(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4104315号
(P4104315)

(45)発行日　平成20年6月18日(2008.6.18)　(24)登録日　平成20年4月4日(2008.4.4)

(51)Int.Cl.		F I		
H04L 9/10	(2006.01)	H04L	9/00	621A
G06F 12/14	(2006.01)	G06F	12/14	320B
G09C 1/00	(2006.01)	G06F	12/14	320F
H04H 20/00	(2008.01)	G09C	1/00	660E
H04L 9/08	(2006.01)	H04H	1/00	F

請求項の数 7　(全 21 頁)　最終頁に続く

(21)出願番号　特願2001-311039(P2001-311039)
(22)出願日　平成13年10月9日(2001.10.9)
(62)分割の表示　特願平9-181186の分割
原出願日　平成9年7月7日(1997.7.7)
(65)公開番号　特開2002-190797(P2002-190797A)
(43)公開日　平成14年7月5日(2002.7.5)
審査請求日　平成16年7月6日(2004.7.6)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(74)代理人　100084032
弁理士　三品　岩男
(72)発明者　伊藤　浩道
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】鍵管理システム、鍵管理装置、情報暗号化装置、情報復号化装置、およびプログラムを記憶した記憶媒体

(57)【特許請求の範囲】

【請求項１】

暗号鍵を用いて情報を暗号化する情報暗号化装置と、復号鍵を用いて情報を復号化する情報復号化装置と、前記情報暗号化装置および前記情報復号化装置で用いる暗号鍵および復号鍵を管理する鍵管理装置と、を備えた鍵管理システムであって、

前記鍵管理装置は、

少なくとも１組の暗号鍵および復号鍵が当該復号鍵の公開日あるいは公開日時に対応付けられて登録された管理テーブルを記憶する管理テーブル記憶手段と、

前記情報暗号化装置より送られてきた日時情報が示す日あるいは日時を公開日あるいは公開日時とする復号鍵と対の暗号鍵を、前記管理テーブルから検索する鍵検索手段と、

前記鍵検索手段で検索した暗号鍵を、前記情報暗号化装置に送信する暗号鍵送信手段と、

前記管理テーブルを参照することで、現在の日あるいは日時を公開日あるいは公開日時とする復号鍵を特定し、当該復号鍵を公開する復号鍵公開手段と、を備えており、

前記情報暗号化装置は、

暗号化すべき情報の機密性が解除される日あるいは日時に関する復号許可日時情報を、前記鍵管理装置に送信する日時情報送信手段と、

前記鍵管理装置より送られてきた、前記日時情報送信手段が送信した日時情報で特定される日あるいは日時に公開される復号鍵に対応する暗号鍵を、受信する暗号鍵受信手段と、

前記暗号鍵受信手段で受信した暗号鍵を用いて、前記暗号化すべき情報を暗号化する暗号化手段と、

前記暗号化手段で暗号化された情報に、当該情報の復号許可日時情報を付与して暗号化情報を作成し、当該暗号化情報を、当該日時情報が示す日あるいは日時に先立って前記情報復号化装置に配布する暗号化情報作成手段と、を備えており、
前記情報復号化装置は、
前記情報暗号化装置によって配布された暗号化情報を取得する暗号化情報取得手段と、
現在日時を取得し、現在日時と、復号許可日時とを比較し、
その結果、現在日時が復号許可日時以降である場合は、
復号鍵を、当該鍵管理装置から取得する復号鍵取得手段と、
現在日時が復号許可日時よりも前の日時である場合は、
情報復号化装置のユーザに対して、現在の日時が復号許可日時になるまで待機するか否かを問い合わせ、ユーザの指示の入力を待ち、
入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機することを示す場合、現在日時を取得し、現在日時と、復号許可日時とを比較し、現在日時が復号許可日時以降となるまで、繰り返し実行し、
復号鍵を、当該鍵管理装置から取得する復号鍵取得手段と、
前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報を復号化する復号化手段と、を備えていること
を特徴とする鍵管理システム。

【請求項２】

請求項１記載の鍵管理システムであって、
前記情報復号化装置は複数あり、
前記鍵管理装置の復号鍵公開手段は、
前記複数の情報復号化装置を宛先とするブロードキャストパケットあるいはマルチキャストパケットにより、復号鍵を、通信ネットワークを介して前記複数の情報復号化装置に一斉同報通信するものであること
を特徴とする鍵管理システム。

【請求項３】

請求項１記載の鍵管理システムであって、
前記情報復号化装置は複数あり、
前記鍵管理装置の復号鍵公開手段は、
無線放送を利用することで、前記複数の情報復号化装置に対して復号鍵の公開を行うものであること
を特徴とする鍵管理システム。

【請求項４】

請求項１、２または３記載の鍵管理システムであって、
前記鍵管理装置は、
前記情報暗号化装置より送られてきた日時情報が示す日あるいは日時を公開日あるいは公開日時とする復号鍵が前記管理テーブルに登録されていない場合に、新たに１組の暗号鍵および復号鍵を生成する鍵生成手段と、
前記鍵生成手段で新たに生成した１組の暗号鍵および復号鍵を、前記日時情報が示す日あるいは日時を当該復号鍵の公開日あるいは公開日時に設定して、前記管理テーブルに追加する管理テーブル作成手段と、をさらに備えていること
を特徴とする鍵管理システム。

【請求項５】

請求項１、２、３または４記載の鍵管理システムであって、
前記情報暗号化装置において、
前記暗号化手段は、
前記暗号化すべき情報をデータ鍵を用いて暗号化するとともに、当該データ鍵を、操作者によって入力された個別暗号鍵および前記暗号鍵受信手段で受信した暗号鍵を用いて二重に暗号化するものであり、

前記暗号化情報作成手段は、
前記暗号化手段で暗号化された情報に、当該情報の機密性が解除される日あるいは日時に関する日時情報および前記暗号化手段で二重に暗号化されたデータ鍵を付与して、前記情報復号化装置に配布する暗号化情報を作成するものであり、
前記情報復号化装置において、
前記復号化手段は、
操作者によって入力された前記個別暗号鍵および前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報に付加された、二重に暗号化されたデータ鍵を復号化するとともに、当該復号化されたデータ鍵を用いて暗号化情報を復号化するものであること
を特徴とする鍵管理システム。
【請求項６】
請求項１、２、３、４または５記載の鍵管理システムであって、
前記情報暗号化装置は、
前記暗号化情報作成手段で作成した暗号化情報を通信ネットワークを介して前記情報復号化装置に送信する暗号化情報送信手段をさらに備えていること
を特徴とする鍵管理システム。
【請求項７】
暗号鍵および復号鍵を管理する鍵管理装置と、当該鍵管理装置から復号鍵を取得して情報の復号化を行う情報復号化装置であって、
情報暗号化装置によって、復号許可日時情報を付与して暗号化情報を作成されて配布された暗号化情報を、当該暗号化情報に付与されている日時情報が示す日あるいは日時に先立って取得する暗号化情報取得手段と、
現在日時を取得し、現在日時と、復号許可日時とを比較し、
その結果、現在日時が復号許可日時以降である場合は、
復号鍵を、当該鍵管理装置から取得する復号鍵取得手段と、
現在日時が復号許可日時よりも前の日時である場合は、
情報復号化装置のユーザに対して、現在の日時が復号許可日時になるまで待機するか否かを問い合わせ、ユーザの指示の入力を待ち、
入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機することを示す場合、現在日時を取得し、現在日時と、復号許可日時とを比較し、現在日時が復号許可日時以降となるまで、繰り返し実行し、
復号鍵を、当該鍵管理装置から取得する復号鍵取得手段と、
前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報を復号化する復号化手段と、を備えていること
を特徴とする情報復号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、暗号データを復号する復号鍵を管理するためのシステムに関し、特に、通信ネットワーク上で、複数のユーザに対する情報の同時公開を実現するのに好適なシステムに関する。
【０００２】
【従来の技術】
近年、インターネットなどの通信ネットワークを介して、複数の端末間での情報のやり取りが盛んに行われている。
【０００３】
ところで、通信ネットワークを介してやり取りされる情報のなかには、ある日時以前は秘密にしておく必要があるが、その後は開示しても構わないといった性質を有するものがある。たとえば、政府の機密情報などである。また、情報の開示が、複数の利用者に対して

同時に行われていること（言い換えれば、複数の利用者が、情報の中身を同時に知ることができる状態にすること）を保証しなければならないものもある。たとえば、入札など商取引に関する情報などである。

【０００４】

このような情報に対して、従来は、情報作成者側の端末において、作成した情報を当該情報の機密性が解除される日あるいは日時まで保持し、機密性が解除されたときに、すなわち機密期限が切れたときに、はじめて、複数の利用者に公開あるいは配布する方法が利用されている。

【０００５】

【発明が解決しようとする課題】

しかしながら、上記の方法では、情報作成者は、公開あるいは配布すべき情報の量が膨大である場合や、配布対象となる利用者の数が多い場合、複数の利用者に対し情報を、同時にしかも確実に開示することが容易でない。

【０００６】

また、情報作成者は、当該情報の公開あるいは配布日時を管理しなければならない。特に、複数種の情報を開示あるいは配布する場合において、これ等の情報の開示あるいは配布の日時が重なった場合、複数の利用者に対し情報の公開あるいは配布の同時性を保証することが困難である。

【０００７】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、複数のユーザに対する情報の同時公開を実現するのに好適なシステムを提供する。

【０００８】

【課題を解決するための手段】

本発明は、ネットワーク上を伝送される情報のセキュリティを確保する技術である鍵暗号方式を利用することで、上記課題を解決している。

【０００９】

具体的には、暗号鍵を用いて情報を暗号化する情報暗号化装置と、復号鍵を用いて情報を復号化する情報復号化装置と、前記情報暗号化装置および前記情報復号化装置で用いる暗号鍵および復号鍵を管理する鍵管理装置とを備え、少なくとも前記情報暗号化装置および前記鍵管理装置間が通信ネットワークで接続された鍵管理システムであって、

前記鍵管理装置は、

少なくとも１組の暗号鍵および復号鍵を記憶する鍵記憶手段と、

前記記憶手段に記憶された復号鍵と、当該復号鍵の公開日あるいは公開日時と、の対応関係を示す管理テーブルを記憶する管理テーブル記憶手段と、

前記管理テーブル記憶手段に記憶された管理テーブルを参照することで、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵と対の暗号鍵を検索する鍵検索手段と、

前記検索手段で検索した暗号鍵を、通信ネットワークを介して前記情報暗号化装置に送信する暗号鍵送信手段と、

前記管理テーブル記憶手段に記憶された管理テーブルにしたがい、現在の日あるいは日時に対応する復号鍵を公開する復号鍵公開手段と、を備えており、

前記情報暗号化装置は、

暗号化すべき情報の機密性が解除される日あるいは日時に関する日時情報を、通信ネットワークを介して前記鍵管理装置に送信する日時情報送信手段と、

通信ネットワークを介して前記鍵管理装置から送られてきた、前記日時情報送信手段が送信した日時情報で特定される日あるいは日時に対応する暗号鍵を受信する暗号鍵受信手段と、

前記暗号鍵受信手段で受信した暗号鍵を用いて、情報を暗号化する暗号化手段と、

前記暗号化手段で暗号化された情報に当該情報についての前記日時情報を付与して、前記情報復号化装置に配布する暗号化情報を作成する暗号化情報作成手段と、を備えており、

前記情報復号化装置は、

前記情報暗号化装置によって作成された暗号化情報を取得する暗号化情報取得手段と、
前記暗号化情報取得手段で取得した暗号化情報に付与された日時情報で特定される日あるいは日時になったときに、前記鍵管理装置で公開されている復号鍵を取得する復号鍵取得手段と、
前記復号鍵取得手段で取得した復号鍵を用いて、前記暗号化情報取得手段で取得した暗号化情報を復号化する復号化手段と、を備えている。

【００１０】

ここで、暗号鍵および復号鍵とは、たとえば、公開鍵暗号方式における公開鍵および秘密鍵である。

【００１１】

本発明は、前記の構成により、情報作成者は、作成した情報を、当該情報の機密性が解除される日あるいは日時以前に、当該情報を暗号化して利用者に配布することができる。したがって、情報作成者は、作成した情報の公開日時を管理する必要がなくなる。

【００１２】

また、情報の利用者は、受け取った暗号化情報の機密性が解除される日あるいは日時になるまで、当該情報を復号化するための復号鍵を取得することができない。したがって、その日あるいは日時まで情報を機密にすることができる。

【００１３】

さらに、情報の利用者は、受け取った情報の機密性が解除される日あるいは日時以降は、当該情報を復号化するための復号鍵を取得することができる。したがって、当該復号鍵を用いて予め受け取った暗号化情報を復号化することにより、複数の利用者に対して、情報公開の同時性を保証することができる。

【００１４】

なお、本発明において、前記情報復号化装置が複数ある場合、当該複数の情報復号化装置各々と前記鍵管理装置とを通信ネットワークを介して接続し、前記鍵管理装置の復号鍵公開手段が、前記複数の情報復号化装置を宛先とするブロードキャストパケットあるいはマルチキャストパケットにより、復号鍵を、通信ネットワークを介して前記複数の情報復号化装置に一斉同報通信するようにしてもよい。あるいは、当該複数の情報復号化装置各々と前記鍵管理装置とを通信ネットワークを介して接続することなく、前記鍵管理装置の復号鍵公開手段が、無線放送を利用することで、前記複数の情報復号化装置に対して復号鍵の公開を行うようにしてもよい。

【００１５】

また、本発明において、前記鍵管理装置に、前記情報暗号化装置が要求した日あるいは日時に対応する復号鍵が前記管理テーブル記憶手段に記憶された管理テーブルにない場合に、新たに１組の暗号鍵および復号鍵を生成する鍵生成手段と、前記鍵生成手段で生成した暗号鍵および復号鍵に、前記情報暗号化装置が要求した日あるいは日時を対応付けて、前記管理テーブルに追加する管理テーブル作成手段と、をさらに備えてもよい。

【００１６】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【００１７】

図１は、本実施形態が適用された鍵管理システムの全体構成を示す図である。

【００１８】

ここで、符号５０は鍵管理装置、符号６０は情報送信装置、符号７０は情報受信装置である。これ等の装置は、ＬＡＮなどの通信ネットワーク９０を介して互いに接続されている。

【００１９】

なお、ここでは、情報送信装置６０および情報受信装置７０を各々１つ示しているが、これに限定されるものではなく、各々複数あってもよい。

【００２０】

図１に示す各装置５０、６０、７０は、通信機能を備えた情報処理装置、たとえばパーソナルコンピュータを用いることで、実現可能である。

【００２１】

鍵管理装置５０は、情報暗号処理に用いる暗号鍵および情報復号処理に用いる復号鍵の管理を行う機能を有する。この機能は、ＣＰＵ１ａが、ディスクコントローラ４ａを介して磁気ディスク５ａからメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１、暗号鍵サービスプログラム２２、復号鍵サービスプログラム２３、および復号鍵配布プログラム２４を実行することで実現される。なお、図１において、符号２０ａはオペレーティングシステム（ＯＳ）、符号３ａは、ネットワーク９０を介した通信を実現するためのネットワークコントローラである。

【００２２】

磁気ディスク５ａには、上記のＯＳ２０ａ、暗号鍵／復号鍵管理プログラム２１、暗号鍵サービスプログラム２２、復号鍵サービスプログラム２３、および復号鍵配布プログラム２４の他、少なくとも１組の暗号鍵および復号鍵が記憶されている。この少なくとも１組の暗号鍵および復号鍵は、各々当該復号鍵の公開日時と対応付けられて、鍵管理テーブル１００として記憶される。

【００２３】

鍵管理テーブル１００の一例を図２に示す。この例では、磁気ディスク５ａに記憶されている複数組の暗号鍵１０２および復号鍵１０３が、各々復号鍵１０３の公開日時である日付時刻１０１に対応付けられている。

【００２４】

ここで、暗号鍵１０２および復号鍵１０３は、公開鍵暗号方式における公開鍵および秘密鍵である。公開鍵暗号方式における公開鍵および秘密鍵は、いずれか一方から他方を求めることが極めて困難であるといった性質を有する。そこで、公開鍵暗号方式では、暗号化用の公開鍵を秘密にせずに公開しておき、復号用の秘密鍵のみを秘密にしておく。すなわち、公開されている公開鍵を取得することで、誰でも情報の暗号化を行うことができるが、当該公開鍵で暗号化された情報の復号化については、当該公開鍵と対の秘密鍵を所有する者のみが行うことができるようにすることで、ネットワーク上を伝送される情報のセキュリティを確保している。

【００２５】

公開鍵暗号方式における公開鍵および秘密鍵は、初期値から結果の値を求めることは容易でも、結果の値から初期値を求めることは極めて困難な一方向性関数を用いて実現されている。ここでは、現在広く用いられているＲＳＡ(Rivest,Shamir,Adleman)と呼ばれるシステムについて簡単に説明する。

【００２６】

まず、二つの大きな素数ｐ、ｑを用意する。そして、ｐとｑとの積ｐｑをｎとする。次に、ｎのオイラー関数

φ（ｎ）＝（ｐ－１）（ｑ－１）

に関し、互いに素である任意の数ｅを選ぶ。そして、φ（ｎ）のモジュロの基でのｅの逆数

ｅｄ＝１ｍｏｄ φ（ｎ）

となる数ｄを求める。すると、平文Ｍ、暗号文Ｃに関して、

$C=(M^{e})\ \mathrm{mod}\ n$

$M=(C^{d})\ \mathrm{mod}\ n$

が成り立つことが証明される。したがって、ｄを秘密鍵とし、ｅとｎの組を公開鍵とすることができる。図２におけるｅ１１２およびｎ１２２は、上記の式におけるe、ｎに相当する。

【００２７】

公開鍵暗号化方式については、たとえば「データ保護と暗号化の研究、一松信監修、日本経済新聞社（昭５８）」などで詳しく述べられている。

【００２８】
情報送信装置６０は、情報の暗号化を行う機能を有する。この機能は、ＣＰＵ１ｂが、ディスクコントローラ４ｂを介して磁気ディスク５ｂからメモリ２ｂ上にロードされた暗号鍵取得プログラム３１およびファイル暗号化プログラム３２を実行することで実現される。なお、図１において、符号２０ｂはＯＳ、符号３ｂは、通信ネットワーク９０を介した通信を実現するためのネットワークコントローラである。
【００２９】
情報受信装置７０は、情報の復号化を行う機能を有する。この機能は、ＣＰＵ１ｃが、ディスクコントローラ４ｃを介して磁気ディスク５ｃからメモリ２ｃ上にロードされた復号鍵取得プログラム４１およびファイル復号化プログラム４２を実行することで実現される。なお、図１において、符号２０ｃはＯＳ、符号３ｃは、通信ネットワーク９０を介した通信を実現するためのネットワークコントローラである。
【００３０】
上記構成の鍵管理システムの動作について簡単に説明する。
【００３１】
まず、情報送信装置６０は、暗号化すべき情報の機密性が解除される日時に関する情報を、通信ネットワーク９０を介して鍵管理装置５０へ送信する。
【００３２】
これを受けて、鍵管理装置５０は、磁気ディスク５ａに記憶されている鍵管理テーブル１００を参照することで、情報送信装置６０から送られてきた情報によって特定される日時に対応する暗号鍵を検索する。そして、検索した暗号鍵を、通信ネットワーク９０を介して、情報送信装置６０へ送信する。
【００３３】
また、鍵管理装置５０は、磁気ディスク５ａに記憶されている鍵管理テーブル１００にしたがい、現在の日時に対応する復号鍵を順次読み出して公開する。
【００３４】
情報送信装置６０は、鍵管理装置５０から送られてきた暗号鍵を用いて、情報受信装置７０へ送信する情報を暗号化する。そして、暗号化した情報（以下、暗号化情報ともいう）に、当該情報の機密性が解除される日時に関する情報を付加して、情報受信装置６０へ、通信ネットワーク９０を介して送信する。
【００３５】
これを受けて、情報受信装置７０は、現在の日時が、情報送信装置６０から送られてきた暗号化情報に付与された日時に関する情報で特定される日時になるまで待ち、当該日時となったときに、鍵管理装置５０で公開されている復号鍵を取得する。そして、取得した復号鍵で、情報送信装置６０から送られてきた暗号化情報を復号化する。
【００３６】
次に、本実施形態システムを構成する各装置の詳細について説明する。
【００３７】
まず、鍵管理装置５０の詳細について説明する。
【００３８】
最初に、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１を実行した場合の動作について説明する。
【００３９】
図３は、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１を実行した場合の動作を説明するためのフロー図である。
【００４０】
まず、図示していない表示装置などを用いて、鍵管理装置５０のオペレータに対して、鍵管理テーブル１００に追加する鍵を特定するための情報である、開始日時、終了日時、および時間間隔を入力するように促す。これを受けて、ステップ６０１～６０３において、図示していない入力装置に入力された開始日時、終了日時、および時間間隔を受け付ける

。
【００４１】
ステップ６０４では、暗号鍵／復号鍵生成ルーチンを呼び出して、一組の暗号鍵（ｅ，ｎ）および復号鍵（ｄ）を生成する。この暗号鍵／復号鍵生成ルーチンについては後述する。
【００４２】
ステップ６０５では、鍵管理テーブル１００に日付時刻を追加する。ここで、日付時刻とは、図３に示すフローにおいて、ステップ６０５での処理が一回目である場合は、ステップ６０１で受け付けた開始日時、二回目以降の場合は、後述するステップ６０９で算出した日付時刻である。
【００４３】
ステップ６０６では、ステップ６０４で生成した暗号鍵（ｅ，ｎ）を、鍵管理テーブル１００の、ステップ６０５で当該鍵管理テーブル１００に追加した日付時刻に対応する欄に追加する。
【００４４】
ステップ６０７では、ステップ６０４で生成した復号鍵（ｄ）を、鍵管理テーブル１００の、ステップ６０５で当該鍵管理テーブル１００に追加した日付時刻に対応する欄に追加する。
【００４５】
ステップ６０８では、ステップ６０５で鍵管理テーブル１００に追加した日付時刻が、ステップ６０２で受け付けた終了日時以降の日時となったか否かを判断する。終了日時以降の日時となっていない場合は、ステップ６０９へ移行して、ステップ６０５で鍵管理テーブル１００に追加した日付時刻に、ステップ６０３で受け付けた日時間隔を加算し、得られた結果を新たな日付時刻に設定する。
【００４６】
一方、終了日時以降の日時となっている場合は、このフローを終了する。
【００４７】
上記のフローにより、ＣＰＵ１ａは、暗号鍵／復号鍵管理プログラム２１を実行することで、図２に示すような、公開鍵及び復号鍵と、復号鍵を公開する日付時刻と、を対応付けた鍵管理テーブル１００を作成することができる。
【００４８】
次に、図３に示すフローのステップ６０４での処理（暗号鍵／復号鍵生成ルーチン）について説明する。
【００４９】
図４は、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１のうちの暗号鍵／復号鍵生成ルーチン７００を実行した場合の動作を説明するためのフロー図である。
【００５０】
まず、二つの大きな素数ｐ、ｑを生成し（ステップ７０１）、その後、この生成したｐとｑとの積ｎ（＝ｐｑ）を生成する（ステップ７０２）。
【００５１】
次に、この積ｎのオイラー関数
φ（ｎ）＝（ｐ－１）（ｑ－１）
に関し、互いに素である任意の数ｅを選択する（ステップ７０３）。そして、φ（ｎ）のモジュロの基でのｅの逆数
ｅｄ＝１ｍｏｄ φ（ｎ）
となる数ｄを求める(ステップ７０４）。次に、上記のステップ７０２～７０４で得たｅ、ｎ、ｄを、戻り値として設定し（ステップ７０５）、その後、呼び出し元にリターンする（ステップ７９９）。
【００５２】

次に、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵サービスプログラム２２を実行した場合の動作について説明する。

【００５３】

図５は、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵サービスプログラム２２を実行した場合の動作を説明するためのフロー図である。なお、暗号鍵サービスプログラム２２は、鍵管理装置５０の常駐プログラムとして動作する。

【００５４】

まず、暗号鍵要求が通信ネットワーク９０経由で送られてくるのを待つ（ステップ８０１）。暗号鍵要求を受信すると、当該要求元から送られてくる日時に関する情報を取得する（ステップ８０２）。

【００５５】

次に、ステップ８０２で取得した情報で特定される日時が、磁気ディスク５ａに記憶された鍵管理テーブル１００に存在するかどうかを調べる（ステップ８０３）。存在しない場合は、暗号鍵／復号鍵管理プログラム２１を呼び出し、ステップ８０２で取得した情報で特定される日時を図３のステップ６０１、６０２で受け付ける開始日時および終了日時に設定し、図３のステップ６０３で受け付ける日時間隔を適当な時間に設定して、当該プログラムを実行する（ステップ８０４）。これにより、当該日時に対応付けられた暗号鍵および公開鍵が鍵管理テーブル１００に追加される。ステップ８０４での処理を完了した後、ステップ８０５へ移行する。

【００５６】

一方、ステップ８０２で取得した情報で特定される日時が鍵管理テーブル１００に存在する場合は、ステップ８０４を実行することなく、ステップ８０５へ移行する。

【００５７】

ステップ８０５では、鍵管理テーブル１００からステップ８０２で取得した情報で特定される日時に対応付けられた暗号鍵を取り出す。その後、取り出した暗号鍵を、暗号鍵の要求元に送信する（ステップ８０６）。以上の処理を行った後、ステップ８０１に戻り、再び、暗号鍵要求が通信ネットワーク９０経由で送られてくるのを待つ。

【００５８】

次に、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵サービスプログラム２３を実行した場合の動作について説明する。

【００５９】

図６は、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵サービスプログラム２３を実行した場合の動作を説明するためのフロー図である。なお、復号鍵サービスプログラム２３は、鍵管理装置５０の常駐プログラムとして動作する。

【００６０】

まず、復号鍵要求が通信ネットワーク９０経由で送られてくるのを待つ（ステップ９０１）。復号鍵要求を受信すると、当該要求元から送られてくる日時に関する情報を取得する（ステップ９０２）。

【００６１】

次に、ステップ９０２で取得した情報で特定される日時が、磁気ディスク５ａに記憶された鍵管理テーブル１００に存在するかどうかを調べる（ステップ８０３）。存在しない場合は、復号鍵の要求元にエラーコードを送信し（ステップ９０６）、その後、ステップ９０１に戻り、再び、復号鍵要求が通信ネットワーク９０経由で送られてくるのを待つ。

【００６２】

一方、ステップ９０２で取得した情報で特定される日時が鍵管理テーブル１００に存在する場合、当該日時に対応付けられた復号鍵を取り出し（ステップ９０４）、取り出した復号鍵を、復号鍵の要求元に送信する（ステップ９０５）。その後、ステップ９０１に戻り、再び、復号鍵要求が通信ネットワーク９０経由で送られてくるのを待つ。

【００６３】

次に、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵配布プ

ログラム２４を実行した場合の動作について説明する。
【００６４】
図７は、鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵配布プログラム２４を実行した場合の動作を説明するためのフロー図である。なお、復号鍵配布プログラム２４は、鍵管理装置５０の常駐プログラムとして動作する。
【００６５】
まず、ＯＳ２０ａが有する機能を利用して現在日時を取得し（ステップ１００１）、その後、取得した現在日時に対応付けられた復号鍵を、鍵管理テーブル１００から取り出す（ステップ１００２）。
【００６６】
次に、鍵管理テーブル１００から、ステップ１００１で取得した日時の次の日時を検索する（ステップ１００３）。そして、ＯＳ２０ａが有する機能を利用して取得した現在日時が、ステップ１００３で検索した次の日時以降となったか否かを判断する（ステップ１００４）。
【００６７】
次の日時以降となっていない場合は、ステップ１００２で取得した復号鍵を、当該復号鍵に対応付けられた日時に関する情報とともに、情報受信装置７０（情報送信装置７０が複数ある場合はその全て）に対して、通信ネットワーク９０を介して一斉同報通信する（ステップ１００５）。一斉同報通信は、通信ネットワークを用いた通信システムで利用されているブロードキャストパケットあるいはマルチキャストパケットを用いることで、実現可能である。ここで、ブロードキャストパケットとは、パケットのヘッダに、複数の宛先のアドレス各々を付与したものである。また、マルチキャストパケットとは、パケットのヘッダに、複数の宛先を示す１つのアドレスを付与したものである。
【００６８】
ステップ１００５での処理を終了した後、ＯＳ２０ａが有する機能を利用して現在日時を取得し（ステップ１００６）、ステップ１００４へ戻る。
【００６９】
一方、ステップ１００４において、次の日時以降となっている場合は、ステップ１００２へ戻る。
【００７０】
上記のフローにより、鍵管理テーブル１００に格納された複数の復号鍵各々は、自己に対応付けられた日時から次に公開すべき復号鍵に対応付けられた日時となるまで、繰り返し一斉同報通信される。ここで、上記のフローによって鍵管理装置５０から送出される復号鍵の履歴の一例を図８に示す。
【００７１】
次に、情報送信装置６０の詳細について説明する。
【００７２】
最初に、情報送信装置６０で生成された暗号化情報の構成について説明する。
【００７３】
図９は、情報送信装置６０で生成された暗号化情報の構成例を説明するための図である。なお、暗号化すべき情報は、データベースや電子メールなど電子的なデータならどのようなものでもよいが、ここでは、情報をファイル単位で暗号化した場合の例について示す。
【００７４】
図９において、符号２０２は、暗号化後の暗号文ファイルである。暗号文ファイル２０２は、平文ファイルを暗号化したデータである暗号文データ２０４と、暗号文データ２０４に付加されたヘッダ２０５と、から成る。
【００７５】
ヘッダ２０５には、復号が可能となる日時（すなわち、機密性が解除される日時）を示す情報である復号許可日時２０６と、暗号文データ２０４の元となる平文ファイルのファイル名２０７と、この平文ファイルのファイルサイズ２０８と、この平文ファイルの暗号化

に用いたデータ鍵を、鍵管理装置５０から取得した暗号鍵および後述する個別暗号鍵を用いて二重に暗号化したデータである二重暗号化データ鍵２０９と、で成る。

【００７６】

図９に示す暗号化情報の構成例から分かるように、本実施形態では、鍵管理装置５０から取得した暗号鍵を用いて、平文ファイルを直接暗号化するのではなく、対称鍵暗号方式で用いられる鍵、すなわち暗号化および復号化の両方に共通して用いられるデータ鍵を用いて、平文ファイルを暗号化するようにしている。そして、鍵管理装置５０から取得した暗号鍵は、平文ファイルの暗号化に用いたデータ鍵を暗号化するのに用いるようにしている。

【００７７】

次に、情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされたファイル暗号化プログラム３２を実行した場合の動作について説明する。

【００７８】

図１０は、情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされたファイル暗号化プログラム３２を実行した場合の動作を説明するためのフロー図である。

【００７９】

まず、図示していない表示装置などを用いて、情報送信装置６０のユーザに対して、暗号化する平文のファイル名および当該ファイルの復号許可日時を入力するように促す。これを受けて、ステップ１１０１、１１０２において、図示していない入力装置に入力されたファイル名、および復号許可日時を受け付ける。

【００８０】

次に、ステップ１１０３において、ステップ１１０１で受け付けたファイル名で特定されるファイルをオープンにする。その後、仮の名称を付けた一時ファイルを作成する（ステップ１１０４）。

【００８１】

次に、ステップ１１０５では、データ鍵である乱数を生成する。その後、暗号鍵取得プログラム３１を実行して、鍵管理装置５０から、ステップ１１０２で受け付けた復号許可日時に公開される復号鍵と対の暗号鍵を取得する（ステップ１１０６）。

【００８２】

ステップ１１０７では、ステップ１１０５で生成したデータ鍵を、ステップ１１０６で鍵管理装置５０から取得した暗号鍵を用いて暗号化して、暗号化データ鍵を生成する。その後、図示していない表示装置などを用いて、情報送信装置６０のユーザに対して、ステップ１１０７で生成した暗号化データ鍵を二重に暗号化するための鍵である個別暗号鍵を入力するように促す。これを受けて、ステップ１１０８において、図示していない入力装置に入力された個別暗号鍵を受け付ける。

【００８３】

次に、ステップ１１０９では、ステップ１１０７で生成した暗号化データ鍵を、ステップ１１０８で受け付けた個別暗号鍵を用いて暗号化して、二重暗号化データ鍵を生成する。

【００８４】

ステップ１１１０では、ステップ１１０４で作成した一時ファイルの先頭部分にヘッダを付加する。そして、付加したヘッダに、ステップ１１０２で受け付けた復号許可日時を特定する情報、ステップ１１０１で受け付けたファイル名、このファイル名で特定されるファイルのサイズ、およびステップ１１０９で生成した二重暗号化データ鍵を、この順序で書き込む（ステップ１１１１）。

【００８５】

次に、ステップ１１１２では、ステップ１１０３でオープンにした平文ファイルからデータを読み出す。そして、読み出したデータを、ステップ１１０９で生成した二重暗号化データ鍵を用いて暗号化して、暗号データを生成し（ステップ１１１３）、その後、この暗号データをステップ１１０４で作成した一時ファイルに書き込む（ステップ１１１４）。

【００８６】

ステップ１１１５では、ステップ１１０３でオープンにした平文ファイルの全データの暗号化が終了したか否かを判定する。終了していない場合は、終了するまで上記のステップ１１１２～ステップ１１１４を繰り返し実行する。そして、平文ファイルの全データの暗号化が終了した後、平文ファイルおよび一時ファイルの両方をクローズにする。

【００８７】

ステップ１１１７では、ステップ１１０１で受け付けた平文ファイルのファイル名と、ステップ１１０４で作成した一時ファイルの仮の名称とが同一であるか否かを判定する。同一である場合は、平文ファイルを削除し（ステップ１１１８）、その後、一時ファイルのファイル名を、ステップ１１０１で受け付けた平文ファイルのファイル名に変更する。そして、このフローを終了する。

【００８８】

一方、同一でない場合は、ステップ１１０４で作成した一時ファイルのファイル名を、ステップ１１０１で受け付けた平文ファイルのファイル名に変更して、このフローを終了する。

【００８９】

情報送信装置６０は、上記のようにして作成した暗号文ファイルを、通信ネットワーク９０を介して、所望の情報受信装置７０に送信することができる。

【００９０】

次に、情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされた暗号鍵取得プログラム３１を実行した場合の動作について説明する。

【００９１】

図１１は、情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされた暗号鍵取得プログラム３１を実行した場合の動作を説明するためのフロー図である。このフローは、図１０に示すフローのステップ１１０６が行われることで、実行される。

【００９２】

まず、ステップ１３０１において、情報送信装置６０を、通信ネットワーク９０を介して、鍵管理装置５０に接続する。

【００９３】

次に、ステップ１３０２において、図１０に示すフローのステップ１１０２で受け付けた復号許可日時を特定する情報を、鍵管理装置５０へ送信する。これを受けて、鍵管理装置５０は、暗号鍵サービスプログラム２２により、鍵管理テーブル１００から復号許可日時に対応付けられた復号鍵を検索して、当該復号鍵を、復号許可日時を特定する情報を送信した情報送信装置６０に送信する。

【００９４】

ステップ１３０３では、鍵管理装置５０から送られてきた、ステップ１３０２で鍵管理装置に送信した復号許可日時に対応付けられた暗号鍵を受信する。次に、鍵管理装置５０との接続を解除し（ステップ１３０４）、その後、ステップ１３０３で受信した暗号鍵を戻り値に設定して（ステップ１３０５）、このフローを終了する。

【００９５】

次に、情報受信装置７０の詳細について説明する。

【００９６】

最初に、情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされたファイル復号化プログラム４２を実行した場合の動作について説明する。

【００９７】

図１２は、情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされたファイル復号化プログラム４２を実行した場合の動作を説明するためのフロー図である。

【００９８】

まず、図示していない表示装置などを用いて、情報受信装置７０のユーザに対して、情報送信装置６０から送られてきた暗号文ファイルのうち、復号しようとしている暗号文ファイルの名称を入力するように促す。これを受けて、ステップ１２０１において、図示して

いない入力装置に入力されたファイル名を受け付ける。
【００９９】
次に、ステップ１２０２において、ステップ１２０１で受け付けたファイル名で特定される暗号文ファイルをオープンにした後、この暗号文ファイルのヘッダから二重暗号化データ鍵を取り出す（ステップ１２０３）。その後、図示していない表示装置などを用いて、情報受信装置６０のユーザに対して、取り出した二重暗号化データ鍵を復号化するのに用いる個別暗号鍵を入力するように促す。これを受けて、ステップ１２０４において、図示していない入力装置に入力された個別暗号鍵を受け付ける。
【０１００】
なお、個別暗号鍵は、暗号文ファイルの送信者から予め知らされているものとする。
【０１０１】
次に、ステップ１２０５では、ステップ１２０３で取り出した二重暗号化データ鍵を、ステップ１２０４で受け付けた個別暗号鍵を用いて、一重の暗号化データ鍵に変換する。
【０１０２】
ステップ１２０６では、ステップ１２０３でオープンにした暗号文ファイルのヘッダから復号許可日時に関する情報を取り出す。その後、この情報で特定される日時を引数として、復号鍵取得プログラム４１を実行する（ステップ１２０７）。これにより、鍵管理装置５０から、復号許可日時に対応付けられた復号鍵を取得する。
【０１０３】
次に、ステップ１２０８では、ステップ１２０７で実行した復号鍵取得プログラム４１からの戻り値を参照することで、復号鍵の取得に成功したか否かを判定する。取得に成功しなかった場合は、ステップ１２０２でオープンにした暗号文ファイルをクローズにし（ステップ１２８９）、このフローを終了する。
【０１０４】
一方、復号鍵の取得に成功した場合は、ステップ１２０９に移行する。
【０１０５】
ステップ１２０９では、ステップ１２０５で得た一重の暗号化データ鍵を、ステップ１２０７で取得した復号鍵を用いて復号化することで、暗号文ファイルの暗号化に用いたデータ鍵を得る。
【０１０６】
次に、ステップ１２１０では、仮の名称を付けた一時ファイルを作成する。その後、ステップ１２０２でオープンにした暗号文ファイルから暗号データを読み出す（ステップ１２１１）。そして、読み出した暗号データを、ステップ１２０９で生成したデータ鍵を用いて復号化して、平文データを生成し（ステップ１２１２）、その後、この平文データをステップ１２１０で作成した一時ファイルに書き込む（ステップ１２１３）。
【０１０７】
ステップ１２１４では、ステップ１２０２でオープンにした暗号文ファイルの全暗号データの復号化が終了したか否かを判定する。終了していない場合は、終了するまで上記のステップ１２１１～ステップ１２１３を繰り返し実行する。そして、暗号文ファイルの全暗号データの復号化が終了した後、暗号文ファイルおよび一時ファイルの両方をクローズにする。
【０１０８】
ステップ１２１６では、ステップ１２０１で受け付けた暗号文ファイルのファイル名と、ステップ１２１０で作成した一時ファイルの仮の名称とが同一であるか否かを判定する。同一である場合は、暗号文ファイルを削除し（ステップ１２１７６）、その後、一時ファイルのファイル名を、ステップ１２０１で受け付けた暗号文ファイルのファイル名に変更する。そして、このフローを終了する。
【０１０９】
一方、同一でない場合は、ステップ１２１０で作成した一時ファイルのファイル名を、ステップ１２０１で受け付けた暗号文ファイルのファイル名に変更して、このフローを終了

する。
【０１１０】
次に、情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされた復号鍵取得プログラム４１を実行した場合の動作について説明する。
【０１１１】
図１３は、情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされた復号鍵取得プログラム４１を実行した場合の動作を説明するためのフロー図である。このフローは、図１２に示すフローのステップ１２０７が行われることで、実行される。
【０１１２】
まず、ステップ１４０１において、ＯＳ２０ｃが有する機能を利用して現在日時を取得する。次に、この取得した現在日時と、引数として受け取った復号許可日時とを比較する（ステップ１４０２）。この結果、現在日時が復号許可日時以降である場合はステップ１４０６に移行し、復号許可日時よりも前の日時である場合はステップ１４０３へ移行する。
【０１１３】
ステップ１４０３では、図示していない表示装置などを用いて、情報受信装置７０のユーザに対して、現在の日時が復号許可日時になるまで待機するか否かを問い合わせる。そして、図示していない入力装置に、ユーザに指示が入力されるの待つ。
【０１１４】
入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機しないことを示す場合は、エラーコードを戻り値に設定し（ステップ１４８９）、その後、このフローを終了する。
【０１１５】
一方、入力されたユーザの指示が、現在の日時が復号許可日時になるまで待機することを示す場合、ＯＳ２０ｃが有する機能を利用して現在日時を取得し（ステップ１４０４）、その後、この取得した現在日時と、引数として受け取った復号許可日時とを比較する（ステップ１４０５）。このステップ１４０４およびステップ１４０５での処理を、取得した現在日時が、引数として受け取った復号許可日時以降となるまで、繰り返し実行する。
【０１１６】
ステップ１４０６では、鍵管理装置５０が公開している（通信ネットワーク９０上を流れている）復号鍵を受信し、その中に、引数として受け取った復号許可日時に対応付けられた復号鍵があるか否かを判定する。この判定は、受信した復号鍵に付加されている日時に関する情報を基に行う。
【０１１７】
引数として受け取った復号許可日時に対応付けられた復号鍵がある場合は、この復号鍵を戻り値に設定して（ステップ１４７９）、このフローを終了する。一方、引数として受け取った復号許可日時に対応付けられた復号鍵がない場合は、ステップ１４０８へ移行する。
【０１１８】
ステップ１４０８では、情報受信装置７０を、通信ネットワーク９０を介して、鍵管理装置５０に接続する。
【０１１９】
次に、ステップ１４０９において、引数として受け取った復号許可日時を特定する情報を、鍵管理装置５０へ送信する。これを受けて、鍵管理装置５０は、復号鍵サービスプログラム２３により、鍵管理テーブル１００から復号許可日時に対応付けられた復号鍵を検索して、当該復号鍵を、復号許可日時を特定する情報を送信した情報受信装置７０に送信する。
【０１２０】
ステップ１４１０では、鍵管理装置５０から送られてきた、復号許可日時に対応付けられた復号鍵を受信する。その後、鍵管理装置５０との接続を解除する（ステップ１４１１）。次に、復号鍵の受信結果を調べて、復号鍵をエラーなく取得することができたか否かを

判断する（ステップ１４１２）。

【０１２１】

エラーなく取得することができた場合は、この取得した復号鍵を戻り値に設定して（ステップ１４７９）、このフローを終了する。一方、エラーがあり、取得に失敗した場合は、エラーコードを戻り値に設定し（ステップ１４８９）、その後、このフローを終了する。

【０１２２】

上記説明した本実施形態の鍵管理システムでは、情報送信装置６０のユーザは、作成した情報を、当該情報の機密性が解除される日時以前に、当該情報を暗号化して利用者に配布することができる。したがって、作成した情報の公開日時を管理する必要がなくなる。

【０１２３】

また、情報受信装置７０のユーザは、受け取った暗号化情報の機密性が解除される日時になるまで、当該情報を復号化するための復号鍵を取得することができない。したがって、その日あるいは日時まで情報を機密にすることができる。

【０１２４】

さらに、情報受信装置７０のユーザは、受け取った情報の機密性が解除される日あるいは日時以降は、当該情報を復号化するための復号鍵を取得することができる。したがって、当該復号鍵を用いて予め受け取った暗号化情報を復号化することにより、複数の情報受信装置７０のユーザに対して、情報公開の同時性を保証することができる。

【０１２５】

なお、上記の実施形態では、鍵管理装置５０での復号鍵の公開（一斉同報通信）を、図８に示すように１個のチャネルを用いて行うものについて説明した。しかしながら、本発明はこれに限定されるものではない。たとえば、図１４に示すように、複数個のチャネルを用いて、復号鍵の公開を行うようにしてもよい。この場合、同一の復号鍵の公開（一斉同報通信）期間を長くすることができる。これにより、情報受信装置７０は、復号許可日時に達してからしばらく経った後でも、当該復号許可日時に対応する復号鍵を、鍵管理装置５０にアクセスすることなく取得することが可能となる。

【０１２６】

また、上記の実施形態では、鍵管理装置５０において、鍵の公開を通信ネットワーク９０を利用したブロードキャストパケットあるいはマルチキャストパケットにより行うものについて説明した。しかしながら、本発明は、これに限定されるものではない。復号鍵の公開は、図１５に示すような衛星などを用いた無線放送によっても実現可能である。衛星などの無線放送を用いることで、複数の情報受信装置７０全てに対して、同時に復号鍵を配布することが可能となる。

【０１２７】

さらに、上記の実施形態では、個別暗号鍵でデータ鍵を暗号化する場合について説明したが、鍵管理装置５０から取得する暗号鍵および復号鍵を、データの暗号化および復号化に直接用いることも可能である。ただし、この場合、復号許可日時が同一である暗号データは、この復号許可日時に対応付けられた復号鍵で全て復号できるという点に注意する必要がある。

【０１２８】

くわえて、上記の実施形態では、情報送信装置６０にて暗号化した情報を、通信ネットワークを介して情報受信装置７０へ送信するものについて説明したが、暗号化した情報の配布は、通信ネットワークを介さずに、たとえば、フロッピーディスクやＣＤ－ＲＯＭなどの記憶媒体に記録して行うようにしてもよい。また、上記の実施形態では、一台の鍵管装置５０を用いて、暗号鍵および復号鍵の管理やサービスなどを行う場合について説明したが、これ等の処理を複数の情報処理装置に分担させるようにしてもよい。

【０１２９】

また、上記の実施形態では、鍵管理システムを構成する各装置で実行される各種プログラムを、磁気ディスクに記憶させたものについて説明した。しかしながら、本発明はこれに限定されるものではなく、たとえばＣＤ－ＲＯＭなどの光ディスクやその他の記録媒体に

記憶するようにしてもよい。
【０１３０】
【発明の効果】
以上説明したように、本発明によれば、複数のユーザに対する情報の同時公開を実現するのに好適なシステムを提供することができる。
【図面の簡単な説明】
【図１】本発明の一実施形態が適用された鍵管理システムの全体構成を示す図である。
【図２】鍵管理装置５０の磁気ディスク５ａに記憶されている鍵管理テーブル１００の一例を示す図である。
【図３】鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１を実行した場合の動作を説明するためのフロー図である。
本発明の実施例における暗号鍵管理システムの一構成例を示す図である。
【図４】鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵／復号鍵管理プログラム２１のうちの暗号鍵／復号鍵生成ルーチン７００を実行した場合の動作を説明するためのフロー図である。
【図５】鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた暗号鍵サービスプログラム２２を実行した場合の動作を説明するためのフロー図である。
【図６】鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵サービスプログラム２３を実行した場合の動作を説明するためのフロー図である。
【図７】鍵管理装置５０において、ＣＰＵ１ａがメモリ２ａ上にロードされた復号鍵配布プログラム２４を実行した場合の動作を説明するためのフロー図である。
【図８】図７に示すフローによって鍵管理装置５０から送出される復号鍵の履歴の一例を示す図である。
【図９】情報送信装置６０で生成された暗号化情報の構成例を説明するための図である。
【図１０】情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされたファイル暗号化プログラム３２を実行した場合の動作を説明するためのフロー図である。
【図１１】情報送信装置６０において、ＣＰＵ１ｂがメモリ２ｂ上にロードされた暗号鍵取得プログラム３１を実行した場合の動作を説明するためのフロー図である。
【図１２】情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされたファイル復号化プログラム４２を実行した場合の動作を説明するためのフロー図である。
【図１３】情報受信装置７０において、ＣＰＵ１ｃがメモリ２ｃ上にロードされた復号鍵取得プログラム４１を実行した場合の動作を説明するためのフロー図である。
【図１４】本発明の一実施形態の変形例を説明するための図であり、複数個のチャネルを用いて復号鍵の配布を行なった場合における、鍵管理装置５０から送出される復号鍵の履歴の一例を示す図である。
【図１５】本発明の一実施形態の変形例を説明するための図であり、復号鍵の配布に衛星などを用いた無線放送を用いた例を示す図である。
【符号の説明】
１ａ～１ｃ　ＣＰＵ
２ａ～２ｃ　メモリ
３ａ～３ｃネットワークコントローラ
４ａ～４ｃ　ディスクコントローラ
５ａ～５ｃ　磁気ディスク
２０ａ～２０ｃ　ＯＳ
２１　暗号鍵／復号鍵管理プログラム
２２　暗号鍵サービスプログラム
２３　復号鍵サービスプログラム
２４　復号鍵配布プログラム
３１　暗号鍵取得プログラム
３２　ファイル暗号化プログラム

４１　復号鍵取得プログラム
４２　ファイル復号化プログラム
５０　鍵管理装置
６０　情報送信装置
７０　情報受信装置

【図１】

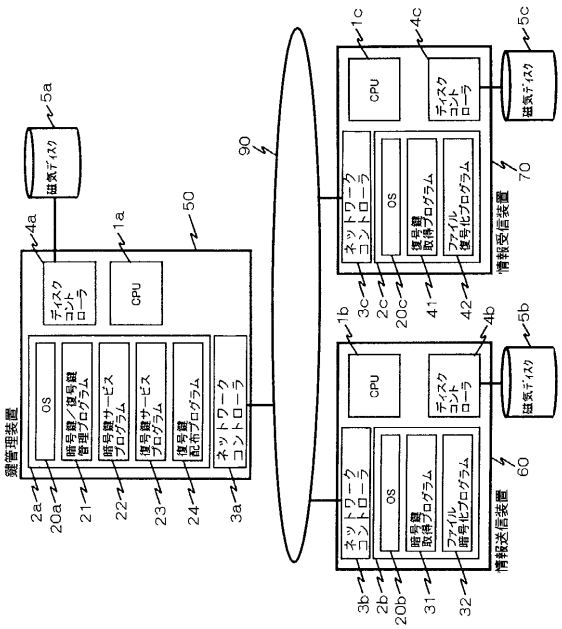


図１

【図２】

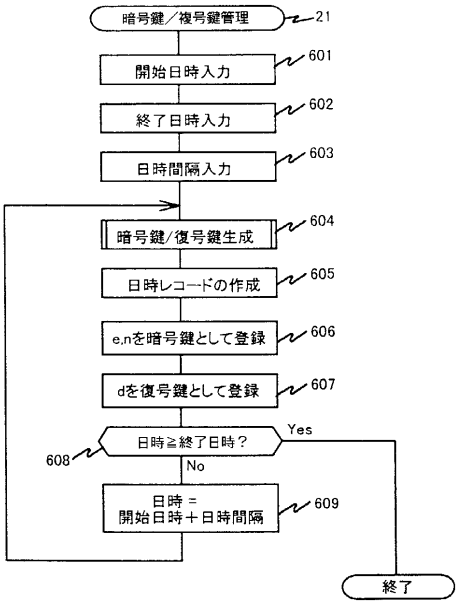
図２

日付時刻	暗号鍵 e	暗号鍵 n	復号鍵 d
199701010000	8F04	1AB3B･･･F3CB	F7C3B･･･935B
199701010100	169B	D5499･･･1CB6	6056D･･･7E9C
199701010200	EE7C	CB69B･･･5FC8	413A6･･･F103
≈	≈	≈	≈
199912312100	8BD7	B1B00･･･912F	36A9B･･･DF83
199912312200	A29F	AB39B･･･55FD	D0923･･･14F3
199912312300	4623	08469･･･EC01	CC08E･･･9FCB

鍵管理テーブル

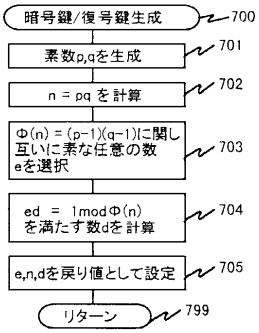
【図３】

図3



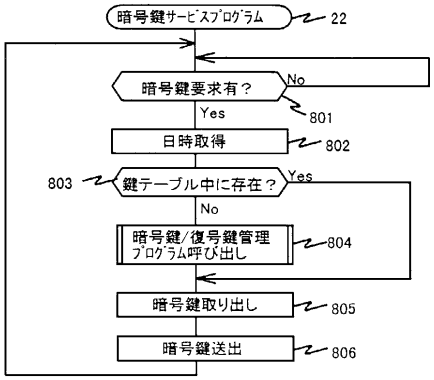
【図４】

図4



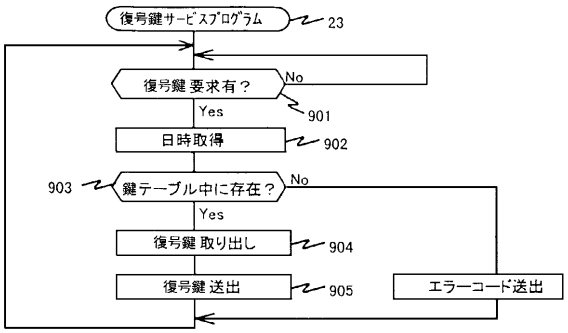
【図５】

図5



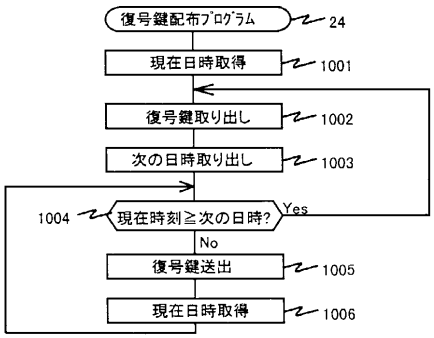
【図６】

図6



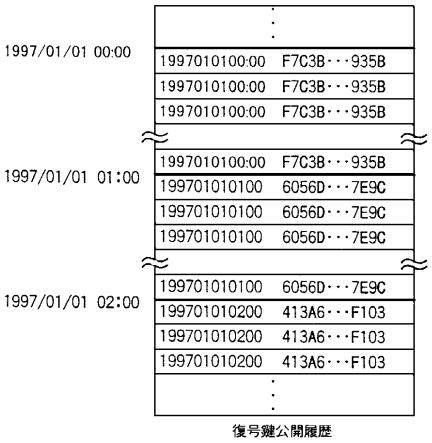
【図７】

図7



【図８】

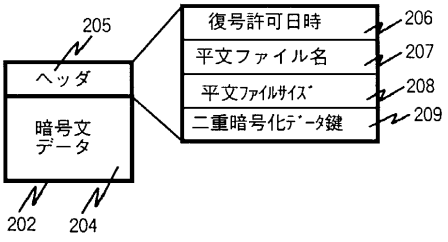
図8



復号鍵公開履歴

【図９】

図9

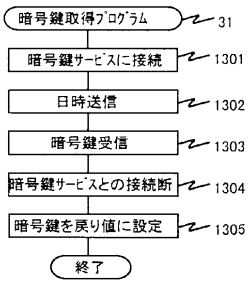


【図１０】

図１０

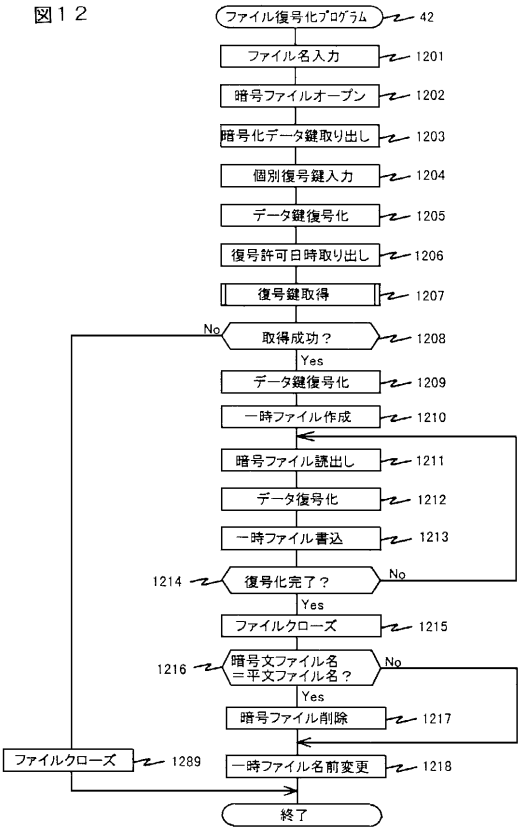
【図１１】

図１１



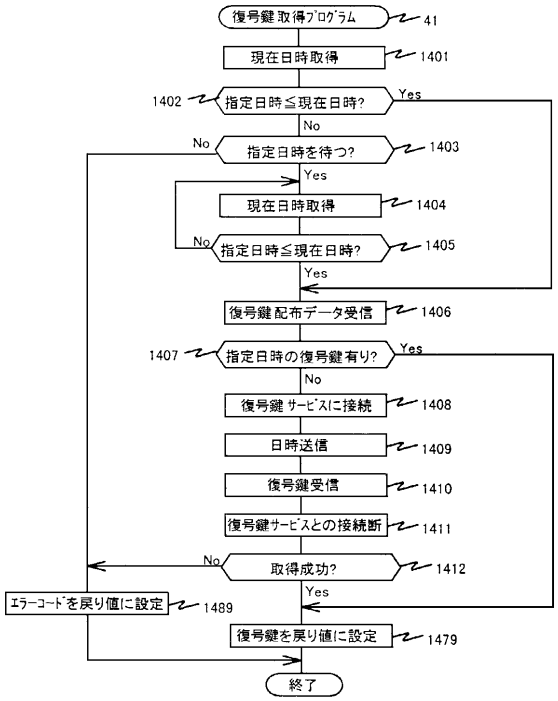
【図１２】

図１２



【図１３】

図１３



【図１４】

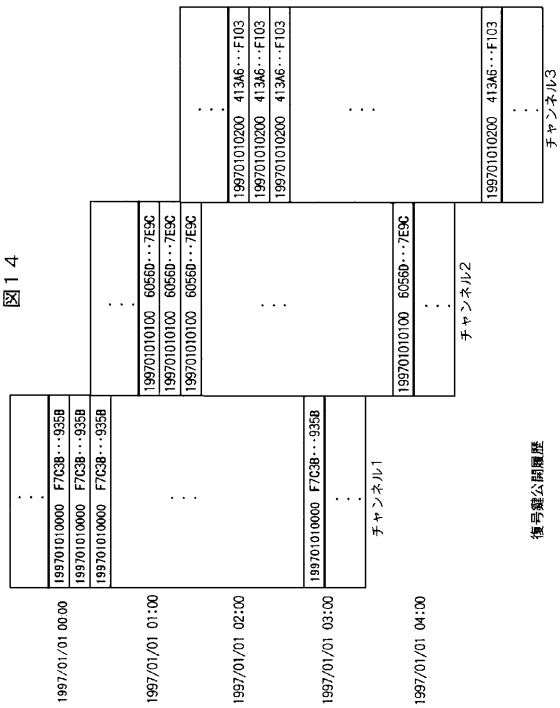


図１４
1997/01/01 00:00
1997/01/01 01:00
1997/01/01 02:00
1997/01/01 03:00
1997/01/01 04:00
チャンネル1
チャンネル2
チャンネル3
復号鍵公開履歴

【図１５】

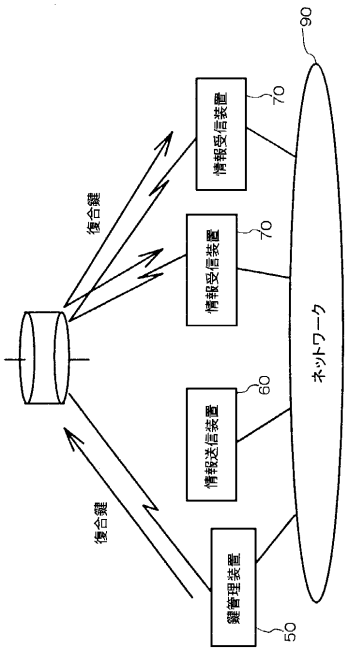


図１５
復合鍵
復合鍵
鍵管理装置
50
情報送信装置
60
情報受信装置
70
情報受信装置
70
ネットワーク
90

フロントページの続き

(51)Int.Cl. FI
H04L 9/00 601F

審査官 石川 正二

(56)参考文献 特開平08－102735（JP，A）
岡本栄司，暗号理論入門，日本，共立出版株式会社，1993年 2月25日，初版1刷，p.111-112

(58)調査した分野(Int.Cl.，DB名)
H04L 9/10
G06F 12/14
G09C 1/00
H04H 20/00
H04L 9/08