様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１３　日現在

機関番号：　１７１０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2017
課題番号：　２６３３００８７

研究課題名（和文）安全かつ迅速なデータ復旧を可能にする遠隔バックアップ相互保持システムの開発

研究課題名（英文）Development of an Off-Site Backup Sharing System Capable of Safe and Quick Data Recovery

研究代表者

天野　浩文（Amano, Hirofumi）

九州大学・情報基盤研究開発センター・准教授

研究者番号：８０２３１９９２

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：１つの組織が持つ情報処理システム全体を壊滅させるような大規模災害の際にも重要な電子情報を失わないためには，遠隔地にバックアップを保存することが必要である．しかし，個々の組織が個別に遠隔地のバックアップ先を確保するのは容易でない．このため，広域に分散する複数の組織が自分の秘密を他の組織に開示することなくバックアップデータを相互に保持できる仕組みを構築することが効果的である．
本研究では，このような遠隔バックアップ相互保持システムにおいて，失われた原データ全体を復元する前に安全かつ迅速にサービスを再開させることのできるような，オンデマンド再構築機能とバックグラウンド再構築機能の開発を行った．

研究成果の概要（英文）：To prevent the loss of important electronic data even after a large-scale disaster which may annihilate the whole information processing systems of an organization, it is vital to store the backup data in a remote location. However, it is not easy for individual organizations to reserve such off-site backup sites on their own. Thus it is effective to develop a framework in which multiple organizations distributed in a wide area can keep their backup data mutually without disclosing their secret to other organizations.
For this off-site backup sharing system, this grant project worked on the development of on-demand reconstruction and back-ground reconstruction features which can restart its services safely and quickly before the whole lost data is restored.

研究分野：　並列処理・分散処理

キーワード：　バックアップ　ストレージ仮想化　秘密分散法　iSCSI　オンデマンド再構築　バックグラウンド再構築

１．研究開始当初の背景

重要な電子情報のバックアップを保持することの必要性はすでに十分認識されており，バックアップ採取は通常の業務の一環として広く行われている．しかし，組織の持つほとんどすべての機能が同時に大きな損害を受けるような大規模災害の際には，災害やシステム障害などに備えて組織内で採取・保持されているバックアップ情報自体も同時に危険にさらされるおそれがある．実際に，先の東日本大震災では，ある期間に自治体に寄せられた戸籍の変更情報が文書・電子情報とも完全に失われ，その復元のために本人による再届け出が必要となった事例もある（参考：法務省ウェブサイト「東日本大震災により滅失した戸籍の再製データの作成完了について」，http://www.moj.go.jp/MINJI/minji04_00024.html，平成 23 年 4 月 26 日）．

このため，地理的に離れた地点にバックアップを保持することが重要となる．しかし，個々の組織がそのような拠点をそれぞれに確保することは決して容易ではない．

この問題を解決するためには，同じようなミッションを持つ複数の組織がバックアップ情報を相互に保持し合うような仕組みを構築することが有用である．

本研究課題の開始に先立ち，研究代表者は，電子情報のバックアップを他組織に一方的に預託するのではなく，秘密を保持したまま相互に預託しあう仕組みを構築する遠隔バックアップ相互保持システムを提案し，そのプロトタイプを開発した（科学研究費助成事業基盤研究（C），課題番号 23500048，「ストレージとネットワークの仮想化による電子情報の遠隔バックアップ技術の開発」）（以下，先行研究課題と呼ぶ）．

先行研究課題では，インターネットを経由して遠隔地の計算機にブロックデバイスのサービスを提供できる iSCSI ターゲットを改良して自動遠隔バックアップ機能を追加する方式を提案した．この方式では，既存の OS・アプリケーションに改変を加えることなく，自動遠隔バックアップ機能を利用することができる．

また，(k, n) しきい値型秘密分散法を利用して，秘密を漏洩させることなく安全にバックアップ情報を相互保持する機構を実現した．

この遠隔バックアップシステムの機能は，オープンソースの iSCSI ターゲット実装である tgt の機能を拡張することで実現した．このシステム（以下，tgt-x と呼ぶ）は，以下のような基本機能を有する．

- (k, n) しきい値型秘密分散法を用いることにより，原データと n 個のシェア（秘密分散法による符号化を適用されたバックアップデータ）のうちの($n-k$)個が失われても，残りの k 個のシェアから原データを復元することができる．バックアップ先の単一のボリュームから原データを復元することは数学的に不可能であり，災害に備えて復号に必要な暗号鍵を外部に保存する必要もない．秘密分散法の概念を図 1 に示す．

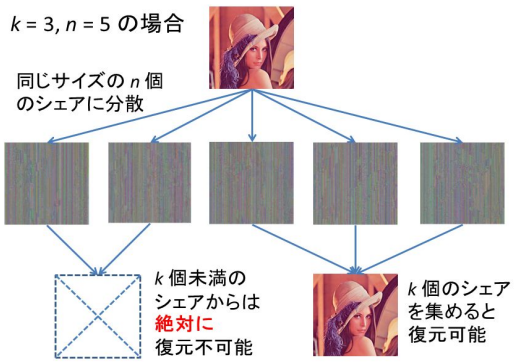

図 1：(k, n)しきい値型秘密分散法の概念

- tgt-x は，対象となる論理ボリュームに対するブロック書き込み要求が来ると，それをローカルボリュームに保存するとともに，秘密分散法を適用して得られたバックアップ用ブロックをログ情報として記録する．このログ情報を元に遅延書き込みを行うため，iSCSI プロトコルの持つ単純な再送・エラー訂正機能等では対処の不可能な比較的長時間の通信途絶や遠隔サイトのシステム保守などの際にもローカルシステムの運用は継続することができる．先行研究課題で開発した遠隔バックアップシステムの概要を図 2 に示す．

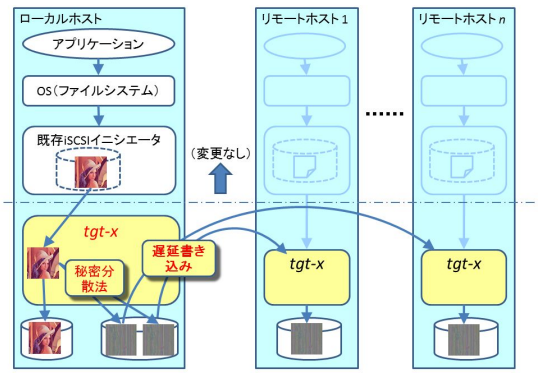

図 2：先行課題のシステムの概要

- ローカルボリューム上の 1 ブロックは，秘密分散法を適用された同じサイズのブロックとして各バックアップ先ボリュームの同じ論理ブロックアドレスに書き込まれる．ボリューム全体に秘密分散法を適用して保存することになるため，iSCSI イニシエータを有する任意の OS から利用可能である．また，ファイルの内容だけでなく，ファイル名・ファイルサイズ・所有者・タイムスタンプなどのメタデータも秘匿化することができる．さらに，遠隔バックアップ先サイトの管理者は，同じサイズのボリュームを用意し，秘密分散法により安全

に符号化された情報を複製することによって，相手の機密情報を知ることなく，古くなったストレージ装置の入れ替えを行うことも可能である．

2．研究の目的

先行研究課題の成果により，大規模災害によって重要な電子情報が失われた場合でも，それを確実に復元することが可能となった．先行課題で開発されたプロトタイプシステムは，災害発生前の定常オペレーションにおいて，原データおよび 5 箇所の遠隔バックアップ先サイトに保存されたシェアのうち 2 つまでが同時に失われるような深刻な状況でも，災害復旧後に原データを復元するのに十分な情報を安全に保存することができるようになっていた．ところが，先行研究課題は災害発生前の定常オペレーションに焦点をあてており，災害発生後の復旧オペレーションまでは十分に考慮できていなかった．このため，実用的なシステムを実現する上では，以下のような問題点が残されていた．

(1) 大規模災害発生後の混乱時に，悪意のある第三者が不当に機密情報を奪取することを防ぐ方法が考慮されていない．

(2) 機密情報が失われた場合，秘密分散法を適用された遠隔バックアップボリュームから当該ボリューム全体を復元した後でなければサービスを再開することができないため，災害発生後のサービス再開までに多大な時間が必要となる．

このうち，問題点(1)については，被災したシステムの復旧がどのような形で実現されるかによって実にさまざまな選択肢が存在しうる．

- 復旧システムは被災地に設置可能か，それとも被災を免れた他の地点に仮設置する必要があるか．
- 被災したシステムの管理者は復旧作業に従事可能か，それとも行動不能になっているのか．
- 被災システムの管理者が行動不能になっている場合，どのような基準を満たす者にその権限を委譲すべきか．
- 上記の権限委譲の判断は，誰が，いつ行うのか．

これらをすべて考慮に入れたシステムをあらかじめ実装するのは困難であると予想した．むしろ，災害の性質や規模に応じて，その場で利用可能な手段を最大限に活用して，臨機応変に復旧作業を行わざるを得ないことが多いであろう．

このため，本研究課題では，復旧システムの管理者は本システム外部の行政的・社会的な手段で別途適正に選任されるものとし，関係者の努力によって代替ハードウェアや臨時の通信回線等が確保されたのちにシステムの復旧作業が開始されるものと仮定した．すなわち，本研究課題では，問題点(2)に焦点をしぼって研究を行うこととした．

先行研究課題と本研究課題が対象とする研究範囲の違いを，図 3 に模式的に示す．

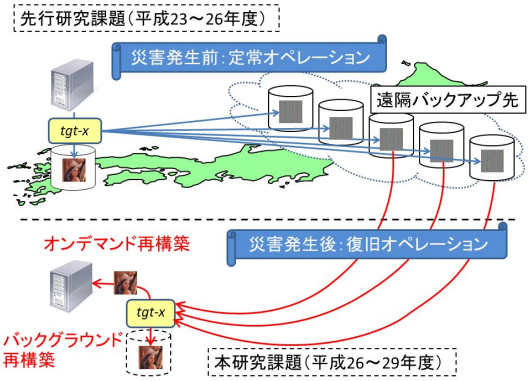

図 3：本課題と先行課題の関連

3．研究の方法

先行研究課題で開発したプロトタイプでは，原データのボリュームが健全な状態にあることを前提としていた．しかし，データを復元するのに必要なシェアは残っているので，理論的には，アプリケーションからのアクセスが来るたびに必要なブロックをその都度復元して渡す（オンデマンド再構築）のでもよいはずである．ただし，オンデマンド再構築による読み出しは通常の読み出しよりも性能が低下するので，復元されていないデータブロックをそのままいつまでも放置するのではなく，アクセスのないときに少しずつ復元しておく（バックグラウンド再構築）ことも重要である．

したがって，問題点(2)は，以下の 2 つの機能を実装することによって改善を図ることが可能である．

【オンデマンド再構築】

この機能の概要を図 4 に示す．図中の番号で示した処理の具体的な内容は以下の通りである．

①アプリケーションがデータブロックを要求する．

②iSCSI イニシエータが，tgt-x にブロックを要求する．

③tgt-x は，それがまだ復元済みでないことを知ると，データ復元デーモンにブロックを要求する．

④データ復元デーモンは，復元に必要なバックアップのブロックをリモートホストから回収し，秘密分散法を逆に適用して元データを復元し，復元されたブロックをローカルボリュームに書き込む．

⑤このとき，データ復元デーモンは，どのブロックを復元したかを示す管理テーブルも合わせて更新する．

⑥tgt-x は，復元後のデータを iSCSI イニシエータに返す．

⑦iSCSI イニシエータは，復元されたデータ

をアプリケーションに返す．

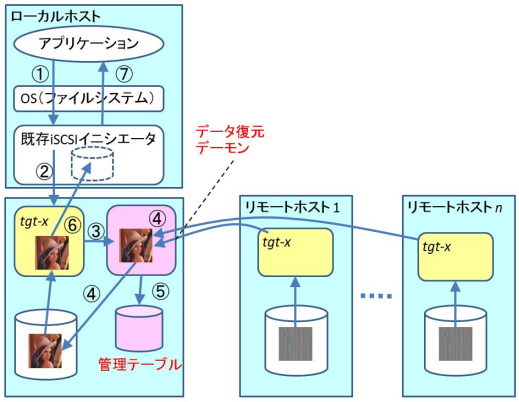

図 4：オンデマンド再構築

【バックグラウンド再構築】
この機能の概要を図 5 に示す．図中の番号で示した処理の具体的な内容は以下の通りである．この機能は，一定時間データアクセス要求が来ていないときに発動する．

①データ復元デーモンが，まだ復元されていないブロックの修復に必要なバックアップのブロックをリモートホストから回収し，秘密分散法を逆に適用して，元データを復元し，復元されたブロックをローカルボリュームに書き込む．

②このとき，データ復元デーモンは，どのブロックを復元したかを示す管理テーブルも合わせて更新する．

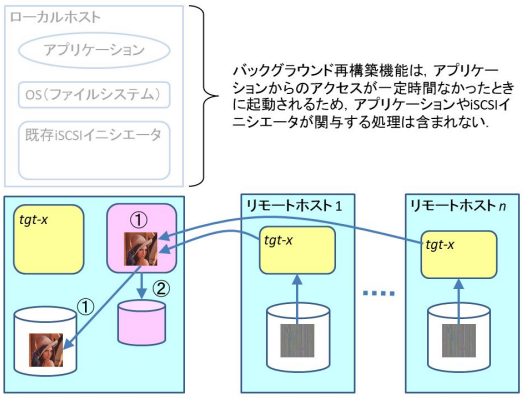

図 5：バックグラウンド再構築

4．研究成果

平成 26（2014）年度には，データ復元デーモンの中に，オンデマンド再構築を行うスレッドおよびバックグラウンド再構築を行うスレッドを設ける方式を考案し，それらお間に必要となる相互排除機能の基本設計を終えた．その成果は雑誌論文 1 件に公表することができた．

平成 27 年度には，前年度着手したオンデマンド再構築機能とバックグラウンド再構築機能およびそれらの間の相互排除機能の試作を継続した．

平成 28 年度には，これらの機能の動作の検証を中心に研究を継続したが，高負荷時の挙動についてはさらに詳細な実験を行って確認する必要のあることが判明した．そこで，研究機関を当初計画の 3 年から 1 年間延長して最終成果をまとめることとした．

平成 29 年度には，試作システムの動作の検証，サービス再開後に全データの復旧が完了するまでに要する時間の短縮について検討を行った．また，第二波・第三波の災害（余震等）によって再度秘密情報が失われる危険性に対処するため，初期災害で失われたシェアの復旧に要する時間の短縮についても検討した．しかし，年度半ばに研究代表者の病気治療のため入院・手術が必要となり，年度末までに研究成果を公開するまでには至らなかった．

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

Hirofumi Amano, Yuki Dohi, Hiromune Ikeda: “A Safe and Versatile Storage Server for Off-Site Backup”, *International Journal of Computer & Information Science (IJCIS)*, Volume 16, No. 1, pp.1-11, 2015.03

〔学会発表〕（計 0 件）

〔図書〕（計 0 件）

〔産業財産権〕
なし

〔その他〕
なし

6．研究組織

(1)研究代表者
天野　浩文（AMANO, Hirofumi）
九州大学・情報基盤研究開発センター・准教授
研究者番号：80231992

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
なし