

## 自律分散アーキテクチャによるデータストレージシステムの性能評価

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。

本システムでは、システムをインストールした PC がネットワーク内の他のクライアント 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。この時保存する分散データは、バックアップしたいデータを元に秘密分散 [1][2] の手法を用いて作成した分散データである。また、保存する分散データに冗長性を持たせることで耐故障性を向上させる。

ネットワーク内のクライアント PC へのルーティング情報は随時取得してデータの送受信を行うため、前回の通信からルーティング情報が変更されていてもシステムは動作する。

### 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。クライアント PC はすべて互いに通信可能なネットワーク内に存在することを前提とする。システムの概要図を図 1 に示す。

システム内の PC がお互いにデータを保存しあうことでデータのバックアップを行う。

データの保存の際には、自身の PC 上で保存したいデータを元に冗長性のある分散データを作成する。作成した分散データを、取得したルーティング情報を元に他のクライアント PC へ分散保存する。分散データは他のクライアント PC に保存されるので、覗き見な

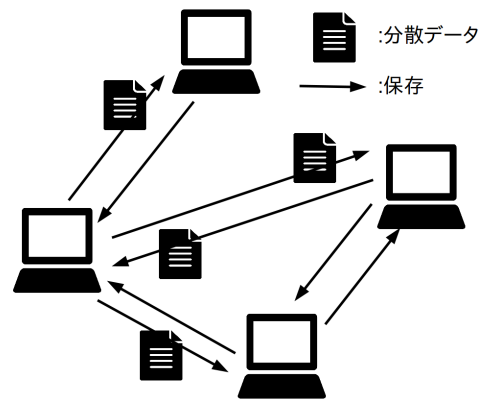


図 1: 自律分散バックアップシステムのシステム概要図

ど防ぐために秘密分散の手法を用いて作成する。また、同時に暗号化も行う。

データの読み出しの際には、読み出したいデータの復元に必要なデータを他のクライアント PC に要求する。要求したデータが必要数取得出来たらデータの復元、復号を行うことで読み出しが完了する。

データの送受信の際のルーティング情報の取得は、ブロードキャストなどでルーティング情報を要求することで行う。

### 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。

具体的には、バックアップするデータを暗号化し、そのデータを元に分散データを作成する。そのデータをいくつかのクライアント PC に送信、保存する。また、その際にバックアップしたデータのリストを作成する。

#### 3.2 リストア部

データの読み出しを行う。

具体的には、バックアップ部で作成したリストから読み出したいデータを選択し、そのデータの復元に必

要な分散データをネットワーク内のユーザに要求する。その後要求したデータが必要数取得出来たら、データの復元、復号をすることでデータの読み出しが完了する。

### 3.3 ネットワーク部

他ユーザへのルーティング情報を取得し、ユーザリストを作成する。

具体的には、ネットワーク内の全 PC にルーティング情報を要求、取得する。このデータを元に、ルーティング情報を含むユーザリストを作成する。作成したユーザリストはバックアップ部とリストア部で使用する。

### 3.4 バックグラウンド部

他ユーザからのデータの要求に対応する。

リストア部の分散データの要求に対しては、要求されたデータを自身が保有していた場合、返信としてそのデータを送信する。

ネットワーク部のルーティング情報の要求に対しては、自身へのルーティング情報を返信する。

## 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の動作実験を行った。

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。

データのバックアップ時、リストア時にそれぞれ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% である。また、データの保存回数は 1000 回である。

計測した結果を表 1、表 2、表 3 に示す。

表 1 の取得分散データ数は、一つの元データに対して 3 つある分散データのうちリストアの際に読み出せたデータの数である。また、1000 個のバックアップデータのうち、その個数のデータの読み出しに成功した回数が表中の回数である。

## 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

表 1: 障害発生率 1% の時のデータ取得率

取得分散データ数	回数	割合
0	0	0
1	0	0
2	31	0.031
3	969	0.969

表 2: 障害発生率 50% の時のデータ取得率

取得分散データ数	回数	割合
0	230	0.230
1	256	0.256
2	267	0.267
3	247	0.247

表 3: 各確率でのデータの復元率

障害発生率	読み出し成功率
1%	1.000
30%	0.791
50%	0.514

た、30% の場合約 80%、50% の場合約 50% でデータの読み出しが行えるため、地震などの災害で一定割合の PC が破損した場合でも一部のデータは読み出せることを示した。一度に複数の PC が破損する被害を受けても、データを保護できることを確認した。

本システムでは分散データを分散データ数 3、必要データ数 2 の (2,3) しきい値法で作成しているが、分散データを増やすことでより冗長性のあるシステムになると考えられる。ただし、分散データが増えると各ユーザが保存するデータの容量も多くなるため、分散データの合計容量は小さいことが望まれる。

## 参考文献

- [1] 山本博資．秘密分散法とそのバリエーション ( 符号と暗号の代数的数理 ). 数理解析研究所講義録 (2004), pp. 1931, 4 2004.
- [2] 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.