

【0112】

また、上述した管理サーバ3が作動することにより実行される情報処理方法は、管理サーバにより行われる情報処理方法であって、第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信し、受取側装置の状態を示す状態情報を受信し、受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する、という方法である。

40

【0113】

上述した構成を有する、プログラム、又は、情報処理方法、の発明であっても、上記管理サーバ3と同様の作用を有するために、上述した本発明の目的を達成することが出来る。

【0114】

また、上記情報共有システム2と同様の目的を達成することの出来る受取側装置4の構成の一例を図20に示す。図20を参照すると、受取側装置4は、送受信手段41と、復号手段42と、を有している。受取側装置4は、例えば、図示しない演算装置と記憶装置

50

とを有しており、記憶装置が有するプログラムを演算装置が実行することで、上記各手段を実現する。

【0115】

送受信手段41は、復号の対象である暗号文を有する管理サーバに対して、受取側装置4の状態を示す情報である状態情報を送信する。また、送受信手段41は、管理サーバから、送信した状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を受信する。

【0116】

復号手段42は、送受信手段41が受信した暗号文を復号する。受取側装置4は状態情報を有しているため、当該状態情報に基づいて暗号鍵を作成することが可能であり、当該作成した暗号鍵を用いて、送受信手段41が受信した暗号文を復号することになる。

10

【0117】

このように、本実施形態における受取側装置4は、送受信手段41と復号手段42とを有している。このような構成により、受取側装置4は、復号の対象である暗号文を有する管理サーバに対して状態情報を送信し、管理サーバから、送信した状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を受信することになる。また、復号手段により復号することになる。これにより、管理サーバには、状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文が格納されることになる。その結果、事前にデータの共有相手に鍵を配布することなく目的の相手以外が暗号化したファイルを復号出来ないようにすることが可能となる。

20

【0118】

また、上記受取側装置4は、当該受取側装置4に所定のプログラムが組み込まれることで実現できる。具体的に、本発明の他の形態であるプログラムは、受取側装置に、復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、管理サーバから、送信した状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する、処理を実現させるためのプログラムである。

【0119】

また、上述した受取側装置4が作動することにより実行される復号方法は、受取側装置により行われる復号方法であって、復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、管理サーバから、送信した状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する、という方法である。

30

【0120】

上述した構成を有する、プログラム、又は、復号方法、の発明であっても、上記受取側装置4と同様の作用を有するために、上述した本発明の目的を達成することが出来る。

【0121】

<付記>

上記実施形態の一部又は全部は、以下の付記のようにも記載されうる。以下、本発明における情報送信方法などの概略を説明する。但し、本発明は、以下の構成に限定されない。

40

【0122】

(付記1)

送付側装置から管理サーバを介して受取側装置に対して情報を送信する情報送信方法であって、

前記管理サーバは、

第1の暗号鍵により暗号化された第1の暗号文を送付側装置から受信し、

前記受取側装置から当該受取側装置の状態を示す情報である状態情報を受信し、

受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する

50

情報送信方法。

【0123】

(付記2)

付記1に記載の情報送信方法であって、

前記管理サーバは、前記状態情報として、前記第2の暗号文の復号を行う装置を特定する情報である装置特定情報を受信する

情報送信方法。

【0124】

(付記3)

付記1又は2に記載の情報送信方法であって、

前記管理サーバは、前記状態情報として、前記第2の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する

情報送信方法。

【0125】

(付記4)

付記1乃至3のいずれかに記載の情報送信方法であって、

前記管理サーバは、前記状態情報として、前記受取側装置の操作者を特定する情報である操作者特定情報を受信する

情報送信方法。

【0126】

(付記5)

付記1乃至4のいずれかに記載の情報送信方法であって、

前記送付側装置は、前記受取側装置に対して送信する情報を秘密分散により2つに分割し、一方を第1の暗号鍵により暗号化した後、第1の暗号文として前記管理サーバに送信し、他方を第1の暗号鍵により暗号化した後、第3の暗号文として前記受取側装置に送信し、

前記受取側装置は、前記管理サーバから受信した前記第2の暗号文と、前記送付側装置から受信した前記第3の暗号文と、に基づいて復号を行い、前記送付側装置が送信する情報を取得する

情報送信方法。

【0127】

(付記6)

付記5に記載の情報送信方法であって、

前記受取側装置は、前記第3の暗号文の復号を行う際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから前記第2の暗号文を受信する

情報送信方法。

【0128】

(付記7)

付記5又は6に記載の情報送信方法であって、

前記受取側装置は、前記送付側装置が送信する情報を取得した後、当該取得した情報を秘密分散して2つに分割し、当該分割したうちの一方を前記第2の暗号鍵に基づいて暗号化した後、前記管理サーバに送信する

情報送信方法。

【0129】

(付記8)

付記1乃至7のいずれかに記載の情報送信方法であって、

前記管理サーバは、

前記第1の暗号文を前記送付側装置から受信するとともに前記第1の暗号鍵を前記送付側装置から受信し、前記第1の暗号鍵に基づいて作成した第3の暗号鍵と前記第1の暗号文とに基づいて、前記第1の暗号文に基づく暗号文を作成して格納し、

前記受取側装置から前記状態情報を受信すると、前記第2の暗号鍵と、前記第1の暗号文に基づく暗号文と、に基づいて作成した前記第2の暗号文を前記受取側装置に対して送信する

情報送信方法。

【0130】

(付記1A)

送付側装置から管理サーバを介して受取側装置に対して情報を送信する情報共有システムであって、

前記管理サーバは、

第1の暗号鍵により暗号化された第1の暗号文を送付側装置から受信するとともに、前記受取側装置から当該受取側装置の状態を示す情報である状態情報を受信する第1送受信手段と、

受信した前記状態情報に基づいて第2の暗号鍵を作成する第1暗号鍵作成手段と、

前記第2の暗号鍵と、前記第1の暗号文と、に基づいて第2の暗号文を作成する第1暗号化手段と、

を有し、作成した第2の暗号文を、前記第1送受信手段を介して前記受取側装置に対して送信するよう構成されている

情報共有システム。

【0131】

(付記2A)

付記1Aに記載の情報共有システムであって、

前記第1送受信手段は、前記状態情報として、前記第2の暗号文の復号を行う装置を特定する情報である装置特定情報を受信する

情報共有システム。

【0132】

(付記3A)

付記1A又は2Aに記載の情報共有システムであって、

前記第1送受信手段は、前記状態情報として、前記第2の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する

情報共有システム。

【0133】

(付記4A)

付記1A乃至3Aのいずれかに記載の情報共有システムであって、

前記第1送受信手段は、前記状態情報として、前記受取側装置の操作者を特定する情報である操作者特定情報を受信する

情報共有システム。

【0134】

(付記5A)

付記1A乃至4Aのいずれかに記載の情報共有システムであって、

前記送付側装置は、前記受取側装置に対して送信する情報を秘密分散により2つに分割する第2分散処理手段と、前記第2分散処理手段が分割したうちの一方を第1の暗号鍵により暗号化するとともに、他方を第1の暗号鍵により暗号化する第2暗号化手段と、を有し、前記第2暗号化手段が暗号化したうちの一方を第1の暗号文として前記管理サーバに送信し、他方を第3の暗号文として前記受取側装置に送信するよう構成され、

前記受取側装置は、前記管理サーバから受信した前記第2の暗号文と、前記送付側装置から受信した前記第3の暗号文と、に基づいて復号を行い、前記送付側装置が送信する情報を取得する復号手段を有する

情報共有システム。

【0135】

(付記6A)

10

20

30

40

50

付記 5 A に記載の情報共有システムであって、

前記復号手段は、前記第 3 の暗号文の復号を行う際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから前記第 2 の暗号文を受信する
情報共有システム。

【0136】

(付記 7 A)

付記 5 A 又は 6 A に記載の情報共有システムであって、

前記受取側装置は、前記復号手段により前記送付側装置が送信する情報を取得した後、当該取得した情報を秘密分散して 2 つに分割する第 3 分散処理手段と、当該分割したうちの一方を前記第 2 の暗号鍵に基づいて暗号化する第 3 暗号化手段と、を有し、前記第 2 の暗号鍵に基づいて暗号化した暗号文を前記管理サーバに送信するよう構成されている
情報共有システム。

10

【0137】

(付記 8 A)

付記 1 A 乃至 7 A のいずれかに記載の情報共有システムであって、

前記第 1 送受信手段は、前記第 1 の暗号文を前記送付側装置から受信するとともに前記第 1 の暗号鍵を前記送付側装置から受信し、前記第 1 暗号鍵作成手段は、前記第 1 の暗号鍵に基づいて第 3 の暗号鍵を作成し、前記第 1 暗号化手段は、前記第 3 の暗号鍵と前記第 1 の暗号文とに基づいて、前記第 1 の暗号文に基づく暗号文を作成するよう構成され、前記管理サーバは、前記第 1 暗号化手段が作成した前記第 1 の暗号文に基づく暗号文を格納するよう構成され、

20

前記第 1 暗号化手段は、前記第 1 送受信手段が前記受取側装置から前記状態情報を受信すると、前記第 2 の暗号鍵と、前記第 1 の暗号文に基づく暗号文と、に基づいて前記第 2 の暗号文を作成し、作成した前記第 2 の暗号文を前記受取側装置に対して送信するよう構成されている
情報共有システム。

【0138】

(付記 9)

管理サーバにより行われる情報処理方法であって、

第 1 の暗号鍵により暗号化された第 1 の暗号文を外部装置から受信し、

30

受取側装置の状態を示す状態情報を受信し、

受信した前記状態情報に基づいて作成した第 2 の暗号鍵と、前記第 1 の暗号文と、に基づいて作成した第 2 の暗号文を前記受取側装置に対して送信する
情報処理方法。

【0139】

(付記 10)

付記 9 に記載の情報処理方法であって、

前記状態情報として、前記第 2 の暗号文の復号を行う装置を特定する情報である装置特定情報を受信する

情報処理方法。

40

【0140】

(付記 11)

付記 9 又は 10 に記載の情報処理方法であって、

前記状態情報として、前記第 2 の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する

情報処理方法。

【0141】

(付記 12)

付記 9 乃至 11 のいずれかに記載の情報処理方法であって、

前記第 1 の暗号文を受信するとともに前記第 1 の暗号鍵を外部装置から受信し、前記第

50

1の暗号鍵に基づいて作成した第3の暗号鍵と前記第1の暗号文とに基づいて、前記第1の暗号文を暗号化して格納し、

前記受取側装置から前記状態情報を受信すると、前記第2の暗号鍵と、暗号化された前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する情報処理方法。

【0142】

(付記9A)

第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信するとともに、受取側装置から当該受取側装置の状態を示す情報である状態情報を受信する第1送受信手段と、

受信した前記状態情報に基づいて第2の暗号鍵を作成する第1暗号鍵作成手段と、

前記第2の暗号鍵と、前記第1の暗号文と、に基づいて第2の暗号文を作成する第1暗号化手段と、

を有し、作成した第2の暗号文を、前記第1送受信手段を介して前記受取側装置に対して送信するよう構成されている

管理サーバ。

【0143】

(付記10A)

付記9Aに記載の管理サーバであって、

前記第1送受信手段は、前記状態情報として、前記第2の暗号文の復号を行う装置を特定する情報である装置特定情報を受信する

管理サーバ。

【0144】

(付記11A)

付記9A又は10Aに記載の管理サーバであって、

前記第1送受信手段は、前記状態情報として、前記第2の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する

管理サーバ。

【0145】

(付記12A)

付記9A乃至11Aのいずれかに記載の管理サーバであって、

前記第1送受信手段は、前記第1の暗号文を前記外部装置から受信するとともに前記第1の暗号鍵を前記外部装置から受信し、前記第1暗号鍵作成手段は、前記第1の暗号鍵に基づいて第3の暗号鍵を作成し、前記第1暗号化手段は、前記第3の暗号鍵と前記第1の暗号文とに基づいて、前記第1の暗号文に基づく暗号文を作成するよう構成され、前記第1暗号化手段が作成した前記第1の暗号文に基づく暗号文を格納するよう構成され、

前記第1暗号化手段は、前記第1送受信手段が前記受取側装置から前記状態情報を受信すると、前記第2の暗号鍵と、前記第1の暗号文に基づく暗号文と、に基づいて前記第2の暗号文を作成し、作成した前記第2の暗号文を前記受取側装置に対して送信するよう構成されている

管理サーバ。

【0146】

(付記13)

管理サーバに、

第1の暗号鍵により暗号化された第1の暗号文を外部装置から受信し、

受取側装置の状態を示す状態情報を受信し、

受信した前記状態情報に基づいて作成した第2の暗号鍵と、前記第1の暗号文と、に基づいて作成した第2の暗号文を前記受取側装置に対して送信する

処理を実現するためのプログラム。

【0147】

(付記 14)

付記 14 に記載のプログラムであって、

前記状態情報として、前記第 2 の暗号文の復号を行う装置を特定する情報である装置特定情報を受信するプログラム。

【0148】

(付記 15)

付記 13 又は 14 に記載のプログラムであって、

前記状態情報として、前記第 2 の暗号文の復号を行う装置の環境を特定する情報である環境特定情報を受信する

プログラム。

【0149】

(付記 16)

付記 13 乃至 15 のいずれかに記載のプログラムであって、

前記第 1 の暗号文を受信するとともに前記第 1 の暗号鍵を外部装置から受信し、前記第 1 の暗号鍵に基づいて作成した第 3 の暗号鍵と前記第 1 の暗号文とに基づいて、前記第 1 の暗号文を暗号化して格納し、

前記受取側装置から前記状態情報を受信すると、前記第 2 の暗号鍵と、暗号化された前記第 1 の暗号文と、に基づいて作成した第 2 の暗号文を前記受取側装置に対して送信するプログラム。

【0150】

(付記 17)

受取側装置により行われる復号方法であって、

復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、

前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する復号方法。

【0151】

(付記 18)

付記 17 に記載の復号方法であって、

前記状態情報として、前記受取側装置を特定する情報である装置特定情報を送信する復号方法。

【0152】

(付記 19)

付記 17 又は 18 に記載の復号方法であって、

前記状態情報として、前記受取側装置の環境を特定する情報である環境特定情報を送信する

復号方法。

【0153】

(付記 20)

付記 17 乃至 19 のいずれかに記載の復号方法であって、

外部装置から暗号文を受信し、受信した当該暗号文を復号する際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから、前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、

前記管理サーバから受信した暗号文と、前記外部装置から受信した暗号文と、に基づいて復号を行う

復号方法。

【0154】

(付記 21)

10

20

30

40

50

付記 20 に記載の復号方法であって、

復号を行った後、当該復号により取得した情報を秘密分散して 2 つに分割し、当該分割したうちの一方を前記状態情報に基づいて作成される暗号鍵に基づいて暗号化した後、前記管理サーバに送信する

復号方法。

【0155】

(付記 17 A)

復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を受信する送受信手段と、

前記送受信手段が受信した暗号文を復号する復号手段と、

を有する

受取側装置。

【0156】

(付記 18 A)

付記 17 A に記載の受取側装置であって、

前記送受信手段は、前記状態情報として、前記受取側装置を特定する情報である装置特定情報を送信する

受取側装置。

【0157】

(付記 19 A)

付記 17 A 又は 18 A に記載の受取側装置であって、

前記送受信手段は、前記状態情報として、前記受取側装置の環境を特定する情報である環境特定情報を送信する

受取側装置。

【0158】

(付記 20 A)

付記 17 A 乃至 19 A のいずれかに記載の受取側装置であって、

前記送受信手段は、外部装置から暗号文を受信し、受信した当該暗号文を復号する際に、前記管理サーバに対して前記状態情報を送信し、前記管理サーバから、前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を受信し、

前記復号手段は、前記管理サーバから受信した暗号文と、前記外部装置から受信した暗号文と、に基づいて復号を行う

受取側装置。

【0159】

(付記 21 A)

付記 20 A に記載の受取側装置であって、

前記復号手段により復号を行った後、当該復号により取得した情報を秘密分散して 2 つに分割する第 3 分散処理手段と、前記第 3 分散処理手段により分割したうちの一方を前記状態情報に基づいて作成される暗号鍵に基づいて暗号化する第 3 暗号化手段と、を有し、前記第 3 暗号化手段により暗号化した情報を管理サーバに送信するよう構成されている

受取側装置。

【0160】

(付記 22)

受取側装置に、

復号の対象である暗号文を有する管理サーバに対して、当該受取側装置の状態を示す情報である状態情報を送信し、

前記管理サーバから、送信した前記状態情報に基づいて作成される暗号鍵に基づいて暗号化された暗号文を取得し、当該取得した暗号文を復号する

処理を実現させるためのプログラム。

10

20

30

40

50

【0161】

(付記23)

付記22に記載のプログラムであって、
前記状態情報として、前記受取側装置を特定する情報である装置特定情報を送信する
プログラム。

【0162】

(付記24)

付記22又は23に記載のプログラムであって、
前記状態情報として、前記受取側装置の環境を特定する情報である環境特定情報を送信
する
プログラム。

10

【0163】

(付記25)

付記22乃至24のいずれかに記載のプログラムであって、
外部装置から暗号文を受信し、受信した当該暗号文を復号する際に、前記管理サーバに
対して前記状態情報を送信し、前記管理サーバから、前記状態情報に基づいて作成される
暗号鍵に基づいて暗号化された暗号文を取得し、
前記管理サーバから受信した暗号文と、前記外部装置から受信した暗号文と、に基づい
て復号を行う
プログラム。

20

【0164】

(付記26)

付記25に記載のプログラムであって、
復号を行った後、当該復号により取得した情報を秘密分散して2つに分割し、当該分割
したうちの一方を前記状態情報に基づいて作成される暗号鍵に基づいて暗号化した後、前
記管理サーバに送信する
プログラム。

【0165】

なお、上記各実施形態及び付記において記載したプログラムは、記憶装置に記憶されて
いたり、コンピュータが読み取り可能な記録媒体に記録されていたりする。例えば、記録
媒体は、フレキシブルディスク、光ディスク、光磁気ディスク、及び、半導体メモリ等の
可搬性を有する媒体である。

30

【0166】

以上、上記各実施形態を参照して本願発明を説明したが、本願発明は、上述した実施形
態に限定されるものではない。本願発明の構成や詳細には、本願発明の範囲内で当業者が
理解しうる様々な変更をすることが出来る。

【符号の説明】

【0167】

- 1 情報共有システム
- 11 送付側装置
- 111 送受信手段
- 112 分散処理手段
- 113 暗号鍵作成手段
- 114 暗号化手段
- 115 情報格納部
- 12 管理サーバ
- 121 送受信手段
- 122 復号手段
- 123 暗号鍵作成手段
- 124 暗号化手段

40

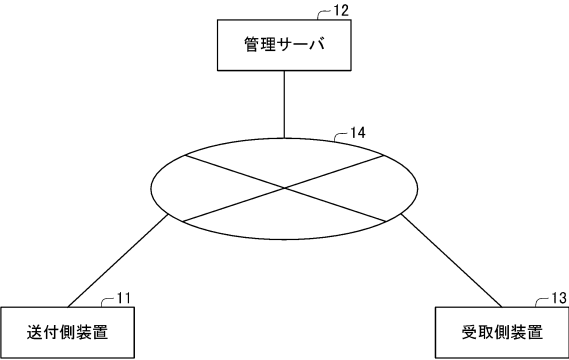
50

- 1 2 5 コンテンツ情報管理手段
- 1 2 6 コンテンツ情報格納部
- 1 2 6 1 コンテンツ情報
- 1 2 7 公開鍵・秘密鍵格納部
- 1 3 受取側装置
- 1 3 1 送受信手段
- 1 3 2 暗号鍵作成手段
- 1 3 3 復号手段
- 1 3 4 分散処理手段
- 1 3 5 暗号化手段
- 1 3 6 情報格納部
- 2 情報共有システム
- 2 1 送付側装置
- 2 2 管理サーバ
- 2 2 1 第1送受信手段
- 2 2 2 第1暗号鍵作成手段
- 2 2 3 第1暗号化手段
- 2 3 受取側装置
- 3 管理サーバ
- 3 1 第1送受信手段
- 3 2 第1暗号鍵作成手段
- 3 3 第1暗号化手段
- 4 受取側装置
- 4 1 送受信手段
- 4 2 復号手段

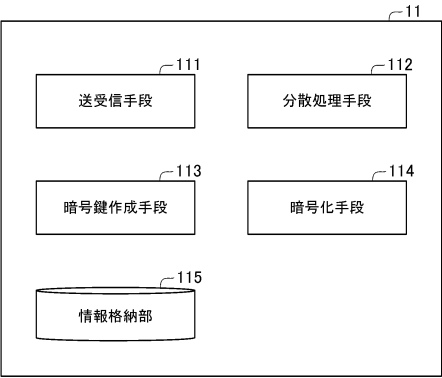
10

20

【図 1】

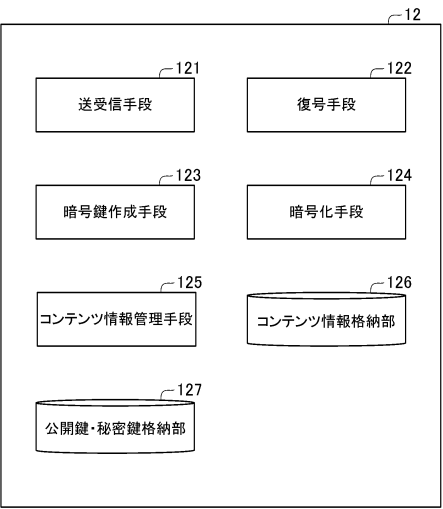


【図 2】

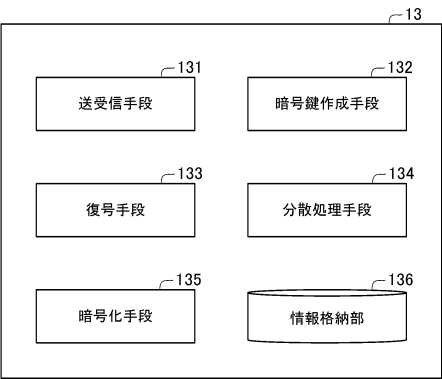


1

【図 3】



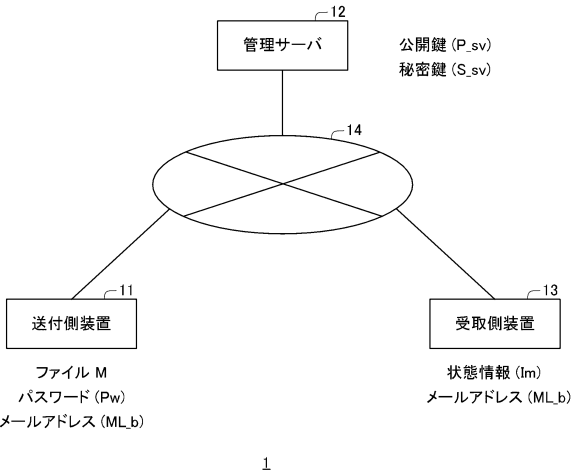
【図 5】



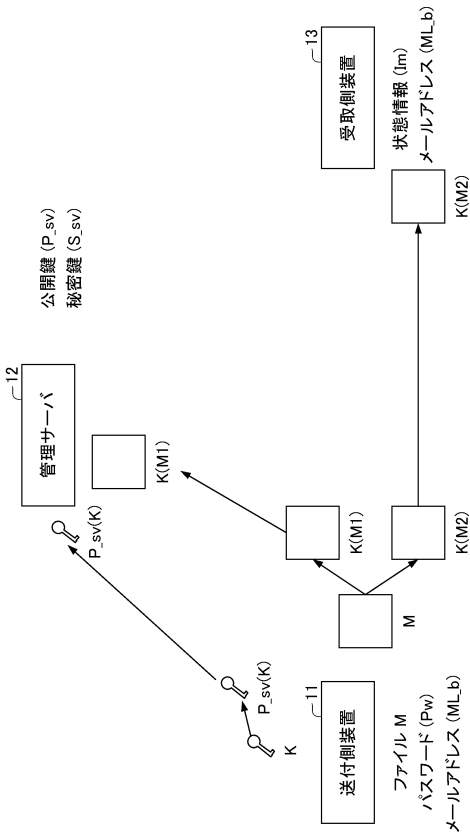
【図 4】

コンテンツID	メールアドレス	ファイル
A	a	α
B	b	β
⋮	⋮	⋮

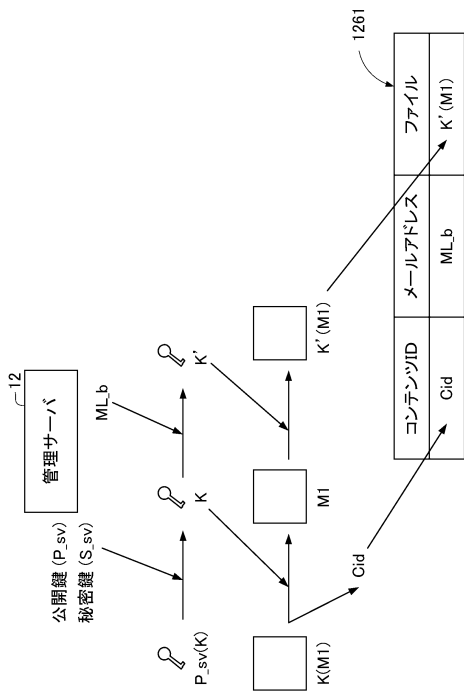
【図 6】



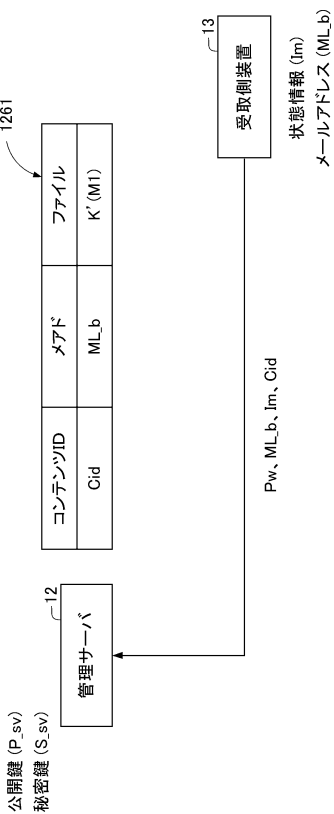
【図 7】



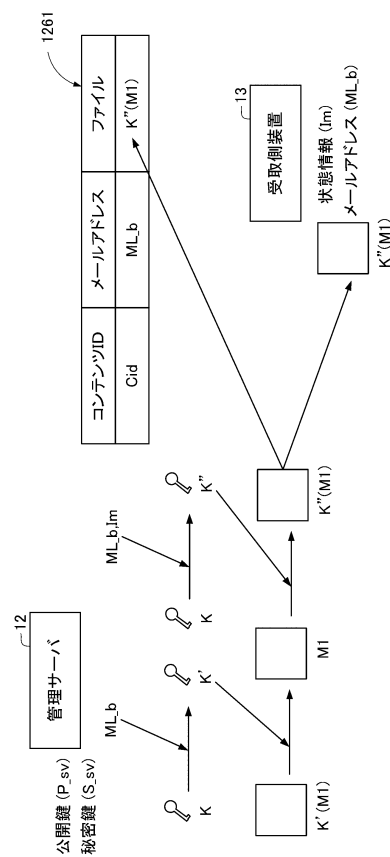
【図 8】



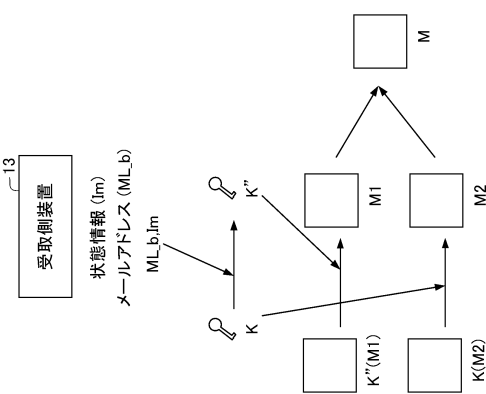
【図 9】



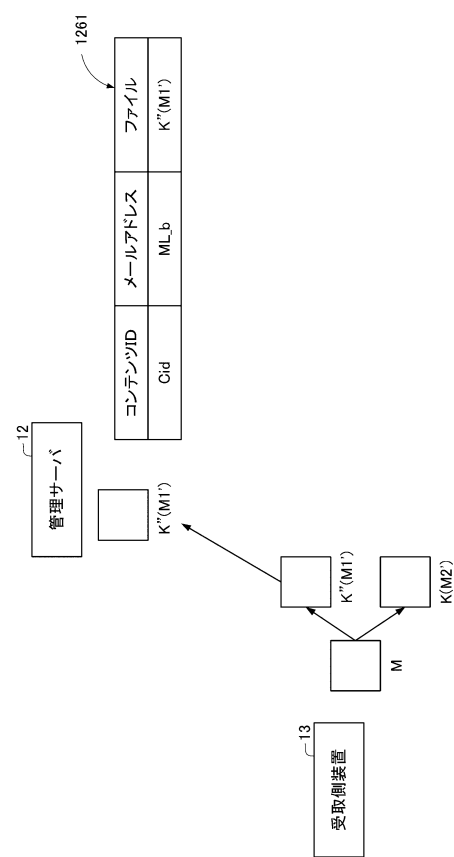
【図 10】



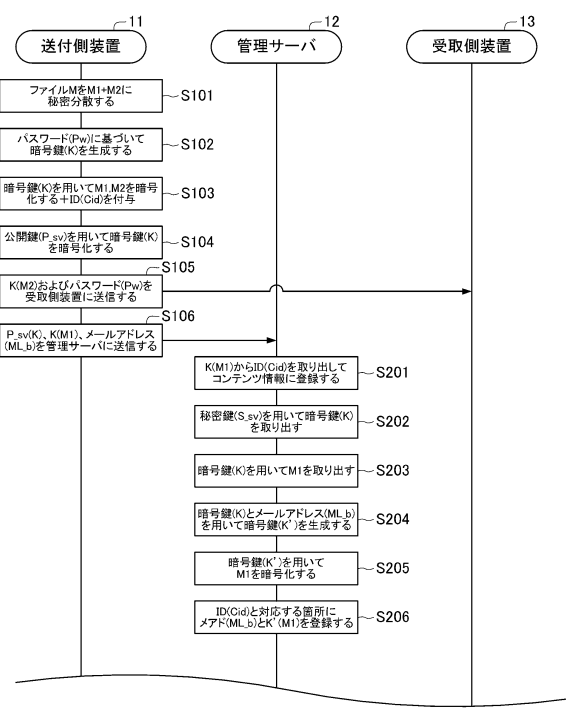
【図 11】



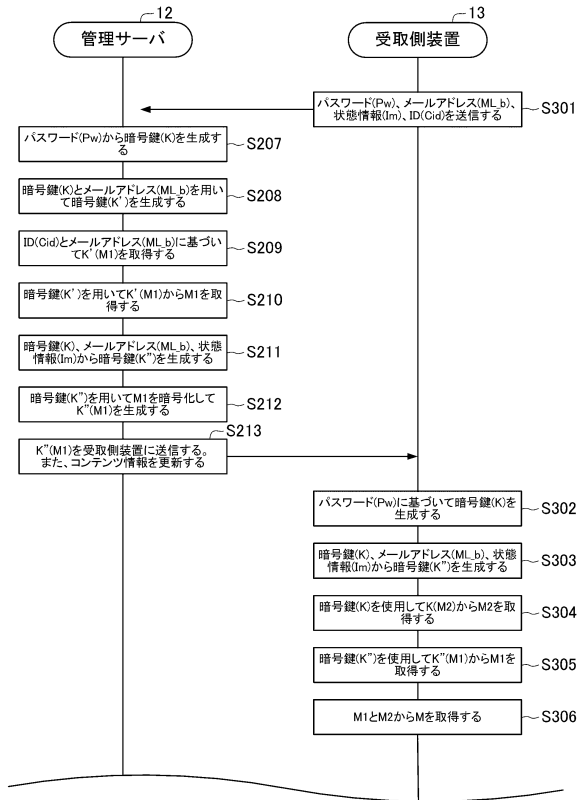
【図 12】



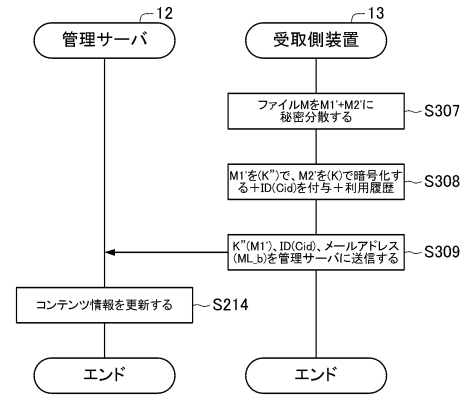
【図 13】



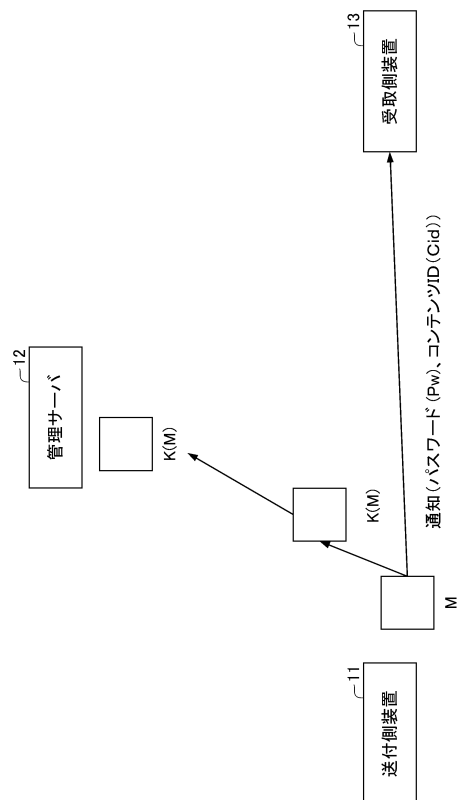
【図 14】



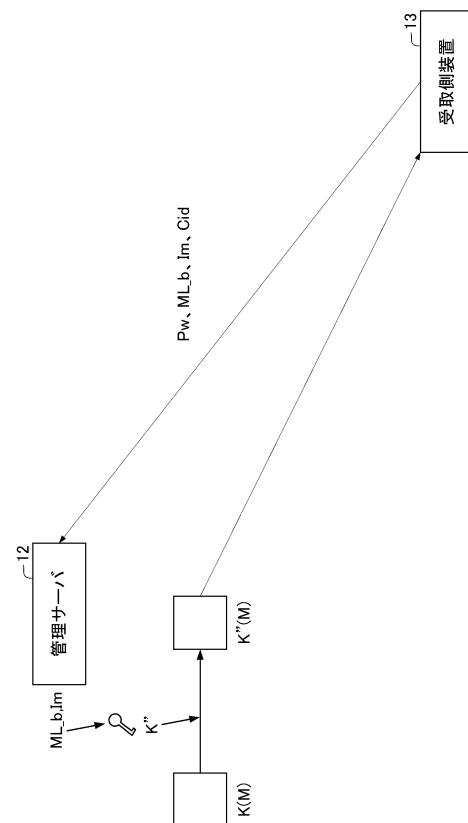
【図 15】



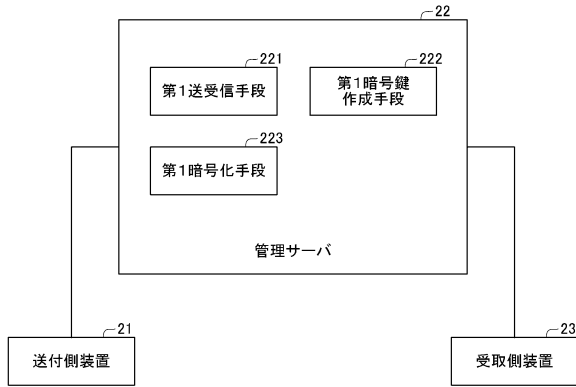
【図 16】



【図 17】

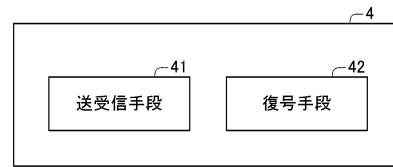


【図 18】

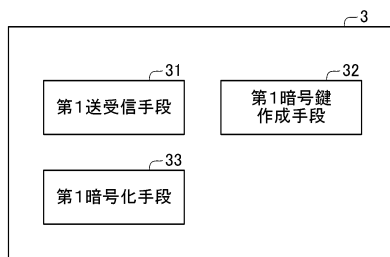


2

【図 20】



【図 19】



フロントページの続き

- (56)参考文献 国際公開第2012/111714 (WO, A1)
特開2006-197640 (JP, A)
国際公開第00/045358 (WO, A1)
特開2014-016584 (JP, A)
特開2013-157765 (JP, A)
特開2006-099697 (JP, A)
国際公開第2016/088250 (WO, A1)
米国特許出願公開第2015/0281193 (US, A1)

- (58)調査した分野(Int.Cl., DB名)
H04L 9/08