

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4538585号
(P4538585)

(45) 発行日 平成22年9月8日(2010.9.8)

(24) 登録日 平成22年7月2日(2010.7.2)

(51) Int. Cl.	F I				
HO4L 9/08 (2006.01)	HO4L	9/00	GO1Z		
HO4L 9/14 (2006.01)	HO4L	9/00	641		
GO6F 21/24 (2006.01)	GO6F	12/14	510F		
HO4L 12/22 (2006.01)	GO6F	12/14	540A		
	HO4L	12/22			

請求項の数 4 (全 33 頁)

(21) 出願番号	特願2008-209152 (P2008-209152)	(73) 特許権者	800000068
(22) 出願日	平成20年8月15日 (2008.8.15)		学校法人東京電機大学
(65) 公開番号	特開2010-45670 (P2010-45670A)		東京都千代田区神田錦町2-2
(43) 公開日	平成22年2月25日 (2010.2.25)	(74) 代理人	100119677
審査請求日	平成21年1月23日 (2009.1.23)		弁理士 岡田 賢治
審判番号	不服2009-22022 (P2009-22022/J1)	(74) 代理人	100115794
審判請求日	平成21年11月11日 (2009.11.11)		弁理士 今下 勝博
早期審理対象出願		(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) 【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。

【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、

10

20

30

40

50

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 x_1, x_2, \dots, 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、 $F_p = Z / (p)$ 、 $(F_p)^* = \{x \in F_p \mid x \neq 0\}$ とする。

【0006】

次に、分散させる情報を作成する。ランダムに $a_1, a_2, \dots, a_{k-1} \in (F_p)^*$ を選ぶ。多項式

10

20

30

40

【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) 、 $(i = 1, 2, \dots, n)$ 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, \dots, 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。

10

【数 2】

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

20

【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 400 n 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

30

【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。

40

【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

50

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、

10

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。

20

【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。

30

【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、複数の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、

40

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る秘密情報分散し、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

50

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る秘密情報分散し、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

10

20

30

40

50

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。

【 0 0 1 9 】

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。

10

【発明の効果】

【 0 0 2 0 】

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る分散配備するので、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】

【 0 0 2 1 】

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 30 a、30 b、30 c と、複数のバックアップ装置 40 a、40 b、40 c 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 30 a、30 b、30 c 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。

20

30

【 0 0 2 2 】

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 30 a、30 b、30 c 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 30 a、30 b、30 c 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 40 a、40 b、40 c 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 40 a、40 b、40 c 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。

40

【 0 0 2 3 】

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 30 a 及び 30 b に送信する。例えば、第 1 の暗号鍵を監視制御装置 30 a に、ファイルシーケンス情報を監視制御装置 30 b 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。

【 0 0 2 4 】

50

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ふ必要があるため、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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

秘匿化手段 2 2 では、一体化手段 2 2 - 2 を省略している。一般には秘匿化手段 2 2 が一体化手段 2 2 - 2 を備えることが好ましいが、第 1 の暗号化手段 2 2 - 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 2 2 - 2 を省略してもよい。一体化手段 2 2 - 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 2 4 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 2 2 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。

【 0 0 3 8 】

秘匿化情報送信手段 2 4 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 2 2 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 2 2 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 2 2 - 3、複製手段 2 2 - 4、及び、第 2 の暗号化手段 2 2 - 5 のログである。

【 0 0 3 9 】

図 4 に示すクライアント端末 1 0 は、暗号化済分割情報受信手段 1 1 と、情報格納手段 1 2 と、生存確認情報送信手段 1 3 と、を備える。暗号化済分割情報受信手段 1 1 は、暗号化済分割情報送信手段 2 3 の送信する暗号化済分割情報を受信する。情報格納手段 1 2 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 1 1 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 1 3 は、クライアント端末 1 0 が稼働状態にあることを示す生存確認情報を、マスターサーバ 2 0 に送信する。

ここで、生存確認情報は、クライアント端末 1 0 が稼働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 3 0 a、3 0 b、3 0 c 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 1 0 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 1 0 へ通知した時には、宛先クライアント端末 1 0 は上記のアドレス情報を確認後に、予め、監視制御装置 3 0 a、3 0 b、3 0 c の中に登録されている、当該の宛先クライアント端末 1 0 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 1 0 が、正常に稼働している旨を監視制御装置 3 0 a、3 0 b、3 0 c 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 3 0 a、3 0 b、3 0 c 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。

【 0 0 4 0 】

図 5 に示す監視制御装置 3 0 は、情報格納手段 3 2 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 2 0 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 3 0 は、情報受信手段 3 1 と、情報格納手段 3 2 と、情報送信手段 3 3 と、を備える。

【 0 0 4 1 】

情報受信手段 3 1 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 2 4 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 1 3 の送信する生存確認情報を受信する。情報格納手段 3 2 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 3 1 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 3 2 の受信する生存確認情報を格納する。情報送信手段 3 3 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

10

20

30

40

50

報格納手段 3 2 の格納する秘匿化情報を、複数のバックアップ装置 4 0 に送信する機能である。

【 0 0 4 2 】

例えば、図 1 に示す監視制御装置 3 0 a であれば、情報受信手段 3 1、情報格納手段 3 2 及び情報送信手段 3 3 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 3 0 b であれば、情報受信手段 3 1、情報格納手段 3 2 及び情報送信手段 3 3 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 3 0 c であれば、情報受信手段 3 1、情報格納手段 3 2 及び情報送信手段 3 3 は、それぞれ、生存確認情報を、受信し、格納し、送信する。

【 0 0 4 3 】

図 6 に示すバックアップ装置 4 0 は、監視制御装置 3 0 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 3 0 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 3 0 a、3 0 b、3 0 c 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 4 0 は、バックアップ情報受信手段 4 1 - 1 及び 4 1 - 2 と、バックアップ情報格納手段 4 2 - 1 及び 4 2 - 2 と、を備える。

【 0 0 4 4 】

バックアップ情報受信手段 4 1 - 1 及び 4 1 - 2 は、それぞれ、複数の監視制御装置 3 0 a、3 0 b、3 0 c 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 4 2 - 1 及び 4 2 - 2 は、それぞれ、バックアップ情報受信手段 4 1 - 1 及び 4 1 - 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 4 1 - 1 及び 4 1 - 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 4 2 - 1 及び 4 2 - 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。

【 0 0 4 5 】

例えば、図 1 に示す監視制御装置 3 0 a であれば、バックアップ情報受信手段 4 1 - 1 及びバックアップ情報格納手段 4 2 - 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 4 1 - 2 及びバックアップ情報格納手段 4 2 - 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 3 0 b であれば、バックアップ情報受信手段 4 1 - 1 及びバックアップ情報格納手段 4 2 - 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 4 1 - 2 及びバックアップ情報格納手段 4 2 - 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 3 0 c であれば、バックアップ情報受信手段 4 1 - 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 4 1 - 2 及びバックアップ情報格納手段 4 2 - 2 は、それぞれ、生存確認情報を、受信し、格納する。

【 0 0 4 6 】

上述した構成例では、マスターサーバ 2 0 から送信された第 1 の暗号鍵は、まず、監視制御装置 3 0 a が受信し、監視制御装置 3 0 a 内の情報格納手段 3 2 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 4 0 a とバックアップ装置 4 0 b に送信する。監視制御装置 3 0 a 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 4 0 a は、その情報を基に、バックアップ情報格納手段 4 2 - 1 のデータベースを更新する。同様に、監視制御装置 3 0 a 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 4 0 b は、その情報を基に、バックアップ情報格納手段 4 2 - 1 のデータベースを更新する。

【 0 0 4 7 】

上述したデータベースの更新処理は、マスターサーバ 2 0 からファイルシーケンス情報を監視制御装置 3 0 b が受信した場合、及び、クライアント端末 1 0 からの生存確認情報を監視制御装置 3 0 c 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 3 0

10

20

30

40

50

a、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

10

20

30

40

50

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るバックアップ装置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。

10

【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クエ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クエ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。

20

【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からファイルシークエ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。

30

【0055】

上記一連の処理の結果、第1の暗号鍵、ファイルシークエンス情報、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

40

50

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。

【 0 0 5 6 】

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 個の情報があれば、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 40 a、40 b、40 c の総数と考えてよい。

【 0 0 5 7 】

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。

【 0 0 5 8 】

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, \dots, 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。

【 0 0 5 9 】

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, \dots, 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

10

20

30

40

50

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 d_0 、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 d_1 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、 $(1, 1, \dots, 1)$ 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】

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

10

20

30

40

50

【 0 0 6 5 】

ステップ S 2 0 6 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 】

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

【 0 0 6 6 】

ステップ S 2 0 7 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 】

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

【 0 0 6 7 】

ステップ S 2 0 8 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 1 0 】

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

【 0 0 6 8 】

ステップ S 2 0 9 では、ステップ S 2 0 4 で得た $d0$ の下に、ステップ S 2 0 6 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 1 1 】

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

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

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。

10

20

30

40

【数 1 2】

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

【 0 0 6 9】

上記のステップ S 2 0 5 からステップ S 2 0 9 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。

10

【 0 0 7 0】

図 1 1 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 d_0 と、完全置換系の表 $S(k, n - 1, d)$ から得られる行列 d_1 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。

20

【 0 0 7 1】

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 2 0 0 桁のとき分散が 2 0 0 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 1 6 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。 $n = 2 0$ 程度が実用的には限界と考えられる。

30

【 0 0 7 2】

(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 3 0 a、3 0 b、3 0 c を複数の異なる地域に設置して、かつ、マスターサーバ 2 0 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、一つもしくは複数の組み合わせた監視制御装置 3 0 a、3 0 b、3 0 c に転送することにより、監視制御装置 3 0 a、3 0 b、3 0 c 自体を、閾値秘密分散配備することを特徴とする。

40

【 0 0 7 3】

マスターサーバ 2 0 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 3 0 a、3 0 b、3 0 c に送信する。クライアント端末 1 0 から送信される生存確認情報は、監視制御装置 3 0 c にのみ送られ、監視制御装置 3 0 c は受信した生存確認情報を監視制御装置 3 0 a と監視制御装置 3 0 b 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。

【 0 0 7 4】

図 1 2 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

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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。

20

【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情報を持ち、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。

30

【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。

40

【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

50

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, \dots, 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するための、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、 \dots 、#N（100 未満）に分け、各々の地域の識別用に 2 桁の整数（01、02、 \dots 、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

10

20

30

40

50

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こと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、第2は複製数、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、・・・、) の中からランダムに選択される。乱数 q は、要素 (1、2、3、・・・、) 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、

10

20

30

40

50

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。

10

【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報が回収、復元できる。

20

【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。

30

40

【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

50

に配布される。

【 0 0 9 8 】

ここで、地域番号 0 2、0 3 及び 0 4 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 0 1 では、分割複製データ 0 3 0 2、0 2 0 3、0 4 0 2 が格納される。また、地域番号 0 4 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 0 4 0 0 2、0 4 0 0 1 の 2 台が存在するため、最初の分割複製データ 0 1 0 3 は 4 番目の順でクライアント端末 0 4 0 0 2 へ転送され、その次に、同じ地域番号 0 4 に転送された分割複製データ 0 3 0 3 は、8 番目の順で、クライアント端末 0 4 0 0 1 へ転送される。さらに、その次に同じ地域番号 0 4 に転送された分割複製データ 0 3 0 1 は、1 2 番目の順で、クライアント端末 0 4 0 0 2 へ転送される。また、地域番号 0 2 には、利用可能な端末がクライアント端末 0 2 0 0 1 の 1 台しかないので、分割複製データ 0 4 0 3、0 1 0 1、0 2 0 2 が、それぞれ、2 番目、6 番目、1 0 番目に分散転送される。

10

【 0 0 9 9 】

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、重みづ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、地域毎の分散転送の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 () = 4 0 0 で、地域数が 1 0 の場合には各地域毎に 4 0 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。

20

【 0 1 0 0 】

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 1 8 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。

30

【 0 1 0 1 】

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。

【 0 1 0 2 】

図 1 4 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 S 3 0 1 では、クライアント端末状態報告要求送信手段 3 7 - 1 が、各クライアント端末 1 0 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 1 5 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 1 0 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。

40

ステップ S 3 0 2 では、スループット等測定手段 3 7 - 3 が、規定時間以内にクライアント端末状態送信手段 1 4 - 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 3 7 - 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 1 4 - 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 S 3 0 3 に移行する。一方、スループット等測定手段 3 7 - 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 1 4 - 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

50

た場合、ステップS 3 0 5に移行する。

【 0 1 0 3 】

ステップS 3 0 3では、スループット等測定手段3 7 - 3が、ステップS 3 0 1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1 4 - 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S 3 0 4では、スループット等測定手段3 7 - 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3 7 - 3が送出した測定用データ量が X (b i t) 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) (b i t / 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3 7 - 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3 2に格納する。

ステップS 3 0 5では、スループット等測定手段3 7 - 3が、クライアント端末状態情報送信手段1 4 - 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1 0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1 4 - 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S 3 0 6では、情報格納手段3 2に、クライアント端末1 0が使用「不能」である旨を登録する。ステップS 3 0 5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1 0の「正常」、「不能」又は「異常」を確認してもよい。

【 0 1 0 4 】

図1 5は、スループット等測定手段3 7 - 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S 4 0 1では、クライアント端末状態報告要求送信手段3 7 - 1が、クライアント端末状態報告要求受信手段1 4 - 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S 4 0 2では、スループット等測定手段3 7 - 3が、クライアント端末状態報告要求受信手段1 4 - 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S 4 0 3へ移行し、応答がなければステップS 4 0 7へ移行する。

ステップS 4 0 7では、スループット等測定手段3 7 - 3が、ステップS 4 0 2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1 0が使用「不能」と決定し、その旨を当該IDに対して登録する。

【 0 1 0 5 】

ステップS 4 0 3では、スループット等測定手段3 7 - 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1 0が高いCPU使用率のもとで、マスターサーバ2 0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2 0 %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1 0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2 0 %を設定する。

ステップS 4 0 4では、スループット等測定手段3 7 - 3が、クライアント端末1 0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1 0が少ない空きメモリ領域のもとで、マスターサーバ2 0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2 G Bのメモリを持つクライアント端末1 0が、空きメモリ領域として全体の5 0 %である1 G Bをもっている場合には、メモリ空き領域が1 G B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1 0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1 G B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）を含めたりリストを作成する。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 ($p < 1$)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 および複製数を設定する。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。

【 0 1 1 4 】

ステップS 6 0 5では、新しく生成されたX (p) 及びY (q) が、既に生成されている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S 6 0 5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S 6 0 9に移行し、登録されていなければステップS 6 0 6に移行する。

ステップS 6 0 6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2 1又は送信先決定手段2 8に、文字列X (p) 及び文字列Y (q) を格納する。

10

ステップS 6 0 7では、登録の組み合わせ総数Nのカウンタアップを行う。ステップS 6 0 8では、登録の組み合わせ総数Nが必要数 (・) に達しているかどうかの判断を行う。

ステップS 6 0 9では、新たな乱数p、qを生成するために必要な、乱数の種S 1及びS 2の数値のカウンタアップを行う。

【 0 1 1 5 】

図1 8は、本実施形態に係る送信先決定手段2 8及び暗号化済分割情報送信手段2 3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S 7 0 1では、分割複製数決定手段2 7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2 1から読み出し、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S 7 0 2では、秘匿化手段2 2がデータファイルを秘匿化し、その後で、送信先決定手段2 8が、どの分散されたクライアント端末1 0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。

20

【 0 1 1 6 】

ステップS 7 0 3では、送信先決定手段2 8が、監視センタ3 0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2 1から取得する。情報格納手段2 1には、各クライアント端末1 0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。

30

ステップS 7 0 4では、暗号化済分割情報送信手段2 3が、ステップS 7 0 3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S 7 0 5では、暗号化済分割情報送信手段2 3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1 0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S 7 0 4に移行し、再度ステップS 7 0 4及びステップS 7 0 5を繰り返す。一方、ステップS 7 0 5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 】

【 0 1 1 7 】

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。

40

【 図面の簡単な説明 】

【 0 1 1 8 】

50

【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。

10

【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。

20

【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

30

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

40

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

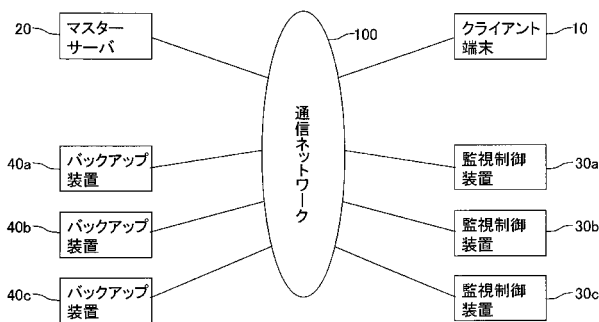
32 情報格納手段

33 情報送信手段

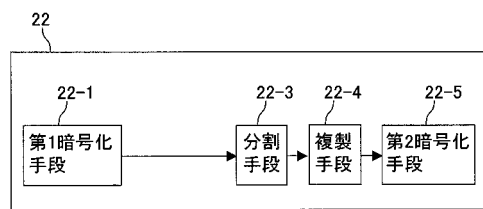
50

- 3 4 秘密分散処理手段
- 3 7 - 1 クライアント端末状態報告要求送信手段
- 3 7 - 2 クライアント端末状態情報受信手段
- 3 7 - 3 スループット等測定手段
- 3 8 クライアント端末リスト送信手段
- 4 0、4 0 a、4 0 b、4 0 c バックアップ装置
- 4 1 - 1、4 1 - 2、4 1 - 3 バックアップ情報受信手段
- 4 2 - 1、4 2 - 2、4 2 - 3 バックアップ情報格納手段
- 1 0 0 通信ネットワーク

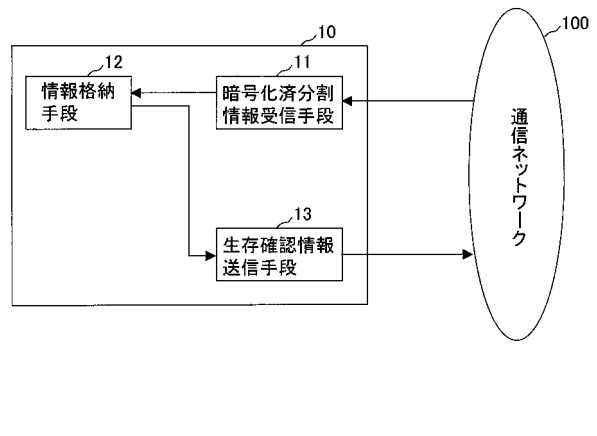
【図 1】



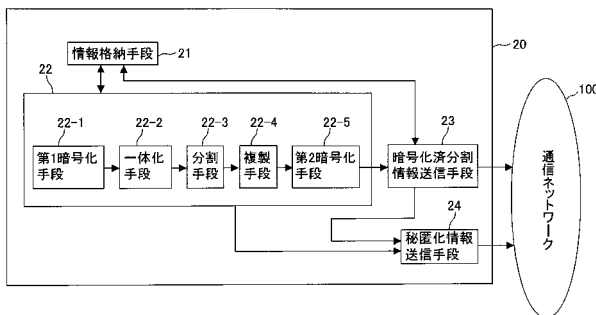
【図 3】



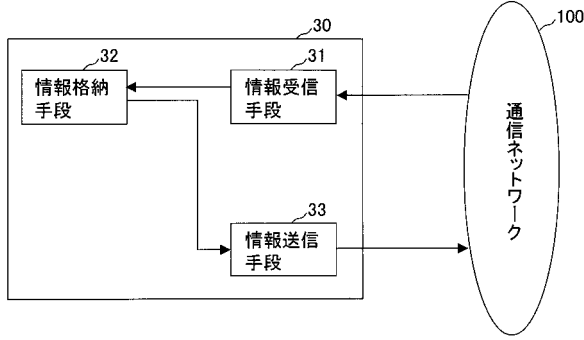
【図 4】



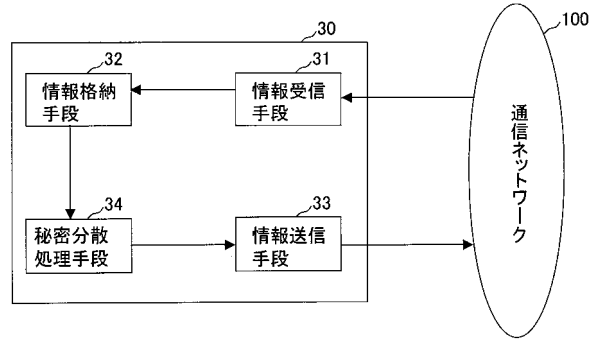
【図 2】



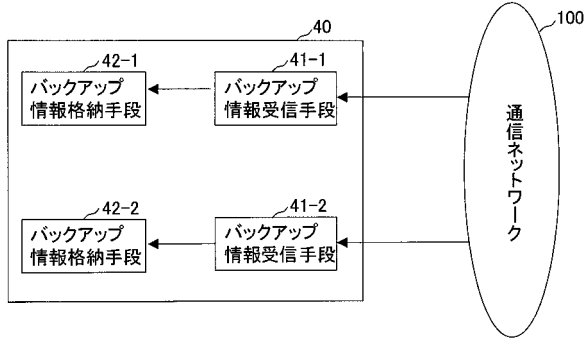
【図5】



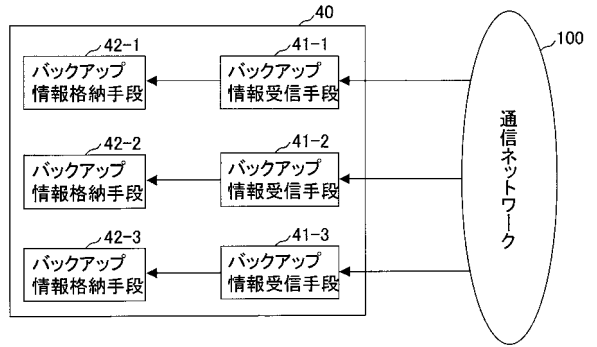
【図7】



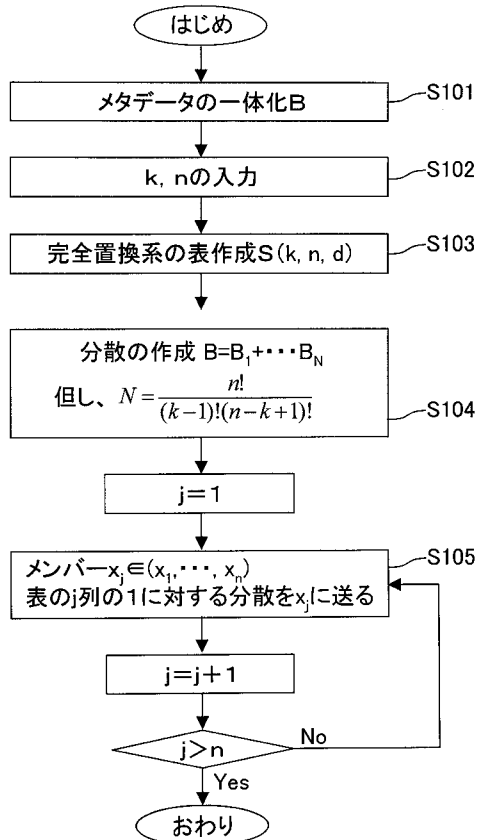
【図6】



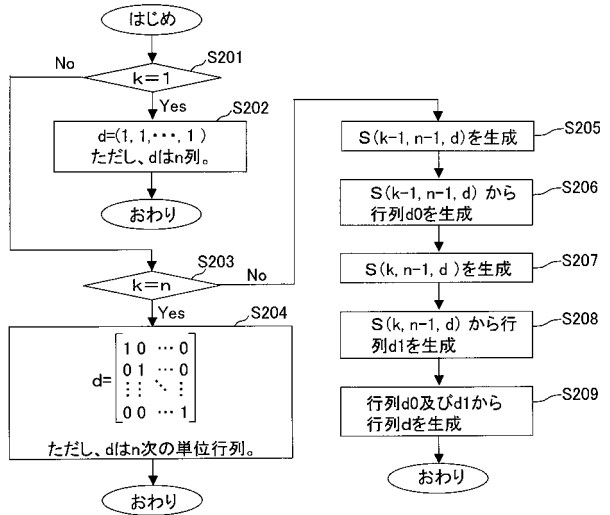
【図8】



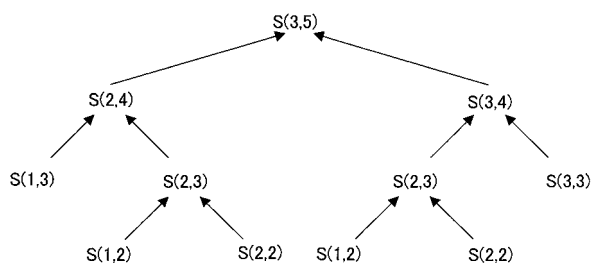
【図9】



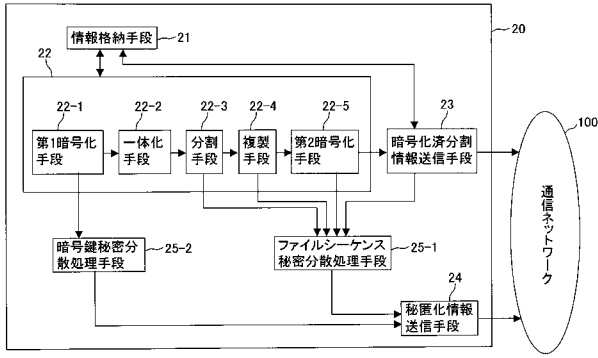
【図10】



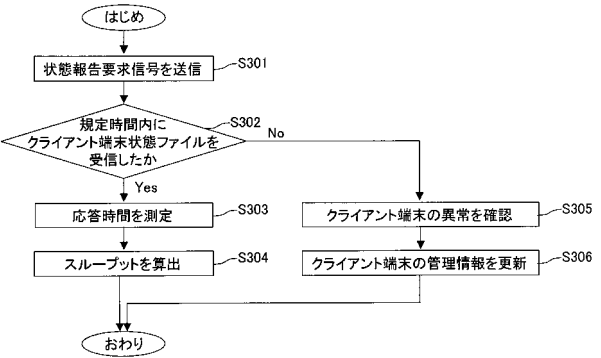
【図11】



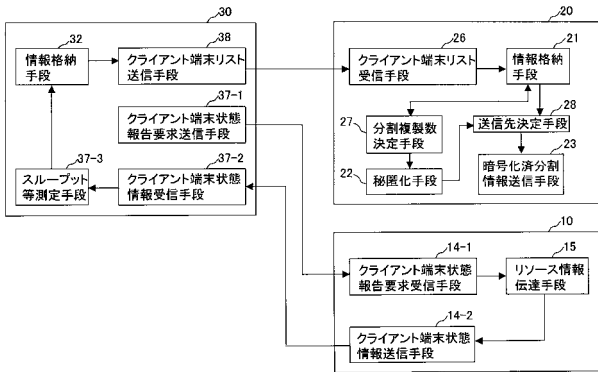
【図12】



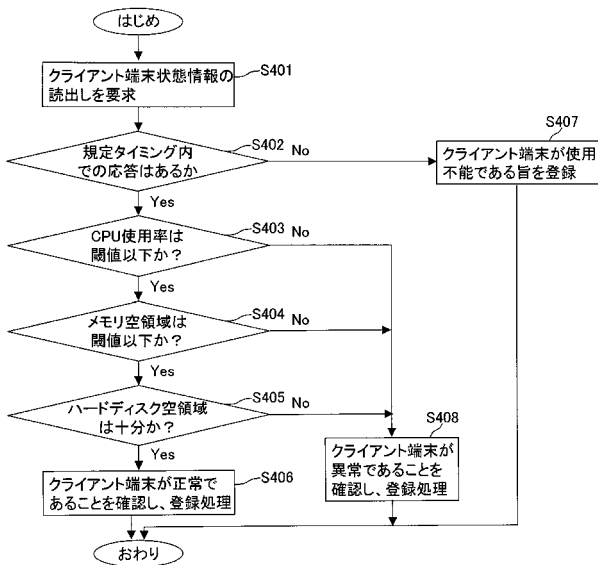
【図14】



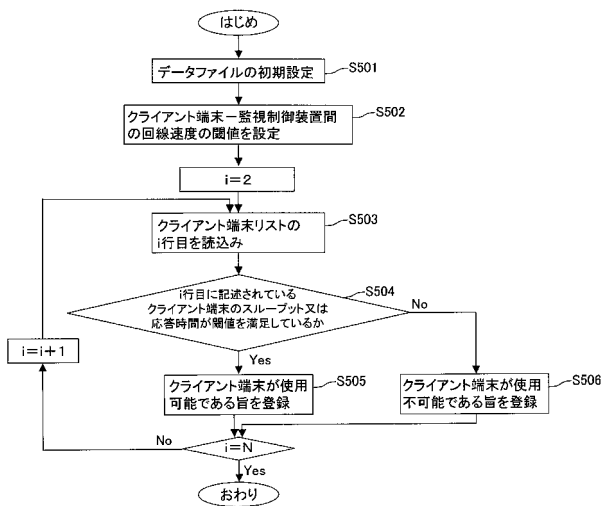
【図13】



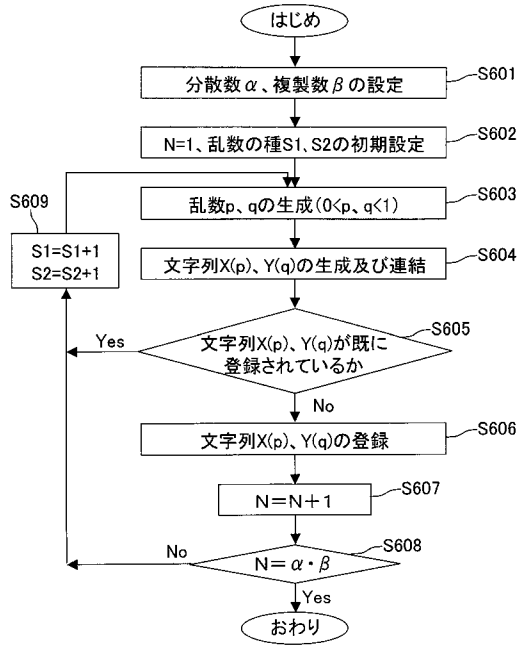
【図15】



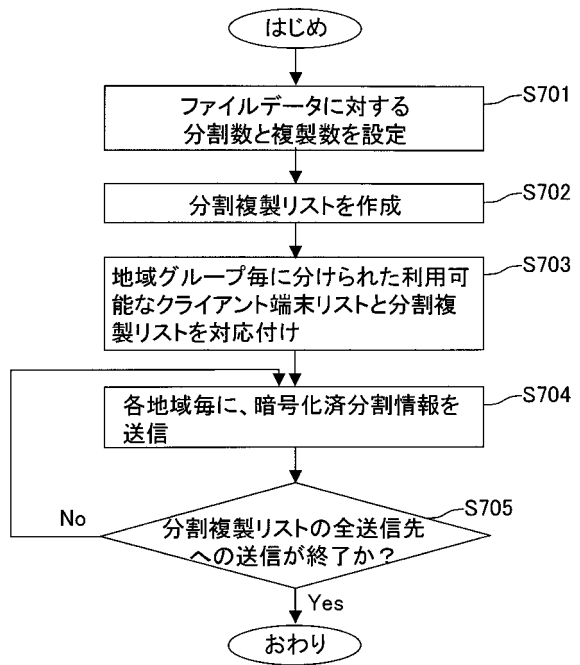
【図16】



【図17】



【図18】



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

合議体

- 審判長 吉岡 浩
審判官 宮司 卓佳
審判官 石井 茂和

(56)参考文献 特開 2007 - 102672 号公報

- 國分建介, 岩本太一, 上野洋一郎, 鈴木秀一, 宮保憲治, 柴田良一, “グリッドコンピューティングを適用したディザスタ・リカバリ・システムの一検討”, 2007年電子情報通信学会総合大会講演論文集, 日本, 社団法人電子情報通信学会, 2007年3月7日, 通信2, p. 283
- 鈴木秀一, “World Wide master key systemにおける秘密情報分散”, 情報処理学会研究報告, 日本, 社団法人情報処理学会, 2002年7月19日, Vol. 2002, No. 68, p. 221 - 224, 2002 - CSEC - 18
- 國分建介, 河合寿洋, 上野洋一郎, 鈴木秀一, 宮保憲治, “グリッド・コンピューティングを適用したディザスタ・リカバリ・システムの一検討”, 2007年電子情報通信学会ソサイエティ大会講演論文集, 日本, 社団法人電子情報通信学会, 2007年 8月29日, 通信2, BS - 5 - 10, p. S - 55 ~ S - 56
- 伊藤義仁, 磯野正雄, 伊藤正晴, 柴田良一, 牧野侑祐, 岩西愛, 宮保憲治, 國分健介, 上野洋一郎, 岩本太一, 和田雄次, 高橋遼平, 鈴木秀一, 山田裕一, 山田慶行, 田窪昭夫, 川口豊, “暗号技術とデータグリッドを活用した災害時データバックアップシステムの実用化に関する研究”, ソフトピアジャパン共同研究報告, 2007年, Vol. 11, p. 4 - 1 ~ 4 - 28
- 國分建介, 河合洋寿, 上野洋一郎, 鈴木秀一, 宮保憲治, “グリッドコンピューティングを適用したディザスタ・リカバリ・システムの性能評価”, 電子情報通信学会技術研究報告, 日本, 社団法人電子情報通信学会, 2007年12月13日, Vol. 107, No. 403, p. 1 - 6, NS2007 - 106 ~ 118, ネットワークシステム

(58)調査した分野(Int.Cl., DB名)

H04L9/00, G06F21/24