10-IS04

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．このため，大企業など，地理的に離れた地点に複数の拠点を持つことのできる大規模な組織や，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電子情報が伝統的に個々の大学内で管理されており，また，その保有形態や管理手順も多種多様であるため，大学向けの統一的な遠隔バックアップサービスが民間企業による有償サービスのメニューとして用意されていない．
- 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．

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

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．

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組織内コンセンサスの得られている大学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ようになれば，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，各大学で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

(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

北海道大学・東北大学・東京大学・名古屋大学・京都大学・大阪大学・九州大学の７情報基盤系センター群の間では，重要な電子情報のバックアップを相互保持する仕組みを構築するための取り組みも開始されている．しかし，規模やキャンパス分散の度合いが大きく異なる大学間でのバックアップ相互保持についてはまだ検討されていない．今回，その規模・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．

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

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．

- 大学の遠隔バックアップシステムに対する要求と開発すべき技術の検討
- 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
- 情報を分散保持するための位置透過性の向上に関する研究

以下，それぞれの研究成果について述べる．

3.1 サブテーマ１：大学の遠隔バックアップシステムに対する要求と開発すべき技術の検討

このサブテーマでは，遠隔バックアップシステムを構築・運用するにあたり，システムが有するべき機能の洗い出しを行い，それを実現するための既存技術の選定や開発すべき技術の選別を行うことを目的とした．

まず，現在大学等の組織が置かれている状況や既存技術の開発状況，クラウド等のサービス要件などから，必要と思われる機能を列挙した．

(1) セキュリティポリシーに違反しないこと
(2) データへのアクセスが自組織の構成員に限定されていること
(3) どのデータがどこにあるかわかること
(4) 確実に消去できること

条件(1)について，大学等ではセキュリティポリシーによって重要な情報の組織外への持ち出しが禁止されている．そのため，データを保管する場所を遠隔部局と定義することで，セキュリティポリシー違反を回避しているのが現状である．これはハウジングサービスと何ら代わりがなく，また本研究の相互保持とも趣旨が異なる．そこで，組織外に持ち出す前に重要情報を非重要情報化する方法の検討を行う．次の条件(2)も考慮し，データの暗号化と秘密分散法を組み合わせて適用することが望ましいと考えた．

条件(2)について，データの転送時および保存時には前述のデータの暗号化と秘密分散法の組み合わせによって実現することが可能である．一方，データの処理時には，条件(1)により組織外でデータの復号を行うことはできない．そこでデータ処理までを対象とする場合には，暗号化したままデータ処理を行うことを可能とする（完全）準同型暗号の採用を検討する必要がある．また条件(2)に関して，利用者の認証情報が組織外に開示されないようにする仕組みも必要である．これには国立情報学研究所が運用する学術認証フェデレーション（学認）[1]を利用する．

条件(3)は，条件(1)に基づくデータの秘密分散化の考え方とは対極に位置するものである．一般にクラウドサービスでは，データまたはその断片がどこに保存されているかを明らかにはしていない．これは情報システム監査においてデータが適正に管理されているかどうかの確認が困難である（あるいは外注業者の運用ポリシーに依存するため，自組織により制御できない）ことを意味する．大学等での利用においてこのようなロックイン（囲い込み）が行われることは運用において足枷となる可能性がある．条件(2)においてもデータ処理時の問題があることも考慮すると，データとサービス（データ処理）を明確に分離し，それらの間のインタフェースを共通化することが重要である．本研究はデータの安全な相互保持を実現する枠組みを構築しようとするものであり，データ処理は

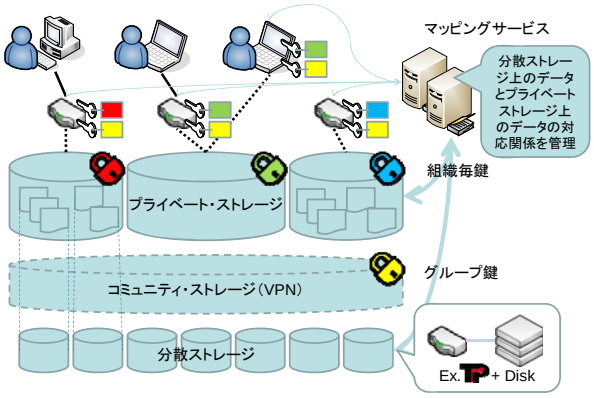

図 1：大学の要求を満たす構成案

それぞれの組織内で行うことを想定しているが，今後の拡張を考慮して，データ処理のためのインタフェースも検討することとした．

条件(4)は，条件(3)と同様に情報システム監査の視点から必要となる機能である．データの完全消去には米国 NIST の基準等があるが，条件(2)で述べた秘密分散法と数学的に十分な安全性が保証された暗号化方式あるいは時限式暗号との併用によって，消去操作後のデータが事実上復号不可であることを保証することで消去に代えることを検討することとした．

上記の条件を満足するシステムの概念図を図 1 に示す．各参加組織に分散配置された分散（個別）ストレージを基本要素として，参加組織全体にまたがるコミュニティ・ストレージを構成する．さらにその上位にそれぞれの組織専用のプライベート・ストレージを構成する．プライベート・ストレージは実際には複数の個別ストレージから構成されており，秘密分散されたファイルの断片の配置はマッピングサービスによって管理される．それぞれの組織では，コミュニティ・ストレージとプライベート・ストレージのアクセス鍵を持つゲートウェイ（アクセスインタフェース）を持ち，自組織のデータにのみアクセスが可能となる．

このとき，個別ストレージとゲートウェイは暗号化と復号および秘密分散の機能を持つ VPN 装置とディスク装置により構成することが可能であるため，組織での導入コストは比較的低く抑えることが可能である．

[1] http://www.gakunin.jp/

3.2 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，サブテーマ１で定めた条件(2)をさらに詳細化して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，プロトタイプの開発を開始した．

(1) すでに多様な OS 上で使用されている既存の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（ファイルサイズ，最終更新日時，オーナーシップなど）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，システム管理者が当然持つべき権限を保持できること．

要件(1)は，すでに各組織で必要不可欠となっている業務アプリケーションが多岐にわたっており，それらすべてに改変を必要とするような解決策は採用できないことによる．自動遠隔バックアップの作成が可能なシステムの一例として DRBD (Distributed Replicated Block Device)[2] があるが，これは Linux 上に実装されそのファイルシステムにアクセスできるアプリケーションからのみ利用可能である．しかし，これは秘密保持機能を有していない上に，他の OS で利用するためには同様の機構を重複してその OS 上に実装しなければならないという欠点がある．

要件(2)および(3)は，各組織が保持する重要な情報の機密性が職務上の守秘義務や各組織のセキュリティポリシーなどで極めて厳格に規定されており，これを勝手に緩和することが受け入れられないことによる．情報の秘密を保持する仕組みとしては暗号化がよく知られている．しかし，鍵やコードブックに基づく暗号化手法は暗号化情報から鍵やコードブックを推定することが「数学的に非常に困難である」という性質に基づいており，秘密情報の不当な取得が「絶対に不可能である」ことを保証するものではない．このため，暗号化後の情報であっても，それを外部に持ち出すこと自体が規制されることもある．一方，秘密を守るために鍵を自組織だけで保有することにすると，大規模災害でそれが失われた場合には，秘密情報を復元するためには秘密情報を不当に得ようとするのと同じだけの困難さが発生してしまう．

要件(4)は，本研究の目指す遠隔バックアップシステムが長期間に渡って利用される場合，バックアップを保持するために各組織が運用するストレージ装置の拡張や更新の作業が必要となることによる．要件(2)や(3)を満たすために，システム管理者がこれらの作業を行うことさえも不可能にしてしまっては，長期運用に支障をきたしてしまう．

以上のような検討を踏まえ，本サブテーマでは，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った．

(a) ストレージ仮想化技術[3]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持つストレージサブシステムとして実装されること．
(b) バックアップすべき秘密情報は，暗号化ではなく秘密分散法[4]によって符号化されること．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[5]を選択する．
(c) メタ情報も隠蔽するために，（個々の）バックアップ情報を格納したボリュームは，ファイルシステムとしてマウントできないようにすること．

このような性質を有するシステムの概念図を図 2 に示す．この図では，ローカルホスト上のアプリケーションから保存される秘密情報が，リモー

[2] http://www.drbd.jp/

[3] Clark, T.: “Storage Virtualization: Technologies for Simplifying Data Storage and Management”, Addison-Wesley, 2005.
[4] 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.
[5] 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.

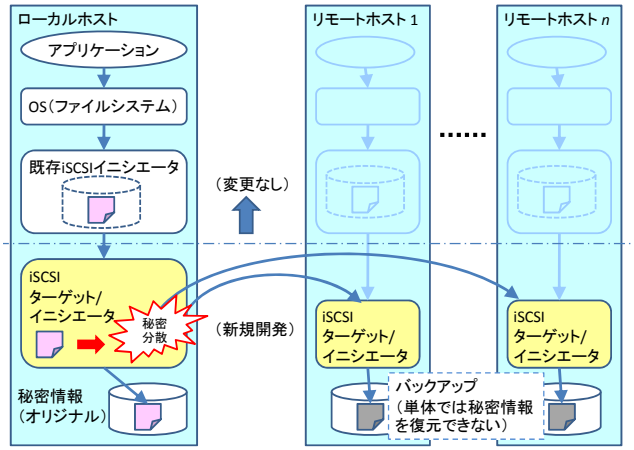

図 2：遠隔バックアップシステムの構成

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．

本サブテーマの目指す遠隔バックアップシステムは，iSCSI[6]プロトコルによってアクセスされる「ターゲット」として実装されるが，同時に iSCSI によって論理ボリュームにアクセスする「イニシエータ」の機能も併せ持つ．

現行の OS の多くはすでに iSCSI プロトコルによってストレージボリュームにアクセスするイニシエータ機能を有しており，その管理下のボリューム上に通常のファイルシステムを構築することもできる．

今日，OS（ファイルシステム）を介さずにローカルストレージを raw device として使用するような事務系アプリケーションはほぼ存在しないと考えられるため，対象となるアプリケーションはほぼすべて，変更なしに新規開発の iSCSI ターゲット／イニシエータにアクセスできることになる．

一方，この iSCSI ターゲット／イニシエータは，既存の iSCSI イニシエータから論理的にはブロックデバイスとして見える．

アプリケーションからストレージへのアクセスは OS によってすべてブロック単位のアクセスに変換されるが，このブロックをローカルストレージにそのまま保存する（秘密情報，オリジナル）他に，そのブロックに秘密分散を適用して，これを複数のリモートホストに分散させる．リモートホスト上にも同様の機能を持った iSCSI ターゲット／イニシエータを配備し，秘密分散が適用されて配布されたバックアップ情報をそれぞれのローカルストレージに保存する．

このとき，ローカルホスト上に作成されるボリュームには当該ホスト上の OS が作成したファイルシステム（およびオリジナルの秘密情報）が存在しているが，リモートホスト上にバックアップされるボリュームは以下のような性質を持つ．

- どのリモートホストが保存するバックアップ情報も，元の秘密情報を復元するのに十分な情報を含んでおらず，悪意のある組織が他の組織の秘密情報を不当に得ようとしても，自己の預かった情報からそれを復元することは（「困難」ではなく）本質的に不可能である．
- 同様に，どのリモートホストが提供するバックアップボリュームも，そのリモートホストからファイルシステムとしてマウントすることはできず，ファイルサイズ，最終更新日時，オーナーシップなどのメタ情報を知ることはできない．
- 鍵やコードブックを用いて暗号化した情報のみを遠隔地にバックアップする手法とは異なり，復号化に必要な情報がすべて，バックアップとして分散されている．このため，大規模災害でローカルホスト上のデータがすべて失われても，オリジナルの秘密情報を復元することが可能である．
- リモートホスト側の管理者が，システム運用上の都合で，バックアップボリュームのコピーを作成しなければならなくなった場合には，ファイルシステムにはよらずに，当該論理ボリュームの全ブロックを別の論理ボリューム上に完全に複製すればよい．バックアップボリュームの拡張が必要となった場合には，当該論理ボリュームの後ろにすべて「ゼロ」が書かれたブロックを必要な数だけ追加すればよい．
- 逆に，ローカルホストが他のリモートホストが保存しようとする秘密情報のバックアップを受け入れる場合には，図 2 に示したのと逆

[6] 脚注 3 に同じ．

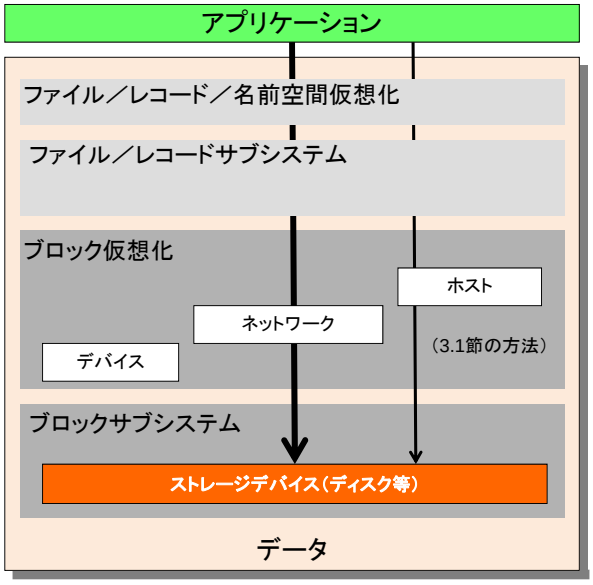

図３：ストレージ仮想化を行う場所

の方向に秘密分散が適用され，ローカルボリューム上にバックアップされる．ローカルホストは，自組織の秘密情報を外部アクセスから保護するのと同じレベルのセキュリティ対策を施したボリューム上にリモートホストからのデータを預かることになる．

上記の性質により，この iSCSI ターゲット／イニシエータは，先に述べた要件(1)～(4)を満たすバックアップ相互保持方式であると言える．

3.3　サブテーマ３：情報を分散保持するための位置透過性の向上に関する研究

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，3.1 節で述べたようなホストやストレージサーバ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が可能である（図 3）．

そこで，本サブテーマでは，ストレージサーバがネットワークの先に分散していることを隠蔽するために，ネットワークにおける位置透過性を向上させることを考える．これは，サブテーマ１で定めた条件(1)を具体化するための試みとなる．

ストレージサーバの位置透過性を提供する代表的な仕組みは，IP anycast 技術および P2P 技術である．

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，OpenFlow[7]技術を用いてこの問題を解決する手法を提案した．

一方，P2P 技術では，情報の格納先（ストレージ）が多数のピアの上に分散され，個々のアクセス要求はピアどうしの通信によって適切なノードへとルーティングされるため，アプリケーションはストレージの位置を意識する必要がなくなる．しかし，物理的な移動の困難なサーバに比べ小回りの利きやすいピアはネットワーク上を簡単に移動しうるという特性がある．このため，IP アドレスが持つ位置情報（ロケータ）と端末識別子（ID）の役割を分離したネットワーク技術についても研究を行い，従来の方式よりも規模適応性に優れた手法を提案した．

4.　これまでの進捗状況と今後の展望

（サブテーマ１）

3.1 節で述べた要件は，大学等におけるセキュリティポリシーの現状や情報システム監査での問題点から抽出したものであり，実際の運用担当者が抱える問題点と完全に一致しているかどうかは明らかではない．今後，これまでの検討結果を元にアンケートを実施することを検討しており，その結果を元に西日本地区における遠隔バックアップシステムの要件についてまとめを行う予定である．

一方，図 4 は仮想化や移動透過通信の技術を応用して，移動に対して透過的にシステムを利用する例を示したものである．仮想化技術や移動透過通信技術により，システムのスケールや移動に対

[7] http://www.openflowswitch.org/

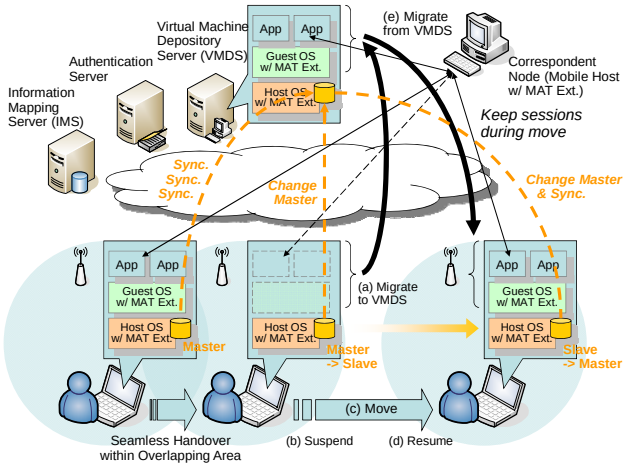

図 4：ストレージ及びネットワークの仮想化による移動透過性の獲得

する自由は獲得された．しかし，ストレージなどの資源に紐付く要素の移動に対する自由の獲得は十分ではない．図 4 の Virtual Machine Depository Server (VMDS)が本研究で構築されるコミュニティ・ストレージ上やプライベート・ストレージ上に配置されることによって，より広域な移動に対する自由を獲得することが可能となる．このように，データの広域分散配置による災害時のデータ保全だけではなく，通常時においては利便性の向上につながるシステムとなるような応用の検討も行っていきたい．

（サブテーマ 2）

3.2 節で述べたような検討の結果，バックアップ情報の相互保持機能を有する iSCSI ターゲット／イニシエータの基本設計を行った．現在，そのプロトタイプの実装を行っており，完成次第，実機を用いたアクセス試験に着手する予定である．

また，このような機能を有する iSCSI ターゲット／イニシエータを実装するにあたって，実験に使用する大規模ストレージ装置のアクセス性能の評価も行っている．

プロトタイプの開発終了後は，性能向上に関する研究を行う予定である．また，ネットワーク帯域や遅延時間の大小に応じて，ブロッキング・非ブロッキング転送やロギングの有無を選択できるような機能拡張も行う．

さらに，秘密分散法の特性を生かし，相互保持の枠組みに参加する組織の中に不正に他組織の情報を得ようとするものが出た場合に自組織の情報を保護するための手法や，そのような悪意を持つ組織に対しての抑止力となり得るような対処法についても検討したい．

（サブテーマ 3）

IP anycast 技術の応用に関する今後の研究課題として，OpenFlow ルータやスイッチの最適な台数および配置の問題がある．

ロケータ/ID 分離ネットワークの応用に関する今後の研究課題としては，規模適応性に加え，位置問い合わせ時間や更新時間の観点による既存の方式との性能比較などが上げられる．

5. 研究成果リスト

(1) 学術論文（投稿中のものは「投稿中」と明記）

・ 渡邉 英伸，大東 俊博，近堂 徹，西村 浩二，相原 玲二，“IP モビリティと複数インタフェースを用いたグローバルライブマイグレーション”，電子情報通信学会論文誌，Vol.J93-B, No.7，pp.893-901，2010 年 7 月．

(2) 国際会議プロシーディングス

・ Othman Othman, M.M. and Okamura, K.: “Improvement of Content Server with Contents Anycasting Using OpenFlow”, Proceedings of Network Research Workshop, August 2010.
・ Othman Othman, M. M. and Okamura, K.: “Design and Implementation of Application Based Routing using OpenFlow”, Proceedings of 5th International Conference on Future Internet Technologies (CFI2010), May 2010.
・ Masaoka, H., Seki, A., Kishiba, S., Kondo, T., Nishimura, K. and Aibara, R.: "Evaluation of P2P File Distribution using IP Mobility", Proceedings of 2010 10th Annual International Symposium on Applications and the Internet (SAINT2010), pp.249-252, July 2010.
・ Watanabe, H., Masaoka, H., Ohigashi, T., Kondo, T., Nishimura, K. and Aibara, R.: "Supporting

USB Devices for the Global Migration," Proceedings of 2010 10th Annual International Symposium on Applications and the Internet (SAINT2010), pp.153-156, July 2010.

- Omori, M. and Okamura, K.: "'Implementation of Green Wireless LAN System by On-Demand Power Supply", Proceedings of IEEE The International Conferece On Information Networking 2011 (ICOIN2011), January 2011 (to appear).
- Kang, J. and Okamura, K.: "Locator/ID Split Network Architecture to Support Mobility", Proceedings of IEEE The International Conferece On Information Networking 2011 (ICOIN2011), January 2011 (to appear).

(3) 国際会議発表

（なし）

(4) 国内会議発表

- 岡村耕二:「遠隔実証研究技術情報のアフリカ連携への応用に関する考察」, 電子情報通信学会インターネット・アーキテクチャ研究会, 2010 年 7 月.
- 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」, 学際大規模情報基盤共同利用・共同研究拠点第 1 回シンポジウム, ポスター展示 IS-4, 2010 年 9 月.
- 平島智将，上田将嗣，戸川忠嗣，小野真，天野浩文:「自動負荷分散機能を有する大規模仮想化ストレージ装置の性能評価」，第 32 回全国共同利用情報基盤センター研究開発連合発表講演会，平成 22 年 11 月.
- 西村浩二:「西日本地区における電子情報の大学間相互保持に向けた取り組み」， 広域分散プライベートクラウドシンポジウム，2010 年 12 月.
- 藤村喬寿，田島浩一，大東俊博，西村浩二，相原玲二 :「大規模キャンパスネットワーク HINET2007 へのシングルサインオン機能の実装および評価」, 情報処理学会インターネットと運用技術シンポジウム（IOTS2010）論文集, pp.111-118，2010 年 12 月（査読有り）.
- 林健太朗，岡村耕二 :「P2P 技術を用いた端末識別子と位置情報の一貫性の改善に関する研究」, 電子情報通信学会情報ネットワーク研究会，2011 年 1 月（予定）.
- 大森幹之，岡村耕二 :「トラフィックに応じた通信機器の給電制御に関する研究」, 電子情報通信学会インターネット・アーキテクチャ研究会，2011 年 2 月（予定）.

(5) その他（特許，プレス発表，著書等）

（なし）