Vol.2016-CSEC-74 No.32
Vol.2016-SPT-19 No.32
2016/7/15

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

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が注目を集め，数多くのプライバシ保護技術が提案されている．しかし，どのような場合にどの加工技術を選択すれば良いか明らかではない．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せる加工技術を選択できるようにする必要がある．本稿では，当該データの一括括示と対話開示における代表的な加工技術を取り上げ，同等の安全性での両者の有用性を評価する．これにより，当該データに含まれる個人と当該データの管理者および利用者が当該活用に安心して参加でき，価値のある知見を得られるようにする．

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

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

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](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][4] 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が，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い．そのため，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，従来明らかではない．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-匿名性を確率的に満たす k-匿名化 (Pk-匿名化)[5] 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 [3] を用いる．評価用データとして MovieLens データセット [6] 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．

[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

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．

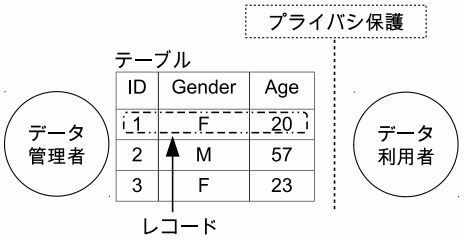


図 1 データ管理者とデータ利用者の関係
Fig. 1 Relationship between data administrator and analyst.

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．

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 [7]．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 [8]，t-近接性 [9] 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 [10]，k-匿名性を確率的に拡張した Pk-匿名化 [5][11] 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 [12][13][14].

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][15] 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 [15] 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 [3]．また，Pk-匿名化と k-匿名化の関係に関する研究成果 [5][3] 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 [5] 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．

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

$a(r'_w|r_w)$ 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．

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 [15] 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 [3]．

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

文献 [3] 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 [16]．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 [17]．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 [18]．差分プライバシに基づく一括開示の有用性評価 [19][20]，および対話開示の有用性評価 [21][22] 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．

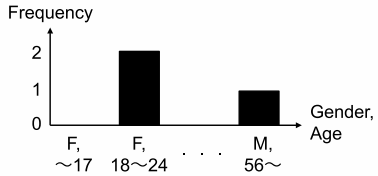
3. 安全性と有用性の評価方針

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 [23]．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

3.3.1 差分プライバシ (ϵ) と摂動の大きさ (λ)

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．

3.3.2 置換の維持パラメータ (ρ) と，差分プライバシ (ϵ) および Pk-匿名性 (k)

ρ_w と ϵ の関係は式 (6) で与えられる．ρ_w は w 毎に変えることが可能であるが，今回は基本性能の比較なので全ての ρ_w を等しい ($\rho = \rho_w$) とし，他は先と同じ設定 ($W = 2$, $V_1 = 2$，$V_2 = 7$) を用いる．ρ と ϵ の関係は**図 3** の左図のようになる．

ρ_w と k の関係は式 (7) で与えられる．N は MovieLens 1M データセットのユーザテーブルのレコード数と同じ 6,040 レコードとし，他は先と同じ設定 ($W = 2, V_1 = 2, V_2 = 7, \rho = \rho_w$) を用いる．$\rho$ と k の関係は図 3 の右図のようになる．

3.3.3 同等の安全性となる ϵ と k と ρ と λ

先行研究では，ϵ の値は $\epsilon = 0.1 \sim 10$ 程度 [20][21][22] が，k の値は $k = 3 \sim 10$ 程度が用いられている．これらの値をカバーするように，ϵ と k と ρ と λ の関係を整理すると**表 2** のようになる．表の上の方ほど安全性を優先したパラメータになっている．安全性を確保するため $k < 3$ の場合は考慮しない．4 章の実験では，$\epsilon = 0.1, 1.0, 4.0$ を用いる．

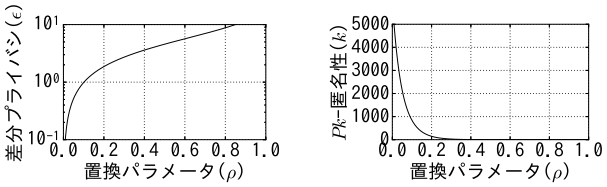


図 3 ρ と ϵ と k の関係
Fig. 3 Relation between ρ, ϵ and k.

表 2 ϵ と k と ρ と λ の関係
Table 2 Relation between ϵ, k, ρ and λ.

ϵ	k	ρ	λ
0.1	5,000	0.01	20
1.0	900	0.10	2.0
2.0	100	0.22	1.0
3.2	10	0.36	0.63
3.7	5	0.41	0.54
4.0	3	0.44	0.50

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 4** に示す．一括開示では，データ管理者はテーブルを 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

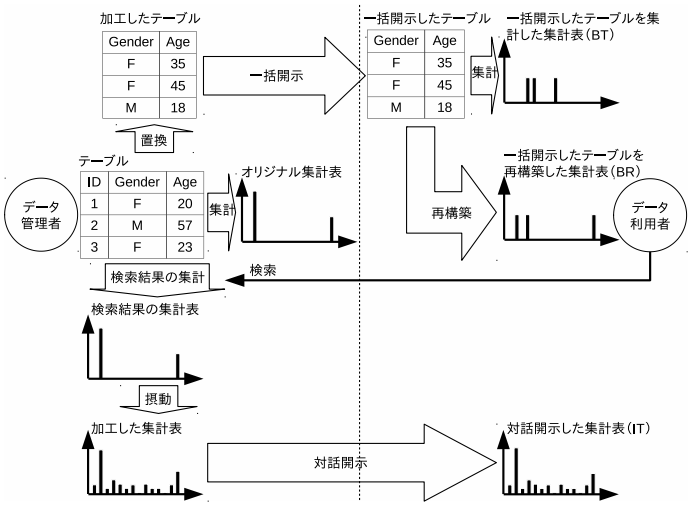


図 4 各プライバシ保護方式の処理フロー
Fig. 4 Data flows of each privacy preserving method.

るいは，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．一括開示の置換と対話開示の摂動の安全性を同じ ϵ で揃える．

上記の 3 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)，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，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 3**).

表 3 処理内容と加工方式の表記
Table 3 Denominating processes of anonymization.

開示種別	処理内容	加工方式の表記
一括開示	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 4** に示す

ユーザの属性には性別，年代，職業，郵便番号があるが，分析で可視化しやすいように性別と年代のみを用いる．性別は Female と Male の 2 種類で，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 種類である．

表 4 MovieLens 1M データセットのユーザテーブルのレコードの例
Table 4 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

4.2 実験結果

4.2.1 集計表の度数の分布

各加工方式は乱数を用いるので，30 回の試行を行い，集計表の各属性毎の度数の分布を求めた．**図 5** に BT(対話開示，再構築なし) の，**図 6** に BR(一括開示，再構築あり) の**図 7** に IT1(対話開示，1 回検索) の試行結果を示す． 横

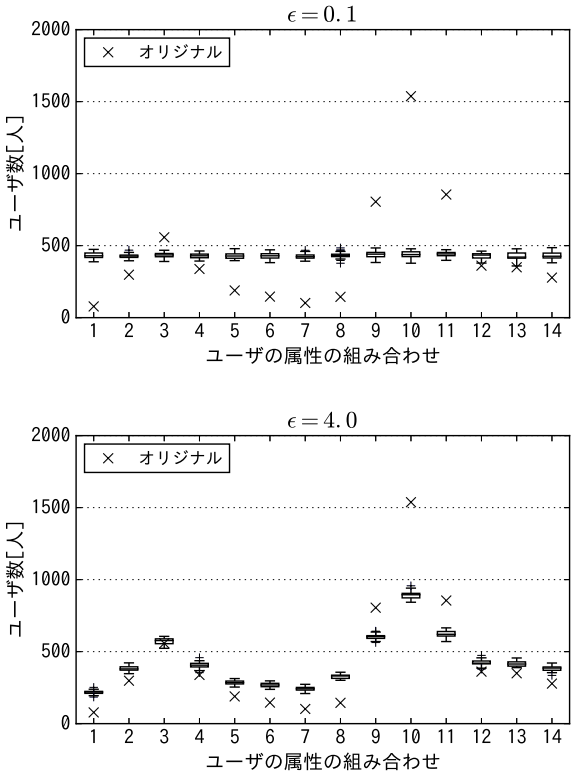


図 5 BT(一括開示, 再構築なし) の度数の分布
Fig. 5 Number of users in non-interactive setting without reconstruction.

軸は性別と年代を組み合わせた 14 種類のユーザ属性であり，例えば横軸の 1 のビンは女性 17 歳以下を表す．縦軸は当該属性の度数の 30 回試行における分布であり，例えば女性 17 歳以下の度数の分布を表す．箱ひげ図の箱の下部は第 1 四分位数を，箱の中の横棒は第 2 四分位数 (中央値) を，箱の上部は第 3 四分位数を表し，＋は外れ値を表す [24]．オリジナルの度数を × でプロットする．各方式の中央値 (箱の中の横棒) とオリジナルの度数 (×) が近いほど有用性が高い．また，各方式の度数の分布の広がりが小さいほど，方式が安定していると言える．

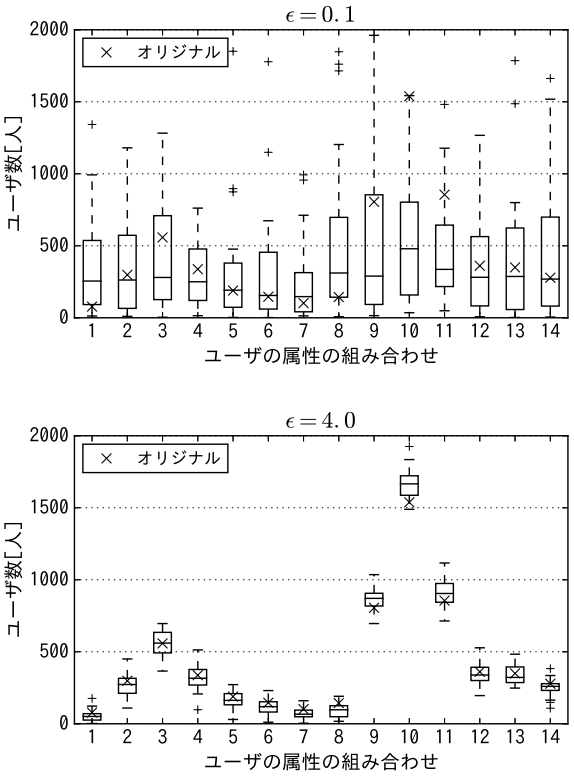


図 6 BR(一括開示，再構築あり) の度数の分布
Fig. 6 Number of users in non-interactive setting with reconstruction.

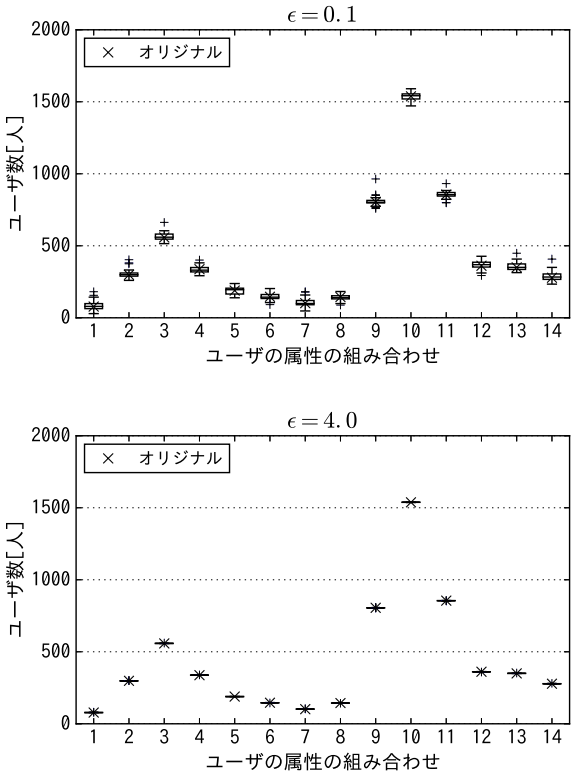


図 7 IT1(対話開示，1 回検索) の度数の分布
Fig. 7 Number of users in interactive setting.

4.2.2 検索回数に対する有用性

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．L2 距離を**図 8** に，順位相関を**図 9** に示す． L2 距離は，各ユーザ属性の組み合わせにおける，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，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，回数を変えて評価する．同等の安全性における，L2 距離と順位相関を**表 5** に示す．一括開示の BT と BR で，有用性が高い (L2 距離が小さい，または順位相関が高い) 方を斜体で示す．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 距離が長くなった，または順位相関が低くなった) 時点での対話開示の L2 距離と順位相関を太字で示す．例えば L2 距離は，$\epsilon = 0.1$ の安全性において，14 回未満の検索では対話開示が，14 回以上の検索では一括開示が有用であることを示す．順位相関は，$\epsilon = 0.1$ では強い相関を殆ど示さないので，表 2 で $\epsilon = 0.1$ 次に大きな $\epsilon = 1.0$ も用いることで，安全性に対する順位相関の強弱の境目を示す．

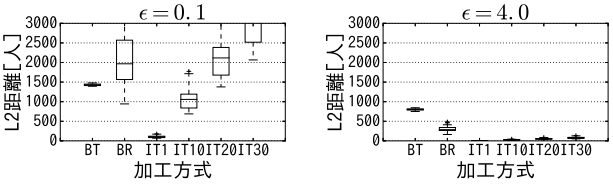


図 8 加工方式による L2 距離
Fig. 8 L2 distance of each method.

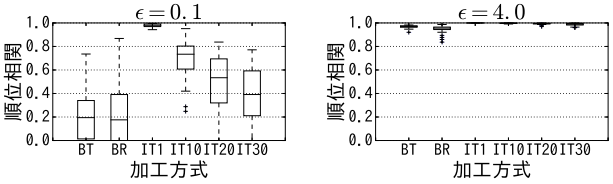


図 9 加工方式による順位相関
Fig. 9 Rank correlation of each method.

5. 有用性の評価

5.1 L2 距離に関する評価

安全性が高い $\epsilon = 0.1$ の場合の L2 距離は，表 5 より，BT が 1,430 人，BR が 1,967 人，IT1 が 106 人，IT14 が 1,482 人である．BT の 1,430 人は図 5($\epsilon = 0.1$) の 14 個の中央値とオリジナルの度数との L2 距離である．中央値は

表 5　各手法での L2 距離と順位相関
Table 5　L2 distance and rank correlation of each method.

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
BT	*1,430*	1,303	800	*0.19*	*0.83*	*0.97*
BR	1,967	*959*	*287*	0.18	0.78	0.96
IT1	106	11	3	0.98	1.00	1.00
IT10	1,058	106	26	0.73	0.98	1.00
IT14	**1,482**	148	37	0.65	0.97	1.00
IT55	5,821	582	146	0.26	**0.83**	0.97
IT62	6,562	656	164	0.25	0.82	**0.97**
IT89	9,419	942	235	**0.18**	0.74	0.95
IT91	9,631	**963**	241	0.18	0.74	0.95
IT109	11,536	1,154	**288**	0.18	0.71	0.93
IT436	46,142	4,614	1,154	0.08	0.28	0.71

属性値によらず殆ど一定となっており，オリジナルの集計表の情報が殆ど失われていることが分かる．ある属性値における中央値とオリジナルの度数の差の絶対値を誤差とみなすと，10 番目のビン (男性 25 歳〜34 歳) の誤差が最も大きく，1,000 人以上になっている．BR の L2 距離は BT より大きい．これは，再構築がうまく働かず，図 6($\epsilon = 0.1$) のように誤差を広げていることを示している．外れ値の影響が大きく，乱数次第で著しく大きな誤差が出る．IT1 では，L2 距離が大幅に縮小しており，図 7($\epsilon = 0.1$) のように若干の外れ値を除き，各属性における誤差は概ね 50 人以内である．外れ値において誤差が 150 人程度になる場合もあるが，BR に比べれば外れ値の影響は小さい．IT14 の 1,482 人は，BT の 1,430 人を超えた時点の L2 距離である．14 回未満で対話開示が有用，14 回以上では一括開示が有用であり，一括開示の中では再構築なしが有用である．

安全性が低い $\epsilon = 4.0$ の場合，BT の L2 距離 800 人は図 5($\epsilon = 4.0$) の中央値とオリジナルの度数の L2 距離である．最も誤差の大きい 10 番目のビンでは 500 人以上である．BR の L2 距離は 287 人と大幅に改善されており，図 6($\epsilon = 4.0$) のように再構築が有効に働いていることを示している．IT1 の L2 距離は 3 人であり，図 7($\epsilon = 4.0$) のように誤差は殆どない．109 回未満では対話開示，109 回以上では一括開示が有用である．

$\epsilon = 1.0$ の場合は，$\epsilon = 0.1$ と 4.0 の中間の特性を示している．3 方式のいずれも，$\epsilon = 0.1$ の場合より誤差が小さく，$\epsilon = 4.0$ の場合より誤差が大きい．再構築は有効であるが，$\epsilon = 4.0$ の場合よりは効果が小さい．検索回数が 1 回の場合は対話開示の有用性が極めて高い．対話開示が一括開示よりも劣る検索回数は 91 回以上である．

5.2　順位相関に関する評価

安全性が高い $\epsilon = 0.1$ の場合の順位相関は，表 5 より，BT が 0.19, BR が 0.18，IT1 が 0.98，IT89 が 0.18 である．BT の 0.19 は，図 5($\epsilon = 0.1$) の 14 個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る．両者に相関は殆どない．BR の順位相関は BT より低い．再構築がうまく働かず，図 6($\epsilon = 0.1$) のように誤差が大きく，外れ値の影響も大きい．IT1 では，順位相関が大幅に向上しており，図 7($\epsilon = 0.1$) のように，若干の外れ値を除き，中央値がオリジナルの度数と殆ど一致している．IT89 の 0.18 は BT の 0.19 を下回った時点の順位相関である．89 回未満で対話開示が有用，89 回以上では一括開示が有用であり，一括開示の中では再構築なしが有用である．

安全性が低い $\epsilon = 4.0$ の場合，BT の順位相関 0.97 は図 5($\epsilon = 4.0$) の中央値の順位とオリジナルの度数の順位の相関である．中央値とオリジナルの度数には差があるものの，両者の順位は維持されており，強い相関がある．BR の順位相関は 0.96 と若干低下しており，図 6($\epsilon = 4.0$) のように再構築で中央値がオリジナルの度数に近づくものの，順位が維持されるとは限らないことを示している．IT1 の順位相関は 1.00 であり，図 7($\epsilon = 4.0$) のように順位が維持されており，有用性が極めて高い．IT62 の 0.97 は，BT の 0.97 を (より小さい少数の桁で) 下回った時点の順位相関である．62 回未満で対話開示が有用，62 回以上では一括開示が有用であり，一括開示の中では再構築なしが有用である．

$\epsilon = 1.0$ の場合は，$\epsilon = 0.1$ と 4.0 の中間の特性で，3 方式とも $\epsilon = 0.1$ より順位相関が高く，$\epsilon = 4.0$ より順位相関が低い．再構築の効果は見られない．検索回数が 1 回の場合は対話開示の有用性が極めて高い．対話開示が一括開示よりも劣る検索回数は 55 回以上である．

5.3　評価のまとめ

一括開示と対話開示の有用性が交差する検索回数を**表 6** に示す．

表 6　一括開示と対話開示の有用性が交差する検索回数
Table 6　Retrieval frequency crossing utility in non-interaction and interaction settings.

ϵ	L2 距離	順位相関
0.1	14 回	89 回
1.0	91 回	55 回
4.0	109 回	62 回

L2 距離に関しては，5.1 節での評価と表 6 から，以下のようにまとめることができる．

(1) $\epsilon = 0.1, 1.0, 4.0$ の場合に，対話開示 1 回は一括開示に比べてオリジナル集計表との誤差が小さい．
(2) 求める安全性が高い (ϵ が小さい) ほど，対話開示の一括開示に対する優位性は小さくなる．しかし，安全性要求が最も高い $\epsilon = 0.1$ の場合は，一括開示に比べて誤差が 1/10 程度である．安全性要求が最も低い $\epsilon = 4.0$ の場合は，一括開示に比べて誤差が 1/100 程度である．

(3) 安全性を保ちながら対話開示を複数回行う場合，有用性が低下する．対話開示の有用性が一括開示の有用性を下回る検索回数は，安全性要求が高いほど小さくなる．つまり，安全性要求が大きいほど，対話開示の有用性が一括開示の有用性と早く交差する．しかし，$\epsilon = 0.1$ の場合でも 13 回までは対話開示の方が有用であり，$\epsilon = 4.0$ の場合は 108 回まで有用である．

(4) 各方式は乱数の影響により外れ値が発生する．外れ値は対話開示に比べて一括開示の方が発生しやすい．

(5) 求める安全性が高い場合は，一括開示における再構築は逆効果であり誤差を広げるが，求める安全性が低い場合には，再構築は誤差を小さくする効果がある．

また，順位相関に関しては，5.2 節での評価と表 6 から，以下のようにまとめることができる．

(1) $\epsilon = 0.1, 1.0, 4.0$ の場合に，対話開示 1 回は一括開示に比べてオリジナル集計表との順位相関が高い．

(2) 安全性を保ちながら対話開示を複数回行う場合，有用性が低下する．しかし，対話開示の有用性が一括開示の有用性と最も早く交差する $\epsilon = 1.0$ の場合でも，54 回の開示までは対話開示の方が有用である．

(3) 一括開示における再構築の効果は見られない．

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，両者の性能を世界で初めて定量的に比較し，以下を明らかにした．

- 差分プライバシにおいて安全性を等しくした時に，対話開示 1 回は一括開示に比べて，データの劣化が著しく小さく，有用性が高い．
- 対話開示は，誤差の低減と順位の維持の両方において，一括開示よりも優位であるが，順位の維持において，より優位性が高い．
- 複数回の検索に応える場合，対話開示の有用性は低下する．安全性要求が高い程，対話開示の有用性は一括開示の有用性を早く下回るようになる．
- 各方式は乱数の影響により外れ値が発生する．外れ値は対話開示に比べて一括開示の方が発生しやすい．

本論文の実験における安全性 (ϵ) の範囲では，対話開示は一括開示よりも常に有用であった．今後，より高い安全性要求における比較を行い，対話開示の優位性の変化を明らかにしたい．

参考文献

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

[2] 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).

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

[4] 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).

[5] 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).

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

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

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

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

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

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

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

[13] 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).

[14] 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）.

[15] 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).

[16] 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).

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

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

[19] 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).

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

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

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

[23] 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）.

[24] Dekking, F. M., Kraaikamp, C., Lopuha, H. P. and Meester, L. E.: *A modern introduction to probability and statistics*, chapter 16.4 The box-and-whisker plot, pp. 236–238, Springer (2005).