

ディザスタリカバリ技術を活用した セキュア分散型ストレージの検討

Study of secure distributed storage utilizing disaster recovery technology

永井 童夢[†] 宮保 憲治[†]
Doumu NAGAI[†] Noriharu MIYAHO[†]

[†] 東京電機大学システムデザイン工学部情報システム工学科
[†] School of System Design and Technology, Tokyo Denki University

1. はじめに

情報化社会の現代において、電子データを安全かつ高速にバックアップする技術は必要不可欠である。バックアップをする際、重要なデータは複数の異なるストレージに保存して冗長性を高めることが一般的である。しかし、セキュアで冗長なバックアップシステムを構築するには高い運用コストが必要なため、個人や小規模な組織での導入は困難な場合が多い。現在ストレージの低価格化が進み、遊休リソースを持って余すユーザも増加しつつある。そこで、P2P 技術を用いてそれらの遊休ストレージを連携させ、HS-DRT (High-Secure Disaster Recovery Technology)^[1] 技術を適用するバックアップ方式を検討した。本稿では、提案方式の概要を述べると共に、当該バックアップシステムの応答性能を実測結果に基づいて評価した結果を述べる。

2. 提案方式

提案するバックアップシステムを図1に示す。

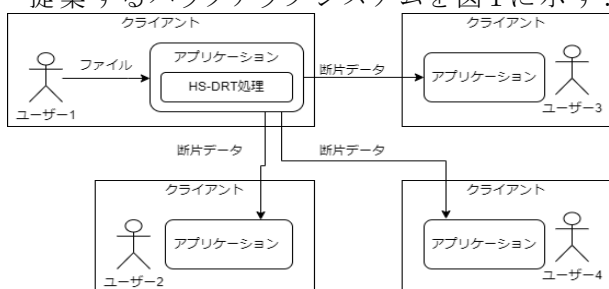


図 1. バックアップシステム構成

本提案方式では、ユーザはクライアント上にインストールしたアプリケーションでバックアップ対象ファイルをHS-DRTを活用して暗号化し、断片データ群を生成する。その後、任意の他ユーザとWebRTC(Web Real-Time Communication)によりP2P接続し、生成された断片データ群を複数のピアに分散転送する。他のユーザのストレージに保管される断片データは単体では無意味なデータであり、仮に全ての断片データの収集に成功したとしても解読するには正しく並び替えるために膨大な処理が必要となる。本方式により、ユーザの遊休ストレージを断片データ群の保管に低コストで利用し、可用性と機密性を同時に向上することが出来る。

3. 性能検証実験

ファイルの分割数を増加させ、断片ファイルの送受信数が増えた場合の処理時間の一次評価を行うため、HS-DRTによる暗号化処理時の複製数を2、ファイルサイズを10MBとし、分割数を変化させて実施した。具体的には暗号化処理後に一つ目の断片データの送信

を開始した時間から送信先のピアが全ての断片データを受信するまでの時間(送信時間)と、復号処理前に一つ目の断片データの要求メッセージ送信時から必要となる全ての断片データを受信するまでの時間(受信時間)を計測した。当該実験では実装容易性を優先したため、送信先のピアを1台としてデータ取得を行った。

4. 実験結果

実験結果を図2に示す。分割数の増加に伴い送受信に要する総時間は概ね単調増加することが分かった。この理由は分割数が増えると同時に、送受信を行う回数が増加するためである。分割数が1の場合と100の場合を比較すると、送信時間はおおよそ1.9秒、受信時間はおおよそ3.2秒増加することが分かった。送信時間は断片データを相手のピアに送信する時間のみであるが、受信時間はそれに加え、受信したい断片データごとに相手のピアに送信要求メッセージを送る時間が含まれている。送受信回数に関しては、受信時は送信時の約2倍必要であるが、この理由は分割数を増加させた際に、送信時間よりも受信時間の方が所要時間の増加幅が大きくなったことに起因すると考えられる。

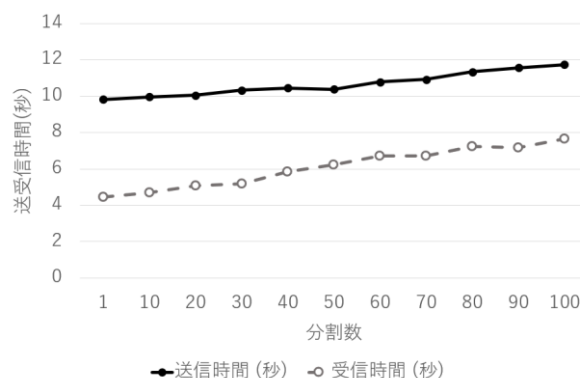


図 2. 送受信時間

7. まとめ

本実験では送信先のピアを1台としたが、ピア数を増加させた場合は、送受信時間の増加が予想される。

今後は、送信先のピアの数を増加させた場合の性能評価を行い、実用的なシステム構成の検討を行う。また、復号鍵(メタデータ)の安全な管理方法についても、併せて検討を進める予定である。

参考文献

- [1] N. Miyaho, S. Suzuki, Y. Ueno, et al. "Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications" IARIA Journals, vol.3, no.1, pp.276-278, 2010.