

令和 5 年 5 月 28 日現在

機関番号：32682

研究種目：基盤研究(A)（一般）

研究期間：2018～2022

課題番号：18H04099

研究課題名（和文）オープンな評価コンテストによる匿名加工アルゴリズムとリスク評価の研究

研究課題名（英文）Study on anonymization algorithm and risk to be re-identified using open data competition

研究代表者

菊池 浩明（Kikuchi, Hiroaki）

明治大学・総合数理学部・専任教授

研究者番号：20266365

交付決定額（研究期間全体）：（直接経費） 33,840,000円

研究成果の概要（和文）：本研究では、データの匿名化とプライバシー保護に焦点をおいている。個人データを匿名化するための様々な手法を評価するため、5回のコンペティションを開催し、匿名化の為の効果的な戦略と課題を明らかにしてきた。位置情報の匿名化に関する論文、医療データの匿名化に関する評価、匿名化のコストに関する数理モデルの提案や、個人データを提供際のユーザの行動因子をジャーナル論文にした。CSS 2022で受賞している。これらは、匿名化の理論や手法の発展に貢献し、個人データの保護という課題に対する実用的な解決策を与え、学術だけでなく社会における個人データの利活用とプライバシー保護の両方に貢献する。

研究成果の学術的意義や社会的意義

本研究により、これまで曖昧な評価基準が確立されていなかった個人データの匿名化技術に対して、定量的なリスク評価手法を提案することができた。位置情報、購買履歴、医療データなどのデータの種類に応じて、重要視される要求条件や再識別の脅威に対するインパクトが異なり、それらの要請を十分に配慮した匿名化手法が必要であることが分かってきた。これらの研究成果により、個人データの提供の背景にある理由のいくつかが明らかになり、個人データに対する漏洩や不正利用の脅威に対する生活者の不安を取り除き、匿名化に関する理解を深めることにより、医療や産業界における個人データ保護に貢献することが期待される。

研究成果の概要（英文）：Our study focused on the important issue of data anonymization and the challenges it poses for protecting individual privacy. We conducted five open competitions to evaluate different approaches to anonymizing personal data and identified both issues and best practices.

Our research resulted in several significant publications, including top conference papers at PET 2023 for anonymizing location traces and an IEEE big data paper studying medical data anonymization.

We published a journal paper studying a mathematical model for the cost of data anonymization and a journal paper that revealed user behavior in providing personal data, which was awarded at the IPSJ Computer Security Symposium. These publications contribute to the development of anonymization theory and methods and provide practical solutions to the challenge of protecting personal data.

Ultimately, our research has important implications for both academia and society, helping to advance the field of data privacy.

研究分野：データプライバシー

キーワード：個人情報 匿名化 プライバシー ビッグデータ k-匿名

1. 研究開始当初の背景

ビッグデータの持つ価値を最大限に利用しようとするビジネス活動が急速に進展している。Google, Amazon, Facebook, Apple(GAFA)の活動に代表されるターゲット広告では、GAFAが収集した個人データをビジネスに最大限に利用して巨額の利益を得ている。一方、個人データは発生源であるデータ主体自身のプライバシー保護を確保することが要請される。プライバシー保護はヨーロッパでは理念、人権として確立しているため、インターネット時代におけるプライバシー保護のための法整備として、2017年EUではGDPR(General Data Protection Regulation)が成立し、2018年に施行される。日本では2016年個人情報保護法が改正され、インターネット時代に対応する法整備が進んでいる。世界では類を見ない独自の概念として匿名加工情報が導入された。匿名加工情報は、個人データをデータ主体が容易に識別できないように処理することによって、ビジネス利用においてデータ主体の同意を必要とすることなく、自由な利活用ができるようにしたデータである。匿名加工情報がビジネスにおいて機能することは個人データの有効利用に資するところが大きい。

個人データの有用性保持とプライバシー保護は相反する目的なので、両者のバランスが重要である。匿名加工情報は、完璧な識別不可能は無理であるにしても、データ主体の識別ができないほど十分な匿名化処理が必要とされるように加工された個人データのデータベースである。しかしながら、匿名加工情報が再識別されるリスクを正しく評価することはそれほど自明ではない。リスクにも様々な種類があり、その脅威のインパクトもまちまちである(問題1 リスクの多様性)ためである。多くの技法が提案されているが、攻撃者に対する仮定に応じてリスクは変動し、万能な匿名化はないと言われている。

2. 研究の目的

そこで、本研究では、多様なデータのそれぞれについて、オープン型の評価コンテストを行い、多くの研究者による集合知により、公平で信頼できる匿名化技術の開発を試みる。参加者らは匿名加工を行うタスクと加工された匿名加工データを再識別してその安全性を正しく評価するタスクの二つに取り組む。コンテストを通じて、加工の際に見落としがちなアルゴリズムの脆弱性などの知見を得ることが出来、有用性と安全性のトレードオフの中で最適と考えられる加工パラメータ(差分プライバシーにおける ϵ)や評価手法の基準値(k-匿名性)の値なども、確立することが期待できる。

3. 研究の方法

本研究を実施するために、次の課題を設定して取り組んだ。

課題1. 匿名加工技術のオープンデータベース開発

本研究を実施するためには、個人情報としての法的な問題がなく、出来るだけ現実に近い大規模なデータベースを必要とする。購買履歴データ、移動履歴データ、ウェブ閲覧履歴、健康診断データなどを検討する。

課題2. 有用性指標の設計

準識別子(Quasi Identifier)とみなす静的属性、加工データの有用性指標、再識別リスクを評価する安全性指標がある。

課題3. 攻撃者の知識モデルと安全性指標

匿名加工データの再識別リスクは、攻撃の際に仮定する背景知識と動機づけなどに大きく依存する。本課題では、より現実的なモデルとして次の複数のモデルを発展させる。

課題4. 多様な匿名化アルゴリズムの開発

集合値データに対する個人適応型匿名化アルゴリズム、局所差分プライバシーに基づく匿名化アルゴリズムなどを検討する。

課題5. 欠損位置情報の推定とテンソル分解に基づく個人毎の遷移行列の学習

個人が普段から(SNSなどで)公開する移動位置情報からの再識別法として個人毎の遷移行列を用いた再識別法などを検討する。

課題6 PWSCUPの継続的实施による匿名化、再識別の評価環境の構築

研究者、技術者、データ保有者、データ消費者、情報サービス業者、医療情報研究者、統計学者を結集して客観的に解決し、その成果を広く一般に周知、発展させるために、匿名化、再識別技術の評価環境を構築する。

4. 研究成果

4.1 匿名化に関する数理モデル

購買履歴データ、医療データ、映画評価データ、移動履歴データなど、データセットに応じて最適な匿名化技術が存在する。k-匿名性を満たすようにするためにダミーデータを追加することで生じるコストとそれによる有用性劣化を定量化する数理モデルなどを提案した。また、局所

差分プライバシーを満たして加工した key-value データから、効果的にノイズを除去するアルゴリズムを提案した。これらの研究は、Springer の Journal of Ambient Intelligence and Humanized Computing や Journal of Medical Systems などの Impact Factor の高いジャーナルや、情報処理学会の英文誌 Journal of Information Processing などでも発表している。また、局所差分プライバシーに関する研究は、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 (DICOM) の優秀論文賞を受賞した。

4.2 リスク評価に関する研究成果

匿名化されたデータから攻撃者の背景知識に応じてどのような情報が漏洩するか、また、各種セキュリティ技術によりそれらのリスクをどれくらい削減できるかについて、数理モデルを提案し、オープンデータやインシデントデータベースを照合して相対リスクを算出した。これらの結果は、情報処理学会論文誌にて発表している。その一つは、情報処理学会論文誌ジャーナル特選論文に選出されている。

4.3 オープンコンテストに関する成果

情報処理学会プライバシーワークショップにおいて、データ匿名化コンテスト PWS Cup を 2018 年から毎年開催して、匿名化における課題や効果的なアルゴリズムなどの知見を共有している。本コンテストには、国内外の大学や企業研究所から 10 から 20 チームが参加し、技術を磨いている。これらのコンテストの設計については、コンピュータセキュリティシンポジウムにて論文として発表し、更に同学会デジタルプラクティスにてジャーナルにまとめている。位置情報に関する 2019 年のコンテストの知見をまとめたジャーナル論文は、プライバシー強化技術のトップカンファレンスである PETS 2023 にて採択されている。

4.4 個人情報の提供に関する社会的許容に関する成果

個人情報を匿名化して二次利用をすることに対する許容度は個人差が大きいが、提供を左右する共通した行動因子が存在する。大規模なユーザ研究により、提供する個人情報の種類や条件によってそれらを明らかにした。本研究は、情報処理学会コンピュータセキュリティシンポジウム 2022 によって、CSS 2022 奨励賞を受賞し、同学会論文誌に推薦論文として採択されている。

以上の様に、匿名化の理論や手法の発展に貢献し、個人データの保護という課題に対する実用的な解決策を与え、学術だけではなく社会における個人データの利活用とプライバシー保護の両方に貢献する。

5. 主な発表論文等

〔雑誌論文〕 計16件（うち査読付論文 15件 / うち国際共著 0件 / うちオープンアクセス 4件）

1. 著者名 Ito, S., Kikuchi, H. & Nakagawa, H.	4. 巻 1
2. 論文標題 Attacker models with a variety of background knowledge to de-identified data	5. 発行年 2019年
3. 雑誌名 Journal of Ambient Intelligence and Humanized Computing	6. 最初と最後の頁 1-11
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s12652-019-01394-z	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 山田 道洋, 菊池 浩明, 松山 直樹, 乾 孝治	4. 巻 60
2. 論文標題 個人情報漏洩の損害額の新しい数理モデルの提案	5. 発行年 2019年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 1528-1537
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -
1. 著者名 中川裕志	4. 巻 1
2. 論文標題 AI倫理指針の分析と個人データ利活用	5. 発行年 2019年
3. 雑誌名 JIPDEC IT-Report	6. 最初と最後の頁 14-18
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 無
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -
1. 著者名 Ryo Nojima, Hidenobu Oguri, Hiroaki Kikuchi, Hiroshi Nakagawa, Koki Hamada, Takao Murakami, Yuji Yamaoka, Chiemi Watanabe	4. 巻 26
2. 論文標題 How to Handle Excessively Anonymized Datasets	5. 発行年 2018年
3. 雑誌名 Journal of Information Processing	6. 最初と最後の頁 477-485
掲載論文のDOI (デジタルオブジェクト識別子) 10.2197/ipsj.jip.26.477	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 小栗 秀暢 , 黒政 敦史 , 中川 裕志 , 菊池 浩明 , 門田 将徳	4. 巻 9
2. 論文標題 個人データの保護と流通を目的とする匿名化と再識別コンテスト : PWSCup	5. 発行年 2018年
3. 雑誌名 デジタルプラクティス	6. 最初と最後の頁 659-684
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Hiroaki Kikuchi, Xuping Huang, Shigeta Ikuji, Manami Inoue	4. 巻 42
2. 論文標題 Privacy-Preserving Hypothesis Testing for Reduced Cancer Risk on Daily Physical Activity	5. 発行年 2018年
3. 雑誌名 Journal of Medical Systems	6. 最初と最後の頁 1月12日
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s10916-018-0930-9	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 Takuma Nakagawa, Hiromi Arai, Hiroshi Nakagawa	4. 巻 11
2. 論文標題 Personalized Anonymization for Set-Valued Data by Partial Suppression	5. 発行年 2018年
3. 雑誌名 Transactions on Data Privacy	6. 最初と最後の頁 219-237
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Yu Zhe, Kazuto Fukuchi, Youhei Akimoto, Jun Sakuma	4. 巻 10
2. 論文標題 Domain Generalization via Adversarially Learned Novel Domains	5. 発行年 2022年
3. 雑誌名 IEEE Access	6. 最初と最後の頁 101855 - 101868
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/ACCESS.2022.3209815	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 山田 道洋, 池上 和輝, 菊池 浩明, 乾孝治	4. 巻 61
2. 論文標題 セキュリティマネジメントによるサイバーインシデントリスク削減の評価	5. 発行年 2020年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 1781-1791
掲載論文のDOI (デジタルオブジェクト識別子) 10.20729/00208739	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Satoshi Ito, Reo Harada, Hiroaki Kikuchi	4. 巻 28
2. 論文標題 De-identification for Transaction Data Secure against Re-identification Risk Based on Payment Records	5. 発行年 2020年
3. 雑誌名 Journal of Information Processing	6. 最初と最後の頁 511-519
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s12652-021-03369-5	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Satoshi Ito, Hiroaki Kikuchi	4. 巻 2022
2. 論文標題 Estimation of cost of k-anonymity in the number of dummy records	5. 発行年 2022年
3. 雑誌名 J Ambient Intell Human Comput	6. 最初と最後の頁 1-10
掲載論文のDOI (デジタルオブジェクト識別子) 10.1007/s12652-021-03369-5	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 伊藤 聡志, 池上 和輝, 菊池 浩明	4. 巻 62
2. 論文標題 健康診断データとレセプトデータの匿名加工情報を用いた疾病リスク分析	5. 発行年 2021年
3. 雑誌名 情報処理学会論文誌,	6. 最初と最後の頁 1560-1574
掲載論文のDOI (デジタルオブジェクト識別子) 10.20729/00212761	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Takao Murakami, Hiromi Arai, Koki Hamada, Takuma Hatano, Makoto Iguchi, Hiroaki Kikuchi, Atsushi Kuromasa, Hiroshi Nakagawa, Yuichi Nakamura, Kenshiro Nishiyama, Ryo Nojima, Hidenobu Oguri, Chiemi Watanabe, Akira Yamada, Takayasu Yamaguchi, and Yuji Yamaoka	4. 巻 2023
2. 論文標題 Designing a Location Trace Anonymization Contest	5. 発行年 2023年
3. 雑誌名 Proceedings on Privacy Enhancing Technologies (PoPETs)	6. 最初と最後の頁 225-243
掲載論文のDOI (デジタルオブジェクト識別子) 10.56553/popets-2023-0014	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 中川 裕志, 菊池 浩明	4. 巻 63
2. 論文標題 個人データの利用に対する許容度に関する社会調査	5. 発行年 2023年
3. 雑誌名 情報処理学会論文誌	6. 最初と最後の頁 TBA
掲載論文のDOI (デジタルオブジェクト識別子) なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

1. 著者名 Yu Zhe, Kazuto Fukuchi, Youhei Akimoto, Jun Sakuma	4. 巻 10
2. 論文標題 Domain Generalization via Adversarially Learned Novel Domains	5. 発行年 2022年
3. 雑誌名 IEEE Access	6. 最初と最後の頁 101855 - 101868
掲載論文のDOI (デジタルオブジェクト識別子) 10.1109/ACCESS.2022.3209815	査読の有無 有
オープンアクセス オープンアクセスとしている (また、その予定である)	国際共著 -

1. 著者名 木村 映善, 窪寺 健, 長瀬 嘉秀	4. 巻 41
2. 論文標題 健診標準フォーマット実装ガイドの開発	5. 発行年 2021年
3. 雑誌名 医療情報学	6. 最初と最後の頁 225-235
掲載論文のDOI (デジタルオブジェクト識別子) 10.14948/jami.41.225	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 -

〔学会発表〕 計51件（うち招待講演 6件 / うち国際学会 19件）

1. 発表者名 Satoshi Ito, Reo Harada and Hiroaki Kikuchi
2. 発表標題 De-identification for Transaction Data Secure against Re-identification Risk Based on Payment Records
3. 学会等名 The 15th International Conference on Modeling Decisions for Artificial Intelligence (MDAI 2019) (国際学会)
4. 発表年 2019年

1. 発表者名 村上隆夫, 荒井ひろみ, 井口誠, 小栗秀暢, 菊池浩明, 黒政敦史, 中川裕志, 中村優一, 西山賢志郎, 野島良, 波多野卓磨, 濱田浩気, 山岡裕司, 山口高康, 山田明, 渡辺知恵美
2. 発表標題 PWS Cup 2019: ID識別・トレース推定に強い位置情報の匿名加工技術を競う
3. 学会等名 コンピュータセキュリティシンポジウム2019
4. 発表年 2019年

1. 発表者名 伊藤 聡志, 菊池 浩明
2. 発表標題 履歴データの数理モデルの提案とk-匿名化に必要なダミーレコード数推定への応用
3. 学会等名 情報処理学会, 研究報告コンピュータセキュリティ (CSEC)
4. 発表年 2019年

1. 発表者名 伊藤 聡志, 菊池 浩明
2. 発表標題 履歴データに対する匿名化モデルk-concealmentの改良手法の提案
3. 学会等名 コンピュータセキュリティシンポジウム2019論文集
4. 発表年 2019年

1. 発表者名 藤田真浩, 飯田泰興, 服部充洋, 山中忠和, 松田規, 菊池浩明
2. 発表標題 匿名加工実施者の意図に着目した匿名加工手法評価システム
3. 学会等名 暗号と情報セキュリティシンポジウム SCIS 2020
4. 発表年 2020年

1. 発表者名 金子侑紀, 小野敦樹, 伊藤 聡, 服部充洋, 飯田泰興, 藤田真浩, 山中忠和, 菊池浩明
2. 発表標題 匿名加工情報取扱事業者を調査するクローラーシステムの開発
3. 学会等名 情報処理学会, 第82回全国大会講演論文集
4. 発表年 2020年

1. 発表者名 伊藤 聡志, 菊池 浩明
2. 発表標題 履歴データの数理モデルの提案とk-匿名化に必要なダミーレコード数推定への応用
3. 学会等名 情報処理学会, 研究報告コンピュータセキュリティ (CSEC)
4. 発表年 2020年

1. 発表者名 Hiroshi Nakagawa
2. 発表標題 AI and Accountability
3. 学会等名 International Symposium on "Digital Science Now" in association with the G20 Ministerial Meeting on Trade and Digital Economy (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 中川裕志
2. 発表標題 AI 倫理と個人データ
3. 学会等名 MyData Japan 2019 (招待講演)
4. 発表年 2019年

1. 発表者名 Hiroshi Nakagawa
2. 発表標題 AI Ethics and Accountability
3. 学会等名 The 21'st Artificial Intelligence Forum(AI Forum 2019) (招待講演) (国際学会)
4. 発表年 2019年

1. 発表者名 石金 正裕, 鈴木 久美子, 郁 傑夫, 木下 典子, 木村 映善, 大曲 貴夫
2. 発表標題 スウェーデンのプライマリケアにおける抗菌薬適正使用に有用な医療 IT システム の実態
3. 学会等名 医療情報学39
4. 発表年 2019年

1. 発表者名 木村 映善
2. 発表標題 フィンランドにおける医療健康情報のレジスタの運用に関する制度の現状
3. 学会等名 2019年度統計関連学会連合大会講演報告集
4. 発表年 2019年

1. 発表者名 大寺 祥佑, 木村 映善, 佐々木 香織, 黒田 知宏
2. 発表標題 本邦がフィンランドにおける医療情報の二次利用の実態から学べること
3. 学会等名 医療情報学39(Suppl.)
4. 発表年 2019年

1. 発表者名 佐々木 香織, 木村 映善, 大寺 祥佑
2. 発表標題 イングランドにおける医療情報の二次利用の制度、特に市民からの信頼再建を試みる社会的なシステム構築から日本の制度基盤を展望する
3. 学会等名 医療情報学39(Suppl.)
4. 発表年 2019年

1. 発表者名 伊藤 伸介, 木村 映善
2. 発表標題 医療情報の二次利用の制度に関する現状
3. 学会等名 医療情報の二次利用の制度に関する現状
4. 発表年 2019年

1. 発表者名 Hiromu Yakura, Youhei Akimoto, Jun Sakuma
2. 発表標題 Generate (non-software) Bugs to Fool Classifiers
3. 学会等名 The 34th AAAI Conference on Artificial Intelligence (AAAI) (国際学会)
4. 発表年 2020年

1 . 発表者名 Hiromu Yakura, Jun Sakuma
2 . 発表標題 Robust Audio Adversarial Example for a Physical Attack
3 . 学会等名 The 28th International Joint Conference on Artificial Intelligence (IJCAI) (国際学会)
4 . 発表年 2019年

1 . 発表者名 Thien Q. Tran, Jun Sakuma
2 . 発表標題 Seasonal-adjustment Based Feature Selection Method for Predicting Epidemic with Large-scale Search Engine Logs
3 . 学会等名 25th ACM SIGKDD Conference On Knowledge Discovery And Data Mining (SIGKDD) (国際学会)
4 . 発表年 2019年

1 . 発表者名 Satoshi Ito, Hiroaki Kikuchi
2 . 発表標題 Risk of Re-identification from Payment Card Histories in Multiple Domains
3 . 学会等名 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (国際学会)
4 . 発表年 2018年

1 . 発表者名 Kodai Nagata, Hiroaki Kikuchi, Chun-I Fan
2 . 発表標題 Risk of Bitcoin Addresses to be Identified from Features of Output Addresses
3 . 学会等名 2018 IEEE Conference on Dependable and Secure Computing (DSC) federated workshop (国際学会)
4 . 発表年 2018年

1. 発表者名 Satoshi Ito, Hiroaki Kikuchi, Hiroshi Nakagawa
2. 発表標題 Risk of Re-identification Based on Euclidean distance in Anonymized Data PWSCUP2015
3. 学会等名 The 15th International Conference on Modeling Decisions for Artificial Intelligence (MDAI 2018) (国際学会)
4. 発表年 2018年

1. 発表者名 濱田 浩気 , 荒井 ひろみ , 小栗 秀暢 , 菊池 浩明, 黒政 敦史, 中川 裕志, 西山 賢志郎 , 波多野 卓磨, 村上 隆夫, 山岡 裕司, 山田 明, 渡辺 知恵美
2. 発表標題 PWS Cup 2018: 匿名加工再識別コンテストの設計～履歴データの一般化・再識別～
3. 学会等名 コンピュータセキュリティシンポジウム2018論文集
4. 発表年 2018年

1. 発表者名 山田 道洋 , 菊池 浩明
2. 発表標題 k-匿名性の安全性について
3. 学会等名 情報処理学会研究報告, コンピュータセキュリティ研究会 (CSEC), Vol. 2019-CSEC-84, No. 34, 2019.
4. 発表年 2018年

1. 発表者名 中川裕志
2. 発表標題 人工知能倫理と社会、法律との係わり方を展望する
3. 学会等名 enPiT第7回シンポジウム、基調講演, 2019年1月24日 (招待講演)
4. 発表年 2019年

1. 発表者名 中川裕志
2. 発表標題 人工知能倫理と法制度、社会
3. 学会等名 情報法制研究所、情報法制学会共催 第5回情報法セミナー in 京都, 京都大学, 2018年12月2日 (招待講演)
4. 発表年 2018年

1. 発表者名 中川裕志
2. 発表標題 AIネットワーク時代に向けた法・政策の在り方
3. 学会等名 "AIネットワーク化における倫理とプライバシーシンポジウム 基調講演, 主催: 大阪大学大学院法学研究科及び高等司法研究科" (招待講演)
4. 発表年 2018年

1. 発表者名 堀込 光, 菊池 浩明
2. 発表標題 Local Differential Privacyによりプライバシーを考慮した位置情報分布推定
3. 学会等名 マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO 2020)
4. 発表年 2020年

1. 発表者名 伊藤 聡志, 池上 和輝, 菊池 浩明
2. 発表標題 匿名加工情報の応用(1): 健康診断データとレセプトデータの分析とプライバシーリスク評価
3. 学会等名 コンピュータセキュリティシンポジウム2020論文集
4. 発表年 2020年

1. 発表者名 池上 和輝 , 伊藤 聡志 , 菊池 浩明
2. 発表標題 匿名加工情報の応用(2): 各種傷病を予測する健康診断モデル
3. 学会等名 コンピュータセキュリティシンポジウム2020論文集
4. 発表年 2020年

1. 発表者名 菊池 浩明
2. 発表標題 匿名化による差分プライベートな購入履歴プロファイリング
3. 学会等名 コンピュータセキュリティシンポジウム2020論文集
4. 発表年 2020年

1. 発表者名 Hiromu Yakura, Youhei Akimoto, Jun Sakuma:
2. 発表標題 Generate (Non-Software) Bugs to Fool Classifiers
3. 学会等名 AAAI 2020 (国際学会)
4. 発表年 2020年

1. 発表者名 Kikuchi H.
2. 発表標題 Differentially Private Profiling of Anonymized Customer Purchase Records
3. 学会等名 Data Privacy Management, Cryptocurrencies and Blockchain Technology, DPM 2020 (国際学会)
4. 発表年 2020年

1. 発表者名 菊池浩明, 馬 瑞強
2. 発表標題 糖尿病罹患リスクを予測するヘルスケアデータの匿名化コンテストPWS Cup 2021 データの解析
3. 学会等名 2022年暗号と情報セキュリティシンポジウム SCIS 2022
4. 発表年 2022年

1. 発表者名 伊藤聡志, 菊池浩明
2. 発表標題 完全 k-concealment 匿名化を求める 精度の高いアルゴリズムの評価
3. 学会等名 コンピュータセキュリティシンポジウム2021論文集
4. 発表年 2021年

1. 発表者名 菊池浩明, 荒井ひろみ, 井口誠, 小栗秀暢, 黒政敦史, 千田浩司, 中川裕志, 中村優一, 西山賢志郎, 野島良, 波多野卓磨, 濱田浩気, 古川諒, 馬瑞強, 前田若菜, 村上隆夫, 山岡裕司, 山田明, 渡辺知恵美
2. 発表標題 PWS Cup 2021 - 糖尿病罹患リスクを予測するヘルスケアデータの匿名化コンテスト
3. 学会等名 コンピュータセキュリティシンポジウム2021論文集
4. 発表年 2021年

1. 発表者名 Kikuchi H.
2. 発表標題 Reidentification Risk from Pseudonymized Customer Payment History
3. 学会等名 Advanced Information Networking and Applications. AINA 2021 (国際学会)
4. 発表年 2021年

1. 発表者名 Kikuchi H., Yamada M., Ikegami K., Inui K.
2. 発表標題 Best Security Measures to Reduce Cyber-Incident and Data Breach Risks
3. 学会等名 Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2021 (国際学会)
4. 発表年 2022年

1. 発表者名 Kikuchi H., Ono A., Ito S., Fujita M., Yamanaka T.
2. 発表標題 Web Crawler for an Anonymously Processed Information Database
3. 学会等名 Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS 2021) (国際学会)
4. 発表年 2021年

1. 発表者名 堀込 光, 菊池 浩明, Chia-Mu Yu
2. 発表標題 key-valueデータにおける局所差分プライバシーアルゴリズムPrivKVの改良
3. 学会等名 マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO 2022)
4. 発表年 2022年

1. 発表者名 中川 裕志, 菊池 浩明
2. 発表標題 個人データの利用に対する許容度に関する社会調査
3. 学会等名 コンピュータセキュリティシンポジウム2022論文集
4. 発表年 2022年

1. 発表者名 Horigome, H., Kikuchi, H., Yu, CM.
2. 発表標題 Expectation-Maximization Estimation for Key-Value Data Randomized with Local Differential Privacy
3. 学会等名 Advanced Information Networking and Applications. AINA 2023 (国際学会)
4. 発表年 2023年

1. 発表者名 Horigome, H., Kikuchi, H.
2. 発表標題 Improvement of Estimate Distribution with Local Differential Privacy
3. 学会等名 Modeling Decisions for Artificial Intelligence. MDAI 2022 (国際学会)
4. 発表年 2022年

1. 発表者名 Hiroaki Kikuchi, Satoshi, Ito, Kazuki Ikegami, and, Shota Shindo
2. 発表標題 Diseases Prediction from Officially Anonymized Medical and Healthcare Big Data
3. 学会等名 2022 IEEE International Conference on Big Data (Big Data) (国際学会)
4. 発表年 2022年

1. 発表者名 Daiki Nishiyama, Kazuto Fukuchi, Youhei Akimoto, Jun Sakuma
2. 発表標題 CAMRI Loss: Improving Recall of a Specific Class without Sacrificing Accuracy
3. 学会等名 IJCNN 2022 (国際学会)
4. 発表年 2022年

1. 発表者名 Shunta Ishihara, Chiemi Watanabe, Toshiyuki Amagasa
2. 発表標題 Supporting Insertion in an Encrypted Multi-Maps with Volume Hiding using Trusted Execution Environment
3. 学会等名 The Proceedings of 24th International Workshop on Design, Optimization, Languages and Analytical Processing of Big Data (DOLAP 2022) (国際学会)
4. 発表年 2022年

1. 発表者名 木村映善
2. 発表標題 認定事業者におけるリモートエグゼキューションの検討
3. 学会等名 2021年度統計関連学会連合大会講演報告集. 2021
4. 発表年 2021年

1. 発表者名 木村 映善
2. 発表標題 観察研究に資するRWD収集におけるCDMの意義
3. 学会等名 日本医療情報学会 第41回医療情報学連合大会
4. 発表年 2021年

1. 発表者名 木村 映善
2. 発表標題 リアルワールドデータを利用した国際的臨床研究への参加にむけて
3. 学会等名 愛媛医学
4. 発表年 2021年

1. 発表者名 木村 映善, 大寺 祥佑, 佐々木 香織, 黒田 知宏
2. 発表標題 フィンランドにおける医療分野レジスタとデータ提供の状況
3. 学会等名 日本統計学会誌
4. 発表年 2020年

1. 発表者名 木村 映善
2. 発表標題 ポータレス時代の IPS へのロードマップ考
3. 学会等名 医療情報学40(Suppl)
4. 発表年 2020年

1. 発表者名 入野 了士, 木村 映善, 石田 博, 栗原 幸男
2. 発表標題 健診データの利活用および外部提供に関する健診機関の方針と課題
3. 学会等名 医療情報学
4. 発表年 2020年

〔図書〕 計2件

1. 著者名 中川裕志	4. 発行年 2019年
2. 出版社 近代科学社	5. 総ページ数 176
3. 書名 裏側から視るAI 脅威・歴史・倫理	

1. 著者名 Kerrie L. Holley、Siupo Becker, M.D. 著、木村 映善 監訳、岡 響 訳	4. 発行年 2022年
2. 出版社 オライリー・ジャパン	5. 総ページ数 268
3. 書名 AIファースト・ヘルスケア 医療現場におけるAIアプリケーションの利用	

〔産業財産権〕

〔その他〕

<p>オープンな評価コンテストによる匿名加工アルゴリズムとリスク評価の研究 https://windy.mind.meiji.ac.jp/Kakenhi-Cup2018/ https://www.kikn.fms.meiji.ac.jp/Kakenhi-Cup2018/</p>

6. 研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究分担者	中川 裕志 (Nakagawa Hiroshi) (20134893)	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・チームリーダー (82401)	
研究分担者	渡辺 知恵美 (Watanabe Chiemi) (20362832)	筑波技術大学・産業技術学部・准教授 (12103)	
研究分担者	木村 映善 (Kimura Eizen) (20363244)	愛媛大学・医学系研究科・教授 (16301)	

6. 研究組織（つづき）

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究分担者	村上 隆夫 (Murakami Takao) (80587981)	国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員 (82626)	
研究分担者	佐久間 淳 (Sakuma Jun) (90376963)	筑波大学・システム情報系・教授 (12102)	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関