様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ８ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)
研究期間：2011～2014
課題番号：２３５０００４８

研究課題名（和文）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

研究課題名（英文）Development of an off-site backup technique based on storage and network virtualization

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）　　3,300,000円

研究成果の概要（和文）：電子情報のバックアップは非常に重要であるが，大規模災害の際にはバックアップ情報自体も失われる危険がある．これを避けるには遠隔地にバックアップを保存することが重要である．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はない．
そこで，本研究では，複数の組織が互いの機密情報を漏洩させることなく相互にバックアップを保持できる安全な遠隔バックアップ機構，また，被災した仮想計算機を別の地点で迅速に再開させるためのライブマイグレーション機能，さらに，災害で機能縮退に陥ったネットワーク上でサービスを再開させるためのOpenFlow技術に関する研究を行った．

研究成果の概要（英文）：Although data backup is very important, a large scale disaster may destroy the backup copy itself. Off-site backup is essential to avoid such data loss. However, it is not easy for individual organizations to secure remote backup sites on their own.
This project worked on a safe off-site backup sharing mechanism which does not leak the secret from one member to another, a live migration mechanism which enables the quick restart of a damaged virtual machine at another site, and the OpenFlow technology which can restart a service quickly on a degraded network after a disaster.

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　ネットワーク仮想化　秘密分散法　iSCSI　OpenFlow　クラウド

1.　研究開始当初の背景

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報告されている（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資金力のある組織では，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，中小規模の組織では，人事・財務・顧客管理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も多い．この理由には，以下のようなものがあげられる．

- 中小規模の組織では，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．組織の規模が小さいと，この傾向がさらに強まる．
- これらの組織内で利用されている情報システムがそれぞれの組織によって個別に構築・管理されてきており，そこに保持される電子情報の形式や管理手順も非常に多種多様である．
- 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組織が個別に自力で構築しようとすると，組織あたりの人員負担・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．

上記のような問題を解決するためには，各組織が共同で費用を負担することによって個々の組織あたりの金銭的負担を軽減するとともに，同じようなミッションを持つ組織どうしが複製情報を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．

2.　研究の目的

そこで，本研究課題では，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ことを目指すこととした．また，さまざまな組織が保持している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こととした．

一方，これらの組織は，すでに重要な電子情報を扱う情報システムを多数有しており，バックアップを採取するために，すでに使用中のこれらのソフトウェアの動作に影響を与えるような変更を加えることは非常に難しい．すなわち，各システムが必要な電子情報をローカルディスク上のファイルに保存するだけで，自動的にバックアップが作成され遠隔地に転送され保存されるような機構を開発する必要がある．既存のソフトウェアの動作に影響を与えずにこのような機能を提供するため，ネットワーク仮想化技術およびストレージ仮想化技術を利用することとした．

3.　研究の方法

現在のオペレーティングシステム（OS）のほとんどは，ネットワーク上で SCSI プロトコルによって遠隔ストレージを制御する iSCSI イニシエータの機能を標準で備えている．本研究では，この iSCSI イニシエータに対してサービスを提供する 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こととした．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ようになる．

また，遠隔地にバックアップ情報を保存する際に，(k, n)しきい値型秘密分散法（図 1 参照）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開発することにした．

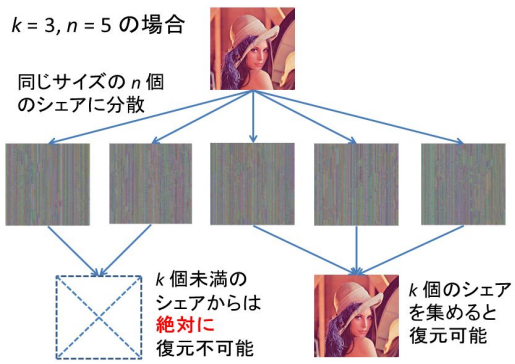

図 1：(k, n)しきい値型秘密分散法の概念

さらに，災害により損傷を受けたシステムおよびサービスの迅速な復旧を図るため，被

災した仮想計算機を疎開先で迅速に再開させるためのライブマイグレーション機能，ならびに，災害で機能縮退に陥ったネットワーク上でサービスを再開させるための OpenFlow 技術についても研究することとした．

4. 研究成果

本研究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．

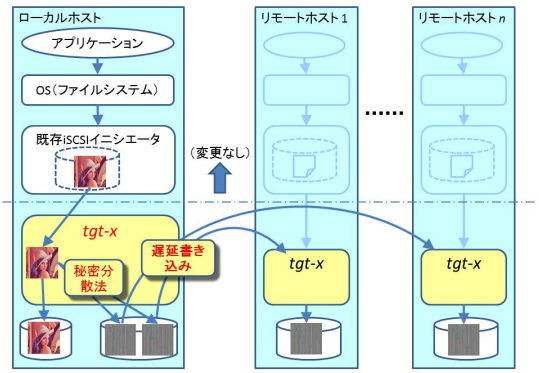

図 2：開発したシステムの概要

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 個のバックアップデータ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．
- 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．
- 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．

上記の他に，以下のような機能も実現した．

- tgt-x は，遠隔バックアップ機能を必要とする複数の（総数が n を上回ってもよい）組織がそれぞれ運用し，互いのバックアップデータを相互に保持する形で利用される．したがって，tgt-x が iSCSI プロトコル経由で受け取る原データのブロック書き込みコマンドは，それぞれ 1 個のローカルブロック書き込みコマンドと n 個の iSCSI リモートブロック書き込みコマンドに変換されて処理される．ただし，遠隔サイトから tgt-x が受け取るブロック書き込みコマンドも，同じ iSCSI 経由で受信される．秘密分散法適用と遠隔バックアップの無限連鎖を防止するため，iSCSI 経由で受け取ったコマンドを，そのままローカルボリュームのみに保存すればよい場合と，ローカル保存に加えて秘密分散法を適用して遠隔保存すべき場合とに分別する．
- (k, n)しきい値型秘密分散法では，アルゴリズム上，復号の際に，k 個のバックアップデータに対して符号化の際に付与された ID（番号）が必要となる．ところが，原データ（ローカルシステム）が被災して壊滅した場合，k 個のバックアップボリュームがどこに保存され，それぞれの ID が何であったかわからなくなる可能性がある．このため，複数のサイトで同時に運用されている tgt-x は，自分の遠隔バックアップ先サイトがどことどこで，それぞれにどの番号を付与しているかの情報を交換し相互に保持する．被災したシステムを復元する際には，再稼働した tgt-x が他の tgt-x に問い合わせを行ってこれらの情報を再取得し，復元処理に使用する．

その他に，被災したシステムを被災していない地域に移設し短時間にサービスを再開させる上で有効なライブマイグレーション技術や，大規模災害で重大な縮退に陥っているネットワーク上で迅速にサービスを再開させるために，OpenFlow 技術を用いたネットワーク再構築手法の研究も行った．

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 20 件）

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

② **吉田耕太**, **西村浩二**, **大東俊博**, **相原玲二：「秘密分散法を利用したクラウドストレージサービスにおけるモバイル機器を考慮した安全な処理委託方式」**, **情報処理学会論文誌**, Vol. 55, No. 3, pp. 1117-1125, 2014.03. **（査読有り）**

③ **大東俊博**, **後藤めぐ美**, **西村浩二**, **相原玲二：「暗号文ポリシー属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と性能評価」**, **情報処理学会論文誌**, Vol. 55, No. 3, pp. 1126-1139, 2014.03. **（査読有り）**

④ Hirofumi Amano, Yuki Dohi, Hiromune Ikeda: “An Approach to Safe Off-Site Backup Utilizing Secret Sharing Scheme and Storage Virtualization,” Proceedings of the IIAI International Conference on Advanced Information Technologies 2013 (IIAI AIT 2013), (CD-ROM), 2013.11. **（査読有り）**

⑤ Othman Othman M. M., Koji Okamura, "Securing Distributed Control of Software Defined Networks", IJCSNS (International Journal of Computer Science and Network Security), Vol. 13, No. 9, pp.5-14, 2013.10. **（査読有り）**

⑥ Othman Othman M. M., Koji Okamura: “Hybrid Control Model for Flow-Based Network,” Computer Software and Applications Conference Workshops (COMPSAC), pp. 765-770, 2013.07. **（査読有り）**

⑦ Othman Othman M. M., Koji Okamura, "Enhancing Control Model to Ease off Centralized Control of Flow-based SDNs", Computer Software and Applications Conference (COMPSAC), pp.467-470, 2013.07. **（査読有り）**

⑧ Othman Othman M. M., Koji Okamura: “Aiding OpenFlow Controller by Enhancing OpenFlow's Control Model, and Behavior of Flows,” International Conference on Future Internet Technologies 2013, (online), 2013.06. **（査読有り）**

⑨ Joonsuk Kang, Koji Okamura: “Multi-Path Mechanism for Audio/Video Streaming Based on Bandwidth Estimation,” IJCSNS (International Journal of Computer Science and Network Security), Vol. 13, No. 2, pp. 24-31, 2013.02. **（査読有り）**

⑩ Ilkwon Cho, Koji Okamura, Tae Wan Kim, Choong Seon Hong: “Performance Analysis of IP Mobility with Multiple Care-of Addresses in Heterogeneous Wireless Networks,” Wireless Networks, The Journal of Mobile Communication, Computation and Information, Volume 19, Issue 1, 2013.01.**（査読有り）**

⑪ **合田憲人，東田学，坂根栄作，天野浩文，小林克志, 棟朝雅晴, 江川隆輔, 建部修見，鴨志田良和，滝澤真一朗，永井亨，岩下武史，石川裕：「高性能分散計算環境のための認証基盤の設計」,情報処理学会論文誌コンピューティングシステム,** Vol. 5, No. 5, pp. 90-102, 2012.10. **（査読有り）**

⑫ Joonsuk Kang, Koji Okamura: “ECN Based Multi-Path Mechanism for VoIP Transmission, Research Reports Information Science and Electrical Engineering of Kyushu University, Vol. 17, No. 2, pp. 41-48, 2012.09. **（査読有り）**

⑬ Othman Othman M. M., Koji Okamura: “Evaluation of OpenFlow's Enhancements,” Proceedings of APAN Research Network Workshop 2012, 2012.08. **（査読有り）**

⑭ Chengming Li, Wenjing Liu and Koji Okamura: “A Greedy Ant Colony Forwarding Algorithm for Named Data Networking,” Proceedings of APAN Research Network Workshop 2012, 2012.08. **（査読有り）**

⑮ Chengming Li, Wenjing Liu, Koji OKAMURA: “Ant Colony based Forwarding Method for Content-Centric Networking,” Proceedings of The 26th IEEE International Conference on Advanced Information Networking and Applications Workshop, 2012.03. **（査読有り）**

⑯ **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. **（査読有り）**

⑰ Othman Othman M. M., 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, pp. 514-522, 2012.02. **（査読有り）**

⑱ Othman Othman M. M., Koji Okamura: “Wider Adaptation and Enhancement of OpenFlow,” Proceedings of Research Network Workshop 2011, RNWS2011,

(CD-ROM), 2011. （査読有り）

⑲ Heru Sukoco, Koji Okamura: “Distant Location Selection Using Genetic Algorithm for Live Migration Method in OpenFlow Networks,” Proceedings of Research Network Workshop 2011, RNWS2011, (CD-ROM), 2011. （査読有り）

⑳ Heru Sukoco, Koji Okamura: “Grouping Packet Scheduling for Virtual Networks by Genetic Algorithm,” Proceedings International Conference on Future Internet Technologies 2011, CFI2011, (CD-ROM), 2011. （査読有り）

〔学会発表〕（計 10 件）

① 吉田耕太, 西村浩二, 大東俊博, 相原玲二：「秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式の実装と評価」, 情報処理学会コンピュータセキュリティシンポジウム(CSS)2013 論文集, 1B1-2, pp. 1-8, 2013.10.

② 吉田耕太, 西村浩二, 大東俊博, 相原玲二：「秘密分散法を利用したクラウドストレージサービスのための安全な処理委託方式」, 情報処理学会研究報告, Vol. 2013-IOT-22, No. 15, pp. 1-6, 2013.08.

③ 後藤めぐ美, 大東俊博, 西村浩二, 相原玲二：「ファイル名/ディレクトリ名を秘匿可能なクラウド向け暗号化ファイル共有システム」, 2013 年暗号と情報セキュリティシンポジウム(SCIS2013)技術展示セッション（デモ展示）, 2013.01. (Poster)

④ 後藤めぐ美, 大東俊博, 西村浩二, 相原玲二：「属性ベース暗号を利用したファイル名暗号化ファイル共有サービスの実装と評価」, 電子情報通信学会技術研究報告, 情報通信システムセキュリティ(ICSS)研究会, Vol. 112, No. 315, ICSS2012-53, pp. 49-54, 2012.11.

⑤ 熊谷悠平, 西村浩二：「認証フェデレーションに基づく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 2012@北海道大学, 2012.08.

⑥ 熊谷悠平, 西村浩二, 大東俊博, 近堂徹, 相原玲二：「認証フェデレーションに基づく分散ファイル管理システムの提案」, 第 18 回インターネットと運用技術研究発表会, 情報処理学会研究報告, Vol. 2012-IOT-18, No .8, pp.1-6, 2012.06.

⑦ 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, 広島市, 2012.02.08.

⑧ 西村浩二: 「電子情報の大学間相互保持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, 広島市, 2012.02.08.

⑨ 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, 広島市, 2012.02.08.

⑩ 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, 佐賀大学, 2011.09.27.

〔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

岡村　耕二（OKAMURA, Koji）
九州大学・情報基盤研究開発センター・教授
研究者番号：70252830

西村　浩二（NISHIMURA, Kouji）
広島大学・情報メディア研究教育センター・教授
研究者番号：90263673

(3)連携研究者
なし