Vol.2017-EIP-76 No.8
2017/6/1

非パーソナルデータ化の実装についての一検討

荒井　ひろみ[1,a)]　加藤　尚徳[†1,b)]

概要：プライバシー保護はパーソナルデータの利活用において重要な課題である．このプライバシー保護のための一つの手法として，匿名化（Annonymization）が挙げられる．法制度上も，十分な匿名化が達成されれば，最早そのようなデータはパーソナルデータでなくなり，規制の対象外となる．他方で，そのような非パーソナルデータ化が達成されるためには，どの程度の匿名化処理が行われればよいか，非パーソナルデータ化が達成されたことを示すために誰がどのような責任を果たすべきなのかの所在は，は明らかではない．そこで，本稿では，パーソナルデータの保護制度における論点を整理し，技術面における具体的要件や実装について検討する．我々はこれまでにプライバシーに関する規制やガイドラインから各ステークホルダーに求められる要件を整理した．さらに非パーソナルデータ化についてのこれまでの技術的研究を整理し，適用可能性を議論した．

A study on implementation of non-personalization in the use of personal data

Arai Hiromi[1,a)]　Kato Naonori[†1,b)]

1. はじめに

パーソナルデータは個別化した推薦システム，広告，ニュースフィードからエネルギー利用の効率化まで様々な用途で利用されている．このようなシステムにおいてはパーソナルデータが自動処理されることも多く，プライバシー保護の重要性は極めて高い [1].

パーソナルデータについての法制度においてもプライバシー保護は重視されており，通常パーソナルデータは特定やセンシティブ情報の漏洩を脅威とし，それらに対する保護を義務付けられる．一方で非パーソナルデータは自由に流通させることができる．パーソナルデータは適切な匿名化や統計値への変換をへると非パーソナルデータとなるとされている．

本研究では，我々はパーソナルデータの利用における責任と義務に着目する．プライバシー保護に対する要請は国や応用領域によって異なる．パーソナルデータの流通や利用のケースは多様で複雑である．よって，パーソナルデータの利用における責任と義務は場合によっては明確ではない．

我々の貢献は以下のようである．我々は最初にパーソナルデータの利用におけるガイドラインや規則をレビューした．さらにパーソナルデータ利用におけるデータフローを整理し，パーソナルデータの利用における責任と義務を整理した．それらを元にデータ処理に必要な方法を議論し，幾つかの具体的なユースケースにおける適用可能性を議論した．

2. 制度的な背景

2.1 パーソナルデータの保護

パーソナルデータの利活用における制度上のプライバシー保護要件について，技術的な要請や望ましい性質を見出すために，いつかの代表的なガイドラインや規制をレビューする．まず，プライバシー保護要件のうち一般的なものについて概観し，その上で非パーソナルデータ化について検討す

[1] 情報通信研究機構
National Institute of Information and Communications Technology
[†1] 現在，KDDI 総合研究所
Presently with KDDI Research
[a)] hiromi.arai@nict.go.jp
[b)] xan-katou.kddi.com

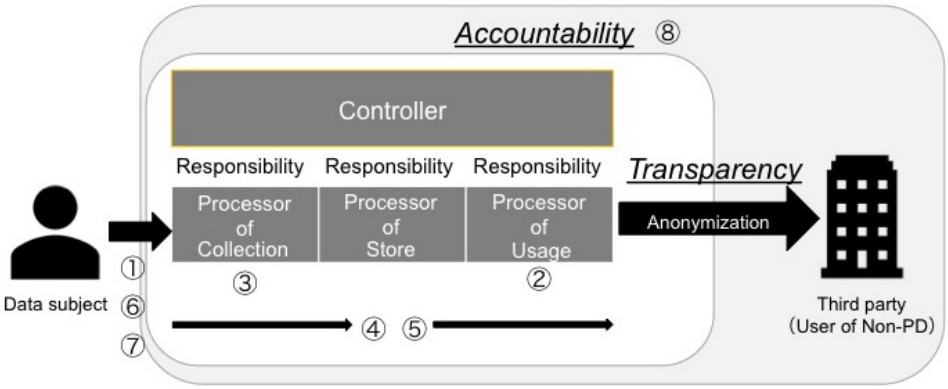

図 1 主体とそれに対応するパーソナルデータの利用を示す．水平なフローはデータ所有者から第三者へのデータ移転を示す．コントローラーによるデータフローは収集 (collect)，保管 (store)，利用 (usage) に分類できる．番号は対応する OECD 8原則に対応する．.

る．本稿においては，我々は OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data（OECD プライバシーガイドライン）[2]，および the 38th International Conference of Data Protection and Privacy Commissioners (ICDPPC2016) における議論を参照した．なお，各国においては，パーソナルデータ・プライバシー保護に関する様々な試みがなされているが，本稿においては，技術の普遍性を鑑みて，国際的な議論に着目した整理を行う．

OECD プライバシーガイドラインは 1980 年 9 月 23 日に採択され，2013 年 7 月 11 日に改正，2013 年 9 月 9 日に公開された．1980 年前後は，1974 年に米国でプライバシー法が制定されるなど，各国がプライバシーに関する法制度を整備しようとしていた時期であった．国際的にプライバシー保護に関する法制化の機運が高まる中で，OECD プライバシーガイドラインは，加盟国間の情報の自由な流通を促進するとこと及び加盟国間の経済的社会的社会的関係の発展に対する不当な障害の創設を回避することを目的として採択された．つまり，OECD プライバシーガイドラインは，国際的なプライバシーに関するルール形成が進められるにあたって，その指針を示したものであるといえる．OECD プライバシーガイドラインにおいては，以下の８つの原則が掲げられている．

① Collection Limitation Principle
② Data Quality Principle
③ Purpose Specification Principle
④ Use Limitation Principle
⑤ Security Safeguards Principle
⑥ Openness Principle
⑦ Individual Participation Principle
⑧ Accountability Principle

これらの８つの原則が，各国の法制化にあたっては尊重されており，例えば我が国の個人情報保護法との関係性においても，８つの原則と条文との対応関係が明らかにされている．

一方で，従来のこのような取り組みに加えて，新たなプライバシー保護の潮流が表れてきた．ICDPPC はプライバシー・パーソナルデータを中心としたデータ保護に関して，世界各国の Data Protection Authority（DPA）が一堂に会して，年に一度行われる国際会議であり，我が国からは個人情報保護法を所管する個人情報保護委員会が DPA として参加している．ICDPPC においては，その時々のデータ保護に関する主要なテーマが議論される．議論の結果は，各国に対して具体的な拘束力を有しないものの，データ保護に関する国際的な方向性に大きな影響を与えている．昨年，2016 年にモロッコで開催された ICDPPC2016 においては，transparency がキーイシューとして議論がなされた．特に，AI 等の処理の過程でパーソナルデータが利用されていく中で，どのように transparency を確保していくかという問題提起がなされたことが注目に値する．この transparency という視点は，従来の OECD プライバシーガイドラインをはじめとした国際的な議論の中では，具体的な法制化が議論されてこなかった論点である．しかしながら，AI の利用に国際的な注目が集まる中で，ICDPPC において transparency に関する問題提起がなされたことは，今後，transparency が主要な論点となりうることを意味している．

2.2 非パーソナルデータ化の取扱いと追加的要件

先述の OECD プライバシーガイドラインをはじめ，多くのデータ保護法制が，パーソナルデータを保護の対象としている．これはつまり，パーソナルデータでないもの，つまり非パーソナルデータは保護の対象にないということを意味する．例えば，我が国の個人情報保護法の比較法の対象として頻繁に参照される EU の General Data Protection Regulation(GDPR) [3] では，自然人を識別または識別する

可能性を持たないような anonymous data（匿名データ）は GDPR の対象外であることが明記されている（前文 26）．加えて，統計目的での利用についても除外されることが明記されている．

一方で，匿名データについては，どのような匿名化処理を行えばパーソナルデータでなくなるのかが大きな議論になっている．我が国の個人情報保護法の改正においては，匿名加工情報が新たに定義に加わった．これはパーソナルデータに関する検討会の技術検討ワーキンググループ報告書（2013 年 12 月 10 日）において，「いかなる個人情報に対しても，識別非特定情報や非識別非特定情報となるように加工できる汎用的な方法は存在しない.」という報告がなされてことに基いている．つまり，非個人情報化するための一般的な匿名化のための基準を定めることは困難であるため，匿名加工情報として一定の技術的な基準を定めつつも，合わせて匿名加工情報を取扱う者に一定の法律上の義務を課すことによって，本人の同意を要しない個人情報の第三者提供を実現するような試みであるといえる．では，我が国において，GDPR のような匿名化による非個人情報化（非パーソナルデータ化）が禁止されているのかといえばそうではない．同報告書においても，「ケースバイケースの対応」によって，「識別非特定情報や非識別非特定情報に加工すること」は不可能ではないと言及されている．つまり，本稿にいう非パーソナルデータ化の可能性を否定するものではないし，匿名加工情報がそのような非パーソナルデータ化されたデータを指すものでもない．

では，仮に，非パーソナルデータ化が可能であるとして，そのような処理に対する制度上の制約はないのか．もちろん，非パーソナルデータ化が偽りであったするならば，データ保護法制の適用対象なり，規制を受けることになる．しかしながら，非パーソナルデータやそこに至る処理については，現行のいずれの制度の対象ともならない．そのような中で我々は，前項でふれたパーソナルデータの保護の趣旨を鑑みつつ，適用が望ましい原則について検討した．図 1 は，OECD プライバシーガイドラインの 8 つの原則及び transparency について，一般的なデータの利活用サイクルと照らし合わせたものである．その結果，8 つの原則のうちの 7 つについては，anonymization（匿名化）処理以前に考慮されるべきものであると整理をした．一方で，anonymization にかかるものとしては，責任の原則（accountability）および，transparency が考えられると整理した．

なお，非パーソナルデータ化については，制度的考察の上でいくつかの段階があると整理した点についても付記する．非パーソナルデータ化にあたっては，パーソナルデータとの二元的な捉え方がなされることが多いが，実際には，我が国の匿名加工情報における議論に見えるように，いくつかの段階がある．つまり，匿名加工情報は非パーソナルデータとしての法的取扱いを受ける一方で，法的な義務が課されるため，GDPR における匿名化が達成されたとは言えない．他方で，匿名化に対して，パーソナルデータに基づく統計処理の結果については，その統計学の分野における適正性の判断とともに，伝統的に非パーソナルデータとしての扱いがなされてきた．この結果，パーソナルデータに近い順に，匿名加工情報，匿名データ，統計処理の結果というような順序付けを行えると整理できた．ただし，このような検討は本稿の射程外となるため，別な機会に考察を進めることとする．

3. パーソナルデータの保護のための技術の検討

本章では，我々はパーソナルデータの利用に際し非パーソナライズデータ化するための技術を検討する．本研究では我々は安全性のシステムのセキュリティの設計及び運用は完璧であると想定し，セキュリティリスク以外の要因からのパーソナルデータの保護を検討する．よって，データの収集と保持に問題はないと想定し利用におけるデータ処理にフォーカスする．まず非パーソナライズデータ化に適用可能と考えられる既存のプライバシー保護技術を概観し，さらにその transparency と accountability を確保するための方法を議論する．

パーソナルデータを非パーソナルデータに変換するアプローチとして，前章での議論を受けて，今回は以下の 2 つを取り扱う．一つは匿名化である．ここで匿名化とは，個人レベルのパーソナルデータを加工することとする．もう一つは抽象化である，これは個々人のパーソナルデータを陽に含まない集団レベルでのパーソナルデータの性質の記述とする．これは，ある集団についての統計情報や統計モデル，集団内のパーソナルデータ群から学習されたモデルなどを考える．また情報推薦や検索などの，学習モデルにパーソナルデータを入力し，それを用いて得られる出力である予測結果なども考慮する．どちらのアプローチもデータの有用性を残しつつ，個人の特定やセンシティブ情報の推測などのプライバシ侵害ができないようにデータを加工する．なお，匿名加工情報についての議論は本稿においては割愛する．適切な非パーソナライズ化は非パーソナルデータ化に対する責任の観点からも必要とされる．適切な非パーソナライズ化の要件は，前章で見たように，プライバシー保護のための十分な非パーソナルデータ化，パーソナライズ化のプロセスにおける transparency，accountability の 3 つである．

Transparency と accountability をどのように実装するかというのは制度面からは具体的な規制がないが，本稿では以下のように考える．Transparency はプライバシー保護の手続きや適切性を分かりやすく説明すること，accountability はプライバシー保護が適切に行われていることに責任をも

ち説明できることである．よって，まずプライバシー保護手法をプライバシ保護の強度に着目し，それを説明するための方法を議論する．その後，手続きの説明について議論を行う．

プライバシー保護のための匿名化について概説する．まずプライバシー保護の適切性について考える．匿名化には，まず明示的な識別子のみを削除する単純匿名化が存在する．しかし，このような匿名化は，個人を絞り込むことができる共通の項目 (準識別子) を持ちかつ識別子を持つデータベースとの突き合わせによって個人の再特定が可能になる可能性がある．このような再特定攻撃のうち，テーブルデータに対するものを record linking として定義し，再特定ができないように準識別子を加工する k 匿名化 [4] が提案されている．テーブルデータ以外にも，例えばグラフにおいても再特定攻撃が可能であることが指摘されている [5]．それに対する k 匿名化 [6] など様々なデータ形式についての匿名化手法が提案されている．k 匿名化は同じ準識別子の組が k 個以上になるように準識別子に抽象化や削除などの加工を施す．準識別子の定義として何が適切かは，攻撃者の持つ知識や計算能力の設定の適切性が求められる．例えば攻撃者が補助情報として用いる社会に流通している識別子付きの情報などの想定である．しかし HIPPA における削除する識別子の定義 [7] で多くの議論がなされたように，適切性の判断は容易ではない．さらに，個人に対応するセンシティブ情報の確定に対するプライバシー保護についてはパーソナルデータをさらに加工して準識別子のある組に対するセンシティブ情報に多様性を持たせる ℓ 多様性 [8] などの方式が提案されている．これらの匿名化は強度を上げるほどデータの情報量が落ちてしまうため，プライバシー保護の強度と有用性のトレードオフが生じる．

抽象化によるプライバシー保護については，本稿で扱う抽象化データにパーソナルデータは陽に含まれないため，抽象化したデータからパーソナルデータが部分的にでも推測できるかどうか，という属性推定がプライバシリスクとなる．このようなプライバシリスクは，実際に攻撃者が個人に関する補助情報を持っている場合に可能であることが指摘されている．コホート研究における統計値及び個人のゲノム情報の一部から疾患の推定 [9]，ワーファリン投与量算出のための学習モデルと学習データの一部から学習データに含まれるゲノム情報の推定 [10] などである．これらのプライバシリスクは問題および攻撃者の設定次第であり，匿名化の準識別子と同様にリスク算定基準の適切性は議論の余地がある．またこれらのプライバシリスクの低減措置としては，クエリ監査 [11] などによる事前検査や十分大きい母集団を取るなどが考えられる．また差分プライバシ [12] などのノイズ加算方式もあるが，いずれも出版できる情報の制限やノイズなどによる有用性の低下があり，やはりプライバシー保護の強度と有用性のトレードオフが生じる．

さらに，非パーソナルデータ化したデータに含まれる属性の持つ相関関係は，非パーソナルデータに含まれないセンシティブ情報との紐付けによる新たなリスクが生じる危険性がある．例えば匿名化したゲノム情報は，ゲノムと相関する表現型の情報によって再特定されるリスクがある [13]．また，個人のゲノム検査結果から元の個人ゲノム情報，さらにそれと関連する疾患の情報が推測されるリスクがある [14]．このようなリスクは現在非パーソナルデータ化におけるリスクとして遡上に登ることは少ないが，考慮することでプライバシリスクを下げることができる．

以上より，非パーソナルデータ化におけるプライバシデータ保護技術は一般的に有用性と強度のトレードオフがあり，また強度の評価における前提は一意に決まるものではないと言える．このような中で適切性を評価するためには，攻撃者や手法の妥当性の評価が必要である．手法の妥当性の評価には，筆者はある手法を適用した際のリスク評価が重要であると考える．集団におけるプライバシリスクの分布やリスクの評価はエントロピーや最大リスク，リスクの分布など様々な評価軸があり，複数の評価軸をもちいて様々な側面を評価することが重要であるという指摘がなされている [15]．

非パーソナルデータの作成についての transparency の説明面についてはまだあまり議論が多くないが，データ処理方法の提供が一つ挙げられる．匿名化については，乱数以外の全てのプロセスを提供すること [16] という提案がなされる一方，ソースコード直接は解釈性やセキュリティの面から適切ではなく，ある程度抽象化したものがよいという提案もある [17]．特に近年の複雑な機械学習アルゴリズムなどは手続きが複雑であり，透明性をどのように確保するかは難しい課題である．また機械学習モデルにを用いる場合のプロセスの解釈性について，近年ディープラーニングなどの複雑なモデルについて，入力が出力に貢献した度合いを定量的に示す [18] といった提案がなされている．さらに，入力と出力の関係には，データ依存の部分とアルゴリズム等のデータ処理手法に依存する部分がある．出力に対する責任を寄り明確にするための方法として，例えば検索における政治的なバイアスにおいて，入力とアルゴリズムそれぞれの貢献度合いを示す [19]，等の研究が応用できると考察される．Accountability については，まず非パーソナルデータ化が正しく行われていることについての説明責任があると考えられる．そのために上述のプライバシリスク評価についての標準化や，アルゴリズムを transparent に説明することが考えられる．

参考文献

[1] O'Leary, D. E., Bonorris, S., Klosgen, W., Khaw, Y.-T., Lee, H.-Y. and Ziarko, W.: Some privacy issues in knowl-

edge discovery: the OECD personal privacy guidelines, *IEEE Expert*, Vol. 10, No. 2, pp. 48–59 (1995).

[2] Organization for Economoic Co-operation and Development: OECD guidelines on the protection of privacy and transborder ows of personal data.

[3] European Commission: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016.

[4] Sweeney, L.: k-anonymity: A model for protecting privacy, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 05, pp. 557–570 (2002).

[5] Narayanan, A. and Shmatikov, V.: De-anonymizing social networks, *Security and Privacy, 2009 30th IEEE Symposium on*, pp. 173–187 (2009).

[6] Liu, K. and Terzi, E.: Towards identity anonymization on graphs, *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pp. 93–106 (2008).

[7] Centers for Disease Control and Prevention and others: HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services.

[8] Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M.: l-diversity: Privacy beyond k-anonymity, *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Vol. 1, No. 1, p. 3 (2007).

[9] Homer, N., Szelinger, S., Redman, M., Duggan, D., Tembe, W., Muehling, J., Pearson, J. V., Stephan, D. A., Nelson, S. F. and Craig, D. W.: Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays, *PLoS genetics*, Vol. 4, No. 8, p. e1000167 (2008).

[10] Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D. and Ristenpart, T.: Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing, *Proceedings of the 23rd USENIX conference on Security Symposium*, pp. 17–32 (2014).

[11] Nabar, S., Kenthapadi, K., Mishra, N. and Motwani, R.: A survey of query auditing techniques for data privacy, *Privacy-Preserving Data Mining*, pp. 415–431 (2008).

[12] Dwork, C., McSherry, F., Nissim, K. and Smith, A.: Calibrating noise to sensitivity in private data analysis, *Theory of Cryptography*, pp. 265–284 (2006).

[13] Humbert, M., Huguenin, K., Hugonot, J., Ayday, E. and Hubaux, J.-P.: De-anonymizing genomic databases using phenotypic traits, *Proceedings on Privacy Enhancing Technologies*, Vol. 2015, No. 2, pp. 99–114 (2015).

[14] Hiromi, A., Jun, S. and Koji, T.: Quantifying Genomic Privacy in Genetic Test Results, *3rd International Workshop on Genome Privacy and Security (GenoPri" 16)* (2016).

[15] Wagner, I.: Genomic privacy metrics: a systematic comparison, *Security and Privacy Workshops (SPW), 2015 IEEE*, pp. 50–59 (2015).

[16] Domingo-Ferrer, J. and Muralidhar, K.: New directions in anonymization: permutation paradigm, verifiability by subjects and intruders, transparency to users, *arXiv preprint arXiv:1501.04186* (2015).

[17] Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G. and Yu, H.: Accountable algorithms (2016).

[18] Datta, A., Sen, S. and Zick, Y.: Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems, *Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 598–617 (2016).

[19] Kulshrestha, J., Eslami, M., Messias, J., Zafar, M. B., Ghosh, S., Gummadi, K. P. and Karahalios, K.: Quantifying search bias: Investigating sources of bias for political searches in social media, *arXiv preprint arXiv:1704.01347* (2017).