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　３０　年　　５　月　　９　日現在

機関番号：　１２６０１
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２７００

研究課題名（和文）情報検索システムにおけるプライバシー保護に関する研究

研究課題名（英文）A　Study of Privacy Protection in Information Retrieval

研究代表者
中川　裕志（NAKAGAWA, Hiroshi）

東京大学・情報基盤センター・教授

研究者番号：２０１３４８９３

交付決定額（研究期間全体）：（直接経費）　　13,400,000円

研究成果の概要（和文）：ビッグデータのうちでも特に有用な個人データの利活用が注目されているが、個人データのプライバシー保護は法律的にも義務付けられており、十分な利活用を実現するためには、プライバシー保護の技術を援用することが必須である。この研究では、プライバシー保護技術として、密度比推定への差分プライバシーの適用、差分プライバシーの理論的拡張、購買履歴データに対する匿名加工アルゴリズム、ダミー質問追加による質問意図の秘匿、質問への回答からのプライバシー漏洩対策、準同型性公開鍵暗号を用いるプライバシー保護技術の各々に対して、新規技術を提案し評価した。

研究成果の概要（英文）：Although the use of personal data which is particularly useful among big data is drawing attention, privacy protection of personal data is legally obligatory, and in order to realize sufficient utilization, it is indispensable to incorporate privacy protection technologies. In this research, as privacy protection technology, we propose new methods and evaluate them for the following research topics: application of differential privacy to density ratio estimation, theoretical expansion of differential privacy, algorithm to anonymize perchase history data, confidentiality of question intention by adding dummy question, countermeasures against leakage of privacy from answers to questions, privacy protection technology using isomorphic public key cryptography.

研究分野：　情報学

キーワード：　情報システム　プライバシー保護　個人情報　質問秘匿　差分プライバシー　準同型公開鍵暗号　匿名加工情報　個人情報保護法

１．研究開始当初の背景

ビッグデータのうちでも特に有用な個人データの利活用が注目されているが、そのためには個人プライバシーの保護が必須である。個人情報の多くは滞在位置情報、購買履歴、累積する特許情報などの時間とともに変動し集積するデータである。そこでデータ収集者がデータベースを保持､管理し、利用者はデータベースへ問い合わせをして望む情報のみを得る情報検索タイプの利用法が上記の欠点を克服する方法として有望であり、かつ完璧ではないにしても個人データの拡散を防ぎやすい。

このデータベースの情報検索におけるプライバシー保護には次の３つの課題が重要である。

・データベースにおける個人情報の保護
・データベースへの検索質問の意図
・データの収集路における個人データ保護

さらに平成 29 年 5 月 30 日に改正個人情報保護法が施行されたが、この改正法では個人データの第 3 者移転を可能とする匿名加工情報の概念が導入された。匿名加工情報はビッグデータとして有用性を活かすための法的な枠組みだが、その技術的定義は確定しておらず、匿名化技術の提案と評価が急務である。

２．研究の目的

データベースにおける個人情報の保護に関しては、以下のテーマ(1)(2)(3)について研究を行う。

データベースにおける情報検索の結果から個人識別を防ぐ方法として差分プライバシーが有力な方法として注目されてきた。ただし差分プライバシーは元データに雑音を加算する方法だが、ラプラス雑音の利用にほぼ限定されるなど汎用性に乏しかった。この状況を改善するために以下の 2 つのテーマを検討する。

(1)サンプリングと密度比推定：サンプリングされたデータから元データを密度比推定という手法で復元する際にさらに差分プライバシーによる雑音加算を適用することによって、元データの個人が識別されることを防ぐこととデータ有用性の両立を図る。

(2) 差分プライバシーの拡張：差分プライバシーでは実際の保護アルゴリズムとしてはほぼラプラス雑音の加算に限定される。この弱点を克服するために、差分プライバシーの数理モデルを拡張する。

(3)匿名加工アルゴリズム：改正個人情報保護法で導入された匿名加工情報を元の個人データのデータベースから変換する手法は個人情報保護委員会規則 19 条に記載されている。19 条 1 号から 4 号で、個人識別符号の削除、元データとの連結を不可能化すること、特異なデータの削除などが記載されている。しかし、個々のデータベースの事情を勘案する記述がある 19 条 5 号においては、個人間のデータの差異から個人が一意的に特定されないように変換することが求められていると解釈できる。ただし、このような目的が書かれているだけで、具体的な変換アルゴリズムが示されていない。したがって、匿名加工情報を実際の場で使おうとすると､19 条 5 号に沿うように元の個人データから匿名加工情報へ変換するアルゴリズムが必要になる。この研究では、このアルゴリズムについて検討する。

データベースへの検索質問の意図に関し

(4)質問意図秘匿：企業秘密保護において重要である特許検索における質問意図の保護方式を検討する。特許検索の場合、検索質問を通信路上で傍受する攻撃者のだけではなく、検索エンジンを提供する事業者が、質問意図を推定しようとする攻撃者である可能性がある。特に後者の場合、検索エンジン側は特定の質問者の質問履歴を保持している場合も想定できるため、質問の意図秘匿は非常に達成困難な目標となる。

(5)データベースに対し利用者が情報検索を行う場合に、利用者の質問およびデータベースにプライベートな情報が含まれる場合には適切な保護手法を取ることが望ましい。秘密計算を用いることによってデータ自体を秘匿することは可能になっていたが、質問の回答からのプライバシー漏洩はあまり議論されてこなかった。また、データベース作成をプライバシーを保護して行う場合、悪意のあるデータを検知、排除する仕組みはゼロ知識証明等を用いるような方法が存在するが、計算コストが高い上に事前に定義したルールでしか排除を行えなかった。

本研究では、まず質問への回答からのプライバシー漏洩の監査を行うために、開示情報におけるプライバシー漏洩評価方法を開発し、実データを用いて評価を行う。さらに、データベースを作成する際にプライバシーを保護しつつ悪意のあるデータ提供者のみを排除するための暗号を用いたフレームワークを開発し、その計算効率と安全性を評価する。

データ収集経路のプライバシー保護に関しては、以下の（6）のテーマについて研究を行う。

(6)暗号技術の利用：購買データや位置データなどの時系列を含む動的データを収集時に暗号技術を用いて加工する方法を提案、評価する。

３．研究の方法

(1)サンプリングデータを用いた場合の差分プライバシー：元々のデータをそのまま用いずに類似のデータ分布を持つ仮想的な分布を密度比推定と呼ばれる方法を利用して生成することによってプライバシー保護

する方法を提案し、シミュレーションで評価する。

(2) 差分プライバシーの拡張：差分プライバシーを包含するモデルとして Gibbs 事後分布を提案し、数理モデルとしての評価を行う。

(3) 匿名加工アルゴリズム： この検討は、すでに情報処理学会にて 2015 年から行われている競争型タスク PWSCUP[雑誌論文④、学会発表⑥⑧]の主催および競技者としての参加によって行う。
PWSCUP では、匿名加工を、a)データの有用性の維持と、b)匿名加工されデータから元の個人の識別率を低くする、という 2 つの相反する目的関数をできるだけ同時に満たすような匿名加工アルゴリズムの開発が求められている。本研究の期間に行われた PWSCUP2016、PWSCUP2017 においては、対象データは 1 年間の個人購買履歴データであった。購買履歴データはビジネス利用での価値が高い。そこで、本研究では、購買履歴の匿名加工情報への変換する匿名加工アルゴリズムを PWSCUP への参加を通して開発する。

(4) 質問意図秘匿：質問を構成する複数の単語に、ダミー質問単語を混合させる方法を検討する。ダミー質問単語の生成方法については研究成果の章で述べる。提案する方法の有用性を評価するために、実際の特許データで、検索意図秘匿性能を評価分析する。

(5)の質問への回答からのプライバシー漏洩対策としては以下の方法を検討する。
(5-a) プライバシー漏洩監査
プライバシー漏洩監査問題を以下のように定式化した。データベースがプライベートデータ x にある処理を行った結果 $f(x)$を回答することを考える。この $f(x)$を開示した場合に攻撃者が x の推定に成功する可能性の評価をプライバシー漏洩の指標とする。具体的な方式としては攻撃者が $f(x)$を取りうる x を列挙する。その候補の中に正解が出現する確率を攻撃成功確率として評価する。
(5-b) プライバシー保護異常検知フレームワーク
匿名に収集したデータに対し任意の異常検知手法を適用し、異常データのみ脱匿名化が可能なプライバシー保護フレームワークを提案する。

(6) 暗号技術の利用：収集時されたデータの持つ有用性を総合的に評価する数理モデルと、準同型性を満たす公開鍵暗号を利用した方法を提案する。

４．研究成果

(1)サンプリングと密度比推定：元データからのサンプル率を下げると、所定のプライバシー保護強度を確保するために必要な差分プライバシーで加算する雑音を低下させることができることをシミュレーションで確認した。つまり、当初の計画通りサンプリングによってプライバシー保護の強化と有用性の確保を両立できることを示した。[学会発表⑩⑫]

(2)差分プライバシーの拡張：元の分布と雑音加算された分布の KL ダイバージェンスが有界となる条件を利用するデータ数、Gibbs 事後分布を規定する逆温度パラメターによって定義できた。この条件は概略、損失関数が L-リプシッツ、事前分布の対数が強凸であるとまとめられる。[学会発表⑨]

(3) 匿名加工アルゴリズム:
ここでは、主に我々のチームが優勝（参加 15 チーム中 1 位）になった PWSCUP2016 で開発した匿名加工アルゴリズムについて説明する。

(3-1)PWSCUP のタスク

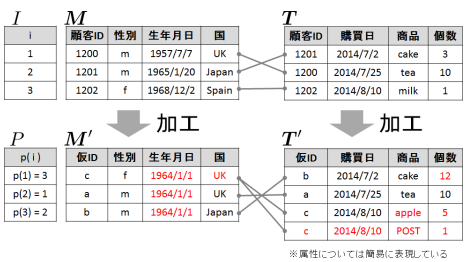

図１　購買履歴データ加工の流れ

PWSCUP では、下の図 1 のような個人購買履歴データの処理の流れとなる。
元データ I はデータベースのレコード ID、M は個人の静的な属性、T は個人の購買履歴データの集合が 1 レコードとなる。この図では一品目の購買だが、実際は 1 年間分の多数の品目の購買履歴が 1 レコードになる。
M´、T´は匿名加工アルゴリズムを適用して変換した結果である。
攻撃者は、M´と T´のレコードをリンクさせ、M´の仮 ID と M の顧客 ID と一致すなわち再識別を試みる。再識別の結果の対応表が P である。
匿名加工における有用性維持に関しては、主として次のような有用性指標を用いる。
・M の属性値によって顧客をクラスタに分

類し、各クラスタ内での集計値の加工前後の絶対誤差の平均値。
・M´からランダムに選んだ 10 人の顧客の連続する 30 日間の総購入額の平均値の M との差の最大値。
・個々の顧客が購入している商品項目の集合の加工前後での差。これは Jaccard 係数の全顧客の平均値で測る。ただし、この項目は Jaccard 係数＜0.7 という制約として働く。

PWSCUP においては、図 2 に示すように、参加各チームは主催者から配布された M、T に対して匿名加工したデータを提出する（匿名加工フェーズ）。各チームからの提出された匿名加工データに対して、他の全チームが再識別の攻撃を試みる（再識別フェーズ）。

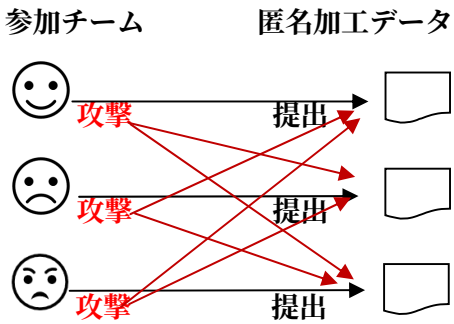

図 2　PWSCUP の競技の進行

有用性指標の値と再識別率の合計で順位はつける。つまり、この合計値が低いほど順位が高い。なお、他のチームから攻撃された結果の再識別率の最大値を順位付けで用いる。

(3-2)匿名加工アルゴリズム
研究代表者のチームは以下のようなアルゴリズムを用いて匿名加工した。
Step1: Jaccard 係数が上限 0.7 にできるだけ近い値になるように購買レコードをクラスタ化する。実際は、Jaccard 係数＝0.69 であり、400 人に購買データレコードは 89 個にクラスタ化された。
Step2:クラスタ内の各データを平均購買額などの有用性指標の悪化が最小になるようにランダムに移動する。例えば、図 3 に示すようにあるデータを右方向に平行移動した場合、同一クラスタ内の別のデータを同じ距離だけ逆方向（左方向）に移動する。

これによって、個人の購買額のクラスタ内平均は変化しない。このようなランダム化が十分であれば、クラスタ内のレコードは区別が困難になるため、攻撃者の再識別攻撃において、再識別に成功するのはクラスタにおいて 1 レコードだけとなるはずである。実際、研究代表者のチームの提出データにおいて再識別されたレコード数はクラスタ数の 89 に一致していたため、ク

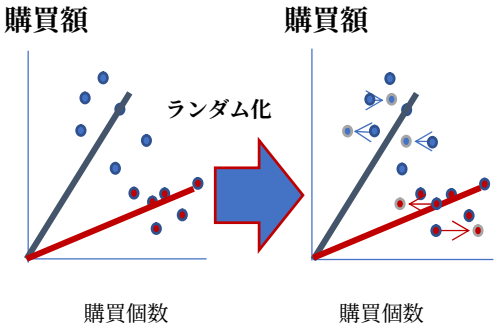

図 3　クラスタ内ランダム化

ラスタ内ランダム化は予想通りの効果を発揮したことになる。これは再識別率＝89/400=0.2225 である。この再識別率は、1 年分の購買履歴データ 400 人というデータに関してのものであり、普遍的な結果ではない。しかし、PWSCUP のタスクの定義から分かるように、攻撃者は元データ M、T を持っている最強の最大知識攻撃者である。また、1 年分の購買履歴は 1 レコードとしてまとめられている。さらに 400 人というのはデータベース収録人数としては小さく、再識別しやすい。これは攻撃側にとっては極めて有利であり、現実的応用では攻撃者はもっと弱いであろう。したがって、実際の再識別率は、この結果 0.2225 よりかなり低くなると予想される。以上の結果を[雑誌論文②、学会発表②③④]に発表した。

(4) 質問意図秘匿：
種々の質問意図秘匿の枠組みの比較調査結果を公開した[その他①]。この調査結果に基づき特許検索の検索質問にダミー質問追加、質問を構成する単語を複数の単語で置き換える曖昧化手法を実装して評価した。

利用した特許データベースは競争型情報検索タスク NTCIR6[引用文献①] で使われたものであり、特許データは 340 万文書、異なり単語数は 290 万である。また、質問数は 2900、質問当たりの平均単語数は 21 である。

上記の 2900 質問から（質問×単語）行列を作り、潜在意味分析（ＬＳＡ）を適用して複数の単語集合{wj:j=1,..}で表されるトピック t を抽出する。質問者が実際に発した質問 q=(q1,q2,..,qn)とする。ただし、ここで qi(i=1,n)は質問を構成する単語である。

まず、質問意図を推定しようとする攻撃者が事前知識を持っていない場合について種々の方法を評価した。その結果、質問 q の属するトピック t と異なるトピックから単語を選んでダミー単語として追加する方法が最も秘匿性能が高かった。具体的には、ダミーとして 5 単語追加した場合に約 20%、7 単語追加した場合に約 12%の場合で攻撃者から質問単語を正しく推定された。これらは、ほぼ理想的な確率で質問単語を秘匿できていると言える。すなわち、1 単語あたり k-1

単語をダミーとして追加すると、攻撃者が真の質問単語を推定できる確率はほぼ 1/k に近い推定率の低減を達成している。

一方、攻撃者が事前知識として質問者の質問履歴を保持している場合は、質問秘匿は困難である。なぜなら、その履歴を用いて新規質問が履歴から推定された質問と類似しているという条件で推定が可能だからである。この場合は、追加する質問を qi が属するトピック t と同じトピック t から単語 wj を選んで追加する方法が秘匿性能が最も高かった。同じトピックから選んだ単語は意味的類似性が高いため、性能がよかったと考えられる。それでも、7 単語ダミー単語を追加した場合ですら約 50%の確率で真の質問単語を正しく推定されてしまった。なお、他の方法では、攻撃者が事前知識を持たない場合に性能のよかった異なるトピックからダミー単語を選ぶ方法でも 70%程度は攻撃者が推定に成功してしまい、その他の方法では 90%以上が正しく推定されてしまった。

この結果からみて攻撃者が事前知識として質問者の質問履歴を保持する場合は、質問秘匿は現実的に困難であると言わざるをえない。これ以外の方法としては、質問、データベースの双方を質問者が秘密鍵と公開鍵を持つ準同型公開鍵暗号で暗号化したうえで検索を行う方法が知られている。この方法であれば、攻撃者に検索過程を知られることはないので、質問の秘匿性能は極めて高い。ただし、大規模データベースを質問ごとに暗号化する計算量は膨大であり、いまだ大規模データベースに適用するには、計算時間の点で実用的レベルに達していない。

(5-a) **プライバシー漏洩監査**
方法で記載した f を線形に変換でき、x が離散の場合は列挙を整数計画問題として評価し、ソルバーを用いて効率的に評価することが可能であった。本研究は実データとしてゲノム検査のデータを用い、実際にゲノム由来の疾患発症確率からゲノム自体の漏洩リスクを 3.20GHz CPU 、4GB RAM の Linux **マシンで 1 秒以下と効率的に評価することに成功した。**

(5-b) **プライバシー保護異常検知フレームワーク**
具体的に、メッセージ依存開示可能グループ署名 (Group signatures with message -dependent opening、 GS-MDO) **及び非対話開示可能公開鍵暗号** (Public key encryption with non-interactive opening, PKENO)**を用い、3 パーティーに権限を分散しデータ提供者を単独で特定可能ないわゆるビッグブラザーがビッグブラザーを作らないシステムを提案した**[学会発表⑤]。**実装の結果、提案フレームワークのオーバーヘッドが高々数 10 ミリ秒程に収まることを確認した。**

(6) **暗号技術の利用：準同型性公開鍵暗号を用いるプライバシー保護技術に関して加法準同型性暗号を用いて、分散したデータベース間で任意のブール関数を適用した部分集合について決定木学習を行うアルゴリズムを発表した**[雑誌論文⑥]。

＜引用文献＞

①Fujii, A., Iwayama, M., and Kando, N. (2007). Overview of the Patent Retrieval Task at the NTCIR-6 Workshop. In *NTCIR*.

５．主な発表論文等

〔雑誌論文〕（計 6 件）
① 中川裕志、プライバシー保護の技術、質問者の保護から個人情報秘匿技術まで, 情報管理 Vol.60、No.10、2017 p. 710-718, https://doi.org/10.1241/johokanri.60.710 , https://www.jstage.jst.go.jp/article/johokanri/60/10/60_710/_article/-char/ja/
② 中川裕志、最強攻撃者モデルにおける履歴データのプライバシー保護, ESTRELA, No.276, 2017、pp.14-20, 公益財団法人 統計情報研究開発センター https://**doi**.org/10.1241/johokanri.60.710
③ Hiroaki Kikuchi, Katsumi Takahashi, Zipf Distribution Model for Quantifying Risk of Re-identication from Trajectory Data, Journal of Information Processing, 査読有、2016、Vol. 24 、No.5 pp. 816-823. (2017 年情報処理学会 JIP Outstanding Paper,) https://doi.org/10.2197/ipsjjip.24.816
④ 菊池浩明、匿名加工･再識別コンテスト Ice and Fire：匿名加工方式とその安全性を評価する試み、情報処理学会論文誌、 査読有、2016、57(9), pp. 1900-1910, (特集号招待論文) http://id.nii.ac.jp/1001/00174619/
⑤ 新原功一、菊池浩明、 e ラーニングをモデルとした内部犯行の予測因子の識別, 情報処理学会論文誌、査読有、Vol. 57, No. 9, pp. 2064 - 2076, 2016. http://id.nii.ac.jp/1001/00174640/
⑥ Hiroaki KIKUCHI, Kouichi ITOH, Mebae USHIDA, Hiroshi TSUDA, Yuji YAMAOKA 、 Privacy-Preserving Decision Tree Learning with Boolean Target Class, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有、Vol. E98.A, No. 11, pp. 2291-2300, 2015. http://doi.org/10.1587/transfun.E98.A.2291

〔学会発表〕（計 12 件）
① Hiroshi Nakagawa, Anonymization and Re-identification for Personal Transaction Data, Workshop on

Design Issues for a data Anonymization Competition (WODIAC) on Privacy Enhancing Technologies Symposium (PETS) 2017, Minneaplos, July 17, 2017

② **中川裕志、出町彰啓、中川拓麻、パーソナル履歴データに対する匿名化と再識別、**SCIS2017(**暗号と情報セキュリティシンポジウム**）2D1-4 **那覇、２０１７年１月２５日**

③ **野島 良、小栗 秀暢、菊池 浩明、中川 裕志、濱田 浩気、村上 隆夫、山岡 裕司、山口 高康、渡辺 知恵美、 購買履歴データの匿名加工における距離関数を使った指標設計法**, SCIS2017、2D1-3 **那覇、２０１７年１月２５日**

④ **小栗 秀暢、菊池 浩明、中川 裕志、野島 良、濱田 浩気、村上 隆夫、山岡 裕司、山口 高康、渡辺 知恵美、 匿名加工・再識別コンテスト** PWSCUP 2016 **の報告 ～安全性と有用性の評価～**, SCIS2017、2D1-1 **那覇、２０１７年１月２５日**

⑤ Hiromi Arai, Keita Emura, Takuya Hayashi. A Framework of Privacy Preserving Anomaly Detection 、 Providing Traceability without Big Brother, Workshop on Privacy in the Electronic Society (WPES 2017), Dallas, USA, 2017.

⑥ H. Kikuchi, T. Yamaguchi, K. Hamada, Y. Yamaoka, H. Oguri and J. Sakuma, Ice and Fire:Quantifying the Risk of Re-identication and Utility in Data Anonymization, IEEE 30th International Conference on Advanced Information Networking and Applications (AINA),pp. 1035-1042, IEEE, 2016 (**査読有**).

⑦ H. Kikuchi, H. Yasunaga, H. Matsui and C. I. Fan, Efficient Privacy -Preserving Logistic Regression with Iteratively Re-weighted Least Squares, 11th Asia Joint Conference on Information Security (AsiaJCIS), pp. 48-54, IEEE, 2016 (査読有).

⑧ Hiroaki Kikuchi, Takayasu Yamaguchi, Koki Hamada, Yuji Yamaoka, Hidenobu Oguri, Jun Sakuma, A Study from the Data Anonymization Competition Pwscup 2015, Data Privacy Management and Security Assurance (DPM 2016), (**査読有**) LNCS, volume 9963, pp. 230-237, Springer, 2016.

⑨ Kentaro Minami, Issei Sato, Hiromi Arai, Hiroshi Nakagawa、 Differential Privacy without Sensitivity. NIPS2016, (**査読有**)December 05-10, 2016,Centre Convencions Internacional Barcelona, Barcelona SPAIN

⑩ **中川裕志、荒井ひろみ、高林裕太、差分プライベート最小二乗密度比推定．第30 回人工知能学会全国大会，**1K2-2,**北九州市 北九州国際会議場，**2016 **年** 6 **月** 6 **日**

⑪ Bing Yang, Issei Sato, Hiroshi Nakagawa、 BayesianDifferential Privacy on Correlated Data. ACM SIGMOD2015. pp747-762, Melbourne, VIC, Australia on May 31 - June 4, 2015

⑫ **高林裕太，荒井ひろみ, 中川裕志、最小二乗密度比推定における差分プライバシー. 情報処理学会 コンピュータセキュリティシンポジウム** 2015, 2B2-2, **長崎ブリックホール**, 2015 **年** 10 **月** 22 **日**

〔**図書**〕（**計 １ 件**）

① **中川裕志、 プライバシー保護入門 -法制度と技術- 、 勁草書房、**2016、246

〔**産業財産権**〕

○**出願状況（計 ０ 件）**

○**取得状況（計 ０ 件）**

〔**その他**〕

ホームページ等

① **情報検索における質問者のプライバシー保護** https://www.slideshare.net/hirsoshnakagawa3/private-information-retrieval

６．研究組織

(1)**研究代表者**

中川 裕志（NAKAGAWA, Hiroshi）

東京大学・情報基盤センター・教授

研究者番号：20134893

(2)**研究分担者**

菊池 浩明（KIKUCHI, Hiroaki）

明治大学・総合理数学部・教授

研究者番号：20266365

荒井 ひろみ（ARAI, Hiromi）

国立研究開発法人理化学研究所･革新知能統合研究センター･研究員

研究者番号： 20631782

(3)連携研究者 なし

(4)研究協力者 なし