(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-103936
(P2008-103936A)
(43)公開日　平成20年5月1日(2008.5.1)

(51)Int.Cl.	F I	テーマコード（参考）
H04L 9/08 (2006.01)	H04L 9/00 601Z	5J104

審査請求 有　請求項の数 6　ＯＬ　（全 24 頁）

(21)出願番号　特願2006-284087 (P2006-284087)
(22)出願日　平成18年10月18日 (2006.10.18)

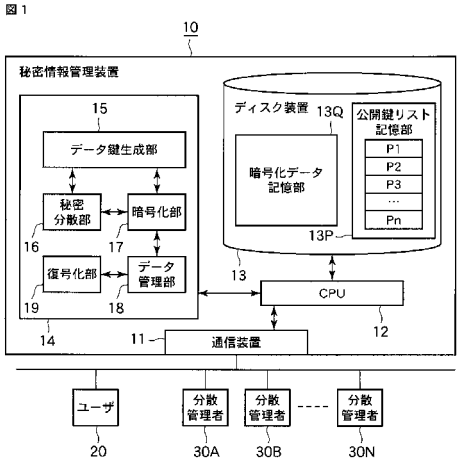
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(71)出願人　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】秘密情報管理装置および秘密情報管理システム

(57)【要約】
【課題】ユーザが暗号鍵をなくした場合にも、暗号化したデータを復号化し得る秘密情報管理装置および秘密情報管理システムを提供する。
【解決手段】秘密情報管理システムにおいて、秘密情報管理装置１０は、ユーザ端末２０から入力されるデータDの暗号化に際し、（ｋ，ｎ）型の秘密分散方式に基づいてデータ鍵Kを秘密分散し、ｎ個の分散鍵B1,B2・・・Bnを生成する秘密分散部１６と、ｎ個の分散管理者公開鍵P1,P2・・・Pnに基づいて、ｎ個の暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)を生成する暗号化部１７と、暗号化データE_K(D)・暗号化データ鍵E_{Px}(K)・ｎ個の暗号化分散鍵を関連付けて記憶する暗号化データ記憶部１３Ｑとを備える。
【選択図】　図１

図1



【特許請求の範囲】
【請求項１】
しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用可能な秘密情報管理装置であって、
データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、ユーザＩＤとを受信するためのデータ受信手段と、
互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個以上含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵とを含む公開鍵リストを予め記憶する公開鍵リスト記憶手段と、
乱数を用いてデータ鍵を生成するデータ鍵生成手段と、
このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、
前記受信したユーザＩＤに基づいて、前記公開鍵リスト記憶手段から前記ユーザ公開鍵を検索し、該ユーザ公開鍵を用いて前記データ鍵を暗号化し、暗号化データ鍵を生成する暗号化データ鍵生成手段と、
前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、
前記データ受信手段が受信するｎ個の分散管理者ＩＤに関連する分散管理者公開鍵を前記公開鍵リスト記憶手段から読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の暗号化分散鍵を生成する暗号化分散鍵生成手段と、
前記暗号化データ、前記暗号化データ鍵および前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と、
前記暗号化データの復号化要求を復号化方式情報とともに受信した場合、該復号化方式情報が、第１復号化方式情報および第２復号化方式情報のいずれであるかを判定する復号化方式判定手段と、
前記復号化方式情報が第１復号化方式情報である場合、前記暗号化データ鍵を該暗号化データ鍵の復号化要求とともに、前記復号化方式情報の送信元に送信する暗号化データ鍵送信手段と、
前記暗号化データ鍵の復号化要求に応じて、前記ユーザ公開鍵に対応するユーザ秘密鍵により復号化されたデータ鍵を前記復号化方式情報の送信元から受信した場合、このデータ鍵を用いて前記暗号化データを復号化して前記データを得る第１復号化手段と、
前記復号化方式情報が第２復号化方式情報である場合、前記公開鍵リストに含まれる分散管理者アドレス情報に基づいて、前記暗号化データ記憶手段内のｎ個の暗号化分散鍵を個別に送信する暗号化分散鍵送信手段と、
前記各暗号化分散鍵の送信先で分散管理者秘密鍵により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を復元するデータ鍵復元手段と、
このデータ鍵に基づいて前記暗号化データを復号化して前記データを得る第２復号化手段と
を備えたことを特徴とする秘密情報管理装置。
【請求項２】
データを入力するためのユーザ端末と、しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用して、前記データを暗号化した暗号化データを記憶するための秘密情報管理装置とを備えた秘密情報管理システムであって、
前記秘密情報管理装置は、
前記データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、ユーザＩＤとを受信するためのデータ受信手段と、
互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個以上含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵とを含む公開鍵リストを予め記憶する公開鍵リスト記憶手段と、

乱数を用いてデータ鍵を生成するデータ鍵生成手段と、
このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、
前記受信したユーザＩＤに基づいて、前記公開鍵リスト記憶手段から前記ユーザ公開鍵を検索し、該ユーザ公開鍵を用いて前記データ鍵を暗号化し、暗号化データ鍵を生成する暗号化データ鍵生成手段と、
前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、
前記データ受信手段が受信するｎ個の分散管理者ＩＤに関連する分散管理者公開鍵を前記公開鍵リスト記憶手段から読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の暗号化分散鍵を生成する暗号化分散鍵生成手段と、
前記暗号化データ、前記暗号化データ鍵および前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と、
前記暗号化データの復号化要求を復号化方式情報とともに前記ユーザ端末から受信した場合、該復号化方式情報が、第１復号化方式情報および第２復号化方式情報のいずれであるかを判定する復号化方式判定手段と、
前記復号化方式情報が第１復号化方式情報である場合、前記暗号化データ鍵を該暗号化データ鍵の復号化要求とともに前記ユーザ端末に送信する暗号化データ鍵送信手段と、
前記暗号化データ鍵の復号化要求に応じて、前記ユーザ公開鍵に対応するユーザ秘密鍵により復号化されたデータ鍵を前記ユーザ端末から受信するデータ鍵受信手段と、
前記データ鍵受信手段により受信したデータ鍵を用いて前記暗号化データを復号化して前記データを得る第１復号化手段と、
前記復号化方式情報が第２復号化方式情報である場合、前記公開鍵リストに含まれる分散管理者アドレス情報に基づいて、前記暗号化データ記憶手段内のｎ個の暗号化分散鍵を個別に送信する暗号化分散鍵送信手段と、
前記各暗号化分散鍵の送信先で分散管理者秘密鍵により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を復元するデータ鍵復元手段と、
このデータ鍵に基づいて前記暗号化データを復号化して前記データを得る第２復号化手段と
を備え、
前記ユーザ端末は、
前記データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、前記ユーザＩＤとを、前記秘密情報管理装置に送信するためのデータ送信手段と、
前記暗号化データの復号化要求を前記復号化方式情報とともに前記秘密情報管理装置に送信する復号化要求送信手段と、
前記暗号化データ鍵及び該暗号化データ鍵の復号化要求を前記秘密情報管理装置から受信した場合、該暗号化データ鍵を前記ユーザ秘密鍵により復号化し、該秘密情報管理装置にデータ鍵を送信するデータ鍵送信手段と
を備えたことを特徴とする秘密情報管理システム。

【請求項３】
データを入力するためのユーザ端末と、しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用して、前記データを暗号化した暗号化データを記憶するための秘密情報管理装置とを備えた秘密情報管理システムであって、
前記秘密情報管理装置は、
前記暗号化データと、データ鍵と、分散数ｎ個分の分散管理者ＩＤと、しきい値ｋと、ユーザＩＤとを受信するための暗号化データ受信手段と、
互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個以上含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵とを含む公開鍵リストを予め記憶する公開鍵リスト記憶手段と、

前記受信したユーザＩＤに基づいて、前記公開鍵リスト記憶手段から前記ユーザ公開鍵を検索し、該ユーザ公開鍵を用いて前記データ鍵を暗号化し、暗号化データ鍵を生成する暗号化データ鍵生成手段と、
前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、
前記データ受信手段が受信するｎ個の分散管理者ＩＤに関連する分散管理者公開鍵を前記公開鍵リスト記憶手段から読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の暗号化分散鍵を生成する暗号化分散鍵生成手段と、
前記暗号化データ、前記暗号化データ鍵および前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と
を備え、
前記ユーザ端末は、
前記データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、前記ユーザＩＤとを入力するための手段と、
乱数を用いてデータ鍵を生成するデータ鍵生成手段と、
このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、
前記暗号化データと、前記データ鍵と、前記ｎ個分の分散管理者ＩＤと、前記しきい値ｋとを前記秘密情報管理装置に送信する暗号化データ送信手段と
を備えたことを特徴とする秘密情報管理システム。

【請求項４】
請求項３に記載の秘密情報管理システムにおいて、
前記秘密情報管理装置は、
前記暗号化データ受信手段、前記公開鍵リスト記憶手段、前記暗号化データ鍵生成手段、前記分散鍵生成手段および前記暗号化分散鍵生成手段を有する鍵管理装置と、
前記暗号化データ記憶手段を有する暗号化データ管理装置と
を備えたことを特徴とする秘密情報管理システム。

【請求項５】
請求項４に記載の秘密情報管理システムにおいて、
前記鍵管理装置は、
前記暗号化データ鍵およびｎ個の暗号化分散鍵を前記ユーザ端末に送信する手段
を備え、
前記ユーザ端末は、
前記暗号化データ、前記暗号化データ鍵およびｎ個の暗号化分散鍵を互いに関連付けて記憶する手段
を備えたことを特徴とする秘密情報管理システム。

【請求項６】
しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用可能な秘密情報管理装置であって、
データと、ユーザＩＤとを受信するためのデータ受信手段と、
互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵を含む公開鍵リストを、前記しきい値ｋに関連付けて予め記憶する公開鍵リスト記憶手段と、
乱数を用いてデータ鍵を生成するデータ鍵生成手段と、
このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、
前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、
前記受信したユーザＩＤから、前記公開鍵リスト内のｎ個の分散管理者公開鍵を読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の

暗号化分散鍵を生成する暗号化分散鍵生成手段と、
前記暗号化データおよび前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と、
前記暗号化データの復号化要求を受信した場合、前記公開鍵リストに含まれるｎ個の分散管理者アドレス情報に基づいて、前記暗号化データ記憶手段内のｎ個の暗号化分散鍵を個別に送信する暗号化分散鍵送信手段と、
前記各暗号化分散鍵の送信先で分散管理者秘密鍵により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を復元するデータ鍵復元手段と、
このデータ鍵に基づいて前記暗号化データを復号化して前記データを得る復号化手段とを備えたことを特徴とする秘密情報管理装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データを暗号化して記憶するための秘密情報管理装置および秘密情報管理システムに係り、例えば、ユーザが暗号鍵をなくした場合にも、暗号化したデータを復号化し得る秘密情報管理装置および秘密情報管理システムに関する。
【背景技術】
【０００２】
近年、秘密情報として管理すべきデータを暗号化して記憶するための秘密情報管理装置が利用されている。例えば、企業においては、ユーザが個人で秘密情報を管理するよりも、会社全体で一元的に秘密情報を管理した方が良い場合がある。このような場合に秘密情報管理装置が利用される。
【０００３】
秘密情報管理装置においては、秘密情報（以下、単にデータともいう）を暗号化および復号化するために、暗号鍵が用いられる。ただし、個々のデータを各々異なる暗号鍵で暗号化する場合には、データの数に比例してユーザの鍵管理の負担が増加してしまう。
【０００４】
係る負担を軽減させる観点から、ユーザに階層的な参照許可を与えることにより、ユーザが管理する鍵情報を少なくできる暗号化ファイル共有方法が提案されている（例えば特許文献１参照）。
【０００５】
特許文献１記載の方法では、複数人がアクセスするサーバ（秘密情報管理装置）において、ディレクトリ毎に同一の暗号鍵でファイル（データ）を暗号化する。このとき、ファイルの参照権限を表現する階層構造と、ディレクトリの階層構造とが一致しており、ディレクトリＩＤｎの中に、その直接下位にある全てのディレクトリの暗号鍵をそのディレクトリＩＤｎの暗号鍵で暗号化して格納しておくので、ユーザは、階層構造のある１つのディレクトリの暗号鍵を持つだけでその下位にある全てのディレクトリを参照できる。
【０００６】
それゆえ、個々のデータを各々異なる暗号鍵で暗号化する場合に比べ、ユーザの鍵管理の負担が軽減される。
【特許文献１】特開平６－１７５９０５号公報（請求項１、第９段落、第１８段落、図1、要約書など）
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、上述した特許文献１記載の方法では、ユーザが暗号鍵をなくした場合には、ディレクトリ内の全てのデータを参照することができなくなる。換言すれば、ユーザの鍵管理の負担が軽減される反面、一つの暗号鍵をなくした場合の影響が大きくなる事態が生じる。

【０００８】
例えば、ＩＣカード等の記憶媒体に暗号鍵を記憶している場合、その記憶媒体を紛失等すると、秘密情報管理装置内の全ての暗号化されたデータを復号化できなくなる。
【０００９】
本発明は上記実情に鑑みてなされたものであり、ユーザが暗号鍵をなくした場合にも、暗号化したデータを復号化し得る秘密情報管理装置および秘密情報管理システムを提供することを目的とする。
【課題を解決するための手段】
【００１０】
第1の発明は上記課題を解決するために、しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用可能な秘密情報管理装置であって、データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、ユーザＩＤとを受信するためのデータ受信手段と、互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個以上含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵を含む公開鍵リストを予め記憶する公開鍵リスト記憶手段と、乱数を用いてデータ鍵を生成するデータ鍵生成手段と、このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、前記受信したユーザＩＤに基づいて、前記公開鍵リスト記憶手段から前記ユーザ公開鍵を検索し、該ユーザ公開鍵を用いて前記データ鍵を暗号化し、暗号化データ鍵を生成する暗号化データ鍵生成手段と、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、前記データ受信手段が受信するｎ個の分散管理者ＩＤに関連する分散管理者公開鍵を前記公開鍵リスト記憶手段から読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の暗号化分散鍵を生成する暗号化分散鍵生成手段と、前記暗号化データ、前記暗号化データ鍵および前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と、前記暗号化データの復号化要求を復号化方式情報とともに受信した場合、該復号化方式情報が、第１復号化方式情報および第２復号化方式情報のいずれであるかを判定する復号化方式判定手段と、前記復号化方式情報が第１復号化方式情報である場合、前記暗号化データ鍵を該暗号化データ鍵の復号化要求とともに、前記復号化方式情報の送信元に送信する暗号化データ鍵送信手段と、前記暗号化データ鍵の復号化要求に応じて、前記ユーザ公開鍵に対応するユーザ秘密鍵により復号化されたデータ鍵を前記復号化方式情報の送信元から受信した場合、このデータ鍵により前記暗号化データを復号化して前記データを得る第１復号化手段と、前記復号化方式情報が第２復号化方式情報である場合、前記公開鍵リストに含まれる分散管理者アドレス情報に基づいて、前記暗号化データ記憶手段内のｎ個の暗号化分散鍵を個別に送信する暗号化分散鍵送信手段と、前記各暗号化分散鍵の送信先で分散管理者秘密鍵により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を復元するデータ鍵復元手段と、このデータ鍵に基づいて前記暗号化データを復号化して前記データを得る第２復号化手段とを備えた秘密情報管理装置を提供する。
【００１１】
第２の発明は、データを入力するためのユーザ端末と、しきい値ｋおよび分散数ｎの（ｋ，ｎ）型の秘密分散方式を使用して、前記データを暗号化した暗号化データを記憶するための秘密情報管理装置とを備えた秘密情報管理システムであって、前記秘密情報管理装置が、前記データと、分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、ユーザＩＤとを受信するためのデータ受信手段と、互いに関連付けられた分散管理者ＩＤと分散管理者公開鍵と分散管理者アドレス情報との組をｎ個以上含み、かつ前記ユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵を含む公開鍵リストを予め記憶する公開鍵リスト記憶手段と、乱数を用いてデータ鍵を生成するデータ鍵生成手段と、このデータ鍵に基づいて前記データを暗号化し、暗号化データを生成する暗号化データ生成手段と、前記受信したユーザＩＤに基づいて、前記公開鍵リスト記憶手段から前記ユーザ公開鍵を検索し、該ユーザ公開鍵を用いて前記データ鍵を暗号化し、暗号化データ鍵を生成する暗号化データ鍵生成

手段と、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を秘密分散し、ｎ個の分散鍵を生成する分散鍵生成手段と、前記データ受信手段が受信するｎ個の分散管理者ＩＤに関連する分散管理者公開鍵を前記公開鍵リスト記憶手段から読み込み、該ｎ個の分散管理者公開鍵に基づいて、前記ｎ個の分散鍵を個別に暗号化し、ｎ個の暗号化分散鍵を生成する暗号化分散鍵生成手段と、前記暗号化データ、前記暗号化データ鍵および前記ｎ個の暗号化分散鍵が記憶される暗号化データ記憶手段と、前記暗号化データの復号化要求を復号化方式情報とともに前記ユーザ端末から受信した場合、該復号化方式情報が、第１復号化方式情報および第２復号化方式情報のいずれであるかを判定する復号化方式判定手段と、前記復号化方式情報が第１復号化方式情報である場合、前記暗号化データ鍵を該暗号化データ鍵の復号化要求とともに前記ユーザ端末に送信する暗号化データ鍵送信手段と、前記暗号化データ鍵の復号化要求に応じて、前記ユーザ公開鍵に対応するユーザ秘密鍵により復号化されたデータ鍵を前記ユーザ端末から受信するデータ鍵受信手段と、前記データ鍵受信手段により受信したデータ鍵により前記暗号化データを復号化して前記データを得る第１復号化手段と、前記復号化方式情報が第２復号化方式情報である場合、前記公開鍵リストに含まれる分散管理者アドレス情報に基づいて、前記暗号化データ記憶手段内のｎ個の暗号化分散鍵を個別に送信する暗号化分散鍵送信手段と、前記各暗号化分散鍵の送信先で分散管理者秘密鍵により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合、前記（ｋ，ｎ）型の秘密分散方式に基づいて前記データ鍵を復元するデータ鍵復元手段と、このデータ鍵に基づいて前記暗号化データを復号化して前記データを得る第２復号化手段とを備え、前記ユーザ端末が、前記データと、前記分散数ｎ個分の分散管理者ＩＤと、前記しきい値ｋと、前記ユーザＩＤとを、前記秘密情報管理装置に送信するためのデータ送信手段と、前記暗号化データの復号化要求を前記復号化方式情報とともに前記秘密情報管理装置に送信する復号化要求送信手段と、前記暗号化データ鍵及び該暗号化データ鍵の復号化要求を前記秘密情報管理装置から受信した場合、該暗号化データ鍵を前記ユーザ秘密鍵により復号化し、該秘密情報管理装置にデータ鍵を送信するデータ鍵送信手段とを備えた秘密情報管理システムを提供する。

【００１２】

なお、以上の各発明では、各装置を「装置」とし、各装置の集合体を「システム」として表現しているが、これに限らず、システム又は装置毎に「プログラム」として表現してもよく、また、システム又は装置毎に「方法」として表現してもよい。すなわち、本発明は、任意の名称やカテゴリーで表現可能となっている。

【００１３】

（作用）

第１および第２の発明では、暗号化データ鍵を送信した後、ユーザ秘密鍵により復号化されたデータ鍵を受信し、このデータ鍵により暗号化データを復号化してデータを得る第1復号化方式と、ｎ個の暗号化分散鍵を送信してｋ個の分散鍵を受信することにより、（ｋ，ｎ）型の秘密分散方式に基づいてデータ鍵を復元し、得られたデータ鍵に基づいて暗号化データを復号化してデータを得る第２復号化方式との２つの復号化方式をそれぞれ用いることができる。

【００１４】

これにより、ユーザが暗号鍵（ユーザ秘密鍵）を保持する場合には第１復号化方式を用いることにより、暗号化したデータを復号化することができる。また、ユーザが暗号鍵（ユーザ秘密鍵）をなくした場合にも第２復号化方式を用いることにより、暗号化したデータを復号化することができる。

【発明の効果】

【００１５】

本発明によれば、ユーザが暗号鍵をなくした場合にも、暗号化したデータを復号化し得る秘密情報管理装置および秘密情報管理システムを提供できる。

【発明を実施するための最良の形態】

【００１６】

以下、図面を参照して本発明の実施形態を説明する。

【００１７】

＜第1の実施形態＞

（１－１．構成）

図１は本発明の第１の実施形態に係る秘密情報管理システムの構成を示す模式図である。

【００１８】

秘密情報管理システムは、データを暗号化した暗号化データを記憶するための秘密情報管理装置１０と、データを入力するためのユーザ端末２０と、分散管理者端末３０Ａ～３０Ｎとを備えている。（以下の説明において、分散管理者端末を総称して説明するときは単に３０と表記し、各端末を個別に説明するときは添え字Ａ～Ｎを付して表記する。）

秘密情報管理装置１０は、「しきい値ｋ」および「分散数ｎ」の（ｋ，ｎ）型の秘密分散方式を使用可能なものであり、一般的なパーソナルコンピュータ（ＰＣ）により構成される。なお、（ｋ，ｎ）型の秘密分散方式とは、秘密情報（ここではデータ鍵）をｎ個の分散情報（ここでは分散鍵）に分割し、ｎ個の分散情報の中から任意のｋ個を集めれば元の秘密情報を復元可能な技術である。但し、ｋ個より１個少ないｋ－１個の分散情報からでは、元の秘密情報に関する情報が全く得られない。すなわち、（ｋ，ｎ）型の秘密分散方式は、しきい値ｋを境にした秘密情報の復元特性をもっている（なお、１＜ｋ＜ｎ）。以下、（ｋ，ｎ）型の秘密分散方式を（ｋ，ｎ）しきい値法ともいう。

【００１９】

秘密情報管理装置１０は、具体的には、通信装置１１とＣＰＵ１２・ディスク装置１３・メモリ１４とを備えている。

【００２０】

通信装置１１は、ユーザ端末２０や分散管理者端末３０とネットワークを介して通信するものであり、「データD」・分散数ｎ個分の分散管理者ＩＤ・しきい値ｋ・ユーザＩＤをユーザ端末２０から受信する。また、通信装置１１は、ユーザ端末２０またはネットワーク上の公開鍵簿（図示せず）からユーザ公開鍵Pxを受信する。

【００２１】

ＣＰＵ１２は、秘密情報管理装置１０の演算処理を実行するものであり、具体的には、ディスク装置１３に記憶された各種プログラムをメモリ１４に読み込んで、後述するデータ鍵生成部１５や秘密分散部１６・暗号化部１７・データ管理部１８・復号化部１９の処理を実行する。ここで、各種プログラムとは、各部１５～１９の機能を秘密情報管理装置１０のコンピュータに実現させるためのプログラムである。

【００２２】

ディスク装置１３は、情報を記憶して保存するためのハードディスク等であり、公開鍵リスト記憶部１３Ｐおよび暗号化データ記憶部１３Ｑとして機能する。

【００２３】

公開鍵リスト記憶部１３Ｐは、互いに関連付けられた分散管理者ＩＤと、分散管理者公開鍵と、分散管理者アドレス情報との組をｎ個以上含み、かつユーザＩＤと該ユーザＩＤに対応するユーザ公開鍵を含む「公開鍵リストＬ」を予め記憶するものである（図２参照）。また、公開鍵リスト記憶部１３Ｐは、通信装置１１によりユーザ端末２０から受信されるデータDのデータ名称（以下、“data”と称する）と、分散数ｎ個分の分散管理者ＩＤと、しきい値ｋとを、データを送信したユーザのユーザＩＤと関連付けて、「分散管理者ＩＤリスト」として記憶する（図２参照）。

【００２４】

なお、データ名称“data”は、例えばデータＤがファイルである場合のファイル名であり、予めデータＤに含まれている。また、しきい値ｋは、必ずしも記憶される必要は無い。例えば（ｋ，ｎ）を固定して（ｋ，ｎ）しきい値法を用いる場合、しきい値ｋの入力が省略されるため、しきい値ｋが記憶されない。

【００２５】

暗号化データ記憶部１３Ｑは、後述する暗号化データ$E_K(D)$・暗号化データ鍵$E_{Px}(K)$・ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を、データ名称“data”と互いに関連付けて記憶する（図３参照）。

【００２６】

メモリ１４は、ＣＰＵ１２が各種プログラムを実行するために用いるＲＡＭ等の記憶装置である。ここでは、ディスク装置１３に記憶された各種プログラムがメモリ１４に読み込まれると、ＣＰＵ１２が、データ鍵生成部１５や秘密分散部１６・暗号化部１７・データ管理部１８・復号化部１９として機能することになる。

【００２７】

データ鍵生成部１５は、ユーザ端末２０からデータDを受信する度に、乱数を用いて「データ鍵K」を生成するものである。生成されるデータ鍵Ｋは、乱数自体でもよく、乱数から算出された値でもよい。

【００２８】

秘密分散部１６は、データ鍵生成部１５により生成されたデータ鍵Kを、（ｋ，ｎ）しきい値法により、「ｎ個の分散鍵B1,B2…Bn」に分散するものである。なお、しきい値ｋおよび分散数ｎは、通信装置１１を介してユーザ端末２０から送信される数値である。

【００２９】

暗号化部１７は、各種データを暗号化するものであり、データ鍵生成部１５で生成されたデータ鍵Kを用いて、ユーザ端末２０から送信されたデータDを暗号化する機能を有する。これにより「暗号化データ$E_K(D)$」が生成される。また、受信したユーザＩＤに基づいて、公開鍵リスト記憶部１３Ｐからユーザ公開鍵Pxを検索し、該ユーザ公開鍵Pxを用いてデータ鍵Kを暗号化し、「暗号化データ鍵$E_{Px}(K)$」を生成する機能を有する。さらに、暗号化部１７は、通信装置１１が受信するｎ個の分散管理者ＩＤに関連する「分散管理者公開鍵P1,P2…Pn」を公開鍵リスト記憶部１３Ｐから読み込み、該ｎ個の分散管理者公開鍵に基づいて、秘密分散部１６により生成されたｎ個の分散鍵B1,B2…Bnを個別に暗号化して、「ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$」を生成する機能を有する。

【００３０】

データ管理部１８は、データDの暗号化または復号化の命令を行なうものである。データの暗号化処理に際しては、各部１５・１６・１７を介して生成された暗号化データ$E_K(D)$・暗号化データ鍵$E_{Px}(K)$・暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を一セットにして暗号化データ記憶部１３Ｑに書き込む機能を有する。また、暗号化データ$E_K(D)$の復号化処理に際しては、暗号化データ記憶部１３Ｑに記憶された暗号化データ$E_K(D)$・暗号化データ鍵$E_{Px}(K)$・暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$等の情報を読み出して復号化部１９に送出する機能を有する。

【００３１】

復号化部１９は、ユーザ端末２０から送信された復号化方式情報が、第１復号化方式情報F1および第２復号化方式情報F2のいずれであるかを判定する機能と、その判定結果に応じて、暗号化データ記憶部１３Ｑに記憶された暗号化データ$E_K(D)$を復号化する機能とを備えている。

【００３２】

詳しくは、復号化方式情報が第１復号化方式情報F1である場合、暗号化データ鍵$E_{Px}(K)$を、その暗号化データ鍵の復号化要求とともにユーザ端末２０に送信する。そして、暗号化データ鍵$E_{Px}(K)$の復号化要求に応じて、ユーザ公開鍵Pxに対応するユーザ秘密鍵Sxにより復号化されたデータ鍵Kをユーザ端末２０から受信した場合、受信したデータ鍵Kにより暗号化データ$E_K(D)$を復号化する。

【００３３】

一方、復号化方式情報が第２復号化方式情報F2である場合、公開鍵リスト記憶部１３Ｐに予め記憶された公開鍵リストLに含まれるｎ個の分散管理者アドレス情報に基づいて、暗号化データ記憶部１３Ｑ内のｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を分散管理者端末３０に個別に送信する。この後、各暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$の送信

先で「分散管理者秘密鍵S1,S2…Sn」により暗号化分散鍵が個別に復号化され、ｋ個の送信先から分散鍵を受信した場合には、（ｋ，ｎ）しきい値法に基づいてデータ鍵Kを復元する。そして、この復元されたデータ鍵Kに基づいて暗号化データ$E_K(D)$を復号化する。

【００３４】

ユーザ端末２０は、通常のパーソナルコンピュータの機能を有し、ユーザの操作により、秘密情報管理装置１０にデータDを入力したり、暗号化データ$E_K(D)$の復号化要求をしたりするものである。ユーザ端末２０は、具体的には図４に示すように、互いにバスを介して接続された記憶部２１と入力部２２・演算部２３・通信部２４・表示部２５とを備えている。

【００３５】

記憶部２１は、ユーザ公開鍵Pxに対応する「ユーザ秘密鍵Sx」を記憶するメモリである。なお、ユーザ秘密鍵Sxは、ユーザのみが知り得るパスワード等により暗号化されてから記憶される。また、ユーザ秘密鍵Sxは、ＩＣカード等の外部記憶装置に記憶されているとしても良い。

【００３６】

入力部２２は、データDの暗号化や復号化を実行するための情報を入力するものである。例えば、データDを暗号化する際には、データD・分散管理者ＩＤ・しきい値ｋや、ユーザを識別するための「ユーザＩＤ」の入力を可能とする。但し、しきい値ｋは、必ずしも入力される必要は無い。例えば（ｋ，ｎ）を固定して（ｋ，ｎ）しきい値法を用いる場合、しきい値ｋを入力しなくてよい。また、暗号化データ$E_K(D)$を復号化する際には、その暗号化データ$E_K(D)$を指定するためのデータ名称“data”や復号化方式情報の入力を可能とする。なお、「復号化方式情報」には、暗号化データ鍵に基づいて暗号化データの復号化を命令するための第1復号化方式情報F1と、暗号化分散鍵に基づいて暗号化データの復号化を命令するための第２復号化方式情報F2とがある。第２復号化方式情報F2を入力する場合で且つ各分散管理者の承認が必要な場合（図５参照）、ユーザの入力操作により、暗号化データ$E_K(D)$の復号化要求にユーザ情報（例、ユーザＩＤ、ユーザ氏名、ユーザ属性）を含め、このユーザ情報を秘密情報管理装置１０が暗号化分散鍵とともに各分散管理者端末３０に送信する構成としてもよい。これに限らず、予め秘密情報管理装置１０がユーザ情報を記憶しておき、暗号化データ$E_K(D)$の復号化要求に含まれるデータ名称“data”に基づいてディスク装置１３を参照し、対応するユーザＩＤに該当するユーザ情報を、暗号化分散鍵とともに各分散管理者端末３０に送信する構成としてもよい。なお、各分散管理者の承認が不要な場合には、これらユーザ情報に関する構成が省略可能となっている。

【００３７】

演算部２３は、秘密情報管理装置１０からの復号化要求に応じて、暗号化データ鍵$E_{Px}(K)$を復号化するためのものである。具体的には、記憶部２１に記憶されたユーザ秘密鍵Sxを用いて、暗号化データ鍵$E_{Px}(K)$を復号化する。また、ユーザ秘密鍵SxがＩＣカードに記憶されている場合には、暗号化データ鍵$E_{Px}(K)$をＩＣカード内で復号化させるコマンドをＩＣカードに送出する。

【００３８】

通信部２４は、秘密情報管理装置１０との通信を可能にするものである。なお、秘密情報管理装置１０と通信する際には、データを送信するユーザを識別するために、ユーザＩＤ等の入力が必要とされる。

【００３９】

表示部２５は、入力部２２の入力情報や秘密情報管理装置１０から送信されるデータ等を表示するためのディスプレイ等である。

【００４０】

分散管理者端末３０は、秘密情報管理装置１０から暗号化分散鍵の復号化要求を受信した場合、必要に応じて、暗号化分散鍵$E_{P1}(B1)$,$E_{P2}(B2)$…$E_{Pn}(Bn)$を「分散管理者秘密鍵S1,S2…Sn」により個別に復号化するものである。また、復号化した分散鍵を、秘密情報管理装置１０に送信する。

【００４１】
なお、分散管理者端末３０は、暗号化分散鍵の復号化要求を受信した場合、図５に画面構成の例を示すように、暗号化データの復号化要求を行なったユーザ情報を画面表示し、分散管理者に復号化の承認を求める機能をもっている（図５において、“NO”ボタンを選択すると、暗号化分散鍵の復号化が拒否される）。したがって、分散管理者端末３０を操作する分散管理者が、暗号化分散鍵の復号化を承認しないと判断した場合には、秘密情報管理装置１０に分散鍵を送信しないようにすることができる。
【００４２】
（１－２．動作）
次に本実施形態に係る秘密情報管理システムの動作を説明する。
【００４３】
（データの暗号化）
まず、本実施形態に係る秘密情報管理システムによるデータの暗号化の動作を図６のフローチャートを用いて説明する。なお、暗号化する際のデータフローの概念を図７に示す。
【００４４】
始めに、ユーザ端末２０では、ユーザの操作により、データD・分散数ｎ個分の分散管理者ＩＤ・しきい値ｋ・ユーザＩＤが入力される。そして、ユーザ端末２０は、これらの入力データを、秘密情報管理装置１０に送信する。
【００４５】
秘密情報管理装置１０は、受信した入力データをメモリ１４に記憶するとともに、ユーザＩＤと、データ名称“data”と、分散管理者ＩＤと、しきい値ｋとを互いに関連付けてなる「分散管理者ＩＤリスト」を公開鍵リスト記憶部１３Ｐに記憶する。
【００４６】
しかる後、秘密情報管理装置１０では、データ鍵生成部１５において乱数を用いてデータ鍵Kを生成する（ステップＳ１，Ｓ２）。さらに、秘密情報管理装置１０では、そのデータ鍵Kにより、暗号化部１７がデータDを暗号化して暗号化データ$E_K(D)$を生成する（ステップＳ３）。
【００４７】
続いて、暗号化部１７は、受信したユーザＩＤに基づいて、公開鍵リスト記憶部１３Ｐからユーザ公開鍵Pxを検索する。そして、そのユーザ公開鍵Pxに基づいて、ステップＳ２で生成したデータ鍵Kを暗号化し、暗号化データ鍵$E_{Px}(K)$を生成する（ステップＳ４）。
【００４８】
また、秘密分散部１６が、（ｋ，ｎ）しきい値法により、ステップＳ２で生成したデータ鍵Kから、ｎ個の分散鍵B1,B2・・・Bnを生成する（ステップＳ５）。
【００４９】
続いて、暗号化部１７は、受信した分散管理者ＩＤに関連する分散管理者公開鍵P1,P2・・・Pnを公開鍵リストＬから読み込み、該ｎ個の分散管理者公開鍵P1,P2・・・Pnに基づいて、秘密分散によって生成された各分散鍵B1,B2・・・Bnを個別に暗号化し、ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を生成する（ステップＳ６）。
【００５０】
そして、秘密情報管理装置１０のデータ管理部１８が、暗号化データ$E_K(D)$・暗号化データ鍵$E_{Px}(K)$・各暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を一セットにして、ディスク装置１３の暗号化データ記憶部１３Ｑに記憶する（ステップＳ７）。
【００５１】
（暗号化データの復号化）
次に、本実施形態に係る秘密情報管理システムによる暗号化データの復号化の動作を図８のフローチャートを用いて説明する。なお、第２復号化方式により復号化する際のデータフローの概念を図９に示す。
【００５２】

始めに、ユーザ端末２０は、ユーザの操作により、暗号化データ$E_K(D)$の復号化要求を秘密情報管理装置１０に送信する。この際、復号化要求とともに、暗号化データ$E_K(D)$のデータ名称“data”や復号化方式情報（F1またはF2）等も送信される。なお、復号化方式情報の送信内容は、ユーザ端末２０の表示部２５上でユーザの操作により選択される。例えば、ユーザ秘密鍵SxがＩＣカードに記憶されているとき、図１０に画面構成の一例を示すように、ＩＣカードの有無に応じて、“ＩＣカードが有る場合”又は“ＩＣカードが無い場合”がユーザの操作により選択されると、“ＩＣカードが有る場合”の選択により第１復号化方式情報F1が送信され、“ＩＣカードが無い場合”の選択により第２復号化方式情報F2が送信される。

【００５３】

秘密情報管理装置１０は、復号化要求等を受信すると、復号化方式情報が第1復号化方式情報F1および第２復号化方式情報F2のいずれであるかを判定する（ステップＴ１，Ｔ２）。

【００５４】

ここで、復号化方式情報が第1復号化方式情報F1である場合、秘密情報管理装置１０では、復号化部１９が、暗号化データ記憶部１３Ｑに記憶された暗号化データ鍵$E_{Px}(K)$を復号化要求とともにユーザ端末２０に送信する（ステップＴ３）。

【００５５】

ユーザ端末２０は、受信した暗号化データ鍵$E_{Px}(K)$をユーザ秘密鍵Sxにより復号化し、得られたデータ鍵Ｋを秘密情報管理装置１０に送信する。

【００５６】

この後、秘密情報管理装置１０では、受信したデータ鍵Kを用いて、復号化部１９が暗号化データ$E_K(D)$を復号化する（ステップＴ５）。

【００５７】

一方、ステップＴ２において、復号化方式情報が第２復号化方式情報F2である場合、秘密情報管理装置１０では、復号化部１９が、公開鍵リスト記憶部１３Ｐ内の公開鍵リストLに含まれるｎ個の分散管理者アドレス情報に基づいて、暗号化データ記憶部１３Ｑ内のｎ個の暗号化分散鍵$E_{P1}(B1)$,$E_{P2}(B2)\cdots E_{Pn}(Bn)$を、各分散管理者端末３０Ａ～３０Ｎに個別に送信する。（ステップＴ６）。

【００５８】

これを受けて、各分散管理者端末３０Ａ～３０Ｎにおいて、復号化を承認するか否かが判断される。具体的には、ユーザ端末２０を介して暗号化データ$E_K(D)$の復号化要求を行なったユーザに対し、データDの参照を許可するか否かが、各分散管理者端末３０Ａ～３０Ｎを利用する分散管理者により個別に判断される。

【００５９】

分散管理者端末３０では、分散管理者がデータDの復号化を許可した場合、受信した暗号化分散鍵を分散管理者秘密鍵により復号化する（図９の分散管理者端末３０Ａ・３０Ｂ）。そして、復号化を許可した分散管理者端末３０Ａ・３０Ｂは、秘密情報管理装置１０に分散鍵を返信する。

【００６０】

一方、分散管理者がデータDの復号化を拒否した場合には、分散管理者端末３０では暗号化分散鍵を復号化しないため、秘密情報管理装置１０に分散鍵が返信されない（図９の分散管理者端末３０Ｃ）。

【００６１】

続いて、秘密情報管理装置１０では、復号化部１９が、公開鍵リスト記憶部１３Ｐ内のしきい値ｋを参照し、複数の分散管理者端末３０から受信した分散鍵の個数がしきい値ｋ個以上であるか否かを判定する（ステップＴ８）。

【００６２】

ｋ個以上であると判定した場合、秘密情報管理装置１０では、復号化部１９が（ｋ，ｎ）しきい値法に基づいて、ｋ個の分散鍵からデータ鍵Kを復元する（ステップＴ８－Ｙｅ

ｓ，Ｔ９）。そして、復号化部１９は、復元したデータ鍵Kにより暗号化データ$E_K(D)$を復号化する（ステップＴ５）。

【００６３】

一方、ステップＴ８において、ｋ個より少ないと判定した場合、秘密情報管理装置１０では、分散鍵からデータ鍵Kを復元せず、暗号化データ$E_K(D)$を復号化できないとして処理を終了する（ステップＴ８－Ｎｏ，Ｔ１０）。

【００６４】

（１－３．効果）

以上説明したように、本実施形態に係る秘密情報管理装置１０は、データDの暗号化に際し、（ｋ，ｎ）型の秘密分散方式に基づいてデータ鍵Kを秘密分散し、ｎ個の分散鍵B1,B2・・・Bnを生成する秘密分散部１６と、公開鍵リストL内のｎ個の分散管理者公開鍵P1,P2・・・Pnに基づいて、ｎ個の分散鍵B1,B2・・・Bnを個別に暗号化し、ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を生成する暗号化部１７と、暗号化データ$E_K(D)$・暗号化データ鍵$E_{Px}(K)$・ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を関連付けて記憶する暗号化データ記憶部１３Ｑとを備えており、また、暗号化分散鍵に基づいて暗号化データを復号化する場合、公開鍵リストLに含まれるｎ個の分散管理者アドレス情報に基づいて、ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を分散管理者端末３０Ａ～３０Ｎに個別に送信し、各暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$の送信先で個別に分散管理者秘密鍵S1,S2…Snにより暗号化分散鍵が復号化され、ｋ個の送信先から分散鍵を受信した場合、（ｋ，ｎ）型の秘密分散方式に基づいてデータ鍵Kを復元し、このデータ鍵Kに基づいて暗号化データ$E_K(D)$を復号化してデータDを得る復号化部１９とを備えているので、ユーザ秘密鍵Sxがなくなった場合にも、しきい値ｋ個以上の分散鍵を収集してデータ鍵Kを復元することによりデータDを復号化できる。

【００６５】

換言すると、秘密情報管理装置１０は、暗号化データ鍵$E_{Px}(K)$を送信した後、ユーザ秘密鍵Sxにより復号化されたデータ鍵Kを受信し、このデータ鍵Kにより暗号化データ$E_K(D)$を復号化してデータを得る第1復号化方式と、ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を送信してｋ個の分散鍵を受信することにより、（ｋ，ｎ）型の秘密分散方式に基づいてデータ鍵Ｋを復元し、得られたデータ鍵Ｋに基づいて暗号化データ$E_K(D)$を復号化してデータＤを得る第２復号化方式との２つの復号化方式をそれぞれ用いることができる。これにより、ユーザが暗号鍵（ユーザ秘密鍵Sx）を保持する場合には第１復号化方式を用いることにより、暗号化したデータを復号化することができる。また、ユーザが暗号鍵（ユーザ秘密鍵Sx）をなくした場合にも第２復号化方式を用いることにより、暗号化したデータを復号化することができる。

【００６６】

また、本実施形態に係る秘密情報管理システムによれば、ユーザ秘密鍵Sxだけをユーザは管理すればよく、分散管理者も分散管理者秘密鍵P1,P2・・・Pnだけを管理すればよいので、各人における鍵の管理を簡易化できる。

【００６７】

特に、各人の秘密鍵をＩＣカードにより管理する場合、安全性および利便性をより高くしたシステムを構築することができる。また、各人に携帯されるＩＣカードを用いることにより、他者の使用可能な端末２０，３０を用いる場合に比べ、データの復号化に関して明確かつ安全に個人の意思を反映することができる。また、ＩＣカードを用いることにより、各人の意思決定から復号化までを一連の暗号技術により提供することができる。

【００６８】

なお、本実施形態に係る秘密情報管理装置１０は、分散数ｎ個分の分散管理者ＩＤと、しきい値ｋとをユーザ端末２０から受信しているが、これらの情報は予め記憶されていても良い。これは、ユーザ毎に分散管理者が予め指定されていることに相当する。具体的には、図１１に示すように、秘密情報管理装置１０のディスク装置１３が、ユーザＩＤ毎に、分散管理者ＩＤとしきい値ｋとを予め「分散管理者ＩＤリスト」として記憶する。これ

により、ユーザからデータが送信された場合に、ユーザＩＤ毎に分散管理者ＩＤリストによって指定される分散管理者ＩＤに関連して、公開鍵リストＬ内の分散管理者公開鍵で分散鍵が暗号化されるようにすることができる。すなわち、ユーザ毎に分散管理者が予め指定されており、その指定された分散管理者の分散管理者端末３０に分散鍵を送信する構成としてもよい。また、どのデータがどのユーザの管理下にあるかというテーブル情報が「データ管理者リスト」としてディスク装置１３に記憶される（図１１参照）。

【００６９】

＜第２の実施形態＞

図１２は本発明の第２の実施形態に係る秘密情報管理システムの構成を示す模式図である。なお、既に説明した部分と同一部分には同一符号を付し、特に説明がない限りは重複した説明を省略する。また、以下の各実施形態も同様にして重複した説明を省略する。

【００７０】

本実施形態においては、第１の実施形態とは異なり、ユーザ端末２０がデータ鍵Kと暗号化データ$E_K(D)$とを生成する構成となっている。すなわち、ユーザ端末２０の演算部２３が、乱数を用いてデータ鍵Kを生成する機能と、このデータ鍵Kに基づいてデータDを暗号化し、暗号化データ$E_K(D)$を生成する機能とを有している。それゆえ、秘密情報管理装置１０Ｓは、図１に示した構成に比べ、データ鍵生成部１５が省略された構成となっている。また、秘密情報管理装置１０Ｓでは、データの暗号化も行なわれない。なお、暗号化データ$E_K(D)$とデータ鍵Kとは、分散管理者ＩＤ・しきい値ｋ・ユーザＩＤとともに通信部２４を介して秘密情報管理装置１０Ｓに送信される。

【００７１】

次に、本実施形態に係る秘密情報管理システムによるデータの暗号化の動作を、図１３のフローチャートおよび図１４のデータフローの概念図を参照して説明する。

【００７２】

始めに、ユーザ端末２０では、ユーザの操作により、データD・分散数ｎ個分の分散管理者ＩＤ・しきい値ｋ・ユーザＩＤが入力される（Ｕ１）。

【００７３】

続いて、ユーザ端末２０の演算部２３が、乱数を用いてデータ鍵Ｋを生成する（Ｕ２）。また、演算部２３は、このデータ鍵Ｋを用いてデータＤを暗号化して、暗号化データ$E_K(D)$を生成する（Ｕ３）。そして、ユーザ端末２０の通信部２４が、これらのデータを記憶部２１内のユーザＩＤとともに秘密情報管理装置１０Ｓに送信する（Ｕ４，Ｕ５）。

【００７４】

次に、秘密情報管理装置１０Ｓは、暗号化データ$E_K(D)$・データ鍵Ｋ・分散管理者ＩＤ（ｎ人分）・しきい値ｋ・ユーザＩＤを入力データとしてユーザ端末２０から受け取ると、これら入力データをメモリ１４に記憶するとともに、ユーザＩＤと、データ名称“data”と、分散管理者ＩＤと、しきい値ｋとを互いに関連付けてなる分散管理者ＩＤリストを公開鍵リスト記憶部１３Ｐに記憶する。

【００７５】

そして、秘密分散部１６が、（ｋ，ｎ）しきい値法により、メモリ１４内のデータ鍵Ｋから、ｎ個の分散鍵B1,B2…Bnを生成する（Ｕ６）。

【００７６】

続いて、秘密情報管理装置１０Ｓでは、前述同様に、暗号化部１７がｎ個の分散鍵B1,B2…Bnを分散管理者公開鍵P1,P2…Pnにより個別に暗号化して、暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を生成する（Ｕ７）。

【００７７】

また、暗号化部１７は、公開鍵リストＬ内のユーザ公開鍵Pxでデータ鍵Ｋを暗号化し、暗号化データ鍵$E_{Px}(K)$を生成する（Ｕ８）。

【００７８】

そして、秘密情報管理装置１０Ｓのデータ管理部１８が、これらの暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$および暗号化データ鍵$E_{Px}(K)$を、ユーザ端末２０から送信された暗

号化データ$E_K(D)$に関連付けて暗号化データ記憶部１３Ｑに記憶する（Ｕ９）。
【００７９】
なお、暗号化データ$E_K(D)$の復号化の動作は、第1の実施形態と同様にして行なわれる。
【００８０】
以上説明したように、本実施形態に係る秘密情報管理システムにおいては、データ鍵Ｋの生成およびデータＤの暗号化をユーザ端末２０で行なう。それゆえ、暗号化されていないデータＤを秘密情報管理装置１０Ｓに送信せずに済むので、データの秘匿性を高めることができる。
【００８１】
補足すると、第1の実施形態に係る秘密情報管理装置１０においては、暗号化されていないデータＤを受け取るので、秘密情報管理装置１０の管理者はデータを閲覧することができる。これに対し、本実施形態に係る秘密情報管理装置１０Ｓでは、暗号化されていないデータＤではなく暗号化データ$E_K(D)$を受け取るので、秘密情報管理装置１０Ｓの管理者は、単純にはデータＤを閲覧することができないことになる。
【００８２】
＜第３の実施形態＞
図１５は本発明の第３の実施形態に係る秘密情報管理システムの構成を示す模式図である。
【００８３】
本実施形態においては、第２の実施形態とは異なり、前述した秘密情報管理装置１０Ｓが鍵管理装置４０と暗号化データ管理装置５０とに分割されている。この鍵管理装置４０と暗号化データ管理装置５０とは、秘密情報管理装置１０Ｔを構成する。
【００８４】
鍵管理装置４０においては、公開鍵リスト記憶部１３Ｐとしてディスク装置４３が機能し、各種プログラムをメモリ４４が読み込んで、ＣＰＵ４２が、秘密分散部１６・暗号化部１７・復号化部１９として機能する。
【００８５】
暗号化データ管理装置５０においては、暗号化データ記憶部１３Ｑとしてディスク装置５３が機能し、各種プログラムをメモリ５４が読み込んで、ＣＰＵ５２がデータ管理部１８として機能する。
【００８６】
また両装置４０・５０は、通信装置４１・５１を介して暗号化データ等の送受信を行なう。
【００８７】
次に、本実施形態に係る秘密情報管理システムによるデータの暗号化の動作を、図１６のフローチャートおよび図１７のデータフローの概念図を参照して説明する。
【００８８】
始めに、ユーザ端末２０では、ユーザの操作により、データＤ・分散管理者ＩＤ・しきい値ｋ・ユーザＩＤが入力される（Ｖ１）。
【００８９】
続いて、ユーザ端末２０の演算部２３が、乱数を用いてデータ鍵Ｋを生成する（Ｖ２）。そして、演算部２３は、このデータ鍵Ｋを用いてデータＤを暗号化し、暗号化データ$E_K(D)$を生成する（Ｖ３）。
【００９０】
次に、ユーザ端末２０は、データ鍵Ｋ・分散管理者ＩＤ・しきい値ｋ・ユーザＩＤを鍵管理装置４０へ送信し（Ｖ４）、暗号化データ$E_K(D)$を暗号化データ管理装置５０へ送信する（Ｖ５）。
【００９１】
鍵管理装置４０では、受信したデータ鍵Ｋ・分散管理者ＩＤ・しきい値ｋ・ユーザＩＤをメモリ４４に記憶するとともに、ユーザＩＤと、データ名称“data”と、分散管理者Ｉ

Ｄと、しきい値ｋとを互いに関連付けてなる分散管理者ＩＤリストをディスク装置４３の公開鍵リスト記憶部１３Ｐに記憶する。しかる後、鍵管理装置４０では、メモリ４４内のデータ鍵Ｋを、秘密分散部１６が公開鍵リストLおよびしきい値ｋに基づき、（ｋ，ｎ）しきい値法により分散して、ｎ個の分散鍵B1,B2…Bnを生成する（Ｖ６）。そして、鍵管理装置４０では、暗号化部１７が、受信した分散管理者ＩＤに関連する分散管理者公開鍵P1,P2・・・Pnを公開鍵リストＬから読み込み、該ｎ個の分散管理者公開鍵P1,P2…Pnに基づいて各分散鍵B1,B2…Bnを個別に暗号化して、ｎ個の暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)を生成する（Ｖ７）。

【００９２】

また、暗号化部１７は、ユーザ公開鍵Pxでデータ鍵Kを暗号化し、暗号化データ鍵E_{Px}(Ｋ)を生成する（Ｖ８）。

【００９３】

しかる後、鍵管理装置４０は、ｎ個の暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)と、暗号化データ鍵E_{Px}(Ｋ)とを暗号化データ管理装置５０に送信する（Ｖ９）。

【００９４】

暗号化データ管理装置５０では、データ管理部１８が、これらｎ個の暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)と暗号化データ鍵E_{Px}(Ｋ)とを、ユーザ端末２０から受け取った暗号化データE_K(D)に関連付けてディスク装置５３の暗号化データ記憶部１３Ｑに記憶する（Ｖ１０）。

【００９５】

なお、暗号化データE_K(D)の復号化の動作は、第1の実施形態と同様にして行なわれる。ただし、復号化動作を行なう主体は、復号化部１９を有する鍵管理装置４０である。

【００９６】

以上説明したように、本実施形態に係る秘密情報管理システムにおいては、秘密情報管理装置１０Ｔを、鍵管理装置４０と暗号化データ管理装置５０との別装置に分割して構成するので、データの秘匿性を高めることができる。

【００９７】

補足すると、第２の実施形態に係る秘密情報管理装置１０Ｓにおいては、データ鍵Ｋを受信する装置と、暗号化データE_K(D)を記憶する装置とが単一の装置であるため、秘密情報管理装置１０Ｓの管理者が、受信したデータ鍵Ｋに基づいて暗号化データE_K(D)を復号化できる。これに対し、本実施形態に係る秘密情報管理装置１０Ｔでは、鍵管理装置４０がデータ鍵Ｋを受信し、暗号化データ管理装置５０が暗号化データE_K(D)等を記憶する。そのため、鍵管理装置４０のメモリ４４がＲＡＭである場合、電源が切れるとデータ鍵Ｋが消去され、暗号化データ管理装置５０に記憶された暗号化データE_K(D)を復号化することができなくなる。それゆえ、データＤの秘匿性を高めることができる。

【００９８】

また、第２の実施形態に係る秘密情報管理装置１０Ｓにおいては、各暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)と暗号化データE_K(D)とを単一の装置に記憶するため、秘密情報管理装置１０Ｓの管理者は、公開鍵リストＬに基づいて暗号化分散鍵E_{P1}(B1),E_{P2}(B2)…E_{Pn}(Bn)を復号化処理することにより、データＤを閲覧できる場合がある。これに対し、本実施形態に係る秘密情報管理装置１０Ｔにおいては、鍵管理装置４０が公開鍵リストＬを記憶し、暗号化データ管理装置５０が暗号化データE_K(D)等を記憶する。それゆえ、鍵管理装置４０と暗号化データ管理装置５０との両装置に記憶された情報を揃えなければ暗号化データE_K(D)を復号化できないので、データＤの秘匿性を高めることができる。

【００９９】

＜第４の実施形態＞

図１８は本発明の第４の実施形態に係る秘密情報管理システムの構成を示す模式図である。

【０１００】

本実施形態においては、第３の実施形態とは異なり、暗号化データ管理装置５０を省略

した構成となっており、鍵管理装置４０が、生成した暗号化データ鍵$E_{Px}(K)$およびｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$をユーザ端末２０に返信する機能をもっている。ユーザ端末２０では、暗号化データ鍵$E_{Px}(K)$およびｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$が返信されると、それらを暗号化データ$E_K(D)$と互いに関連付けて記憶部２１に記憶する。

【０１０１】

次に、本実施形態に係る秘密情報管理システムによるデータの暗号化の動作を、図１９のフローチャートおよび図２０のデータフローの概念図を参照して説明する。

【０１０２】

始めに、ユーザ端末２０は、前述した処理Ｖ１～Ｖ４と同一の処理Ｗ１～Ｗ４を実行し、データ鍵K・分散管理者ＩＤ（ｎ人分）・しきい値ｋ・ユーザＩＤの情報を鍵管理装置４０へ送信する（Ｗ４）。

【０１０３】

鍵管理装置４０では、受信したデータ鍵Ｋ・分散管理者ＩＤ・しきい値ｋ・ユーザＩＤをメモリ４４に記憶するとともに、ユーザＩＤと、データ名称“data”と、分散管理者ＩＤと、しきい値ｋとを互いに関連付けてなる分散管理者ＩＤリストを公開鍵リスト記憶部１３Ｐに記憶する。

【０１０４】

しかる後、鍵管理装置４０では、前述した処理Ｖ６～Ｖ８と同一の処理Ｗ５～Ｗ７を実行し、ｎ個の暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$を生成する（Ｗ６）とともに、暗号化データ鍵$E_{Px}(K)$を生成する（Ｗ７）。

【０１０５】

それから、鍵管理装置４０は、これらの暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$および暗号化データ鍵$E_{Px}(K)$を、データ鍵Kの送信元であるユーザ端末２０に返信する（Ｗ８）。

【０１０６】

ユーザ端末２０では、暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$および暗号化データ鍵$E_{Px}(K)$を受信すると、それらを暗号化データ$E_K(D)$と互いに関連付けて記憶部２１に記憶する（Ｗ９）。

【０１０７】

なお、暗号化データ$E_K(D)$の復号化の動作は、第1の実施形態と同様にして行なわれる。ただし、復号化動作を行なう主体は、復号化部１９を有する鍵管理装置４０であり、復号化部１９は、暗号化データ鍵および暗号化分散鍵をユーザ端末２０から読み込む。

【０１０８】

以上説明したように、本実施形態に係る秘密情報管理システムによれば、鍵管理装置４０により生成された暗号化分散鍵$E_{P1}(B1),E_{P2}(B2)\cdots E_{Pn}(Bn)$をユーザ端末２０が記憶するので、ユーザ秘密鍵Sxをなくした場合にも、しきい値ｋ個以上の分散鍵を収集してデータ鍵Kを復元することにより暗号化データ$E_K(D)$ を復号化できる。

【０１０９】

また、本実施形態に係る秘密情報管理システムを用いれば、暗号化したデータをユーザ端末２０に記憶しておくことにより、ユーザ端末２０を他人に使用されてもデータを閲覧されることがなく、かつユーザ秘密鍵Sxをなくしても暗号化データ$E_K(D)$を復号化し得るシステムを構築することができる。

【０１１０】

なお、復号化動作を行なう主体は、鍵管理装置４０に限らず、あらゆる可能性が考えられる。例えば、復号化部１９の機能をコンピュータに実現させるためのプログラムをユーザ端末２０又は分散管理者端末３０にインストールすることにより、ユーザ端末２０又は分散管理者端末３０に復号化動作を行なわせるように変形することができる。

【０１１１】

＜その他＞

なお、上記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。

【０１１２】

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。

【０１１３】

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。

【０１１４】

さらに、本発明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。

【０１１５】

また、記憶媒体は１つに限らず、複数の媒体から上記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。

【０１１６】

尚、本発明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。

【０１１７】

また、本発明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。

【図面の簡単な説明】

【０１１８】

【図１】本発明の第１の実施形態に係る秘密情報管理システムの構成を示す模式図である。

【図２】同実施形態に係る公開鍵リスト記憶部の構成を示す模式図である。

【図３】同実施形態に係る暗号化データ記憶部の構成を示す模式図である。

【図４】同実施形態に係るユーザ端末の構成を示す模式図である。

【図５】同実施形態に係る分散管理者装置の画面構成の例を示す模式図である。

【図６】同実施形態に係る暗号化の動作を説明するためのフローチャートである。

【図７】同実施形態に係る暗号化のデータフローの概念図である。

【図８】同実施形態に係る復号化の動作を説明するためのフローチャートである。

【図９】同実施形態に係る第２復号化方式による復号化のデータフローの概念図である。

【図１０】同実施形態に係るユーザ端末の画面構成の一例を示す模式図である。

【図１１】同実施形態に係るディスク装置の変形例を示す模式図である。

【図１２】本発明の第２の実施形態に係る秘密情報管理システムの構成を示す模式図である。

【図１３】同実施形態に係る暗号化の動作を説明するためのフローチャートである。

【図１４】同実施形態に係る動作を説明するためのデータフローの概念図である。

【図１５】本発明の第３の実施形態に係る秘密情報管理システムの構成を示す模式図である。

【図１６】同実施形態に係る暗号化の動作を説明するためのフローチャートである。

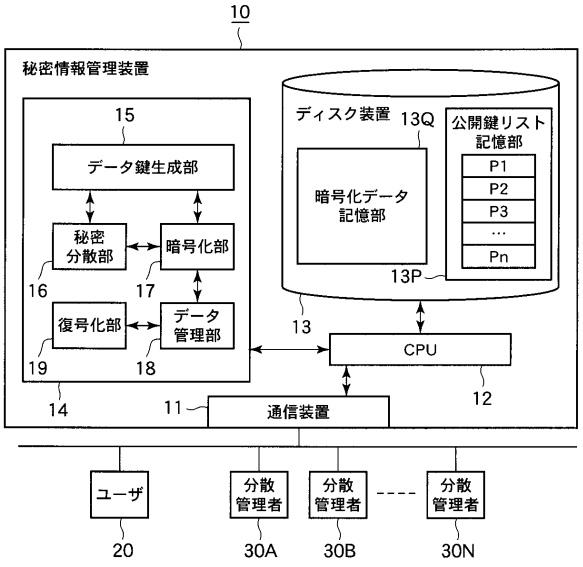
【図１７】同実施形態に係る動作を説明するためのデータフローの概念図である。

【図１８】本発明の第４の実施形態に係る秘密情報管理システムの構成を示す模式図であ

る。
【図１９】同実施形態に係る暗号化の動作を説明するためのフローチャートである。
【図２０】同実施形態に係る動作を説明するためのデータフローの概念図である。
【符号の説明】
【０１１９】
１０・１０Ｓ・１０Ｔ・・・秘密情報管理装置、１１・・・通信装置、１２・・・ＣＰＵ、１３・・・ディスク装置、１３Ｐ・・・公開鍵リスト記憶部、１３Ｑ・・・暗号化データ記憶部、１４・・・メモリ、１５・・・データ鍵生成部、１６・・・秘密分散部、１７・・・暗号化部、１８・・・データ管理部、１９・・・復号化部、２０・・・ユーザ端末、２１・・・記憶部、２２・・・入力部、２３・・・演算部、２４・・・通信部、２５・・・表示部、３０・・・分散管理者端末、４０・・・鍵管理装置、４１・・・通信装置、４２・・・ＣＰＵ、４３・・・ディスク装置、４４・・・メモリ、５０・・・暗号化データ管理装置、５１・・・通信装置、５２・・・ＣＰＵ、５３・・・ディスク装置、５４・・・メモリ。

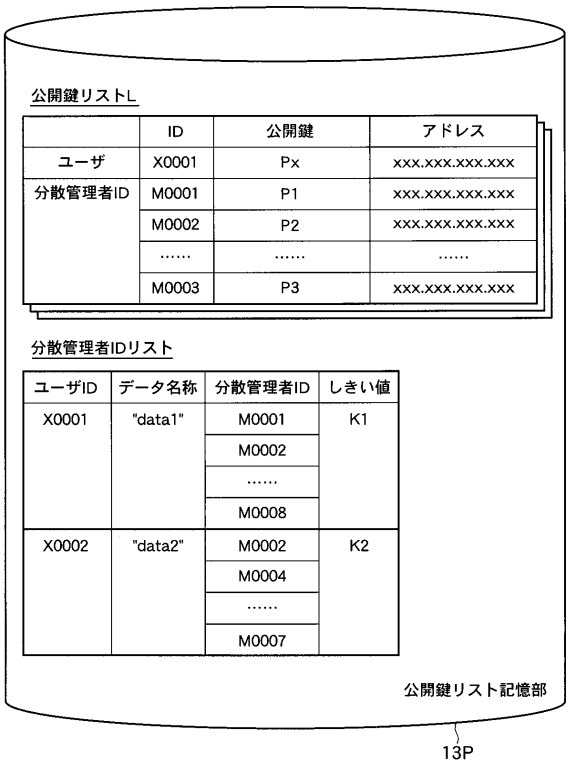
【図１】

図1



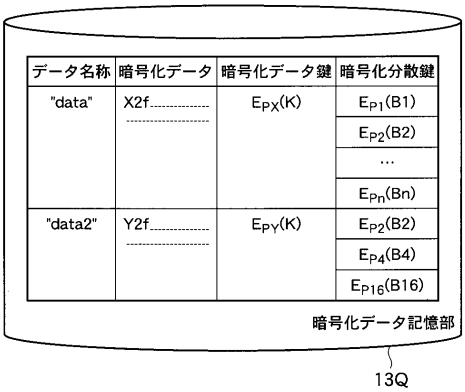
【図２】

図2



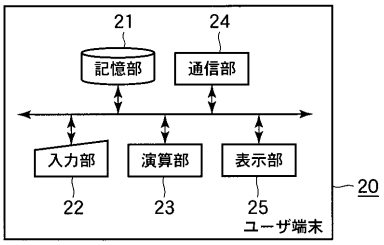
【図３】

図３



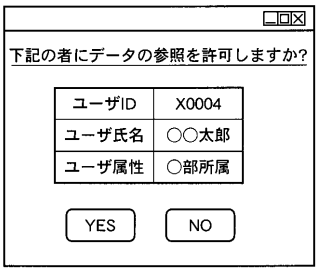
【図４】

図４



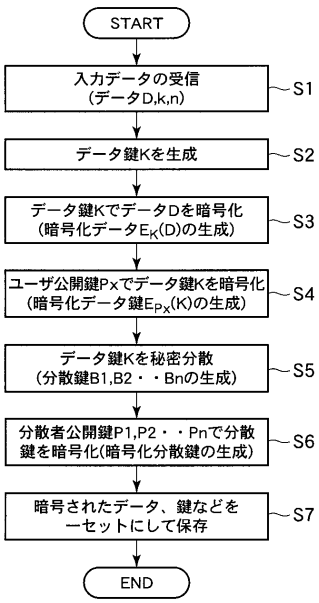
【図５】

図５



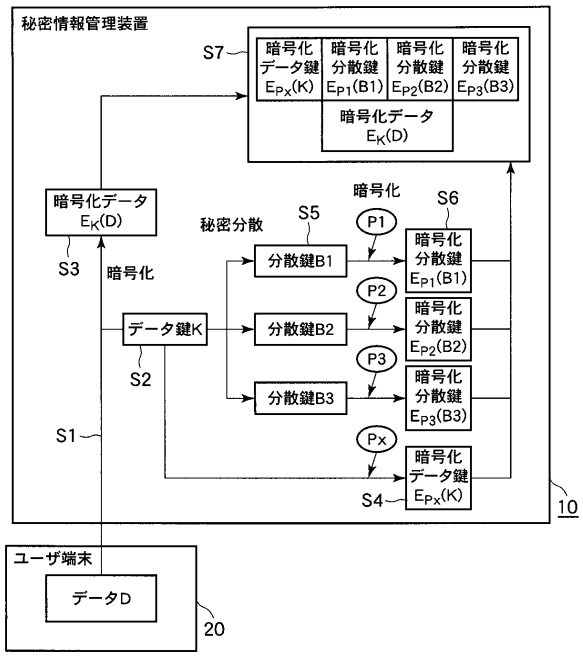
【図６】

図６



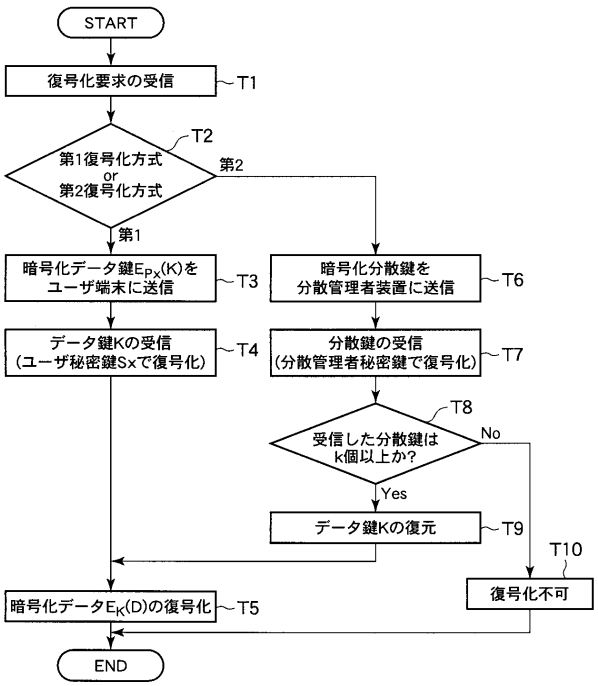
【図７】

図７



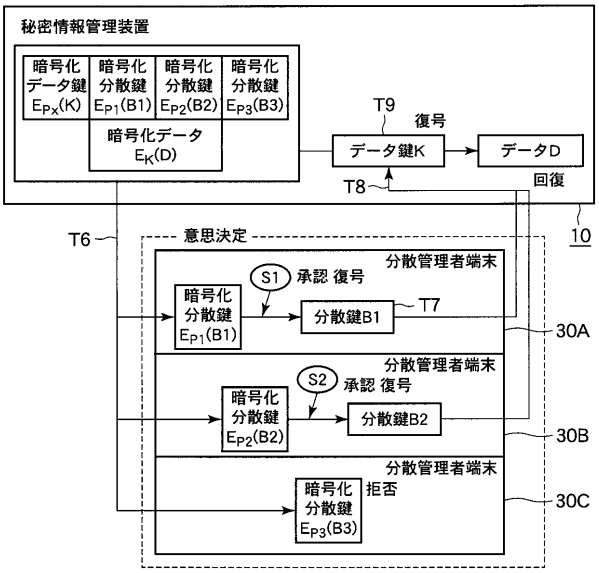
【図８】

図８



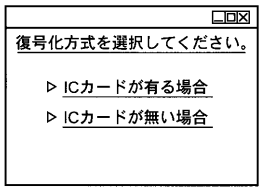
【図９】

図９



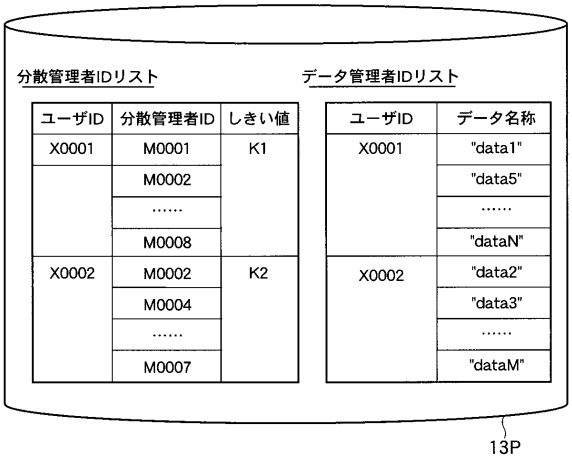
【図１０】

図10



【図１１】

図11



分散管理者IDリスト

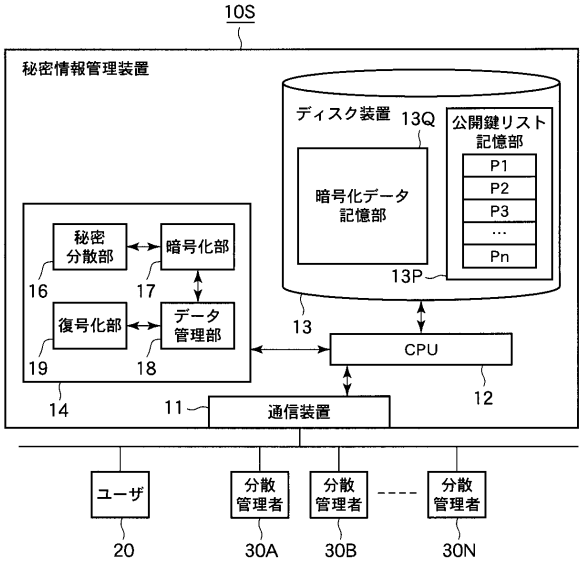
ユーザID	分散管理者ID	しきい値
X0001	M0001	K1
	M0002	
	……	
	M0008	
X0002	M0002	K2
	M0004	
	……	
	M0007	

データ管理者IDリスト

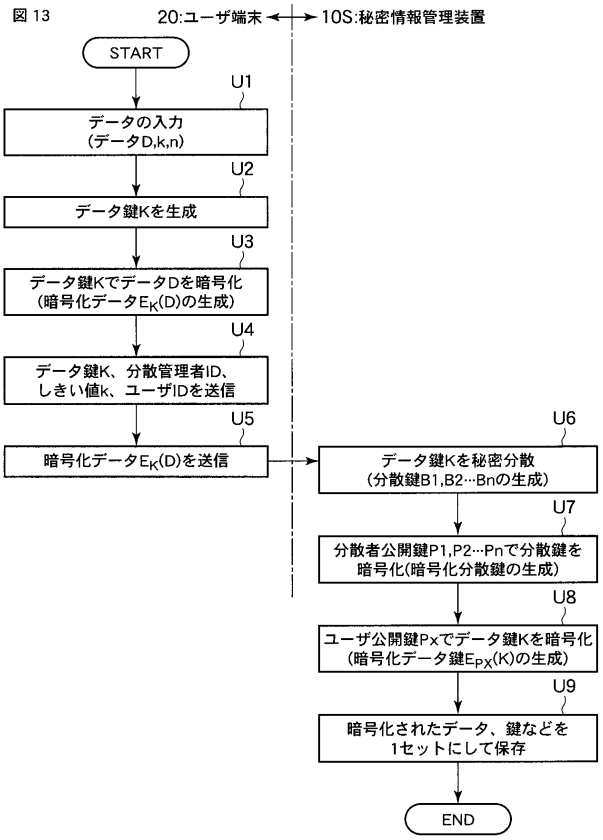
ユーザID	データ名称
X0001	"data1"
	"data5"
	……
	"dataN"
X0002	"data2"
	"data3"
	……
	"dataM"

【図１２】

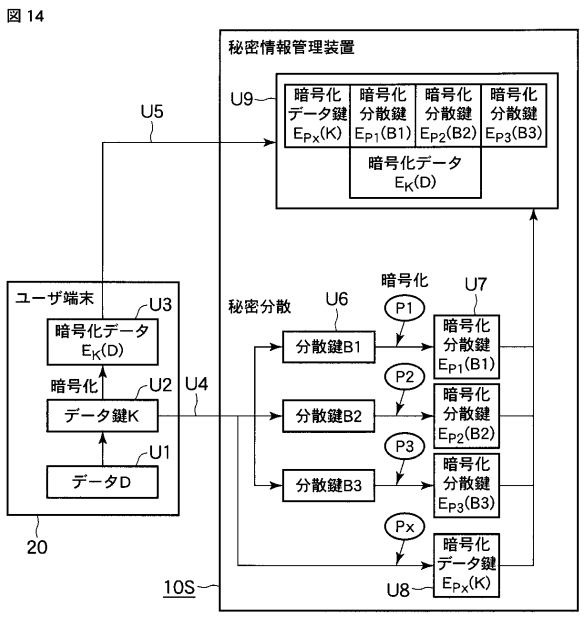
図12



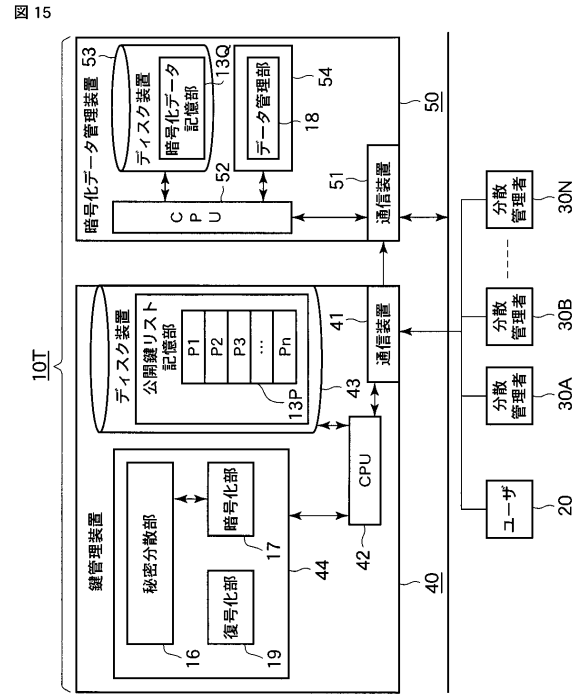
【図１３】



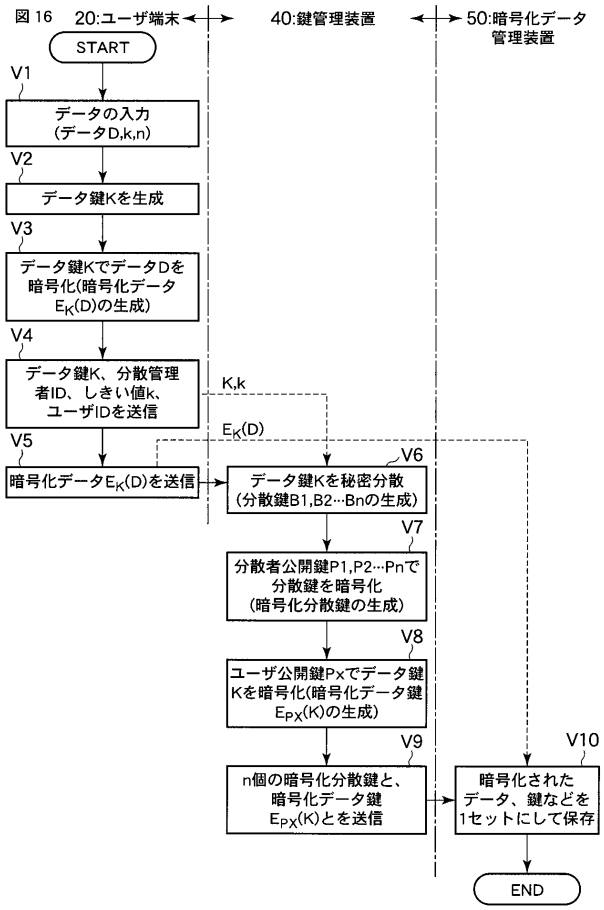
【図１４】



【図１５】

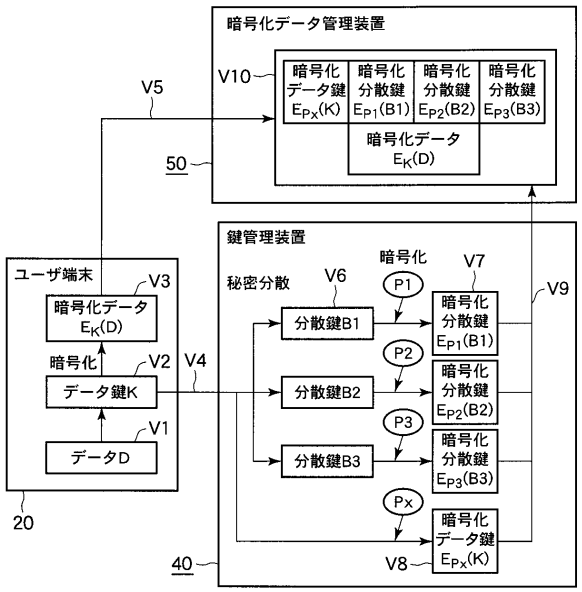


【図１６】



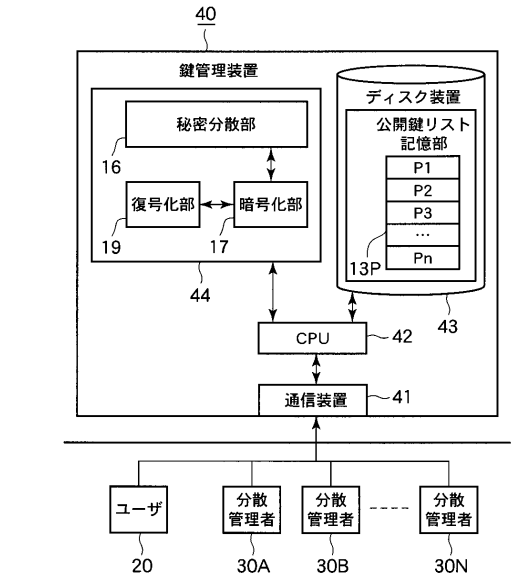
【図１７】

図 17



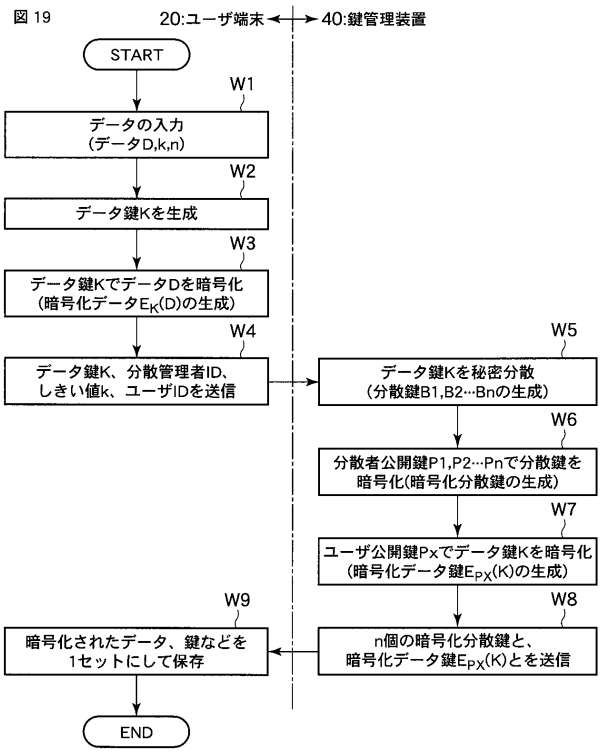
【図１８】

図 18



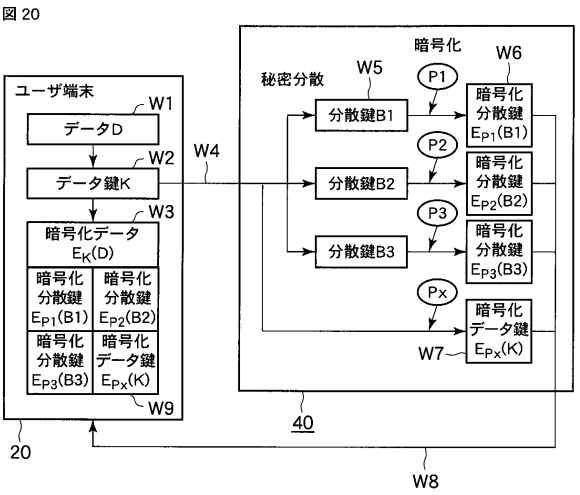
【図１９】

図 19



【図２０】

図 20



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 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 楯岡 正道
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 田中 友也
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
Ｆターム(参考) 5J104 AA16 EA04 EA11 EA13 JA21 MA05 NA02 NA27 NA37