(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2010-45670
(P2010-45670A)
(43)公開日　平成22年2月25日(2010.2.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601Z	5B017
H04L 12/22	(2006.01)	H04L	12/22		5J104
H04L 9/14	(2006.01)	H04L	9/00	641	5K030
G06F 21/24	(2006.01)	G06F	12/14	510F	
		G06F	12/14	540A	

審査請求 有　請求項の数 4　ＯＬ　（全 34 頁）

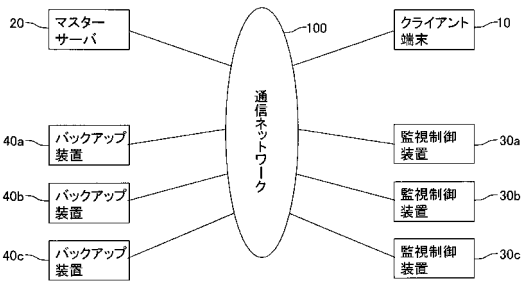
(21)出願番号　特願2008-209152 (P2008-209152)
(22)出願日　平成20年8月15日 (2008.8.15)

(71)出願人　800000068
学校法人東京電機大学
東京都千代田区神田錦町２－２
(74)代理人　100119677
弁理士　岡田　賢治
(74)代理人　100115794
弁理士　今下　勝博
(72)発明者　上野　洋一郎
東京都千代田区神田錦町２－２　学校法人東京電機大学内
(72)発明者　宮保　憲治
東京都千代田区神田錦町２－２　学校法人東京電機大学内

最終頁に続く

(54)【発明の名称】ネットワークシステム

(57)【要約】
【課題】本発明は、安全かつ高信頼性のファイルバックアップ用ネットワークシステムを構築することを目的とする。
【解決手段】上記目的を達成するために、本発明に係るネットワークシステムは、複数のクライアント端末１０と、マスターサーバ２０と、複数の監視制御装置３０ａ、３０ｂ、３０ｃと、複数のバックアップ装置４０ａ、４０ｂ、４０ｃと、を備え、一台で構成されることを前提としていた監視制御装置に対して、データファイルの復号に必要な情報に応じて監視制御装置３０ａ、３０ｂ、３０ｃを分散配備することを特徴とする。機能分散化された監視制御装置３０ａ、３０ｂ、３０ｃのすべてが外部より侵入されない限り、データファイルの復元及び漏洩を防止することができる。
【選択図】図１



【特許請求の範囲】
【請求項１】
少なくとも１つのマスターサーバと、複数の監視制御装置と、複数のクライアント端末と、が通信ネットワークを介して互いに接続されたネットワークシステムにおいて、
前記マスターサーバは、
データファイルを第１の暗号鍵で暗号化し、暗号化した前記ファイルデータを複数の分割データに分割し、前記分割データを複製し、複製した前記分割データを第２の暗号鍵で暗号化して出力する秘匿化手段と、
前記秘匿化手段の出力する暗号化済分割情報を前記複数のクライアント端末に送信する暗号化済分割情報送信手段と、
前記第１の暗号鍵で暗号化した前記ファイルデータの分割から前記分割データを第２の暗号鍵で暗号化するまでの前記秘匿化手段の手順を記録したファイルシーケンス情報及び前記第１の暗号鍵をそれぞれ複製し、前記複数の監視制御装置のうちの異なる監視制御装置に送信する秘匿化情報送信手段と、を備え、
前記複数のクライアント端末は、
前記暗号化済分割情報送信手段の送信する暗号化済分割情報を受信する暗号化済分割情報受信手段と、
前記暗号化済分割情報受信手段の受信する前記暗号化済分割情報を格納する暗号化済分割情報格納手段と、を備え、
前記複数の監視制御装置は、
前記秘匿化情報送信手段の送信する前記ファイルシーケンス情報又は前記第１の暗号鍵を受信する秘匿化情報受信手段と、
前記秘匿化情報受信手段の受信する前記ファイルシーケンス情報又は前記第１の暗号鍵を格納する秘匿化情報格納手段と、を備えることを特徴とするネットワークシステム。
【請求項２】
前記監視制御装置と通信ネットワークを介して接続された複数のバックアップ装置をさらに備え、
前記監視制御装置は、
前記秘匿化情報格納手段の格納する前記ファイルシーケンス情報又は前記第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、秘密分散法を用いて複数のバックアップ情報に分散させる秘密分散処理手段と、
前記秘密分散処理手段からの前記バックアップ情報を、前記複数のバックアップ装置のうちの異なるバックアップ装置に送信するバックアップ情報送信手段と、をさらに備え、
前記バックアップ装置は、
前記バックアップ情報送信手段の送信する前記バックアップ情報を受信するバックアップ情報受信手段と、
前記バックアップ情報受信手段の受信する前記バックアップ情報を格納するバックアップ情報格納手段と、をさらに備え、
前記秘密分散法は、前記秘密分散化情報送信手段が前記秘密分散化情報を送信する前記バックアップ装置の数をｎとし、前記ファイルシーケンス情報又は前記第１の暗号鍵を復元するために必要な前記バックアップ装置の数をｋとした場合に、完全置換系の表Ｓ（ｋ，ｎ，ｄ）が、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）の第ｎ列に０を追加した表、及び、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）の第ｎ列に１を追加した表で表されることを特徴とする請求項１に記載のネットワークシステム。
【請求項３】
前記マスターサーバは、
前記ファイルシーケンス情報を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させるファイルシーケンス秘密分散処理手段と、
前記第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させる暗号鍵秘密分散処理手段と、をさらに備え、

前記秘匿化情報送信手段は、前記ファイルシーケンス秘密分散処理手段及び前記暗号鍵秘密分散処理手段からの前記ファイルシーケンス情報及び前記第１の暗号鍵を送信し、
前記秘密分散法は、前記バックアップ装置の数をｎとし、前記ファイルシーケンス情報又は前記第１の暗号鍵を復元するために必要な前記バックアップ装置の数をｋとした場合に、完全置換系の表Ｓ（ｋ，ｎ，ｄ）が、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）の第ｎ列に０を追加した表、及び、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）の第ｎ列に１を追加した表で表されることを特徴とする請求項１又は２に記載のネットワークシステム。
【請求項４】
前記監視制御装置は、
前記クライアント端末の状態を示すクライアント端末状態情報の送信を要求するクライアント端末状態報告要求を、前記複数のクライアント端末に送信するクライアント端末状態報告要求送信手段と、
前記クライアント端末から送信された前記クライアント端末状態情報を受信するクライアント端末状態情報受信手段と、
クライアント端末状態情報受信手段の受信する前記クライアント端末状態情報、及び、前記クライアント端末状態報告要求を送信してから前記クライアント端末状態情報を受信するまでの応答時間に基づいて、前記クライアント端末との間のスループットを測定するスループット等測定手段と、
クライアント端末状態情報受信手段の受信する前記クライアント端末状態情報及び前記スループット等測定手段の測定したスループットをクライアント端末リストとして前記マスターサーバに送信するクライアント端末リスト送信手段と、をさらに備え、
前記クライアント端末は、
前記クライアント端末状態報告要求送信手段の送信するクライアント端末状態報告要求を受信すると、クライアント端末の状態を検出してクライアント端末状態情報を出力するリソース情報伝達手段と、
前記リソース情報伝達手段の出力するクライアント端末状態情報を、前記監視制御装置へ送信するクライアント端末状態情報送信手段と、を備え、
前記マスターサーバは、
前記クライアント端末リスト送信手段の送信するクライアント端末リストに基づいて、前記秘匿化手段における分割数及び複製数を決定する分割複製数決定手段と、
前記クライアント端末リスト送信手段の送信するクライアント端末リストに基づいて、前記暗号化済分割情報送信手段における前記暗号化済分割情報を送信する前記クライアント端末を決定する送信先決定手段と、をさらに備え、
前記秘匿化手段は、前記分割複製数決定手段の決定する分割数及び複製数に分割及び複製し、
前記暗号化済分割情報送信手段は、前記送信先決定手段の決定する前記クライアント端末に前記暗号化済分割情報を送信することを特徴とする請求項１から３のいずれかに記載のネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ファイルバックアップ用のネットワークシステムに関し、特に、ディザスタリカバリ技術を用いて、バックアップファイルの復元に必要な情報の秘密分散技術に関する。
【背景技術】
【０００２】
現在、使用される社会インフラを構成するための各種システム構築に係る情報や各種の個人情報等のデータベース化が進んでいる。地方自治体や病院などの公共施設においても例外ではなく、住民の個人情報や医療情報といった各種のデータファイルを格納するデータベースを、災害時に迅速に復旧するためのバックアップが求められている。

【０００３】
システムの障害がもたらす損失を減らすために、種々のバックアップシステムが提案されている。例えば、主及び副の２つのサイトを用意し、通信ネットワークを介して副サイトへデータファイルをバックアップするためのシステムや、ＧＲＩＤ技術を用いて、大規模データファイルをバックアップするためのシステムである（例えば、特許文献１参照。）。
【０００４】
一方、秘密情報分散の方式に関しては、Ａｄｉ　Ｓｈａｍｉｒの（ｋ，ｎ）閾値秘密情報分散が知られている（例えば、非特許文献１参照。）。この方法は連立一次方程式を用いて次のように実現される。この方式では暗号鍵Ｋを秘密分散で配布することになる。
【０００５】
まず初期設定として、十分大きな素数ｐに対して整数ｘ１，ｘ２，・・・，x_n，Ｋ∈$(F_p)^*$をランダムにとる。ここで、Ｋは暗号鍵である。また、Ｚを有理整数環として、F_p＝Ｚ／（ｐ）、$(F_p)^*$＝｛ｘ∈Ｆ｜ｘ≠０｝とする。
【０００６】
次に、分散させる情報を作成する。ランダムにa_1，a_2，・・・，a_{k-1}∈$(F_p)^*$を選ぶ。多項式
【数１】

$$a(x)=K+\sum_{j=1}^{k-1}a_j x^j \pmod p$$

を用いて、y_i＝ａ（x_i）を計算し、ｎ人のメンバーに（x_i，y_i）、（ｉ＝１，２，・・・，ｎ）を配布する。
【０００７】
最後に分散させた情報から暗号鍵Ｋの復元を行う。（i_1，・・・，i_k）のｋ人が集まって暗号鍵Ｋを復元する場合、次の連立一次方程式を解くと、Ｋ＝a_0として暗号鍵Ｋが復元される。
【数２】

$$\begin{pmatrix}1 & x_{i1} & x_{i1}^2 & \cdots & x_{i1}^{k-1}\\ 1 & x_{i2} & x_{i2}^2 & \cdots & x_{i2}^{k-1}\\ \vdots & \vdots & \vdots & & \vdots\\ 1 & x_{ik} & x_{ik}^2 & \cdots & x_{ik}^{k-1}\end{pmatrix}\begin{pmatrix}a_0\\ a_1\\ \vdots\\ a_{k-1}\end{pmatrix}=\begin{pmatrix}y_{i1}\\ y_{i2}\\ \vdots\\ y_{ik}\end{pmatrix}$$

【０００８】
Ｓｈａｍｉｒの方程式の特徴としては、大きなｋ，ｎに対しても閾値分散構造を定義できる。しかし素数ｐが２００桁程度である場合、２００桁の鍵Ｋに対する分散（x_i，y_i）は各４００桁程度になるので、分散全体では４００ｎ桁のデータになる。また計算量も、数百桁の整数の連立一次方程式を解くので、Ｏ（k^3）程度の演算回数を要し、リアルタイムに計算できるほど高速ではない。このため、データファイルのバックアップに用いることは、事実上不可能と考えられる。
【特許文献１】特開２００６－６７４１２号公報
【非特許文献１】Ｓｔｉｎｓｏｎ，Ｄｏｕｇｌａｓ，‘‘Ｃｒｙｐｔｏｇｒａｐｈｙ：Ｔｈｅｏｒｙ　ａｎｄ　ｐｒａｃｔｉｃｅ’’，ＣＲＣ　Ｐｒｅｓｓ，Ｉｎｃ．，ＵＳＡ，１９９５

【発明の開示】
【発明が解決しようとする課題】
【０００９】
従来のネットワークシステムでは、データファイルの復号に必要な情報が１台の監視制御装置に集中していた。そのため、監視制御装置に障害等が発生した場合の、当該情報の保全及びバックアップの方法を確立することが課題となる。また、悪意のある第三者が監視制御装置に侵入した場合には、データファイルの復号に必要な情報の漏洩及び破壊はもちろんのこと、バックアップ先に格納されている情報が復元される危険性も存在していた。
【００１０】
そこで、本発明は、安全かつ高信頼性のファイルバックアップ用ネットワークシステムを構築することを目的とする。
【課題を解決するための手段】
【００１１】
上記目的を達成するために、本発明に係るネットワークシステムは、一台で構成されることを前提としていた監視制御装置に対して、データファイルの復号に必要な情報に応じて監視制御装置を分散配備することを特徴とする。機能分散化された監視制御装置のすべてが外部より侵入されない限り、データファイルの復元及び漏洩を防止することができる。
【００１２】
具体的には、本発明に係るネットワークシステムは、少なくとも１つのマスターサーバと、複数の監視制御装置と、複数のクライアント端末と、が通信ネットワークを介して互いに接続されたネットワークシステムにおいて、
前記マスターサーバは、データファイルを第１の暗号鍵で暗号化し、暗号化した前記ファイルデータを複数の分割データに分割し、前記分割データを複製し、複製した前記分割データを第２の暗号鍵で暗号化して出力する秘匿化手段と、前記秘匿化手段の出力する暗号化済分割情報を前記複数のクライアント端末に送信する暗号化済分割情報送信手段と、前記第１の暗号鍵で暗号化した前記ファイルデータの分割から前記分割データを第２の暗号鍵で暗号化するまでの前記秘匿化手段の手順を記録したファイルシーケンス情報及び前記第１の暗号鍵をそれぞれ複製し、前記複数の監視制御装置のうちの異なる監視制御装置に送信する秘匿化情報送信手段と、を備え、
前記複数のクライアント端末は、前記暗号化済分割情報送信手段の送信する暗号化済分割情報を受信する暗号化済分割情報受信手段と、前記暗号化済分割情報受信手段の受信する前記暗号化済分割情報を格納する暗号化済分割情報格納手段と、を備え、
前記複数の監視制御装置は、前記秘匿化情報送信手段の送信する前記ファイルシーケンス情報又は前記第１の暗号鍵を受信する秘匿化情報受信手段と、前記秘匿化情報受信手段の受信する前記ファイルシーケンス情報又は前記第１の暗号鍵を格納する秘匿化情報格納手段と、を備えることを特徴とする。
【００１３】
データファイルを秘匿化して複数のクライアント端末に分散配備し、さらに、ファイルシーケンス情報及び第１の暗号鍵をそれぞれ異なる監視制御装置が格納するので、それぞれの監視制御装置が外部より侵入されない限り、データファイルの復元及び漏洩を防止することができる。また、秘匿化情報送信手段を備えることで、ファイルシーケンス情報及び第１の暗号鍵が、１台の監視制御装置又は１つの地域に集中しないように論理的に分散配備することができる。マスターサーバだけでなく監視制御装置も被災した場合であっても、被災していないクライアント端末及び監視制御装置に格納されている情報を収集することで、データファイルを復元することができる。
【００１４】
本発明に係るネットワークシステムでは、前記監視制御装置と通信ネットワークを介して接続された複数のバックアップ装置をさらに備え、

前記監視制御装置は、前記秘匿化情報格納手段の格納する前記ファイルシーケンス情報又は前記第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、秘密分散法を用いて複数のバックアップ情報に分散させる秘密分散処理手段と、前記秘密分散処理手段からの前記バックアップ情報を、前記複数のバックアップ装置のうちの異なるバックアップ装置に送信するバックアップ情報送信手段と、をさらに備え、

前記バックアップ装置は、前記バックアップ情報送信手段の送信する前記バックアップ情報を受信するバックアップ情報受信手段と、前記バックアップ情報受信手段の受信する前記バックアップ情報を格納するバックアップ情報格納手段と、をさらに備え、

前記秘密分散法は、前記秘密分散化情報送信手段が前記秘密分散化情報を送信する前記バックアップ装置の数をｎとし、前記ファイルシーケンス情報又は前記第１の暗号鍵を復元するために必要な前記バックアップ装置の数をｋとした場合に、完全置換系の表Ｓ（ｋ，ｎ，ｄ）が、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）の第ｎ列に０を追加した表、及び、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）の第ｎ列に１を追加した表で表されることが好ましい。

【００１５】

また、監視制御装置のバックアップを行う際に、一体化及び秘密分散法を組み合わせて秘密情報分散し、機能的には同等である複数台の監視制御装置に対して、同時に分散配備を行うことにより、監視制御装置自体のバックアップ機能を実現することができる。この場合、同時に複数台の監視制御装置に侵入されない限りは、ファイルシーケンス情報及び第１の暗号鍵が漏洩することを防止でき、ネットワークシステムの安全性を飛躍的に向上させることができる。

さらに、本発明による秘密分散法は完全置換系の表Ｓ（ｋ，ｎ）を再帰的に求められるので、演算回数が少なく高速処理が可能である。このため、データファイルのバックアップにおいて実用可能な秘密情報分散法を提供することができる。さらに、演算負荷の少ない一体化処理を組み合わせることで、演算負荷が少なくかつ安全性の高い情報の秘匿化が可能となる。

【００１６】

本発明に係るネットワークシステムでは、前記マスターサーバは、前記ファイルシーケンス情報を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させるファイルシーケンス秘密分散処理手段と、前記第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させる暗号鍵秘密分散処理手段と、をさらに備え、

前記秘匿化情報送信手段は、前記ファイルシーケンス秘密分散処理手段及び前記暗号鍵秘密分散処理手段からの前記ファイルシーケンス情報及び前記第１の暗号鍵を送信し、

前記秘密分散法は、前記バックアップ装置の数をｎとし、前記ファイルシーケンス情報又は前記第１の暗号鍵を復元するために必要な前記バックアップ装置の数をｋとした場合に、完全置換系の表Ｓ（ｋ，ｎ，ｄ）が、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）の第ｎ列に０を追加した表、及び、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）の第ｎ列に１を追加した表で表されることが好ましい。

【００１７】

ファイルシーケンス情報及び第１の暗号鍵のバックアップを行う際に、一体化及び秘密分散法を組み合わせて秘密情報分散し、機能的には同等である複数台の監視制御装置に対して、同時に分散配備を行うことにより、監視制御装置自体で、バックアップ機能を実現することができる。この場合、同時に複数台の監視制御装置に侵入されない限りは、ファイルシーケンス情報及び第１の暗号鍵の漏洩によりデータファイルが漏洩することを防止でき、ネットワークシステムの安全性を飛躍的に向上させることができる。

【００１８】

本発明に係るネットワークシステムでは、前記監視制御装置は、前記クライアント端末の状態を示すクライアント端末状態情報の送信を要求するクライアント端末状態報告要求を、前記複数のクライアント端末に送信するクライアント端末状態報告要求送信手段と、

前記クライアント端末から送信された前記クライアント端末状態情報を受信するクライアント端末状態情報受信手段と、クライアント端末状態情報受信手段の受信する前記クライアント端末状態情報、及び、前記クライアント端末状態報告要求を送信してから前記クライアント端末状態情報を受信するまでの応答時間に基づいて、前記クライアント端末との間のスループットを測定するスループット等測定手段と、クライアント端末状態情報受信手段の受信する前記クライアント端末状態情報及び前記スループット等測定手段の測定したスループットをクライアント端末リストとして前記マスターサーバに送信するクライアント端末リスト送信手段と、をさらに備え、

前記クライアント端末は、前記クライアント端末状態報告要求送信手段の送信するクライアント端末状態報告要求を受信すると、クライアント端末の状態を検出してクライアント端末状態情報を出力するリソース情報伝達手段と、前記リソース情報伝達手段の出力するクライアント端末状態情報を、前記監視制御装置へ送信するクライアント端末状態情報送信手段と、を備え、

前記マスターサーバは、前記クライアント端末リスト送信手段の送信するクライアント端末リストに基づいて、前記秘匿化手段における分割数及び複製数を決定する分割複製数決定手段と、前記クライアント端末リスト送信手段の送信するクライアント端末リストに基づいて、前記暗号化済分割情報送信手段における前記暗号化済分割情報を送信する前記クライアント端末を決定する送信先決定手段と、をさらに備え、前記秘匿化手段は、前記分割複製数決定手段の決定する分割数及び複製数に分割及び複製し、前記暗号化済分割情報送信手段は、前記送信先決定手段の決定する前記クライアント端末に前記暗号化済分割情報を送信することが好ましい。

【００１９】

本発明により、監視制御装置は、データを試験的に送受信し、災害時のバックアップを効率的に行うためのクライアント端末群の優先順位を推定し、マスターサーバへ通知することができる。マスターサーバは、この情報を基に、あて先クライアント端末群及びクライアント端末を決定することで、ファイルデータのバックアップ時間の短縮化を行うことができる。また、地理的に均等に選択することにより地域分散させ、かつ、分散化された監視制御装置内のデータベースを、より安全にかつ高信頼性のある形態で保護することができる。

【発明の効果】

【００２０】

本発明によれば、データファイルについては暗号化を行った後に分散配備し、データファイルの復号に必要な情報については情報の内容に応じて機能分散配備するので、一体化と暗号化又は秘密分散を組み合わせて分散配備するので、安全かつ高信頼性のファイルバックアップ用ネットワークシステムを構築することができる。

【発明を実施するための最良の形態】

【００２１】

添付の図面を参照して本発明の実施の形態を説明する。以下に説明する実施の形態は本発明の構成の例であり、本発明は、以下の実施の形態に制限されるものではない。

（実施形態１）

図１は、本実施形態に係るネットワークシステムの構成概略図である。本実施形態に係るネットワークシステムは、複数のクライアント端末１０と、マスターサーバ２０と、複数の監視制御装置３０ａ、３０ｂ、３０ｃと、複数のバックアップ装置４０ａ、４０ｂ、４０ｃと、を備え、互いに通信ネットワークで接続されている。本実施形態では、理解を容易にするため、図１ではクライアント端末１０を１つのみ記載し、他を省略した。また、３つの監視制御装置３０ａ、３０ｂ、３０ｃの例について説明するが、監視制御装置は２つ以上のいずれであってもよい。

【００２２】

本実施形態に係るネットワークシステムは、監視制御装置３０ａ、３０ｂ、３０ｃが機能別に分割されている。また、クライアント端末１０の識別情報及び生存確認情報の格納

されるデータベース、マスターサーバの記憶するデータファイルが暗号化される際に使用される第１の暗号鍵が格納されるデータベース、データファイルの暗号化後に、更に複数のファイルに分割して各々の分割ファイルに対して使用される第２の暗号鍵の格納されるデータベース等のデータベースを、監視制御装置３０ａ、３０ｂ、３０ｃをアクセス可能な端末から、ネットワークを通じてアクセスする手段を用い、複数の異なる地域に設置されたバックアップ装置４０ａ、４０ｂ、４０ｃに、データベース毎に分離し、かつ、複数の地域に設置されたバックアップ装置４０ａ、４０ｂ、４０ｃに冗長に複製して、転送することにより、監視制御装置側で必要となるデータベースの情報を、機能分散的に配備することを特徴とする。

【００２３】

マスターサーバ２０は、ファイルデータを秘匿化して暗号化済分割情報を生成し、複数のクライアント端末１０に送信する。そして、マスターサーバ２０は、秘匿化に関する情報を異なる監視制御装置３０ａ及び３０ｂに送信する。例えば、第１の暗号鍵を監視制御装置３０ａに、ファイルシーケンス情報を監視制御装置３０ｂに送信する。第１の暗号鍵及びファイルシーケンス情報は、ファイルデータの復元のために必要な情報であるため、機能分散配備することで、安全性を高めることができる。

【００２４】

クライアント端末１０は、マスターサーバ２０からの暗号化済分割情報を受信し、格納する。災害復旧の迅速のため、複数のクライアント端末１０は、地域的に分散していることが好ましい。そして、クライアント端末１０は、生存確認情報及び自己の識別情報を、監視制御装置３０ｃに送信することが好ましい。

【００２５】

複数の監視制御装置３０ａ、３０ｂ、３０ｃは、ファイルデータの復元のために必要な情報を受信して格納する。例えば、監視制御装置３０ａは、第１の暗号鍵を受信して格納する。監視制御装置３０ｂは、ファイルシーケンス情報を受信して格納する。

【００２６】

また、複数の監視制御装置３０ａ、３０ｂ、３０ｃのうちの少なくとも１つの監視制御装置３０ｃは、生存確認情報及び識別情報を、クライアント端末１０から受信し、格納している。生存確認情報及び識別情報は、専門の監視制御装置３０ｃが行うことが好ましい。さらに、監視制御装置３０ａ、３０ｂ、３０ｃは、秘匿化に関する情報を、バックアップ装置４０ａ、４０ｂ、４０ｃに分散して格納する。

【００２７】

複数のバックアップ装置４０ａ、４０ｂ、４０ｃは、監視制御装置３０ａ、３０ｂ、３０ｃに格納されている情報の複製を格納する。災害復旧の迅速のため、バックアップ装置４０ａ、４０ｂ、４０ｃは、それぞれ、複数の監視制御装置３０ａ、３０ｂ、３０ｃと地理的に異なる地域に配置されることが好ましい。

【００２８】

ここで、システムの安全のため、いずれのバックアップ装置４０ａ、４０ｂ、４０ｃにも、複数の監視制御装置３０ａ、３０ｂ、３０ｃに格納されている全ての情報が揃わないようになっていることが好ましい。例えば、バックアップ装置４０ａは、監視制御装置３０ａに格納されている情報の一部の複製と、監視制御装置３０ｂに格納されている情報の一部の複製を、格納する。バックアップ装置４０ｂは、監視制御装置３０ａに格納されている情報の一部の複製と、監視制御装置３０ｃに格納されている情報の一部の複製を、格納する。バックアップ装置４０ｃは、監視制御装置３０ｂに格納されている情報の一部の複製と、監視制御装置３０ｃに格納されている情報の一部の複製を、格納する。なお、各々の監視制御装置３０ａ、３０ｂ、３０ｃは、通信ネットワーク１００を介して、複数のバックアップ装置４０ａ、４０ｂ、４０ｃのうちの少なくとも２つにより情報のバックアップが実施される例を示しているが、この例に限定されるものではなく、３つ以上のバックアップ装置により情報のバックアップが実施されてもよい。

【００２９】

マスターサーバ２０が監視制御装置３０ａ、３０ｂ、３０ｃに送信する情報は、秘匿化情報送信手段（図２の符号２４）を用いて、それぞれに該当する各種情報が、監視制御装置３０ａ及び３０ｂに向けて機能分散して転送され、かつ、配備される。なお、暗号化済分割情報は、暗号化済分割情報送信手段（図２の符号２３）を用いて、クライアント端末１０に転送され、その後、当該クライアント端末１０からは、生存確認情報送信手段（図３の符号１３）を用いて、当該クライアント端末１０の生存確認情報を格納するための専用の監視制御装置３０に転送され、ここで格納及び保持される。

【００３０】

監視制御装置３０ａは、マスターサーバ２０から秘匿化情報として第１の暗号鍵を受信し、監視制御装置３０ｂはマスターサーバ２０から秘匿化情報としてファイルシーケンス情報を受信する。監視制御装置３０ｃはクライアント端末１０から生存確認情報を受信する。クライアント端末１０に分散配備された重要情報を回収した後に結合し、復号するためには、生存確認情報、ファイルシーケンス情報、第１の暗号鍵すべてがそろう必要があるため、３台の監視制御装置３０ａ、３０ｂ、３０ｃに保持されているデータベースのすべてにアクセスができない限り、当該重要情報の漏洩は起こらない。

【００３１】

データベースの複製を作成する手段としては、監視制御装置を、例えば２倍又は３倍に増設し、完全に同一機能単位で、同一のデータベース内容を保持する装置を、複数台設置する方法も考えられる。又は、当該データベースのバックアップ装置４０ａ、４０ｂ、４０ｃを、地理的に異なる地域に、複数台配備し、監視制御装置３０ａ、３０ｂ、３０ｃのデータベースの複製を実現する方法も考えられる。図１は、３台の監視制御装置３０ａ、３０ｂ、３０ｃに対して、３台のバックアップ装置４０ａ、４０ｂ、４０ｃを配備し、データベースのバックアップを、１台の監視制御装置３０ａに対して少なくとも２つのバックアップ装置４０ａ、４０ｂ、１台の監視制御装置３０ｂに対して少なくとも２つのバックアップ装置４０ａ、４０ｃを組み合わせて活用して実現するとともに、いずれのバックアップ装置４０ａ、４０ｂ、４０ｃにも、監視制御装置３０ａ、３０ｂ、３０ｃのデータベースが、すべてはそろわないように割り当てる。

【００３２】

次に、各構成の詳細について、図１、図２、図３、図４、図５及び図６を用いて説明する。図２、図３、図４、図５及び図６は、それぞれ、本実施形態に係るマスターサーバ、クライアント端末、監視制御装置及びバックアップ装置の一例を示す概略構成図である。

【００３３】

図２に示すマスターサーバ２０は、情報格納手段２１と、秘匿化手段２２と、暗号化済分割情報送信手段と２３、秘匿化情報送信手段２４と、を備える。

【００３４】

情報格納手段２１は、ファイルデータ、第１の暗号鍵、第２の暗号鍵、識別情報、ファイルシーケンス情報を格納する。ここで、ファイルシーケンス情報は、データファイルを復元するために必要な情報であり、例えば、分割手段２２－３、複製手段２２－４及び第２暗号化手段２２－５の実行手順の記録である。ファイルシーケンス情報は、秘匿化手段２２全体での実行手順の記録であってもよい。さらに、暗号化済分割情報送信手段２３の実行手順の記録が組み合わせられていてもよい。上記実行手順の記録は、各構成がログとして出力する。例えば、分割手段２２－３を用いて作成された分割情報、複製手段２２－４を用いて作成された複製情報、第２暗号化手段２２－５に使用された第２の暗号鍵、および暗号化済分割情報送信手段２３が暗号化済分割情報を送信したクライアント端末の識別情報を組み合わせた情報である。本実施形態では一例として、監視制御装置に分散させる情報を第１の暗号鍵とファイルシーケンス情報として説明する。

【００３５】

秘匿化手段２２は、情報格納手段２１から読出したデータファイルを第１の暗号鍵で暗号化し、暗号化したファイルデータを複数に分割して互いに可逆演算することで一体化し、一体化したファイルデータを複数の分割データに分割し、分割データを複製し、複製し

た分割データを第２の暗号鍵で暗号化して、暗号化済分割情報を生成し、出力する。ここで、分割数及び複製数は、予め定められていてもよいし、ファイルデータの容量などに応じて異なる数であってもよい。第１の暗号鍵及び第２の暗号鍵は、情報格納手段２１から読出してもよいし各暗号化手段にて生成してもよい。そして、暗号化済分割情報送信手段２３は、秘匿化手段２２の出力する暗号化済分割情報を複数のクライアント端末１０に送信する。

【００３６】

秘匿化手段２２は、例えば、第１の暗号化手段２２－１と、一体化手段２２－２と、分割手段２２－３と、複製手段２２－４と、第２の暗号化手段２２－５と、を備える。この場合、第１の暗号化手段２２－１は、データファイルを第１の暗号鍵で暗号化する。一体化手段２２－２は、第１の暗号化手段２２－１からのファイルデータを複数に分割して互いに可逆演算することで一体化する。分割手段２２－３は、一体化手段２２－２からのファイルデータを分割する。複製手段２２－４は、分割手段２２－３からの分割データを複製する。第２の暗号化手段２２－５は、複製手段２２－４からの複製した分割データを第２の暗号鍵で暗号化して、暗号化済分割情報を出力する。

【００３７】

図３は、マスターサーバの秘匿化手段の別の一例を示す概略構成図である。図３に示す秘匿化手段２２では、一体化手段２２－２を省略している。一般には秘匿化手段２２が一体化手段２２－２を備えることが好ましいが、第１の暗号化手段２２－１で用いる第１の暗号鍵の強度が十分の場合には一体化手段２２－２を省略してもよい。一体化手段２２－２を省略することで処理速度を向上させることが可能である。この場合、秘匿化情報送信手段２４は、第１の暗号鍵で暗号化したファイルデータの分割から分割データを第２の暗号鍵で暗号化するまでの秘匿化手段２２の手順を記録したファイルシーケンス情報及び第１の暗号鍵を複製し、それぞれ複数の監視制御装置のうちの異なる監視制御装置に送信する。

【００３８】

秘匿化情報送信手段２４は、一体化したファイルデータの分割から分割データを第２の暗号鍵で暗号化するまでの秘匿化手段２２の手順を記録したファイルシーケンス情報及び第１の暗号鍵を複製し、それぞれ複数の監視制御装置のうちの異なる監視制御装置に送信する。ファイルシーケンス情報は、秘匿化手段２２がデータファイルに行った秘匿化の手順の一覧であり、例えば、分割手段２２－３、複製手段２２－４、及び、第２の暗号化手段２２－５のログである。

【００３９】

図４に示すクライアント端末１０は、暗号化済分割情報受信手段１１と、情報格納手段１２と、生存確認情報送信手段１３と、を備える。暗号化済分割情報受信手段１１は、暗号化済分割情報送信手段２３の送信する暗号化済分割情報を受信する。情報格納手段１２は、暗号化済分割情報格納手段としての機能を有する。暗号化済分割情報格納手段は、暗号化済分割情報受信手段１１の受信する暗号化済分割情報を格納する。生存確認情報送信手段１３は、クライアント端末１０が稼動状態にあることを示す生存確認情報を、マスターサーバ２０に送信する。

ここで、生存確認情報は、クライアント端末１０が稼動状態にあることを示す情報である。「生存確認情報」の具体例としては、たとえば、監視制御装置３０ａ、３０ｂ、３０ｃが、ＵＤＰまたはＴＣＰ等のプロトコルを用い、宛先クライアント端末１０への問い合わせ情報として、自信のＩＰアドレスとポート番号とを、宛先クライアント端末１０へ通知した時には、宛先クライアント端末１０は上記のアドレス情報を確認後に、予め、監視制御装置３０ａ、３０ｂ、３０ｃの中に登録されている、当該の宛先クライアント端末１０のＩＰアドレスと、ポート番号とが、規定の時間内に返送されることにより、当該の宛先クライアント端末１０が、正常に稼働している旨を監視制御装置３０ａ、３０ｂ、３０ｃが認識できる。この動作により、宛先クライアント端末の「生存確認」が実現できる。なお、宛先クライアント端末のクライアントプログラムは、監視制御装置３０ａ、３０ｂ

、３０ｃへの応答時に、データ情報として、例えば、特定の文字列「ＫＥＥＰ　Ａｌｉｖｅ」や「ＩＰアドレス」「ポート番号」等をメッセージの一部として含めるように構成することも同様に可能である。

【００４０】

図５に示す監視制御装置３０は、情報格納手段３２にデータベースを格納し、ファイルシーケンス情報又は第１の暗号鍵をマスターサーバ２０より受信する機能、及び受信したファイルシーケンス情報又は第１の暗号鍵を、データベースの複製を作成したバックアップ情報を送信する機能を備える。具体的には、監視制御装置３０は、情報受信手段３１と、情報格納手段３２と、情報送信手段３３と、を備える。

【００４１】

情報受信手段３１は、秘匿化情報受信手段としての機能を有する。秘匿化情報受信手段は、秘匿化情報送信手段２４の送信するファイルシーケンス情報又は第１の暗号鍵を受信する機能である。また、生存確認情報送信手段１３の送信する生存確認情報を受信する。情報格納手段３２は、秘匿化情報格納手段としての機能を有する。秘匿化情報格納手段は、情報受信手段３１の受信するファイルシーケンス情報又は第１の暗号鍵を格納する機能である。また、情報格納手段３２の受信する生存確認情報を格納する。情報送信手段３３は、バックアップ情報送信手段としての機能を有する。バックアップ情報送信手段は、情報格納手段３２の格納する秘匿化情報を、複数のバックアップ装置４０に送信する機能である。

【００４２】

例えば、図１に示す監視制御装置３０ａであれば、情報受信手段３１、情報格納手段３２及び情報送信手段３３は、それぞれ、第１の暗号鍵を、受信し、格納し、送信する。監視制御装置３０ｂであれば、情報受信手段３１、情報格納手段３２及び情報送信手段３３は、それぞれ、ファイルシーケンス情報を、受信し、格納し、送信する。監視制御装置３０ｃであれば、情報受信手段３１、情報格納手段３２及び情報送信手段３３は、それぞれ、生存確認情報を、受信し、格納し、送信する。

【００４３】

図６に示すバックアップ装置４０は、監視制御装置３０からデータベースのバックアップ情報を受信する機能と、バックアップ情報をデータベースに反映させる機能と、監視制御装置３０からのデータベースのバックアップ情報を受信する機能と、バックアップ情報をデータベースに反映させる機能を備える。そして、複数の監視制御装置３０ａ、３０ｂ、３０ｃに格納されている情報のうちの一部、例えば２台の情報をバックアップする。具体的には、バックアップ装置４０は、バックアップ情報受信手段４１－１及び４１－２と、バックアップ情報格納手段４２－１及び４２－２と、を備える。

【００４４】

バックアップ情報受信手段４１－１及び４１－２は、それぞれ、複数の監視制御装置３０ａ、３０ｂ、３０ｃから送信された異なる秘匿化情報を受信する。バックアップ情報格納手段４２－１及び４２－２は、それぞれ、バックアップ情報受信手段４１－１及び４１－２の受信する秘匿化情報を格納する。バックアップ情報格納手段４１－１及び４１－２は、共通の構成としてもよい。バックアップ情報格納手段４２－１及び４２－２は、２つのデータベースを格納する共通の情報格納手段としてもよい。

【００４５】

例えば、図１に示す監視制御装置３０ａであれば、バックアップ情報受信手段４１－１及びバックアップ情報格納手段４２－１は、それぞれ、第１の暗号鍵を、受信し、格納する。バックアップ情報受信手段４１－２及びバックアップ情報格納手段４２－２は、それぞれ、ファイルシーケンス情報を、受信し、格納する。監視制御装置３０ｂであれば、バックアップ情報受信手段４１－１及びバックアップ情報格納手段４２－１は、それぞれ、第１の暗号鍵を、受信し、格納する。バックアップ情報受信手段４１－２及びバックアップ情報格納手段４２－２は、それぞれ、生存確認情報を、受信し、格納する。監視制御装置３０ｃであれば、バックアップ情報受信手段４１－１及びバックアップ情報格納手段４

２－１は、それぞれ、ファイルシーケンス情報を、受信し、格納する。バックアップ情報受信手段４１－２及びバックアップ情報格納手段４２－２は、それぞれ、生存確認情報を、受信し、格納する。

【００４６】

上述した構成例では、マスターサーバ２０から送信された第１の暗号鍵は、まず、監視制御装置３０ａが受信し、監視制御装置３０ａ内の情報格納手段３２に格納されているデータベースが更新された後に、データベースの複製を作成するためのバックアップ情報を作成して、バックアップ装置４０ａとバックアップ装置４０ｂに送信する。監視制御装置３０ａのデータベースのバックアップ情報を受信したバックアップ装置４０ａは、その情報を基に、バックアップ情報格納手段４２－１のデータベースを更新する。同様に、監視制御装置３０ａのデータベースのバックアップ情報を受信したバックアップ装置４０ｂは、その情報を基に、バックアップ情報格納手段４２－１のデータベースを更新する。

【００４７】

上述したデータベースの更新処理は、マスターサーバ２０からファイルシーケンス情報を監視制御装置３０ｂが受信した場合、及び、クライアント端末１０からの生存確認情報を監視制御装置３０ｃが受信した場合にも、同様に実施される。これら一連の処理の結果、第１の暗号鍵、ファイルシーケンス情報及び生存確認情報は、３台の監視制御装置３０ａ、３０ｂ、３０ｃと３台のバックアップ装置４０ａ、４０ｂ、４０ｃを活用する場合においては、監視制御装置３０ａ、３０ｂ、３０ｃとバックアップ装置４０ａ、４０ｂ、４０ｃの情報共有関係は次のようになる。監視制御装置３０ａが第１の暗号鍵を格納し、監視制御装置３０ｂがファイルシーケンス情報を格納し、監視制御装置３０ｃが生存確認情報を格納する。バックアップ装置４０ａが第１の暗号鍵及びファイルシーケンス情報を格納し、バックアップ装置４０ｂが第１の暗号鍵及び生存確認情報を格納し、バックアップ装置４０ｃがファイルシーケンス情報及び生存確認情報を格納する。

【００４８】

上記の情報共有関係により、個々の情報は、監視制御装置３０ａ、３０ｂ、３０ｃ及びバックアップ装置４０ａ、４０ｂ、４０ｃの中の３台に分散配備されているため、任意の２台が損壊した場合においても、重要情報を完全に回復することが可能となる。

また、上記の例では、悪意のある第三者の侵入等に対しても、監視制御装置３０ａ、３０ｂ、３０ｃは、重要情報のバックアップに係る必要情報を１種類持ち、バックアップ装置は、必要情報を２種類もつだけなので、監視制御装置３０ａ、３０ｂ、３０ｃ又はバックアップ装置４０ａ、４０ｂ、４０ｃのいずれか１台に侵入された場合でも、クライアント端末１０に分散配備された重要情報が漏洩する危険性を回避することができる。

【００４９】

（実施形態２）

本実施形態に係るネットワークシステムは、図１に示すネットワークシステムにおいて、監視制御装置３０ａ、３０ｂ、３０ｃの格納するファイルシーケンス情報及び第１の暗号鍵を、監視制御装置３０ａ、３０ｂ、３０ｃから、通信ネットワーク１００を通じてアクセスする手段を用い、一体化処理及び秘密分散法を用いて複数の秘密分散情報に変換した後、一つ一つの秘密分散情報を異なる地域に設置された、一つ若しくは複数を組み合わせたバックアップ装置４０ａ、４０ｂ、４０ｃに転送することにより、監視制御装置３０ａ、３０ｂ、３０ｃ側で復元に必要となるデータベース情報を、閾値秘密分散配備することを特徴とする。例えば、図１において、監視制御装置３０ａに格納されているデータベースを（２，３）閾値秘密情報分散処理により３個の秘密分散情報を生成し、３台別々のバックアップ装置４０ａ、４０ｂ、４０ｃにバックアップする。

【００５０】

ここで、（２，３）閾値秘密情報とは、３台のうち任意の２台が正常であれば、監視制御装置３０ａに格納されているデータベースのバックアップが完全に表現されているときの表記法を意味している。本実施形態では、（２，３）閾値秘密情報分散処理の例を示すが、この場合に限定されるものではないことは言うまでもない。たとえば、（ｋ，ｎ）閾

値秘密情報分散処理において、ｎは任意であり、ｋもｎ以下の任意の整数とすることができる。さらに、閾値秘密情報分散は、完全閾値秘密情報分散であってもよいし、不完全閾値秘密情報分散であってもよい。不完全閾値秘密情報分散は、例えば閾値ランプ型秘密分散である。完全閾値秘密情報分散は分散した情報のうち一定数が集まらなければ復元できないので、秘匿性を高めることができる。不完全閾値秘密情報分散は分散した情報のうち一定数が集まらない場合でも一部の秘密情報は解読可能となる。また、閾値秘密情報分散は、一体化や暗号化をしない完全置換系による秘密情報分散であってもよい。

【００５１】

図７は、本実施形態に係る監視制御装置の一例を示す概略構成図である。本実施形態に係る監視制御装置３０は、図５に示した実施形態１に係る監視制御装置３０に秘密分散処理手段３４をさらに備える。秘密分散処理手段３４は、情報格納手段３２と情報送信手段３３の間に設けられ、ファイルシーケンス情報又は第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、秘密分散法を用いて複数のバックアップ情報に分散させる。情報送信手段３３は、秘密分散処理手段３４の分散化したバックアップ情報を、バックアップ装置４０ａ、４０ｂ、４０ｃに送信する。例えば、図１に示す監視制御装置３０ａであれば、情報格納手段３２を備え、第１の暗号鍵をマスターサーバ２０より受信する機能、受信した第１の暗号鍵を情報格納手段３２に格納する機能、情報格納手段３２に格納された第１の暗号鍵に対して（２，３）閾値秘密分散処理を行い、３つのバックアップ情報を生成する機能、及び、生成されたバックアップ情報をそれぞれ異なったバックアップ装置４０ａ、４０ｂ、４０ｃに送信する機能を有する。

【００５２】

図８は、本実施形態に係るバックアップ装置の一例を示す概略構成図である。本実施形態に係るバックアップ装置４０は、図６に示した実施形態１に係るバックアップ装置４０に、バックアップ情報受信手段４１－３と、バックアップ情報格納手段４２－３をさらに備える。バックアップ情報受信手段４１－１、４１－２、４１－３は、実施形態１と同様に、それぞれ、複数の監視制御装置３０ａ、３０ｂ、３０ｃのうちの異なる監視制御装置から送信されたバックアップ情報を受信する。バックアップ情報格納手段４２－１、４２－２及び４２－３は、バックアップ情報受信手段４１－１、４１－２及び４１－３の受信する秘密分散化情報を格納する。

【００５３】

例えば、図１に示すバックアップ装置４０ａであれば、監視制御装置３０ａから秘密分散化された第１の暗号鍵を受信する機能と、受信した秘密分散化された第１の暗号鍵をデータベースに格納する機能と、監視制御装置３０ｂから秘密分散化されたファイルシーケンス情報を受信する機能と、受信した秘密分散化されたファイルシーケンス情報をデータベース３０ｂに格納する機能と、監視制御装置３０ｃから秘密分散化された生存確認情報を受信する機能と、受信した秘密分散化された生存確認情報をデータベースに格納する機能を備える。３台のバックアップ装置４０ａ、４０ｂ、４０ｃで構成されたネットワークシステムで使用されるすべての情報種別に関しては、バックアップ装置４０ｃに格納されている各種のデータベース情報と共通であることに注意する。

【００５４】

図１の構成では、マスターサーバ２０から送信された第１の暗号鍵の情報は、まず、監視制御装置３０ａが受信し、監視制御装置３０ａ内部のデータベースに格納する。次に、監視制御装置３０ａは、データベースに新たに格納した、第１の暗号鍵を読み出して、（２，３）閾値秘密分散処理を行い、３つの秘密分散化された第１の暗号鍵を生成して、３台のバックアップ装置４０ａ、４０ｂ、４０ｃに１つずつ送信する。監視制御装置３０ａから秘密分散化された第１の暗号鍵を受信したバックアップ装置４０ａは、その秘密分散化された第１の暗号鍵をバックアップ装置４０ａの内部のデータベースに格納する。バックアップ装置４０ｂ及び４０ｃについても同様に、監視制御装置３０ａから送信された秘密分散化されている第１の暗号鍵を、各々の装置内部のデータベースに格納する。同様の格納処理は、マスターサーバ２０からファイルシーケンス情報を監視制御装置３０ｂが受

信した場合と、クライアント端末１０から生存確認情報を監視制御装置３０ｃが受信した場合においても行われる。

【００５５】

上記一連の処理の結果、第１の暗号鍵、ファイルシーケンス情報、生存確認情報、及び各々が秘密分散処理された秘密分散化情報は、３台の監視制御装置３０ａ、３０ｂ、３０ｃと、３台のバックアップ装置４０ａ、４０ｂ、４０ｃにおいて配備される。（２，３）閾値秘密分散処理により生成されているため、３つのバックアップ装置４０ａ、４０ｂ、４０ｃに分散配備した３つの秘密分散化情報のうち、２つ以上を集めれば、データファイルを復元することができる。すなわち、同一地域に設置する監視制御装置３０ａ、３０ｂ、３０ｃ及びバックアップ装置４０ａ、４０ｂ、４０ｃが２台までの範囲であれば、天災などにより、装置が同時に損壊した場合にも、重要情報のデータファイルの完全なバックアップが実現できる。また、悪意ある第三者の侵入に対しては、監視制御装置３０ａ、３０ｂ、３０ｃ及びバックアップ装置４０ａ、４０ｂ、４０ｃのいずれか１台に侵入された場合でも、クライアント端末１０に分散配備された暗号化済分割情報が漏洩することを同時に防止できる。この理由は、バックアップ装置４０ａ、４０ｂ、４０ｃは３つの情報をすべて備えているが、（２，３）秘密分散処理により、１台のバックアップ装置４０ａ、バックアップ装置４０ｂ又はバックアップ装置４０ｃの持つ情報だけでは秘密分散処理される前の情報には戻せないアルゴリズムを用いているからである。

【００５６】

本実施形態に係る秘密分散法の一例について説明する。本実施形態に係る秘密分散法では、完全置換系による（ｋ，ｎ）閾値秘密情報分散法に基づく。ここで、（ｋ，ｎ）は、秘密的に分散された解読用のｎ個の情報のうち、少なくともｋ個の情報が揃えば、メタデータが復元できることを意味している。すなわち、ｋは、復元のための閾値に対応しており、ｎは秘密分散するメンバーすなわち図１に示すバックアップ装置４０ａ、４０ｂ、４０ｃの総数と考えてよい。

【００５７】

図９は、秘密分散処理手段の動作の一例を示すフローチャートである。監視制御装置３０が保有するメタデータ、すなわち第１の暗号鍵、ファイルシーケンス情報又は生存確認情報を一体化し、ネットワーク管理者またはユーザのデータのバックアップ上の信頼性に関わる条件等を勘案してｋ及びｎを設定し、この情報を用いて、秘密分散を実現するための完全置換系の表Ｓ（ｋ，ｎ，ｄ）を作成する。ここで、ｄは、記憶空間での所有の有無を表現する配列である。以下に具体的に説明する。

【００５８】

ステップＳ１０１では、メタデータを一体化する。一体化とは、メタデータを複数に分割して互いに可逆演算することであり、データの空間分散化ともいえる。可逆演算は、例えば、加算、減算又はＥＯＲ、あるいは、これらの組み合わせである。分割数は、例えば、秘密分散させる数ｎである。ステップＳ１０２では、完全置換系の表Ｓ（ｋ，ｎ，ｄ）におけるｋ及びｎを取得する。ステップＳ１０３では、ステップＳ１０２で取得したｋ及びｎを用いて完全置換系の表Ｓ（ｋ，ｎ，ｄ）を作成する。具体的には、Ｓ（３，４）の場合、表Ｓ（ｋ，ｎ，ｄ）は次式で表される。

【数３】

$$S(3,4)=\begin{pmatrix}1&1&0&0\\1&0&1&0\\0&1&1&0\\1&0&0&1\\0&1&0&1\\0&0&1&1\end{pmatrix}$$

表Ｓ（ｋ，ｎ，ｄ）のうち、各列がバックアップ情報を保有するメンバーを、各行がバ

ックアップ情報の情報種別番号を表す。メンバーは、分散場所、あるいは、バックアップ情報を保有するバックアップ装置に対応する。バックアップ情報の情報種別番号は、メタデータＢが分散される分散B_1，・・・，B_Nに対応する。行列ｄの配列要素の中で、「１」が記されている箇所は、バックアップ情報を保有していることを意味し、ｉ番目のメンバーは表のｉ列の１の立っている情報種別番号のバックアップ情報を保持する。

【００５９】

ステップＳ１０４では、ステップＳ１０１によって得た一体化後のメタデータＢの分散B_1，・・・，B_Nを作成する。ステップＳ１０３で作成される表Ｓ（ｋ，ｎ，ｄ）はｎ行Ｎ列となるので、メタデータＢを、次式で表されるＮ個に分割する。これによって秘密分散化したバックアップ情報を得る。

【数４】

$$N = \frac{n!}{(k-1)!(n-k+1)!}$$

具体的には、Ｓ（３，４）の場合、Ｓ（３，４，ｄ）は６行４列であり、Ｎ＝６となる。分散B_1，B_2，B_3，B_4，B_5及びB_6の作成方法は任意だが，一例としてメタデータＢを６等分に分割する方法が有る。

【００６０】

ステップＳ１０５では、ステップＳ１０４によって得たバックアップ情報を、メンバーすなわち図１に示すバックアップ装置４０ａ、４０ｂ、４０ｃに送信する。表Ｓ（ｋ，ｎ，ｄ）において１の立っている情報種別番号のバックアップ情報が、ステップＳ１０５でメンバーに送付されることになる。例えば、情報種別番号２、３及び６のバックアップ情報を、３番目のメンバーへ送信する。

【００６１】

上記ステップＳ１０３においては、情報送信手段３３がバックアップ情報を送信するバックアップ装置の数をｎとし、第１の暗号鍵又はファイルシーケンス情報を復元するために必要なバックアップ装置の数をｋとした場合に、完全置換系の表Ｓ（ｋ，ｎ，ｄ）が、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）の第ｎ列に０を追加した表ｄ０、及び、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）の第ｎ列に１を追加した表ｄ１で表されることが好ましい。以下、ｎが３の場合の完全置換系の表Ｓ（ｋ，ｎ，ｄ）の作成例について説明する。

【００６２】

図１０は、完全置換系の表作成アルゴリズムの一例を示すフローチャートである。ステップＳ２０１では、入力されたｋが１と等しいか否かを判定する。ｋ＝１であればステップＳ２０２へ移行し、ｋ＝１でなければステップＳ２０３へ移行する。ステップＳ２０２では、行列ｄとして、（１，１，・・・，１）の１行ｎ列の行列を作成する。例えば、ｋ＝１の場合、行列ｄとして、

【数５】

$$d = (1,1,1)$$

を作成する。このとき、３つのバックアップ装置が同じバックアップ情報を保有していることを意味する。

【００６３】

ステップＳ２０３では、入力されたｋがｎと等しいか否かを判定する。ｋ＝ｎであればステップＳ２０４へ移行し、ｋ＝ｎでなければステップＳ２０５へ移行する。ステップＳ２０４では、行列ｄとして、ｎ行ｎ列の単位行列を作成する。例えば、ｋ＝３の場合、行列ｄとして、

【数６】

$$d = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

を作成する。このとき、３つの各々のバックアップ装置が別々の分割されたバックアップ情報を保有していることを意味する。

【００６４】

ステップＳ２０５では、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）を作成する。

例えば、ｋ＝２の場合、Ｓ（ｋ－１，ｎ－１，ｄ）すなわちＳ（１，２，ｄ）を作成する。具体的には次式で表される。

【数７】

$$S(1,2,d) = (1,1)$$

【００６５】

ステップＳ２０６では、Ｓ（ｋ－１，ｎ－１，ｄ）における各行の第ｎ列に０を追加する。例えば、ｋ＝２の場合、Ｓ（１，２，ｄ）の第ｎ列の各行に０を追加して、次式で表される。

【数８】

$$d0 = (1,1,0)$$

【００６６】

ステップＳ２０７では、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）を作成する。例えば、ｋ＝２の場合、Ｓ（ｋ，ｎ－１，ｄ）すなわちＳ（２，２，ｄ）を作成する。具体的には次式で表される。

【数９】

$$S(2,2,d) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

【００６７】

ステップＳ２０８では、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）における各行の第ｎ列に１を追加し、行列ｄ１とする。例えば、ｋ＝２の場合、Ｓ（２，２，ｄ）の第ｎ列の各行に１を追加して、次式で表される。

【数１０】

$$d1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

【００６８】

ステップＳ２０９では、ステップＳ２０４で得たｄ０の下に、ステップＳ２０６で得たｄ１を追加して、完全置換系の表Ｓ（ｋ，ｎ，ｄ）の表としての行列ｄを作成する。ｄ０は縦Ｎ０、横ｎの配列になっている。ｄ１は縦Ｎ１、横ｎの配列になっている。

【数１１】

$$N0 = \frac{(n-1)!}{(k-2)!(n-k+1)!}$$

$$N1 = \frac{(n-1)!}{(k-1)!(n-k)!}$$

ｄとして縦Ｎ＝Ｎ０＋Ｎ１、横ｎの配列を取り、１行目からＮ０行目までに０を追加済のｄ０を、（Ｎ０＋１）行目から（Ｎ０＋Ｎ１）行目までに１を追加済のｄ１を格納してｄを生成する。例えば、ｋ＝２の場合、数式（８）及び数式（１０）から、次式で表される行列ｄが得られる。

【数１２】

$$d = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

【００６９】

上記のステップＳ２０５からステップＳ２０９までの処理は、ｋ＝２、ｎ＝３の時の完全置換系の表Ｓ（２，３）を求める方法が、完全置換系の表Ｓ（１，２）及びＳ（２，２）によって求められることを意味する。完全置換系の表Ｓ（ｋ，ｎ）の一般的な求め方が、再帰的に求められることを意味する。

【００７０】

図１１は、完全置換系の表作成アルゴリズムの説明図である。完全置換系の表Ｓ（２，３，ｄ）であれば、完全置換系の表Ｓ（１，２）及びＳ（２，２）によって求められる。完全置換系の表Ｓ（２，４，ｄ）であれば、完全置換系の表Ｓ（１，３）及びＳ（２，３）によって求められる。完全置換系の表Ｓ（３，４，ｄ）であれば、完全置換系の表Ｓ（２，３）及び表Ｓ（３，３）によって求められる。完全置換系の表Ｓ（３，５，ｄ）であれば、完全置換系の表Ｓ（２，４）及び表Ｓ（３，４）によって求められる。このように、完全置換系の表ｄは、完全置換系の表Ｓ（ｋ－１，ｎ－１，ｄ）から得られる行列ｄ０と、完全置換系の表Ｓ（ｋ，ｎ－１，ｄ）から得られる行列ｄ１とを用いて再帰的に求められる。このように、本実施形態に係る秘密分散法は、連立一次方程式を解く必要がないので、データファイルのバックアップにおける秘密分散法の利用を現実的なものとすることができる。

【００７１】

本実施形態に係る秘密情報分散方式においては、Ｓｈａｍｉｒの方式のようなことはなく、鍵データ（メタデータ）Ｋが２００桁のとき分散が２００桁以上になることはない。また実質的な演算は一体化演算のみなのでメタデータのサイズをｍとするときＯ（ｍ）程度であり、大きなＫに対しても高速に計算できる。ただ、バックアップ情報は１６バイト以上の大きさが必要であるので、ｋ、ｎの値は大きくできない。ｎ＝２０程度が実用的には限界と考えられる。

【００７２】

（実施形態３）

本実施形態に係るネットワークシステムは、図１に示す実施形態１に係るネットワークシステムにおいて、監視制御装置３０ａ、３０ｂ、３０ｃを複数の異なる地域に設置して、かつ、マスターサーバ２０が、第１の暗号鍵、ファイルシーケンス情報を、秘密分散法

を用いて複数の秘密情報に変換した後、一つ一つの秘密情報を異なる地域に設置された、一つもしくは複数を組み合わせた監視制御装置３０ａ、３０ｂ、３０ｃに転送することにより、監視制御装置３０ａ、３０ｂ、３０ｃ自体を、閾値秘密分散配備することを特徴とする。

【００７３】

マスターサーバ２０は、（２，３）閾値秘密情報分散処理により、秘密分散化した第１の暗号鍵、及びファイルシーケンス情報を、すべての監視制御装置３０ａ、３０ｂ、３０ｃに送信する。クライアント端末１０から送信される生存確認情報は、監視制御装置３０ｃにのみ送られ、監視制御装置３０ｃは受信した生存確認情報を監視制御装置３０ａと監視制御装置３０ｂに再送信することが好ましい形態であるが、特にこの場合に限られるものではない。

【００７４】

図１２は、実施形態３に係るマスターサーバの一例を示す概略構成図である。実施形態３に係るマスターサーバ２０は、図２に示す実施形態１に係るマスターサーバに、ファイルシーケンス秘密分散処理手段２５－１と、暗号鍵秘密分散処理手段２５－２と、をさらに備える。ファイルシーケンス秘密分散処理手段２５－１及び暗号鍵秘密分散処理手段２５－２は、それぞれ秘匿化手段２２と秘匿化情報送信手段２４との間に接続される。また、図１２に示す秘匿化手段２２は、一体化手段２２－２を省略した図３の構成を用いることも可能である。

【００７５】

ファイルシーケンス秘密分散処理手段２５－１は、ファイルシーケンス情報を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させる。暗号鍵秘密分散処理手段２５－２は、第１の暗号鍵を、複数に分割して互いに可逆演算することで一体化し、かつ、秘密分散法を用いて分散させる。例えば、第１の暗号鍵は、主記憶またはハードディスクに記憶された後に、（２，３）閾値秘密情報分散処理により、３つの秘密分散情報に変換される。そして、３つの秘密分散化された第１の暗号鍵は、秘匿化情報送信手段２４により、図１に示す相異なる３つの監視制御装置３０ａ、３０ｂ、３０ｃに送信される。ファイルシーケンス情報も同様に、（２，３）閾値秘密情報分散処理の後、相異なる３つの監視制御装置３０ａ、３０ｂ、３０ｃに送信される。

【００７６】

ここで、秘密分散法による分散は、実施形態２と同様の方法を用いることができる。ただし、本実施形態では、分散先が複数の監視制御装置３０ａ、３０ｂ、３０ｃであるため、秘密分散処理におけるメンバーをバックアップ装置４０ａ、４０ｂ、４０ｃから監視制御装置３０ａ、３０ｂ、３０ｃに替えて算出する。本実施形態では、（２，３）閾値秘密情報分散処理の例を示すが、この場合に限定されるものではないことは言うまでもない。また、実施形態２と同様に、閾値秘密情報分散は、完全閾値秘密情報分散であってもよいし、不完全閾値秘密情報分散であってもよい。閾値秘密情報分散は、一体化や暗号化をしない完全置換系による秘密情報分散であってもよい。

【００７７】

実施形態３に係る監視制御装置３０ａ、３０ｂ、３０ｃは、図５に示す情報受信手段３１の受信するファイルシーケンス情報及び第１の暗号鍵が秘密分散化されている。情報受信手段３１は、さらに、生存確認情報を、監視制御装置３０ｃから受信することが好ましい。情報格納手段３２は、３つのデータベースを備え、情報受信手段３１の受信する秘密分散化されたファイルシーケンス情報、第１の暗号鍵及び生存確認情報を格納する。

【００７８】

これらマスターサーバ２０及び監視制御装置３０による一連の処理の結果、ファイルシーケンス情報及び第１の暗号鍵は３台の監視制御装置３０ａ、３０ｂ、３０ｃにおいて、（２，３）閾値秘密情報分散処理された形式で保持され、生存確認情報は、３台の監視制御装置３０ａ、３０ｂ、３０ｃにおいて、３重化された複製を保持する。仮に監視制御装置３０ａ、３０ｂ、３０ｃの１台が故障または損壊しても、第１の暗号鍵と、ファイルシ

ーケンス情報は、残りの２台の情報から、生存確認情報は、任意の１台の情報から回復することが可能であり、監視制御装置の再構成も可能となることは、（２，３）閾値秘密情報分散処理をされたことから明らかである。また、上記の例では、悪意のある第三者が、いずれか監視制御装置３０ａ、３０ｂ、３０ｃの１台に侵入した場合においても、生存確認情報のみ漏洩するが、第１の暗号鍵及びファイルシーケンス情報が解読できないことは、（２，３）閾値秘密情報分散処理されたことから明らかである。このことから、クライアント端末１０に分散配備された重要情報が、漏洩する危険性も、回避することができる。

【００７９】

（実施形態４）

本実施形態に係るネットワークシステムは、図１に示す実施形態１に係るネットワークシステムにおいて、マスターサーバ２０から、クライアント端末１０が分散配置された各転送先に対して、地域ごと、またはクライアント端末１０ごとの、暗号化済分割情報の分散配備する方法について、クライアント端末１０の監視制御装置３０ａ、３０ｂ、３０ｃに対するスループット、または、応答遅延時間の計測結果等に基づいて、転送する宛先を適宜、選択して決定できるように、冗長転送することを特徴とする。

【００８０】

図１３は、本実施形態に係るネットワークシステムの一例を示す概略構成図である。本実施形態に係るネットワークシステムは、図５に示す監視制御装置３０が、さらに、クライアント端末状態報告要求送信手段３７－１と、クライアント端末状態情報受信手段３７－２と、スループット等測定手段３７－３と、クライアント端末リスト送信手段３８を備え、情報格納手段３２に新たな機能が加わっている。図４に示すクライアント端末１０が、さらに、クライアント端末状態報告要求受信手段１４－１と、リソース情報伝達手段１５と、クライアント端末状態情報送信手段１４－２を備える。図２に示すマスターサーバ２０が、さらに、クライアント端末リスト受信手段２６と、分割複製数決定手段２７と、送信先決定手段２８を備え、情報格納手段２１に新たな機能が加わっている。

【００８１】

図１３に示すクライアント端末状態報告要求送信手段３７－１は、クライアント端末状態情報の送信を要求するクライアント端末状態報告要求を、それぞれのクライアント端末１０に送信する。クライアント端末状態情報は、クライアント端末１０の状態を示す情報であり、クライアント端末自身のリソース管理の状態を示す。クライアント端末状態報告要求受信手段１４－１は、クライアント端末状態報告要求送信手段３７－１の送信するクライアント端末状態報告要求を受信する。リソース情報伝達手段１５は、クライアント端末状態報告要求受信手段１４－１がクライアント端末状態報告要求を受信すると、クライアント端末１０の状態を検出してクライアント端末状態情報を出力する。クライアント端末状態情報送信手段１４－２は、リソース情報伝達手段１５の出力するクライアント端末状態情報を、監視制御装置３０へ送信する。

【００８２】

ここで、クライアント端末状態情報は、クライアント端末１０が管理するリソース情報であり、例えば、クライアント端末ＩＤ、ＣＰＵ使用管理情報、メモリ空き領域情報、ハードディスク空き領域情報である。各々のクライアント端末は、個別のクライアント端末ＩＤ情報をもち、これにより、監視制御装置は、各々のクライアント端末を識別する。各クライアント端末ＩＤ毎に、リソース管理情報として、自身のリソース管理の状態を管理する。ここで、リソース管理の状態は、例えば、ＣＰＵの使用率、メモリ空き領域、ハードディスクの空き領域である。ＣＰＵの使用率は％の単位で、メモリ空き領域はＧＢ（ギガバイト）の単位で、ハードディスクの空き領域はＧＢギガバイトの単位で管理されることが好ましいが、この単位に限定されるものではない。リソース情報伝達手段１５は、パソコンなどの一般的な情報端末に具備されている機能に該当する。クライアント端末１０は、自身のリソース管理の状態を測定し、クライアント端末状態ファイルに書き込み、クライアント端末状態を示すリソース管理用のファイルをクライアント端末リストとして監

視制御装置３０に送信する。

【００８３】

また、クライアント端末ＩＤは、マスターサーバ２０、監視制御装置３０がクライアント端末１０を識別する際に用いるＩＤである。クライアント端末ＩＤは、クライアント端末ＩＤの所持するＩＰアドレスと、通常は、１対１の関係をもつ。例えば、５桁の数字で表現されるクライアント端末ＩＤのなかで、前半の２桁は地域の識別情報であり、後半の３桁は地域内でのクライアント端末を識別するためのクライアント端末の識別情報である。

【００８４】

図１３に示すクライアント端末状態情報受信手段３７－２は、クライアント端末１０から送信されたクライアント端末状態情報を受信する。スループット等測定手段３７－３は、クライアント端末１０との間のスループットを測定する。ここで、スループットは、例えば、クライアント端末状態報告要求送信手段３７－１がクライアント端末状態報告要求を送信してから、クライアント端末状態情報受信手段３７－２がクライアント端末状態情報を受信するまでの応答時間に基づいて測定する。この際、クライアント端末１０から送信されたクライアント端末状態情報を考慮することが好ましい。情報格納手段３２は、クライアント端末状態情報受信手段３７－２の受信するクライアント端末状態情報と、スループット等測定手段３７－３の測定したスループットを、クライアント端末リストの情報として情報格納手段３２に格納する。監視制御装置３０内のクライアント端末リスト送信手段３８は、情報格納手段３２に格納されているクライアント端末リストを、マスターサーバ２０に送信する。

【００８５】

例えば、監視制御装置３０は、クライアント端末状態を、受信するのに要する時間を測定し、クライアント端末１０－監視制御装置３０間のスループット、応答時間などを測定する。もし、クライアント端末１０のリソース管理状態が、予め想定された閾値を超えるものであることを監視制御装置３０が判定した場合には、その旨を示す登録情報を監視制御装置内のデータベースに保持する（図１４）。試験データなどのデータファイルの受信が、監視制御装置３０において、不可能であった場合は、クライアント端末１０は使用不可能であるとみなし、その旨を通知する。

【００８６】

また、予め定めた規定タイミング内での応答が、当該クライアント端末１０からない場合には、当該クライアント端末１０は、使用不能である旨の登録処理を情報格納手段３２を用いて実施する。また、予め定めた規定タイミング内での応答が、当該クライアント端末からあった場合には、当該クライアント端末のリソース使用状況を示す指標である、３つの条件が、当該クライアント端末からの返送データにより、すべて満足していることが明らかになった場合にのみ、当該クライアント端末が「正常」に使用可能であることを確認し、「正常」である旨の登録処理を、情報格納手段３２を用いて実施する。３つの条件は、第１にＣＰＵ使用率は閾値以下であること、かつ、第２にメモリ空き領域は閾値以下であること、かつ、第３にハードディスク空き領域は十分であることである。上記３つの条件のいずれか、１つでも満足できない状況が、当該クライアント端末からの返送データにより、明らかになった場合には、当該クライアント端末が、異常であると確認し、「異常」状態にある旨の登録処理を、情報格納手段３２を用いて実施する（図１５）。

【００８７】

図１３に示す情報格納手段３２には、クライアント端末ごとのスループットを格納することが好ましい。例えば、スループット等測定手段３７－３を用いてクライアント端末ＩＤ毎に取得できたデータに基づいて、使用可能である端末群の情報が情報格納手段３２へ格納される。ここで、一般にクライアント端末１０は複数の地域（例えば、$Ｊ_{1}$，$Ｊ_{2}$，・・・$Ｊ_{N}$）に分散して配備される。監視制御装置３０の中の情報格納手段３２には、当該クライアント端末ＩＤ毎のスループットは、たとえばＭｂ／ｓを単位として格納される。この結果、監視制御装置３０は、どのクライアント端末１０が使用可能であるかが判断

できる。監視制御装置３０は、上記の手順で取得したクライアント端末状態情報に基づいて、使用可能である端末群を選択し、さらに、暗号化済分割情報の受信可否を判断できるための、クライアント端末リストを作成し、マスターサーバ２０へ送信する。

【００８８】

ここで、クライアント端末リストとは、情報格納手段２１に格納される、暗号化済分割情報のデータ転送先として適切な転送先端末リストであり、これは、地域グループＩＤ毎に分割され、地域グループ毎のクライアント端末群を示したリストであることが好ましい。具体的には、例えば、地域グループを＃１、＃２、・・・、＃Ｎ（１００未満）に分け、各々の地域の識別用に２桁の整数（０１、０２、・・・、Ｎ）を使用し、同一地域内の端末識別用には、たとえば３桁の整数を用いることができる。

【００８９】

図１３に示すクライアント端末リスト受信手段２６は、クライアント端末リスト送信手段３８の送信するクライアント端末リストを受信する。情報格納手段２１は、クライアント端末リスト受信手段２６の受信するクライアント端末リストを格納する。マスターサーバ２０内の分割複製数決定手段２７は、クライアント端末リスト送信手段３８の送信するクライアント端末リストに基づいて、秘匿化手段２２における分割数及び複製数を決定する。マスターサーバ２０内の秘匿化手段２２は、分割複製数決定手段の決定する分割数及び複製数に、分割及び複製する。マスターサーバ２０内の送信先決定手段２８は、クライアント端末リスト送信手段３８の送信するクライアント端末リストに基づいて、暗号化済分割情報を送信するクライアント端末１０を決定する。

【００９０】

ここで述べる分割データは、分割手段（図２に示す符号２２－３）からの出力データを示す。分割データに付与されるファイル名は、例えば、２桁の数字で表現され、その２桁の数字により、データファイルを何番目に分割したものであるかが識別できる。また、分割複製データは、第２暗号化手段（図２に示す符号２２－５）からの出力データすなわち暗号化済分割情報を示す。分割複製データのファイル名は、例えば、４桁の数字で表現され、前半の２桁が、データファイルを何番目に分割したものであるかを識別する分割番号を示し、後半の２桁が何番目に複製された分割データであるかを識別する複製データ番号を示す。例えば、分割数２、複製数２の時は、合計で４つの分割複製データが生成され、ファイル名は、それぞれ、０１０１、０１０２、０２０１、０２０２で表現できる。分割複製データはすべて異なる暗号鍵で暗号化されるため、見かけ上は、全く異なるファイルに見えることは言うまでもない。分割複製データには、分割番号が付与され、また、複製されたファイルに対しても、複製順の複製データ番号が付与され、これらの値は、互いに重複がないように、設定されるため、見かけ上は、１つの元ファイルに対して、（分割数）×（複製数）に対応する数の別個のファイルが生成され、さらに各々は、別別の異なる暗号鍵で、暗号化されている。

【００９１】

マスターサーバ２０は、クライアント端末群リストの情報と、送信すべきデータファイルの容量等を総合的に判断して、スループットが一定値以下のクライアント端末１０を、クライアント端末群リストから削除して、自身のデータベース内に保持することが好ましい。図１６に、送信先決定手段２８によるクライアント端末１０の使用可否の登録を行うフローを示す。送信先決定手段２８は、上記手順の結果、データ転送先として適切と考えられるクライアント端末リストを地域グループＩＤ毎に分割し、地域グループ毎のクライアント端末群リストを作成する。

【００９２】

この後、暗号化済分割情報を適切にシャフリングし、最終的なデータ転送用の分割複製データファイル名リストを作成する。ここで、シャフリングは、分割数が２、複製数が２であれば、４個の暗号化済分割情報が生成される。この場合、４種類の暗号化済分割情報の並べ方は４！通りあり、この中の１つの組み合わせが、暗号化済分割情報の更新の都度、任意に選択できる。図１７に、一般的な、送信先決定手段２８における暗号化済分割情

報のランダム並べ替えのための実施例を示す。一例として、分割数αが１０のときの文字列Ｘ（ｐ）の設定例を述べる。

【００９３】

図１３に示す送信先決定手段２８において、暗号化済分割情報の送信先をランダムに並べてシャフリングするための実施例を以下に説明する。例えば、シャフリングするに当たって必要な各種のパラメータとしては、以下のパラメータが存在する。第１は分割数α、第２は複製数β、第３は乱数ｐ、第４は乱数ｑ、第５は乱数ｐ用の種、第６は乱数ｑ用の種、第７は文字列Ｘ、第８は文字列Ｙ、第９は文字列Ｘと文字列Ｙを連結した文字列ＸＹである。乱数ｐは、要素（１、２、３、・・・、α）の中からランダムに選択される。乱数ｑは、要素（１、２、３、・・・、β）の中からランダムに選択される。ここで、分割数、複製数の値を元に、分割複製データファイル名リストに順次、ファイルの生成が実施された順に登録処理を行う必要がある。例えば、分割数２、複製数２の時は、暗号化済分割情報として合計で４つのファイルが生成される。この場合、分割複製データ０１０１、０１０２、０２０１、０２０２の順に登録処理を行う。

【００９４】

生成・登録された分割複製データ転送先リストを地域グループ毎に分けられたクライアント端末リストに対応させる必要がある。この場合の上記のシャフリングの例として、例えば、クライアント端末リスト順番に配布する際の順番は、分割数が４、複製数が３の場合には、クライアント端末１０に転送される対象となるファイル数は、合計１２（＝３×４）個、存在し、分割複製データファイル名リストから、分割複製データを1つずつ、抜き出し、地域グループ毎のクライアント端末群リストに順次、対応させ、分割複製データ転送先リストを作成する。このとき、生成順で表現された分割複製データの並べ方は、０１０１、０１０２、０１０３、０２０１、０２０２、０２０３、０３０１、０３０２、０３０３、０４０１、０４０２、０４０３であるが、この順序は、一例として、各地域に、次の更新時には、０３０２、０４０３、０１０２、０１０３、０２０３、０１０１、０４０１、０３０３、０４０２、０２０２、０２０１、０３０１となる。分割複製データ転送先リストの情報は、固定的に保持されるものではない。例えば、クライアント端末リストは監視制御装置３０から随時送信される。時々刻々変化するクライアント端末リストの情報に基づいて、任意に変更できることは言うまでもない。

【００９５】

分割複製データファイル名リストの各々は、元ファイルデータの分割番号と複製データ番号の対とで構成され、これらが各地域毎に、登録される。従って、分割複製データ０３０２、０４０３、０１０２、０１０３、０２０３、０１０１、０４０１、０３０３、０４０２、０２０２、０２０１、０３０１の順序で、マスターサーバ２０の暗号化済分割情報送信手段２３を用いて各クライアント端末１０へ送信され、安全性を高めることが可能となる。この時、マスターサーバ２０は、データファイルを暗号化した際に用いた暗号鍵や、分割複製データ転送先リストを、シーケンス情報として、監視制御装置３０へ、同時に秘匿化情報送信手段２４を用いて、送信する。監視制御装置３０が、元データファイルを復元する際には、分割複製データ転送先リストを参照し、クライアント端末１０の選択を行うことにより、必要な暗号化済分割情が回収、復元できる。

【００９６】

図１３に示す送信先決定手段２８において、地域グループを考慮したクライアント端末への暗号化済分割情報の送信例について説明する。地域グループ数が４、各地域グループ内のクライアント端末数が、地域番号０１、地域番号０２、地域番号０３、地域番号０４のそれぞれに対して、４、１、３、２である場合を想定した例を示す。この場合、地域グループ内の端末の識別番号を３桁の数字で表示すると、地域番号０１の４台のクライアント端末名は、それぞれ、０１００１、０１００２、０１００３、０１００４と表示できる。各地域番号対応に利用可能なクライアント端末は、事前に、監視制御装置３０からの試験データ送信時の応答時間が、基準値を満足しているか、または、推定できる当該端末からのスループット値が、基準値を満足しているもののみが、地域毎のリストに、上位が高

い優先転送先を示すように、登録される場合を想定する。優先順位の高い順番にリストを構成する並べ替えの手法は、一般的に使用されている、バブルソートや手法やクイックソート手法等の技術を適用すれば、容易に実現可能である。

【００９７】

地域毎に利用可能なクライアント端末は、通常は、各地域毎に、できるだけ、均等に暗号化済分割情報が、暗号化済分割情報送信手段２３を用いて分散転送されることを想定する場合、各地域毎に転送されるファイル数の平均は３（＝１２÷４）である。例えば、分割複製データは、１番目に０３０２、２番目に０４０３、３番目に０１０２、４番目に０１０３、５番目に０２０３、６番目に０１０１、７番目に０４０１、８番目に０３０３、９番目に０４０２、１０番目に０２０２、１１番目に０２０１、１２番目に０３０１、の順番で転送される。１、２、３、４番目は、順番に地域番号０１、０２、０３、０４に配布される。次は、５、６、７、８番目が同様に、地域番号０１、０２、０３、０４に配布される。最後に、９、１０、１１、１２番目も同様に、地域番号０１、０２、０３、０４に配布される。

【００９８】

ここで、地域番号０２、０３及び０４のように、同一の地域番号内で利用可能なクライアント端末数が少ない、３未満の場合には、１つのクライアント端末に、複数の暗号化済分割情報が転送される場合が発生する。従って、地域番号０１では、分割複製データ０３０２、０２０３、０４０２が格納される。また、地域番号０４に対応する場所では、利用可能なクライアント端末がクライアント端末０４０００２、０４０００１の２台が存在するため、最初の分割複製データ０１０３は４番目の順でクライアント端末０４０００２へ転送され、その次に、同じ地域番号０４に転送された分割複製データ０３０３は、８番目の順で、クライアント端末０４０００１へ転送される。さらに、その次に同じ地域番号０４に転送された分割複製データ０３０１は、１２番目の順で、クライアント端末０４０００２へ転送される。また、地域番号０２には、利用可能な端末がクライアント端末０２００１の１台しかないので、分割複製データ０４０３、０１０１、０２０２が、それぞれ、２番目、６番目、１０番目に分散転送される。

【００９９】

この例では、地域間で、均等に分割する場合を想定した例を示したが、地域毎に、重みつけを変更して分散転送する方法も、同様に可能であることは言うまでもない。また、地域毎の分散転送する際のバランスを無視し、ランダムに分散転送する方法も、容易に実現可能である。また、分割複製総数（α・β）＝４００で、地域数が１０の場合には各地域毎に４０端末以上が利用可能であれば十分であり、産業利用上の実用性も十分に高いと考えられる。以上述べたように、クライアント端末名と、ランダムに並べ替えられた、分割複製データファイル名リストとは、対応付けを考慮して転送する必要がある。

【０１００】

以上述べたように、クライアント端末と、ランダムに並べ替えられた分割複製データとは、対応付けを考慮して転送する必要がある。図１８に、地域グループ内のクライアント端末への分割複製データの転送処理フローを示す。クライアント端末に優先順位毎に転送されることを想定している。実際の運用に当たっては、１つの地域グループ内に、暗号化済分割情報のすべてがそろわないようにする工夫は、当該の地域ごとに、分割されたデータファイルがどのように配備されているかのデータを参照することにより、容易に可能である。

【０１０１】

以上、説明したように、第１の暗号化鍵及びファイルシーケンス情報やクライアント端末情報など、それぞれ、別の地域、あるいは、同一地域内の物理的に異なるサーバに、監視制御装置側からの、制御コマンド等により、分散配置することが、自由に制御できるネットワークメカニズムを具備することにより、グリッドコンピューティング技術を用いたディザスタリカバリシステムの安全性及び信頼性を飛躍的に向上することが可能となる。

【０１０２】

図１４は、本実施形態に係る監視制御装置の動作の一例を示すフローである。
ステップＳ３０１では、クライアント端末状態報告要求送信手段３７－１が、各クライアント端末１０に対し、クライアント端末状態報告要求を送信する。ここで、クライアント端末状態報告要求は、リソース情報伝達手段１５に格納されているクライアント端末状態を送信する旨の要求である。クライアント端末状態とは、クライアント端末１０自身の状態示す情報であり、例えば、ＣＰＵの使用率、メモリ、ハードディスクの空き容量である。
ステップＳ３０２では、スループット等測定手段３７－３が、規定時間以内にクライアント端末状態送信手段１４－２からクライアント端末状態情報を受信したか否かを判断する。スループット等測定手段３７－３が、規定時間以内にクライアント端末状態情報送信手段１４－２からクライアント端末状態情報を受信したと判断した場合、ステップＳ３０３に移行する。一方、スループット等測定手段３７－３が、規定時間以内にクライアント端末状態情報送信手段１４－２からクライアント端末状態情報を受信しなかったと判断した場合、ステップＳ３０５に移行する。
【０１０３】
ステップＳ３０３では、スループット等測定手段３７－３が、ステップＳ３０１におけるクライアント端末状態報告要求の送信から、クライアント端末状態情報送信手段１４－２からのクライアント端末状態情報の受信までの応答時間を測定する。
ステップＳ３０４では、スループット等測定手段３７－３が、受信したクライアント端末状態情報及び測定した応答時間から、スループットを算出する。ここで、スループットは、例えば、スループット等測定手段３７－３が送出した測定用データ量がＸ（ｂｉｔ）であり、この返信要求に対する応答までにＹ（秒）の応答時間を要した場合には、（Ｘ／Ｙ）（ｂｉｔ／ｓ）をスループット値として算出する。そして、スループット等測定手段３７－３は、受信したクライアント端末状態情報、測定した応答時間及びスループットを、情報格納手段３２に格納する。
ステップＳ３０５では、スループット等測定手段３７－３が、クライアント端末状態情報送信手段１４－２から規定時間以内にクライアント端末状態情報を受信しなかったことを確認し、クライアント端末１０の使用不可能と決定する。ここで、確認は、例えばクライアント端末状態報告要求受信手段１４－１において受信が正常に行われなかったことを認識することで行う。
ステップＳ３０６では、情報格納手段３２に、クライアント端末１０が使用「不能」である旨を登録する。ステップＳ３０５において規定時間内に当該ファイルを受信できない場合のほかに、次の手順によってクライアント端末１０の「正常」、「不能」又は「異常」を確認してもよい。
【０１０４】
図１５は、スループット等測定手段３７－３がクライアント端末の「正常」、「不能」又は「異常」を確認する動作の一例を示すフローチャートである。
ステップＳ４０１では、クライアント端末状態報告要求送信手段３７－１が、クライアント端末状態報告要求受信手段１４－１に、クライアント端末状態報告要求を送信する。
ステップＳ４０２では、スループット等測定手段３７－３が、クライアント端末状態報告要求受信手段１４－１から、規定タイミング内での応答があったか否かを判定する。応答があった場合ステップＳ４０３へ移行し、応答がなければステップＳ４０７へ移行する。
ステップＳ４０７では、スループット等測定手段３７－３が、ステップＳ４０２において規定タイミング内での応答がなかった当該ＩＤを持つクライアント端末１０が使用「不能」であると決定し、その旨を当該ＩＤに対して登録する。
【０１０５】
ステップＳ４０３では、スループット等測定手段３７－３が、ＣＰＵ使用率は閾値以下か否かを判定する。ここで、閾値は、クライアント端末１０が高いＣＰＵ使用率のもとで、マスターサーバ２０からの暗号化済分割情報を受信しないような状態を実現せしめるた

めに適切な値を設定する。例えば、ＣＰＵ使用率が２０％以下であれば、他のプロセスの実行には大きな影響を与えないとの判断を行った場合、または、クライアント端末１０からの要求条件がこの値であれば使用可能との別途の契約があった場合には、当該閾値として２０％を設定する。

ステップＳ４０４では、スループット等測定手段３７－３が、クライアント端末１０が十分な空きメモリをもっているかどうかを判定することにより使用可能か否かの判断を行う。ここで、閾値は、クライアント端末１０が少ない空きメモリ領域のもとで、マスターサーバ２０からの暗号化済分割情報を受信し得ないような状態を実現せしめるために適切な値を設定する。例えば、全体で２ＧＢのメモリを持つクライアント端末１０が、空きメモリ領域として全体の５０％である１ＧＢをもっている場合には、メモリ空き領域が１ＧＢ以上であれば、他のプロセスの実行には大きな影響を与えないとの判断を行った場合、または、クライアント端末１０からの要求条件が、この値であれば使用可能との別途の契約があった場合には、当該閾値として１ＧＢを設定する。

ステップＳ４０５では、スループット等測定手段３７－３が、クライアント端末１０が十分なハードディスク空き領域をもっているかどうかを判定することにより使用可能か否かの判断を行う。ここで、十分かどうかは、例えば、全体で１００ＧＢのハードディスク領域を持つクライアント端末が、空きハードディスク空き領域として全体の８０％である８０ＧＢをもっている場合には、ハードディスク空き領域が８０ＧＢ以上であれば、他のプロセスの実行には大きな影響を与えないとの判断を行った場合、または、クライアント端末１０からの要求条件が、この値であれば使用可能との別途の契約があった場合には、当該閾値として８０ＧＢで十分と判断する。

【０１０６】

ステップＳ４０６では、スループット等測定手段３７－３が、ステップＳ４０３からステップＳ４０５での判断が正常であったことを「正常」と決定し、その旨を当該ＩＤに対して登録する。

ステップＳ４０８では、スループット等測定手段３７－３が、当該ＩＤを持つクライアント端末に対して、ステップＳ４０３からステップＳ４０５までの判断のうち、いずれかが、満足されなかったことを「異常」と決定し、その旨を当該ＩＤに対して登録する。ここで、確認は、スループット等測定手段３７－３に返信されたメッセージの内容を照合することにより行う。また、登録処理では、情報格納手段３２に、全てのクライアント端末１０のＩＤに対して、「正常」、「異常」、「不能」の識別を行うと共に、関連する詳細情報（例えばリソース情報）を含めたリストを作成する。例えば、ステップＳ４０３～Ｓ４０５での判断が正常であったことを確認できた場合には、当該クライアント端末１０に対して正常登録処理が行われた旨の結果を格納する。

【０１０７】

図１６は、クライアント端末１０の使用可否の登録の一例を示すフローチャートである。

ステップＳ５０１では、データファイルの初期設定を行う。初期設定は、バックアップの対象となるデータファイルのファイルサイズ、クライアント端末１０の故障率、依頼者が要求する暗号強度に応じた分割数、暗号化済分割情報の数に対応したバックアップ確率、利用可能となるクライアント端末数を、情報格納手段２１から読み出し、総合的に判断して、ファイルの分割数、分割ファイルの複製数を決定する。

【０１０８】

例えば、秘匿化手段２２における、分割手段でのデータファイルの分割数がｎ、複製手段での分割ファイル当たりの複製数がｍ、クライアント端末１０の故障率がｐ（＜＜１）である場合を想定し、クライアント端末１０がランダムに故障すると仮定すると、マスターサーバ２０が故障した時のファイルの復元確率は、回復率　$(1-P^m)^n$　$1-nP^m$となる。したがって、仮に、合計１００ＭＢのデータファイルをバックアップする場合、利用可能クライアント端末１０の数が２００あり、かつ、クライアント端末１０の故障率が２０％（＝１／５）であり、バックアップ依頼者の要求するディザスタ発生時の回復

確率が、９９．９９９％以上である場合を仮定する。この時、分割数ｎを２０、複製数ｍを１０と設定すると、回復率　１－ｎＰ^{m}＝０．９９９９９８となり、バックアップ依頼者の要求条件を満足することができる。

【０１０９】

ステップＳ５０２では、送信先決定手段２８が、クライアント端末と監視制御装置間で必要となる実効的な回線速度の閾値に対する判断および設定を行う。ここで、閾値は、仮にディザスタがマスターサーバ２０で発生した時の分割データの回収時間が大幅に遅れないようにするための必要十分な時間を、監視制御装置３０が推定することによりマスターサーバ２０（あるいは、場合によっては監視制御装置３０）が設定する。

ステップＳ５０３では、送信先決定手段２８が、監視制御装置３０から転送された全クライアント端末リストのクライアント端末状態情報の読み出し及び確認を行う。ここで、クライアント端末リストは情報格納手段２１から取得する。クライアント端末リストは、スループット、ＣＰＵの使用率、メモリ空き領域、ハードディスクの空き領域の大きさや、「正常」「異常」「使用不能」状態などが記されており、ｉ行目を読み込むため、「正常」情報が格納されていることが好ましい。

【０１１０】

ステップＳ５０４では、送信先決定手段２８が、クライアント端末１０の使用可否の登録を当該クライアント端末の応答時間またはスループットを読み出し、この値が予め設定された閾値を満足しているか否かの判断を行う。ここで、閾値は、クライアント端末１０がバックアップ処理を実施することにより、他のプロセスの実行に影響を与えないことと、迅速なバックアップが実現できるように実行できることを可能とすることを目標として設定する。

ステップＳ５０５では、送信先決定手段２８が、クライアント端末１０が使用可能である旨を登録する。例えば、情報格納手段２１に、「正常」すなわち使用可能な状態にある旨を表記する情報を格納する。「正常」の旨を表記する情報は、互いにクライアントＩＤ、ＣＰＵ使用率、空きハードディスク容量、応答時間等と関連付けられていることが好ましい。

そして、ステップＳ５０３からステップＳ５０５までをｉの値が２からＮになるまで繰り返し、ｉの値がＮになると終了する。

一方、ステップＳ５０６では、送信先決定手段２８が、クライアント端末１０が使用不可能である旨を登録する。例えば、情報格納手段２１に、「異常」または「不能」の旨を表記する情報を格納する。「異常」または「不能」の旨を表記する情報は、互いにクライアントＩＤ、ＣＰＵ使用率、空きハードディスク容量、応答時間等と関連付けられていることが好ましい。この登録の後、まだ、すべてのクライアントに対する処理が終了していない場合には、端末リスト番号を１追加して、クライアント端末リストのｉ行目の読み込みの処理（Ｓ５０３）に遷移する。

【０１１１】

図１７は、送信先決定手段２８による暗号化済分割情報のランダム並べ替えのための実施例の一例を示すフローチャートである。

ステップＳ６０１では、前述した暗号化の強度や回復時間、利用可能端末数の情報に基づいて、分割数αおよび複製数βを設定する。ステップＳ６０２では、乱数の種Ｓ１及びＳ２を設定する。これにより、どの分散されたクライアント端末１０に、適切にシャフリングして転送するかに関わる処理を行うことができる。ここで、乱数の種Ｓ１及びＳ２とは、ステップＳ６０３で生成させる乱数の種類であり、例えば、５桁程度の整数乱数発生アルゴリズムを用いて作成される。基本的には、周期性が容易に推定できない程度のものに選定されることで足りる。初期設定においても、周期性が推定できないような基準で行えばよい。例えば、現在の時刻を秒単位で表現したときの上位５桁などで足りる。

【０１１２】

ステップＳ６０３では、暗号鍵となる文字列Ｘ（ｐ）及び文字列Ｙ（ｑ）を生成するための前準備として、乱数ｐ及びｑを生成する。例えば、（０．１）の範囲内で、一様分布

に従う乱数ｐ及びｑの生成を行う。ステップＳ６０４では、文字列Ｘ（ｐ）、Ｙ（ｑ）の生成および連結を行う。例えば、分割数αが１０であり、仮に、乱数ｐを０．３３と仮定すると、文字列Ｘ（ｐ）は、次式で求められる。

【数１３】

$$X(p)=\text{整数部}[\alpha\times 0.33]+1$$

$$=\text{整数部}[10\times 0.33]+1=3+1=4$$

【０１１３】

ここで、文字列Ｘ（ｐ）を例えば、１０進２桁の数値で表現すると仮定すると、文字列Ｘ（ｐ）＝”０４”となる。実際には、分割数の大きさによって、３桁以上で表現する場合も同様に可能である。また、複製数βの設定により、文字列Ｙ（ｑ）も同様に決定することができ、Ｘ（ｐ）及びＹ（ｑ）を相互に組み合わせて連結することにより、最終的な文字列の組み合わせとしてＸ（ｐ）及びＹ（ｑ）を生成することができる。

【０１１４】

ステップＳ６０５では、新しく生成されたＸ（ｐ）及びＹ（ｑ）が、既に生成されていた一連の組み合わせを参照し、新しい文字列Ｘ（ｐ）及びＹ（ｑ）が既に登録されているか否かを判定する。ステップＳ６０５において、文字列Ｘ（ｐ）及び文字列Ｙ（ｑ）が既に登録されていればステップＳ６０９に移行し、登録されていなければステップＳ６０６に移行する。

ステップＳ６０６では、文字列Ｘ（ｐ）及び文字列Ｙ（ｑ）を登録する。例えば、情報格納手段２１又は送信先決定手段２８に、文字列Ｘ（ｐ）及び文字列Ｙ（ｑ）を格納する。

ステップＳ６０７では、登録の組み合わせ総数Ｎのカウントアップを行う。ステップＳ６０８では、登録の組み合わせ総数Ｎが必要数（α・β）に達しているかどうかの判断を行う。

ステップＳ６０９では、新たな乱数ｐ、ｑを生成するために必要な、乱数の種Ｓ１及びＳ２の数値のカウントアップを行う。

【０１１５】

図１８は、本実施形態に係る送信先決定手段２８及び暗号化済分割情報送信手段２３における動作の一例を示すフローチャートである。

ステップＳ７０１では、分割複製数決定手段２７が、ファイルデータに対する分割数と複製数を設定する。ここで、設定は、前述した暗号化の強度や回復時間、利用可能端末数の情報を基準に行う。例えば、分割数は、データファイルを情報格納手段２１から読出し、読み出したデータファイルの容量に応じて設定する。ステップＳ７０２では、秘匿化手段２２がデータファイルを秘匿化し、その後で、送信先決定手段２８が、どの分散されたクライアント端末１０に、適切にシャフリングして転送するかに関わる処理を行うことで、分割複製データファイル名リストを作成する。

【０１１６】

ステップＳ７０３では、送信先決定手段２８が、監視センタ３０から転送された全クライアント端末リストのリソースに関する情報の読み出し・チェックを行う。クライアント端末リストは、情報格納手段２１から取得する。情報格納手段２１には、各クライアント端末１０の識別情報とともに地域情報が格納されており、地域グループに属するか否かは、地域情報に基づいて判断する。

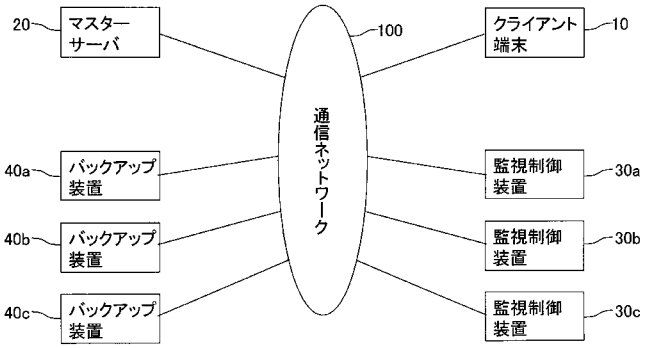
ステップＳ７０４では、暗号化済分割情報送信手段２３が、ステップＳ７０３で対応付けたクライアント端末に対して、暗号化済分割情報を送信する。

ステップＳ７０５では、暗号化済分割情報送信手段２３が、分割複製データファイル名リストに対応付けられたクライアント端末１０の全てに対する送信が終了したか否かを判定する。送信が終了していない場合にはステップＳ７０４に移行し、再度ステップＳ７０４及びステップＳ７０５を繰り返す。一方、ステップＳ７０５において送信が終了した場

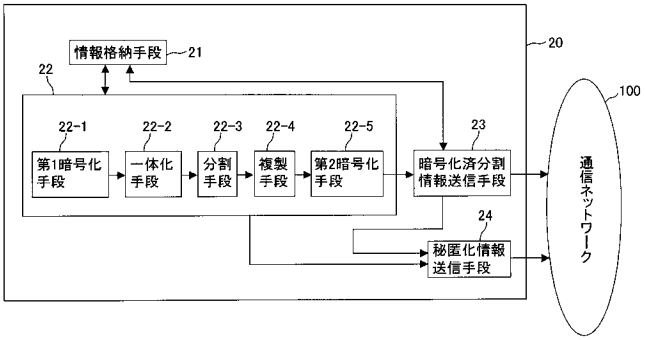
合には、処理を終了する。
【産業上の利用可能性】
【０１１７】
本発明は、通信ネットワークを用いて、データファイルをリカバリするために必要となるメタデータを含むデータベース情報を、超分散化し、かつネットワーク上に分散配備されるメタデータを含むデータベース用サーバに分散転送することにより、マスターサーバが管理する重要なデータファイルを安全かつ効率的にバックアップすることができるため、大規模かつ重要なデータベースを災害から保護し、画期的な安全と信頼性向上の効用の双方を、産業界に提供することができる。特に、分散されたＰＣを対象としてバックアップ手法以外に、携帯端末を、グリッドクライアントノードとしても、活用することにより、その産業界に与える効用は計り知れない。
【図面の簡単な説明】
【０１１８】
【図１】実施形態１に係るファイルバックアップ用ネットワークシステムの一例を示す概略構成図である。
【図２】実施形態１に係るマスターサーバの一例を示す概略構成図である。
【図３】マスターサーバの秘匿化手段の別の一例を示す概略構成図である。
【図４】実施形態１に係るクライアント端末の一例を示す概略構成図である。
【図５】実施形態１に係る監視制御装置の一例を示す概略構成図である。
【図６】実施形態１に係るバックアップ装置の一例を示す概略構成図である。
【図７】実施形態２に係る監視制御装置の一例を示す概略構成図である。
【図８】実施形態２に係るバックアップ装置の一例を示す概略構成図である。
【図９】秘密分散処理手段の動作の一例を示すフローチャートである。
【図１０】完全置換系の表作成アルゴリズムの一例を示すフローチャートである。
【図１１】完全置換系の表作成アルゴリズムの説明図である。
【図１２】実施形態３に係るマスターサーバの一例を示す概略構成図である。
【図１３】実施形態４に係るファイルバックアップ用ネットワークシステムの一例を示す概略構成図である。
【図１４】実施形態４に係る監視制御装置の動作の一例を示すフローチャートである。
【図１５】スループット等測定手段３７－３がクライアント端末の「正常」、「不能」又は「異常」を確認する動作の一例を示すフローチャートである。
【図１６】クライアント端末１０の使用可否の登録の一例を示すフローチャートである。
【図１７】送信先決定手段２８における暗号化済分割情報のランダム並べ替えのための実施例の一例を示すフローチャートである。
【図１８】送信先決定手段２８及び暗号化済分割情報送信手段２３における動作の一例を示すフローチャートである。
【符号の説明】
【０１１９】
１０　クライアント端末
１１　暗号化済分割情報受信手段
１２　情報格納手段
１３　生存確認情報送信手段
１４－１　クライアント端末状態報告要求受信手段
１４－２　クライアント端末状態情報送信手段
１５　リソース情報伝達手段
２０　マスターサーバ
２１　情報格納手段
２２－１　第１暗号化手段
２２－２　一体化手段
２２－３　分割手段

２２－４　複製手段
２２－５　第２暗号化手段
２３　暗号化済分割情報送信手段
２４　秘匿化情報送信手段
２５－１　ファイルシーケンス秘密分散処理手段
２５－２　暗号鍵秘密分散処理手段
２６　クライアント端末リスト受信手段
２７　分割複製数決定手段
２８　送信先決定手段
３０、３０ａ、３０ｂ、３０ｃ　監視制御装置
３１　情報受信手段
３２　情報格納手段
３３　情報送信手段
３４　秘密分散処理手段
３７－１　クライアント端末状態報告要求送信手段
３７－２　クライアント端末状態情報受信手段
３７－３　スループット等測定手段
３８　クライアント端末リスト送信手段
４０、４０ａ、４０ｂ、４０ｃ　バックアップ装置
４１－１、４１－２、４１－３　バックアップ情報受信手段
４２－１、４２－２、４２－３　バックアップ情報格納手段
１００　通信ネットワーク

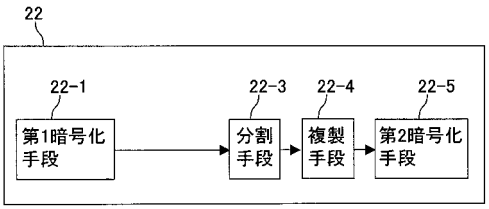
【図１】



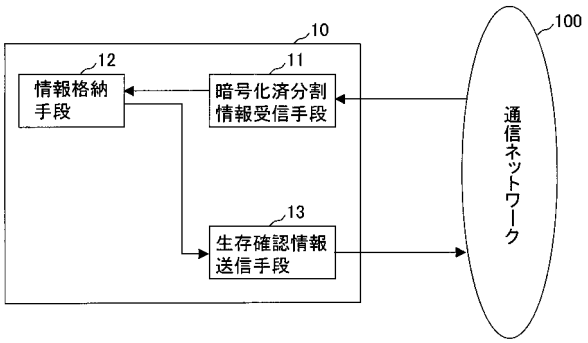
【図２】



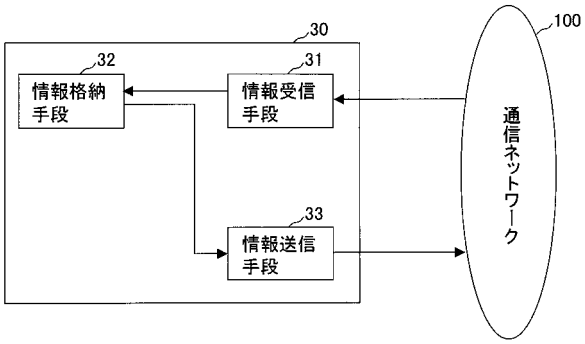
【図３】



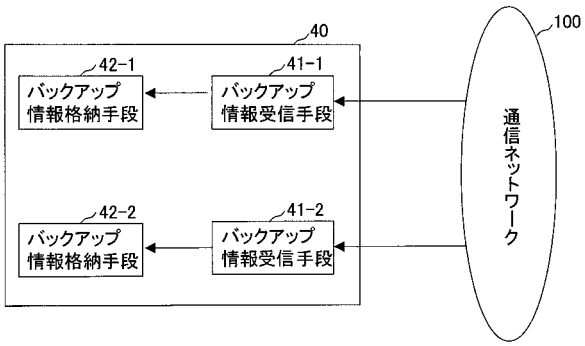
【図４】



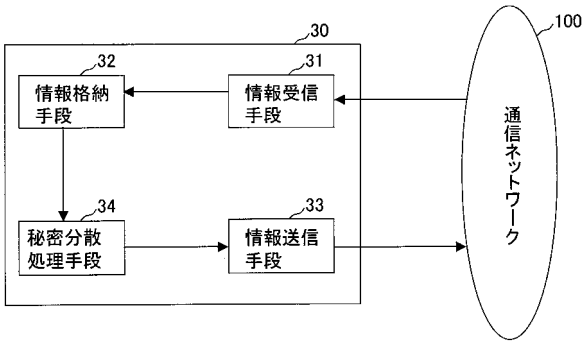
【図５】



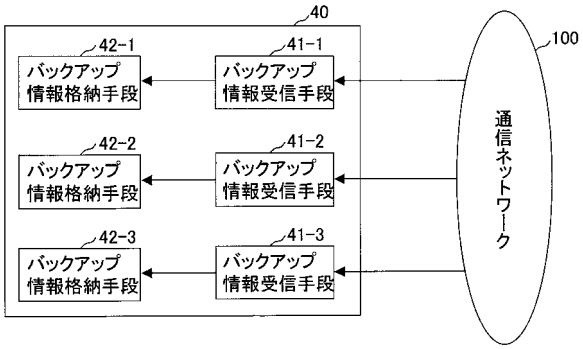
【図６】



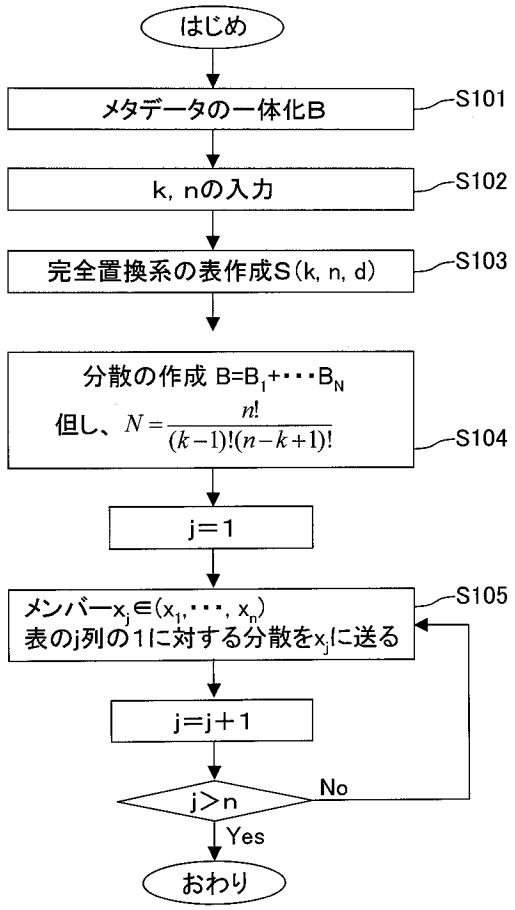
【図７】



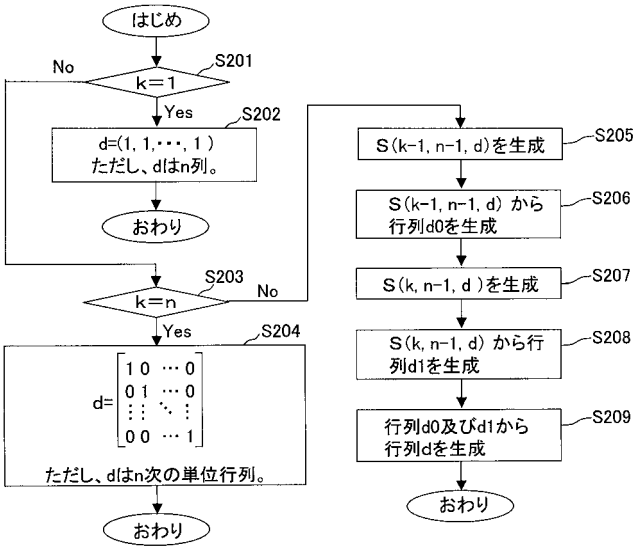
【図８】



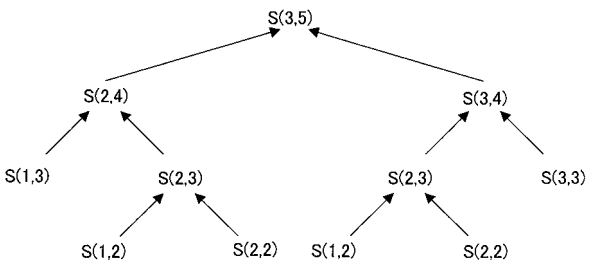
【図９】



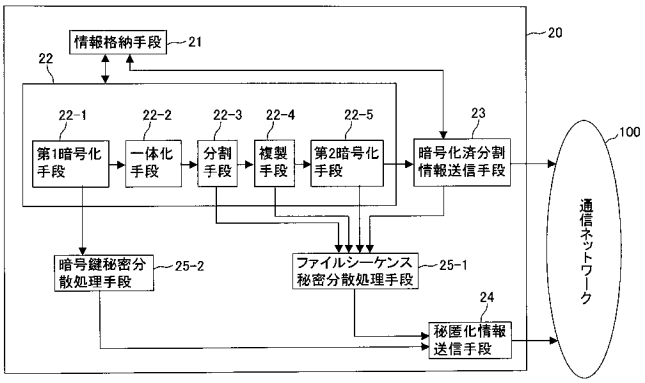
【図１０】



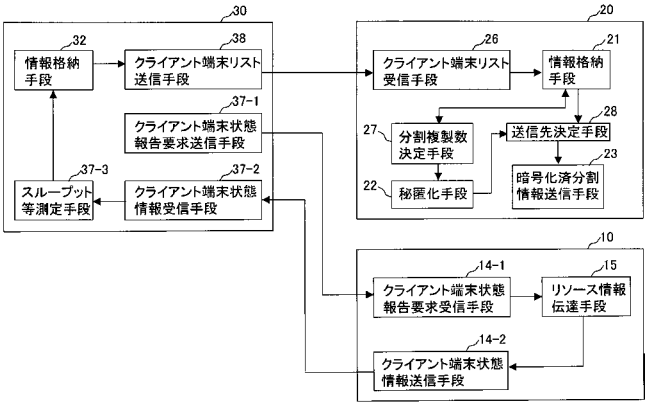
【図１１】



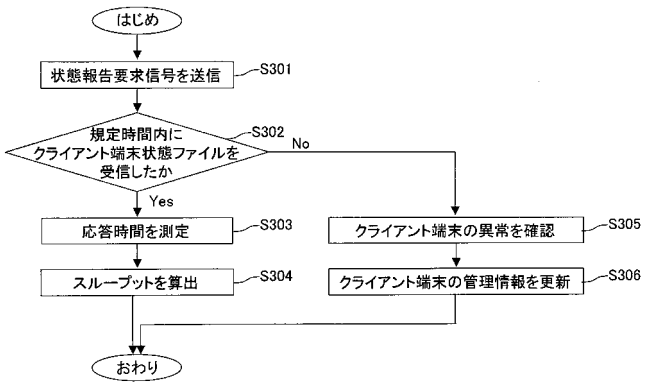
【図１２】



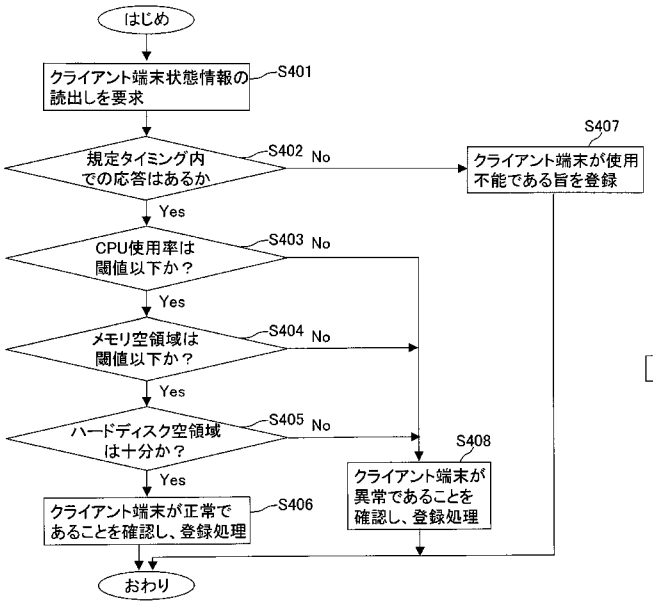
【図１３】



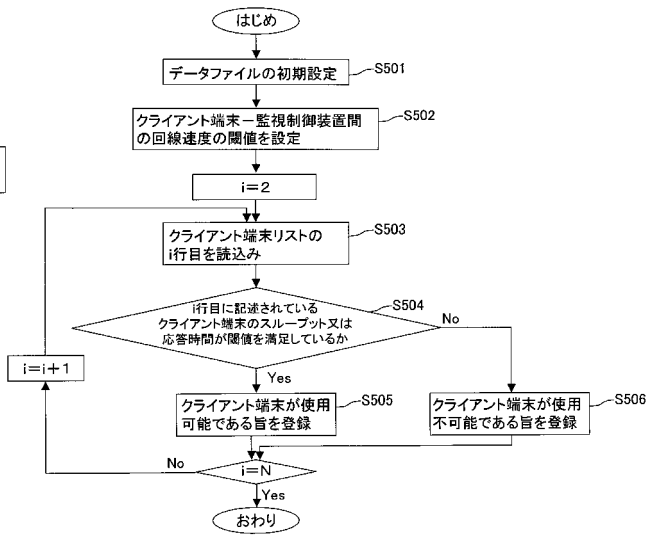
【図１４】



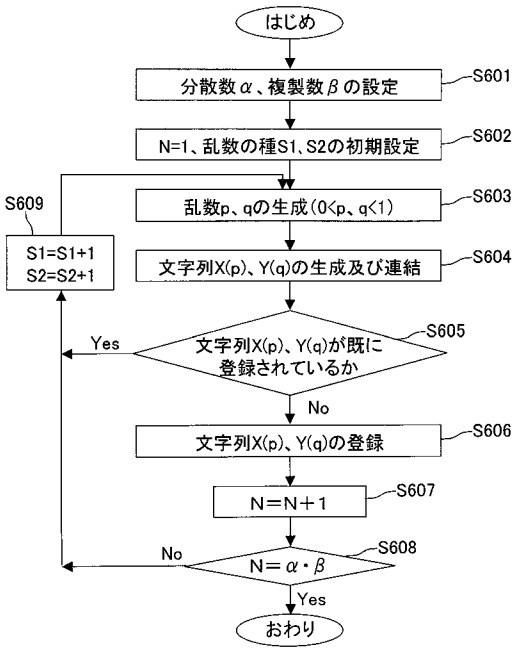
【図１５】



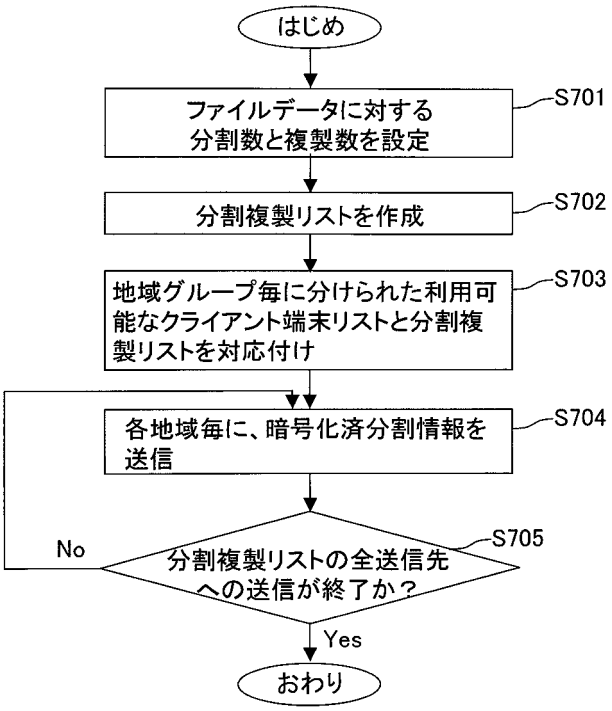
【図１６】



【図１７】



【図１８】



【手続補正書】
【提出日】平成21年7月24日(2009.7.24)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】請求項１
【補正方法】変更
【補正の内容】
【請求項１】
少なくとも１つのマスターサーバと、複数の監視制御装置と、複数のクライアント端末と、が通信ネットワークを介して互いに接続されたネットワークシステムにおいて、
前記マスターサーバは、
データファイルを第１の暗号鍵で暗号化し、暗号化した前記ファイルデータを複数の分割データに分割し、前記分割データを複製し、複製した前記分割データを第２の暗号鍵で暗号化して出力する秘匿化手段と、
前記秘匿化手段の出力する暗号化済分割情報を前記複数のクライアント端末に送信する暗号化済分割情報送信手段と、
前記第１の暗号鍵で暗号化した前記ファイルデータの分割から前記分割データを第２の暗号鍵で暗号化するまでの前記秘匿化手段の手順を記録したファイルシーケンス情報及び前記第１の暗号鍵をそれぞれ複製し、前記ファイルシーケンス情報と前記第１の暗号鍵が異なる監視制御装置に格納されるように、前記ファイルシーケンス情報及び前記第１の暗号鍵を前記複数の監視制御装置のうちの異なる監視制御装置に送信する秘匿化情報送信手段と、を備え、
前記複数のクライアント端末は、
前記暗号化済分割情報送信手段の送信する暗号化済分割情報を受信する暗号化済分割情報受信手段と、

前記暗号化済分割情報受信手段の受信する前記暗号化済分割情報を格納する暗号化済分割情報格納手段と、を備え、

前記複数の監視制御装置は、

前記秘匿化情報送信手段の送信する前記ファイルシーケンス情報又は前記第１の暗号鍵を受信する秘匿化情報受信手段と、

前記秘匿化情報受信手段の受信する前記ファイルシーケンス情報又は前記第１の暗号鍵を格納する秘匿化情報格納手段と、を備えることを特徴とするネットワークシステム。

フロントページの続き

(72)発明者　鈴木　秀一
東京都千代田区神田錦町２－２　学校法人東京電機大学内
(72)発明者　田窪　昭夫
東京都千代田区神田錦町２－２　学校法人東京電機大学内
(72)発明者　和田　雄次
東京都千代田区神田錦町２－２　学校法人東京電機大学内
(72)発明者　國分　建介
東京都千代田区神田錦町２－２　学校法人東京電機大学内

Ｆターム(参考) 5B017 AA03 BA07 BA10 CA16
5J104 AA16 AA32 AA41 EA04 EA18 JA03 NA02 NA27 NA37 PA14
5K030 GA15 JA10 KA02 LE01