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　６ 年　 ６ 月 １０ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2020～2023
課題番号：２０Ｋ１１８３０

研究課題名（和文）プライバシーと情報価値のバランスを考慮したIoT情報の記録および共有方法の研究

研究課題名（英文）Study on Method for Storing and Sharing IOT information that takes into account privacy and utility

研究代表者

森本　康彦（MORIMOTO, Yasuhiko）

広島大学・先進理工系科学研究科（工）・教授

研究者番号：００３６３０１０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究では以下のような成果を得ることができた．（１）住所や位置情報サービスの緯度経度情報を，ｋ匿名化という観点でリスクを測定する方法を提案し，（２）その測定値のもとで，よりリスクの低い，位置情報匿名化手法を考案した．（３）また，画像データに関するプライバシー問題にも取り組み，そこでは，医療画像データをその画像としての視覚的情報を過度に失わないための多段階暗号化の研究を行った．（４）並行してブロックチェーン技術を利用した医療情報の共有手法，および，秘密分散計算技術に基づくスカイライン問合せ（広い意味でデータマイニング手法の１つ）による分散知識発掘手法を開発することができた．

研究成果の学術的意義や社会的意義
近年，人工知能が飛躍的に発展しているが，その発展に欠かせないのがビッグデータで，その質と量が知能の優劣に大きく影響を与える．そのため，データを保有する巨大プラットフォーマーが人工知能市場において圧倒的に優位に立っている．しかし，ビッグデータを保有しないものでも，多数が参加する情報分散共有プラットフォームが整備され，そのサイズが十分巨大になることで，人工知能市場における競争に加わることが可能となり，より健全な発展が期待できる．本研究で得られた成果は，そうした情報共有，利用（知識発掘）におけるプライバシーリスクを減らすための技術と位置付けることができ，概要欄に示した各成果は学術雑誌に公表している．

研究成果の概要（英文）：This research has achieved the following results: (1) We proposed a method to measure the risk of address and latitude and longitude information from location information services in terms of k-anonymization, and (2) devised a location information anonymization method with lower risk based on these measurements. (3) We also addressed privacy issues related to image data, researching multi-stage encryption of medical image data to prevent excessive loss of visual information as an image. (4) In parallel, we were able to develop a medical information sharing method using blockchain technology, and a distributed knowledge mining method using skyline queries (a data mining method in a broad sense) based on secure distributed computation technology.

研究分野：知能情報学関連

キーワード：匿名化加工　ユーティリティ　プライバシー保護データマイニング　秘密計算　位置情報　医療情報

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

すべての人とモノがつながる Society5.0 と呼ばれる社会がまもなく到来する．そのような社会において各機器に保管される情報，機器間でやり取りされる情報がより安全に管理，有効利用できるよう，今のうちに知能情報学の視点で問題を洗い出し，対策を検討するため本研究は開始された．

信頼できる管理者の管理下にあるデータは，利用，開示するにあたって，適切な匿名化加工を施すなどプライバシーへの配慮がなされている．しかし，このように適切に保護されている情報が，その管理者の管理下から離れ，他の管理者の管理下にあるデータや外部知識などとリンクすることで，想定外の個人情報の特定にいたることがある．Society5.0 で提唱される社会は，これまで以上に個人情報漏洩リスクの高い状況も生み出しうる社会でもあるため，（研究当初の）情報共有の状態，分散計算のプロトコルが，プライバシー面でそれほど信頼はできないものと想定したうえで各部分問題を設定し，それらの課題を解き明かそうとした．

２．研究の目的

情報機器がつながることで生じうるプライバシー問題，プライバシーリスクについて検討し，対策する必要があると考え，それに関連する以下のような部分課題を設定し，その各課題について研究を進め，Society5.0 社会の発展に貢献することを目的とした．

（１）IoT 機器を通して，ほとんど無意識に様々な情報が記録されることになる．そのような情報のうち直接的，または間接的にプライバシーを侵害しうる要素を特定し，それぞれのリスクを測定する．以降，直接的，間接的にプライバシーを侵害しうる情報を「プライバシー情報」と呼ぶ．（２）プライバシー情報のうち，データマイニングなどの分析を行う価値の高いものに対して，その価値をできるだけ保った匿名化加工法を考案する．（３）分析価値の高いプライバシー情報のうち，比較的価値の低い別の関連情報を，削除あるいは加工することなどで，元データを匿名化加工せずに非プライバシー情報化する手法を考案する．（４）フィジカル空間で収集された IoT 情報の移動をサイバー空間でできるだけ局所化した状態で分析するプライバシー保護データマイニング手法（秘密分散計算技術）を開発する．以上の４つの要素技術を研究開発することで，プライバシーのリスクと情報価値のバランスを考慮した IoT 情報の記録および共有が可能となる．

３．研究の方法

本章，研究の方法，および，次章の研究成果は，前章，研究目的に記した（１）～（４）の部分課題番号を使用して，部分課題ごとに記載する．

【部分課題（１－２）の研究方法】

部分課題（１－２）に関連して，住所などの位置情報の匿名化手法について研究した．住所や位置情報は分析価値が高い一方で，プライバシーに特段の配慮が必要な情報である．

位置情報に関しては，正確な位置を特定できない程度のノイズを加えたり，点の情報をある程度の広さをもつ領域に置き換えたりするなどの匿名化手法が知られている．まずは，従来の手法で匿名化されたデータで，位置情報に関するマイニングがどの程度まで制約を受けるかを検証する研究を行った．具体的には，共同研究を行っているスーパーマーケットの ID-POS データを使って位置情報の匿名化を行ったうえで，我々が研究してきた時空間情報マイニングの様々な機能を使用し，位置情報に関する知見の発掘を試みた．距離との相関をある程度推定する問題においては，匿名化を行っていても,多くの価値のある知見を発見することができることを確認できた一方で，立地に関連する知見は大きく制約を受けることが分かった．

住所（空間上の点）はプライバシーの観点から強固な匿名化を必要とする．しかし，その分析価値は，位置そのものより，その立地に関わることからもたらされることが多いことがわかり，我々はその立地に注目した匿名化とデータマイニングについて検討を進めた．そこで．住所（空間上の点）やその緯度経度情報を完全に削除する代わりに，駅，スーパーマーケット，コンビニなど立地に関係する各種施設からの距離の「順位」に置き換えるという匿名化手法を考案した．位置情報がそのまま記録された実データを使ったマイニング結果と，同じデータを提案手法により匿名化したデータを使ったデータマイニング結果を比較したところ，得られる知見がほぼ

同じで，それでありながらプライバシーは保たれていることが確認できた．

【部分課題（３）の研究方法】

研究期間開始からほどなく，コロナ感染症が全世界的に流行した．その影響で，実際の移動や接触に対して想定外の制約を受けることになったため，位置情報に関する実データの収集はできず，まずは接触や移動をともなう実証実験を必要としない理論的な研究と研究用に提供されている公開データベースのみを使用する範囲内で実験できる課題にしぼって実施した．当初は時期を遅らせて実際の IoT 機器などを利用して教師データとなる実データを得ることを見込んでいたが，研究期間が４年間で，その３年目になっても事態が好転する気配がなかったため，最終的には，理論的な研究と研究用に提供されている公開データベースを使用する範囲内で実験できる課題の範囲でこの部分課題の研究を行った．

SNS 等でランドマークが映り込んだ写真等から，居住地，勤務地，学校名などが特定される事案が多く報告されている．我々は，このような問題に関連する研究課題として，画像データの暗号化，匿名化について検討した．この過程で医療データに対する多段階暗号化の研究を実施し，研究用に提供されている医療画像データに対して，実装し，検証を行った．提案した多段階暗号化手法は，主なベンチマークにおいて既存手法より高いセキュリティレベルを達成できた．

【部分課題（４）の研究方法】

医療情報などプライバシー情報を含むデータは，広く共有されることは望ましくないため，それを保有する組織にて局所的に保有，管理される．これら分散保有されたデータを統合した分析を安全に実行する問題にも取り組んだ．

この過程で，医療情報の共有をブロックチェーン技術を利用して安全に行う手法を発案し，その有効性を検証した．また，分散されたデータを巨大ビッグデータと見なし，そこからデータマイニングする意義はとても大きい．その第一歩として，秘密分散計算技術に基づくスカイライン問合せ（広い意味でデータマイニング手法の１つ）も開発した．

４．研究成果

【部分課題（１－２）の研究成果】
（情報価値とプライバシーのバランスを考慮した匿名化に関すること）

共同研究を行っているスーパーマーケットの ID-POS データを使って位置情報の匿名化を行ったうえで，顧客の居住地と当該スーパーマーケットの最寄り支店との距離，同居住地と競合店との距離が売り上げにどう影響しているかを分析し，販売戦略を立案するための参考情報として提供することができた．また，この分析手法を国際会議で発表し，そのビジネス上の価値を評価され，その国際会議において「Best Paper Award」を受賞した．

Yepeng Cheng, Yasuhiko Morimoto, “Competitors’ Influence Analysis of a Retailer by Using Customer Value and Huff’s Gravity Model,” International Journal of Physical and Mathematical Sciences, vol. 14, no. 8, pp. 67-75, 2020. (ICPTSP 2020: International Conference on Probability Theory and Stochastic Processes, Vancouver, Canada, September 23-24, 2020.)

住所（空間上の点）を，駅，スーパーマーケット，コンビニなど立地に関係する各種施設からの距離の「順位」に置き換えるという匿名化手法についても国際会議論文として報告した．

Naoto Iwata, Sayaka Kamei, Kazi Md. Rokibul Alam, Yasuhiko Morimoto, “Location Data Anonymization Retaining Data Mining Utilization,” Proceedings of International Conference on Advanced Data Mining and Applications (ADMA 2022), Springer LNAI 13726 (Part II), pp. 407-418, 2022.

これらの技術を適切に適用することで，情報の価値を保ちながら，特に住所（位置情報）を起点としたプライバシーリスクを大きく低減させられると期待できる．

【部分課題（３）の研究成果】

（安全なデータ共有と分散管理に関すること）

医療データなど，ユーザにとってデリケートな情報は組織内でも一部の人にしか情報は公開するべきではないため，暗号化した状態で保存する．その状態でも検索や比較が可能な状態とすることで，一部のデータマイニング機能も暗号化したままで実行できる．そのための手法を以下の国際会議論文で公表した．

Md. Shafiq Newaj Shovo, Kazi Md. Rokibul Alam, Dhrubajotee Howlader, Yasuhiko Morimoto, “A Sorting and Searching Scheme for Relational Database Using Searchable Encryption,” Proceedings of the 5th International Conference on Electrical Information and Communication Technology (EICT), pp. 1-5, 2021.

Md. Ahsan Habib, Kazi Md. Rokibul Alam, Yasuhiko Morimoto, "A Secure Medical Record Sharing Scheme Based on Blockchain and Two-fold Encryption," 2022 25th International Conference on Computer and Information Technology (ICCIT), IEEE, pp. 78-83, 2022.

情報によってはより高いセキュリティレベルが求められる．そのような要求に応えられる暗号化手法として以下の技術を発表した．

Md. Siddiqur Rahman Tanveer and Kazi Md. Rokibul Alam, Yasuhiko Morimoto, “A multi-stage chaotic encryption technique for medical image,” Information Security Journal: A Global Perspective, Taylor & Francis, Vol. 31, No. 6, pp. 657-675, 2022.

【部分課題（４）の研究成果】
（分散管理された情報源からの安全なデータマイニングに関すること）

秘密計算の枠組みを使ったスカイライン問合せ手法として，ブロックチェーンを利用したものとタグを利用したものの２種類開発し，それぞれ論文として発表した．

Md. Motaleb Hossen Manik, Kazi Md. Rokibul Alam, Yasuhiko Morimoto, “A Blockchain Based Secure Framework for User-centric Multi-party Skyline Queries,” Proceedings of International Conference on Computer and Information Technology (ICCIT), IEEE, pp. 90-95, 2022.

Dola Das, Kazi Md. Rokibul Alam, Yasuhiko Morimoto, " An Anonymity Retaining Framework for Multiparty Skyline Queries Based on Unique Tags," IEEE Transactions on Dependable and Secure Computing (Early Access), 2023.

スカイライン問合せとは，何らかの指標で他のデータに負けないデータだけを取り出す問い合わせで，その結果はあらゆる知識発掘の元として利用できる．スカイライン問合せから先の知識発掘は今後の課題となったが，分散管理された情報源から知識発掘の一部が行えるということは，ビッグデータを保有する巨大プラットフォーマでない，個々人でもネット上に分散するデータをビッグデータとして活用できる社会への第一歩となったと考えられる．

５．主な発表論文等

〔雑誌論文〕　計14件（うち査読付論文　14件／うち国際共著　10件／うちオープンアクセス　6件）

１．著者名 Tang Huidong、Kamei Sayaka、Morimoto Yasuhiko	４．巻 16
２．論文標題 Data Augmentation Methods for Enhancing Robustness in Text Classification Tasks	５．発行年 2023年
３．雑誌名 Algorithms	６．最初と最後の頁 59～59
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/a16010059	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 Iwata Naoto、Kamei Sayaka、Alam Kazi Md. Rokibul、Morimoto Yasuhiko	４．巻 -
２．論文標題 Location Data Anonymization Retaining Data Mining Utilization	５．発行年 2022年
３．雑誌名 Proceedings of International Conference on Advanced Data Mining and Applications (ADMA 2022)	６．最初と最後の頁 407～418
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-22137-8_30	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 該当する

１．著者名 Hossen Manik Md. Motaleb、Md. Rokibul Alam Kazi、Morimoto Yasuhiko	４．巻 -
２．論文標題 A Blockchain Based Secure Framework for User-centric Multi-party Skyline Queries	５．発行年 2022年
３．雑誌名 Proceedings of International Conference on Computer and Information Technology (ICCIT2022)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICCIT57492.2022.10055315	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 該当する

１．著者名 Habib Md. Ahsan、Md. Rokibul Alam Kazi、Morimoto Yasuhiko	４．巻 -
２．論文標題 A Secure Medical Record Sharing Scheme Based on Blockchain and Two-fold Encryption	５．発行年 2022年
３．雑誌名 Proceedings of International Conference on Computer and Information Technology (ICCIT2022)	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICCIT57492.2022.10054827	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 該当する

1．著者名 Tanveer Md. Siddiqur Rahman、Md. Rokibul Alam Kazi、Morimoto Yasuhiko	4．巻 -
2．論文標題 A multi-stage chaotic encryption technique for medical image	5．発行年 2021年
3．雑誌名 Information Security Journal: A Global Perspective	6．最初と最後の頁 1～19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/19393555.2021.1934197	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 該当する

1．著者名 Das Dola、Alam Kazi Md. Rokibul、Morimoto Yasuhiko	4．巻 -
2．論文標題 A Framework for Multi-party Skyline Query Maintaining Privacy and Data Integrity	5．発行年 2021年
3．雑誌名 Proceedings of the 24th International Conference on Computer and Information Technology (ICCIT)	6．最初と最後の頁 1～6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ICCIT54785.2021.9689854	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 該当する

1．著者名 Shovo Md. Shafiq Newaj、Alam Kazi Md. Rokibul、Howlader Dhrubajotee、Morimoto Yasuhiko	4．巻 -
2．論文標題 A Sorting and Searching Scheme for Relational Database Using Searchable Encryption	5．発行年 2021年
3．雑誌名 Proceedings of the 5th International Conference on Electrical Information and Communication Technology (EICT)	6．最初と最後の頁 1～5
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/EICT54103.2021.9733450	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 該当する

1．著者名 Yepeng Cheng, Yasuhiko Morimoto	4．巻 14
2．論文標題 Competitors’ Influence Analysis of a Retailer by Using Customer Value and Huff’s Gravity Model	5．発行年 2020年
3．雑誌名 International Journal of Physical and Mathematical Sciences	6．最初と最後の頁 67～75
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 オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　6件）

1．発表者名
Iwata Naoto、Kamei Sayaka、Alam Kazi Md. Rokibul、Morimoto Yasuhiko

2．発表標題
Location Data Anonymization Retaining Data Mining Utilization

3．学会等名
International Conference on Advanced Data Mining and Applications (ADMA 2022)（国際学会）

4．発表年
2022年

1．発表者名
Hossen Manik Md. Motaleb、Md. Rokibul Alam Kazi、Morimoto Yasuhiko

2．発表標題
A Blockchain Based Secure Framework for User-centric Multi-party Skyline Queries

3．学会等名
International Conference on Computer and Information Technology (ICCIT2022)（国際学会）

4．発表年
2022年

1．発表者名
Habib Md. Ahsan、Md. Rokibul Alam Kazi、Morimoto Yasuhiko

2．発表標題
A Secure Medical Record Sharing Scheme Based on Blockchain and Two-fold Encryption

3．学会等名
International Conference on Computer and Information Technology (ICCIT2022)（国際学会）

4．発表年
2022年

1．発表者名
Das Dola、Alam Kazi Md. Rokibul、Morimoto Yasuhiko

2．発表標題
A Framework for Multi-party Skyline Query Maintaining Privacy and Data Integrity

3．学会等名
International Conference on Computer and Information Technology (ICCIT)（国際学会）

4．発表年
2021年

１．発表者名
Shovo Md. Shafiq Newaj、Alam Kazi Md. Rokibul、Howlader Dhrubajotee、Morimoto Yasuhiko

２．発表標題
A Sorting and Searching Scheme for Relational Database Using Searchable Encryption

３．学会等名
International Conference on Electrical Information and Communication Technology (EICT)（国際学会）

４．発表年
2021年

１．発表者名
Yepeng Cheng, Yasuhiko Morimoto

２．発表標題
Competitors' Influence Analysis of a Retailer by Using Customer Value and Huff's Gravity Model

３．学会等名
International Conference on Probability Theory and Stochastic Processes (ICPTSP 2020)（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
Dr. Kazi Md. Rokibul Alam
http://www.kuet.ac.bd/cse/rokib/

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

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			
バングラデシュ	KUET			