LO_001

特定少数のグループ向けP2P型バックアップシステム

P2P-type backup system for specified minority group

中居 大昭 * 岩野 桂太 * 毛利 公美 * 福田 洋治 † 白石 善明 ‡
Hiroaki Nakai Keita Iwano Masami Mohri Youji Fukuta Yoshiaki Shiraishi

1. はじめに

重要な情報を含むデータは，その複製を異なるストレージに保存して冗長度を高め，データ消失時に備えるといったファイルバックアップが一般に実施されている．ファイルバックアップを行うシステムには耐故障性と利便性が要求されることから，機器の多重化による冗長性の向上と，ファイルサーバの設置によるアクセスの容易化を図るなど，システムの構築/運用に関わるコストや管理者の負担が増加する傾向にある．

システムの構築/運用の低コスト化と冗長化を実現するためのアプローチとして，例えば，文献 [1] で示されているようなP2Pネットワークに基づくファイルバックアップに注目する．

本稿では，特定少数のメンバで構成されたグループ内で利用するための，利他的行動に基づくP2P型バックアップシステムを提案する．各メンバの操作するノードは，Hybrid型P2Pネットワーク [2] の形態で相互接続され，ピアのランデブーおよびピアの情報管理は中央サーバを介して実現される．バックアップされるファイルは，中央サーバの選択した複数のピアの余剰ディスクスペースに複製，保存される．バックアップされたデータの機密性と完全性の保証，および，そのバックアップを依頼したピアと保存先のピアの証明を，暗号/認証技術により実現し，バックアップ依頼元のピアだけがファイルの内容にアクセスできるようにしている．

提案システムでは，他のピアのファイルを保存したピアは，自身が所有するファイルを他のピアにバックアップしてもらう権利を得るという利他的な行動に基づくことで，ピアへ提供されるバックアップサービスの公平性を実現するという特徴を有する．

2. 想定環境

提案システムは特定少数のメンバ向けサービスであるが，LAN内での使用に制限するものではなく，図1のような組織の内部および外部のネットワークに接続されたホストが相互連携する環境を想定する．ノードは互いに連携して，クライアントとサーバの両方の振る舞いをするピアと中央サーバから成るHybrid型P2Pネットワークを形成する．そして，中央サーバとピアが連携してファイルバックアップサービスが実現される．

本システムは，特定少数メンバで構成されたグループ内で利用されることから，ある利用者にとって自身の不利益であるが，他の利用者の利益になるような行動をとるという，利他的行動を利用者に許容してもらうことが可能となる．ここでの利他的行動とは，余剰ディスクスペースを他の利用者のバックアップ領域として供出することを指す．そして，非匿名である特定少数のメンバ内では，悪意あるノードの存在を仮定したファイルの保存拒否や不正削除，意図的なオフライン行為，結託によるサービス妨害等は行われないことを前提にすることが可能となる．

しかしながら，メンバ間は外部のネットワークを介して接続されていることを想定しており，グループのメンバ以外の第三者による通信内容の盗聴/偽造/改ざんや，ピアおよび中央サーバへのなりすましについて検討する必要がある．また，ピアと中央サーバでの障害発生時の復旧方法も考慮しておかなければならない．

以下では，第三者による不正行為とノードの障害復旧に備え，利他的行動に基づくことでバックアップ数という観点で公平なバックアップシステムについて述べる．

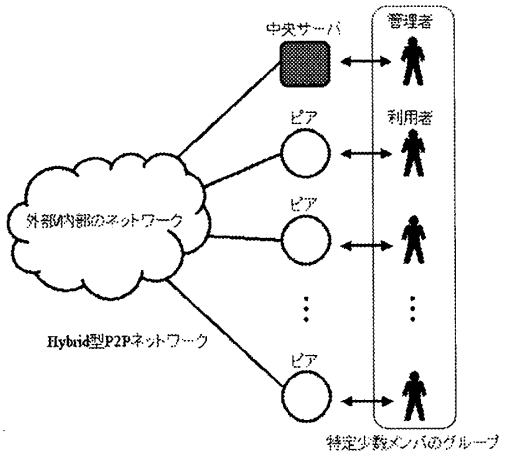

図 1: システムの想定環境

*徳島大学, The University of Tokushima
†愛知教育大学, Aichi University of Education
‡名古屋工業大学, Nagoya Institute of Technology

3. 特定少数のグループ向けP2P型バックアップシステム

3.1 構成

特定少数メンバで構成されたグループ内で利用することを想定した，利他的行動に基づくP2P型バックアップシステムを提案する．

提案システムは，次のエンティティで構成される．

中央サーバ (S) システム動作を管理するノードであり，ファイルのバックアップ，ファイルのリカバリ，ピアの障害発生の際に，オンラインのピアに各動作に対応した情報を提供する．

ピア (P_C, P_{S_i}) ファイルバックアップサービスを提供・享受するノードであり，中央サーバから提供された情報に基づいて，オンラインの他のピアと連携してファイルのバックアップ，ファイルのリカバリ，中央サーバ障害の補償処理を行う．サービスを要求するクライアントとして振る舞うピア P_C，サービスを提供するサーバとして振る舞うピア $P_{S_i}, i = 1, 2, \ldots$ が存在する．

以降の節で，中央サーバからピアへ提供される情報や，ファイルのバックアップとリカバリの動作について述べる．本システムはPGPを利用し，各ノードは，グループの他のメンバの公開鍵証明書をあからじめ所有しているものとする．なお，ピアの障害に備えて，利用者は自身の公開鍵証明書を外部メディアに保存しておく．

ノード間の通信の際には，送信側で通信内容にタイムスタンプと乱数を含め，通信内容に対して公開鍵暗号の秘密鍵で署名を行い，受信側でその署名の正当性を検証するものとする．このことは，動作を簡単に示すため次節の動作説明では省略している．

他のピアの1つのファイルを保存したノードは，他のピアに対して自身の所有する1つのファイルをバックアップしてもらう権利を得るという仕組みを採用している．初期段階では，各ピアは一定数の権利を持っているものとする．

3.2 基本動作

3.2.1 ファイルのバックアップ

ファイルのバックアップ時の動作を図2に示す．

Step-B1 バックアップ依頼元のピア P_C は，バックアップしたいファイルデータを自身だけが所有する秘密鍵を使って共通鍵暗号で暗号化し，その暗号化されたデータ d のハッシュ値 h を計算する．ここでファイル識別子 fid とファイルサイズ l，および h を記録する．次に P_C は，中央サーバ S に自身のピア識別子 pid と fid，h，l を送り，バックアップ先のピアを照会する．

Step-B2 S は，各ピアに同数のファイルが分散するように，バックアップ先のピア $P_{S_i}, i = 1, 2, \ldots, n$ を選択する．ここで P_C のバックアップ権利が0の場合は処理を中断する．次に S は，$P_{S_i}, i = 1, 2, \ldots, n$ に pid，fid，h，l を送り，バックアップするファイルをディスクに収容できるかどうかを問い合わせる．

Step-B3 $P_{S_i}, i = 1, 2, \ldots, n$ は，S にファイル収容可能/不可能のメッセージを返す．ここでファイルを収容できるピアは pid，fid，h，l を一定時間記録する．

Step-B4 S は，ファイル収容可能メッセージを返したピア $P_{S_j}, j = 1, 2, \ldots, m < n$ のピア識別子 $\mathrm{pid}_j, j = 1, 2, \ldots, m$ と pid，fid，h，l を一定時間記録する．なお，P_{S_j} は P_{S_i} の集合のうちで該当するピアの添字を整理したものである．次に S は，P_C に $P_{S_j}, j = 1, 2, \ldots, m$ と接続するための情報を提供する．

Step-B5 P_C は，$P_{S_j}, j = 1, 2, \ldots, m$ に pid，fid，h，l，d を送る．

Step-B6 $P_{S_j}, j = 1, 2, \ldots, m$ は，Step-B3 で記録したデータと Step-B5 で送られたデータが一致するか検証する．一致する場合はタイムスタンプと pid，fid，h，l，d を記録し，一致しない場合は処理を中断する．次に $P_{S_j}, j = 1, 2, \ldots, m$ は，P_C と S にバックアップ完了メッセージを送る．

Step-B7 S は，Step-B6 で送られたバックアップ完了メッセージを受けると，タイムスタンプとバックアップを完了したピア識別子 $\mathrm{pid}_j, j = 1, 2, \ldots, m$，pid，fid，h，l を記録する．次に，$P_C$ のバックアップ権利を1つ減算し，$P_{S_j}, j = 1, 2, \ldots, m$ のバックアップ権利を1つ加算する．

中央サーバには全ピアが保存しているファイル情報 (タイムスタンプ，依頼元ピア識別子，ファイル識別子，ファイルのハッシュ値，ファイルのサイズ，保存先のピア識別子) とピア情報 (ピア識別子，バックアップ権利の個数) が管理される．ピアにはファイル情報 (タイムスタンプ，依頼元ピア識別子，ファイル識別子，ファイルのハッシュ値，ファイルのサイズ，ファイルデータ) と自身の情報 (ピア識別子，バックアップ権利の個数) が管理される．

提案システムでは，他のピアの1つのファイルを保存したピアは，他のピアに対して自身の所有する1つのファイルをバックアップしてもらう権利を得るという仕組みを採用している．各ピアは，1つのファイルのバッ

クアップを依頼するとバックアップ権利が1つ減り，1つのファイルを保存するとバックアップ権利が1つ増える．初期のバックアップ権利の個数だけ，同時にファイルをバックアップすることができるが，それ以上は他のピアのファイルを保存する必要があり，特定のピアがバックアップサービスを独占するような行為を防ぐことができ，ピア毎のサービスの公平性が保たれている．

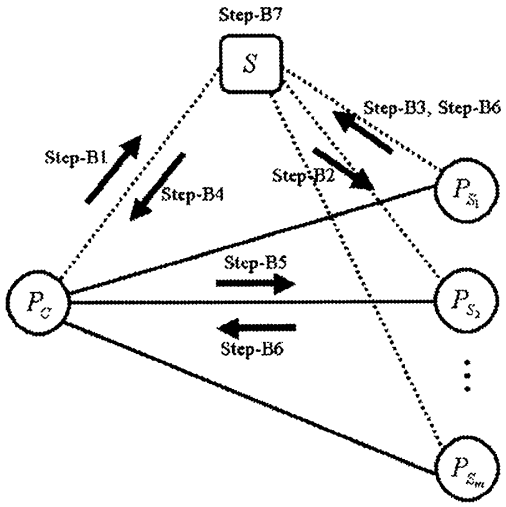

図 2: ファイルのバックアップ時の動作手順

3.2.2 ファイルのリカバリ

ファイルのリカバリ時の動作を図3に示す．

Step-R1 P_C はリカバリするファイル識別子 fid とピア識別子 pid を S に送り，バックアップしているピアの照会をする．

Step-R2 S は，P_C に $P_{S_j}, j = 1, 2, \ldots, m$ と接続するための情報を提供する．

Step-R3 P_C は，$P_{S_j}, j = 1, 2, \ldots, m$ の中からオンラインのピア P_{S_i} を探す．次に P_C は，P_{S_i} に pid，fid，h，l を送り，リカバリデータの送信を要求する．

Step-R4 P_{S_i} は，Step-B6 で記録したデータと Step-R3 で送られたデータが一致するか検証する．一致する場合は P_C に fid，h，l，d を送り，一致しない場合は処理を中断する．

Step-R5 P_C は，Step-R4 で送られて来たデータ d からファイルを復元する．

1つのピアが1つのファイルのバックアップ要求を出すと，中央サーバに選択された他の複数のピアが自身の余剰ディスクスペースにファイルを保存する．保存先のピアには同一の暗号化されたファイルが保存され，あるピアが故障したとしても，少なくとも1つのピアがオンラインならばファイルの復元が可能となる．

リカバリの依頼をするために Step-R1 で必要な fid などの情報が破損した場合には，Step-R1 の前で S に自身の pid を送信し，ファイル識別子のリストをもらうことでリカバリの処理が可能となる．また，中央サーバに障害が発生した場合，各ピアの保持するシステムの情報を集めることで，容易に復旧できる．

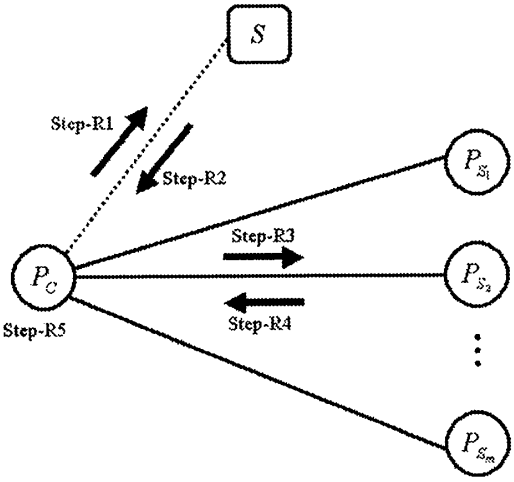

図 3: ファイルのリカバリ時の動作手順

4. システムの実装

4.1 実装システムの構成

提案システムの実装を行った．プログラミング言語には Java を使用した．P2P の環境構築には JXTA を使用した．JXTA は P2P 型アプリケーションを容易に開発できる環境を提供するプロトコル群である．

実装した中央サーバとピアの構成を図4に示す．S のバックアップ先照会部は，ファイル情報管理部とピア情報管理部と連携しながら，サーバとして振る舞う．P_C のバックアップ依頼部とリカバリ依頼部は，クライアントとして振る舞う．P_{S_i} のバックアップ部とリカバリ部は，ファイル管理部と連携して，サーバとして振る舞う．

4.2 動作実験

表1の仕様の PC を6台用意して，各 PC 上で試作したピアのプログラムを動作させて実験を行った．図5は実装システムの動作画面である．10MB のファイルを用意し，1つのピアから他の3つのピアにファイルをバックアップ，1つのピアからファイルをリカバリした際の

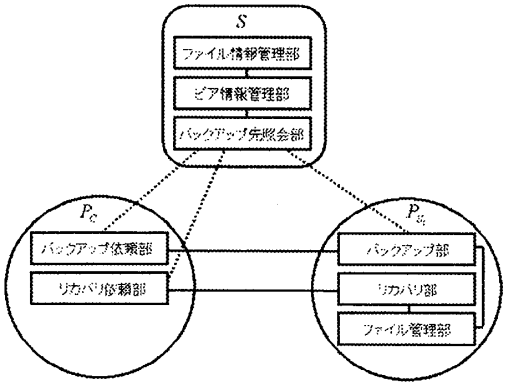

図 4: 実装システムの構成

時間を測定した．そして，バックアップに約6秒，リカバリに約2秒という結果を得た．試作システムはバックアップシステムとして利用者が不快にならない速度で動作することを確認した．

表 1: 実験用機器の仕様

OS	Windows XP Pro.
CPU	Pentium M 1.4GHz
Memory	512MB
NIC	Realtek RTL8139/810X
JDK	J2SE v.1.5.0
P2P	JXTA v.2.3.5

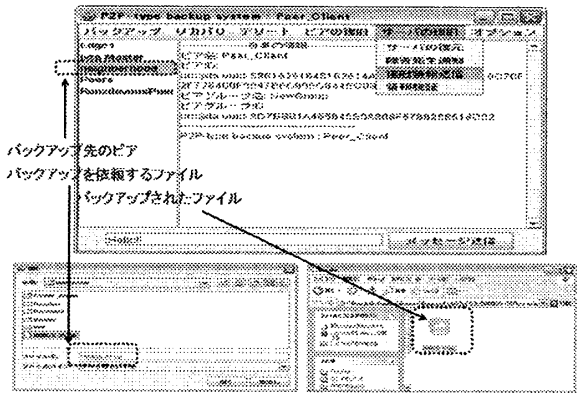

図 5: 実装システムの動作画面

5. おわりに

本稿では，特定少数のメンバで構成されたグループ内での利用を想定した，利他的行動に基づく P2P 型バックアップシステムを提案し，その実装についてまとめた．

提案システムは，Hybrid 型 P2P ネットワークによって実現しており，各ピアからバックアップ依頼のあったファイルを他のノードの余剰スペースに分散多重化して保存することで，新たなハードウェアを導入することなく低コストで耐障害性のあるファイルシステムを実現することが可能となる．

特に，提案システムは，既存のシステムとは異なり，各ピアで保存するバックアップファイルの個数に偏りが生じないように，利他的行動の概念に基づいて各ピアのバックアップ依頼を行う権利を基準に，バックアップ先を決定するという仕組みを取り入れることでサービスの公平性を保つという特徴を有する．また，バックアップされたデータの機密性と完全性の保証，および，そのバックアップを依頼したピアと保存先のピアの証明を，暗号/認証技術により実現し，バックアップ依頼元のピアだけがファイルの内容にアクセスできるような機構を与えた．さらに，提案システムを JXTA によって実装し，実用的な時間でファイルバックアップ/リカバリが可能であることを実験によって示した．

本稿で与えたバックアップシステムは，特定少数のメンバで構成した小規模グループを想定して設計したが，大規模環境に適応したファイルバックアップシステムへの拡張を今後の課題とする．

参考文献

[1] 鹿島隆行, 宇田隆哉, 伊藤雅仁, 市村哲, 田胡和哉, 星徹, 松下温, “PC 共有による安全で低コストな P2P ファイル分散システム,” 電子情報通信学会 SCIS2005 予稿集, vol.1, pp.1-6, 2005.

[2] A. Oram, PEER-TO-PEER Harnessing the Power of Disruptive Technologies, O'Reilly, March 2001.