11-IS-02

電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究

西村　浩二（広島大学）

概要
本研究では，大学のような組織の持つ電子情報が大規模災害時にも失われることのないよう，重要な電子情報を遠隔地にバックアップを保持する技術の開発を目指している．このため，ストレージ仮想化技術および秘密分散法を用いた遠隔バックアップ相互保持方式や，ネットワークにおける位置透過性の向上に関する研究を行った．また，大規模災害時のサービス停止時間を最小化するため，移動透過性の向上に関する研究も行っている．本稿では，平成 22 年度に行った研究の成果について報告する．

1. 研究の目的と意義

社会における電子情報の重要性が増すにつれ，災害やシステム障害等でそれが失われた場合の影響も深刻になる．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ほとんどすべての組織で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[1]も報告されている．

このため，地理的に離れた地点に複数の拠点を持つことのできる全国的な組織や，金銭的な負担を心配せずに外部の組織にバックアップ保持を委託できるような大企業では，地理的に離れた地点に電子情報のバックアップを保持することも多い．

一方，我が国の大学では，人事・財務・学務などに関する重要な電子情報を大量に保持しているにも関わらず，そのバックアップは組織内にとどまっていることが多い．この理由には，以下のようなものがあると推測される．

- ほとんどの部局が少数かつ近距離に分散するキャンパス内に存在していることが多く，大規模災害の影響を受けにくいほど地理的に離れた拠点を自組織内では確保しにくい．大学の規模によってはこの傾向がさらに強まる．
- 人事・財務・学務などに関する重要な情報システムがサーバから PC に至るまで伝統的に個々の大学内で管理されており，また，電子情報の保有形態や管理手順も非常に多種多様である．このような電子情報を簡単に遠隔地にて一括でバックアップするような有償サービスはまだ整っていない．
- 電子情報の複製を遠隔地にバックアップする仕組みを個々の大学が個別に自力で構築しようとすると，大学あたりの人員負担・費用負担が大きくなり過ぎる．
- 自組織の持つ重要な電子情報のすべてを一方的に他の組織に預託することに対する心理的な抵抗も大きい．

このような問題を解決するためには，将来的に，各大学が共同で費用を負担することによって個々の大学あたりの金銭的負担を軽減するとともに，同等の重要度を持つ情報を組織内で安全に保持する能力を有する大学どうしが複製情報を同等のセキュリティレベルで相互に保持し合うことによって心理的な抵抗も軽減できるような仕組みを構築することが有用である．

[1] 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．

そこで，本研究課題では，電子情報のバックアップを各大学で相互に保持しあう仕組みを構築するため，さまざまな大学が保持している電子情報の多様性とそれらの相互保持に必要となるセキュリティレベルを調査し，大学の電子情報の相互保持を実現するのに必要なバックアップ技術・ストレージ管理技術の開発を目指す.

本研究課題の成果を生かして将来各大学が業務で実際に使用する電子情報のバックアップを遠隔保存できるようになれば，それらの大学の遂行する基幹業務の大規模災害に対する耐性と復旧力を飛躍的に高めることができる.

また，現状では大学の電子情報がもっぱら各大学内部に保持されているため，すでに民間で利用の始まっている最先端のストレージ仮想化技術・ネットワークストレージ技術等はバックアップ業務に活用できていない．これを活用した遠隔バックアップサービスが構築できるようになれば，既存技術の利用範囲の拡大としても非常に意義が大きい.

さらに，組織内に電子情報を保持することについてはコンセンサスの得られている組織どうしが相互に協調することによってバックアップ情報を相互保持できる枠組みが完成すれば，今後，地上自治体等がバックアップ先を民間企業のサービスに求める場合に比べて，すでに行われている ICT 技術への投資をより有効に活用することにもつながる.

2. 当拠点公募型共同研究として実施した意義

(1) 共同研究を実施した大学名

広島大学, 山口大学, 九州大学, 九州工業大学, 佐賀大学，長崎大学，熊本大学，大分大学，宮崎大学，鹿児島大学，琉球大学，九州産業大学，福岡大学の教員・職員計 15 名

(2) 共同研究分野

大規模情報システム関連研究分野

(3) 当公募型共同研究ならではという事項など

規模・地理的分散・ミッションなどが大きく異なりその電子情報の種類や管理方法にも大きな多様性があると予想される複数の大学が参加する取り組みは，上述の取り組みを補完する上で重要な役割を担うことができる.

本研究課題に参加する共同研究者はいずれも，各大学において学内情報通信基盤の管理・運営・将来設計などを担っている情報関連センター所属の研究者であり，上記のような調査・検討に必要な知識と経験を有する．具体的には，インターネット，計算機ソフトウェア，データ工学などの分野の専門的知識を有する研究者が参画している.

また，本研究は技術開発の位置づけのため，各大学の業務で使用されている実データを実験に使用することはないが，各大学の基幹情報システムにおける各大学固有の事情を熟知している研究者が参画することには重要な意義がある.

3. 研究成果の詳細と当初計画の達成状況

(1) 研究成果の詳細について

本研究課題では，以下の３つのサブテーマについて研究を行っている.

●クラウド技術を利用した安全な分散ファイル管理システムの研究

●秘密分散法とストレージ仮想化技術に基づく遠隔バックアップ相互保持方式

●ストレージの所在を仮想化するためのネットワークの高度化に関する研究

以下，それぞれの研究成果について述べる.

サブテーマ１：クラウド技術を利用した安全な分散ファイル管理システムの研究

地理的に離れた地点にバックアップを保持することについては，設備投資や人員確保に伴う財政的な負担の増加など, 組織運営上の障壁が大きい. これに対して，クラウド技術の応用により，クラウド上に安価に，または無償でバックアップを作成することが可能となってきている．しかし，組織のセキュリティポリシーによる制限や情報システム監査対策，外部の組織に重要情報を含む電子

情報を預託することに対する心理的な抵抗感など，解決しなければならない問題が山積している．例えば以下である．

- セキュリティポリシーに違反しないこと（組織外への重要情報の持ち出し禁止）
- 自組織以外の者に見られないこと（情報漏洩防止）
- データがどこにあるかわかること（情報システム監査対応）
- データを確実に消去できること（情報システム監査対応）

これらを解決する策として，暗号や秘密分散法などを応用したコンシューマ向けのサービスが開発されている．しかし，セキュリティポリシーの問題や外部の組織に電子情報を預託する心理的な抵抗感を払拭するには，これまでと異なるアプローチが必要である．

この問題に対し，同様なセキュリティポリシーや目的を持つ組織同士が，相互にかつ安全に電子情報を保持し合う枠組みを構築することで，大規模な災害やシステム障害に備えようという取り組みが行われている．組織間が連携するシステムでは，上記に加えて次の条件を考慮する必要がある．

- 組織の都合でノードの停止・廃止ができること（システムの構成変更への適応性）

このような要求に対して，本サブテーマでは，一定の制約のもと各組織のシステム管理者がそれぞれの権限で他のシステムにファイルの管理替えができる，ファイルの分散管理手法等の検討を行った．検討したシステムの概要図を図 1 に示す．

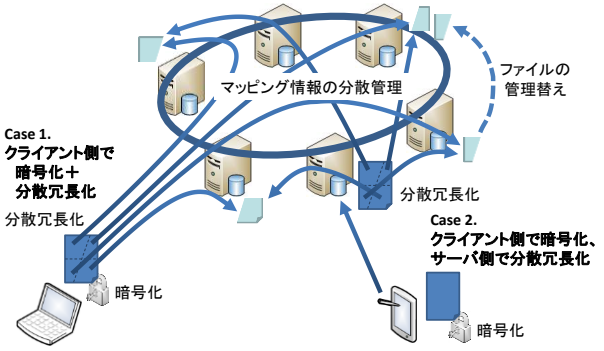

図 1：分散ファイル管理システムの概要

このシステムは，以下の参加者によるシングルサインオン(SSO)フェデレーション上に構築される（図 2）．

- ストレージ提供者(SP)
- 認証機能提供者(IdP)

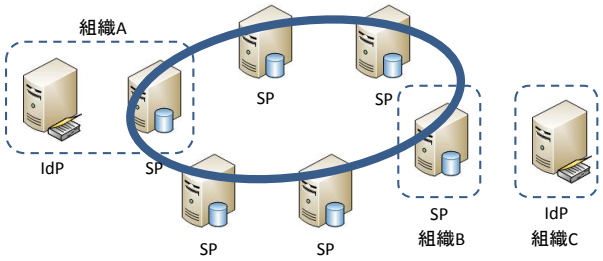

図 2：SSO フェデレーションの概要

ここで，遠隔バックアップ機能を利用しようとする組織は，以下のいずれかの形態によって分散ファイル管理に参加することができる．

- IdP と SP の両方を供出する（図中の組織 A）．
- SP のみを供出する（図中の組織 B）．
- IdP のみを供出する（図中の組織 C）．

ただし，B のような組織は C のような組織と契約し，その認証機能を利用する必要がある．また，この方式では，C のような組織と契約することのできる個人も，分散バックアップ機能を利用することができようになる．このような SP 群によるストレージクラウド上に，通常の Key Value Store (KVS)が構築されているものとし，この上に分散ファイル管理機構を構築することを考える．

ファイルを分割して格納する際，および，格納したファイルを取り出す際には，ファイル名とそのファイルのチェックサムに対してハッシュ関数を二段階で適用して，分割ファイルの名前とその格納位置を決定する．一段目のハッシュでは，分割ファイルの名前を決定する．二段目のハッシュでは，各分割ファイルの格納位置を決定する．各分割ファイルには，適切な暗号化を行って秘密情報を保護する．

このとき，ファイルの所有者は自分の所有するファイル名とそのファイルのチェックサムに対す

る一段目のハッシュ値および二段目のハッシュ値の両方を見ることができるのに対して，SP の管理者は，分割ファイルの名前とそのチェックサムに対する二段目のハッシュ値のみを見ることができるものとする（図 3）.

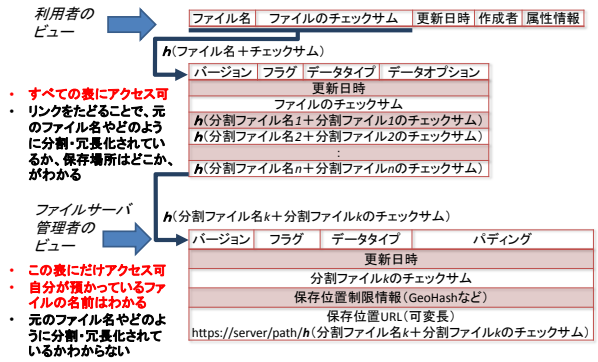

図 3：ハッシュの多段化

この方式では，ファイルの所有者は，自分のファイルがどのように分割されているか，および，それらの分割ファイルがどの SP に分散保存されているかを，リンクをたどることによってすべて知ることができる．一方で，SP 管理者は，自分の預かっている分割ファイルの名前を知ることはできるが，それの元になったファイルの名前を知ることはできない．

平成 23 年度の研究により，集中型の管理機構を持たずに SSO フェデレーションを形成しているストレージクラウド上で，情報漏洩を防止しながら分散ファイル管理機能を実現する手法が得られた．また，ハッシュの多段化によって，ファイル所有者とストレージ管理者それぞれが持つべき権限を分離できることもわかった．

サブテーマ２：秘密分散法とストレージ仮想化技術に基づく遠隔バックアップ相互保持方式

このサブテーマでは，平成 22 年度に，遠隔バックアップ機構が持つべき最低限の要件を次のように定めた．

(1) 既存の OS やアプリケーションを変更することなく利用できること．

(2) 秘密情報の内容は，そのバックアップを預かった側に決して知られないこと．

(3) 秘密情報に関するメタ情報も，そのバックアップを預かった側に決して知られないこと．

(4) 各参加組織は，外部の秘密情報のバックアップを預かるために提供するボリュームのコピー・容量拡大など，ローカルストレージの管理者が当然持つべき権限を保持できること．

そして，以上のような条件を満たすために，少なくとも以下のような機能を持つ遠隔バックアップシステムが適切であるとの結論に至り，プロトタイプの設計と開発を行った．

(a) ストレージ仮想化技術[2]を応用して，ローカルドライブと等価なアクセシビリティを Linux SCSI target framework （tgt）の機能を拡張する形で実装する．これを tgt-x と呼称する．

(b) バックアップすべき論理ボリューム全体に，暗号化ではなく秘密分散法[3]を適用し，秘密の保持およびデータ管理者とストレージ管理者の権限の分離を図る．秘密分散に用いられるアルゴリズムは，符号化・復号化を高速に行うため，各種方式の中から XOR 演算に基づく方式[4]を選択する．

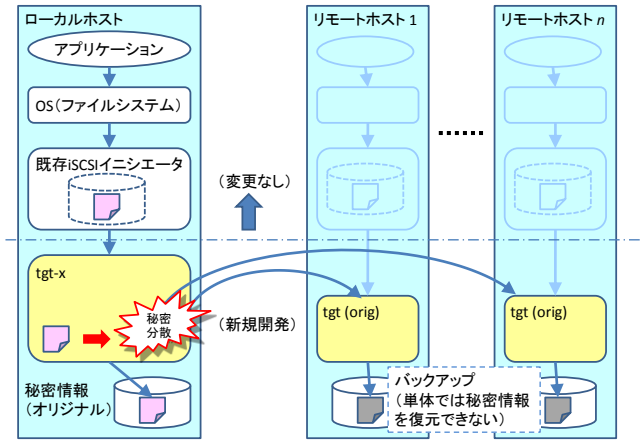

図 4：バックアップシステムの基本構成

このプロトタイプシステムの概念図を図 4 に示す．この図では，ローカルホスト上のアプリケー

[2] T. Clark: “Storage Virtualization: Technologies for Simplifying Data Storage and Management”, Addison-Wesley, 2005.
[3] 山本：「秘密分散法とそのバリエーション」，数理解析研究所講究録，第 1361 巻，pp. 19-31，2004 年.
[4] 多田，他：「しきい値 3 の秘密分散法の構成法」，情報処理学会コンピュータセキュリティシンポジウム論文集，Vol. 2，pp. 637-642，2005 年 10 月.

ションから保存される秘密情報から「シェア」と呼ばれる副次的なデータが生成され，リモートホスト 1～*n* に分散してバックアップされる様子を表している．

プロトタイプシステムにより，前述の(1)～(4)の要件を満たせることは確認できたが，実用的なシステムとしてはいくつかの機能が未実装であった．このため，平成 23 年度は，以下の機能を完成させた．

- **遅延更新機能**のサポート

プロトタイプは，tgt-x 自身がリモートのターゲットへの書き込みまでを担当しブロッキング動作を行っていたため，応答性能に大きく影響を与えていた．また，iSCSI プロトコルが備える貧弱なエラー処理機能に依存していたため，ネットワーク障害やバックアップ先ホストの運転停止等による通信途絶に対処する機能がほとんど備わっていなかった．

そこで，tgt-x がオリジナルの秘密情報（遠隔地との通信途絶の影響を受けずに書き込みが可能）を保存する際に，即時に遠隔地へのシェアの書き込みを行うのではなく，シェアとタイムスタンプからなるログ情報を保存することにした（図 5）．遠隔地へのバックアップは，この保存されたログ情報に基づき，tgt-x とは別のデーモンプロセスが非同期で実行する．

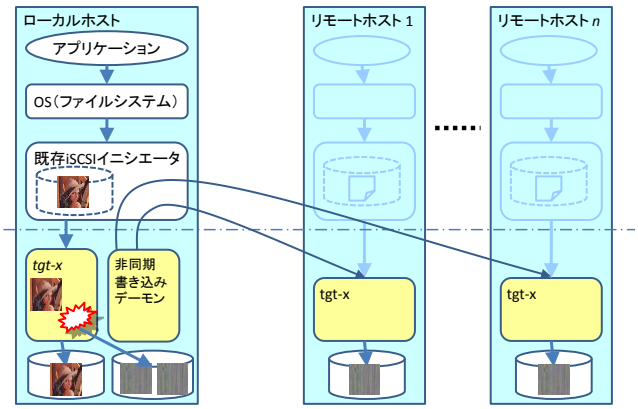

図 5：遅延書き込み機構の実装

これにより，昨年度のプロトタイプに比べ，書き込みの応答性能を約 2～10 倍程度向上させることができた．さらに，一次的な通信途絶やリモートホストの保守作業の際でも業務を停止させることなく，バックアップシステムを運用させることができるようになった．

なお，遠隔地のボリュームに保存されるデータのタイムスタンプ等は，ローカルホストの OS がソフトウェアによって生成するため，ログ情報に基づいて遅延書き込みを行っても，それらの書き込みの順序さえ保存できれば，タイムスタンプを含めたオリジナルのデータが持っている属性情報すべてを（秘密分散が適用された形で）シェア上に完全に再現することが可能である．

- 迅速な復旧のための**自動復旧機構**

プロトタイプシステムは，失われた電子情報を復元するのに必要な情報を安全に遠隔地に保存することに主眼を置いて設計されており，復旧を行う際の自動化機能は実装されていなかった．一方，実用的なシステムにおいては，大規模災害後の事業継続計画（BCP）も重要となる．このため，安全に保存されている分散情報からオリジナルの秘密情報を迅速に復元する機構が必要となる．

本システムが採用している秘密分散法では，オリジナルデータの復元にあたり，作成したすべてのシェアが得られなくとも，符号化時に設定したしきい値以上の個数のシェアを集められれば復元が可能である．しかし，使用するシェアの ID をすべて正しく知っていることが必要となる（図 6）．

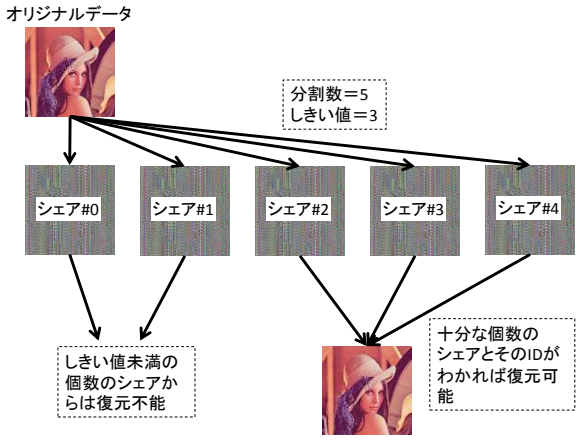

図 6：秘密分散法と復元処理の概要

一方，オリジナル情報が失われるような規模の

災害時には，シェアを作成して配布した（当然，作成した各シェアの ID とそれをどこに配置したかを知っている）ホスト自身も完全に機能を失っている可能性が高いため，自動復旧機構は，災害で機能を失ったホストがどの遠隔サイトに何番目のシェアを保存していたかを知らない状態でデータ復旧を開始しなくてはならない．

そこで，通常運用フェーズでは全ての tgt-x が互いのシェアの所在情報を共有しておき，災害発生後の復旧フェーズでは，残っている拡張 iSCSI ターゲットのいずれかがその情報を自動復元機構に供給するようにした．

- **バックアップ相互保持機能**

プロトタイプシステムは，秘密情報を安全に分散させる機能のみを実装しており，遠隔バックアップの相互保持機能は有していなかった．このため，バックアップ先の iSCSI ターゲットは，図 4 に示すように，改造を施されていないオリジナルの tgt であった．しかし，これを tgt-x に単純に置き換えただけでは，バックアップ先に書き込まれるシェアにも再帰的に秘密分散が適用され，秘密分散の無限連鎖が発生してしまう．

そこで，図 5 のように tgt-x を各サイトに配備した場合でも，相互にバックアップを保持しながら，秘密分散の無限連鎖適用を抑止する機構も実装した．

サブテーマ３：ストレージの所在を仮想化するためのネットワークの高度化に関する研究

情報システムの対障害性を高めるためにデータの保存先をネットワーク上に分散させることを考える．このとき，既存のアプリケーションを変更することなく，分散するストレージに透過的にデータが保存できることが必要である．このような分散するストレージをローカルストレージであるかのように見せる「仮想化」を行う「場所」として，サブテーマ１やサブテーマ２で選択しているような，ホスト上で動作するソフトウェアに仮想化機能を持たせる方法以外に，ネットワークに仮想化機能を持たせる方法も可能である（図 6）．

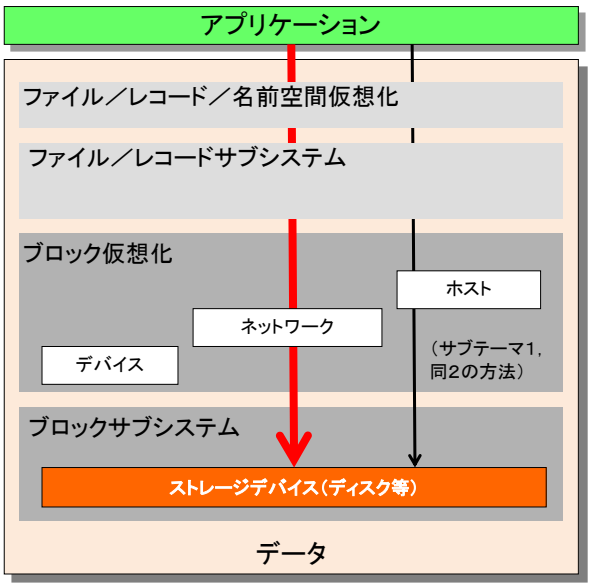

図 7：ストレージ仮想化を行う場所

近年の新しい新世代ネットワーク技術では，実体の識別子と，ネットワーク上の位置や経路情報を分離するアーキテクチャが提案され，新しいネットワークの主流となりはじめている．この技術を使えば，従来のモバイル IP のように，識別子を変えずに実体が物理的に移動しても，効率の悪い経路制御が行なわれることがなくなる．本研究では，この技術を用いれば，災害などでネットワーク単位での移動が必要になった時に，移動してもなお，効率のよい通信が提供される．

現在，このような新しい通信を行なえるものして，OpenFlow[5] や LISP（Locator/ID Separation Protocol）があり，本サブテーマでは，特に OpenFlow の実証実験を通じ評価などとともに研究を行なった．

IP anycast を用いると，アプリケーションを変更することなく，１つの IP アドレスで代表されるストレージサービスを複数のサーバ上に透過的に分散させることが容易になる．しかし，大容量のデータを保存する場合にはサーバの過負荷の問題が生じる．そこで，本サブテーマでは，パケット転送機能とルーティングに関する意思決定機能を

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner: “OpenFlow: enabling innovation in campus networks”, ACM SIGCOMM Computer Communication Review, 38(2):69–74, April 2008.

分離する OpenFlow 技術を用いてこの問題を解決することを考え，OpenFlow を用いた IP Anycast に関する研究を行った．また，IP Anycast の高度化に加えて，OpenFlow そのものの改良の提案も行った．

ここで，この OpenFlow 技術の研究を通じ，これを応用することによって，災害からの復旧作業の迅速化に役立てられることもわかってきた．

大規模災害によって機能を失ったサーバを復旧させる際には，遠隔地に保存されているデータを回収し失われた情報を復元することがまず必要となる．ところが，災害によって重大な機能縮退に陥っているネットワーク上で迅速に保存データを回収しサービスを再開できるためには，被災状況に応じたネットワーク再構築技術が重要となる．パケット転送機能とフロー制御に関する意思決定機能を分離し，広域に分散するネットワーク機器上で柔軟に転送経路の再構成を行うことを可能にする OpenFlow 技術は，一時的にサーバの全機能が失われるような規模の災害からの普及にも役立つ．

さらに，OpenFlow 技術は，被災したサーバの持っていた機能を災害の影響を受けていない遠隔地に移送するライブマイグレーションにも応用することが可能であり，マイグレーション先の決定に遺伝的アルゴリズムを応用する手法の提案も行った．

(2) 当初計画の達成状況について

サブテーマ 1 では，集中型の管理機構を持たずに SSO フェデレーションを形成しているストレージクラウド上で，情報漏洩を防止しながら分散ファイル管理機能を実現する手法が得られた．

サブテーマ 2 では，実用的な遠隔バックアップシステムに不可欠となる，遅延更新機能，自動復旧機能，バックアップ相互保持機能の 3 つを新たに実装することができた．

サブテーマ 3 では，新世代ネットワーク技術を用いて，ストレージ装置の所在情報の仮想化や，災害後に重大な機能縮退に陥ったネットワーク上での迅速な復旧や事業の継続を可能にするための新たな手法を得ることができた．

以上のようなことから，本研究課題は，当初の計画の目標を十分に達成できたと考える．

4. 今後の展望

サブテーマ１：クラウド技術を利用した安全な分散ファイル管理システムの研究

ファイル所有者とファイルサーバ管理者の権限を分離しながら分散ファイル管理機能を実現する手法が得られたので，今後は，緯度経度情報を符号化する GeoHash 情報を用いて分割ファイルの保存先を適切に制御する機構などの検討を行い，高機能化を図る．

サブテーマ２：秘密分散法とストレージ仮想化技術に基づく遠隔バックアップ相互保持方式

実用的な遠隔バックアップシステムに必要な基本機能が実現できたので，システムを各サイトに配備して，現実的なネットワーク環境下における遠隔データ転送実験を行う．

サブテーマ３：ストレージの所在を仮想化するためのネットワークの高度化に関する研究

OpenFlow を用いた IP Anycast，P2P の高度化に関する研究成果を活用し，OpenFlow の機能拡張に関する提案や，OpenFlow を用いたサーバのライブマイグレーションに関する研究を進める．

5. 研究成果リスト

(1) 学術論文

- Othman Othman M. M. and Koji Okamura: “On Demand Content Anycasting to Enhance Content Server Using P2P Network”, 電子情報通信学会英文論文誌, Vol.E95-D, No.2, 2012.02.
- 藤村喬寿，西村浩二，近堂徹，大東俊博，田島浩一，相原玲二:「スイッチベースの認証ネットワークへのシングルサインオン機能の実

装と評価」, 情報処理学会論文誌, Vol.53, No.3, pp. 958-968, 2012.03.

(2) 国際会議プロシーディングス

- Othman Othman M. M., Koji Okamura: “Wider Adaptation and Enhancement of OpenFlow”, Proceedings of the 32nd Asia-Pacific Advanced Network Meeting, 2011.08.
- Heru Sukoco, Koji Okamura: “Distant Location Selection Using Genetic Algorithm for Live Migration Method in OpenFlow Networks”, Proceedings of the Research Network Workshop 2011, 2011.08.
- Heru Sukoco, Koji OKAMURA: “Grouping Packet Scheduling for Virtual Networks by Genetic Algorithm,” Proceedings Int. Conf. on Future Internet Technologies 2011, 2011.06.

(3) 国際会議発表

（なし）

(4) 国内会議発表

- 天野浩文:「秘密分散法とストレージ仮想化技術に基づく遠隔バックアップ相互保持方式」, アカデミッククラウドワークショップ 2012@広島, 2012.02.
- 西村浩二:「「電子情報の大学間相互保持に向けた遠隔バックアップ技術の研究」の取り組みについて」, アカデミッククラウドワークショップ 2012@広島, 2012.02.
- 岡村耕二:「新世代ネットワークを利用したストレージ位置の仮想化に関する研究」, アカデミッククラウドワークショップ 2012@広島, 2012.02.
- 伊藤弘宗, 土肥祐樹, 天野浩文:「秘密分散機能を有する遠隔バックアップシステムの開発」, 平成 23 年度(第 64 回)電気関係学会九州支部連合大会, 2011.09.
- 西村浩二:「組織間連携による分散ファイル管理システムの開発」, アカデミッククラウドシンポジウム 2011@北海道大学, 2011.08.
- 鎌田恵介, 近堂徹, 西村浩二, 相原玲二:「移動透過 IP マルチキャストに対応するグローバルライブマイグレーションの設計と性能評価」, 情報処理学会第 4 回インターネットと運用技術シンポジウム(IOTS2011), 2011.12.
- 西村浩二:「組織間連携による電子情報の遠隔バックアップの検討」, クラウドサービスのための SINET&学認説明会, 2011.12.

(5) その他（特許, プレス発表, 著書等）

（なし）