属性推定確率を制御する撹乱手法

千田 浩司† 菊池 亮† 五十嵐 大† 高橋 克巳†

†日本電信電話株式会社 NTT セキュアプラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11

あらまし パーソナルデータ開示のプライバシリスクは再識別 (re-identification) と属性暴露 (attribute disclosure) に大別される．属性暴露に対しては，完全な保護は不可能である事が示されているため，適切で受容性の高いプライバシ指標の確立が望まれる．本稿では，属性暴露に関する既存のプライバシ指標に基づいた，直感的で分かり易い指標を与える．具体的には，元のパーソナルデータに含まれる任意の個人の属性値が，一定の範囲内の確率でしか推定出来ないかどうかを指標とする．また，当該プライバシ指標を満たすための撹乱手法を提案し，撹乱されたパーソナルデータの有用性について考察する．

A Perturbation Method for Limiting Probability of Attribute Inference

Koji Chida† Ryo Kikuchi† Dai Ikarashi† Katsumi Takahashi†

†NTT Secure Platform Laboratories
3-9-11 Midori-cho, Musashino, Tokyo 180-8585, JAPAN

Abstract Privacy risk of personal data disclosure is roughly divided into *re-identification* and *attribute disclosure*. For attribute disclosure, since it has been proven complete protection is impossible, the establishment of appropriate and widely acceptable privacy criteria is desired. In this paper, based on the existing privacy criteria related to attribute disclosure, we propose an intuitive and easy to understand privacy criterion. The criterion guarantees that the attribute value of any individual can be deduced only within a certain probability. We also propose a perturbative method for meeting the privacy criteria and consider the utility of the anonymized personal data.

1 はじめに

ICT の発達に伴い多種多様な大量の情報が容易に収集出来るようになり，情報の利活用による新たな価値創造への期待が高まっている．しかしパーソナルデータ（個人に関する情報）を扱う際はプライバシ保護に十分配慮する必要がある．

本稿では，パーソナルデータを所持する主体が，当該データを別の主体またはオープンに開示する際のプライバシリスクに着目する．パーソナルデータ開示のプライバシリスクは**再識別** (*re-identification*) と**属性暴露** (*attribute disclosure*) に大別される．簡単に言えば，再識別は誰のパーソナルデータか知られてしまうリスクであり，属性暴露はパーソナルデータの開示によって特定の個人のセンシティブな属性値を知られてしまうリスクである．

パーソナルデータが再識別されると，一般に属性暴露のリスクが高まる．そのため，再識別は間接的なプライバシリスクであり，属性暴露は直接的なプライバシリスクと言える．しかし属性暴露はこれまで様々なプライバシ指標や保護手法が提案されているものの，完全な保護は不可能である事が示されている [1, 2, 3]．従って，適切で受容性の高いプライバシ指標の確立が望まれる．

本稿では，属性暴露に関する既存のプライバ

名前 （識別子）	性別 （準識別子）	年齢 （準識別子）	年収 （非識別子：SA）	好物 （非識別子）
Alice	F	24	$46K	Coffee
Bob	M	25	$52K	Beer
Chris	M	30	$57K	Cola
Dan	M	30	$81K	Milk
Eve	F	32	$50K	Cola
Flora	F	32	$104K	Whiskey

図 1: 元のパーソナルデータの例

シ指標に基づいた，直感的で分かり易い指標を与える．具体的には，元のパーソナルデータに含まれる任意の個人のセンシティブな属性値が，一定の範囲内の確率でしか推定出来ないかどうかを指標とする．また，当該プライバシ指標を満たすための撹乱手法を提案し，撹乱されたパーソナルデータの有用性について考察する．

2 準備

本稿で扱う元のパーソナルデータは，図 1 に例示するように各個人のデータが 1 レコードに記載された表形式データとする．各レコード r は M 種類の属性 A の属性値からなる．属性値は質的データ（カテゴリデータ）と仮定し，属性 A には m 種類の属性値 a_u $(u = 1, \ldots, m)$ があるものとする．属性は便宜上，識別子，準識別子，非識別子の何れかに分類する場合がある．識別子は個人を一意に識別できる属性とし，図 1 の例では「名前」を識別子としている．準識別子は間接的に個人を識別できる属性とし，図 1 の例では「性別」や「年齢」を準識別子としている．非識別子は識別子と準識別子以外の属性とする．ここで非識別子はセンシティブな属性 SA (Sensitive Attribute) を含むものとし，図 1 の例では「年収」を SA としている．

再識別や属性暴露のリスクを低減するためのパーソナルデータの加工処理を**匿名化**と呼ぶ．匿名化したパーソナルデータを**匿名化データ**と呼ぶ．匿名化は，非撹乱的な手法と撹乱的な手法に大別される [4, 5]．非撹乱的な手法は，リコーディング，データの削除，トップ（またはボトム）・コーディング等がある．リコーディングはデータを一般化する手法であり，例えば年齢を「年代」に変更する．トップ・コーディングは，一定以上の値をまとめる手法であり，例えば 85 歳以上の年齢を全て「85 歳以上」に変更する．一方，撹乱的な手法は，ノイズ付加，スワッピング，ラウンディング（丸め），ミクロアグリゲーション，PRAM 等がある．属性値が質的データの場合，スワッピングや PRAM を適用出来る．スワッピングは，複数のレコード間の属性値を入れ替える．PRAM は，事前に設定されたマルコフ連鎖遷移行列に基づいて属性値を確率的に別の値に入れ替える．

3 関連研究

再識別を防ぐためには，少なくともパーソナルデータから識別子を削除または識別されない別の値に変更する必要がある．以降では簡単のため，識別子が削除されたパーソナルデータについて考える．しかし識別子の削除だけでは再識別の対策として不十分な場合があり，準識別子の値によっては再識別のリスクが残る．Sweeney は，準識別子の値の組が同一となるレコードが k 個以上存在するかどうかを指標とする ***k*-匿名性** (*k-anonymity*) を提案した [6]．以降，準識別子の値の組が同一となるレコード群を *EQI* (*Equivalent Quasi-Identifier class*: 等準識別子クラス) と呼ぶ．k-匿名性を満たすように匿名化すれば，任意の個人のレコードを k 個未満に絞り込む事が出来ない．k-匿名性を満たすための加工処理として，準識別子に対して非撹乱的な手法が一般に用いられる．

五十嵐らは，k-匿名性を確率的指標に拡張した ***Pk*-匿名性**を提案し，PRAM を用いて Pk-匿名性を満たす手法を提案した [7]．Pk-匿名性は，任意の個人のレコードを $1/k$ を超える確率で推定出来ないかどうかを指標とする．

再識別が困難であっても，SA の値 (SA 値) によっては属性暴露のリスクがある．Machanavajjhala らは，具体的なリスクとして**同種攻撃** (*homogeneity attack*) と**背景知識攻撃** (*background knowledge attack*) を挙げている [1]．同種攻撃は，匿名化データの SA 値の分布から特定の個人 (ターゲット) の SA 値を推定する攻撃であり，例えば EQI の SA 値が全て同じであれば，EQI のレコード群から再識別は出来なくてもターゲットの SA 値を知り得てしまう．背景知識攻撃は，ターゲットの EQI について，SA 値に関する背景知識を利用してターゲットの SA 値を推定する攻撃である．背景知識は例えば，ターゲットの年収は「500 万円未満」(または 500 万円以上ではない) 等の事前に知っている情報である．

同種攻撃を考慮したプライバシ指標として，Wong らは **(α, k)-匿名性**を提案した [8]．任意

の EQI について，任意の SA 値の出現頻度の割合が α 以下かどうかを指標とする．[8] では，(α, k)-匿名性を満たすための匿名化としてリコーディングを用いている．一方，背景知識攻撃を考慮したプライバシ指標として，Truta らは **p-センシティブ k-匿名性**を提案した [9]．任意の EQI の SA 値が p 種類以上存在するかどうかを指標とする．攻撃者がターゲットの SA 値について $p-2$ 種類までの可能性を排除出来たとしても，SA 値を特定出来ない．Machanavajjhala らも [1] において背景知識攻撃を考慮したプライバシ指標 **ℓ-多様性** (ℓ-*diversity*) を提案した．具体的には 3 種類の指標を与えており，例えば **帰納的 (c, ℓ)-多様性** (*recursive* (c, ℓ)-*diversity*) は，c を定数，f_i をセンシティブな属性 A の i 番目に頻度の高い SA 値の頻度とした時，

$$f_1 < c \sum_{\ell \leq u \leq m} f_u$$

を満たすかどうかを指標とする．さらに五十嵐らは帰納的 (c, ℓ)-多様性を確率的指標に拡張した**帰納的 $P(c, \ell)$-多様性**を提案した [10]．

Evfimievski らは，匿名化データの開示前後における攻撃者の知識の差を確率的に評価する **ρ_1-to-ρ_2 プライバシ侵害** (ρ_1-*to*-ρ_2 *privacy breach*)(または (α, β)-プライバシ [11]) を提案した [12]．具体的には，X, Y をそれぞれ匿名化前後のデータの確率変数，$Q(x)$ を匿名化前のデータを入力とする述語関数とした時，$0 < \rho_1 < \rho_2 < 1$ を満たす定数 ρ_1, ρ_2 について

$$\Pr(Q(X)) \leq \rho_1 \wedge \Pr(Q(X)|Y = y) \geq \rho_2$$

であれば (上向き (upward))ρ_1-to-ρ_2 プライバシ侵害と呼ぶ．即ち，$Q(X)$ が真となる確率が匿名化データ y の開示によって ρ_1 以下から ρ_2 以上になるとリスクが高いと見なす．[12] では，ρ_2 以上から ρ_1 以下になる場合 (下向き (downward)) も同様にリスクが高いとしている．

最後に，本稿で提案するプライバシ指標とは関連性が低いが，属性暴露のリスクに対するその他の代表的な既存プライバシ指標を 7 節で後述する．

4 課題

3 節で紹介したように，属性暴露についてこれまで様々なプライバシ指標が提案されている．しかし属性暴露に対する完全な保護は不可能であるため，適切で受容性の高いプライバシ指標の確立が望まれる．これが本稿で扱う一つ目の課題である．

もう一つの課題は，属性暴露を防ぐための匿名化がパーソナルデータの**有用性** (*utility*) を著しく低下させない事である．例えば (c, ℓ)-多様性を満たすために，k-匿名性を満たす以上に準識別子をより一般化する必要が生じ得るが，準識別子を一般化するほど有用性が下がってしまう．

5 提案方式

本稿では，プライバシ指標の受容性を高める要因として「指標の分かり易さ」と「他の指標との組み合わせ」に着目する．例えば k-匿名性は，「任意の個人のレコードを k 個未満に絞り込む事が出来ない」という，再識別に対する直感的で分かり易い指標と言える．また優劣を付け難い複数のプライバシ指標は，両方満たせばより受容性が高まると考えられる．

提案方式の説明の前に，再識別されても属性暴露になるとは限らない事を強調しておきたい (3 節では，再識別されなくても属性暴露となる場合を述べた)．SA 値を加工しなければ，再識別されれば直ちに属性暴露に繋がるが，SA 値に PRAM 等の撹乱的な加工を施したり，暗号化する事で属性暴露を防げる可能性がある．

5.1 指標

提案指標は，(α, k)-匿名性と同様，SA 値を一定以上の確率で推定出来ないかどうかをプライバシ指標の一つとする．但し (α, k)-匿名性は，p-センシティブ k-匿名性のような一部の SA 値の可能性の排除については考慮していない．そこでどの SA 値も一定以上の確率で存在するよう指標を追加する．具体的には，属性暴露に対する確率的なプライバシ指標として，以下の **$P(\alpha, \gamma)$-プライバシ**を定義する．

定義 5.1 ($P(\alpha, \gamma)$-プライバシ)**.** α, γ を $0 \leq \gamma < \alpha \leq 1$ を満たす定数とする．Y, A をそれぞれ匿名化データ，及び Y に含まれるセンシティブな属性とする．このとき，A の任意の *SA* 値 a_u について，任意のレコード r の *SA* 値が a_u となる条件付き確率 $\Pr(A = a_u|Y)$ が

$$\gamma \leq \Pr(A = a_u|Y) \leq \alpha \qquad (1)$$

となるとき，Y は $P(\alpha,\gamma)$-プライバシを満たすという．

上記定義は ρ_1-to-ρ_2 プライバシ侵害と異なり，攻撃者の事前知識は指標に含まれない．但し後述するように式 (1) を満たすかどうか判定する際に事前知識を用いる．また下向き ρ_1-to-ρ_2 プライバシ侵害において $Q(x)$ を “レコード r の SA 値が x” という述語とすれば，上記定義は ρ_1-to-ρ_2 プライバシ侵害に類似する．しかし ρ_1-to-ρ_2 プライバシ侵害が匿名化データの開示によって生じる個々のデータの推定確率の差を指標としているのに対し，上記定義はデータ全体の推定確率の上下限を指標としている．

5.2 匿名化手法

$P(\alpha,\gamma)$-プライバシを満たすための匿名化として，[10] 等と同様，PRAM の適用を考える．なお簡単のため，匿名化データ Y に含まれる SA は一種類とする．SA が複数の場合については 6.3 節で考察する．

PRAM は，ρ を 0 以上 1 以下の確率パラメータとして属性値を確率的に置き換える．本稿では [10] と同様，$a_u \in A$ が $a_v \in A$ に遷移する確率 $q_{u,v}$ を次式で与える．

$$q_{u,v} = \begin{cases} \rho + \frac{1-\rho}{m} & (u = v) \\ \frac{1-\rho}{m} & (u \neq v) \end{cases} \tag{2}$$

即ち，ρ の値が大きい程，遷移後の属性値は元の属性値のままである確率が高い．逆に言えば，ρ の値が小さい程，遷移後の属性値から元の属性値の推定が一般に困難となる．以降，遷移後の属性及び属性値を便宜上それぞれ A', a'_v と表記する．従って式 (2) の左辺は $\Pr(A' = a'_v | A = a_u)$ となる．

定義 5.1 の条件付き確率は，ベイズの定理より

$$\Pr(A{=}a_u|Y){=}\frac{\Pr(A{=}a_u)\Pr(Y|A{=}a_u)}{\sum_w \Pr(A{=}a_w)\Pr(Y|A{=}a_w)} \tag{3}$$

が成り立つ．従って，レコード r の任意の SA 値の事前確率 $\Pr(A = a_w)$，及び Y の条件付き確率 $\Pr(Y|A = a_w)$ が決まれば式 (1) の指標を満たすかどうか分かる．

$\Pr(Y|A = a_w)$ について，$P(\alpha,\gamma)$-プライバシを最も満たしにくい Y の SA 値は，遷移後の値が全て等しい場合である．この時，ターゲットの SA 値はそれ以外の SA 値と独立であると仮定し，ターゲット以外の個人の SA 値が全て a'_v となる確率を θ とすれば，式 (3) は以下のようになる．

$$\begin{aligned} \Pr(A = a_u|Y) &= \frac{\Pr(A = a_u)\theta q_{u,v}}{\sum_w \Pr(A = a_w)\theta q_{w,v}} \\ &= \frac{\Pr(A = a_u) q_{u,v}}{\sum_w \Pr(A = a_w) q_{w,v}} \end{aligned} \tag{4}$$

従って，式 (4) を式 (1) に代入すれば，

$$\begin{aligned} \max_{a_u, a'_v} \frac{\Pr(A = a_u) q_{u,v}}{\sum_w \Pr(A = a_w) q_{w,v}} \leq \alpha, \\ \min_{a_u, a'_v} \frac{\Pr(A = a_u) q_{u,v}}{\sum_w \Pr(A = a_w) q_{w,v}} \geq \gamma \end{aligned} \tag{5}$$

の関係式を得る．

最後に式 (5) を判定するためには，$q_{w,v}$ の変数である確率パラメータ ρ と SA 値の種類数 m，及びターゲットに対する攻撃者の事前知識である $\Pr(A = a_w)$ が決まればよい．本稿では攻撃者の事前知識について，

1. 全ての SA 値の確率が等しい (攻撃者は何も知らない)
2. レコード全体の SA 値の分布

の 2 種類を例に，$m = 3$ として式 (5) に代入して評価した．図 2,3 は，各 ρ における SA 値の事後確率の最大値及び最小値を示している．図 2 の SA 値の事前確率は全て $1/m$ となる．図 3 の SA 値の事前確率は $\Pr(A = a_1) = 0.7$, $\Pr(A = a_2) = 0.2$, $\Pr(A = a_3) = 0.1$ とした．

図 2,3 から分かるように，ρ が小さくなる程，SA 値の事後確率の最大値及び最小値ともに事前確率の値に近づく (ρ が小さい程，一般に有用性が下がる事に注意)．但し常に事後確率の最大値は事前確率の最大値以上であり，事後確率の最小値は事前確率の最小値以下である．即ち α は事前確率の最大値以上とし，γ は事前確率の最小値以下とする必要がある．

これまでは匿名化データ Y が攻撃者にとって最も都合の良い場合，即ち Y の SA 値が全て等しい場合について，元のパーソナルデータの SA 値の事後確率を考えた．そこで次に条件を緩和し，Y の確率を考慮した SA 値の事後確率

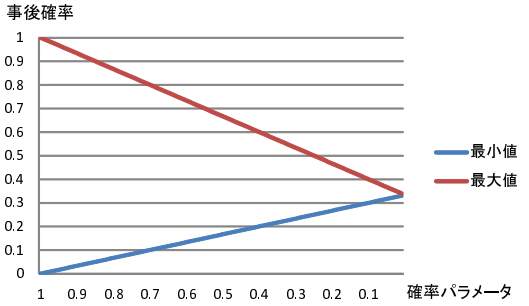

図 2: 3 種類の SA 値の事後確率の最大値と最小値 (事前確率が等確率の場合)

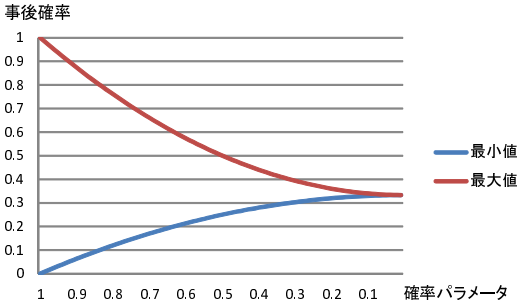

図 4: 3 種類の SA 値の事後確率の最大値と最小値 (2)(事前確率が等確率の場合)

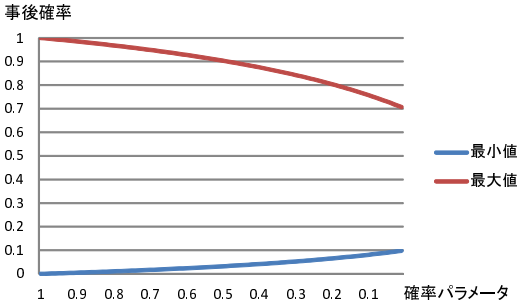

図 3: 3 種類の SA 値の事後確率の最大値と最小値 (事前確率を 0.7, 0.2, 0.1 とした場合)

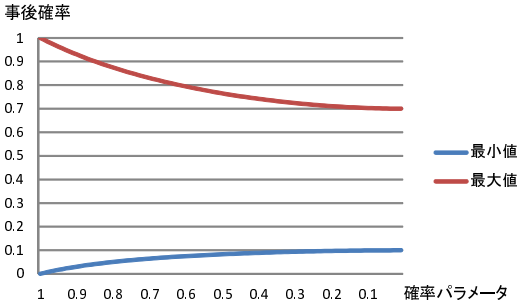

図 5: 3 種類の SA 値の事後確率の最大値と最小値 (2)(事前確率を 0.7, 0.2, 0.1 とした場合)

を考える．元のパーソナルデータが $P(\alpha,\gamma)$-プライバシを最も満たしにくい場合は，元のパーソナルデータの SA 値が全て等しい場合である．この時，Y の期待値における SA 値 a'_v の頻度の割合は，元のパーソナルデータの SA 値を a_t とすれば式 (2) より $q_{t,v}$ で与えられる．従って，式 (3) は式 (4) に Y の確率を考慮すれば以下のようになる．

$$\Pr(A=a_u|Y)=\sum_v q_{t,v}\frac{\Pr(A=a_u)q_{u,v}}{\sum_w \Pr(A=a_w)q_{w,v}} \quad (6)$$

従って，式 (6) を式 (1) に代入すれば，

$$\begin{aligned}\max_{a_u,a'_v,a_t}\sum_v q_{t,v}\frac{\Pr(A=a_u)q_{u,v}}{\sum_w \Pr(A=a_w)q_{w,v}} &\le \alpha,\\ \min_{a_u,a'_v,a_t}\sum_v q_{t,v}\frac{\Pr(A=a_u)q_{u,v}}{\sum_w \Pr(A=a_w)q_{w,v}} &\ge \gamma\end{aligned} \quad (7)$$

の関係式を得る．

図 4,5 は，式 (6) を式 (1) に代入し，それぞれ図 2,3 と同じ条件における SA 値の事後確率の最大値及び最小値を示している．図 2,3 と比べ，SA 値の事後確率の最大値は減少，最小値は増加している事が分かる．従って，プライバシの観点からは α をより小さい値，γ をより大きい値とし，有用性の観点からは ρ の値をより大きく取れる．

更に α をより小さい値，γ をより大きい値とする，あるいは ρ の値をより大きく取れる方法として，元のパーソナルデータの SA 値にある程度多様性を持たせる方法が考えられる．例えば元のパーソナルデータを，(α,k)-匿名性を満たすよう事前に加工しておく．すると当該加工データの任意の EQI について，SA 値の最頻値の頻度の割合は高々 α と見なせるから，当該加工データが $P(\alpha,\gamma)$-プライバシを最も満たしにくい場合は，当該加工データの任意の EQI について SA 値の最頻値の頻度の割合が α，次に高い頻度の割合が $1-\alpha$ の場合である．このような加工データから得られる匿名化データ Y について，Y の確率を考慮した SA 値の事後確率を考えれば良い．予め任意の EQI の SA 値が多様性を持っていれば，遷移確率 ρ の値を大きく取れるという，直感的な考えに基づいている．但

し前記のような多様性を持たせるためにはEQIの存在を仮定，即ち再識別が困難である事を前提としているのに対し，式(4),(6)は再識別の困難性を前提としていない．従って，図2–5の場合は準識別子を加工する必要が無いという特徴がある．

6 考察

6.1 Pk-匿名性との組み合わせ

複数のプライバシ指標を組み合わせて評価する事は，プライバシや受容性の向上に繋がり得る．そこで提案方式と同様，PRAMを用いて指標を満たす手法が知られている，Pk-匿名性との組み合わせについて考える．Pk-匿名性は基本的に，準識別子や非識別子を問わず，全ての属性値についてPRAMを適用する．そしてkとPRAMの撹乱パラメータρの間には以下の関係式がある．

$$k \leq 1 + (n-1)(\prod_{A} \frac{1-\rho_A}{1+(m_A-1)\rho_A})^2 \quad (8)$$

ここでnはパーソナルデータのレコード数，ρ_A, m_Aはそれぞれパーソナルデータに含まれる属性Aの撹乱パラメータ及び属性値の種類数とする．以降，話しを簡単にするためρ_Aは全て等しいものとし，ρと表記する．するとPk-匿名性及び$P(\alpha,\gamma)$-プライバシをともに満たすためには，式(5)(あるいは式(7))及び式(8)を満たすρを求めれば良い．

6.2 有用性

$P(\alpha,\gamma)$-プライバシを満たす匿名化データの有用性について考察する．匿名化データの有用性指標は多数存在し，匿名化データの用途によっても異なる．そこで本稿では，6.1節の考察に基づき，Pk-匿名性を満たす匿名化データとの比較を実験的に行う事とした．具体的には，UCI Machine Learning Repository の Census Income Data Set[13] を用いて，Pk-匿名性及び$P(\alpha,\gamma)$-プライバシを満たすρの値を算出した．Pk-匿名性を満たすためのρの値がより小さければ，Pk-匿名性を満たす匿名化データは$P(\alpha,\gamma)$-プライバシも満たすため，$P(\alpha,\gamma)$-プライバシを満たすための匿名化は不要となる．

Census Income Data Setは，1994年のアメリカのセンサスデータベースから抽出・加工された14の属性からなる32,561件の公開データセットである．本実験では14の属性から表1に示す質的データを抽出した．なお表1の各属性について，各属性値の頻度の最大値と最小値を求めたところ，表2の結果となった．そこで最小値の割合が比較的大きい(即ち条件がより厳しい) Income と Relationship を SA と見なして実験を行った．

表 1: 本実験で用いた属性

属性名	属性値数: 属性値
Income	2: “>50K”, “<=50K”
Marital-status	7: Married-civ-spouse, Divorced, Never-married, Separated, Widowed, Married-spouse-absent, Married-AF-spouse
Relationship	6: Wife, Own-child, Husband, Not-in-family, Other-relative, Unmarried
Race	5: White, Asian-Pac-Islander, Amer-Indian-Eskimo, Other, Black

表 2: Census Income Data Set における各属性値の頻度の最大値と最小値

属性名: 属性値数	最大値 (割合)	最小値 (割合)
Income: 2	24,720 (75.9%)	7,841 (24.1%)
Marital-status: 7	14,976 (46.0%)	23 (0.07%)
Relationship: 6	13,193 (40.5%)	981 (3.01%)
Race: 5	27,816 (85.4%)	271 (0.83%)

$P(\alpha,\gamma)$-プライバシについて，式(7)を基準にSA値の事前確率をレコード全体のSA値の分布とした．そしてk, α, γの値をいくつか決め，Pk-匿名性及び$P(\alpha,\gamma)$-プライバシを満たすρの条件を算出した(表3)．表3の“ρ (Pk)”の列は，Pk-匿名性を満たすρの条件を示し，“ρ (α)”及び“ρ (γ)”の列は，それぞれ(α,γ)-プライバシの閾値α及びγを満たすρの条件を示している．なおPk-匿名性を満たすρの条件はSAの取り方によらず不変となる(kの値と属性の組み合わせに依存する)．最終的にこれらのアンドを取った“ρ”の列が，Pk-匿名性及び$P(\alpha,\gamma)$-プライバシをともに満たすρの条件となる．表3から，今回の例ではPk-匿名性を満たすρが(α,γ)-プライバシも満たす場合が少なからずある事を確認出来た．

表 3: Pk-匿名性及び $P(\alpha,\gamma)$-プライバシを満たす ρ の条件

Case	SA	k	(α,γ)	ρ (Pk)	ρ (α)	ρ (γ)	ρ
# 1	Income	3	$(0.8, 0.1)$	≤ 0.3343	≤ 0.4678	≤ 0.8113	≤ 0.3343
# 2	Income	3	$(0.77, 0.22)$	≤ 0.3343	≤ 0.2476	≤ 0.3397	≤ 0.2476
# 3	Income	5	$(0.77, 0.22)$	≤ 0.3063	≤ 0.2476	≤ 0.3397	≤ 0.2476
# 4	Income	10	$(0.77, 0.22)$	≤ 0.2738	≤ 0.2476	≤ 0.3397	≤ 0.2476
# 5	Relationship	3	$(0.5, 0.02)$	≤ 0.3343	≤ 0.3416	≤ 0.7482	≤ 0.3343
# 6	Relationship	3	$(0.47, 0.025)$	≤ 0.3343	≤ 0.2756	≤ 0.5416	≤ 0.2756
# 7	Relationship	5	$(0.47, 0.025)$	≤ 0.3063	≤ 0.2756	≤ 0.5416	≤ 0.2756
# 8	Relationship	10	$(0.47, 0.025)$	≤ 0.2738	≤ 0.2756	≤ 0.5416	≤ 0.2738

6.3 センシティブな属性が複数ある場合

これまでは元のパーソナルデータに含まれる SA は一属性のみと仮定していた．しかし実際には複数の SA を扱える方が望ましい．複数の SA を扱う場合，SA 間の依存関係に考慮しなければいけない．各 SA が他の SA と独立であれば，SA 毎に式 (3) を考えれば済む．しかし SA 間の依存関係を考慮すると，SA 値の事後確率の算出は自明で無い．また，SA 数が増える毎に SA 値の組み合わせが指数的に増加し，全ての組み合わせが確率 β 以上となるように匿名化するためには，β の値を相当下げざるを得ない．このように複数の SA を扱う場合はいくつか課題がある．

6.4 複数回の匿名化データ開示

パーソナルデータの属性数が多くなる程一般に匿名化の度合いが高まり，有用性が低下してしまう．そこで，元のパーソナルデータの一部の属性を抽出して都度匿名化を行う方法が考えられる．例えば図 1 の例では，{ 性別，年収，好物 }，{ 年齢，年収 } の二つの属性の組に分け，各々を匿名化する事で，{ 性別，年齢，年収，好物 } を一括して匿名化するよりも有用性が高くなる可能性がある．このように複数回に分けて匿名化データを開示する場合には，属性の重複開示に注意する必要がある．前記の例では,「年収」が重複している．SA を重複開示する場合，SA 値の事後確率を利用出来る．例えば { 性別，年収，好物 } を $P(\alpha,\gamma)$-プライバシを満たすよう式 (5) に基づいて匿名化した時，年収の各 SA 値の事後確率が求まるため，これを { 年齢，年収 } について匿名化する際の年収の各 SA 値の事前確率に用いる．しかし式 (7) に基づいて匿名化した時の各 SA 値の事後確率の算出方法等，今後更なる検討が必要である．

7 その他のプライバシ指標

本節では，属性暴露のリスクに対して 3 節で挙げた以外の代表的なプライバシ指標を紹介し，本稿で提案した指標との差異や今後の展望について述べる．

3 節で述べたように，ℓ-多様性は帰納的 (c,ℓ)-多様性の他に二つの指標が提案されている．一つは**離散的 ℓ-多様性** (*distinct ℓ-diversity*) と呼ばれ，任意の EQI について ℓ 種類以上の SA 値が存在するかどうかを指標とする．p-センシティブ k-匿名性と本質的に等しく，$\ell = m$ (または $p = m$) とすればどの SA 値も存在する事になる．もう一つはエントロピー ℓ-多様性と呼ばれ，任意の EQI における SA 値のエントロピー $-\sum_u s_u \log(s_u)$ が $\log(\ell)$ 以上となるかどうかを指標とする．ここで s_u は EQI における SA 値 a_u の頻度の割合とする．離散的 ℓ-多様性における SA 値の条件を強めた指標と言える．当該指標を確率的な指標に拡張すれば，$P(\alpha,\gamma)$-プライバシとの組み合わせも可能と考えられる．

Li らは，属性暴露のリスクとして**歪み攻撃** (*skewness attack*) を挙げ，当該攻撃を考慮した指標として ***t*-近似性** (*t-closeness*) を提案した [14]．歪み攻撃は，ターゲットの EQI の SA 値の分布とレコード全体の SA 値の分布との差異を利用した攻撃であり，t-近似性は当該二つの分布の距離が一定以下であるかどうかを指標とする．ρ_1-to-ρ_2 プライバシ侵害に近い考え方と言えよう．

最後に，攻撃者の事前知識を仮定しないプライバシ指標として近年注目を集めている**差分プライバシ** (*differential privacy*)[2] を紹介する．差分プライバシは，対話型データベースにおいて「特定の個人のデータがデータベースに入っていてもいなくても開示される出力がほぼ変化しない」かどうかを指標とする．質的データからなるパーソナルデータは高次元の度数表と見

なせ，度数表において差分プライバシを満たす手法は Dwork によって提案されている [2]．また五十嵐らは [3] において，PRAM を用いて差分プライバシを満たせる事を示した．従って，$P(\alpha,\gamma)$-プライバシと差分プライバシの両方を満たすパラメータの決定も可能と考えられる．

8 まとめ

パーソナルデータ開示における属性暴露のプライバシリスクについて，直感的で分かり易い指標「$P(\alpha,\gamma)$-プライバシ」を定義し，撹乱的な手法である PRAM を用いて当該指標を満たす匿名化手法を提案した．$P(\alpha,\gamma)$-プライバシは，パーソナルデータに含まれるセンシティブな値に対する攻撃者の事前知識，及び匿名化データから，攻撃者が任意の個人のセンシティブな値を α を超える確率で推定出来ず，かつどの値も確率 γ 以上で存在する多様性を保証する．

公開データセットを用いて，提案手法を適用した匿名化データの有用性を評価した．特に再識別のプライバシ指標である Pk-匿名性との組み合わせについて考察し，Pk-匿名性を満たせば同時に $P(\alpha,\gamma)$-プライバシも満たす場合がある事を実験的に確認した．即ちこの場合は Pk-匿名性以上に有用性を損ねずに済む．

今後の課題として，元のパーソナルデータに複数のセンシティブな属性が含まれる場合，及び複数回の匿名化データを開示する事を考慮した指標の確立が挙げられる．t-近似性や差分プライバシ等の代表的な指標との組み合わせも今後の検討課題としたい．また今回は質的データを仮定したが，量的データを含む匿名化データについても検討予定である．

参考文献

[1] A. Machanavajjhala, J. Gehrke, D. Kiefer, and M. Venkitasubramanian, "ℓ-diversity: privacy beyond k-anonymity," ACM Trans. Knowl. Discov. Data 1 (1), 2007.

[2] C. Dwork, "Differential privacy," Proc. of ICALP (2), pp.1-12, 2006.

[3] 五十嵐大, 千田浩司, 高橋克巳, 「Differential Privacy の数理的解析」CSS2009 論文集，情報処理学会, 2009.

[4] L. Willenborg and T. de Waal, "Elements of statistical disclosure control," Springer, New York, 2001.

[5] 伊藤伸介，村田磨理子，高野正博,「ミクロデータにおける匿名化技法の適用可能性の検証 — 全国消費実態調査と家計調査を用いて —」統計研究彙報，第 71 号，pp.83-124, 2014 年 3 月.

[6] L. Sweeney, "k-anonymity: A model for protecting privacy," Int' l Journal on Uncertainty, Fuzziness and Knowledge-based Systems, Vol.10, No.5, pp.557-570, 2002.

[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」CSS2009 論文集，情報処理学会, 2009.

[8] R. Wong, J. Li, A. Fu, and K. Wang, "(α,k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing," Proc. of ACM SIGKDD 2006, pp.754-759, 2006.

[9] T.M. Truta and B. Vinay, "Privacy protection: p-sensitive k-anonymity property," Proc. of 22nd IEEE Int ' l Conf. on Data Engineering Workshops, 2006.

[10] 五十嵐大, 千田浩司, 高橋克巳,「$P\ell$-多様性 : 属性推定に対する再構築法のプライバシーの定量化」CSS2010 論文集，情報処理学会, 2010.

[11] B.-C. Chen, D. Kifer, K. LeFevre, and A. Machanavajjhala, "Privacy-preserving data publishing," Foundations and Trends(r) in Databases, October 9, 2009.

[12] A. Evfimievski, J. Gehrke, and R. Srikant, "Limiting privacy breaches in privacy preserving data mining," Proc. of PODS '03, pp.211-222, 2003.

[13] UCI Machine Learning Repository, Census Income Data Set, 1996, `https://archive.ics.uci.edu/ml/datasets/Census+Income`.

[14] N. Li and T. Li, "t-closeness: privacy beyond k-anonymity and ℓ-diversity," Proc. of IEEE Int'l Conf. on Data Engineering, 2007.