講演番号：76　ディザスタリカバリ技術を活用したクラウドバックアップ方式の性能評価

B-6　Evaluation of Performance for Cloud Back up using Disaster Recovery Technology

齊藤　歩†　上野　洋一郎†　宮保　憲治†

Ayumi SAITO†　Youichiro UENO†　Noriharu MIYAHO†

†東京電機大学　情報環境学部　情報環境学科

†School of Information Environment, Tokyo Denki University

1. はじめに

ほとんどの社会情報活動が情報基盤上で実現され,災害やテロ発生時における社会基盤システムの脆弱性が指摘されている.一方，データバックアップ事業の継続性を可能にする技術として,伝送回線の冗長化,データセンタの二重化,複数の通信事業者への二重帰属などの対策が可能であるが，これらは災害発生時の重要データの保全に関して万全とは言い難い.そのため，電子データのバックアップを,経済的にかつ高いセキュリティのもとで実現する技術が社会的に要請されている.

本稿では，日本，米国，仏国の都市に分散したクラウドサービスを活用して，広域バックアップサービスを実現するための提案方式の概要を述べると共に，当該バックアップサービスの性能を実測結果に基づいて評価した結果を報告する.

2. 提案方式

提案方式の構成概要を図 1 に示す. 提案方式では，クラウド上で複数の地域にサーバを配備することで，経済的で安全な広域分散クラウドバックアップサービスを実現できる. バックアップ時は，ストリーム暗号と一体化処理を組み合わせ，重要データを暗号化後，複数のファイルに分割する(以降，分割ファイルを断片データと呼称). 元のメッセージに復元するために必要な鍵情報が記述されたファイル(以降，メタデータと呼称)を同時に作成する. 断片データはクラウドを活用したストレージサーバへ，メタデータは監視サーバへ転送する. 提案方式では，閾値秘密分散を用いることで断片データおよびメタデータを万全に管理する技術を活用した. 本検討では実装上の簡略化を図るため(2,3)閾値秘密分散を用いた. 復元時には，アプリケーションサーバに保存されたメタデータの送信先情報をもとに，メタデータを収集し，メタデータの情報をもとに断片データを収集し，復号する.

3. 性能評価

実験環境としては AWS，JavaScript，C++,https などを用い，当該の暗号化処理を搭載したバックアップ機能をクラウドに実装し,処理時間を計測・評価した. 具体的には，実験 1 ではファイルサイズを1MB，複製数を2とし，分割数が与える影響を評価した. 実験2にでは分割数を 40，複製数を2としファイルサイズが与える影響を評価した. 実験 1，2 では，それぞれ 5 回実施し、95%信頼区間で平均値で評価した。

図 2 より，分割数を増加させると，サーバ処理時間が増加することが判明した. ファイル分割数に比例してサーバ間通信におけるコネクション確立と切断の回数が増加したことに起因すると考えられる.一回のファイル転送におけるコネクションの確立と切断には,5 回程度のパケットデータの往復が必要である.東京-オハイオ間,東京-パリ間を10000kmとし,東京でのサーバ間通信距離は無視するとサーバ相互間の平均通信距離は約 6600 ㎞(≒(10000+10000+0)/3)となる.光ファイバーによる伝搬遅延時間を 5ns/m とするとパケットデータの往復には約 0.066s(=6600×1000×5×10^{-9}×2)が必要である. 即ち一回のパケットデータの往復時間が 66ms の場合,コネクションの確立と切断に必要な時間は分割数を D とすると,5×0.066×2D(秒)である. AES128 と同等以上の暗号強度を得るためにファイルの分割数を 40 とした場合，コネクションの確立と切断には,26(≒5×0.066×2×40)秒が必要である.

図 2 において,ファイル分割数が 40 の時の処理時間が約 30 秒であることを考慮すると，処理時間の大半はコネクションの確立と切断で占められていることが明らかとなった. すなわちネットワーク遅延時間が大きいときには、効率的なセッションの管理が必要である.

図 3 より，サーバ処理時間はファイルサイズの増加量に比べて極めて小さな増加量に留まることが判明した.この理由は,ファイルサイズを大きくすることで,暗号化および復号処理の効率が高められることに起因すると考えられ,本方式の特長の優位性を示すものと考えられる.

4. まとめ

経済的でセキュアなバックアップ方式を提案し，性能評価を実施した. 今後はディザスタリカバリ技術の他分野への適用性を検討する.

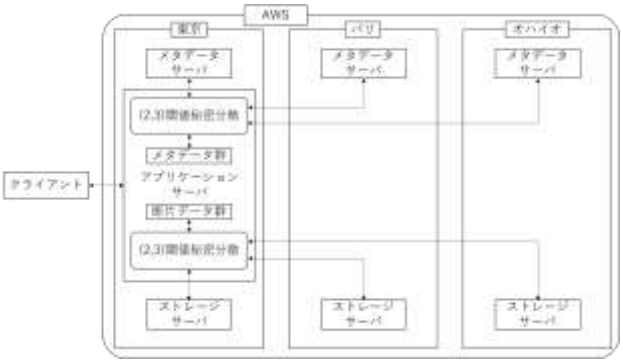

図 1　広域クラウドバックアップサービスの概要

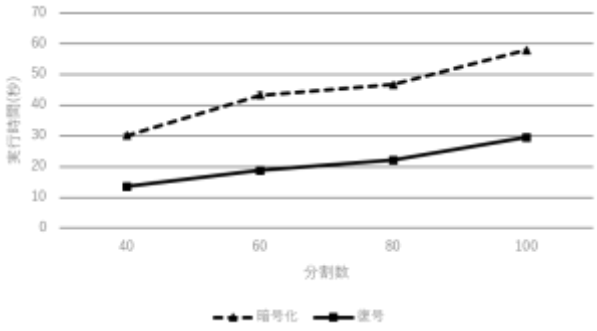

図 2　実験1　分割数を変化させたときの実行時間

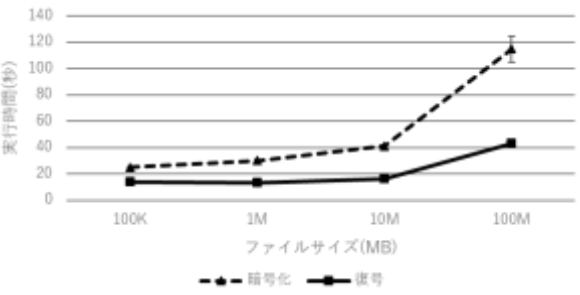

図 3　実験 2 ファイルサイズ変化時の実行時間

参考文献

[1]宮保憲治他，“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技術” 特願 2008-507405,2008