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

特許第4296304号
(P4296304)

(45)発行日　平成21年7月15日(2009.7.15)　(24)登録日　平成21年4月24日(2009.4.24)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	510F
G06F 12/00	(2006.01)	G06F	12/14	540B
G09C 1/00	(2006.01)	G06F	12/00	531M
H04L 9/08	(2006.01)	G06F	12/00	537H
H04L 9/14	(2006.01)	G06F	12/00	545A

請求項の数 9　(全 35 頁)　最終頁に続く

(21)出願番号　特願2008-507405 (P2008-507405)
(86)(22)出願日　平成19年3月6日(2007.3.6)
(86)国際出願番号　PCT/JP2007/054234
(87)国際公開番号　WO2007/111086
(87)国際公開日　平成19年10月4日(2007.10.4)
審査請求日　平成21年1月23日(2009.1.23)
(31)優先権主張番号　特願2006-88020 (P2006-88020)
(32)優先日　平成18年3月28日(2006.3.28)
(33)優先権主張国　日本国(JP)

早期審査対象出願

(73)特許権者　800000068
学校法人東京電機大学
東京都千代田区神田錦町２－２
(73)特許権者　504237050
独立行政法人国立高等専門学校機構
東京都八王子市東浅川町７０１番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　宮保　憲治
東京都千代田区神田錦町２丁目２番地
学校法人東京電機大学内

最終頁に続く

(54)【発明の名称】ディザスタリカバリ装置及びディザスタリカバリプログラム及びその記録媒体及びディザスタリカバリシステム

(57)【特許請求の範囲】

【請求項１】

１つまたは複数のデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化し、一体化した前記データファイルを複数の分割データに分割し、前記分割データごとに異なる暗号鍵を用いて暗号化し、暗号化した前記分割データを、分散配置された複数のクライアント端末のうち決定したクライアント端末に通信ネットワークを介して記憶させ、前記暗号化、前記一体化、前記分割及び前記記憶の時系列情報を前記クライアント端末と通信ネットワークで接続されている管理端末へ送信することを特徴とするディザスタリカバリ装置。

【請求項２】

分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置であって、

前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手段と、

前記マスターサーバの記憶するデータファイルを暗号化するデータファイル暗号化かつ一体化手段と、

前記データファイル暗号化かつ一体化手段の暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、

前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異な

る暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手段と、
前記分割データを送信するクライアント端末を前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末から決定し、前記分割データ暗号化手段の出力する前記暗号化データを、決定した前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手段と、
前記データファイル暗号化かつ一体化手段、前記分割データ暗号化手段及び前記暗号化データ送信手段の時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手段の暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手段の暗号化した前記暗号鍵及び時系列情報並びに前記暗号化データ送信手段の送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手段と、
を有することを特徴とするディザスタリカバリ装置。
【請求項３】
分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置であって、
前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手段と、
前記マスターサーバの記憶するデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化するデータファイル暗号化かつ一体化手段と、
前記データファイル暗号化かつ一体化手段の暗号化して一体化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、
前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手段と、
前記分割データを送信するクライアント端末を前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末から決定し、前記分割データ暗号化手段の出力する前記暗号化データを、決定した前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手段と、
前記データファイル暗号化かつ一体化手段、前記分割データ暗号化手段及び前記暗号化データ送信手段の時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手段の暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手段の暗号化した前記暗号鍵及び時系列情報並びに前記暗号化データ送信手段の送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手段と、
を有することを特徴とするディザスタリカバリ装置。
【請求項６】
前記クライアント端末のそれぞれに記憶されている前記暗号化データを読み出し、前記クライアント端末識別情報の異なる前記クライアント端末に記憶されている前記暗号化データと交換し、交換後の前記暗号化データを、前記クライアント端末のそれぞれに記憶させる暗号化データ交換手段をさらに有することを特徴とする請求項１、２又は３に記載のディザスタリカバリ装置。
【請求項９】
分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置を実現するためのディザスタリカバリプログラムであって、
前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手順と、

前記マスターサーバの記憶するデータファイルを暗号化するデータファイル暗号化かつ一体化手順と、
前記データファイル暗号化かつ一体化手順で暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手順と、
前記データファイル分割手順で出力した前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手順と、
前記分割データを送信するクライアント端末を前記識別情報受信手順で受信した前記クライアント端末識別情報の前記クライアント端末から決定し、前記分割データ暗号化手順で出力した前記暗号化データを、決定した前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手順と、
前記データファイル暗号化かつ一体化手順、前記分割データ暗号化手順及び前記暗号化データ送信手順における時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手順で暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手順で暗号化した前記暗号鍵及び時系列情報並びに前記分割データ送信手順で送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手順と、
を前記ディザスタリカバリ装置に実行させるためのディザスタリカバリプログラム。
【請求項１０】
分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置を実現するためのディザスタリカバリプログラムであって、
前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手順と、
前記マスターサーバの記憶するデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化するデータファイル暗号化かつ一体化手順と、
前記データファイル暗号化かつ一体化手順で暗号化して一体化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手順と、
前記データファイル分割手順で出力した前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手順と、
前記分割データを送信するクライアント端末を前記識別情報受信手順で受信した前記クライアント端末識別情報の前記クライアント端末から決定し、前記分割データ暗号化手順で出力した前記暗号化データを、決定した前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手順と、
前記データファイル暗号化かつ一体化手順、前記分割データ暗号化手順及び前記暗号化データ送信手順における時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手順で暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手順で暗号化した前記暗号鍵及び時系列情報並びに前記分割データ送信手順で送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手順と、
を前記ディザスタリカバリ装置に実行させるためのディザスタリカバリプログラム。
【請求項１３】
前記クライアント端末のそれぞれに記憶されている前記暗号化データを読み出し、前記クライアント端末識別情報の異なる前記クライアント端末に記憶されている前記暗号化データと交換し、交換後の前記暗号化データを、前記クライアント端末のそれぞれに記憶させる暗号化データ交換手順を、前記暗号化データ送信手順の後に前記ディザスタリカバリ

装置にさらに実行させることを特徴とする請求項９又は１０に記載のディザスタリカバリプログラム。
【請求項１６】
請求項９、１０又は１３に記載のディザスタリカバリプログラムを格納した読み取り可能な記録媒体。
【請求項１７】
マスターサーバと、前記マスターサーバから分散設置されている複数のクライアント端末とが互いに通信ネットワークで接続されているディザスタリカバリシステムであって、
前記クライアント端末は、
遊休状態であることを判定し、遊休状態であるとの判定を契機に、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、前記マスターサーバへ送信する識別情報送信手段と、
前記マスターサーバの送信する前記暗号化データを受信する暗号化データ受信手段と、
前記暗号化データ受信手段の受信する暗号化データを記憶する暗号化データ記憶手段と、
前記マスターサーバは、
データファイルを記憶するデータファイル記憶手段と、
前記識別情報送信手段の送信する前記クライアント端末識別情報を受信する識別情報受信手段と、
前記データファイル記憶手段の記憶する前記データファイルを暗号化するデータファイル暗号化かつ一体化手段と、
前記データファイル暗号化かつ一体化手段の暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、
前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した前記暗号化データを出力する分割データ暗号化手段と、
前記分割データを送信するクライアント端末を前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末から決定し、前記分割データ暗号化手段の出力する前記暗号化データを、決定した前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手段と、
前記データファイル暗号化かつ一体化手段、前記分割データ暗号化手段及び前記暗号化データ送信手段の時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手段の暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手段の暗号化した前記暗号鍵及び時系列情報並びに前記暗号化データ送信手段の送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手段と、
を有することを特徴とするディザスタリカバリシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信ネットワークに接続されたマスターサーバが記憶している情報を、当該のコンピュータセンターが万が一の災害時にも、遠隔地に分散設置されている複数のコンピュータ端末へバックアップを行うディザスタリカバリ装置と、ディザスタリカバリ装置を実現するためのプログラムと、当該プログラムを記録したコンピュータ読み取り可能な記録媒体と、ディザスタリカバリシステムに関する。
【背景技術】
【０００２】
現在、あらゆる情報がデータベース化されている。地方自治体や病院等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構築又は提案されている。例えば、主／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システムがある（例えば、特許文献１参照。）。
【０００４】
一方、住民の個人情報や医療情報といった秘匿性の高いデータファイルを送受信するためには、盗聴の防止が不可欠となる。盗聴を防止する技術としては、例えば暗号化技術がある。暗号化技術には、ブロック暗号化技術とストリーム暗号化技術が存在する。前者はデータを一塊にしてある塊毎にそれを符号化処理するものであり、後者はデータが１つ到着する度にそれを処理する点がメカニズム上の違いである。一般に前者は暗号化・復号化に時間を要するが、後者は暗号化・復号化の速度が速いという特質を有する。
【特許文献１】特開２００６－６７４１２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかし、従来のバックアップシステムでは、主／副の２つのサイトでの１対１の暗号化通信を前提としていた。このため、両方のサイトが被災した場合には、データファイルの復旧は不可能であった。又、バックアップの途中で災害が発生した場合は、データファイルの一部しか復元ができないので、データファイルを復旧することはできなかった。又、盗聴された場合に、データファイルが復元される危険があった。
【０００６】
そこで本発明は、マスターサーバと通信ネットワークで接続され、かつ、分散設置されている複数のクライアント端末へ、マスターサーバのデータファイルのバックアップを行うことで、マスターサーバの災害時におけるデータファイルの復旧を可能とすることを目的とする。
【課題を解決するための手段】
【０００７】
本発明は、マスターサーバの記憶するデータファイルを、分散配置されている遊休状態にあるクライアント端末に、グリッドコンピューティングによる分散化技術を用いて記憶させることでバックアップを行う。クライアント端末に記憶させる際に、データファイルの秘匿化のために、データファイルを暗号化したものを分割して断片化し、さらに断片化したものをそれぞれ異なる暗号鍵を用いて暗号化し、暗号化データのそれぞれを異なるクライアント端末へ送信する。これにより、クライアント端末に記憶させる際に暗号化データが漏洩した場合であっても、データファイルの復元を不可能にすることができる。
【０００８】
具体的には、本発明に係るディザスタリカバリ装置は、１つまたは複数のデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化し、一体化した前記データファイルを複数の分割データに分割し、前記分割データごとに異なる暗号鍵を用いて暗号化し、暗号化した前記分割データを、分散配置された複数のクライアント端末に通信ネットワークを介して記憶させることを特徴とする。
【０００９】
具体的には、本発明に係るディザスタリカバリ装置は、分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置であって、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手段と、前記マスターサーバの記憶するデータファイルを暗号化するデータファイル暗号化かつ一体化手段と、前記データファイル暗号化かつ一体化手段の暗号化した暗号

化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手段と、前記分割データ暗号化手段の出力する前記暗号化データを、前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手段と、を有することを特徴とする。

【００１０】

又、本発明に係るディザスタリカバリ装置は、分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置であって、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手段と、前記マスターサーバの記憶するデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化するデータファイル暗号化かつ一体化手段と、前記データファイル暗号化かつ一体化手段の暗号化して一体化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手段と、前記分割データを送信する前記クライアント端末を秘匿された方法で決定し、前記分割データ暗号化手段の出力する前記暗号化データを、前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手段と、を有することを特徴とする。

【００１１】

ディザスタリカバリ装置が、データファイル暗号化かつ一体化手段、データファイル分割手段、分割データ暗号化手段及び暗号化データ送信手段を有するので、分散設置されている複数のクライアント端末のうちの遊休状態にある複数のクライアント端末に、分割及び暗号化を施した暗号化データのバックアップを行うことができる。これにより、マスターサーバのある地域に災害が発生し、マスターサーバのデータファイルが使用不可能となった場合であっても、分散設置されているクライアント端末の記憶する暗号化データを基にデータファイルを復旧することができる。

【００１２】

ここで、データファイル暗号化かつ一体化手段によってランダムな状態になっているデータファイルを分割し、さらに分割データごとに異なる暗号鍵を用いて暗号化する。これにより、分割した順番を正確に再現できなければデータファイルの解読をすることが不可能になる。更に乱数と区別できない平文を乱数と区別できない暗号文に暗号化するので、解読される可能性を極めて低くすることができる。これにより、高速なストリーム暗号を用い、安全にかつ効率的にデータファイルをクライアント端末に分散させることができる。よって、ネットワークを活用して、災害が発生した場合であっても、安全にかつ効率的にデータファイルを復旧することができる。

【００１３】

本発明に係るディザスタリカバリ装置では、前記クライアント端末に動作をさせる暗号鍵更新命令と共に新たな暗号鍵を前記クライアント端末へ送信する暗号鍵送信手段をさらに有し、前記暗号鍵更新命令は、前記クライアント端末に、当該暗号鍵を用いて当該クライアント端末の記憶する前記暗号化データを暗号化させ、当該クライアント端末の記憶する前記暗号化データを更新させることが好ましい。クライアント端末に格納されている時間の経過に伴い、暗号化データの盗聴される危険性が増す。しかし、クライアント端末にバックアップされている暗号化データをさらに暗号化し、暗号鍵を更新することで、この危険性を回避することができる。

【００１４】

本発明に係るディザスタリカバリ装置では、前記暗号化データ送信手段は、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）装置を介して前記通信ネットワークと接続されており、前記ＶＰＮ装置は、前記暗号化データ送信手段の送信した前記暗号化データを更に暗号化して前記クライアント端末へ送信することが好ましい。ＶＰＮに用いられる暗号化技術によって、暗号化データをさらに暗号化することができる。これにより、情報の安全性及び秘匿性を向上することができる。

【００１５】

本発明に係るディザスタリカバリ装置では、前記クライアント端末のそれぞれに記憶されている前記暗号化データを読み出し、前記クライアント端末識別情報の異なる前記クライアント端末に記憶されている前記暗号化データと交換し、交換後の前記暗号化データを、前記クライアント端末のそれぞれに記憶させる暗号化データ交換手段をさらに有することが好ましい。クライアント端末の記憶する暗号化データを交換して変更するので、もともとのデータファイルの復元は、これら分割及び暗号化に加え、さらに交換を含む一連のシーケンスを知っているものでなければ不可能とすることができる。これにより、盗聴によってデータファイルを復元可能なまでに暗号化データを収集することを困難にすることができる。

【００１６】

本発明に係るディザスタリカバリ装置では、前記データファイル暗号化かつ一体化手段、前記分割データ暗号化手段及び前記暗号化データ送信手段の時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手段の暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手段の暗号化した前記暗号鍵及び時系列情報並びに前記暗号化データ送信手段の送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手段をさらに有することが好ましい。時系列情報送信手段が分割データ暗号化手段及び暗号化データ送信手段の時系列情報を管理端末に送信するので、マスターサーバが破壊された場合であっても、管理端末がデータファイルの復旧をすることができる。

【００１７】

本発明に係るディザスタリカバリ装置では、前記管理端末が複数であり、前記時系列情報送信手段は、複数の前記管理端末のそれぞれに前記暗号鍵及び前記クライアント端末識別情報並びにこれらの時系列情報を送信することが好ましい。管理端末を冗長配備することで、複数の管理端末にてデータファイルの復旧が可能となる。これにより、安全性を一層向上させるとともに、迅速なデータファイルの復旧が可能となる。

【００１８】

本発明に係るディザスタリカバリプログラムは、分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接続されるディザスタリカバリ装置を実現するためのディザスタリカバリプログラムであって、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手順と、前記マスターサーバの記憶するデータファイルを暗号化するデータファイル暗号化かつ一体化手順と、前記データファイル暗号化かつ一体化手順で暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手順と、前記データファイル分割手順で出力した前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手順と、前記分割データ暗号化手順で出力した前記暗号化データを、前記識別情報受信手順で受信した前記クライアント端末識別情報の前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手順と、を前記ディザスタリカバリ装置に実行させることを特徴とする。

【００１９】

又、本発明に係るディザスタリカバリプログラムは、分散設置されている複数のクライアント端末とマスターサーバとが通信ネットワークで接続され、前記マスターサーバに接

続されるディザスタリカバリ装置を実現するためのディザスタリカバリプログラムであって、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、遊休状態にある前記クライアント端末から受信する識別情報受信手順と、前記マスターサーバの記憶するデータファイルを暗号化し、暗号化した前記データファイルを複数のデータピースに分割して前記データピース同士を可逆演算することで一体化するデータファイル暗号化かつ一体化手順と、前記データファイル暗号化かつ一体化手順で暗号化して一体化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手順と、前記データファイル分割手順で出力した前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した暗号化データを出力する分割データ暗号化手順と、前記分割データを送信する前記クライアント端末を秘匿された方法で決定し、前記分割データ暗号化手順で出力した前記暗号化データを、前記識別情報受信手順で受信した前記クライアント端末識別情報の前記クライアント端末へ送信し、前記クライアント端末に記憶させる暗号化データ送信手順と、を前記ディザスタリカバリ装置に実行させることを特徴とする。

【００２０】

ディザスタリカバリプログラムが、データファイル暗号化かつ一体化手順、データファイル分割手順、分割データ暗号化手順及び分割データ送信手順を実行させるので、分散設置されている複数のクライアント端末のうちの遊休状態にある複数のクライアント端末に、分割及び暗号化を施した暗号化データのバックアップをすることができる。これにより、マスターサーバのある地域に災害が発生し、マスターサーバのデータファイルが使用不可能となった場合であっても、分散設置されているクライアント端末の記憶する暗号化データを基にデータファイルを復元することができる。

【００２１】

ここで、データファイル暗号化かつ一体化手段によってランダムな状態になっているデータファイルを分割し、さらに分割データごとに異なる暗号鍵を用いて暗号化する。これにより、分割した順番を正確に再現できなければデータファイルの解読をすることが不可能になる。更に乱数と区別できない平文を乱数と区別できない暗号文に暗号化するので、解読される可能性を極めて低くすることができる。これにより、高速なストリーム暗号を用い、安全にかつ効率的にデータファイルをクライアント端末に分散させることができる。よって、ネットワークを活用して、災害が発生した場合であっても、安全にかつ効率的にデータファイルを復旧することができる。

【００２２】

本発明に係るディザスタリカバリプログラムでは、前記クライアント端末に動作をさせる暗号鍵更新命令と共に新たな暗号鍵を前記クライアント端末へ送信する暗号鍵送信手順を、前記暗号化データ送信手順の後に前記ディザスタリカバリ装置にさらに実行させ、前記暗号鍵更新命令は、前記クライアント端末に、当該暗号鍵を用いて当該クライアント端末の記憶する前記暗号化データを暗号化させ、当該クライアント端末の記憶する前記暗号化データを更新させることが好ましい。クライアント端末に格納されている時間の経過に伴い、暗号化データの盗聴される危険性が増す。しかし、クライアント端末にバックアップされている暗号化データをさらに暗号化し、暗号鍵を更新することで、この危険性を回避することができる。

【００２３】

本発明に係るディザスタリカバリプログラムでは、前記暗号化データ送信手順において、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を介して前記通信ネットワークへ送信し、当該ＶＰＮを介しての送信の際に、前記暗号化データ送信手順において送信した前記暗号化データを更に暗号化して前記クライアント端末へ送信することが好ましい。ＶＰＮに用いられる暗号化技術によって、暗号化データをさらに暗号化することができる。これにより、情報の安全性及び秘匿性を向上することができる。

【００２４】

本発明に係るディザスタリカバリプログラムでは、前記クライアント端末のそれぞれに

記憶されている前記暗号化データを読み出し、前記クライアント端末識別情報の異なる前記クライアント端末に記憶されている前記暗号化データと交換し、交換後の前記暗号化データを、前記クライアント端末のそれぞれに記憶させる暗号化データ交換手順を、前記暗号化データ送信手順の後に前記ディザスタリカバリ装置にさらに実行させることが好ましい。クライアント端末の記憶する暗号化データを交換して変更するので、もともとのデータファイルの復元は、これら分割及び暗号化に加え、さらに交換を含む一連のシーケンスを知っているものでなければ不可能とすることができる。これにより、盗聴によってデータファイルを復元可能なまでに暗号化データを収集することを困難にすることができる。

【００２５】

本発明に係るディザスタリカバリプログラムでは、前記データファイル暗号化かつ一体化手順、前記分割データ暗号化手順及び前記暗号化データ送信手順における時系列情報の送信を指示する時系列情報送信命令の入力を契機に、前記データファイル暗号化かつ一体化手順で暗号化した暗号鍵及び時系列情報、前記分割データ暗号化手順で暗号化した前記暗号鍵及び時系列情報並びに前記分割データ送信手順で送信した前記クライアント端末の前記クライアント端末識別情報及び時系列情報を、前記マスターサーバ及び前記クライアント端末と通信ネットワークで接続されている管理端末へ送信する時系列情報送信手順を前記ディザスタリカバリ装置にさらに実行させることが好ましい。時系列情報送信手順によって分割データ暗号化手順及び分割データ送信手順の時系列情報を管理端末に送信するので、マスターサーバが破壊された場合であっても、管理端末がデータファイルの復旧をすることができる。

【００２６】

本発明に係るディザスタリカバリプログラムでは、前記管理端末が複数であり、前記時系列情報送信手順において、複数の前記管理端末のそれぞれに前記暗号鍵及び前記クライアント端末識別情報並びにこれらの時系列情報を送信することが好ましい。管理端末を冗長配備することで、複数の管理端末にてデータファイルの復旧が可能となる。これにより、安全性を一層向上させるとともに、迅速なデータファイルの復旧が可能となる。

【００２７】

本発明に係る記録媒体は、前記ディザスタリカバリプログラムを格納した読み取り可能な記録媒体であることを特徴とする。ディザスタリカバリプログラムを格納した読み取り可能な記録媒体が本発明に係るディザスタリカバリプログラムを実行させることができるので、ネットワークを活用して、災害が発生した場合であっても、安全にかつ効率的にデータファイルを復旧することができる。

【００２８】

本発明に係るディザスタリカバリシステムは、マスターサーバと、前記マスターサーバから分散設置されている複数のクライアント端末とが互いに通信ネットワークで接続されているディザスタリカバリシステムであって、前記クライアント端末は、遊休状態であることを判定し、遊休状態であるとの判定を契機に、前記クライアント端末のそれぞれに固有のクライアント端末識別情報を、前記マスターサーバへ送信する識別情報送信手段と、前記マスターサーバの送信する前記暗号化データを受信する暗号化データ受信手段と、前記暗号化データ受信手段の受信する暗号化データを記憶する暗号化データ記憶手段と、前記マスターサーバは、データファイルを記憶するデータファイル記憶手段と、前記識別情報送信手段の送信する前記クライアント端末識別情報を受信する識別情報受信手段と、前記データファイル記憶手段の記憶する前記データファイルを暗号化するデータファイル暗号化かつ一体化手段と、前記データファイル暗号化かつ一体化手段の暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力するデータファイル分割手段と、前記データファイル分割手段の出力する前記分割データを、前記分割データごとに異なる暗号鍵を用いて暗号化した前記暗号化データを出力する分割データ暗号化手段と、前記分割データ暗号化手段の出力する前記暗号化データを、前記識別情報受信手段の受信する前記クライアント端末識別情報の前記クライアント端末へ送信する暗号化データ送信手段と、を有することを特徴とする。

【００２９】
マスターサーバが、データファイル暗号化かつ一体化手段、データファイル分割手段、分割データ暗号化手段及び暗号化データ送信手段を有するので、分散設置されている複数のクライアント端末のうちの遊休状態にある複数のクライアント端末に、分割及び暗号化を施した暗号化データのバックアップをすることができる。これにより、マスターサーバのある地域に災害が発生し、マスターサーバのデータファイルが使用不可能となった場合であっても、分散設置されているクライアント端末の記憶する暗号化データを基にデータファイルを復元することができる。
【００３０】
ここで、データファイル暗号化かつ一体化手段によってランダムな状態になっているデータファイルを分割し、さらに分割データごとに異なる暗号鍵を用いて暗号化する。これにより、分割した順番を正確に再現できなければデータファイルの解読をすることが不可能になる。更に乱数と区別できない平文を乱数と区別できない暗号文に暗号化するので、解読される可能性を極めて低くすることができる。これにより、高速なストリーム暗号を用い、安全にかつ効率的にデータファイルをクライアント端末に分散させることができる。よって、ネットワークを活用して、災害が発生した場合であっても、安全にかつ効率的にデータファイルを復旧することができる。
【発明の効果】
【００３１】
本発明により、分散設置されている複数のクライアント端末のうちの遊休状態にある複数のクライアント端末に、マスターサーバの保有するデータファイルのバックアップを行うことができる。これにより、マスターサーバのある地域に災害が発生し、マスターサーバのデータファイルが使用不可能となった場合であっても、分散設置されているクライアント端末の記憶する暗号化データを基にデータファイルを復旧することができる。
【００３２】
ここで、データファイル暗号化かつ一体化手段によってランダムな状態になっているデータファイルを分割し、さらに分割データごとに異なる暗号鍵を用いて暗号化する。これにより、分割した順番を正確に再現できなければデータファイルの解読をすることが不可能になる。更に乱数と区別できない平文を乱数と区別できない暗号文に暗号化するので、解読される可能性を極めて低くすることができる。これにより、高速なストリーム暗号を用い、安全にかつ効率的にデータファイルをクライアント端末に分散させることができる。よって、本発明により、ネットワークを活用して、災害が発生した場合であっても、安全にかつ効率的にデータファイルを復旧することができる。
【図面の簡単な説明】
【００３３】
【図１】本実施形態に係るディザスタリカバリシステムの一例を示す構成図である。
【図２】ディザスタリカバリ装置の構成を示す拡大図である。
【図３】識別情報管理手段の記憶する情報の一例を示す表である。
【図４】データファイル暗号化かつ一体化の一例を示す流れ図である。
【図５】図４に示す一体化処理関数Ｆによる処理の一例を示す流れ図である。
【図６】一体化処理関数Ｆの逆関数F^{-1}の実施の一例を示す流れ図である。
【図７】データファイル分割手段の動作の一例を示す時系列グラフである。
【図８】時系列情報記憶手段の記憶する時系列情報の一例を示す表である。
【図９】暗号化データ交換手段の動作の一例を示す流れ図である。
【図１０】クライアント端末の構成を示す拡大図である。
【図１１】管理端末の構成を示す拡大図である。
【図１２】ディザスタリカバリ装置の動作の一例を示す流れ図である。
【図１３】暗号化データを送信するまでのディザスタリカバリ装置の機能の一例を示す模式図である。
【図１４】データファイルの分割および配布先クライアント端末の選択を行う機能ｆの一

例を示す流れ図である。
【図１５】データファイルの分割および配布先クライアント端末の選択を行う際に用いる攪拌関数Ｐ（ｓ）の一例を示す流れ図である。
【図１６】暗号化データ復元手段の一例を示す模式図である。
【図１７】配布された暗号化データの復元を行う機能f^{-1}の一例を示す流れ図である。
【図１８】データファイル暗号化かつ一体化手段の機能の第１例を示す説明図である。
【図１９】データファイル暗号化かつ一体化手段における一体化の一例を示す説明図である。
【図２０】データファイル暗号化かつ一体化手段の機能の第２例を示す説明図である。
【図２１】複数のデータファイルを扱う場合のデータフォーマットの一例を示す説明図である。
【図２２】複数のデータファイルを扱う場合のデータファイルの読み出し方法の一例を示す流れ図である。
【符号の説明】
【００３４】
１１　マスターサーバ
１２　クライアント端末
１２Ａ、１２Ｂ、１２Ｃ　論理グループ
１３　管理端末
１４　ディザスタリカバリ装置
１５　通信ネットワーク
２１　識別情報送信手段
２２　暗号化データ受信手段
２３　暗号化データ記憶手段
２４　暗号鍵更新手段
２５　暗号化データ更新手段
２６　暗号化データ転送手段
３１　データファイル暗号化かつ一体化手段
３２　識別情報受信手段
３３　データファイル分割手段
３４　分割データ暗号化手段
３５　暗号化データ送信手段
３６　暗号鍵送信手段
３７　暗号化データ交換手段
３８　時系列情報送信手段
４１　暗号化情報送受信手段
４２　識別情報管理手段
４３　暗号化情報記憶手段
４４　暗号化データ収集手段
４５　暗号化データ復元手段
５１　データファイル記憶手段
５２　データファイル送受信手段
５３　識別情報管理手段
５４　暗号鍵記憶手段
５５　時系列情報記憶手段
６１　分割データ復号化手段
６２　暗号化データファイル復元手段
６３　データファイル復号化手段
６４　データファイル格納手段
９１　ディザスタリカバリシステム

１０１、１０２、１０３、１０４、１０５　データファイル
２００、２０１、２０２、２０３、２０４、２０５、２０６、２０７、２０８、２０９　ステップ

【発明を実施するための最良の形態】

【００３５】

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。図１は、本実施形態に係るディザスタリカバリシステムの一例を示す構成図である。本実施形態に係るディザスタリカバリシステム９１は、マスターサーバ１１と、マスターサーバ１１から分散設置されている複数のクライアント端末１２と、複数の管理端末１３と、が互いに通信ネットワーク１５で接続されている。本実施形態に係るディザスタリカバリシステム９１は、マスターサーバ１１に接続されたディザスタリカバリ装置１４を備える。

【００３６】

通信ネットワーク１５は、通信可能な情報伝達網であり、例えばインターネットである。通信ネットワーク１５がインターネットであることで、より多くのクライアント端末１２がディザスタリカバリシステム９１に参加することが可能となる。本実施形態では、通信ネットワーク１５上で通信される内容の全てが暗号化されていることが好ましい。例えば通信ネットワーク１５は、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）通信又はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）暗号通信を用いたものであることが好ましい。本実施形態では、クライアント端末１２がディザスタリカバリシステム９１を構成するグリッドコンピューティングネットワークに参加をすることに同意した、あらかじめ定められた端末である。このため通信ネットワーク１５上に、ディザスタリカバリシステム９１に固有のＶＰＮが形成されていることが好ましい。ＶＰＮの形成は、マスターサーバ１１の有するデータファイル送受信手段５２と、クライアント端末１２の有する送受信手段と、管理端末１３の有する送受信装置と、のそれぞれに、通信ネットワーク１５上でＶＰＮ接続するためのＶＰＮ装置を搭載することで、通信ネットワーク１５上でＶＰＮを形成することができる。この場合、データファイル送受信手段５２と通信ネットワーク１５との間のデータファイル送受信手段５２に搭載されたＶＰＮ装置は、ディザスタリカバリ装置１４の送信した暗号化データを更に暗号化し、通信ネットワーク１５を介してクライアント端末１２へ送信する。通信ネットワーク１５がＶＰＮであることで、マスターサーバ１１とクライアント端末１２との間で送受信されるあらゆる情報を、ＶＰＮ装置に搭載されている暗号化手段を用いて暗号化することができる。暗号化手段には、例えばＩＰＳＥＣ（インターネット　プロトコル　セキュリティ）方式を用いて暗号化するものがある。

【００３７】

マスターサーバ１１は、例えば、データファイルを記憶するデータファイル記憶手段５１と、通信ネットワーク１５を介してデータファイル記憶手段５１の記憶するデータファイルを送受信するデータファイル送受信手段５２と、を備えるものである。データファイル記憶手段５１の記憶するデータファイルの内容は限定するものではない。しかし、本実施形態に係るディザスタリカバリシステム９１では、自治体の保管する戸籍などの個人情報や病院の保管するカルテなどの医療情報といった秘匿性の高いデータファイルであっても適用することができる。例えば、マスターサーバ１１は、データファイル記憶手段５１の記憶するカルテを、データファイル送受信手段５２を介してクライアント端末１２に開示するものである。

【００３８】

ディザスタリカバリ装置１４は、マスターサーバ１１のデータファイル記憶手段５１に格納されているデータファイルのバックアップを行うものである。本実施形態では、一例として、マスターサーバ１１に接続されている例を示した。ディザスタリカバリ装置１４は、データファイル記憶手段５１からデータファイルを取得することが可能であれば、有線や無線のローカルエリアネットワークを介してマスターサーバ１１と接続されていても

よい。通信ネットワークを介してマスターサーバ１１と接続されることで、分散型のマスターサーバ１１についても適用することができる。通信ネットワークを介することで盗聴が危惧される場合には、マスターサーバ１１と直接接続することが好ましい。

【００３９】

又、ディザスタリカバリ装置１４は、ディザスタリカバリ装置１４に備わる各手段として機能させるためのディザスタリカバリプログラムとすることも可能であり、この場合には、マスターサーバ１１にディザスタリカバリプログラムを格納し、マスターサーバ１１にディザスタリカバリプログラムを実行させることで、ディザスタリカバリ装置１４に備わる各機能を実現することができる。ディザスタリカバリ装置１４は、ディザスタリカバリプログラムを格納したコンピュータ読み取り可能な記録媒体によって実現されるものであってもよい。

【００４０】

図２は、ディザスタリカバリ装置の構成の一例を示す拡大図である。ディザスタリカバリ装置１４は、データファイル暗号化かつ一体化手段３１と、識別情報受信手段３２と、データファイル分割手段３３と、分割データ暗号化手段３４と、暗号化データ送信手段３５と、を有する。ディザスタリカバリ装置１４は、さらに、暗号鍵送信手段３６と、暗号化データ交換手段３７と、時系列情報送信手段３８とをさらに有することが好ましい。又、識別情報管理手段５３と、暗号鍵記憶手段５４と、時系列情報記憶手段５５と、をさらに有することが好ましい。

【００４１】

ここで、識別情報受信手段３２と、データファイル暗号化かつ一体化手段３１と、データファイル分割手段３３と、分割データ暗号化手段３４と、暗号化データ送信手段３５と、暗号鍵送信手段３６と、暗号化データ交換手段３７と、時系列情報送信手段３８は、これらの手段として機能させるためのディザスタリカバリプログラムとすることも可能である。ディザスタリカバリプログラムは、例えば、識別情報受信手段３２を実行する識別情報受信手順と、データファイル暗号化かつ一体化手段３１を実行するデータファイル暗号化かつ一体化手順と、データファイル分割手段３３を実行するデータファイル分割手順と、分割データ暗号化手段３４を実行する分割データ暗号化手順と、暗号化データ送信手段３５を実行する暗号化データ送信手順と、暗号鍵送信手段３６を実行する暗号鍵送信手順と、暗号化データ交換手段３７を実行する暗号化データ交換手順と、時系列情報送信手段３８を実行する時系列情報送信手順とを有する。この場合、ディザスタリカバリプログラムをマスターサーバ１１に実行させることで、ディザスタリカバリ装置１４を省略することができるので、省スペース化を図ることができる。

【００４２】

図２に示す識別情報受信手段３２は、クライアント端末１２から送信されたクライアント端末識別情報を受信する。クライアント端末識別情報は、クライアント端末１２のそれぞれが所有する固有の識別情報である。ディザスタリカバリシステム９１では、マスターサーバ１１を介してディザスタリカバリ装置１４とクライアント端末１２とでグリッドコンピューティングネットワークを構成しており、遊休状態となったクライアント端末１２はグリッドコンピューティングネットワークにログインするためのクライアント端末識別情報を識別情報受信手段３２へ送信する。ここで、遊休状態となったクライアント端末１２がログイン情報などのクライアント端末識別情報以外の情報を送信する場合は、識別情報受信手段３２は、それらの情報も受信することが好ましい。クライアント端末１２が遊休状態である情報を識別情報受信手段３２が取得することで、遊休状態のクライアント端末１２を有効利用して、グリッドコンピューティングネットワークを形成することができる。

【００４３】

図２に示す識別情報管理手段５３は、クライアント端末１２に関する情報を記憶する。図３は、識別情報管理手段の記憶する情報の一例を示す表である。図３では、一例として、クライアント端末識別情報ごとに、ユーザ名、論理グループ、端末状況を示した。端末

状況は、例えば、グリッドコンピューティングネットワークにログインしているか否かである。グリッドコンピューティングネットワークにログインしていればＯＫ、グリッドコンピューティングネットワークにログインしていなければＮＧと記憶される。識別情報管理手段５３の記憶するクライアント端末１２に関する情報は、随時更新され、最新情報は、マスターサーバ１１や管理端末１３の管理人が閲覧可能となっていることが好ましい。クライアント端末１２に関する情報の盗聴を防止するため、マスターサーバ１１と管理端末１３との送受信は、ＳＳＬなどの通信の内容すべてを暗号化する通信方式によって行うことが好ましい。

【００４４】

図３において、クライアント端末識別情報ＩＤ＿１２ａ１は、図１に示す論理グループ１２Ａに属するクライアント端末１２ａ１を示す。クライアント端末１２ａ１の端末状況はＯＫとなっており、ディザスタリカバリシステムのグリッドコンピューティングネットワークに参加している状態にある。又、クライアント端末識別情報ＩＤ＿１２ａ２は、図１に示す論理グループ１２Ａに属するクライアント端末１２ａ２のクライアント端末識別情報を示す。クライアント端末１２ａ２の端末状況はＮＧとなっており、ディザスタリカバリシステムのグリッドコンピューティングネットワークに参加していない状態にある。又、クライアント端末識別情報ＩＤ＿１２ｃｎは、図１に示す論理グループ１２Ｃに属するクライアント端末１２ｃｎのクライアント端末識別情報を示す。クライアント端末１２ｃｎの端末状況はＯＫとなっており、ディザスタリカバリシステムのグリッドコンピューティングネットワークに参加している状態にある。

【００４５】

図２に示すデータファイル暗号化かつ一体化手段３１は、マスターサーバ１１の記憶するデータファイルを暗号化する。例えば、マスターサーバ１１の記憶するデータファイルを取得し、ストリーム暗号等の共通鍵暗号でデータファイルをランダムな状態にする。この場合、共通鍵暗号として、加法的暗号のような高速なストリーム暗号を用いることが好ましい。ディザスタリカバリ装置１４は、データファイル暗号化かつ一体化手段３１の後段に分割データ暗号化手段３４を有し、分割データ暗号化手段３４がさらに分割データを暗号化するので、高速なストリーム暗号であっても、解読される可能性を極めて低くすることができる。これによりデータファイルの効率的な暗号化を行うことができる。データファイル暗号化かつ一体化手段３１は、ストリーム暗号の場合には、更に、一体化処理関数Ｆを複数回、実施し、全体を攪拌することが、好ましい。暗号化かつ一体化処理関数Ｆの実行は、６回以上であることが、好ましい。データファイル暗号化かつ一体化手段３１の具体的な実施例を図４に示し、一体化処理関数Ｆの実施例を図５に示す。また、一体化処理関数Ｆの逆関数のF^{-1}の実施例を図６に示す。一方、ブロック暗号を使用する場合には、通常のＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）モードで暗号化した後で、上記と同様の手順で一体化かつ暗号化処理を行うことが、同様に可能である。データファイル暗号化かつ一体化手段３１は、暗号化に用いた暗号鍵を、暗号化した時系列情報と共に時系列情報記憶手段５５に出力する。

【００４６】

図１８は、データファイル暗号化かつ一体化手段の機能の第１例を示す説明図である。暗号化は、例えば、リカバリの対象となるデータファイルと乱数列との演算処理を行う。ここで行う演算処理は、例えば、排他的論理輪（ＥＯＲ）演算である。暗号化されているデータファイル１０１を生成する。暗号化後に行う一体化では、暗号化したデータファイルを複数のデータピースに分割してデータピース同士を可逆演算する。一体化は、例えば、データの空間分散化である。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。

【００４７】

一体化では、例えば、暗号化したデータファイル１０１をｎ個（ｎは２以上の整数。）に分割して当該分割されたそれぞれのデータピースをｍサイクルにわたり２進加算する。一体化が終了した後のデータファイルは、他のデータピースを暗号化している乱数が混入

しているので、「・・・※ａｐ／・・・Ａｂ・・・」のように、無意味な乱数列となる。仮に１つのデータピースを解読できたとしても、分割及び配布の順序を特定できない限りは、データファイルの正しい情報を取り出すことはほとんど不可能である。このため、例えデータピース＃２がハッキングされたとしても、正解のデータファイルを回復することはできない。

【００４８】

図１９は、データファイル暗号化かつ一体化手段における一体化の一例を示す説明図である。データファイル１０１が＃１から＃ｎのｎ個のデータピースに分割されている。図では、簡単のため、データファイル１０１を８ｂｉｔ×ｎワードで表現した。データピースは、たとえば、データピース＃１が１１０００００００、データピース＃２が０００００００１、データピース＃３が０００００００１０、データピース＃４が０００００００００、データピース＃ｎが１０００００００で表される。

【００４９】

一体化においては、データピースの可逆演算を行う。本実施形態では、隣接するデータピース同士を２進加算する場合について説明する。データファイル１０２は、データファイル１０１から一体化に関わる初めの２進加算が行われた後のファイルである。データファイル１０２のデータピース＃２’は、データピース＃１とデータピース＃２が２進加算された１１０００００１となっている。データファイル１０３は、データファイル１０２から一体化に関わる２回目の処理が行われた後のファイルである。データファイル１０３のデータピース＃３’は、データピース＃２’とデータピース＃３が２進加算された１１０００００１１となっている。データファイル１０１からデータファイル１０２への一体化、データファイル１０２からデータファイル１０３への一体化のように、データピース＃（ｎ－１）’までの一体化が行われる。データファイル１０４は、データピース＃ｎ’までの一体化が行われた後のファイルである。データファイル１０４のデータピース＃ｎ’は、データピース＃（ｎ－１）’とデータピース＃ｎが２進加算されている。データファイル１０５のデータピース＃１’は、データピース＃ｎ’とデータピース＃１が２進加算されている。このように、１からｎまでのデータピースを２進加算し、すべてのデータピースを暗号化して、１サイクル目の一体化を行う。

【００５０】

ここで、２進加算を行うデータピースの番号は、隣接する番号に限定しない。例えば、データピース＃２’は、データピース＃４などの一定間隔を離れた番号のデータピースであってもよい。また、一体化は、複数サイクル行うことが好ましく、例えば６サイクル以上行うことが好ましい。一体化を複数回行うことで、ストリーム暗号方式によっても暗号強度を大幅に向上することができる。また、一体化のサイクルごとに、演算処理するデータピースを変更することが好ましい。例えば、データピース＃２’について、２サイクル目の一体化ではデータピース＃３と演算処理し、３サイクル目の一体化ではデータピース＃４と演算処理する。また、一体化に用いる演算処理は、一体化のサイクルごとに変更してもよい。

【００５１】

一体化を用いた暗号化を行うことで、ストリーム暗号方式を用いた場合であっても、読解を困難にすることができる。また、データピース毎の一体化による暗号化が施されており、かつ、データファイルを分割して複数のクライアントへデータ拡散するので、「暗号鍵の強化」と「データ拡散」の作用を生ずる２つの機能があり、暗号強度を大幅に向上させることができる。この二重の安全性を担保によって、分割化された元のデータファイルの各データピース毎の正常な組み合せを発見することは殆ど困難となる。仮に、正しい組み合せ方が何らかの手段で見出されたとしても、データファイルの盗聴者による復元化処理が殆ど不可能である。

【００５２】

図２０は、データファイル暗号化かつ一体化手段の機能の第２例を示す説明図である。暗号化は、例えば、リカバリの対象となるデータファイルと乱数列との演算処理を行う。

暗号化後には、複数回にわたり一体化を行う。そして、一体化のサイクルごとに、演算処理するデータピースの数を一定にすることも変更することもできる。例えば、一番単純な場合は、１サイクル目では、＃１から＃ｎまでのデータピースのうちの，隣り合う２つのデータピースを用い、全データピースの攪拌を行うための演算処理を行う。２サイクル目でも同様に、＃１から＃ｎまでのデータピースのうちの隣あう２つのデータピースを用いて全データピースの攪拌を行うための演算処理を行う。３サイクル目でも同様に、＃１から＃ｎまでのデータピースのうちの隣あう２つデータピースを用いて全データピースの攪拌を行うための演算処理を行う。そして、６サイクル目でも同様に、＃１から＃ｎまでのデータピースのうちの隣あう２つデータピースを用いて全データピースの攪拌を行うための演算処理を行う。このように、一体化のサイクルごとに、攪拌を行うための演算処理を行うことにより、等価的に、複数個（７個）の暗号鍵を用いてデータを攪拌したことと等価になり、このことは、言い換えると、暗号鍵の長さを、等価的に、長くすることに対応している。

【００５３】

上述した例では、一体化処理の６サイクルの間において、＃１から＃ｎまでのデータピースのうちの隣あう２つデータピースを用いて攪拌する場合を示しているが、本発明における一体化の処理は、この方法に限定されるものではない。すなわち、２サイクル目では＃１から＃ｎまでのデータピースのうちの３つデータピースを用いて演算処理を行う。３サイクル目では、＃１から＃ｎまでのデータピースのうちの４つのデータピースを用いて演算処理を行う。そして、６サイクル目では、＃１から＃ｎまでのデータピースのうちの７つのデータピースを用いて演算処理を行う、などの方法をとることも、同様に可能であり、これらのうち、どの方法をとるかについては、秘匿されている。すなわち、一体化のサイクルごとに演算処理を行うデータピースの数を増やす場合も、あるいは、減らす方法を用いる場合も同様に可能であり、これらの方法を複数回適用することにより、暗号鍵の長さを等価的に長くする効果を持たせることができる。

【００５４】

以上、説明した例では、一体化の対象とするファイルが１つの場合の例を示しているが、一体化の対象とするファイルが複数ある場合も同様に可能である。例えば、簡単化のために、一体化の対象とするファイルの容量が同じで、かつ、個数がｍ個存在した場合には、上述の例における１サイクル目の＃１から＃ｎまでのデータピースの数が、＃１から＃（ｎ×ｍ）までのデータピースの数まで、増加しただけであり、これらの各々のデータピースに対して、隣り合う２つのデータピースを可逆演算処理を行い、全（ｎ×ｍ）データピースの攪拌を行うことにより、当該のｍ個のファイルに対しても、同様な演算処理を行う形態を適用するだけで、全てのファイルの内容は、１つのファイルを扱う場合と同様に、攪拌することが可能となる。

【００５５】

複数サイクルにわたって一体化したデータファイルは、データファイル分割手段にて分割され、分割データ暗号化手段にて暗号化され、暗号化データ送信手段にてクライアント端末へ送信される。例えば、６サイクル以上の一体化による暗号化処理されたデータファイルが、分割されてクライアント端末ＣＬ$_a$、ＣＬ$_b$、ＣＬ$_c$、ＣＬ$_d$へ送信される。クライアント端末へ送信する際、各々のデータファイルをコピーして冗長転送する場合には、データファイル暗号化かつ一体化手段の一体化において、別の暗号鍵となるデータピースでの一体化を行うことが好ましい。また、各々のデータファイルをコピーして冗長転送する際には、分割データ暗号化手段にて、データファイルをコピーするたびに、異なる暗号鍵を用いて暗号化することが好ましい。

【００５６】

図２１は、複数のデータファイルを扱う場合のデータフォーマットの一例を示す説明図である。データファイルが複数ある場合は、複数のデータファイルを単一の新たなデータファイルにする。１つの新たなデータファイルとすることで、前述の一体化と同様の方法で、複数のファイルについても一体化することができる。単一の新たなデータファイルは

、例えば、予め定められたバイト数のヘッダと、ｎ個のデータファイルを有する。ヘッダは、含まれているデータファイル数ｎと、含まれているデータファイルのデータファイル名f_i（ｉ＝１～ｎ）及びデータファイルの長さL_i（ｉ＝１～ｎ）の情報を有する。データファイル名f_i及びデータファイルの長さL_iについての情報のバイト数は予め定められている。例えば、データファイル名f_iは１２バイトでありであり、データファイルの長さL_iは４バイトである。この場合、ヘッダのバイト数は、（４＋１６×ｎ）バイトとなる。

【００５７】

図２２は、複数のデータファイルを扱う場合のデータファイルの読み出し方法の一例を示す流れ図である。まず、ステップ２０１においては、図２１に示す単一の新たなデータファイルのデータ形式を読み込む。ステップ２０２においては、単一の新たなデータファイルのヘッダから、データファイル数ｎを読み取る。ステップ２０３においては、データファイルの番号ｉを１に設定する。データファイルの番号ｉは、データファイルがｎ個ある場合、１からｎまでの自然数である。ステップ２０４においては、データファイルの番号ｉがデータファイル数ｎよりも大きいか否かを判定する。データファイルの番号ｉがデータファイル数ｎよりも小さい場合、ステップ２０５へ移行する。一方、データファイルの番号ｉがデータファイル数ｎよりも大きい場合、ステップ２０９へ移行し、終了する。ステップ２０５においては、ヘッダから、データファイル名f_i及びデータファイルの長さL_iを取得する。ステップ２０６においては、ステップ２０５で取得したデータファイル名f_iのデータファイルを、データファイルの長さL_iだけ読み取る。ステップ２０７においては、ステップ２０５で取得したデータファイル名f_iを出力する。ステップ２０８においては、データファイルの番号ｉに１を加算し、ステップ２０４へ移行する。

【００５８】

図４は、データファイル暗号化かつ一体化の一例を示す流れ図である。図４に示す流れ図は、ｎ＋１ワードのデータをストリーム暗号を使用して暗号化する場合を示す。まず、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードのデータをストアする（Ｓ５０１）。ここで、ｘ（０）からｘ（ｎ）は、それぞれ１ワードのデータであり、通常３２ｂｉｔである。そして、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードのデータをストリーム暗号で暗号化する（Ｓ５０２）。そして、一体化処理関数Ｆによる処理を６回行った後（Ｓ５０３～Ｓ５０６）、ｎ＋１ワードのデータを出力する（Ｓ５０７）。

【００５９】

図５は、図４に示す一体化処理関数Ｆによる処理の一例を示す流れ図である。まず、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードのデータをストアする（Ｓ５１１）。そして、ワードｘ（ｉ）とワードｘ（ｉ＋１）を加算したものをワードｘ（ｉ＋１）とし（Ｓ５１４）、これをワードｘ（０）からワードｘ（ｎ－１）まで行う（Ｓ５１２～Ｓ５１５）。そして、ワードｘ（０）とワードｘ（ｎ）を加算したものをワードｘ（０）とし（Ｓ５１６）、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードを出力する（Ｓ５１７）。

【００６０】

図６は、一体化処理関数Ｆの逆関数F^{-1}の実施の一例を示す流れ図である。まず、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードのデータをストアする（Ｓ５２１）。そして、ワードｘ（０）からワードｘ（ｎ）を減算してワードｘ（０）とする（Ｓ５２２）。そして、ワードｘ（ｎ－ｉ）からワードｘ（ｎ－ｉ－１）を減算したものをワードｘ（ｎ－ｉ）とし（Ｓ５２５）、これをｉ＝０からｉ＝ｎ－１まで繰り返す（Ｓ５２３～Ｓ５２６）。そして、ワードｘ（０）からワードｘ（ｎ）までのｎ＋１ワードのデータを出力する（Ｓ５２７）。

【００６１】

ディザスタリカバシステムでは、複数地域に分散されたクライアント端末へデータファイルを配布することが前提である。この時に、当該データファイルに関して、以下の分割数を想定した場合の総当り方式による解読に必要な暗号強度を概算した。例えば、分割数

が２０の場合、ファイルの並べ方の組み合せは、２０！　2^{61}　10^{18}となる。この組み合せ数はＤＥＳ（５４ビット）暗号以上の安全性をもつ。又、分割数が４０の場合、ファイルの並べ方の組み合せは、４０！　2^{160}　10^{47}となる。この組み合せ数は、ＡＥＳ（１２８ビット）暗号以上の安全性をもつ。又、分割数が８０の場合、ファイルの並べ方の組み合せは、８０！　2^{400}　10^{120}となる。この組み合せ数は、４００ビット暗号の安全性をもつことと等価であり、このレベルに匹敵する安全性をもつ暗号は、まだ、実用化されていない。すなわち、データファイルは、暗号化されており、さらに、ブロック毎の一体化による暗号化が施されている。このように、データファイルの暗号化によって、分割化された元ファイルの各ブロック毎の正常な組み合せ方を発見することが、殆ど困難な状況である条件に加え、更に、ブロック毎の一体化による暗号化が同時に施されているので、二重の安全性を担保している。仮に、万が一、正しい組み合せ方が何らかの手段で見出されたとしても、ファイルの盗聴者による復元化処理は、殆ど不可能である。

【００６２】

図２に示すデータファイル分割手段３３は、データファイル暗号化かつ一体化手段３１の暗号化した暗号化データファイルを分割し、当該暗号化データファイルを分割した分割データを出力する。図７は、データファイル分割手段３３の動作の一例を示す時系列グラフである。データファイル分割手段は、例えば、入力されたデータファイルを定められた容量ごとに分割する。分割する容量は、分割データ暗号化手段（図２の符号３４）の暗号化する暗号鍵に適したビット数が好ましい。データファイル分割手段（図２の符号３３）は、分割データのそれぞれが生成された時刻ごとに、固有の識別情報を割り当てることが好ましい。例えば、時刻ＴＤｍに分割された分割データについて識別情報ＦＤｍを割り当てる。さらにデータファイル分割手段（図２の符号３３）は、時系列情報として、時刻ＴＤｍと識別情報ＦＤｍを時系列情報記憶手段（図２の符号５５）に出力することが好ましい。ここで、時系列情報には、分割データそのものが含まれていてもよい。

【００６３】

図２に示す暗号鍵記憶手段５４は、データファイル暗号化かつ一体化手段３１の用いる暗号鍵と、分割データ暗号化手段３４の用いる暗号鍵を記憶する。暗号鍵記憶手段５４は、暗号鍵を生成させ、生成させた暗号鍵を記憶するものであってもよい。暗号鍵記憶手段５４は、データファイル暗号化かつ一体化手段３１及び又は分割データ暗号化手段３４が複数回暗号化を行う場合には、それぞれの回に応じた暗号鍵を記憶することが好ましい。

【００６４】

図２に示す分割データ暗号化手段３４は、データファイル分割手段３３の出力する分割データを、それぞれ異なる暗号鍵を用いて暗号化する。そして、暗号化した暗号化データを出力する。分割データ暗号化手段３４の暗号化する暗号化方式は、例えば、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）又はＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）等の共通鍵暗号方式である。分割データ暗号化手段３４の暗号化は、ブロック暗号又はストリーム暗号のいずれでもよいが、ストリーム暗号であれば高速な暗号化を行うことができる。又、ブロック暗号を使用する場合は、ＣＢＣモードを使用することが好ましい。さらに分割データ暗号化手段３４の暗号化は、２回以上、より好ましくは６回以上繰り返すことが好ましい。例えばＤＥＳを３回繰り返すトリプルＤＥＳが好ましい。暗号化を繰り返す場合、繰り返しの度に異なる暗号鍵を用いて暗号化することが好ましく、例えば５６ｂｉｔの暗号鍵を用いてトリプルＤＥＳを行い、１１２ｂｉｔの暗号鍵とすることが好ましい。分割データ暗号化手段３４は、暗号化に用いた暗号鍵を、暗号化した時系列情報と共に時系列情報記憶手段５５に出力する。ここで、暗号鍵を、暗号化した分割データの識別情報（図７の符号ＦＤｍ）と関連付けて出力することが好ましい。

【００６５】

図２に示す暗号化データ送信手段３５は、分割データ暗号化手段３４の出力する暗号化データを、識別情報受信手段３２の受信するクライアント端末識別情報のクライアント端

末１２へ送信する。例えば、送信先のクライアント端末１２は、識別情報管理手段５３に記憶されているクライアント端末１２のうちの、グリッドコンピューティングネットワークにログインしているクライアント端末１２である。ここで、暗号化データ送信手段３５が暗号化データを送信するクライアント端末１２は、１つ以上である。すなわち分散配置されているクライアント端末１２のうちの１台以上に送信する。送信先が２箇所以上である場合は、異なる論理グループに送信することが好ましい。又、本実施形態では通信ネットワーク１５上にＶＰＮが形成されていることが好ましく、この場合、暗号化データ送信手段３５はＶＰＮ装置を介して通信ネットワーク１５と接続される。この場合、ＶＰＮ装置において、暗号化データ送信手段３５の送信した暗号化データを更に暗号化してクライアント端末１２へ送信することができる。よって、ＶＰＮ装置が暗号化データをさらに暗号化してクライアント端末１２へ送信するので、情報の安全性及び秘匿性を向上することができる。

【００６６】

暗号化データ送信手段３５は、更に、分割データを送信するクライアント端末１２を秘匿された方法で決定する。秘匿された方法とは、暗号化データ送信手段３５の送信する先のクライアント端末１２を秘匿化できる方法であり、例えば、ランダムに選択するアルゴリズムを用いた方法である。ランダムに選択する際においても、その「ランダム性」においては、データ発信元のデータセンタ側では、当該の「ランダム性」を実現するためのアルゴリズムを知っていることが前提となる。通常は、データセンタ側では、暗号化されたデータファイルを可能な範囲で地域分散化して、安全性およびデータ回復率を向上させることが望ましいため、これに適合可能な分割転送するアルゴリズムを使用することが好ましい。さらに、各地域のクライアント端末１２への分割データの割り当て法は、クライアント端末１２に分散させる暗号化データの更新、追記又は上書きを定期的に行う場合にも、秘匿された方法で決定することが望ましい。例えば、１日に１回定期更新する場合においても、前日に、あるクライアント端末１２へ送信した分割データは、通常は、翌日において、同一のクライアント端末１２へ送信した分割データと、内容が、異なるようにすることが、好ましい使用方法である。

【００６７】

暗号化データ送信手段３５は、更に、クライアント端末１２に暗号化データを記憶させる。例えば、クライアント端末１２に暗号化データを記憶させる命令である暗号化データ記憶命令をクライアント端末１２に送信し、クライアント端末１２に当該暗号化データ記憶命令を実行させることでクライアント端末１２に暗号化データを記憶させる。

【００６８】

図２に示す時系列情報記憶手段５５は、データファイル暗号化かつ一体化手段３１の時系列情報と、分割データ暗号化手段３４の暗号化した時系列情報と、暗号化データ送信手段３５の出力した時系列情報を記憶する。図８は、時系列情報記憶手段の記憶する時系列情報の一例を示す表である。図８には、データファイル暗号化かつ一体化手段（図２の符号３１）及び分割データ暗号化手段（図２の符号３４）の出力する時系列情報として、識別情報ＦＤｍの分割データを暗号化した時刻ＴＥｍと、識別情報ＦＤｍの分割データを暗号化した暗号鍵Ｋｍと、が例示されている。ここで、暗号鍵Ｋｍには、データファイル暗号化かつ一体化手段３１の暗号化に用いた暗号鍵が含まれる。すなわち、分割データの識別情報ＦＤ１から識別情報ＦＤｍのそれぞれに、同一の暗号鍵及び暗号化の時刻のペアが記憶されている。又、１つの分割データが複数の暗号鍵によって暗号化されている場合がある。この場合は、１つの分割データの識別情報ＦＤｍに対して、暗号化した時刻ＴＥｍとして複数の時刻が記憶され、それぞれの時刻に対応する暗号鍵が暗号鍵Ｋｍとして記憶されている。

【００６９】

又、図８には、暗号化データ送信手段（図２の符号３５）の出力する時系列情報として、暗号化データ送信時刻ＴＳｍと、クライアント端末識別情報ＩＤ＿１２ｃｎとが例示されている。ここで、暗号化データ送信時刻ＴＳｍは、例えば、識別情報ＦＤｍの分割デー

タが暗号化された暗号化データを、暗号化データ送信手段（図２の符号３５）が送信した時刻である。又、クライアント端末識別情報ＩＤ＿１２ｃｎは、識別情報ＦＤｍの分割データが暗号化されている暗号化データを、暗号化データ送信手段（図２の符号３５）が送信した送信先のクライアント端末１２のクライアント端末識別情報である。

【００７０】

図２に示すように、ディザスタリカバリ装置１４が暗号鍵送信手段３６をさらに有する場合、暗号鍵送信手段３６は、暗号鍵更新命令と共に新たな暗号鍵をクライアント端末１２へ送信する。ディザスタリカバリ装置１４が暗号鍵送信手段３６をさらに有することで、クライアント端末に格納されている時間の経過に伴い、暗号化データの盗聴される危険性が増す。しかし、クライアント端末にバックアップされている暗号化データをさらに暗号化し、暗号鍵を更新することで、この危険性を回避することができる。暗号鍵送信手段３６は、例えば、暗号鍵記憶手段５４から新たな暗号鍵を取得する。そして、識別情報管理手段５３を参照してクライアント端末識別情報を取得し、取得したクライアント端末識別情報のクライアント端末１２へ暗号鍵及び暗号鍵更新命令を送信する。ここで、暗号鍵送信手段３６が暗号鍵及び暗号鍵更新命令を送信するクライアント端末１２は、ディザスタリカバリシステム９１のグリッドコンピューティングネットワークにログイン中であることが好ましいが、定期的にすべてのクライアント端末１２に送信することが好ましい。暗号鍵送信手段３６は、暗号鍵送信手段３６の実行した時系列情報を、時系列情報記憶手段５５へ出力する。時系列情報は、例えば、新たな暗号鍵を送信した時刻と、その新たな暗号鍵の送信先のクライアント端末１２のクライアント端末識別情報である。この時系列情報を取得した時系列情報記憶手段５５は、暗号鍵送信手段３６の出力した時系列情報を、前述の図８に示したクライアント端末１２のクライアント端末識別情報に追加する。

【００７１】

ここで、暗号鍵更新命令は、クライアント端末１２に動作をさせる命令である。暗号鍵更新命令を受信することによって、クライアント端末１２は、記憶している暗号化データを読み出し、暗号鍵更新命令と共に受信した新たな暗号鍵を用いて読み出しや暗号化データをさらに暗号化する。そして、暗号鍵更新命令を受信する前に記憶していた暗号化データを、新たな暗号鍵を用いて暗号化した暗号化データに更新する。このように、暗号鍵送信手段３６を有することで、ディザスタリカバリ装置１４は、遠隔地域にバックアップされる暗号化データの暗号鍵を更新することができる。暗号鍵送信手段３６の実行は、定期的に行うことが好ましい。クライアント端末１２に格納されている時間の経過に伴い、暗号化データの盗聴される危険性が増す。そこで、定期的に暗号鍵を更新することで、この危険性を回避することができる。又、暗号鍵送信手段３６の実行は、不定期に行ってもよい。例えば、暗号鍵送信手段３６は、暗号化データ送信手段３５と同期しており、暗号化データ送信手段３５の送信先のクライアント端末１２に暗号鍵及び暗号鍵更新命令を送信する。暗号鍵送信手段３６を実行することで、各地域に分散バックアップする情報を、更新の都度、異なった暗号鍵で暗号化することができる。これにより容易には通信ネットワーク１５上からデータの盗聴が実施できず、かつ、復元を困難にすることができる。

【００７２】

又、図２に示すように、ディザスタリカバリ装置１４が暗号化データ交換手段３７をさらに有する場合、暗号化データ交換手段３７は、クライアント端末１２のそれぞれに記憶されている暗号化データを読み出し、クライアント端末識別情報の異なるクライアント端末１２に記憶されている暗号化データと交換し、交換後の暗号化データを、クライアント端末１２のそれぞれに記憶させる。

【００７３】

図９は、暗号化データ交換手段の動作の一例を示す流れ図である。暗号化データ交換手段３７は、クライアント端末１２のクライアント端末識別情報を識別情報管理手段（図２の符号５３）から読み出す（Ｓ４０１）。暗号化データ交換手段３７は、識別情報管理手段（図２の符号５３）から読み出したクライアント端末１２のそれぞれに対して読出命令を送信する（Ｓ４０２）。クライアント端末１２のそれぞれは、この読出命令を受信する

と、暗号化データを読み出し（Ｓ４１１）、読み出した暗号化データを暗号化データ交換手段３７へ送信する（Ｓ４１２）。

【００７４】

暗号化データ交換手段３７は、クライアント端末１２のそれぞれから受信した暗号化データに基づき、クライアント端末識別情報に対応する暗号化データの表を構築する（Ｓ４０３）。暗号化データ交換手段３７は、構築した表の暗号化データのそれぞれを、クライアント端末１２のクライアント端末識別情報の異なる暗号化データと交換する（Ｓ４０４）。暗号化データ交換手段３７は、暗号化データを交換した後の暗号化データを、対応するクライアント端末識別情報のクライアント端末１２へそれぞれ送信すると共に、クライアント端末１２に新たな暗号化データを記憶させる命令を送信する（Ｓ４０５）。クライアント端末１２は、新たな暗号化データを記憶させる命令を受信すると、あらかじめ記憶していた暗号化データを、当該命令と共に受信した暗号化データに書き換えて更新する（Ｓ４１３）。

【００７５】

一方、暗号化データ交換手段３７は、暗号化データ交換手段３７の時系列情報を、時系列情報記憶手段（図２の符号５５）へ出力する（Ｓ４０６）。時系列情報は、例えば、交換した暗号化データを送信した時刻と、送信先のクライアント端末１２のクライアント端末識別情報である。この時系列情報を取得した時系列情報記憶手段（図２の符号５５）は、前述の図８に示したクライアント端末１２のクライアント端末識別情報を追加又は上書して更新する。

【００７６】

クライアント端末１２は、暗号化データの更新が完了すると、完了を暗号化データ交換手段３７へ通知する（Ｓ４１４）。暗号化データ交換手段３７は、クライアント端末１２からの通知（Ｓ４１４）を受信すると、暗号化データ交換手段３７を終了する（Ｓ４０７）。

【００７７】

上記のように、図２に示す暗号化データ交換手段３７は、複数の遠隔地にあるクライアント端末１２に記憶されている暗号化データを変更することができる。ディザスタリカバリ装置１４が暗号化データ交換手段３７を有することで、すべての分割データの復元に必要な並べ替えも考慮した解読操作が、全地域に分散したデータを対象に、同時に、実施されない限り、解読を不可能とすることができる。

【００７８】

なお、暗号化データ交換手段３７による暗号化データの交換は、遊休状態にあるクライアント端末１２に対して行うことが好ましい。例えば、暗号化データ交換手段３７は暗号化データ送信手段３５と同期しており、クライアント端末識別情報の読み出し（Ｓ４０１）の際に、暗号化データ送信手段３５の送信するクライアント端末１２のクライアント端末識別情報を取得する。これにより、エンドユーザに全く関知されずにアクセスし、暗号化データを交換することができる。

【００７９】

又、暗号化データ交換手段３７による暗号化データの交換は、定期的に行うことが好ましい。クライアント端末１２に格納されている時間の経過に伴い、暗号化データの盗聴される危険性が増す。そこで、一定時間以上暗号化データの交換が行われていないクライアント端末１２がある場合は、暗号化データ交換手段３７は、当該一定時間の経過を契機に、そのクライアント端末１２の暗号化データの交換を行うことが好ましい。この場合、ディザスタリカバリシステム９１のグリッドコンピューティングネットワークへのログイン中であるか否かに関わらず、暗号化データの交換を行うことが好ましい。

【００８０】

又、図２に示すように、ディザスタリカバリ装置１４が時系列情報送信手段３８をさらに有する場合、時系列情報送信手段３８は、時系列情報送信命令の入力を契機に、時系列情報記憶手段５５から時系列情報を読み出して管理端末１３へ送信する。時系列情報送信

命令は、ディザスタリカバリ装置１４に動作をさせる命令であり、データファイル暗号化かつ一体化手段３１、分割データ暗号化手段３４及び暗号化データ送信手段３５の時系列情報の送信を指示する命令である。データファイル暗号化かつ一体化手段３１、分割データ暗号化手段３４及び暗号化データ送信手段３５の時系列情報は、例えば、時系列情報記憶手段５５の記憶する時系列情報のうちの暗号鍵及びその時系列情報と、クライアント端末識別情報及びその時系列情報である。例えば、図８に示す分割データの識別情報ＦＤｍが共通する暗号鍵Ｋｍ及びクライアント端末１２のクライアント端末識別情報ＩＤ＿１２ｃｎである。クライアント端末１２に記憶されている暗号化データは、暗号鍵送信手段３６によって複数回にわたり暗号化されている場合があるので、その場合は、暗号鍵送信手段３６の送信した新たな暗号鍵及びその時刻と、当該暗号鍵の送信先のクライアント端末識別情報を、暗号鍵送信手段３６の時系列情報として送信する。又、暗号化データ交換手段３７がクライアント端末１２に記憶されている暗号化データを交換した場合は、暗号化データ交換手段３７の交換した時刻とその交換したクライアント端末１２のクライアント端末識別情報を暗号化データ交換手段３７の時系列情報として送信する。なお、時系列情報送信手段３８の送信する時系列情報には上記以外の情報が含まれていてもよい。時系列情報送信命令は、例えば、ディザスタリカバリ装置１４の有する時計が定期的に入力する。又、時系列情報送信命令は、管理端末１３の使用者によって管理端末１３に入力された時系列情報送信命令を、管理端末１３がディザスタリカバリ装置１４へ送信したものであってもよい。管理端末１３が常時最新の時系列情報を取得するため、時系列情報送信命令は頻繁に入力されることが好ましい。これにより災害が発生した場合であっても被害を最小に留めることができる。

【００８１】

このように、ディザスタリカバリ装置１４が時系列情報送信手段３８を有することで、管理端末１３は、データファイル暗号化かつ一体化手段３１、分割データ暗号化手段３４及び暗号化データ送信手段３５の時系列情報を常時取得することができる。さらに、暗号鍵送信手段３６及び暗号化データ交換手段３７の時系列情報を取得することができる。よって、マスターサーバ１１に加えてクライアント端末１２の一部が破壊された場合においても、管理端末１３は、クライアント端末１２の記憶している暗号化データを収集することで、収集した暗号化データを基に、マスターサーバ１１の格納しているデータファイルの復旧をすることができる。

【００８２】

ここで、図１に示すディザスタリカバリシステム９１のように、管理端末１３が複数備わる場合には、時系列情報送信手段３８は、複数の管理端末１３のそれぞれに暗号鍵及びクライアント端末識別情報並びにこれらの時系列情報を送信することが好ましい。管理端末１３を冗長配備することにより、災害時のデータファイルの復旧のための安全性を一層向上させることが可能となる。

【００８３】

図１に示すクライアント端末１２は、通信ネットワーク１５を介してマスターサーバ１１と接続されているコンピュータである。さらに、クライアント端末１２は、ディザスタリカバリシステム９１の構成するグリッドコンピューティングネットワークに参加をすることに同意しており、ディザスタリカバリシステム９１に参加するための設定を行ったコンピュータである。例えば、ディザスタリカバリシステム９１において固有のクライアント端末識別情報をクライアント端末１２のそれぞれが所有しており、ディザスタリカバリ装置１４にクライアント端末１２に関する情報が記憶されている。又、クライアント端末１２のそれぞれは、ディザスタリカバリシステム９１の一部として動作する際に受け付けるプログラムファイルをあらかじめ格納しており、ディザスタリカバリ装置１４からの命令を受けて命令に応じたプログラムを実行する。

【００８４】

更に、クライアント端末１２は分散設置されており、図１では、一例として、論理グループ１２Ａ、論理グループ１２Ｂ及び論理グループ１２Ｃに地理的に分散化されている例

を示した。論理グループ１２Ａ、１２Ｂ、１２Ｃはそれぞれ、災害があった場合に同時に被災しない程度にまで離れた遠隔の地に分散化されていることが好ましい。例えば、マスターサーバ１１が東京であれば、論理グループ１２Ａは京都、論理グループ１２Ｂは沖縄、論理グループ１２Ｃは北海道である。各論理グループには、複数のクライアント端末１２が含まれており、論理グループ１２Ａに含まれるｎ台のクライアント端末１２をクライアント端末１２ａ１からクライアント端末１２ａｎとして示した。論理グループ１２Ｂ及び論理グループ１２Ｃについても同様である。

【００８５】

図１０は、クライアント端末の構成を示す拡大図である。クライアント端末１２は、識別情報送信手段２１と、暗号化データ受信手段２２と、暗号化データ記憶手段２３と、を有する。クライアント端末１２は、さらに、暗号鍵更新手段２４と、暗号化データ更新手段２５と、暗号化データ転送手段２６と、を有することが好ましい。

【００８６】

識別情報送信手段２１は、遊休状態であることを判定する。遊休状態であることの判定は、例えば、クライアント端末１２に入力がない状態が所定時間継続したことを遊休状態と判定する。又、学校等の教育機関で使用されるコンピュータのように、例えば２３時から朝５時までの間は使用していないことが明らかであることが事前に判っている場合には、あらかじめ定められた時間とすることができる。又、クライアント端末１２のバックグラウンドで走る通知用の固有のソフトウェアを実装しておき、当該固有のソフトウェアが遊休状態と判定する。当該固有のソフトウェアは、例えば、プロセッサの使用率やディスクメモリの使用率が、ある閾値以下である場合に遊休状態と判定する。さらに、これらの組み合わせとしてもよい。

【００８７】

識別情報送信手段２１は、遊休状態であるとの判定を契機に、個々のクライアント端末１２に固有のクライアント端末識別情報を、ディザスタリカバリ装置１４へ送信する。識別情報送信手段２１は、クライアント端末１２に固有のクライアント端末識別情報と共に、ディザスタリカバリシステム９１の構成するグリッドコンピューティングネットワークにログインする旨を通知してもよい。ディザスタリカバリ装置１４への送信は、図１のように、ディザスタリカバリ装置１４がマスターサーバ１１に接続されている場合は、マスターサーバ１１を介してディザスタリカバリ装置１４へ送信する。又、ディザスタリカバリ装置１４がマスターサーバ１１に格納されているプログラムである場合には、マスターサーバ１１へ送信する。

【００８８】

暗号化データ受信手段２２は、ディザスタリカバリ装置１４の送信する暗号化データを受信する。暗号化データ記憶手段２３は、暗号化データ受信手段２２の受信する暗号化データを記憶する。例えば、暗号化データ受信手段２２が暗号化データ記憶命令ともに暗号化データを受信すると、暗号化データ受信手段２２は、暗号化データ記憶命令に従って、受信した暗号化データを暗号化データ記憶手段２３へ記憶する。暗号化データ記憶手段２３は、クライアント端末１２のユーザが読み出し不可能な領域又はデータ形式で記憶することが好ましい。ただし、部外者から暗号化データを読まれた場合でも、部外者は、暗号化データからデータファイルを復元することは極めて困難であるため、マスターサーバ（図１の符号１１）の格納するデータファイルが盗聴される可能性は少ない。

【００８９】

クライアント端末１２がさらに暗号鍵更新手段２４を有する場合は、暗号鍵更新手段２４は、ディザスタリカバリ装置１４の送信する新たな暗号鍵及び暗号鍵更新命令を受信する。そして、暗号鍵更新命令に基づき、暗号化データ記憶手段２３の記憶する暗号化データを、暗号鍵更新手段２４の受信した新たな暗号鍵を用いて暗号化する。そして、暗号鍵更新手段２４は、暗号化データ記憶手段２３の記憶する暗号化データを、暗号鍵更新手段２４の暗号化した暗号化データに更新する。

【００９０】

又、クライアント端末１２がさらに暗号化データ更新手段２５を有する場合は、暗号化データ更新手段２５は、ディザスタリカバリ装置１４から読出命令を受信すると、暗号化データ記憶手段２３の記憶する暗号化データを読み出し、ディザスタリカバリ装置１４へ送信する。そして、ディザスタリカバリ装置１４から新たな暗号化データ及び新たな暗号化データを記憶させる命令を受信すると、当該命令に従って新たな暗号化データを暗号化データ記憶手段２３に記憶する。

【００９１】

又、クライアント端末１２がさらに暗号化データ転送手段２６を有する場合は、暗号化データ転送手段２６は、管理端末１３の送信する暗号化データ転送命令の受信を契機に、暗号化データ記憶手段の２３記憶する暗号化データを読み出し、管理端末１３へ転送する。ここで、図１に示すディザスタリカバリシステム９１のように、管理端末１３が複数備わる場合には、暗号化データ転送手段２６は、クライアント端末１２の記憶する暗号化データを複数の管理端末１３のそれぞれへ転送することが好ましい。

【００９２】

図１に示す管理端末１３は、通信ネットワーク１５を介してマスターサーバ１１と接続され、災害時にデータファイル記憶手段５１の記憶するデータファイルを復元するものである。マスターサーバ１１と接続されることで、ディザスタリカバリ装置１４と送受信を行う。なお、管理端末１３は、通信ネットワーク１５を介してディザスタリカバリ装置１４と直接接続されていてもよい。又、管理端末１３は、通信ネットワーク１５を介してクライアント端末１２とも接続されている。

【００９３】

図１１は、管理端末の構成を示す拡大図である。図１１に示す管理端末１３は、暗号化情報送受信手段４１と、識別情報管理手段４２と、暗号化情報記憶手段４３と、暗号化データ収集手段４４と、暗号化データ復元手段４５と、を有する。

【００９４】

暗号化情報送受信手段４１は、ディザスタリカバリ装置１４から送信されたディザスタリカバリ装置１４の識別情報管理手段４２の最新の情報を受信する。そして、識別情報管理手段４２は、ディザスタリカバリ装置１４の識別情報管理手段の最新の情報を記憶する。

【００９５】

又、暗号化情報送受信手段４１は、ディザスタリカバリ装置１４の送信する暗号鍵及びクライアント端末識別情報並びにこれらの時系列情報を受信する。そして、暗号化情報送受信手段４１は、受信した暗号鍵及びクライアント端末識別情報並びにこれらの時系列情報を、暗号化情報記憶手段４３へ出力する。暗号化情報記憶手段４３は、暗号化情報送受信手段４１の受信する暗号鍵及びクライアント端末識別情報並びに時系列情報を記憶し、ディザスタリカバリ装置１４の実行するそれぞれの手段の時系列情報を収集する。

【００９６】

暗号化データ収集手段４４は、クライアント端末１２に動作をさせる暗号化データ転送命令をクライアント端末１２へ送信する。暗号化データ転送命令は、クライアント端末１２の記憶する暗号化データを、管理端末１３へ転送させる命令である。そして、クライアント端末１２から送信された暗号化データを、送信元のクライアント端末１２のクライアント端末識別情報と関連付けて記憶する。暗号化データ収集手段４４は、ディザスタリカバリシステム９１を構成するグリッドコンピューティングにクライアント端末１２がログインしているか否かに関わらず、暗号化データを記憶しているクライアント端末１２のすべてに暗号化データ転送命令を送信することが好ましい。

【００９７】

暗号化データ復元手段４５は、暗号化情報記憶手段４３の記憶する暗号鍵及びクライアント端末識別情報並びにこれらの時系列情報に基づいて、暗号化データ収集手段４４の記憶する暗号化データからデータファイルを復旧する。例えば、暗号化データ収集手段４４の記憶するクライアント端末１２のクライアント端末識別情報を、暗号化情報記憶手段４

３の記憶する最新のクライアント端末１２のクライアント端末識別情報と照合する。そして、暗号化データ収集手段４４の記憶する暗号化データの分割データの識別情報を特定する。暗号化情報記憶手段４３の記憶する暗号鍵及びクライアント端末識別情報並びに時系列情報は、分割データの識別情報ごとに暗号化した暗号鍵が管理されているので、暗号化した時系列情報に基づいて復号化し、分割データを復元する。そして、分割データの識別情報に基づいて分割データを配列し、さらに暗号化情報記憶手段４３の記憶する暗号鍵を用いて復号化することで、データファイルを復旧する。このように、ディザスタリカバリ装置１４が時系列情報送信手段（図２の符号３８）を有することで、暗号化データ復元手段４５は、クライアント端末１２のそれぞれから収集した暗号化データに基づいて、マスターサーバ１１の記憶するデータファイルを復旧することができる。

【００９８】

なお、分割データの識別情報ごとに暗号鍵を管理しない場合であっても、暗号化データ収集手段４４の記憶する送信元のクライアント端末１２のクライアント端末識別情報を、暗号化情報記憶手段４３の記憶するクライアント端末１２のクライアント端末識別情報と照合し、暗号鍵の時系列情報とクライアント端末１２のクライアント端末識別情報の時系列情報を遡りながら復号化を繰り返すことで分割データを復元することができる。そして、データファイル分割手段（図２の符号３３）の時系列情報を基に分割データを配列し、さらにデータファイル暗号化かつ一体化手段（図２の符号３１）の時系列情報を基に復号化してデータファイルを復旧することができる。

【００９９】

ディザスタリカバリシステム９１の動作の一例について図１２及び図２を用いて説明する。図１２はディザスタリカバリシステムの動作の一例を示す流れ図である。クライアント端末１２は、遊休状態であることを判定すると（Ｓ１０１）、クライアント端末１２のそれぞれに固有のクライアント端末識別情報を、識別情報受信手段３２へ送信する（Ｓ１０２）。

【０１００】

識別情報受信手段３２は、クライアント端末１２の送信したクライアント端末識別情報を受信し（Ｓ２０１）、受信したクライアント端末１２のクライアント端末識別情報が識別情報管理手段５３にあらかじめ記憶されている否かを判定する（Ｓ２０２）。識別情報管理手段５３が記憶している場合は、ディザスタリカバリシステム９１の構成するグリッドコンピューティングネットワークの参加者としてログインを許可する。そして、識別情報管理手段５３の管理しているクライアント端末１２のクライアント端末識別情報とその参加状況を更新する（Ｓ２０４）。一方、識別情報管理手段５３が記憶していない場合には、受信したクライアント端末１２のクライアント端末識別情報を破棄する（Ｓ２０３）。識別情報管理手段５３に記憶されているクライアント端末１２のクライアント端末識別情報とその参加状況を更新することで（Ｓ２０４）、ディザスタリカバリ装置１４は、暗号化データ送信手段３５の暗号化データの送信先となるクライアント端末１２を決定することができる。又、暗号鍵送信手段３６の暗号鍵の送信先や暗号化データ交換手段３７の暗号化データを更新するクライアント端末１２についても決定することができる。

【０１０１】

クライアント端末１２は、遊休状態が終了したか否かを判定し（Ｓ１０３）、遊休状態が終了した場合には、ログオフの通知を識別情報受信手段３２へ送信する（Ｓ１０４）。識別情報受信手段３２は、クライアント端末１２からログオフの通知を受信した場合についてもクライアント端末識別情報の認証を行い（Ｓ２０２）、識別情報管理手段５３に記憶されているクライアント端末１２のクライアント端末識別情報とその参加状況を更新する（Ｓ２０４）。

【０１０２】

一方、データファイル暗号化かつ一体化手段３１は、マスターサーバ１１の記憶するデータファイルを取得し、取得したデータファイルを暗号化した後に一体化する（Ｓ２０５）。データファイル分割手段３３は、データファイル暗号化かつ一体化手段３１の暗号化

した暗号化データファイルを分割する（Ｓ２０６）。そして。分割データ暗号化手段３４がデータファイル分割手段３３の出力する分割データを暗号化する（Ｓ２０７）。暗号化データ送信手段３５は、識別情報管理手段５３を参照してログイン中のクライアント端末１２へ、分割データ暗号化手段３４の出力する暗号化データを送信する。

【０１０３】

ここで、図１に示す論理グループ１２Ａ、１２Ｂ、１２Ｃに関しては、１つの論理グループ内に、ランダムに、地域のクライアント端末１２を選定して割り当てる処理が可能であり、ランダムに地域が選ばれることが、好ましい。すなわち、本実施形態に係るこのための実施例を図１３、図１４、図１５、図１６、図１７に示す。この方法により、例えば、京都、沖縄、北海道に存在するクライアント端末１２が複数台、含まれるような、柔軟な論理グループの構成法が可能である。この方法は、特定の地域に配備されたクライアント端末１２群が、同時に、破壊、あるいは、使用不可の状態に陥った場合にも、もとのデータの回復確率を向上させるだけでなく、情報の秘匿性を一層、向上させることも可能となる。従って、論理グループ１２Ａ、１２Ｂ、１２Ｃに帰属させるクライアント端末１２は、例えば図１３、図１４、図１５、図１６、図１７に示した実施例を用いて、選択する方法をとり、可能な限り、ランダムに地域配備されたクライアント端末１２群から、選択することが好ましい。ここで、関数Ｐ（ｓ）機能は機能ｆを実現するために使用される攪拌関数の実施例であり、機能ｆはデータファイルの分割および配布先クライアント端末１２の選択を行うためのものである。また、機能$ｆ^{-1}$は、配布されたデータの復元を行うためのものである。

【０１０４】

図１３は、暗号化データを送信するまでのディザスタリカバリ装置の機能の一例を示す模式図である。図１３に示すデータファイル記憶手段５１と、データファイル暗号化かつ一体化手段３１と、データファイル分割手段３３と、分割データ暗号化手段３４と、暗号化データ送信手段３５と、通信ネットワーク１５は、前述の図１で説明したものである。データファイル暗号化かつ一体化手段３１は、データファイル記憶手段５１のデータファイルを暗号化して一体化処理関数Ｆを実施する。データファイル分割手段３３は、データファイル暗号化かつ一体化手段３１によって暗号化した上にさらに攪拌されたデータファイルを分割する。分割データ暗号化手段３４は、分割データごとに異なる暗号鍵で暗号化する。暗号化データ送信手段３５は、データファイルの分割および配布先クライアント端末の選択を行う機能ｆを行う。

【０１０５】

図１４は、データファイルの分割および配布先クライアント端末の選択を行う機能ｆの一例を示す流れ図である。図１４では、データファイルをｎ’個に分割した場合を示し、ｍは全てのクライアント端末の数を示す。まず、擬似乱数の生成器Ｇを初期化し、保存する（Ｓ６１１）。そして、データファイルを分割データ$ｘ_{0}$から分割データ$ｘ_{ｎ'-1}$までのｎ’個の分割データ$ｘ_{ｉ}$に分割する（Ｓ６１２）。そして、クライアント番号Ｓ［０］からクライアント番号Ｓ［ｍ－１］までのｍ個のクライアント番号Ｓと、データファイルの分割された分割データのｋ個のブロック番号ｒ＝（０～ｎ’－１、０～ｎ’－１、・・・０～ｎ’－１）をストアする（Ｓ６１３）。ここで、ブロック番号ｒは、ファイル分割されたブロック番号であり、０～ｎ’－１の部分がｋ個出現する。すなわちデータファイルはｎ’個に分割されていることから、ｋ＝ｍ／ｎ’の関係が成立する。例えば、ｋ＝３、ｎ’＝３の場合、ｒ＝（０、１、２、０、１、２、０、１、２）となり、０、１、２の組み合わせを３回繰り返す。このとき、クライアント端末の数ｍは３×３＝９となる。

【０１０６】

次に、ブロック番号ｒの並べ替え処理Ｐ（ｒ）と、クライアント番号Ｓの並べ替え処理Ｐ（Ｓ）を行う（Ｓ６１４）。そして、ブロック番号ｒ［ｉ］のデータ$Ｘ_{ｒ［ｉ］}$について、擬似乱数の生成器Ｇから取得した暗号鍵で暗号化し、暗号化データ$Ｙ_{ｒ［ｉ］}$を発生させる（Ｓ６１６）。そして、クライアント番号Ｓ［ｉ］のクライアント端末$Ｃ_{Ｓ［ｉ］}$へ暗号化データ$Ｙ_{ｒ［ｉ］}$を送信する（Ｓ６１７）。そして、暗号化したデータ$Ｘ_{ｒ［ｉ$

］のワード数ｌｅｎｇｔｈ（$X_{r[i]}$）を前回までのワード数Ｌに加算する（Ｓ６１８）。そして、ブロック番号ｒ［ｉ］、クライアント番号Ｓ［ｉ］、ブロックのワード数の始めL_0、及び終わりのワード数Ｌの含まれる情報ｄ［ｉ］を時系列情報として時系列情報記憶手段に出力する（Ｓ６１９）。これらの処理をすべてのクライアント端末に対して、ブロック番号ｒ［ｉ］ごとに行う。

【０１０７】

図１５は、データファイルの分割および配布先クライアント端末の選択を行う際に用いる攪拌関数Ｐ（ｓ）の一例を示す流れ図である。まず、クライアント番号Ｓ［０］からクライアント番号Ｓ［ｍ－１］までのすべてのｍ個のクライアント番号Ｓをストアする（Ｓ６０１）。そして、擬似乱数生成器Ｇから生成した擬似乱数をモジュロｍで計算し（ｍで割った余り）これをａ、ｂとして格納する（Ｓ６０３）。これはクライアント番号の配列Ｓ［ｉ］の中の二つをランダムに指定することを意味する。そして、ランダムに指定した二つのメモリＳ［ａ］，Ｓ［ｂ］の中身を入れ替える（Ｓ６０４）。これを指定回数Ｍ回繰り返す（Ｓ６０３～Ｓ６０６）。つまり配列Ｓをランダムに攪拌する。このように、上述の論理グループ１２Ａ、１２Ｂ、１２Ｃに関しては、１つの論理グループ内に、ランダムに、地域のクライアント端末１２を選定して割り当てる処理が可能であり、ランダムに地域が選ばれることが、好ましい。

【０１０８】

配布された分割データの復元について図１６及び図１７を用いて説明する。図１６は、暗号化データ復元手段の一例を示す模式図である。図１６に示す暗号化データ復元手段４５は、暗号化データを復号化する分割データ復号化手段６１と、分割データ復号化手段６１の復号化した分割データを暗号化された状態のデータファイルに復元する暗号化データファイル復元手段６２と、暗号化データファイル復元手段６２の復元した暗号化データファイルを復号化してデータファイルを復元するデータファイル復号化手段６３と、復元したデータファイルを格納するデータファイル格納手段６４を備える。分割データ復号化手段６１は、配布された分割データの復元機能f^{-1}を行う。又、データファイル復号化手段６３は、復号化と共に、データファイル暗号化かつ一体化手段（図２の符号３１）で行った一体化処理関数Ｆの逆関数のF^{-1}を行う。

【０１０９】

図１７は、配布された暗号化データ（図１４の符号$Y_{r[i]}$）の復元を行う機能f^{-1}の一例を示す流れ図である。まず、ディザスタリカバリ装置の発生した擬似乱数生成器Ｇの発生させた暗号鍵を読み込むと共に、データファイルのうちまだ入手できていないｎ’個のブロックｂのフラグを取得する（Ｓ６３１）。ここで、ｂ［ｎ’］＝｛１、１、・・・１｝の「１」は、データファイルの復元に必要なファイルが見つかっていないことを示すフラグである。一方「０」であれば、データファイルの復元に必要なファイルが見つかっていることを示す。そして、図１４で説明した情報ｄ［ｉ］のブロック番号に対応するブロック番号ｒのブロックｂ［ｒ］ごとに、フラグが「１」であるか、すなわちファイルが見つかっているか否かを判定する（Ｓ６３３）。ブロックｂ［ｒ］のフラグが「０」、すなわちファイルが見つかっていれば、次のブロック番号のブロックへ進む（Ｓ６３４）。一方、フラグが「１」であれば、ディザスタリカバリ装置から管理端末に送信された時系列情報ｄ［ｉ］のクライアント番号Ｓと、クライアント端末から収集した暗号化データY_rを読み込む（Ｓ６３５）。暗号化データY_rの受信に成功した場合（Ｓ６３６）、ブロックｂ［ｒ］のフラグを「０」とする（Ｓ６３７）。そして、次のブロックへ進む（Ｓ６３９）。一方、暗号化データY_rの読み込みが成功しなければ、次のブロック番号のブロックへ進む（Ｓ６３８）。これを繰り返して全部のブロックを取得したかどうか調べる。

【０１１０】

次に、擬似乱数生成器Ｇから暗号化の際に使用した暗号鍵を取得する（Ｓ６３９～Ｓ６４１）。ここで、取得した時系列情報ｄ［ｉ］には、本当のブロック番号ｒ［ｉ］と実際にそのブロックを配布したクライアント番号ｓ［ｉ］、ディザスタリカバリ装置がクライ

アント端末へ送信したブロックのワード数の始めＬ$_0$、及び終わりのワード数Ｌを保持しているので、ブロック番号ｒ［ｉ］の暗号化に使用した暗号鍵を取得することができる。そして、擬似乱数生成器Ｇからの暗号鍵を用いてデータＸ$_r$を復号化する（Ｓ６４２）。以上の手順をすべてのクライアント端末数ｍになるまで繰り返し（Ｓ６４３）、フラグが「１」のブロックｂがなくなると（Ｓ６４４）、データファイルの復元が可能になる。一方、フラグが「１」のブロックｂが１つでも残っている場合は、データファイルの回復は失敗となる（Ｓ６４５）。本実施形態では、遠隔地に分散配置したクライアント端末に暗号化データＹ$_r$を複数格納することができるので、１つのブロックｂに対して複数の暗号化データＹ$_r$が存在しうる。このためフラグが「０」とならないブロックｂの存在確率を極めて少なくすることができる。

【０１１１】

以上、図１に示す本実施形態に係るディザスタリカバリシステム９１の動作によって、マスターサーバ１１の記憶するデータファイルを一括して暗号化した後に、随時分割し、さらに暗号化して、遊休状態にあるクライアント端末１２のそれぞれへ暗号化データのバックアップを行うことができる。

【０１１２】

データセンタの故障時におけるファイルの復元率を見積もった。ファイルの分割数をｎ、冗長度をｍ、クライアント端末の故障率をｐ（＜＜１）とした場合、回復率は、（１－Ｐ^m）^{n}　１－ｎＰ^{m}と表せる。合計で１００ＭＢのデータファイルを２０分割し、冗長度が１０、端末の故障率が２０％である場合を想定すると、本実施形態に係るディザスタリカバリ装置の故障率Ｐは０．９９９９９８となった。また、合計で１ＧＢのデータファイルを４０分割し、冗長度が１０、端末の故障率が３３％である場合を想定すると、本実施形態に係るディザスタリカバリ装置の故障率Ｐは０．９９９３９となった。

【０１１３】

更に、暗号鍵送信手段３６は、暗号化データ送信手段３５の送信の際に（Ｓ２０９）、新たな暗号鍵及び暗号鍵更新命令をクライアント端末１２へ送信する（Ｓ２１０）。又、暗号鍵送信手段３６は、一定時間が経過すると（Ｓ２０９）、新たな暗号鍵及び暗号鍵更新命令をクライアント端末１２へ送信する（Ｓ２１０）。暗号鍵送信手段３６から暗号鍵更新命令を受信したクライアント端末１２は、新たな暗号鍵を用いて、記憶している暗号化データをさらに暗号化する（Ｓ１０７）。

【０１１４】

更に、図１２及び図２に示すディザスタリカバリシステム９１では、暗号化データ交換手段３７は、暗号化データ送信手段３５の送信の際に（Ｓ２０９）、遊休状態にあるクライアント端末１２の記憶している暗号化データ同士を交換する（Ｓ２１１）。又、暗号化データ交換手段３７は、一定時間が経過すると（Ｓ２０９）、クライアント端末１２へ読出命令を送信し、暗号化データ同士を交換し、新たな暗号化データ及びそれを記憶させる命令を送信する（Ｓ２１１）。暗号化データ交換手段３７から読出命令を受信したクライアント端末１２は、暗号化データを暗号化データ交換手段３７へ送信する。その後、クライアント端末１２は、暗号化データ交換手段３７から送信された新たな暗号化データ及びそれを記憶させる命令を受信すると、新たな暗号化データを記憶する（Ｓ１０８）。

【０１１５】

上記のように、暗号鍵送信手段３６及び暗号化データ交換手段３７は、定期的又は不定期にクライアント端末１２に記憶されている暗号化データを変更し、暗号化データの盗聴をさらに困難にする。ここで、本実施形態においては、暗号鍵送信手段３６及び暗号化データ交換手段３７のうち、暗号鍵送信手段３６のみを実行してもよいし、暗号化データ交換手段３７を実行してもよい。これらの暗号化データの分散のさせ方を、複数の遠隔地にあるクライアント端末１２のエンドユーザにとって全く関知しない時間間隔で、従前にバックアップした暗号化データとは別の内容をもつ新たな暗号化データに置換処理させれば、もともとの、一体化された、データファイルの復元は、暗号鍵送信手段３６及び暗号化データ交換手段３７の時系列情報を含む一連のシーケンスを知っている管理端末１３のみ

しか実施できない。

【０１１６】

以上説明したように、本実施形態に係るディザスタリカバリシステム９１は、ディザスタリカバリ装置１４が、データファイル暗号化かつ一体化手段３１、データファイル分割手段３３、分割データ暗号化手段３４及び暗号化データ送信手段３５を有するので、分散設置されている複数のクライアント端末１２に、データファイルのバックアップをすることができる。ここで、データファイル暗号化かつ一体化手段３１によってランダムな状態になっているデータファイルをデータファイル分割手段３３が分割する。これにより、データファイル分割手段３３によって分割された順番を正確に再現できなければ、マスターサーバの記憶するデータファイルの解読をすることが不可能となる。更に、分割データ暗号化手段３４が、乱数となっている分割データをさらに乱数に暗号化するので、解読される可能性を極めて低くすることができる。これにより、高速なストリーム暗号を用い、安全にかつ効率的にデータファイルをクライアント端末に分散させることができる。

【０１１７】

このように、暗号化されているデータファイルを適切な大きさに分割し、更に、それらの分割された分割データを地理的に異なる地域に、異なる暗号鍵で暗号化して分散配備する。よって、マスターサーバ１１のある地域に災害が発生した場合であっても、分散格納されている複数のクライアント端末１２の記憶する暗号化データを基にデータファイルを復旧することができる。

【０１１８】

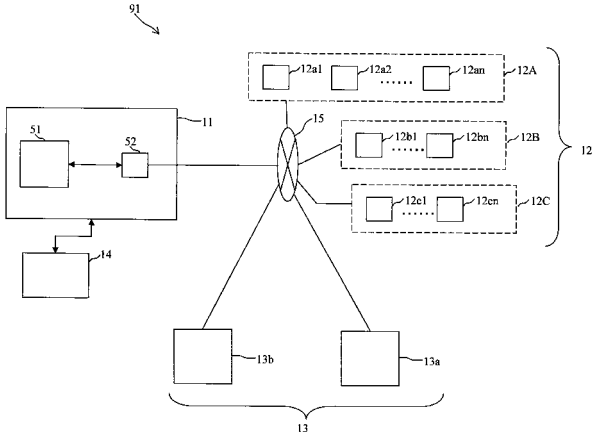
ネットワーク１５に接続された自治体や病院内にあるコンピュータセンターが保有している各種の重要データを遠隔地に分散設置されている複数のクライアント端末１２を効果的に活用して、分散配備させ、当該のコンピュータセンターが万が一の災害時に備え、効果的なバックアップを行うことができる。グリッドコンピューティング技術を用いて、更に、暗号化と暗号解読用の暗号鍵の複数の管理端末１３への効果的なバックアップを、ネットワーク技術を活用して実施し、当該の重要データが災害時に殆どが、破壊された場合においても、また、遠隔地におけるクライアント端末１２の一部または、殆どが破壊された場合においても、予め地域に分散格納されているクライアント端末１２上のデータを転送する手段を用いることにより当該重要データのバックを実現することができる。特に、遠隔地域にバックアップされる情報は、全て定期的に、かつ不定期に暗号化キーを更新させることにより、更に、当該データファイルの分割された断片情報を変更することができる。これにより、容易にはネットワーク１５上からデータの盗聴が実施できず、かつ、復元も殆ど不可能にすることができる。更に、そのデータファイルをネットワーク１５内のルータ等の交換ノード間でＶＰＮ接続による暗号化技術を活用することにより、情報の安全性・秘匿性等を高いレベルまでに向上することができる。

【産業上の利用可能性】

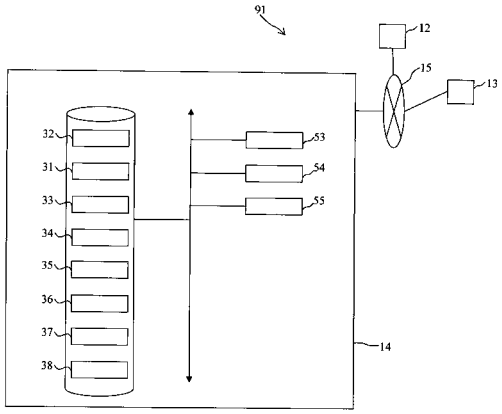
【０１１９】

本発明は、通信ネットワークを用いて、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ので、大規模かつ重要なデータベースを災害から保護することができる。

【図１】



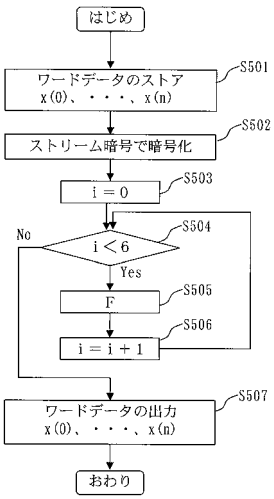
【図２】



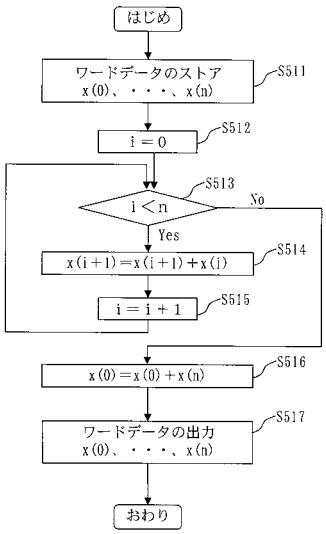
【図３】

クライアント端末識別情報	ユーザ名	論理グループ	端末状況 OK/NG
ID_12a1	ユーザ名_12a1	12A	OK
ID_12a2	ユーザ名_12a2	12A	NG
⋮	⋮	⋮	⋮
ID_12cn	ユーザ名_12cn	12C	OK

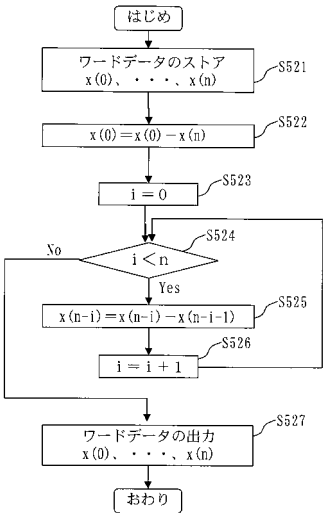
【図４】



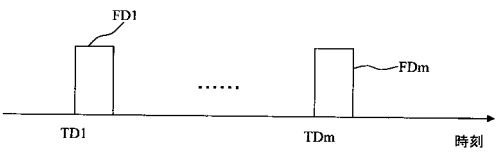
【図５】



【図６】



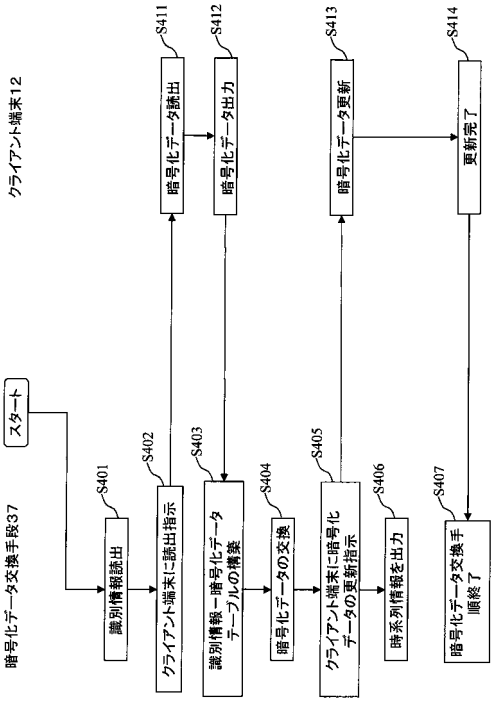
【図７】



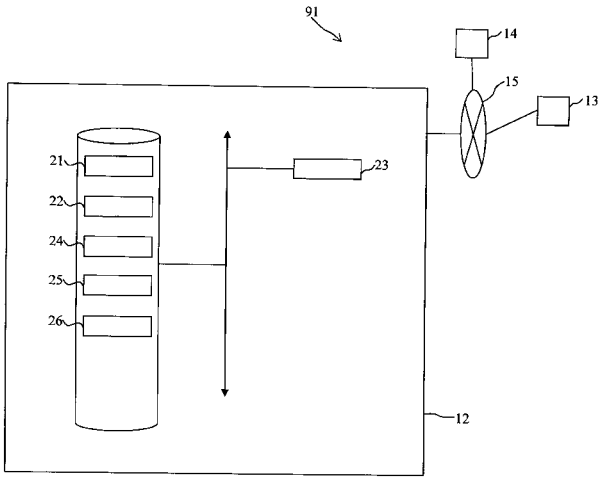
【図８】

分割データ発生時間	分割データの識別情報	暗号化データ発生時刻	暗号鍵	暗号化データ送信時間	クライアント端末識別情報
TD1	FD1	TE1	K1	TS1	ID_12a1
……	……	……	……	……	……
TDm	FDm	TEm	Km	TSm	ID_12cn

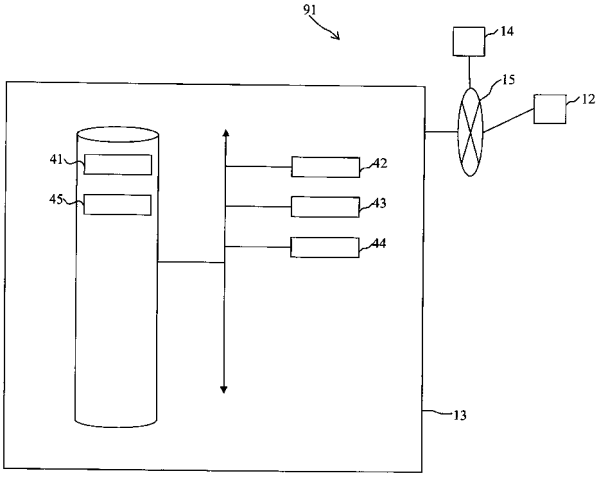
【図９】



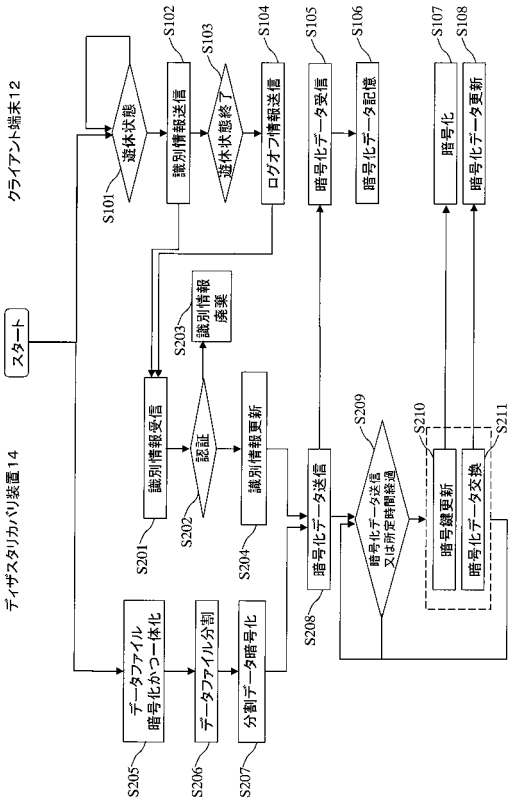
【図１０】



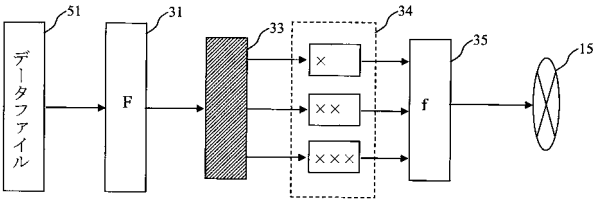
【図１１】



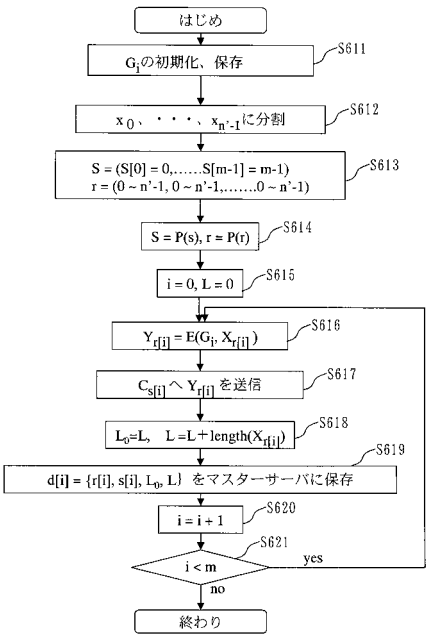
【図１２】



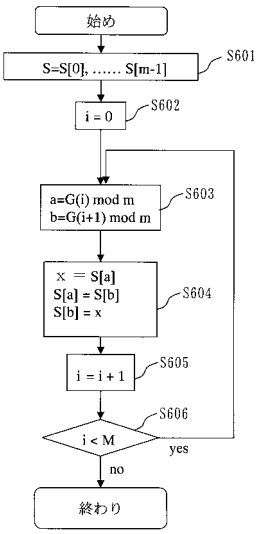
【図１３】



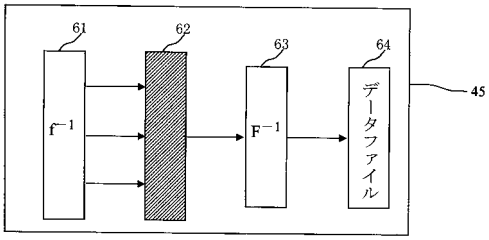
【図１４】



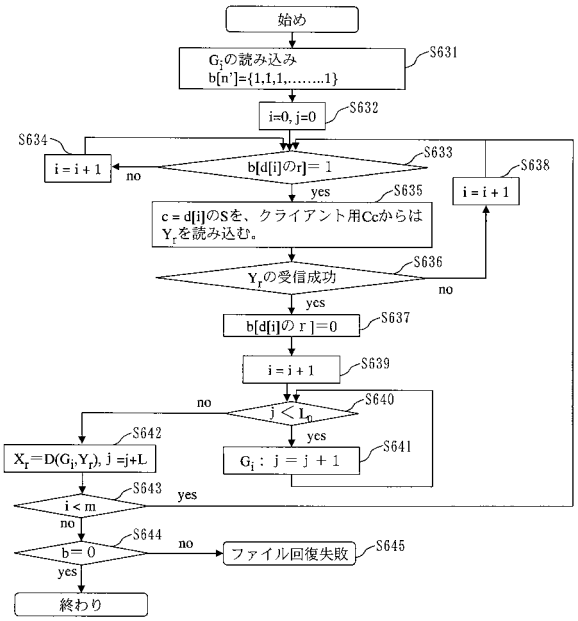
【図１５】



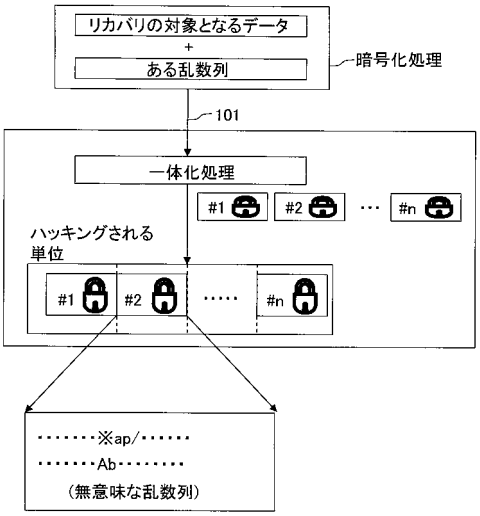
【図１６】



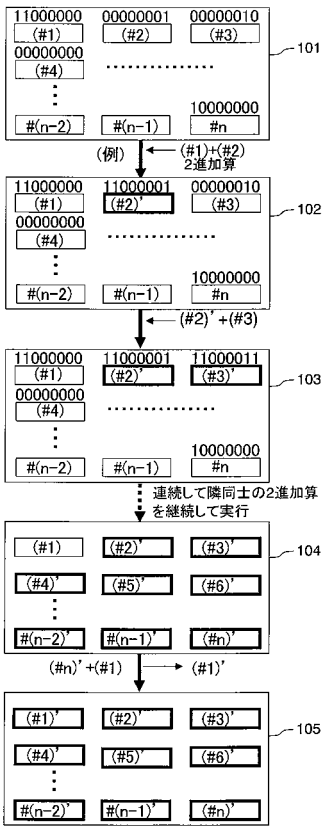
【図１７】



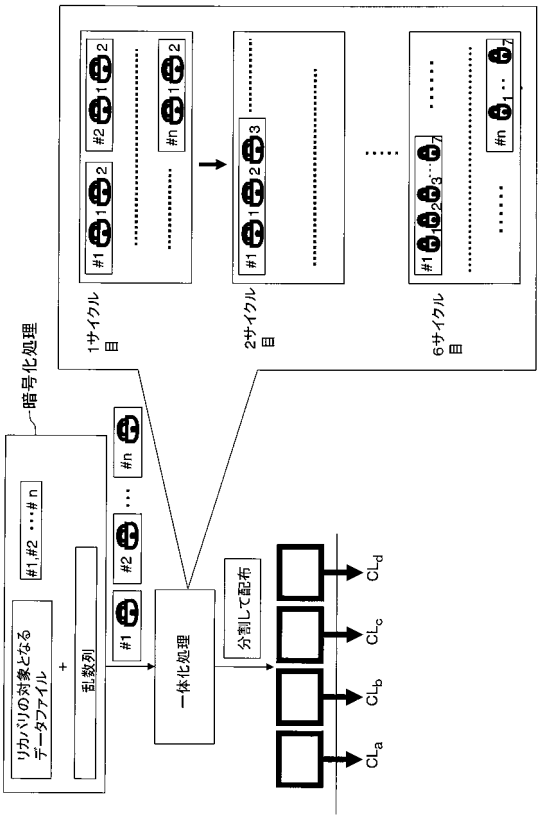
【図１８】



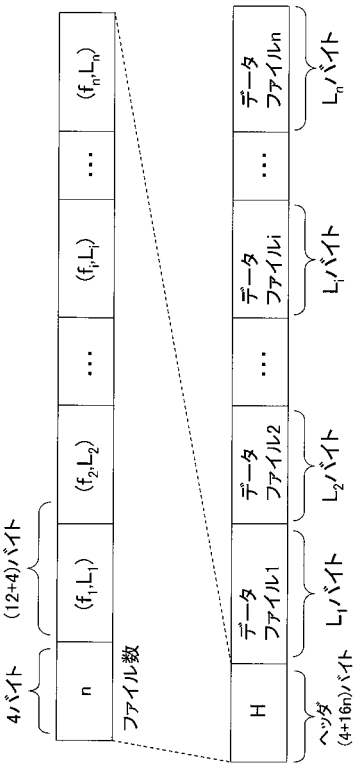
【図１９】



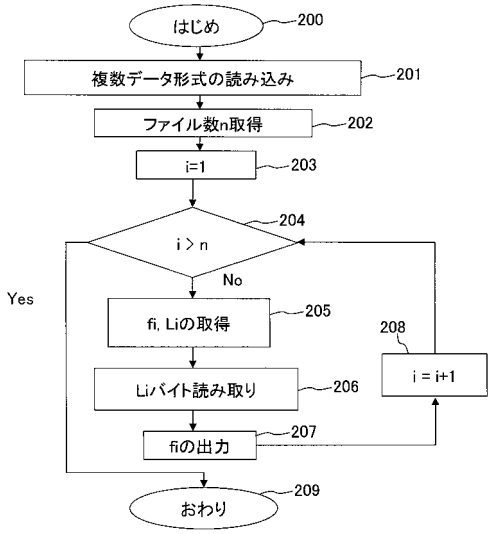
【図２０】



【図２１】


4バイト
(12+4)バイト
n
ファイル数
(f1,L1)
(f2,L2)
(fi,Li)
(fn,Ln)
H
ヘッダ
(4+16n)バイト
データファイル1
データファイル2
データファイルi
データファイルn
L1バイト
L2バイト
Liバイト
Lnバイト

【図２２】


はじめ
200
複数データ形式の読み込み
201
ファイル数n取得
202
i=1
203
i > n
204
No
Yes
fi, Liの取得
205
Liバイト読み取り
206
fiの出力
207
i = i+1
208
おわり
209

フロントページの続き

(51)Int.Cl.	FI		
	G09C	1/00	660D
	H04L	9/00	601B
	H04L	9/00	641

(72)発明者 鈴木 秀一
東京都千代田区神田錦町２丁目２番地 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丁目２番地 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丁目２番地 学校法人東京電機大学内
(72)発明者 上野 洋一郎
東京都千代田区神田錦町２丁目２番地 学校法人東京電機大学内
(72)発明者 柴田 良一
岐阜県本巣市上真桑２２３６番２ 独立行政法人国立高等専門学校機構 岐阜工業高等専門学校内

審査官 高橋 克

(56)参考文献 特開２００５－２０２４５８（ＪＰ，Ａ）
特開２００５－２０９０８６（ＪＰ，Ａ）
特開２００５－２１５７３５（ＪＰ，Ａ）
国際公開第２００４／０８８５２０（WO，Ａ１）
特開２００５－２５２３８４（ＪＰ，Ａ）
特開２００５－１８２６９１（ＪＰ，Ａ）
特開平１１－０６５９１１（ＪＰ，Ａ）
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，電子情報通信学会２００７年総合大会講演論文集 通信２，社団法人電子情報通信学会，２００７年，B-7-193，pp.283
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，Vol.107，No.403，pp.1-6
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書，財団法人ソフトピアジャパン，２００７年，Vol.11，No.4，pp.1-28，ＵＲＬ，http://www.softopia.or.jp/rd/pdf/research/h18_report_04.pdf

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
G06F 12/00
G09C 1/00
H04L 9/08
H04L 9/14