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　２９　年　　６　月　１３　日現在

機関番号：　１２６０８
研究種目：　基盤研究(A)（一般）
研究期間：　2013～2016
課題番号：　２５２４００１４

研究課題名（和文）災害後の復旧・復興における共有情報管理のための基盤技術に関する研究

研究課題名（英文）Research on basic technologies for sharing the information in a disaster recovery

研究代表者

横田　治夫（Yokota, Haruo）

東京工業大学・情報理工学院・教授

研究者番号：１０２４２５７０

交付決定額（研究期間全体）：（直接経費）　　34,900,000円

研究成果の概要（和文）：大規模な災害からの復旧・復興のために、被災者間、支援者間、あるいは被災者と支援者間等で適切な情報共有が必須である。本研究では、災害後のネットワーク、情報機器、電源等が不安定な情報環境下を想定し、被災者の個人的な機微な内容も含む情報を、医療従事者や自治体関係者、報道関係者、ボランティアといった支援者のタイプ、あるいは家族、友人といった被災者との関係等によって異なる開示対象者に、セキュリティを保ちながら適切に提供するためのデータ管理に関する様々な基盤技術を提案し、評価を行ってその有効性を示した。

研究成果の概要（英文）：For the recovery from a large disaster, it is essential to share the information about victims of the disaster among its supporters and the victims themselves. In this research project, we developed a number of basic data management technologies to provide the information appropriately with keeping security and privacy to the targets of disclosure, such as medical teams, local government staffs, press, volunteers, and friends or families of the victims, under the unstable situation of the network, equipment, and power supply environment after the disaster. We demonstrate the effectiveness of these proposed technologies by evaluations.

研究分野：　データ工学

キーワード：　情報共有　暗号化 RDF　グラフ構造検索　秘匿性管理　プライバシー保護　災害復旧・復興　被災者支援　セキュリティ

１．研究開始当初の背景

科学技術・学術審議会の「東日本大震災を踏まえた今後の科学技術・学術政策の在り方について」の中間まとめでも示されているように、震災後の復旧・復興において、これまでの我が国の学術研究成果が十分に貢献できていないことが大きな問題となっている。情報分野に関する動向としても、様々な情報基盤は今や日々の生活に欠かせないものとなっているが、大規模な災害の復旧・復興に必要な共有情報管理という面から見たときに、十分に貢献できずに来たと言わざるを得ない。このことは、国内に限らず海外の状況を見ても同様である。

例えば、東日本大震災後、Google は安否確認情報を電子化して Web 経由でアクセス可能にすることや、車の GPS 情報を Google マップの上にプロットして物資の供給経路決定に役立てるといった機能の提供をしてきた。しかし、それらは、データの提供のレベルに留まり、必要とされる情報に関してプライバシーを考慮して的確に統合し、維持管理して有効利用するところまではできていなかった。

災害の影響で電源、ネットワーク、計算環境等が安定しない中で、個人に関する情報を含む災害からの復旧・復興に関する情報を、プライバシーを考慮して維持管理し、必要な情報を的確に共有するための基盤的技術が求められていた。

２．研究の目的

地震、津波、豪雨等の大規模な災害からの復旧･復興のためには､被災者間､支援者間、あるいは被災者と支援者間等で適切な情報共有が必須である。そのような災害復旧・復興における共有に必要な情報を蓄積する装置や情報を通信する装置が災害によって損傷し、共有すべき情報の一部が消失することや、不確実になることが想定される。また、災害復旧・復興のための情報には、被災者の個人に関する情報が多く含まれる。特に、それらの情報の開示可能な範囲は、対象とする情報の種類と開示対象者、例えば、医療従事者や自治体関係者、あるいはボランティアといった支援者のタイプ、あるいは家族、友人といった被災者との関係等で変化する。このため、本研究では、災害後の部分的で不確実な情報から、開示範囲の異なる秘匿性を考慮しながら、復旧・復興に必要な関係者間の共有情報を構築するためのデータ管理技術を確立することを目的としてきた。

具体的には、災害後のセキュリティ的にも不安定な分散した環境において、個人に関わる情報を暗号化することを前提に、情報提供可能な範囲で共有する方法、分散した部分的共有情報を効率よく収集するためのネットワーク管理、データ移動管理、データベース技術等に関する基盤技術を提供することで、災害の復旧・復興に貢献できるように当該技術分野を発展させることを目指してきた。

３．研究の方法

災害復旧・復興時の情報共有に必要な基盤技術に関し、ネットワーク管理、データ移動管理、データベース技術に詳しい研究代表者、研究分担者が協力して研究を推進した。その際、被災者のプライバシーを考慮しながら情報共有のための暗号化技術や検索技術の利用に関して研究を行う上位層と、災害の影響で一部損傷を受けている情報を蓄積するストレージ装置や情報を転送するネットワーク装置等を利用して情報を効率よく収集・共有する下位層に分けて研究を進めた。上位層は下位層の構成を前提に研究を進める必要があり、下位層も上位層の機能実現を前提に研究を進める必要があるため、相互に密に連携しながら研究を進めた。

（１）上位層では、災害後の復旧・復興活動での、医療関係者、自治体関係者、ボランティア、あるいは被災者の関係者等の利用者のクラスに対応してプライバシーを考慮する必要がある。秘匿性等の情報の特性を考慮して必要な情報を提供可能とするグラフ構造を構築するため、暗号化した RDF を利用し、階層的なアクセス管理を取り入れるアプローチをとった。その中で、様々な暗号化手法を組み合わせ、機能を評価するためのベンチマークを用意することにした。この他、画像を扱った安否確認のアプローチも取る。

（２）下位層では、上位層で扱う暗号化された RDF で記述された共有情報を蓄積し、災害後の部分的に損傷を受けた情報蓄積装置やネットワーク装置、あるいは制限のある電源環境等の状況に対応しながら、必要に応じてデータ移動やデータ復旧を行うアプローチをとった。その中で、分散状況を想定するストレージ管理として、暗号化 RDF の特徴を考慮し、暗号修理、復号処理を行う効率的な格納を想定するとともに、部分的に利用ができない分散ノードのレプリカの配置とその暗号化、およびネットワークが再結合された場合のデータ移動量の削減等も想定して研究を進める方法を取った。また、ネットワークの環境が不安定な状況において、情報が比較的流通しやすい SNS 上の情報に基づいた大規模災害時のネットワーク制御も取り入れた。

４．研究成果

ここでは、上記の研究の方法で述べた上位層と下位層に分けて研究成果を報告する。

（１）上位層においては、様々な利用者のクラス、あるいは親類や友人といった被災者の個人的関係に基づいて情報共有の範囲を設定するための機構や、暗号化されたグラウ構造上で効率よく検索を行うための手法の提案を行うとともに、それらに関連するインデックス構造やデータ配置方法に関しても提案を行った。

本研究で対象とする大規模災害後の支援活動に関わる利用者としては、医療従事者、自治体関係者、ボランティア、報道関係者、他の被災者といった異なるクラスが想定される。このため、利用者クラスに適合した情報開示の範囲を設定する必要がある。また、親類や友人の友人といった、人のつながりを考慮する必要もある。そこで、被災者の避難状況や関係者の間の関係、その他の情報を暗号化した RDF でグラフ構造として保持し、セキュリティを保ちながら開示範囲に対する当事者の意思を尊重して利用者クラスと適切に情報を共有する機構を開発してきた[学会発表 16,17,22,23,24 等]。

まず、暗号化 RDF データベースに対して、プロキシ再暗号化手法と検索可能暗号を利用することで利用者クラスとアクセスレベルのマッピングを行う手法を提案してきた。利用者クラスとアクセスレベルのマッピングの様子を図 1 に示す。

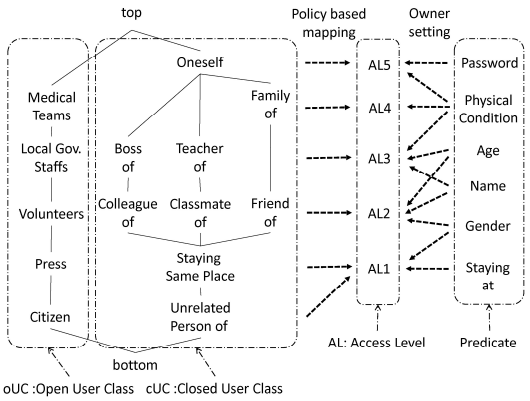


図 1　アクセスレベルのマッピング

利用者は PKI を想定した個人の公開鍵と秘密鍵のペアを保持し、公開鍵で暗号化した問い合わせをプロキシサーバに渡す。プロキシサーバは、認証局の生成した再暗号化鍵でアクセスレベルに対応した公開鍵で暗号化した問い合わせに再暗号化し、データベースサーバに渡す。データベースサーバでは、検索可能暗号方式によって、RDF データベースを検索し、アクセスレベルに対応した公開鍵で暗号化された結果結果をプロキシサーバに返す。プロキシサーバでは、利用者の公開鍵で暗号化された結果に再暗号化し利用者に返す。利用者は、自分の持つ秘密鍵で復号し平文の結果を得ることができる。提案するシステム構成を図 2 に示す。

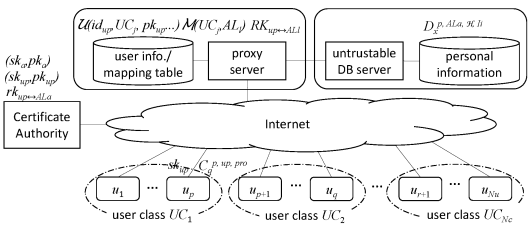


図 2　提案のシステム構成

提案手法を評価するために、被災の状況をシミュレートするベンチマークの開発も行った[学会発表 23]。提案ベンチマークでは、公開されている避難場所の位置や収容可能人数の情報と、日本人の統計情報に基づき、災害発生個所からの距離と規模により、人工的な RDF データを生成することができるようになっている。

プロキシ再暗号化可能で、検索可能な暗号について、いくつかの候補があるが、第一段階の評価として、BBS 暗号を確定暗号化して検索可能としたものと、被災者毎に乱数を割り当て確定暗号と排他的論理和計算によって疑似確率的暗号化したものに対して、提案ベンチマークで実験を行い、オーバーヘッドが少ないことを示した[学会発表 16 等]。その結果を図 3 に示す。

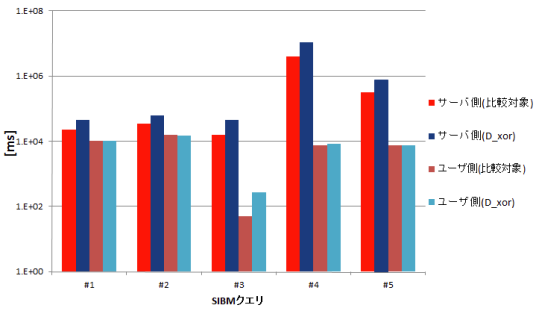


図 3　検索ベンチマーク結果

さらに、セキュリティを保ちながら大規模な災害後に支援物資や支援活動の手配を適切に行うためには、暗号化された RDF データベースに対して集約演算を行う必要があるが、暗号化したまま計算が可能な準同型暗号を使う場合、計算コストが高い。このため、推定を行う方法と、他の暗号と組み合わせる方法を提案し、評価を行った[学会発表 17 等]。図 4 に他の暗号と組み合わせた場合の性能評価の結果を示す。グラフより組み合わせによる効果が分かる。

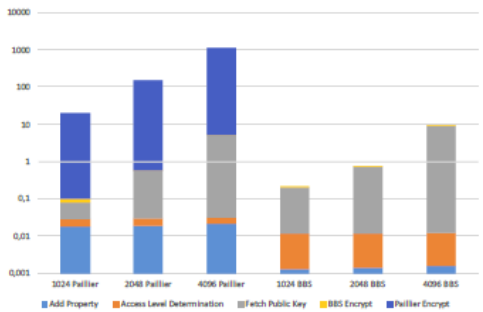


図 4　組み合わせ方式の評価結果

上位層の機能として、画像を扱った安否確認システムに関しても提案、評価も行っている[学会発表 2]。

（2）下位層については、複数の避難所等で格納形態である RDF データを分散して格納し効率よく処理する方法、被災地での制限された電源環境で要求に応じた性能を提供する

ための機能、災害によってネットワーク等の環境が悪化した場合にも適切にネットワークを切り替えて被災地間で情報を共有する機構等を提案した。

RDF データの分散格納に関しては、RDF の Subject、Predicate、Object に対する問い合わせパターンを反映させた格納方法とそれに対するインデックスを提案し、従来手法との比較評価を行った[学会発表 12]。評価結果を図５に示す。グラフより、ベンチマークの全ての問い合わせに対して、提案手法（JARS）が比較手法（RDF-3X）より短時間で結果を返していることが分かる。

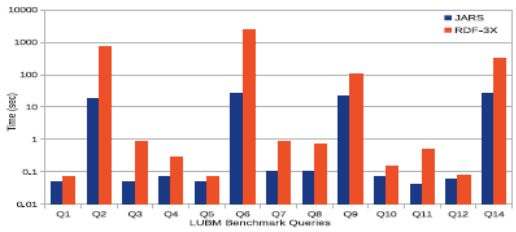


図５ RDF 分散格納手法の評価結果

被災地での制限された電源環境で要求に応じた性能を提供するための機能に関しては、これまでにない分散環境のレプリカの配置方法を提案した[雑誌論文 3,4]。提案手法では、従来の配置方法に比べ、ノード数を増やすためのデータ移動が少なく、短時間で対応できる。図 6 のグラフは、提案手法（Accordion-DP）が、システムの大小に関わらず従来手法（Rabbit、Sierra）と比べてスループットが優れていることを示している。

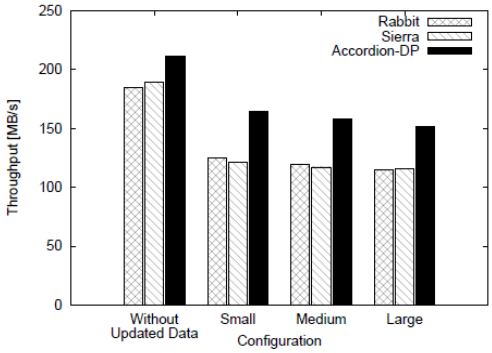
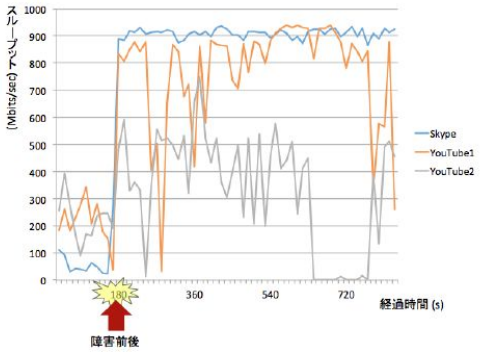


図６　スループットの比較

災害によってネットワーク等の環境が悪化した場合にも適切にネットワークを切り替えて被災地間で情報を共有する機構に関しては、SNS 上の情報に基づき最適な切り替え先を選出する手法を提案し、評価を行った[学会発表 3,4,13,14,15,18,19,21 等]。図 7 に災害発生後にアプリケーション毎のスループットを制御する方法の評価結果を示す。

上記以外にも、下位層に関連する技術として、位置情報等の多次元データベース用インデックス[学会発表 1,6]、マルチコアを使ったデータベースの性能向上手法[雑誌論文 2]、ストリーム処理技術[学会発表 20]、各種検索技術[学会発表 5,6,7,9,10]等の基盤技術を提案している。

図７　スループット制御の効果



以上述べたように、大規模な災害の復旧・復興に求められる共有情報管理のための上位層および下位層の基盤技術に関して様々な手法を提案して有効性を評価し、関連技術分野の発展に貢献した。

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　４件）

(1) Asami Higai, Atsuko Takefusa, Hidemoto Nakada, Masato Oguchi, “A Study of Effective Replica Reconstruction Schemes for the Hadoop Distributed File System”, IEICE Transactions on Information and Systems, 査読有, Vol. E98-D, No.4, pp.872-882, 2015. http://doi.org/10.1587/transinf.2014EDP7242

(2) Fang XI, Takeshi MISHIMA, Haruo YOKOTA,"Cache-Conscious Data Access for DBMS in Multicore Environments", IEICE Transactions on Information and Systems, IEICE, 査読有, Vol. E98-D, No. 5, pp. 1001-1012, 2015.5. http://doi.org/10.1587/transinfo.2014DAPP004

(3) Hieu Hanh LE, Satoshi HIKIDA, Haruo YOKOTA, "Accordion: An Efficient Gear-Shifting for a Power-Proportional Distributed Data-Placement Method", IEICE Transactions on Information and Systems, IEICE, 査読有, Vol. E98-D, No. 5, pp. 1013-1026, 2015.5. http://doi.org/10.1587/transinfo.2014DAPP007

(4) Hieu Hanh LE, Satoshi HIKIDA, Haruo YOKOTA, "NDCouplingHDFS: A Coupling Architecture for a Power-proportional Hadoop Distributed File System”, IEICE Transactions on Information and Systems, IEICE, 査読有, Vol. E97-D, No. 2, pp. 213-222, 2014.2. http://doi.org/10.1587/transinf.E97.D.213

〔学会発表〕（計　24 件）

(1) Shoji Nishimura, Haruo Yokota. “QUILTS: Multidimensional Partitioning Framework Based on Query-Aware and Skew-Tolerant Space-Filling Curves”, International Conference on Management of Data, Proc. of the 43rd ACM International Conference on Management of Data (SIGMOD), pp. 1525-1537, Chicago(USA), May. 2017.
http://doi.org/10.1145/3035918.3035934

(2) 高田 千暁, 本橋 史帆, 大和田 泰伯, 高井 峰生, 小口 正人,「災害時における画像を扱った安否確認システムの評価」, マルチメディア, 分散, 協調とモバイル (DICOMO2016)シンポジウム, 鳥羽シーサイドホテル（三重・鳥羽), 2016.7.

(3) 丸 千尋, 榎 美紀, 中尾 彰宏, 山本 周, 山口 実靖, 小口 正人,「ネットワーク QoE 制御のための大規模災害時における SNS による集合知に基づいた情報抽出」, 第 9 回データ工学と情報マネジメントに関するフォーラム, 高山グリーンホテル（岐阜・高山), 2017.3
http://db-event.jpn.org/deim2017/papers/168.pdf

(4) 柳田 晴香, 中尾 彰宏, 山本 周, 山口 実靖, 小口 正人,「大規模災害時における SNS 情報を用いたアプリケーション毎の QoS 制御手法の実装と評価」,, 第 9 回データ工学と情報マネジメントに関するフォーラム, 高山グリーンホテル（岐阜・高山), 2017.
http://db-event.jpn.org/deim2017/papers/105.pdf

(5) 伊藤寛祥, 駒水孝裕, 天笠俊之, 北川博之,「ノードが複数の属性を持つグラフにおけるコミュニティ検出」, 第 9 回データ工学と情報マネジメントに関するフォーラム, 高山グリーンホテル（岐阜・高山), 2017.3.
http://db-event.jpn.org/deim2017/papers/262.pdf

(6) 渡 佑也, 欅 惇志, 宮崎 純,「多次元データに対する集約演算の効率化手法におけるデータ挿入 スループットの向上」, 第 9 回データ工学と情報マネジメントに関するフォーラム, 高山グリーンホテル（岐阜・高山), 2017.3.
http://db-event.jpn.org/deim2017/papers/182.pdf

(7) 欅 惇志, 宮崎 純, 波多野 賢治,「部分文書検索を用いた高精度なモバイル情報検索」, 第 9 回データ工学と情報マネジメントに関するフォーラム, 高山グリーンホテル（岐阜・高山), 2017.3.
http://db-event.jpn.org/deim2017/papers/27.pdf

(8) Chihiro Maru, Miki Enoki, Akihiro Nakao, Shu Yamamoto, Saneyasu Yamaguchi, Masato Oguchi, “QoE Control of Network using Collective Intelligence of SNS in Large-Scale Disasters 16th IEEE International Conference on Computer and Information Technology (CIT2016), Yanuca Island(Fiji), 2016.12.
http://doi.org/10.1109/CIT.2016.68

(9) Yume Sasaki, Takuya Komatsuda, Atsushi Keyaki, Jun Miyazaki,“A New Readability Measure for Web Documents and its Evaluation on an Effective Web Search Engine”, 18th International Conference on Information Integration and Web-based Applications & Services, Singapore(Singapore), 2016.11.
http://doi.org/10.1145/3011141.3011172

(10) Takuya Komatsuda, Atsushi Keyaki, Jun Miyazaki, “A Score Fusion Method Using a Mixture Copula”, 27th International Conference on Database and Expert Systems Applications (DEXA 2016), Porto(Portugal) 2016.9.
http://doi.org/10.1007/978-3-319-44406-2_16

(11) Takamitsu Shioi, Kenji Hatano, “Rule- and Cost-Based Optimization of OLAP Workloads on Distributed RDBMS with Column-Oriented Storage Function, 3rd International Symposium on Big Data Research and Innovation (BigR&I 2016), Vienna(Austria), 2016.8.
http://doi.org/10.1109/W-FiCloud.2016.44

(12) Anjali Rajith, Shoji Nishimura, Haruo Yokota, "JARS: Join-Aware Distributed RDF Storage", Proceedings of IDEAS 2016, pp. 264-271, Montreal(Canada), 2016.7.
http://dx.doi.org/10.1145/2938503.2938548

(13) Chihiro Maru, Miki Enoki, Akihiro Nakao, Shu Yamamoto, Saneyasu Yamaguchi, Masato Oguchi, “Development of Failure Detection System for Network Control using Collective Intelligence of Social Networking Service in Large-Scale Disaster”, 27th ACM Conference on Hypertext and Social Media (HT2016), Halifax(Canada), 2016.7.
http://doi.org/10.1145/2914586.2914620

(14) 高田 千暁, 黒崎 裕子, 本橋 史帆, 大和田 泰伯, 高井 峰生, 小口 正人,「実地図を用いた災害時通信システムのシミュレーション評価」 第 8 回データ工学と情報マネジメントに関するフォーラム論文集, E7-3, ヒルトン福岡（福岡・福岡), 2016.3
http://db-event.jpn.org/deim2016/papers/121.pdf

(15) 丸 千尋, 榎 美紀, 中尾 彰宏, 山本 周, 山口 実靖, 小口 正人,「大規模災害時におけるネットワーク制御のための SNS による集合知に基づいた障害検知システムの構築と評価」, 第 8 回データ工学と情報マネジメントに関するフォーラム論文集, ヒルトン福

岡（福岡・福岡），E7-3，2016.3.
http://db-event.jpn.org/deim2016/papers/168.pdf
(16) 杉原 弘祐，三上 英明，横田 治夫，「プロキシ暗号を用いた被災者情報アクセス制御手法の評価」，第 8 回データ工学と情報マネジメントに関するフォーラム論文集，E7-3，ヒルトン福岡（福岡・福岡），2016.3.
http://db-event.jpn.org/deim2016/papers/370.pdf
(17) 三上 英明，杉原 弘祐，横田 治夫，「階層的なアクセスレベル制御を行う RDF データに対する集約計算結果の推定」，第 8 回データ工学と情報マネジメントに関するフォーラム論文集，F8-4，ヒルトン福岡（福岡・福岡），2016.3.
http://db-event.jpn.org/deim2016/papers/153.pdf
(18) Yuko Kurosaki, Atsuko Takefusa, Hidemoto Nakada, Masato Oguchi, “A Study of Load Balancing between Sensors and the Cloud for a Real-Time Video Streaming Analysis Application Framework, 10th ACM International Conference on Ubiquitous Information Management and Communication (IMCOM2016), Danang(Vietnam), 2016.1
http://doi.org/10.1145/2857546.2857601
(19) Chihiro Maru, Miki Enoki, Akihiro Nakao, Shu Yamamoto, Saneyasu Yamaguchi, Masato Oguchi, “Network Failure Detection System for Traffic Control using Social Information in Large-Scale Disasters”, ITU Kaleidoscope Conference 2015: Trust in the Information Society, Barcelona(Spain), 2015.12.
(20) Yousuke Watanabe, Haruo Yokota, "Dynamic Modification of Continuous Queries by Using RDF Metadata of Information Sources", Proc. of 015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), pp. 754-759, Krakow(Poland), 2015.11.
http://dx.doi.org/10.1109/3PGCIC.2015.105
(21) Chihiro Maru, Miki Enoki, Akihiro Nakao, Shu Yamamoto, Saneyasu Yamaguchi, Masato Oguchi, “Network Failure Detection System for Traffic Control using Social Information in Large-Scale Disasters”, IEEE Global Humanitarian Technology Conference (GHTC2015), Washington(USA), 2015.10.
http://doi.org/10.1109/Kaleidoscope.2015.7383642
(22) Vu Tuan Dat, 横田 治夫，「MapReduce による大規模な RDF データ復号化手法の評価」，第 7 回データ工学と情報マネジメントに関するフォーラム論文集，ホテル華の湯（郡山・福島），2015.3.
http://db-event.jpn.org/deim2015/paper/284.pdf
(23) グエン ホアイ ナム，荒堀 喜貴，横田 治夫，「SIBM - 避難場所情報に対する RDF データセットベンチマークツール」，第 7 回データ工学と情報マネジメントに関するフォーラム論文集，ホテル華の湯（郡山・福島），2015.3.
http://db-event.jpn.org/deim2015/paper/288.pdf
(24) 児玉 快，横田 治夫，「データやユーザの効率的な追加・削除が可能な秘匿情報アクセス手法」，第 7 回データ工学と情報マネジメントに関するフォーラム論文集，ホテル華の湯（郡山・福島），2015.3.
http://db-event.jpn.org/deim2015/paper/293.pdf

６．研究組織

(1)研究代表者

横田　治夫（YOKOTA, Haruo）
東京工業大学・情報理工学院・教授
研究者番号：１０２４２５７０

(2)研究分担者

宮崎　純（MIYAXAKI, Jun）
東京工業大学・情報理工学院・教授
研究者番号：　４０２９３３９４

小林　隆志（KOBAYASHI, Takashi）
東京工業大学・情報理工学院・准教授
研究者番号：　５０３４５３８６

荒堀　喜貴（ARAHORI, Yoshitaka）
東京工業大学・情報理工学院・助教
研究者番号：　５０６１３４６０

欅　惇志（KEYAKI, Atsushi）
東京工業大学・情報理工学院・助教
研究者番号：　００７３３９５８

小口　正人（OGUCHI, Masato）
お茶の水女子大学・基幹研究院・教授
研究者番号：　６０３２８０３６

天笠　俊之（AMAGASA, Toshiyuki）
筑波大学・システム情報系・教授
研究者番号：　７０３１４５３１

波多野　賢治（HATANO, Kenji）
同志社大学・文化情報学部・教授
研究者番号：　８０３１４５３２

渡辺　陽介（WATANABE, Yosuke）
名古屋大学・未来社会創造機構・特任准教授
研究者番号：８０５３２９４４