差分プライバシに基づく 一括開示と対話開示のデータ有用性の評価 ―多属性に関する考察―

山口 高康[1,2,a)]　寺田 雅之[2,b)]　吉浦 裕[1,c)]

概要：パーソナルデータの活用に向けて数多くのプライバシ保護技術が提案されている．当該データの安全性を保証した上で，その価値を最大限に引き出したいが，どのような場面でどのような加工技術を選択すれば良いか明らかではない．筆者らは，同等の安全性におけるプライバシ保護後のデータの有用性を評価し，7 月の CSEC 研究会で報告した．しかし，この評価はデータセットのユーザ属性の一部での評価であったため，本稿では全てのユーザ属性を用いた評価結果について述べる．

キーワード：プライバシ保護，差分プライバシ，*Pk*-匿名化，ラプラスメカニズム

On Utility Comparison of Differential-private Information Disclosure in Non-interactive and Interactive Settings

Takayasu Yamaguchi[1,2,a)]　Masayuki Terada[2,b)]　Hiroshi Yoshiura[1,c)]

Abstract: There has been a great attention about utilizing the personal data, and many techniques dealing with it have been proposed. The problem seems to lie in the fact that you don't know which approach should apply in the real cases. It is important that how you choose the appropriate means to bring the useful analysis along with the reliable personal data security is discussed. We evaluate the usefulness of the popular bulk and dialogue methods on the same security, Differential Privacy. The present study was undertaken in order to provide you with the steady privacy preservation and worthwhile insights and encourage people to participate in it.

Keywords: privacy preserving, differential privacy, *Pk*-anonymization, laplace mechanism

1. はじめに

近年，個人に関わる情報 (以下，パーソナルデータと呼ぶ) を保護しながら有効活用することへの期待が高まっている．しかし，パーソナルデータの利用については，プライバシへの配慮が求められる．そのため，置換や摂動などのプライバシ保護技術が重要視されている．当該技術の有効性は，プライバシ保護後の情報の安全性と有用性とのトレードオフによって決まる．安全性については，差分プライバシ [1] が注目を集めている．差分プライバシは様々なプライバシ保護技術の安全性を統一的に評価可能な指標である．また，数学的な裏付けがあり，プライバシの安全性を定量的に議論することができる．

プライバシ保護技術は，1) パーソナルデータを含むデータ一式を加工して利用者に渡す方式 [2][3][4](以下，一括開示と呼ぶ) と，2) パーソナルデータを含むデータに対して

[1] 電気通信大学大学院情報理工学研究科
Graduate School of Informatics and Engineering, The University of Electro-communications
[2] 株式会社 NTT ドコモ先進技術研究所
Research Laboratories, NTT DOCOMO, Inc., Yokosuka, Kanagawa 239-8536, Japan
[a)] yamaguchitaka@uec.ac.jp
[b)] teradam@nttdocomo.com
[c)] yoshiura@uec.ac.jp

利用者が検索した結果を加工して渡す方式 (以下，対話開示と呼ぶ)[1][5] に大別できる．両者の技術には長所・短所，あるいは適した応用があると考えられる．しかし，筆者が知る限り安全性と有用性のトレードオフの観点から両者の実証的な比較を行った研究はなく，実用の場面でどのように判断してどちらの方式を選択すれば良いか，従来明らかではなかった．また，対話開示の場合，利用者の検索が複数回に及ぶ場合には，安全性が低下すると考えられる．

そこで筆者らは，同等の安全性におけるプライバシ保護後のデータの有用性を評価し，7 月の CSEC 研究会で報告した [6]．しかし，この評価はデータセットのユーザ属性の一部での評価であったため，本稿では全てのユーザ属性を用いた評価結果について述べる．

本研究では，安全性と有用性のトレードオフにおいて，一括開示と対話開示を実証的に比較する．その一環として，対話開示を複数回実施する場合も定量的に評価する．

一括開示のプライバシ保護技術の例として，k-匿名性を満たす k-匿名化 [2] と，k-匿名性を確率的に満たす k-匿名化 (Pk-匿名化)[7] を取り上げる．対話開示のプライバシ保護技術の例として，差分プライバシの実現方式として注目されているラプラスメカニズム [1] を取り上げる．差分プライバシの観点から安全性が等しくなるように，両手法を用いてパーソナルデータを加工し，その有用性を実証的に比較する．差分プライバシの安全性を揃えるために五十嵐らの研究成果 [4] を用いる．評価用データとして MovieLens データセット [8] を用いる．有用性の評価手法としては，両手法により加工した集計表を，オリジナルの MovieLens データから作成した集計表と比較し，両手法による集計表の歪み度合いを，L2 距離および順位相関により定量化する．

2. 先行研究

2.1 概要

企業などの組織がパーソナルデータを収集する場合には，個人に利用目的を明示することが個人情報保護法により義務付けられている．パーソナルデータを目的外利用したり第 3 者に提供する場合は，十分な匿名加工処理を施してパーソナルデータに含まれるプライバシを保護する必要がある．以下では，パーソナルデータを収集・管理している組織をデータ管理者，目的外利用を行う者および第 3 者をデータ利用者と呼ぶことにする (**図 1**)．プライバシ保護の点線の左右はプライバシ保護の加工処理前後を表す．パーソナルデータはテーブルの形式で表現できる場合が多いので，本論文では収集した個人情報の集合をテーブル，テーブル内の個々の個人情報をレコードと呼ぶことにする．

プライバシ保護技術は 2 つの軸により分類することができる．1 つ目の軸は，パーソナルデータを含むデータ一式を加工してデータ利用者に渡すか，パーソナルデータを含むデータに対して検索した結果を加工して渡すかであり，前者を一括開示，後者を対話開示と呼ぶことにする．2 つ目の軸は具体的な加工手法に関する分類である．

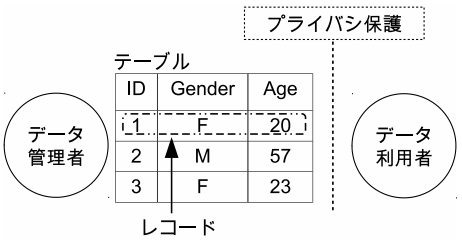


図 1 データ管理者とデータ利用者の関係
Fig. 1 Relationship between data administrator and analyst.

具体的な加工手法としては，複数のレコード間の識別性を低下させる手法，データの属性値を確率的に置換する手法，ノイズ重畳などによりデータの数値を摂動する手法が代表的である．識別性低下手法の代表例としては，k-匿名化が有名である [2]．k-匿名性は，レコードと個人との対応の防止に関する指標であり，レコードに対応する個人を k 人未満に絞り込めないことを意味する．k-匿名化では，準識別属性の値が k レコードに渡って等しくなるように加工することで，k-匿名性を満たす．k-匿名化は一括開示で利用される．k-匿名性から派生した指標として，l-多様性 [9]，t-近接性 [10] などが提案されており，それらを満たす加工手法が検討されている．

置換手法には，レコード間をランダムに置換する初期の手法 [11]，k-匿名性を確率的に拡張した Pk-匿名化 [7][12] などがある．Pk-匿名化は，「個人を k 人未満に絞り込めない」という k-匿名性を，「個人を $1/k$ 以上の確率で特定できない」と確率的に解釈し，属性値の交換によって確率的な k-匿名性を実現している．一括開示での利用が提案されている．置換によって歪められたデータから統計値を算出する際に，ベイズ推定等を用いることで，オリジナルデータから算出した統計値に近い値を得る手法 (再構築法と呼ばれる) も検討されている [13][14][15].

摂動手法には，ラプラスノイズを重畳することにより差分プライバシを実現するラプラスメカニズム [1] が代表例として挙げられる．詳細については後述する．

プライバシ保護技術の開発，評価，利用にあたっては，プライバシの度合いを表す指標が重要である．このプライバシ指標として，上述した k-匿名性，l-多様性，t-近接性などが知られているが，近年，注目されているのが差分プライバシである．差分プライバシは，「ある個人がいてもいなくても出力に差分が殆どない」[1][16] という概念を定式化したものであり，式 (1) により表現される．

$$Pr[\mathcal{K}(D_1) \in S] \leq \exp(\epsilon) \times Pr[\mathcal{K}(D_2) \in S]. \qquad (1)$$

この式の詳細な解説は [1] および [16] を参照していただきたいが，ϵ はある個人がデータベースに含まれている場合と

含まれていない場合の出力の差を表しており，差分プライバシにおけるプライバシ度合いを表すパラメータになっている．差分プライバシは，当初はラプラスメカニズムを用いた対話開示型の加工技術として実現法が示されたが，より広範囲の加工技術の指標として利用できる．たとえば，Pk-匿名化を用いた一括開示も ϵ によってプライバシ度合を評価することができる [4]．また，Pk-匿名化と k-匿名化の関係に関する研究成果 [7][4] により，差分プライバシと k-匿名性の関係も間接的に評価することができる．

2.2 関連研究

本論文では，一括開示の代表例として Pk-匿名化，対話開示の代表例としてラプラスメカニズムを取り上げる．差分プライバシに基づく比較のために，差分プライバシを Pk-匿名化に適用した研究成果，および Pk-匿名化と k-匿名化の関係に関する研究成果を用いる．

2.2.1 *Pk*-匿名化と再構築

Pk-匿名化の具体例として，五十嵐らの Pk-匿名化 [7] を説明する．Pk-匿名化では，一括開示の際にレコードの値を確率的に置換してテーブルを撹乱する．任意のレコードの w 番目の属性値を r_w から r'_w に置換する確率を $a(r'_w|r_w)$ で表す (式 (2))．式 (2) において，w 番目の属性の値の種類数が V_w，w 番目の属性の置換パラメータが ρ_w である．ρ_w の値が小さいほど置換されやすい．

$$a(r'_w|r_w) = \begin{cases} \rho_w + \frac{1-\rho_w}{V_w} (r_w = r'_w) \\ \frac{1-\rho_w}{V_w} (r_w \neq r'_w) \end{cases} . \tag{2}$$

$a(r'_w|r_w)$ を属性毎の置換確率を格納するマトリクス A_w に格納する．w 番目の属性は置換によって V_w 種類だけ変化する可能性があるので，A_w のサイズは $V_w \times V_w$ である．個々の属性の A_w のクロネッカ積を全ての属性の維持置換確率を格納するマトリクス A とする．属性の数を W とすると，全ての属性の値の組み合わせは $V = \prod_{1 \leq w \leq W} V_w$ であり，A のサイズは $V \times V$ である．属性を増やすと A のサイズが大きくなり，メモリが逼迫しやすくなるため，文献 [17] の工夫を施す．

置換によって歪められたデータから統計値を算出する際に，式 (3) の再構築によって，元のデータの統計値に近い値を得る．

$$\boldsymbol{z}^{t+1} = \boldsymbol{z}^t \left(A \left(\frac{\boldsymbol{y}}{\boldsymbol{z}^t A} \right)^T \right)^T . \tag{3}$$

$\boldsymbol{y}$ は再構築前の統計値を表すベクトル，$\boldsymbol{z}$ は再構築後の統計値を表すベクトル，t は反復ベイズ法の反復回数である．$\boldsymbol{z}^t$ と $\boldsymbol{z}^{t+1}$ の差が小さくなったことをもって計算が収束したとみなす．

2.2.2 ラプラスメカニズムと差分プライバシ

ラプラスメカニズム [16] では，検索応答の際にラプラス分布に従う摂動を加える (式 (4))．

$$p(z) = \frac{1}{2\lambda} \exp\left(-\frac{|z-x|}{\lambda} \right) . \tag{4}$$

x はデータに対するオリジナルの検索結果，$p(z)$ はラプラスノイズによって摂動を加えた検索結果がとる確率分布，λ がノイズの大きさを表す．

式 (5) を満足するように λ を設定すると差分プライバシを満たすことができる．

$$\lambda \geq \frac{\Delta f}{\epsilon} . \tag{5}$$

Δf はセンシティビティであり，テーブルの任意の 1 レコードの値を置換した場合に検索応答に生じる最大の変化量である．

2.2.3 差分プライバシの適用範囲の拡大

Pk-匿名化では，式 (6) を満足するように ρ_w を設定すると，ϵ によるラプラスメカニズムと同等の差分プライバシを満たせる [4]．具体的に ϵ から ρ_w を求める際は，ρ_w を全て等しいと仮定して設定することも考えられるが，それぞれの属性 w に応じて個別に ρ_w を設定する方が (同じ安全性でも) 有用性を高められると考えられるので，式 (6) を変形した文献 [18] の式を用いる．

$$\epsilon = \sum_{1 \leq w \leq W} \ln \frac{1 + (V_w - 1)\rho_w}{1 - \rho_w} . \tag{6}$$

文献 [4] には ρ_w と k の関係も示されている (式 (7))．

$$k = 1 + (N-1) \left(\prod_{1 \leq w \leq W} \left(\frac{1-\rho_w}{1 + (V_w - 1)\rho_w} \right)^2 \right) . \tag{7}$$

N はレコード数である．ρ_w を小さくすると置換されやすくなるので，k は大きくなって Pk-匿名性が向上する．全てのレコードに対してこの確率的な置換を施すので，N が大きいほど匿名性を向上させやすい．

2.2.4 同等の安全性での一括開示と対話開示の有用性

Adam らは一括開示と対話開示の安全性について議論したが，当時は差分プライバシがなく，定性的な比較であった [19]．後に Ghosh らは差分プライバシで安全性を担保しつつ，有用性を最大化する手法を示した [20]．しかし，Brenner らはその手法を一般に適用することは困難であることを示した [21]．差分プライバシに基づく一括開示の有用性評価 [22][23]，および対話開示の有用性評価 [24][25] はそれぞれ行われているが，同等の安全性での一括開示と対話開示の有用性は明らかではない．

3. 安全性と有用性の評価方針

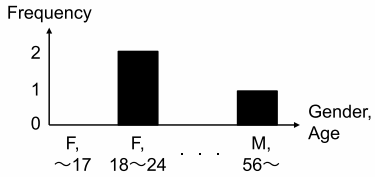
3.1 パーソナルデータの利用形態

プライバシ保護されたパーソナルデータのテーブルでは，一般に，個人毎の情報であるレコードは元情報が推定できないほど加工されている．しかし，テーブルから得られる統計情報は，元の統計情報から大きく外れないことが期待

される．すなわち，プライバシ保護されたパーソナルデータは，一般に統計情報として利用される．統計情報の代表的な表現形態として，度数の分布が挙げられる．度数の分布は属性毎の該当数であり，例えば，Gender が Female と Male の 2 種類 (それぞれ F,M と表記する．$V_1 = 2$)，Age が Movie Lens 1M データセットの年代と同じ，17 歳以下, 18 歳〜24 歳, 25 歳〜34 歳, 35 歳〜44 歳, 45 歳〜49 歳, 50 歳〜55 歳, 56 歳以上の 7 種類 ($V_2 = 7$) とすると，図 1 のテーブルは F18 歳未満に 0 人，F18 歳-24 歳に 2 人，...，M56 歳以上に 1 人該当し，14 種類 ($V = 14$) の度数の分布を持つ集計表で表せる (**図 2**)．以下，グラフで簡潔に表示する．

Gender	Age	Freqency
F	～17	0
	18～24	2
	25～34	0
	35～44	0
	45～49	0
	50～55	0
	56～	0
M	～17	0
	18～24	0
	25～34	0
	35～44	0
	45～49	0
	50～55	0
	56～	1

(a)集計表



(b)グラフ表示

図 2 集計表とそのグラフ表示

Fig. 2 Table and graph to represent frequency of each gender and age.

度数の分布はそれ自体が有用な統計量を示すだけでなく，度数の分布から平均，分散，尖度，歪度などの他の主要な統計量を算出できる [26]．本稿では，データ利用者はパーソナルデータを集計表の形で利用することを前提とする．

3.2 有用性の評価方法

集計表の典型的なユースケースとして，量的な予測と順位の予測がある．前者の応用については，公共では交通量や患者数，申請者数の予測などが，マーケティングでは売上数や売上額，利益額の予測などが考えられる．後者の応用については，公共では政策の順位付け，重点化などが，マーケティングではターゲティング型の広告，研究開発活動の選択と集中などが考えられる．量的な予測の応用においては，量的な正確さが重要であるため，オリジナルの集計表と加工した集計表の距離 (L2 距離) で評価する．順位の予測の応用においては，順位の正確さが重要であるため，オリジナルの集計表と加工した集計表の順位相関 (スピアマンの順位相関係数) で評価する (**表 1**)．

表 1 ユースケースと要求と評価尺度

Table 1 Use cases, requirements and measures of evaluation.

ユースケース	要求	評価尺度
量的な予測	集計表の個々のセルの値の誤差が小さいこと	L2 距離 (小さな値が良い)
順位の予測	集計表のセルの値の順位が維持されること	順位相関 (大きな値が良い)

3.3 安全性の設定方法

ϵ と λ の関係は式 (5) で与えられる．個々のユーザがテーブルにいるかいないかを秘匿する場合は，テーブルから任意のユーザを削除しても集計値は 1 人しか変わらないので，$\Delta f = 1$ で良い．だが，個々のユーザの性別や年代の属性値を秘匿する場合は，任意のユーザの属性値を置換すると 2 箇所で変化が起こる．本稿では，属性値を秘匿することとし，最大の変化量である $\Delta f = 2$ を式 (5) で用いる．なお，式 (5) は等号付き不等号であるが，有用性を高めるためにノイズは小さい方が好ましいので等号で λ を求める．

ϵ の値は，先行研究で $\epsilon = 0.1 \sim 10$ 程度が用いられている [23][24][25]．4 章の実験では，これらの値をカバーするように，$\epsilon = 0.1, 1.0, 4.0$ を用いる．なお，ϵ に応じた ρ_w は，文献 [18] の式を用いて属性毎に設定する．

3.4 トレードオフの評価方法

3.3 節の方法で安全性を揃えて，3.2 節の方法で有用性を評価して比較する．評価実験のイメージを**図 3** に示す．一括開示では，データ管理者はテーブルを k-匿名化 (識別

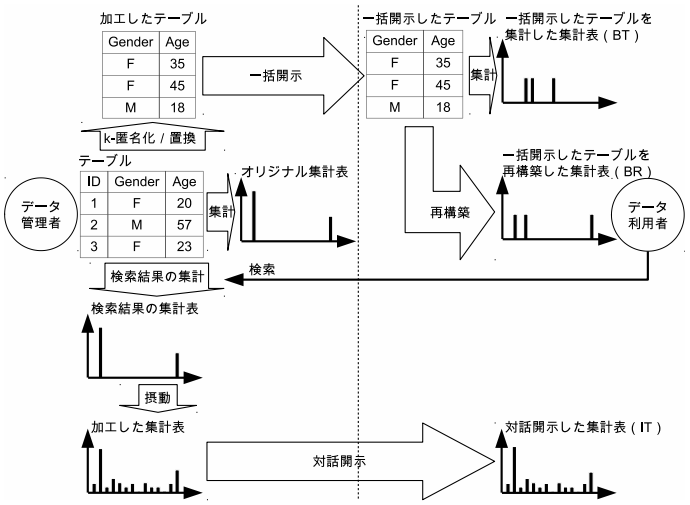


図 3 各プライバシ保護方式の処理フロー

Fig. 3 Data flows of each privacy preserving method.

性低下) または Pk-匿名化 (置換) によってプライバシ保護し，加工後のテーブル全体を開示する．データ利用者はこのテーブルを集計した集計表，あるいは Pk-匿名化については，このテーブルを再構築した集計表を利用する．対話開示では，データ利用者がデータを検索する．データ管理

者はテーブルから検索結果の集計表を算出し，この集計表をラプラスメカニズム (摂動) によってプライバシ保護して，データ利用者に開示する．一括開示の識別性低下と置換，および対話開示の摂動の安全性を，同じ ϵ で揃える．

上記の 4 つの集計表のうち，一括開示から直接集計したものを BT(Batch disclosure)，そのうち k-匿名化によるものを BTk(Batch disclosure with k-anonymization)，一括開示から再構築したものを BR(Batch disclosure and Reconstruction)，対話開示したものを IT(Interactive disclosure) と表すことにする．

有用性の評価では，BTk，BT，BR，IT について，プライバシ保護する前のオリジナル集計表との L2 距離および順位相関を求めて比較する．

対話開示の安全性は検索回数に応じて低下する．具体的には，1 回の開示における安全性が ϵ の場合，X 回の開示における安全性の最悪値は Xϵ となる [1]．そのため，複数検索における安全性を一括開示と揃えるためには，1 回の開示における安全パラメータを $\frac{\epsilon}{X}$ にする必要がある．その結果，X が大きくなるほど強いノイズを付加することになり，有用性が低下する．本論文では，X を変えて有用性を評価する (**表 2**)．

表 2 処理内容と加工方式の表記
Table 2 Denominating processes of anonymization.

開示種別	処理内容	加工方式の表記
一括開示	k-匿名化と集計	BTk
	置換と集計	BT
	置換と再構築	BR
対話開示	検索結果の集計と摂動を X 回実施	ITX

4. 実験

4.1 MovieLens データセット

実際のパーソナルデータを用いて安全性と有用性を評価するため，公開データセットの一つである MovieLens データセットを用いる．レーティングのレコード数が異なる 4 種類のデータセット (100k, 1M, 10M, 20M) が公開されている．10M と 20M のデータセットにはユーザの年代や性別などの属性が付与されていないので，属性がある中で最も大きい MovieLens 1M データセットを用いる．データセットには，4,000 種類の映画に対して 6,040 人のユーザが付与した 100 万レコードのレーティングが収録されている．収録された時期は 2003 年 2 月である．データセットのユーザテーブルの一部を**表 3** に示す

レコード数はユーザ数と等しく 6,040 行 ($N = 6,040$) である．ユーザの属性には性別，年代，職業，郵便番号の 4 つの属性 ($W = 4$) がある．性別は Female と Male の 2 種類 ($V_1 = 2$) である．年代は 17 歳以下, 18 歳〜24 歳, 25 歳〜34 歳, 35 歳〜44 歳, 45 歳〜49 歳, 50 歳〜55 歳, 56 歳以上の 7 種類 ($V_2 = 7$) である．職業は**表 4** に示す 21 種類 ($V_3 = 21$) である．郵便番号は 5 桁の数字列に含まれる 3,402 種類 ($V_4 = 3,402$) である．

表 3 MovieLens 1M データセットのユーザテーブルのレコードの例
Table 3 Some records in user table of MovieLens 1M Dataset.

ID	Gender	Age	Occupation	Zip-code
1000	F	25〜34	6	90027
1001	M	25〜34	4	90210
1002	M	50〜55	11	07043

表 4 データセットに含まれる職業と，k-匿名化で指定するヒューリステティックな一般化階層
Table 4 Occupation list and its heuristic hierarchy settings for k-anonymization.

職業 (第 1 階層)	職業 (第 2 階層)	職業 (第 3 階層)
artist doctor / health care farmer homemaker technician / engineer	Category1	*
college / grad student K-12 student retired unemployed	Category2	
academic / educator clerical/admin customer service executive / manjobrial lawyer programmer sales/marketing scientist self-employed tradesman / craftsman writer	Category3	
other / not specified	Category4	

全ての属性を用いた場合，属性値の組み合わせはおよそ 100 万種類 ($V = 2 \times 7 \times 21 \times 3,402 = 1,000,188$) である．$V \times V$ のサイズを持つ A の要素の値を 64bit の Float で構成すると，行列の対称性で約半分の要素数を減らせるとはいえ，およそ 4TByte のメモリが必要となるので，文献 [17] の工夫を施す．

4.2 k-匿名化ツール

k-匿名化には，一般的な匿名加工ツールである ARX を用いる [27][28]．ARX はオープンソースで誰でも利用でき，Java で実装されていて動作環境の自由度も高い．また，同じくオープンソースで公開されている UTD Anonymization ToolBox[29] と比較したところ，ARX の方が処理が高速であったのでこれを用いる．ただし，ARX(バージョン

3.4.1) では，k-匿名化に指定できる k の値は 1,000 が上限である．

k-匿名化では，値の一般化の方法を指定する必要があり，次に述べるようにヒューリステティックに指定する．性別と年代については，隣接する属性値を 2 つ (ペアになれない余りが生じた場合は 3 つ) ずつ纏める．すなわち，性別は 1 階層目で Female，Male か，2 階層目で*(アスタリスクで任意の値を表す) の 3 パターンに一般化する．年代は 1 階層目で 17 歳以下, 18 歳〜24 歳, 25 歳〜34 歳, 35 歳〜44 歳, 45 歳〜49 歳, 50 歳〜55 歳, 56 歳以上か，2 階層目で 24 歳以下, 25 歳〜44 歳, 45 歳以上か，3 階層目で*の 11 パターンに一般化する．職業については，表 4 に示す 3 階層で 26 パターンに一般化する．郵便番号については，5 桁の数値列の桁を 5 つの階層とみなして下の桁から順に*でマスクしていき，10 万 ($= 10^5$) パターンに一般化する．

4.3 実験結果

一括開示と対話開示について，同じ ϵ における有用性を L2 距離と順位相関で定量化する．その他の加工方式は乱数を用いるので，30 回の試行を行って中央値を測定する．L2 距離は，各ユーザ属性の組み合わせにおける，加工後の度数の中央値とオリジナルの度数との差の二乗和の平方根であり，L2 距離が小さければ誤差は少ない．順位相関は，各ユーザ属性の組み合わせにおける，加工後の度数の中央値の順位とオリジナルの度数の順位との相関であり，順位相関が高ければ度数の大小関係が維持されている．順位相関は，一般に 0.7 以上であれば相関が強い．

対話型の安全性は検索回数に依存するので，回数を 1 回,10 回, 20 回,...,100 回と変化させて評価する．同等の安全性において，性別と年代の属性を持つデータを加工した場合の L2 距離と順位相関を**表 5** に，性別と年代と職業の場合を**表 6** に，性別と年代と職業と郵便番号の場合を**表 7** に示す．一括開示の BTk と BT と BR のうち，最も有用性が高い (L2 距離が小さい，または順位相関が高い) 値を斜体で示す．検索を繰り返し，一括開示よりも対話開示の有用性が低くなった (L2 距離が大きくなった，または順位相関が低くなった) 時点の値を太字で示す．

5. 有用性の評価

5.1 L2 距離に関する評価

求める安全性が低い ($\epsilon = 4.0$) 場合，表 5 に示すように性別と年代の 2 属性のみであれば，一括開示では BTk の L2 距離が最も小さくて 0 である．対話開示では，検索回数が 1 回の IT1 の L2 距離が 3 である．よって，BTk の一括開示が優れている．表 6 に示すように性別と年代と職業の 3 属性にすると，一括開示では BTk の L2 距離が最も小さくて 539 である．対話開示では，IT1 が 12 で IT40 が 477 である．よって，40 回まで対話開示が優れている．表 7 に示すように性別と年代と職業と郵便番号の 4 属性にすると，一括開示では BT の L2 距離が最も小さくて 0 である．対話開示では，IT1 が 707 である．よって，BT の一括開示が優れている．

求める安全性が中程度 ($\epsilon = 1.0$) の場合，2 属性のみであれば，一括開示では BR の L2 距離が最も小さくて 925 である．対話開示では，IT1 が 11 で IT80 が 847 である．よって，80 回まで対話開示が優れている．3 属性にすると，一括開示では BTk の L2 距離が最も小さくて 637 である．対話開示では，IT1 が 48 で IT10 が 477 である．よって，10 回まで対話開示が優れている．4 属性にすると，一括開

表 5 各手法での L2 距離と順位相関 (性別，年代)
Table 5 L2 distance and rank correlation of each method processing sex and age.

方式	L2 距離			順位相関		
	ϵ=0.1	ϵ=1.0	ϵ=4.0	ϵ=0.1	ϵ=1.0	ϵ=4.0
	k=4,945	k=818	k=3	k=4,945	k=818	k=3
BTk	-	1,261	*0*	-	0.49	*1.00*
BT	*1,431*	1,258	638	0.19	*0.77*	0.92
BR	2,074	*925*	221	*0.36*	0.74	0.98
IT1	106	11	**3**	0.98	1.00	1.00
IT10	1,058	106	26	0.73	0.98	1.00
IT20	**2,117**	212	53	0.53	0.96	1.00
IT30	3,175	317	79	0.39	0.92	**0.99**
IT40	4,233	423	106	**0.32**	0.89	0.98
IT50	5,292	529	132	0.28	0.86	0.97
IT60	6,350	635	159	0.25	0.82	0.97
IT70	7,408	741	185	0.24	0.78	0.96
IT80	8,467	847	212	0.20	**0.75**	0.96
IT90	9,525	**952**	238	0.18	0.74	0.95
IT100	10,583	1,058	265	0.18	0.73	0.94

表 6 各手法での L2 距離と順位相関 (性別，年代，職業)
Table 6 L2 distance and rank correlation of each method processing sex, age and occupation.

方式	L2 距離			順位相関		
	ϵ=0.1	ϵ=1.0	ϵ=4.0	ϵ=0.1	ϵ=1.0	ϵ=4.0
	k=4,945	k=818	k=3	k=4,945	k=818	k=3
BTk	-	*637*	*539*	-	0.21	*0.54*
BT	*657*	644	584	0.03	0.18	0.49
BR	737	1,223	800	*0.13*	*0.27*	0.42
IT1	477	48	12	**0.54**	0.94	0.99
IT10	**4,767**	477	119	0.08	0.54	0.84
IT20	9,534	**953**	238	0.03	0.36	0.71
IT30	14,301	1,430	358	0.01	0.27	0.61
IT40	19,068	1,907	477	0.01	**0.21**	0.54
IT50	23,835	2,383	**596**	0.00	0.18	**0.48**
IT60	28,602	2,860	715	0.00	0.15	0.43
IT70	33,369	3,337	834	-0.01	0.12	0.39
IT80	38,136	3,814	953	-0.01	0.11	0.36
IT90	42,903	4,290	1,073	-0.01	0.09	0.33
IT100	47,670	4,767	1,192	-0.01	0.08	0.31

表 7 各手法での L2 距離と順位相関 (性別，年代，職業，郵便番号)
Table 7 L2 distance and rank correlation of each method processing sex, age, occupation and ZIP code.

方式	L2 距離			順位相関		
	ϵ=0.1	ϵ=1.0	ϵ=4.0	ϵ=0.1	ϵ=1.0	ϵ=4.0
	k=4,945	k=818	k=3	k=4,945	k=818	k=3
BTk	-	*83*	*83*	-	0.01	0.02
BT	113	113	113	*1.00*	*1.00*	*1.00*
BR	*372*	1.43k	1.54k	*1.00*	*1.00*	*1.00*
IT1	**28.3k**	**2.82k**	**707**	**0.00**	**0.03**	**0.10**
IT10	283k	28.3k	7.07k	0.00	0.00	0.01
IT20	566k	56.6k	14.1k	0.00	0.00	0.01
IT30	848k	84.8k	21.2k	0.00	0.00	0.00
IT40	1.13M	113k	28.3k	0.00	0.00	0.00
IT50	1.41M	141k	35.3k	0.00	0.00	0.00
IT60	1.70M	170k	42.4k	0.00	0.00	0.00
IT70	1.98M	198k	49.5k	0.00	0.00	0.00
IT80	2.26M	226k	56.6k	0.00	0.00	0.00
IT90	2.54M	254k	63.6k	0.00	0.00	0.00
IT100	2.83M	283k	70.7k	0.00	0.00	0.00

示では BT の L2 距離が最も小さくて 0 である．対話開示では，IT1 が 2,828 である．よって，BT の一括開示が優れている．

求める安全性が高い ($\epsilon = 0.1$) 場合，2 属性のみであれば，一括開示では BT の L2 距離が最も小さくて 1,431 である．BTk は匿名加工ツールの仕様で $k = 4,945$ に加工できないので-(ハイフンで正しく測定できないことを表す)とする．対話開示では，IT1 が 106 で IT10 が 1,058 である．よって，10 回まで対話開示が優れている．3 属性にすると，一括開示では BT の L2 距離が最も小さくて 657 である．対話開示では，IT1 が 477 である．よって，対話開示の 1 回が優れている．4 属性にすると，一括開示では BT の L2 距離が最も小さくて 0 である．対話開示では，IT1 が 28,277 である．よって，BT の一括開示が優れている．

5.2 順位相関に関する評価

求める安全性が低い ($\epsilon = 4.0$) 場合，2 属性のみであれば，一括開示では BTk の順位相関が最も高くて 1.00 である．対話開示では，IT1 から IT20 まで 1.00 である．よって，BTk の一括開示と 20 回までの対話開示が優れている．3 属性にすると，一括開示では BTk の順位相関が最も高くて 0.54 である．対話開示では，IT1 が 0.99 で IT40 が 0.54 である．よって，40 回未満まで対話開示が優れている．4 属性にすると，一括開示では BT と BR の順位相関が最も高くて共に 1.00 である．対話開示では，IT1 が 0.10 である．よって，BT と BR の一括開示が優れている．

求める安全性が中程度 ($\epsilon = 1.0$) の場合，2 属性のみであれば，一括開示では BT の順位相関が最も高くて 0.77 である．対話開示では，IT1 が 1.0 で IT70 が 0.78 である．よって，70 回まで対話開示が優れている．3 属性にすると，一括開示では BR の順位相関が最も高くて 0.27 である．対話開示では，IT1 が 0.94 で IT30 が 0.27 である．よって，30 回未満まで対話開示が優れている．4 属性にすると，一括開示では BT と BR の順位相関が最も高くて共に 1.00 である．対話開示では，IT1 が 0.03 である．よって，BT と BR の一括開示が優れている．

求める安全性が高い ($\epsilon = 0.1$) 場合，2 属性のみであれば，一括開示では BR の順位相関が最も高くて 0.36 である．対話開示では，IT1 が 0.98 で IT30 が 0.39 である．よって，30 回まで対話開示が優れている．3 属性にすると，一括開示では BR の順位相関が最も高くて 0.13 である．対話開示では，IT1 が 0.54 である．よって，対話開示の 1 回が優れている．4 属性にすると，一括開示では BT と BR の順位相関が最も高くて共に 1.00 である．対話開示では，IT1 が 0 である．よって，BT と BR の一括開示が優れている．

5.3 評価のまとめ

加工対象とする属性に応じて，同等の安全性でより高い有用性が得られる開示方法を明らかにする．5.1 節での L2 距離に関する評価を**表 8** に，5.2 節での順位相関に関する評価を**表 9** にまとめる．

表 8 L2 距離の観点で高い有用性が得られる加工手法
Table 8 Anonymization methods getting small L2 distance.

加工対象の属性	求める安全性		
	ϵ=0.1	ϵ=1.0	ϵ=4.0
	k=4,945	k=818	k=3
性別，年代	IT10	IT80	BTk
性別，年代，職業	IT1	IT10	IT40
性別，年代，職業，郵便番号	BT	BT	BT

表 9 順位相関の観点で高い有用性が得られる加工手法
Table 9 Anonymization methods getting high Spearman's rank correlation coefficient.

加工対象の属性	求める安全性		
	ϵ=0.1	ϵ=1.0	ϵ=4.0
	k=4,945	k=818	k=3
性別，年代	IT30	IT70	BTk,IT20
性別，年代，職業	IT1	IT30	IT40
性別，年代，職業，郵便番号	BT,BR	BT,BR	BT,BR

まず，L2 距離について．表 8 から，2 属性または 3 属性の場合は，概ね対話開示が優れる．一点，2 属性の ϵ=4.0 は一括開示の BTk が優れているが，表 5 に示したように，L2 距離の ϵ=4.0 の BTk と IT1 の差は僅か 3 である．4 属性の場合は一括開示が優れる．

表 7 に示した通り，4 属性の L2 距離は $BTk \sim BT < IT < BR$ という結果になった．ここで $\epsilon = 4.0$ の場合を例

に挙げて，理由を考察する．1)BT は 6,040 人を 100 万種類のユーザ属性にランダムに置換するので，各属性にほぼフラットに散らばる．オリジナルと全く重なりが無ければ $L2 = \sqrt{\sum_{2\times 6{,}040}(1-0)^2} = 110$ となる．表 7 の実験結果は 113 である．BTk は一般化された属性値から可能性のある範囲で復元するので，BT と同様に属性が散らばり似た傾向にある．実験結果は 83 である．2)BR は BT が散らした値を再構築するので，フラットであった分布に変化が現れ，L2 距離は大きくなる．具体的に BR のユーザ数を多い方から 3 つ並べると 1,024 人，644 人，597 人であり，これだけでも $L2 = \sqrt{(1{,}024-0)^2+(644-0)^2+(597-0)^2} = 1{,}348$ となる．実験結果は 1,544 である．3)IT は可能性のある属性全てにノイズを加えるので，V に応じて L2 距離は大きくなる．ノイズだけで生じる L2 距離は $L2 = \sqrt{V\lambda} = \sqrt{V\frac{\Delta f}{\epsilon}} = \sqrt{10^6\frac{2}{4.0}} = 707$ となる．実験結果も 707 である．

次に，順位相関について．表 9 から，2 属性または 3 属性の場合は，概ね対話開示が優れる．4 属性の場合は一括開示が優れる．しかし，BT も BR がゼロが 99 パーセント以上と支配的であるため，ゼロ同士の順位が変わっていないというだけで順位相関が高くなってしまう．

6. おわりに

パーソナルデータを対象とするプライバシ保護技術は，一括開示型と対話開示型に大きく分類できる．本論文では，差分プライバシに基づいて，両者の性能を定量的に比較し，特に加工対象とする属性の増加に応じた有用性を明らかにした．また，一般な k-匿名化ツールで作成したデータとの有用性の違いを定量的に示した．今後，別データを用いて評価を行い，各手法の適用範囲と，安全性と有用性のトレードオフの一般性を明らかにしたい．

参考文献

[1] Dwork, C.: Differential Privacy, *Automata, Languages and Programming: 33rd ICALP* (2006).

[2] Sweeney, L.: K-anonymity: A Model for Protecting Privacy, *IJUFKS*, Vol. 10, No. 5, pp. 557–570 (2002).

[3] Gouweleeuw, J., Kooiman, P., Willenborg, L. and de Wolf, P.-P.: The Post Randomisation Method for Protecting Microdata, *QUESTIIO, Vol.22, No.1*, pp. 145–156 (1998).

[4] Ikarashi, D., Kikuchi, R., Chida, K. and Takahashi, K.: k-anonymous Microdata Release via Post Randomisation Method, *10th IWSEC* (2015).

[5] Weber, G., Murphy, S., McMurry, A., MacFadden, D., Nigrin, D., Churchill, S. and Kohane, I.: The Shared Health Research Information Network (SHRINE): a prototype federated query tool for clinical data repositories, *JAMIA*, Vol. 16, pp. 624–630 (2009).

[6] 山口高康，寺田雅之，吉浦　裕：差分プライバシに基づく一括開示と対話開示のデータ有用性の評価，情報処理学会研究報告, Vol.2016-CSEC-74 No.32 (2016).

[7] 五十嵐大，千田浩司，高橋克巳：k-匿名性の確率的指標への拡張とその適用例，*CSS* (2009).

[8] GroupLens: MovieLens 1M Dataset, GroupLens (online), available from ⟨http://grouplens.org/datasets/movielens/1m⟩ (accessed 2016-04-26).

[9] Machanavajjhala, A., Kifer, D., Gehrke, J. and Venkitasubramaniam, M.: l-Diversity: Privacy Beyond k-Anonymity, *TKDD* (2007).

[10] Li, N., Li, T. and Venkatasubramanian, S.: t-Closeness; Privacy Beyond k-Anonymity and l-Diversity, *23rd ICDE* (2007).

[11] Kooiman, P., Willenborg, L. and Gouweleeuws, J.: PRAM: A method for disclosure limitation of microdata, *Reseach paper No. 9705*, CBS (1997).

[12] Soria-Comas, J. and Domingo-Ferrer, J.: Probabilistic k-anonymity through microaggregation and data swapping, *ICFS*, pp. 1–8 (2012).

[13] Agrawal, R., Srikant, R. and Thomas, D.: Privacy Preserving OLAP, *SIGMOD*, pp. 251–262 (2005).

[14] 高橋 克己佐藤 一郎：匿名化技術の最新動向とその課題，国立情報学研究所ニュース，Vol. 64, pp. 10–11 (2016).

[15] 独立行政法人統計センター：国勢調査匿名データ及び国勢調査結果の構成，（オンライン），入手先 ⟨http://www.stat.go.jp/info/tokumei/pdf/ccgraph.pdf⟩（参照 2016-5-28）.

[16] 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).

[17] 永井　彰，五十嵐大，濱田浩気，松林達史：クロネッカー積を含む行列積演算の最適化による効率的なプライバシー保護データ公開技術，*SCIS* (2010).

[18] 寺田雅之，山口高康，本郷節之：匿名化個票への差分プライバシー基準の適用に関する一考察，情報処理学会研究報告, Vol.2016-CSEC-73 No.26 (2016).

[19] Adam, N. R. and Worthmann, J. C.: Security-control Methods for Statistical Databases: A Comparative Study, *CSUR*, Vol. 21, No. 4, pp. 515–556 (1989).

[20] Ghosh, A., Roughgarden, T. and Sundararajan, M.: Universally Utility-maximizing Privacy Mechanisms, *41st STOC*, pp. 351–360 (2009).

[21] Brenner, H. and Nissim, K.: Impossibility of Differentially Private Universally Optimal Mechanisms, *CoRR* (2009).

[22] Chen, R., Mohamme, N., Fung, B. C. M., Desai, B. C. and Xiong, L.: Publishing set-valued data via differential privacy, *VLDB*, Vol. 4, No. 11, pp. 1087–1098 (2011).

[23] Mohamme, N., Chen, R., Fung, B. C. M. and Yu, P. S.: Differentially Private Data Release for Data Mining, *KDD* (2011).

[24] Xiao, X. and Tao, Y.: Output Perturbation with Query Relaxation, *VLDB*, Vol. 1, No. 1, pp. 857–869 (2008).

[25] Mohan, P., Thakurta, A., Shi, E., Song, D. and Culler, D.: GUPT: Privacy Preserving Data Analysis Made Easy, *SIGMOD*, pp. 349–360 (2012).

[26] 船津好明：統計計算の方法, 明星大学（オンライン），入手先 ⟨http://www.wwq.jp/stacal.htm⟩（参照 2016-5-28）.

[27] Prasser, F., Kohlmayer, F., Lautenschlger, R. and Kuhn, K. A.: ARX - A Comprehensive Tool for Anonymizing Biomedical Data, *AMIA*, pp. 984–993 (2014).

[28] Kohlmayer, F., Prasser, F., Eckert, C., Kemper, A. and Kuhn, K. A.: Flash: Efficient, Stable and Optimal K-Anonymity, *PASSAT*, pp. 984–993 (2012).

[29] Security, U. D. and Lab, P.: UTD Anonymization ToolBox, , available from ⟨http://www.cs.utdallas.edu/dspl/cgi-bin/toolbox⟩ (accessed 2016-7-15).