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

令和　　元 年　　６ 月 １４ 日現在

機関番号：３２６６１
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８１３

研究課題名（和文）秘密分散・秘密計算に基づくクラウドサービスの安全化と安全性能評価手法の提案

研究課題名（英文）A proposal of a method of securing cloud services based on secret sharing / secure computation and a proposal of safety performance evaluation method

研究代表者

佐藤　文明（SATO, Fumiaki）

東邦大学・理学部・教授

研究者番号：４０２７３１６４

交付決定額（研究期間全体）：（直接経費）　　12,600,000円

研究成果の概要（和文）：実数に基づく簡易型秘密計算方式を提案し、クラウド間で中間結果を安全に交換することで中間結果をクライアントに戻すことなく効率よく計算する方法を確立した。また、FFT、位置情報の範囲検索、外れ値の検出、機械学習などへの適用方法を示した。更にクラウドの安全性を分析する方法として、ハードウェア信頼性を扱う従来の信頼性理論の手法に倣い、安全性を定量的に評価するためのモデルを提案した。ハードウェアの信頼性、ソフトウェア及び人間系の安全性を含めた情報システム全体としての安全性を確率モデルによって定式化する方法を提案し評価した。

研究成果の学術的意義や社会的意義
近年、企業やその他の組織において、内部不正による情報セキュリティ事故が原因で事業の根幹を脅かすような事案が目立つようになってきた。秘密分散に基づく秘密計算技術は、一部のクラウドから情報漏洩しても、元の情報は再現できないため情報漏洩対策として有効である。また、我々の提案する実数による簡易型秘密計算は、既存の方式より通信量やサーバが保持するシェアの量が少なくて済み、大規模なデータベースや教師データを使った深層学習にも適用しやすいため、今後のAIを用いた多くのシステムにも利用できる技術となる。

研究成果の概要（英文）：We proposed a simplified real-number-based secret computation method, and established a method to calculate the intermediate result efficiently without returning the intermediate result to the client by exchanging the intermediate result safely between the clouds. In addition, the application method to FFT, range search of position information, outlier detection, machine learning, etc. is shown. Furthermore, as a method to analyze cloud security, we proposed a model to evaluate security quantitatively, following the method of conventional reliability theory dealing with hardware reliability. We proposed and evaluated a method to formulate the security of the whole information system including hardware reliability, software and security of human system by probabilistic model.

研究分野：情報ネットワーク

キーワード：秘密計算　秘密分散　クラウドコンピューティング　セキュリティ　暗号　安全性分析

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年、企業やその他の組織において、内部不正による情報セキュリティ事故が原因で事業の根幹を脅かすような事案が目立つようになってきた。内部不正による情報漏洩は、情報を扱う当事者が不正を犯すという意味で、防ぐことや発見することが難しく、見つかった時には既に被害が拡大し関係者に多大な迷惑が及んでしまうことが多い。また、個人情報漏洩や技術情報流出の懸念から、企業がクラウド等の社外サービスを使った情報管理に踏み切れない例も多数みられる。

これらの課題を解決するための技術として、秘密分散及び秘密計算技術が提案されてきた。秘密分散は、情報を符号化してｎ台のサーバに分散させ、そのうちのｋ台以上のサーバからの情報を集めないと元の情報が得られない技術である（k out of n と称する）。このとき、ｋ－１台以下のサーバからの情報が流出したとしても、元の情報は得られないため、情報流出のリスクを著しく下げることができる。また、秘密計算技術とは、情報の復号を行わずに符号化したままサーバ側で計算した結果から、クライアントで復号化することで計算結果を得られる技術である。サーバ側では情報の復号をしないため、計算の過程で情報が流出しないという利点がある。

NTT は近年、秘密分散に基づく計算量の少ない整数ベースのマルチパーティ秘密計算方式（以下 NTT 方式）を提案した。秘密分散方式では、分散されたデータ（シェアと呼ぶ）についての加減算の結果を集めると、元の加減算の計算結果を得ることが可能である。分散されたデータは、それぞれ意味を持たないデータであるため、情報漏洩に強い性質があるとともに、k out of n の場合ｎ台の分散されたサーバが一部故障してもｋ台のサーバから元のデータを復元できるので信頼性の向上というメリットもある。

しかし、NTT 方式では乗算ではサーバ間で複雑な計算途中情報のやりとりが必要であり、通信データ量が大きくなることが問題である。また、通信を回避するには、2 out of 3 の場合、３台のすべてのサーバが正常に動作している必要があり、システムの信頼性は低下するという課題があった。

２．研究の目的

本研究の目的は、クラウドサービスにおいて内部不正や外部からの不正アクセスによる情報流出を防ぎ、安全に秘密情報を保持するための軽量な秘密計算方式を提案し、様々な応用に適用することでその有効性を評価することである。また、秘密計算によってクラウドでの情報管理の安全化を行う上で必要となる安全性評価指標の提案を行い、その有効性を評価することである。具体的には、（１）実数に基づく秘密分散型の秘密計算方式の提案とアルゴリズムの確立、（２）具体的な応用システムへの適用、（３）信頼性理論の考え方を発展させたセキュリティに関わるクラウドの安全性分析手法の確立である。

３．研究の方法

本研究は、大きく３つのパートに分かれている。

（１）実数に基づく秘密分散型の秘密計算方式の提案とアルゴリズムの確立については、佐藤と金岡が主に担当し、はじめに四則演算が混在する複雑な計算を秘密計算で実行する方式を確立し、次にクラウドサーバ間で連携して中間データを交換する方式を確立する。

（２）具体的な応用システムへの適用では、主に白鳥と佐藤が担当し、教師データを使った機械学習や、大量のデータから外れ値と呼ばれる例外データを検知する応用、位置情報の管理と範囲検索への適用を実施する。

（３）クラウドの安全性分析手法の確立では、主に白鳥が担当し、ハードウェアの信頼性評価の理論をクラウドの安全性評価に適用する方法を提案する。また、具体的な構成に対して分析評価を行い、必要な安全性を提供できているかを評価できることを示す。

４．研究成果

(1)実数に基づく秘密分散型の秘密計算方式の提案とアルゴリズムの確立

①はじめに

マルチパーティ法による秘密計算はデータが 2 つの場合は、図１に示すようにあらかじめ(c0, c1)、(c1, c2)、(c2, c0) を計算し、その結果を 1 組のシェアとして、各サーバに保持すればいい。しかし、データが多くなるに従い、2 項の乗算の場合に限っても、組み合わせ数の 2 分の 1 の数の組をシェアとして保持する必要がある。データ種類（属性）の数を p とすると、シェアの組の数 q は q=p・(p-1)/2 となる。RDB の場合、これに行の数が乗算される。この (c0, c1)、(c1, c2)、(c2, c0) をシェアとして保持する方式では、データの量が課題になるという問題がある。

そこでこれらの問題を回避するために我々は簡易的秘密計算法を提案している。この簡易的秘密計算法はセキュアマルチパーティ法の加減算用シェアに加え乗除算用のシェアを作ることで問題を回避している(図 2)。

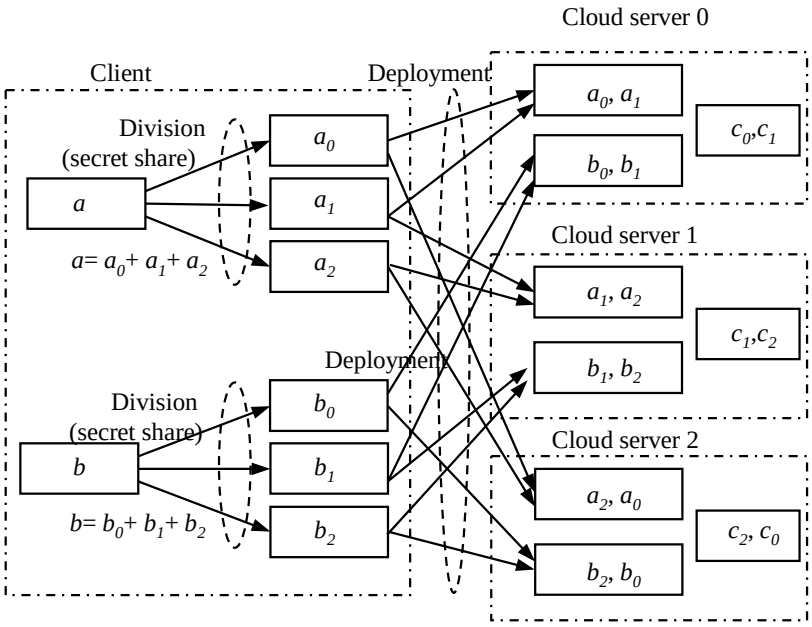

図１　マルチパーティ法

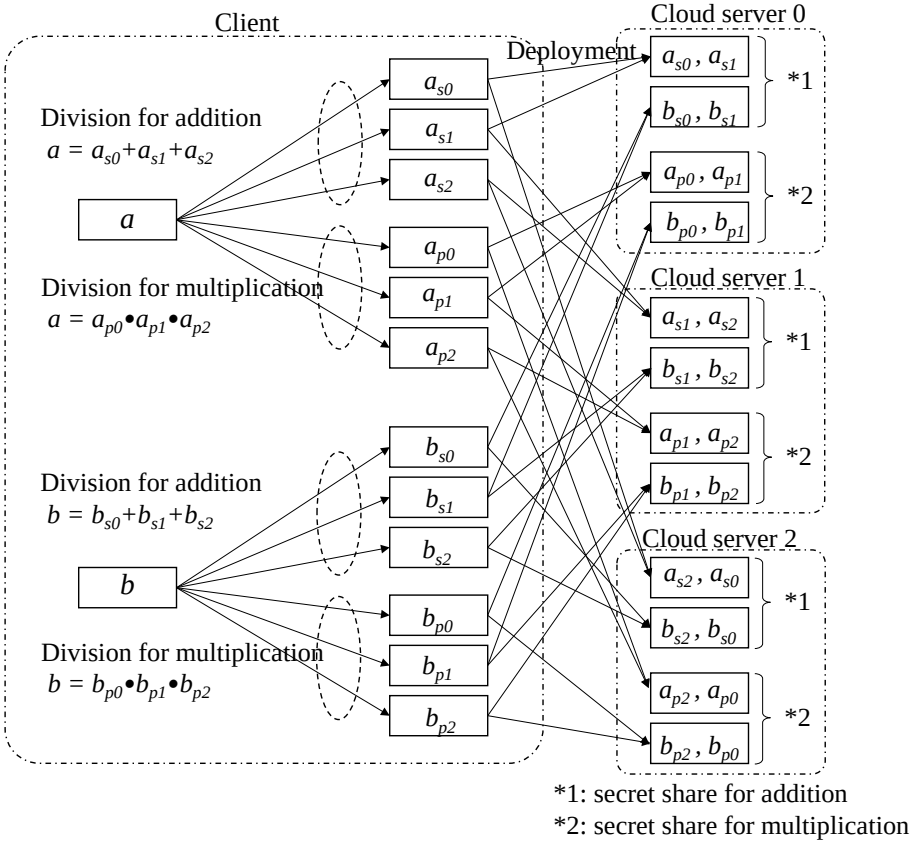

図２　簡易型秘密計算法

加減算用のシェアは従来のセキュアマルチパーティ法と同様に、数値 a、b を、乱数を使って a=Sa0+Sa1+Sa2、b=Sb0+Sb1+Sb2 となるように(Sa0, Sa1, Sa2)および(Sb0, Sb1, Sb2)を自社サーバで分割し、(Sa0, Sa1)、(Sb0, Sb1)を外部サーバ 0 に、(Sa1, Sa2)、(Sb1, Sb2)を外部サーバ 1 に、(Sa2, Sa0)、(Sb2, Sb0)を外部サーバ 2 に分散配置する。

次に乗除算用のシェアとして数値 a、b を乱数を使って a=Pa0･Pa1･Pa2、b=Pb0･Pb1･Pb2 となるように(Pa0, Pa1, Pa2)および(Pb0, Pb1, Pb2)を自社サーバで分割し、(Pa0, Pa1)、(Pb0, Pb1)を外部サーバ 0 に、(Pa1, Pa2)、(Pb1, Pb2)を外部サーバ 1 に、(Pa2, Pa0)、(Pb2, Pb0)を外部サーバ 2 に分散配置する。

従来の方式と同じように k=2、n=3 としたときを考える。加減算は同じである。乗算はサーバ n で Pan と Pbn および Pan+1 と Pbn+1 の乗算を行う。3 つのうち 2 つから結果を得られれば Pa0･Pb0、Pa1･Pb1、Pa2･Pb2 が揃うのでそれをかければ a･b を求めることができる。

(Pa0・Pb0)・(Pa1・Pb1)・(Pa2・Pb2)
＝(Pa0・Pa1・Pa2)・(Pb0・Pb1・Pb2)
＝a・b

除算についても同様に、サーバ n で Pan と Pbn および Pan+1 と Pbn+1 の除算を行う。3 つのうち 2 つから結果を得られれば Pa0/Pb0、Pa1/Pb1、Pa2/Pb2 が揃うのでそれをかければ a/b を求めることができる。

(Pa0/Pb0)・(Pa1/Pb1)・(Pa2/Pb2)
＝(Pa0・Pa1・Pa2)/(Pb0・Pb1・Pb2)
＝a/b

これら全ての場合も各サーバが持っているシェアは 3 つのうちの 2 つのみであり、秘密は保持される。また、k、n に対しても単純な計算方法なので、自由に選択し、システムを構成することができる。また、この簡易的秘密計算法では一度分けた和用乱数、積用乱数をそのまま使用するため、保存データ量は 0(データ数)となる。

②簡易的秘密計算の課題
簡易的秘密計算法では、加減算と乗除算が混在する計算、範囲検索のような比較計算では、中間結果を一旦クライアントに戻す必要がある。中間結果を一度クライアントに戻さない計算方法としては、サーバ間で情報を交換してサーバで最終結果まで計算してもらう仕組みが必要となる。
単にサーバで情報を交換すると、計算結果が漏れてしまうことになるため、中間結果に乱数を加えるかあるいは掛けることで、中間結果が漏れないようにする。また、サーバが中間結果を、交換して計算したのち、その最終結果をクライアントに戻すときには、中間結果に加えた乱数の逆数を加えることで、最終的な計算結果を得るものとする。
具体的には次のように計算する。
例えば、a、b、c、d の４つのデータを２つのクラウドサーバに秘密分散しているとする。それぞれ積のシェアを ap0, ap1, bp0, bp1, cp0, cp1, dp0, dp1 とする。このときに、となるような y の計算を要請したとする。すると、クラウドサーバ 0 では、x0＝ap0・bp0、y0＝cp0・dp0、クラウドサーバ１では、x1＝ap1・bp1、y1＝cp1・dp1 を計算するが、これをクラウド上で足すことはできず、クライアントに返して加算をする必要があった。この状況では、２つの配列データの積の総和といった計算がクラウド上でできない。

③サーバ間での中間結果交換方式の提案
上記の課題に対して、サーバ間の安全な中間結果の交換方式を提案する。クラウドサーバ 0 に r0、クラウドサーバ 1 に r1 という乱数を配置し、サーバ間で情報を交換する。つまり、クラウドサーバ 0 上の x0, y0 に r0 をかけたものをクラウドサーバ 1 に送り、クラウドサーバ 1 上の x1, y1 に r1 を掛けたものをクラウドサーバ 0 に送る。その結果、各クラウドには、r0・x0、r0・y0、r1・x1、r1・y1 がある。これから、

T= r0・x0・r1・x1＋r0・y0・r1・y1
= (r0・r1)(x0・x1＋y0・y1)
= (r0・r1)(ap0・bp0・ap1・bp1+ cp0・dp0・cp1・dp1)
= (r0・r1)(a・b + c・d)

が計算できる。T をクライアントに返せば、1/(r0・r1)で y が求まる。また、この計算を使うことで、クライアントに返すことなく、２つの配列データの積の総和といった計算ができるようになる。
我々は上記のアルゴリズムを、ＦＦＴ、位置情報サーバでの範囲検索、外れ値の検出についての秘密計算に適用できることを示した（学会発表論文①)。

(2)より複雑な計算への応用、Ｎパーティへの拡張アルゴリズム
提案した簡易型秘密計算アルゴリズムを機械学習に適用する方式について提案し、その有効性を確認した（成果雑誌論文①, ⑥、⑦)。機械学習では、大量の教師データからその特徴を抽出して学習する必要があるため、近年はクラウドにおける大量のデータストアとＣＰＵ資源を使った学習が行われる。しかし、教師データが機密情報である場合、情報漏洩リスクを考慮してクラウドで学習することに躊躇することも考えられる。秘密計算を適用することができるようになることで、情報漏洩のリスクを低下させることができるようになり、クラウドでの秘密情報を使った機械学習が利用できるようになる。
また、我々のアルゴリズムは、主に２～３パーティでの秘密分散を中心に検討してきたが、さらにＮパーティを使って秘密情報を分散する方式を提案している（学会発表論文③)。この方式

によって、多数のクラウドに情報を分散させることができるようになるため、情報の信頼性向上と漏洩リスクの低減に役立つ。

(3)クラウドの安全性分析手法の確立

クラウドの安全性を分析する方法として、ハードウェア信頼性(reliability)を扱う従来の信頼性理論の手法に倣い、安全性(security)を定量的に評価するためのモデルを提案した。ハードウェアの信頼性、ソフトウェア及び人間系の安全性を含めた情報システム全体としての安全性(safety and security)を確率モデルによって定式化し、これを安心性(trust-ability)の定量化の指標とした。
ハードウェアの可用率は、以下の式で評価される。

$$Availability \quad Av = \frac{MTBF}{MTBF + MTTR}$$

これに対して、安全可用性（Secure Availability）は以下の式で評価する。

$$SecureAvailability \quad SAv = \frac{MTBB}{MTBB + MTTS}$$

ここで、ＭＴＢＢは平均破断間隔（Mean Time Between Break of security)、ＭＴＴＳは平均回復時間（Mean Time To Secure state）である。
また、安全可用性は、システムを並列に配置した場合と直列に配置した場合では、そのトータルの可用性が以下のようになる。

(並列時) $SAv = \prod_{i=1}^{n} SAv_i$ （直列時） $SAv = 1 - \prod_{i=1}^{n} (1 - SAv_i)$

このモデルを複数のクラウドサーバを用いた秘密分散型のシステムに適用し、異なるシステム構成における安全可用性を算出した。そして、安全可用性の比較評価ができることを示した。この成果は、学会発表論文⑪で報告している。

５．主な発表論文等

〔雑誌論文〕（計 7 件）

①Hirofumi Miyajima, Noritaka Shigei, Hiromi Miyajima, and Norio Shiratori, ″Analog Q-learning Methods for Secure Multiparty Computation,″ IAENG International Journal of Computer Science, vol. 45, no. 4, pp623-629, 2018, 査読有, http://www.iaeng.org/IJCS/issues_v45/issue_4/IJCS_45_4_14.pdf

②Satoshi Utsumi, Salahuddin Muhammad Salim Zabir, Yuto Usuki, Seisho Takeda, Norio Shiratori, Yasushi Kato, Jeyeon Kim, “A new analytical model of TCP Hybla for satellite IP networks,” Journal of Network and Computer Applications, Elsevier, vol. 124, 15 December 2018, pp.137-147, 査読有, https://doi.org/10.1016/j.jnca.2018.09.015

③H. Miyajima, H., H. Miyajima, N. Shiratori, “Proposal of Security Preserving Machine Learning of IoT,” Artificial Intelligence Research, Vol.7, No.2, pp.26-33, 2018, 査読有, DOI: 10.5430/air.v7n2p26

④Yuria Oigawa, Fumiaki Sato, ″Improvement in IntErzone Routing Protocol of ZRP Based on Bloom Filter,″ Journal of Information Processing (JIP), vol. 26, pp. 124-131, 2018, 査読有, https://doi.org/10.2197/ipsjjip.26.124.

⑤Jia Liu, Yang Xu,Yulong Shen, Xiaohong Jiang, Norio Shiratori, ″Physical Layer Security-Aware Routing and Performance Tradeoffs in Wireless Ad Hoc Networks,″ Computer Networks, vol. 123, pp. 77-87, 2017, 査読有, https://arxiv.org/pdf/1609.02288.pdf

⑥Hirofumi Miyajima, Noritaka Shigei , Hiromi Miyajima, Yohtaro Miyanishi, Shinji Kitagami, Norio Shiratori, “New privacy preserving clustering methods for Secure Multiparty Computation,” Artificial Intelligence Research, Vol.6, No.1, pp27-36, DOI: 10.5430/xyz.vlnlpl, 2017, 査読有, https://doi.org/10.5430/air.v6n1p27

⑦Hirofumi Miyajima, Noritaka Shigei, Hiromi Miyajima, Yohtaro Miyanishi, Shinji Kitagami, and Norio Shiratori, ″New Privacy Preserving Back Propagation Learning for Secure Multiparty Computation,″ IAENG International Journal of Computer Science, vol. 43,no. 3, pp270-276, 2016, 査読有, http://www.iaeng.org/IJCS/issues_v43/issue_3/IJCS_43_3_01.pdf

〔学会発表〕(計 11 件)

①Kouta Takahashi, Fumiaki Sato, ″Securing of Clouds Based on Lightweight Secure Multi-party Computation,″ The 12th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS2018), 2018, 査読有

②Nonoko Ai, Akira Kanaoka, ″Empirical Analysis of Japanese Passwords,″ The 2018 IEEE Workshop on System Dependability and Security (WSDS 2018), 2018, 査読有

③滝 雄太郎, 藤田 茂, 宮西 洋太郎, 白鳥 則郎,“軽量 N パーティ秘匿関数計算の一般解と情報銀行の分散型セキュアストレージへの応用,” 情報処理学会マルチメディア, 分散協調とモバイルシンポジウム(DICOMO2017)論文集, 2017 年 6 月,定山渓.［優秀論文賞］・論文誌への推薦論文に選出, 査読有

④S. Sakumoto and A. Kanaoka, ″Improvement of Privacy Preserved Rule-Based Risk Analysis via Secure Multi-Party Computation,″ 12th Asia Joint Conference on Information Security (AsiaJCIS), 2017, 査読有

⑤Shota Kubota and Fumiaki Sato, ″Load Balancing in Wireless Mesh Networks Based on OpenFlow,″ The 20-th International Conference on Network-Based Information Systems (NBiS2017), pp.328-338, 2017.8.24, 査読有

⑥Fumiaki Sato, ″Indoor Navigation System Based on Augmented Reality Markers,″ The 11th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2017), pp.266-274, 2017.7.11, 査読有

⑦Shugo Miyamoto, Takamasa Koshizen, Takanari Matsumoto, Hiroaki Kawase, Makoto Higuchi, Yasuo Torimoto, Koji Uno, Fumiaki Sato, ″An Application Using a BLE Beacon Model Combined with Fully Autonomous Wheelchair Control,″ The 11th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS2017), pp.323-335, 2017.7.10, 査読有

⑧Hirofumi Miyajima, Noritaka Shigei, Hiromi Miyajima and Norio Shiratori, ″A Profit Sharing Method for Secure Multiparty Computation,″ IEEE 12th International Conference on Innovative Computing, Information and Control (ICICIC2017), Kurume, August 2017, 査読有

⑨Hirofumi Miyajima, Noritaka Shigei, Hiromi Miyajima, Yohtaro Miyanishi, Shinji Kitagami and Norio Shiratori, ″Privacy Preserving Fuzzy Modeling for Secure Multiparty Computation,″ Proceedings of the International Multi Conference of Engineers and Computer Scientists 2017 Vol I, IMECS2017, March 2017, Hong Kong, 査読有

⑩Ryohei Kikuchi, Fumiaki Sato, ″Hybrid Routing Scheme Combining with Geo-Routing and DTN in VANET″, 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2016, 査読有

⑪宮西 洋太郎, 北上 眞二, 荻野 正, 佐藤 文明, 浦野 義頼, 白鳥 則郎, ″情報システムの「安心性」評価モデルの提案″, 電子情報通信学会 SWIM 研究会, 2016 年 8 月 26 日, 査読無

６．研究組織

(1)研究分担者
研究分担者氏名：白鳥則郎
ローマ字氏名：(SHIRATORI, norio)
所属研究機関名：中央大学
部局名：研究開発機構
職名：機構教授
研究者番号（8 桁）：60111316

研究分担者氏名：金岡 晃
ローマ字氏名：(KANAOKA, akira)
所属研究機関名：東邦大学
部局名：理学部
職名：准教授
研究者番号（8 桁）：00455924

(2)研究協力者
研究協力者氏名：宮西 洋太郎
ローマ字氏名：(MIYANISHI, yotaro)