L-001

自律分散アーキテクチャによる データバックアップシステムにおける耐故障性の検討

阪井 凌也† 小高 知宏† 黒岩 丈介† 諏訪 いずみ† 白井 治彦‡
† 福井大学工学研究科 ‡ 福井大学工学部

1 はじめに

私達が日常でコンピュータを使用する中で, コンピュータの故障やヒューマンエラーによるデータの削除, クラッキングやコンピュータウイルスによる破損など, 常にデータの破損の可能性が潜んでいる. これらの損害を回避するために多くの個人や企業がデータのバックアップを行っているが, バックアップの信頼性を高めるには, 地理的な分散性とデータの一部が破損してもデータを復元できる冗長性が必要である. 本研究は, 自律分散アーキテクチャを用いて, 分散性, 冗長性を確保し, 耐故障性の高いバックアップシステムを構築することを目的とする. 本システムは, ネットワーク内の他の PC にデータを分散保存することでデータのバックアップを行う. 分散データは秘密分散法 [1] を用いて作成したものである. こうすることで, 保存するデータに分散性と冗長性を確保し, システムの耐故障性を向上させる. また, 本システムでは保存データのリスト等の, データの読み出しに必要なデータをすべてネットワーク上に保有する. そのため, 自身が故障した場合でも環境の復元のみでシステムへの復帰が可能である.

2 方法

本研究では, クライアント PC へのデータの保存や読み出しを各クライアント PC が自律的に動作することで行う. システムの概要図を図 1 に示す.

バックアップはシステム内の PC が互いにデータを保存しあうことで行う. 保存するデータは自身の PC 上で作成した分散データである. 分散データの作成には秘密分散法を用いることで, 保存先や通信過程でのデータの覗き見を防止する. また, 同時にそれまでバックアップしたデータのリストについても同様にバックアップをする.

読み出しの際には, 読み出したいデータの復元に必要な分散データを取得し, 自身の PC 上でデータを復元する. データの取得は, 通信可能なすべての他ユーザに対して必要データを要求し, そのデータを所有するユーザが応答することで行う.

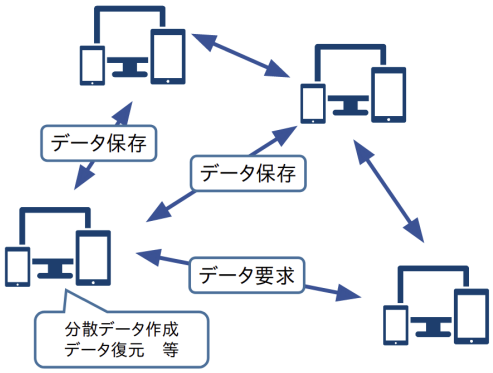

図 1: 自律分散バックアップシステムのシステム概要図

データ送信の際に必要となるルーティング情報の取得・更新は, 自身へのルーティング情報が変更された際にそのユーザが通信可能な全ユーザに対して変更を通知することで行う.

3 システム構築

構築したシステムについて述べる.

本システムは, バックアップ部, リストア部, ネットワーク部, バックグラウンド部からなる.

以下に, それぞれのシステムの概要を述べる.

3.1 バックアップ部

データのバックアップを行う. 元データから秘密分散法を用いて分散データを作成し, そのデータを他ユーザに送信する.

また, その際にバックアップリストを更新し, そのリスト自体のバックアップも行う. 尚, このリストの名前は決められたものである.

3.2 リストア部

データのリストアを行う. バックアップ部で作成したリストを元に, 自身と通信可能なユーザに対してデータの復元に必要な分散データの要求を行う. この要求は要求先のバックグラウンド部で処理され, 必要データが応答として取得できる. また, 取得した分散データを

Examination of autonomous distributed data backup system
†Ryoya Sakai †Tomohiro Odaka †Jousuke Kuroiwa
†Izumi Suwa ‡Haruhiko Shirai
†Graduate School of Engineering, University of Fukui
‡Faculty of Engineering, University of Fukui

元にデータの復元を行い, リストアを完了する. バックアップリストについても同様に読み出しが可能であるが, その際にはバックアップリストは不要である.

3.3 ネットワーク部

他 PC へのルーティング情報を管理する. 具体的には, 自身の IP アドレスなど, ルーティング情報が変更された場合に他の PC へその変更を通知する. 通知を受けっとったユーザはそのデータをバックグラウンド部で処理し, 自身の持つ各ユーザへのルーティング情報 (以下ユーザリストとする) を更新する.

3.4 バックグラウンド部

他ユーザからの情報を処理する.

リストア部でのデータの要求に対しては, 要求されたデータを自身が所有しているかを確認し, 所有していた場合は応答としてそのデータを送信する.

ネットワーク部での, ルーティング情報の更新通知に対しては, ユーザリスト内のそのユーザの古い情報を削除し, 変更後の情報を追記することで対応する.

4 実験

本システムは, システム全体に影響を及ぼすシステム障害が発生した場合にも一定以上の性能を維持している必要がある. そのため, 構築したシステムの一部が破損した場合を想定した動作実験を行った.

動作環境は, ユーザ数が 6, 使用 OS は ubuntu16.04LTS, バックアップに使用するデータは約 3.5MB である.

データのリストア時に, 一定の確率で他のクライアント PC と通信できない通信障害が発生すると想定して, それぞれの障害発生率での分散データの取得率, データの復元率を計測した.

通信障害の発生率は 1%,30%,50%,70%である. データの保存回数は 1000 回であり, 読み出しの際には 1000 個のバックアップデータを 1 つずつ読みだす. 通信障害はその各読み出しに対して一定確率で発生する.

計測した結果を表 1, 表 2, 表 3 に示す.

表 1 の”取得できた分散データ数”は, 一つの元データに対して 4 つある分散データのうち, 分散データ要求の際に取得できたデータの数である. また, 表中の”回数”は 1000 個のバックアップデータのうち, 各”取得できた分散データ数”の回数である.

表 1: 障害発生率 1%の時のデータ取得率

取得できた分散データ数	回数	割合
0	0	0
1	0	0
2	0	0
3	35	0.035
4	965	0.965

表 2: 障害発生率 50%の時のデータ取得率

取得できた分散データ数	回数	割合
0	61	0.061
1	265	0.265
2	371	0.371
3	246	0.246
4	57	0.057

表 3: 各確率でのデータの復元率

障害の発生率	読み出し自体の成功率
1%	1.000
30%	0.638
50%	0.303
70%	0.090

5 考察・まとめ

本研究では自律分散バックアップシステムを構築し, その性能評価を行った. 実験結果より障害発生率 1%の場合データの読み出しは 100%行えるため, 日常での使用では問題なく使用できることを示した. また, 各障害発生率において一定の割合で読み出しに成功しており,70%の場合でも 1 割以上の読み出しが可能である. 動作実験ではシステム全体において一定の確率で通信障害が発生する場合を想定したが, 実際に災害などでノードの破損や故障などが発生した場合は, システムが大規模になるほど全体における障害の割合は小さくなると考えられる.

本システムでは, バックアップリストに記録するのはデータの名前と日時のみであり, 保存先の情報は記録しない. 読み出しの際にもユーザリストの他にはデータ名と日時のみ使用する. 自身の初期の情報のみでバックアップリストが読み出せるため, 自身が破損した場合でもバックアップデータの復元が可能である.

参考文献

[1] 保坂範和 , 多田美奈子 , 加藤岳久 . 秘密分散法とその応用 . 東芝レビュー , Vol. 62, No. 7, pp. 2326, 2007.