

(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 W02007/111086
 (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 官保 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

10

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、

20

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、

30

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。

40

【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段と、

50

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、

10

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】

20

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、

30

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、

40

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

50

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

10

20

30

40

50

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、主ノ副の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、主ノ副の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

10

20

30

40

50

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。

【 0 0 1 0 】

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。

【 0 0 1 1 】

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。

【 0 0 1 2 】

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。

【 0 0 1 3 】

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。

【 0 0 1 4 】

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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。

10

【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

20

【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。

30

【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。

40

【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

50

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

10

20

【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。

30

【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。

40

50

【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

10

20

30

40

50

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。

10

【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
- 12 A、12 B、12 C 論理グループ
- 13 管理端末
- 14 ディザスタリカバリ装置 20
- 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 30
- 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 40
- 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 50

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。

10

【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

20

30

【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。

40

【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

50

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。

10

【 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 】

20

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。

30

【 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。

40

【 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

50

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。ここでいう演算処理は、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

10

20

30

40

50

しているので、「・・・ a p / ・・・ A b ・・・」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、例えばデータピース#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8bitxn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11000000、データピース#2が00000001、データピース#3が00000010、データピース#4が00000000、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11000011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わせを発見することは殆ど困難となる。仮に、正しい組み合わ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。

10

【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。

20

【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。

30

【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。

40

【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

50

、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 ($i = 1 \sim n$) 及びデータファイルの長さ L_i ($i = 1 \sim n$) 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、 $(4 + 16 \times n)$ 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

10

20

30

40

50

が20の場合、ファイルの並べ方の組み合わせは、 $20! \cdot 2^{61} \cdot 10^{18}$ となる。この組み合わせ数は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わせは、 $40! \cdot 2^{160} \cdot 10^{47}$ となる。この組み合わせ数は、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わせは、 $80! \cdot 2^{400} \cdot 10^{120}$ となる。この組み合わせ数は、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わ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、正しい組み合わ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。

10

【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のが好ましい。例えば、時刻T_{Dm}に分割された分割データについて識別情報F_{Dm}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T_{Dm}と識別情報F_{Dm}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。

20

【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。

30

【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F_{Dm})と関連付けて出力することが好ましい。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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

50

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

10

20

30

40

50

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）。

10

【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きして更新する。

20

【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。

30

【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。

40

【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

50

命令は、ディザスタリカバリ装置 1 4 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 3 1、分割データ暗号化手段 3 4 及び暗号化データ送信手段 3 5 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 3 1、分割データ暗号化手段 3 4 及び暗号化データ送信手段 3 5 の時系列情報は、例えば、時系列情報記憶手段 5 5 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 F D m が共通する暗号鍵 K m 及びクライアント端末 1 2 のクライアント端末識別情報 I D _ 1 2 c n である。クライアント端末 1 2 に記憶されている暗号化データは、暗号鍵送信手段 3 6 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 3 6 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 3 6 の時系列情報として送信する。又、暗号化データ交換手段 3 7 がクライアント端末 1 2 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 3 7 の交換した時刻とその交換したクライアント端末 1 2 のクライアント端末識別情報を暗号化データ交換手段 3 7 の時系列情報として送信する。なお、時系列情報送信手段 3 8 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 1 4 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 1 3 の使用者によって管理端末 1 3 に入力された時系列情報送信命令を、管理端末 1 3 がディザスタリカバリ装置 1 4 へ送信したものであってもよい。管理端末 1 3 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。

【 0 0 8 1 】

このように、ディザスタリカバリ装置 1 4 が時系列情報送信手段 3 8 を有することで、管理端末 1 3 は、データファイル暗号化かつ一体化手段 3 1、分割データ暗号化手段 3 4 及び暗号化データ送信手段 3 5 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 3 6 及び暗号化データ交換手段 3 7 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 1 1 に加えてクライアント端末 1 2 の一部が破壊された場合においても、管理端末 1 3 は、クライアント端末 1 2 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 1 1 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。

【 0 0 8 2 】

ここで、図 1 に示すディザスタリカバリシステム 9 1 のように、管理端末 1 3 が複数備わる場合には、時系列情報送信手段 3 8 は、複数の管理端末 1 3 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 1 3 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。

【 0 0 8 3 】

図 1 に示すクライアント端末 1 2 は、通信ネットワーク 1 5 を介してマスターサーバ 1 1 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 1 2 は、ディザスタリカバリシステム 9 1 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することに同意しており、ディザスタリカバリシステム 9 1 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 9 1 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 1 2 のそれぞれが所有しており、ディザスタリカバリ装置 1 4 にクライアント端末 1 2 に関する情報が記憶されている。又、クライアント端末 1 2 のそれぞれは、ディザスタリカバリシステム 9 1 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 1 4 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。

【 0 0 8 4 】

更に、クライアント端末 1 2 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 1 2 A、論理グループ 1 2 B 及び論理グループ 1 2 C に地理的に分散化されている例

10

20

30

40

50

を示した。論理グループ 1 2 A、1 2 B、1 2 C 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 1 1 が東京であれば、論理グループ 1 2 A は京都、論理グループ 1 2 B は沖縄、論理グループ 1 2 C 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 1 2 が含まれており、論理グループ 1 2 A に含まれる n 台のクライアント端末 1 2 をクライアント端末 1 2 a 1 からクライアント端末 1 2 a n として示した。論理グループ 1 2 B 及び論理グループ 1 2 C についても同様である。

【 0 0 8 5 】

図 1 0 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 1 2 は、識別情報送信手段 2 1 と、暗号化データ受信手段 2 2 と、暗号化データ記憶手段 2 3 と、を有する。クライアント端末 1 2 は、さらに、暗号鍵更新手段 2 4 と、暗号化データ更新手段 2 5 と、暗号化データ転送手段 2 6 と、を有することが好ましい。

10

【 0 0 8 6 】

識別情報送信手段 2 1 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 1 2 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 2 3 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。又、クライアント端末 1 2 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。

20

【 0 0 8 7 】

識別情報送信手段 2 1 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 1 2 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 1 4 へ送信する。識別情報送信手段 2 1 は、クライアント端末 1 2 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 9 1 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 1 4 への送信は、図 1 のように、ディザスタリカバリ装置 1 4 がマスターサーバ 1 1 に接続されている場合は、マスターサーバ 1 1 を介してディザスタリカバリ装置 1 4 へ送信する。又、ディザスタリカバリ装置 1 4 がマスターサーバ 1 1 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 1 1 へ送信する。

30

【 0 0 8 8 】

暗号化データ受信手段 2 2 は、ディザスタリカバリ装置 1 4 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 2 3 は、暗号化データ受信手段 2 2 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 2 2 が暗号化データ記憶命令と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 2 2 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 2 3 へ記憶する。暗号化データ記憶手段 2 3 は、クライアント端末 1 2 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 1 1) 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。

40

【 0 0 8 9 】

クライアント端末 1 2 がさらに暗号鍵更新手段 2 4 を有する場合は、暗号鍵更新手段 2 4 は、ディザスタリカバリ装置 1 4 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 2 3 の記憶する暗号化データを、暗号鍵更新手段 2 4 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 2 4 は、暗号化データ記憶手段 2 3 の記憶する暗号化データを、暗号鍵更新手段 2 4 の暗号化した暗号化データに更新する。

【 0 0 9 0 】

50

又、クライアント端末 1 2 がさらに暗号化データ更新手段 2 5 を有する場合は、暗号化データ更新手段 2 5 は、ディザスタリカバリ装置 1 4 から読出命令を受信すると、暗号化データ記憶手段 2 3 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 1 4 へ送信する。そして、ディザスタリカバリ装置 1 4 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 2 3 に記憶する。

【 0 0 9 1 】

又、クライアント端末 1 2 がさらに暗号化データ転送手段 2 6 を有する場合は、暗号化データ転送手段 2 6 は、管理端末 1 3 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 2 3 記憶する暗号化データを読み出し、管理端末 1 3 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 9 1 のように、管理端末 1 3 が複数備わる場合には、暗号化データ転送手段 2 6 は、クライアント端末 1 2 の記憶する暗号化データを複数の管理端末 1 3 のそれぞれへ転送することが好ましい。

10

【 0 0 9 2 】

図 1 に示す管理端末 1 3 は、通信ネットワーク 1 5 を介してマスターサーバ 1 1 と接続され、災害時にデータファイル記憶手段 5 1 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 1 1 と接続されることで、ディザスタリカバリ装置 1 4 と送受信を行う。なお、管理端末 1 3 は、通信ネットワーク 1 5 を介してディザスタリカバリ装置 1 4 と直接接続されていてもよい。又、管理端末 1 3 は、通信ネットワーク 1 5 を介してクライアント端末 1 2 とも接続されている。

20

【 0 0 9 3 】

図 1 1 は、管理端末の構成を示す拡大図である。図 1 1 に示す管理端末 1 3 は、暗号化情報送受信手段 4 1 と、識別情報管理手段 4 2 と、暗号化情報記憶手段 4 3 と、暗号化データ収集手段 4 4 と、暗号化データ復元手段 4 5 と、を有する。

【 0 0 9 4 】

暗号化情報送受信手段 4 1 は、ディザスタリカバリ装置 1 4 から送信されたディザスタリカバリ装置 1 4 の識別情報管理手段 4 2 の最新の情報を受信する。そして、識別情報管理手段 4 2 は、ディザスタリカバリ装置 1 4 の識別情報管理手段の最新の情報を記憶する。

【 0 0 9 5 】

又、暗号化情報送受信手段 4 1 は、ディザスタリカバリ装置 1 4 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 4 1 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 4 3 へ出力する。暗号化情報記憶手段 4 3 は、暗号化情報送受信手段 4 1 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 1 4 の実行するそれぞれの手段の時系列情報を収集する。

30

【 0 0 9 6 】

暗号化データ収集手段 4 4 は、クライアント端末 1 2 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 1 2 へ送信する。暗号化データ転送命令は、クライアント端末 1 2 の記憶する暗号化データを、管理端末 1 3 へ転送させる命令である。そして、クライアント端末 1 2 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 1 2 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 4 4 は、ディザスタリカバリシステム 9 1 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 1 2 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 1 2 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。

40

【 0 0 9 7 】

暗号化データ復元手段 4 5 は、暗号化情報記憶手段 4 3 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 4 4 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 4 4 の記憶するクライアント端末 1 2 のクライアント端末識別情報を、暗号化情報記憶手段 4

50

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。

10

【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】

20

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。

30

【0101】

40

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

50

した暗号化データファイルを分割する (S 2 0 6)。そして、分割データ暗号化手段 3 4 がデータファイル分割手段 3 3 の出力する分割データを暗号化する (S 2 0 7)。暗号化データ送信手段 3 5 は、識別情報管理手段 5 3 を参照してログイン中のクライアント端末 1 2 へ、分割データ暗号化手段 3 4 の出力する暗号化データを送信する。

【 0 1 0 3 】

ここで、図 1 に示す論理グループ 1 2 A、1 2 B、1 2 C 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 1 2 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 1 3、図 1 4、図 1 5、図 1 6、図 1 7 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 1 2 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 1 2 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 1 2 A、1 2 B、1 2 C に帰属させるクライアント端末 1 2 は、例えば図 1 3、図 1 4、図 1 5、図 1 6、図 1 7 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 1 2 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 1 2 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。

【 0 1 0 4 】

図 1 3 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 1 3 に示すデータファイル記憶手段 5 1 と、データファイル暗号化かつ一体化手段 3 1 と、データファイル分割手段 3 3 と、分割データ暗号化手段 3 4 と、暗号化データ送信手段 3 5 と、通信ネットワーク 1 5 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 3 1 は、データファイル記憶手段 5 1 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 3 3 は、データファイル暗号化かつ一体化手段 3 1 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 3 4 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 3 5 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。

【 0 1 0 5 】

図 1 4 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 1 4 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 (S 6 1 1)。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 (S 6 1 2)。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 $r = (0 \sim n'-1, 0 \sim n'-1, \dots, 0 \sim n'-1)$ をストアする (S 6 1 3)。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、 $0 \sim n'-1$ 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 $3 \times 3 = 9$ となる。

【 0 1 0 6 】

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 (S 6 1 4)。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 (S 6 1 6)。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 (S 6 1 7)。そして、暗号化したデータ $X_{r[i]}$

10

20

30

40

50

」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。

10

【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。

20

【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、 $b[n'] = \{1, 1, \dots, 1\}$ 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ら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ま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ま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。

30

40

【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

50

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 を保持しているため、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。

10

【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 ($p < 1$) とした場合、回復率は、 $(1 - p^m)^n = 1 - n p^m$ 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。

20

【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)。

30

【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)。

40

【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

50

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。

10

【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】

20

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。

30

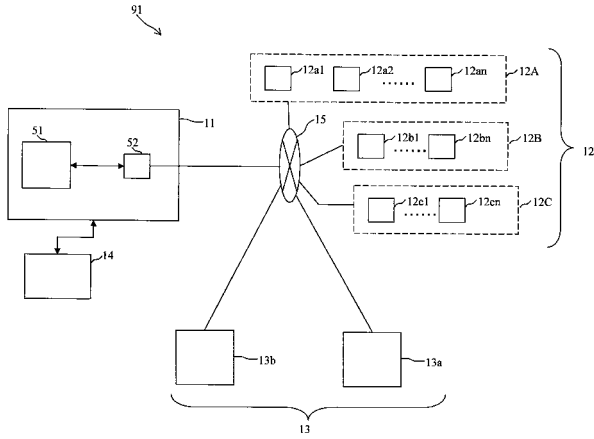
【産業上の利用可能性】

【0119】

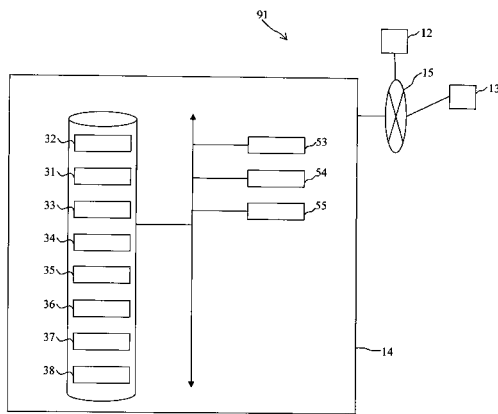
本発明は、通信ネットワークを用いて、データファイルを安全かつ効率的にバックアップすることができるので、大規模かつ重要なデータベースを災害から保護することができる。

40

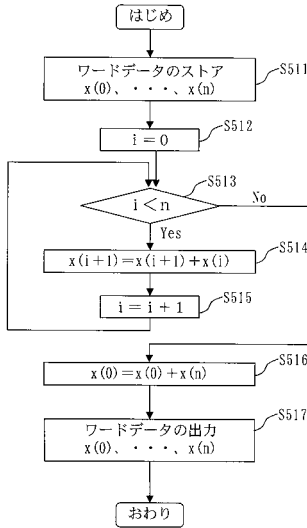
【図1】



【図2】



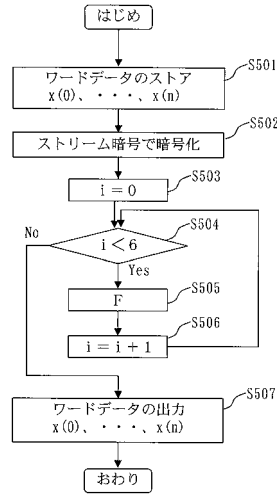
【図5】



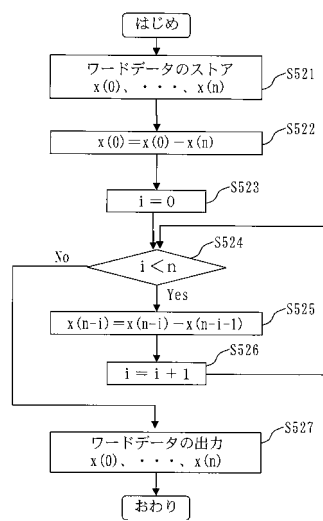
【図3】

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

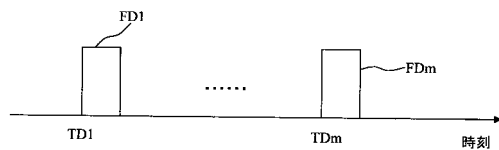
【図4】



【図6】



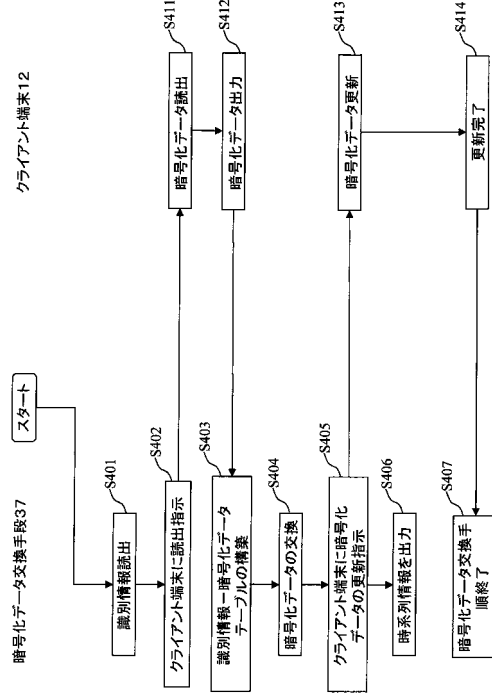
【図7】



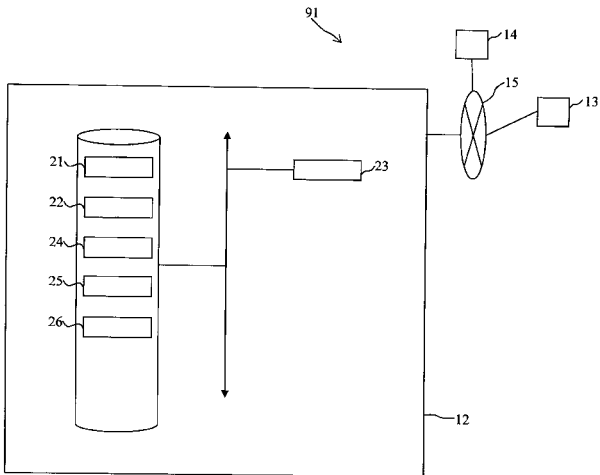
【図8】

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

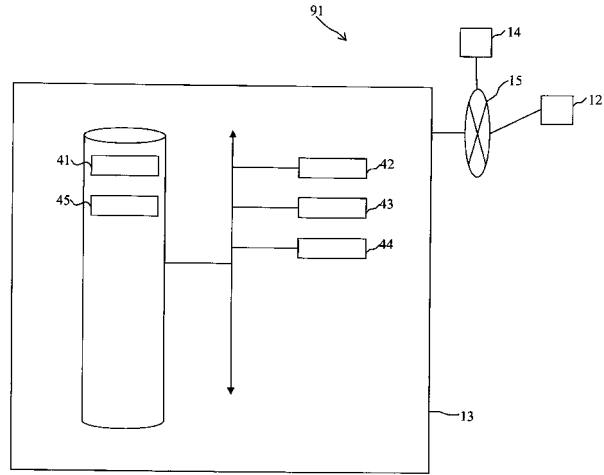
【図9】



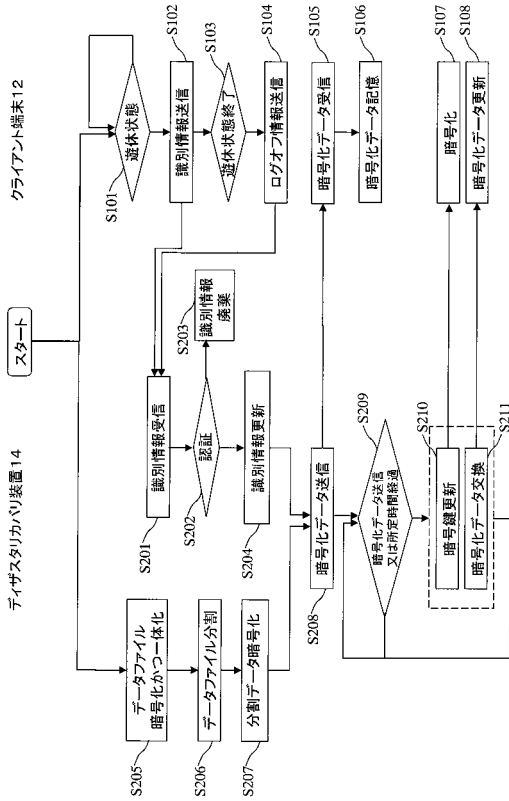
【図10】



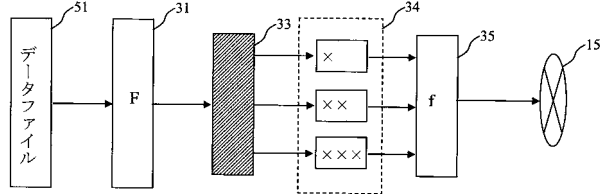
【図11】



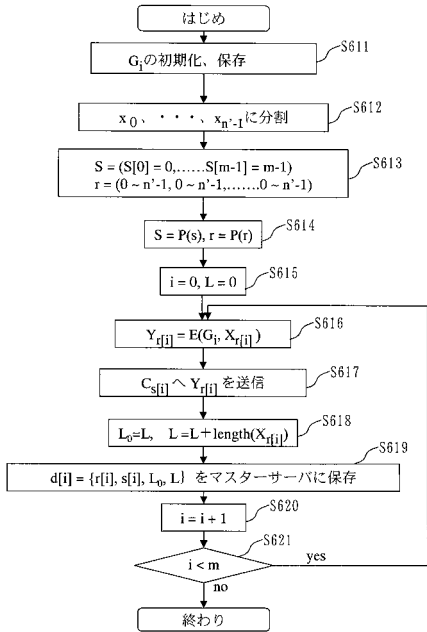
【図12】



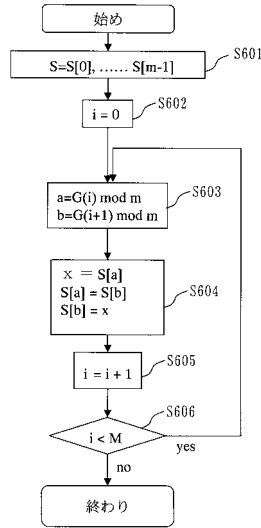
【図13】



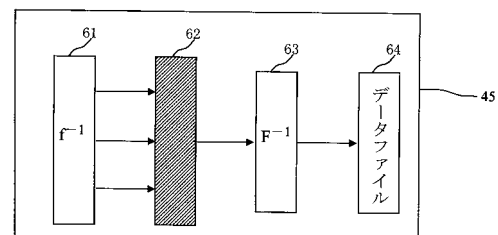
【図14】



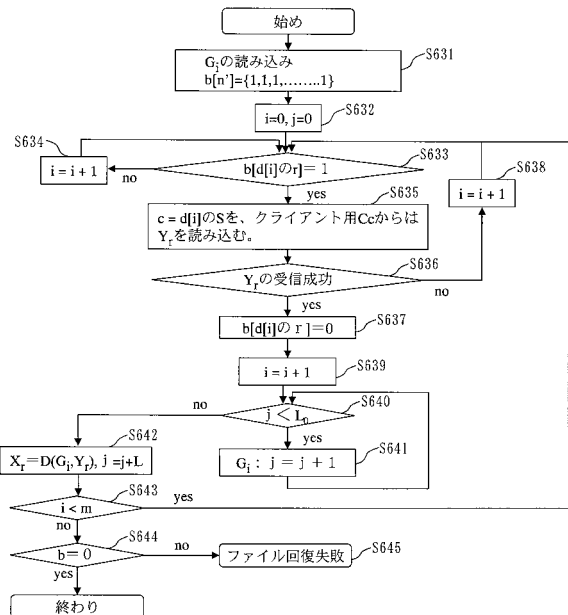
【図15】



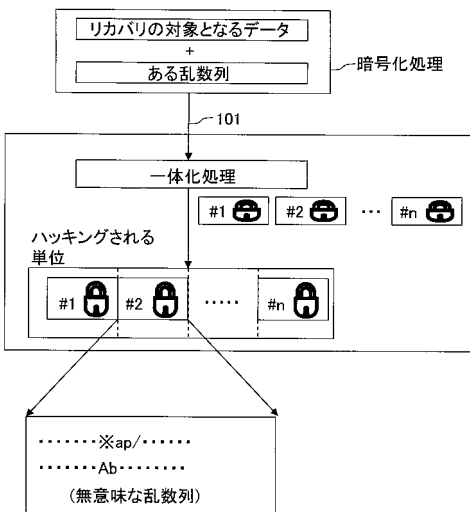
【図16】



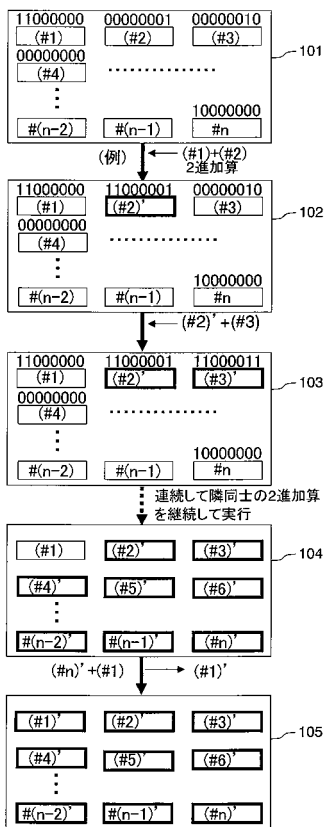
【図17】



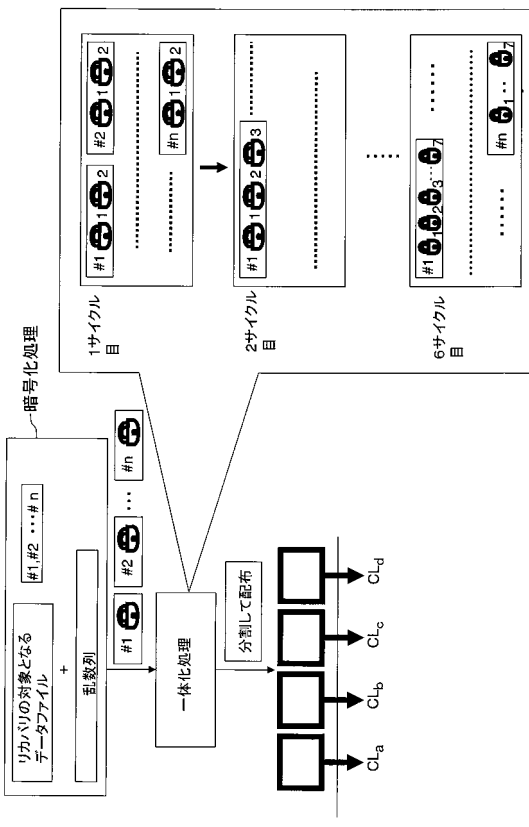
【図18】



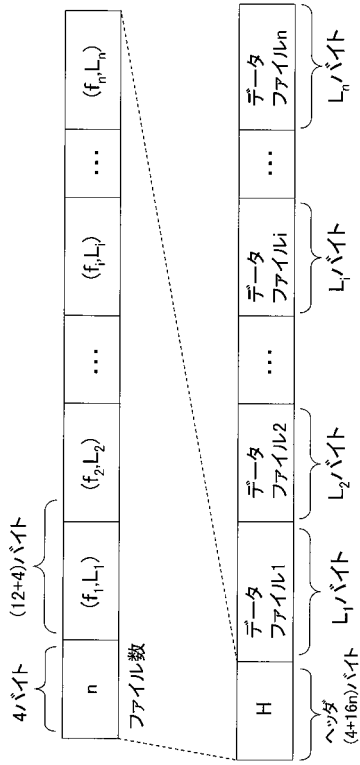
【図19】



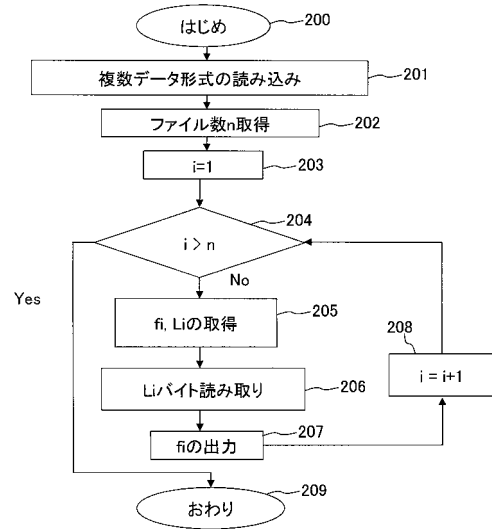
【図20】



【図 2 1】



【図 2 2】



フロントページの続き

(51)Int.Cl.

F I

G 0 9 C 1/00 6 6 0 D
 H 0 4 L 9/00 6 0 1 B
 H 0 4 L 9/00 6 4 1

(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 健介, 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 健介, 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