研究レポート　No.10　～プライバシー保護と匿名化技術～

2020 年 10 月 28 日　株式会社アイズファクトリー　https://bodais.com/company/

概要

日々膨大なデータがビッグデータとして蓄積され、活用されている。そのデータの中には、パーソナルデータと呼ばれる、個人のプライバシーを侵害しうるデータも含まれている。2015 年には、個人情報保護法も改正され、データ活用もより一層進むと考えられ、パーソナルデータの取り扱いにも、より一層な取り扱いが求められる。本稿では、匿名化の差分プライバシーの例を用いて、安全にパーソナルデータを活用するための PPDM（プライバシー保護データマイニング）について概説する。

1.　はじめに

ビッグデータや IoT 技術の普及により、さまざまなデータが日々蓄積・活用されている。これらのデータの中には、氏名・年齢などの個人情報や、GPS による位置情報、オンラインショッピングにおける購買データなど、個人に関わるデータが多く含まれている。このような位置情報や購買データなど、個人の行動に関わるデータや、個人の属性に関するデータはパーソナルデータと呼ばれる。パーソナルデータの中には我々のプライバシーを侵害しうるデータも多く含まれ、その取扱いには慎重さが求められる。

2005 年、情報化社会の進展を背景に、個人のプライバシー保護のため、個人情報保護法が制定された。この法律の中では、データ分析を第三者に依頼する場合、データに含まれるすべての人の同意が必要とされていた。このことがデータ分析を困難にする一因となっていたが、2015 年に施行された改正個人情報保護法では、個人を特定できないよう加工されたデータについては、提供項目と提供方法を公表すれば、同意なく第三者へデータを提供することが認められた[1]。データ活用への制限が一部緩和されたが、パーソナルデータの取り扱いに慎重さが求められることは変わらない。プライバシーを保護しつつも、パーソナルデータをうまく活用するためのプライバシー保護技術が求められている。本稿では、データ活用におけるプライバシー保護技術として、プライバシー保護データマイニング（PPDM, Privacy Preserving Data Mining）について説明する。

2.　PPDM とは

PPDM とは、個人のプライバシーを守りながらデータ分析を行うための技術のことをいい、プライバシー保護データマイニングと呼ばれる[2]。2000 年に Agrawal と Srikant によって提唱された[3]。PPDM と情報セキュリティ技術は、プライバシーの保護という目的は同じだが、その方法において区別される。情報セキュリティ技術では、機密性・完全性・可用性を担保することを目的としているが、情報が流出してしまった場合や分析者により閲覧されてしまった場合など、プライバシーが侵害されてしまうことがある[2]。一方 PPDM では、データに対して匿名化や暗号化などの加工を行うことで、プライバシーを侵害しうるデータへのアクセスを難しくする。

PPDM の技術は、「入力プライバシー」と「出力プライバシー」という軸で分類することができる[4]。「入力プライバシー保護技術」では、分析に利用する入力データにおけるプライバシーを、分析者から保護する。分析者からのプライバシーを保護できるため、分析処理を外部に委託できるというメリットがある。代表的な手法として、データが見られても安全なようにデータベース全体を加工する、プライバシー保護データ開示（PPDP, Privacy Preserving Data Publishing）技術が挙げられる。「出力プライバシー保護技術」では、出力される分析結果のプライバシーを保護する。例えば、分析結果として 100 人の平均点が出力された場合、99 人分の点数が判明すると、残る 1 人の点数も明らかになってしまう。ここで出力プライバシーの問題が発生する。出力プライバシーの保護技術では、出力データだけを加工するため、前述の PPDP に比べて情報の劣化が小さくなることが期待できる[4]。代表的な技術として、差分プライバシーという技術が挙げられる。

以下では、入力プライバシー保護技術の例として、k-匿名化と l-多様性、t-近接性を例に、匿名化について説明し、出力プライバシー保護技術として、差分プライバシーを紹介する。

3.　k-匿名化

匿名化技術は、パーソナルデータ中に含まれる名前・住所・年齢など、個人の特定が可能な情報を削除・加工することで、個人の識別を困難にする技術である。パーソナルデータに含まれるデータのうち、氏名や住所など、そのデータだけで個人の識別が可能な情報を直接識別子といい、性別や年齢など、ほかの項目と組み合わせることで個人が特定でき得る情報を準識別子という。また、病歴や宗教など、公表されることが好ましくないデータはセンシティブ属性という。個人のセンシティブ属性が暴露されないことが PPDM の目的の一つである。

匿名化の代表的な技法としては、識別子を削除する方法や、別の値に置き換える仮名化、属性値を階級ごとにまとめるグルーピングなどの技法がある[1]。しかし、これらの技術を用いて匿名化したデータでも、各属性値を組み合わせることで個人の特定が可能な危険性はある。ここで k-匿名化という技術が用いられる。k-匿名化は、同じ準識別子を持つレコードが k 個以上になるようにデータを加工し、k 人未満へのデータの絞り込みを困難にする方法である[5]。手順は以下のとおりである[6]。

① 識別子属性を削除する。
② 準識別子の属性値を一般化する。
③ 準識別子の組み合わせに対して、k 個以上のレコードになるまで②を繰り返す。

ここで一般化と言っている処理は、グルーピングのような処理を指す。図 1 は k-匿名化（k＝3）されたデータの例である。ここで、「職業」、「性別」、「年齢」を準識別子属性、「病名」をセンシティブ属性とする。図 1 では、準識別子の属性値がユニークなレコー

職業	性別	年齢	病名
専門職	男	[35-40)	肝炎
専門職	男	[35-40)	ねんざ
専門職	男	[35-40)	エイズ
芸術家	女	[30-35)	インフルエンザ
芸術家	女	[30-35)	エイズ
芸術家	女	[30-35)	エイズ
芸術家	女	[30-35)	エイズ

図 1　k-匿名化された医療データ（k＝3）[6]

Copyright© 2020　i's FACTORY Co., Ltd. All Rights Reserved.

ドは存在せず、各レコードについて、準識別子が同一のレコードが少なくとも3つ以上存在している。データを絞り込もうとしても、3つ以上の候補までしか絞り込めないことがわかる。図1を見るとわかるように、職業の値がより一般的な名称でラベリングされ、年齢がある程度幅を持つデータに変更されている。これによって準識別子属性からは個人の特定が難しくなっている。一方で、元のデータの情報量が削減されており、有用性が低下する可能性がある。一般に、kを大きくすると匿名性は高まるが、情報量が減り、有用性は低下する。この匿名性と有用性の両立がk-匿名化の課題である。k-匿名化アルゴリズムの1つ、Mondrian[7]は、情報損失量が少ないアルゴリズムとして知られている。

4. l-多様性／t-近接性

k-匿名化されたデータでも、センシティブ属性が漏洩してしまう危険性はある。図1において、病名の列の値がすべてエイズだった場合などである。この場合、レコードごとに個人を識別しなくても、準識別子の属性値との対応から、各人の病名を推定することが可能になる。ここで、l-多様性という概念が導入される。l-多様性は、準識別子の組み合わせが同一のレコードのグループに対して、少なくとも1個以上のセンシティブ属性をもつことを要求する性質である[6]。図2にl-多様性を満たすデータの例を示す。図2の各レコードは、準識別子属性は共通しているが、病名は3種類存在するため、準識別子の情報だけでは、各人の病名を知ることはできない。

さらに、l-多様性を満たしたデータでも、準識別子属性とセンシティブ属性の分布の特性などから、センシティブ属性が推定される危険性がある。例えば、患者の15%が肝炎であるというデータがあったとする。図1を見ると、全体として15%の肝炎患者が、男性に限ると約30%となり、本来の確率より高い確率で肝炎患者を推定できることになる。この問題に対処するため導入されるt-近接性では、l-多様化されたデータに対して、全体と各グループのセンシティブ属性の分散の差がt以下になることを要求する。しかし、t-近接性では準識別子の加工が増えるため、有用性が著しく低下してしまう[6]。

職業	性別	年齢	病名
芸術家	女	[30-35)	エイズ
芸術家	女	[30-35)	はしか
芸術家	女	[30-35)	胃潰瘍

図 2 l-多様性を満たすデータ (l = 3) [6]

5. 差分プライバシー

匿名化においては、データ中のレコードに対して個人の特定を防ぐことで、プライバシーの保護を実現している。一方、分析結果に対して、個人のデータが含まれているという情報自体がプライバシーとなる可能性もある。例えば、性別ごとに検査結果を公開したデータがあったとする。男性で検査結果が陰性となったデータが0件だったとすると、男性という性別がわかっただけで、その人が陽性であったという検査結果が漏洩してしまう。この問題を考慮した指標が差分プライバシーである。差分プライバシーの考え方を説明する[8]。

① 2つのデータベース、D1とD2があるとする。D2では、D1中のAさんのデータが抜かれている。
② D2から得られた情報には、Aさんのデータが含まれないため、Aさんのプライバシーが保護されているといえる。
③ D1のデータにはAさんのデータが含まれるが、D1から得られるデータがD2のデータと見分けがつかなければ、D1についてもAさんのプライバシーは保護されているといえる。D1とD2がどれくらい似ているかの指標として、ϵを用いることとする。
④ D1とD2以外のデータベースとAさん以外の人にとっても①～③が満たされていれば、すべての人にとってプライバシーが保護されているといえる。

この方法は、出力結果に対して、ある分布に従うノイズを付与するなどの方法で実現することができる [9]。差分プライバシーでは、攻撃対象とするレコード以外のすべてのレコードの情報を外部知識に持つ攻撃者からの安全性も保証されており[6]、iphoneのセキュリティ技術としても用いられている[10]。

6. まとめ

本稿では、PPDMについて、匿名化と差分プライバシーを用いて、その技術の概要を説明した。本稿では紹介しなかったが、PPDMの技術として、秘密計算という手法も存在する。秘密計算は、分析対象のデータを暗号化したまま処理をすることで、分析時の情報の暴露を防ぐための手法である[2]。

今後もより一層データの活用は進み、より多くの詳細なパーソナルデータが、蓄積・活用されていくことと思う。個人のプライバシーを守りながら、より安全にデータを蓄積・活用する技術の発展が期待される。

7. 参考文献

[1] 高橋克巳「プライバシー保護データマイニング」システム/制御/情報, Vol. 63, No. 2, pp. 43-50 (2019)
[2] 小栗秀暢「プライバシー保護データ流通のための匿名化手法」システム/制御/情報, Vol. 63, No. 2, pp. 51-57 (2019)
[3] Rakesh Agrawal and Ramakrishnan Srikant, Privacy Preserving Data Mining
[4] 五十嵐大, 高橋克巳「注目のプライバシー Differential Privacy」コンピュータソフトウェア, Vol. 29, No. 4, pp. 40-49 (2012)
[5] 村本俊祐, 上土井陽子, 若林真一「プライバシー保護データ公開に向けたl-多様化適性の評価」データベース, Vol. 4, No. 2, pp. 126-141 (2011)
[6] 南和宏「プライバシー保護データパブリッシング」情報処理, Vol. 54, No. 9, pp. 938-946 (2013)
[7] Kristen LeFevre, David J. DeWitt and Raghu RamakrishnanMondrian Multidimentional K-Anonimity
[8] 寺田雅之「差分プライバシーとは何か」システム/制御/情報, Vol. 63, No. 2, pp. 58-63 (2019)
[9] 寺田雅之, 竹内大二朗, 齊藤克哉, 本郷節之「差分プライバシー基準に基づく情報秘匿手法の一考察」マルチメディア、分散協調とモバイルシンポジウム2014論文集, pp. 224-233 (2014)
[10] Apple, 差分プライバシーに関するホワイトペーパー, https://www.apple.com/jp/privacy/features/

Copyright© 2020 i's FACTORY Co., Ltd. All Rights Reserved.