情報処理学会論文誌 Vol.56 No.12 2230–2243 (Dec. 2015)

安心できるプライバシ指標の調査

清 雄一[1,a)] 稲葉 緑[2] 大須賀 昭彦[1]

受付日 2015年3月9日, 採録日 2015年9月2日

概要：個人の属性（年齢や病名等）に関する情報データベースを他事業者と共有する場合，プライバシへの配慮が必要である．近年，プライバシを保護したままデータマイニングを行う試みがさかんに行われており，プライバシをどれだけ保護するかを決定する指標（プライバシ保護目的指標）が数多く提案されている．しかし，個人の感じ方に深く関わりを持つ指標であるにもかかわらず，プライバシ保護目的指標のパラメータの値によって，個人の感じ方がどのように変わるかを調査した例はこれまでなく，これらの指標が，本当にプライバシを計測できるかどうかについて明確になっていない．本研究ではまず，代表的なプライバシ保護目的指標を大きく5つのグループに分類した．次に個人の属性値を保護することを目的としている3グループを対象として各グループから1つずつプライバシ保護目的指標を選択し，それぞれプライバシ保護レベルを変動させた場合に，ユーザの感じ方がどのように変わるかを400人に対するアンケートを行って調査・分析した．分析の結果，プライバシ保護レベルを変動させても感じ方にほとんど影響を与えない場合があることが分かった．また，プライバシ保護レベルに依存せず，自分の属性値によって感じ方が大きく変わることが明らかになった．

キーワード：プライバシ保護目的指標，プライバシ保護レベル，アンケート調査

A Survey on Perception of Privacy Metrics

Yuichi Sei[1,a)] Midori Inaba[2] Akihiko Ohsuga[1]

Received: March 9, 2015, Accepted: September 2, 2015

Abstract: When a data holder wants to share databases that contain personal attributes, individual privacy needs to be considered. A lot of privacy metrics regarding anonymized databases of personal information have been proposed. Although privacy metrics are largely dependent on human factors, there are no studies that survey how the parameters of the privacy metrics effect on a person's way of thinking. Therefore, it is not clear whether or not the privacy metrics can surely measure privacy. In this study, we divide existing privacy metrics according to their characteristics into five groups. Then we select three groups where privacy metrics can protect attribute values directly, then we select a representative privacy metric from each group, and we conducted a survey with 400 persons to know how the parameters of them effect on a person's way of thinking. As a result of the survey, we know that the parameters of several privacy metrics do not effect on a person's way of thinking in some cases and we know that people have more to do with their sensitive values than the parameters of the privacy metrics.

Keywords: privacy metrics, privacy-preservation level, questionnaire

1. はじめに

近年，多くの組織が個人に関する情報を収集している．新しいサービス創出のために異なる事業者間で情報を共有する試みも行われている．しかし，秘匿性の高い情報を，個人を特定できるような状態のまま共有することは許されない．このため，匿名化に関する研究が数多く提案されて

[1] 電気通信大学大学院情報システム学研究科
Graduate School of Information Systems, The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[2] JR 東日本研究開発センター安全研究所
Safety Research Laboratory, East Japan Railway Company Saitama, Saitama 331–8513, Japan
[a)] sei@is.uec.ac.jp

いる [12], [13], [25].

本研究では，個人の属性（年齢，職業，病名等）に関する**生データ**を保有する**データ保有者**が存在していると想定する．このデータ保有者は，プライバシを保護するようデータを加工した後，データを利用したい業者に提供する．この業者を**データ利用者**と呼ぶ．また，プライバシを保護するよう加工されたデータを**匿名化データ**と呼ぶ．

ここで，以下の語句を導入する．

Definition1（プライバシ保護目的指標） 個人に関する情報を含んだデータに関し，プライバシがどれだけ保護されているかを測るために提案された指標を，プライバシ保護目的指標と定義する．

Definition2（プライバシ保護レベル） あるプライバシ保護目的指標 P において，P のパラメータを変動させることによって調整可能な，その指標の提案者が考えるプライバシを保護する度合いを，プライバシ保護レベルと定義する．

現在様々なプライバシ保護目的指標が提案されており，また，指標ごとにプライバシ保護レベルを調整するパラメータが用意されている．しかし，提案されているプライバシ保護目的指標が本当に「プライバシ保護を実現する指標」となっているかについてはほとんど議論されていない．ここでさらに，以下の語句を導入する．

Definition3（プライバシ保護実現指標） あるプライバシ保護目的指標 P におけるプライバシ保護レベルを上昇させると，「プライバシがより保護されている」と多くの人が感じるとき，P をプライバシ保護実現指標であると定義する．

プライバシ保護目的指標およびプライバシ保護レベルは，各指標の提案者がそのように主張するだけで成立する定義である．一方，プライバシ保護実現指標は，人々の感じ方に依存する定義である．

たとえば，ϵ-差分プライバシは，非負パラメータ ϵ の値を 0 に向かって減少させることによってプライバシ保護レベルが上昇する性質を持つプライバシ保護目的指標の 1 つであるが，ϵ の値を減少させると「プライバシがより保護されている」と多くの人が本当に感じるかどうかは明確になっていない．プライバシ保護データマイニングの分野では，与えられたプライバシ保護レベルを満たす範囲で，できるだけ情報量を保ったまま匿名化するアルゴリズムを提案することがほとんどである．しかし，ある状況においてプライバシ保護レベルを 0（まったく保護されていない）から 0 より大きい値に変動させても人々の感じ方が変化しないのであれば，少なくともその状況下では，そのプライバシ保護目的指標に基づく匿名化アルゴリズムを提案することの意義が損なわれてしまう．したがって，各プライバシ保護目的指標が，本当にプライバシ保護実現指標となっていることを確認することは重要である．

本研究では，代表的なプライバシ保護目的指標を 5 グループに分類し，その中から個人の属性値を保護することを目的としている 3 グループについて，それぞれから重要だと考えられるプライバシ保護目的指標を 1 つずつ抽出した．抽出したものは，l-多様性，ϵ-差分プライバシ，γ-amplification である．20 代〜60 代，男女別それぞれ 40 人，合計 400 人に対し，抽出した 3 つのプライバシ保護目的指標について，プライバシ保護レベルや，プライバシ保護レベルに依存しない状況を変動させながら，ユーザの感じ方がどのように変わるかについてアンケート調査を行った．アンケート調査の結果，プライバシ保護レベルを変動させても，感じ方にほとんど違いが生じない場合があることが分かった．

また，プライバシ保護レベルよりも，個人がどの属性値を持っているかということのほうが，感じ方に大きな影響を与えることが分かった．プライバシ保護データマイニングではたとえば，匿名化データを基にしてある病院の患者における年収の分布はどうなっているか？という分析を行う．このとき，年収が高い人の多くが，自身のデータが匿名化データに含まれることを許諾し，年収の低い人の多くが，自身のデータが匿名化データに含まれることを許諾しなかった場合，匿名化データから得られる年収の分布と，真の年収の分布が大きく乖離してしまうことになる．既存研究は暗黙的に，属性値によって，自身のデータが匿名化データに含まれることを許諾する率が変わらないことを前提としている．この前提が正しくない場合に，どのように分析を行えばよいかについて議論することが重要であることが本研究により明らかになった．

このように本研究は，ヒューマンファクタを考慮したプライバシ保護データマイニングにおける第一歩目の位置付けとなると考えている．

本論文の構成を示す．2 章において，既存のプライバシ保護目的指標を分類し，本研究で分析対象とする指標を選定する．3 章において本研究で行ったアンケートの概要を記す．4 章において，アンケートを行ううえで調整したプライバシ保護目的指標について説明する．アンケート結果を 5 章で述べ，6 章において考察する．最後に 7 章でまとめる．

2. プライバシ保護目的指標の分類と調査対象の抽出

2.1 プライバシ保護目的指標の分類

ほとんどの研究が，保護すべき属性と保護する必要のない属性が存在するという前提をおいている．本論文でもこの前提をおく．以下では，保護すべき属性を**センシティブ属性**と呼ぶ．

本研究においては，プライバシ保護目的指標を大きく 5 グループに分類した（**表 1**）．このうち，センシティブ属性

表 1 プライバシ保護目的指標の分類
Table 1 Classification of privacy metrics.

Group	Privacy metrics
Group 1	l-Diversity [16], (α, k)-Anonymity [7], (X, Y)-Privacy [24], (k, e)-Anonymity [30], (ϵ, m)-Anonymity [14], m-Invariance [27]
Group 2	t-Closeness [15], ϵ-Differential Privacy [8], (α, β)-Distributional Privacy [3]
Group 3	γ-amplification [10], ρ_1-to-ρ_2 Privacy [10], (c, t)-Isolation [5], (d, γ)-Privacy [20]
Group 4	k-Anonymity [21], Pk-Anonymity [32], (w, k)-Anonymity [34]
Group 5	δ-Presence [18]

値を保護の直接の対象としている Group 1〜3 に属するプライバシ保護目的指標を本研究の調査対象とする．Group 4〜5 に属するプライバシ保護目的指標も間接的にはセンシティブ属性値を想定した指標であると考えられるが，これらの指標を本研究のスコープ外とした．具体的には以下のとおりである．Group 4 のプライバシ保護目的指標は多くの場合，個人のセンシティブ属性値を保護するために利用されているものであるが，その保護については何ら保証していない．この問題点を解決するために Group 1 に属する l-多様性等が提案されている．Group 5 のプライバシ保護目的指標も同様に，センシティブ属性値を直接の保護対象としていない．Group 4 や 5 のように，匿名化データにおける各個人のセンシティブ属性値に対して直接的には何の保証もしておらず，間接的な保護を目的としているプライバシ保護目的指標に関する調査は，将来課題とする．

以下に，各グループの要点を示す．

Group 1) 匿名化データを見ることによって客観的に得られる，ある個人のセンシティブ属性値に関する知識の正確さを測る指標

Group 2) データ保有者が保有する生データのセンシティブ属性値の相対度数分布から客観的に得られる知識と，匿名化データを見ることによって客観的に得られるある個人のセンシティブ属性値に関する知識との差を測る指標

Group 3) ある個人のセンシティブ属性値に関するデータ利用者の事前知識と，データ利用者が匿名化データを見ることによって更新されるその個人のセンシティブ属性値に関する事後知識との差の大きさを測る指標

Group 4) 匿名化データを見ることによって客観的に得られる，匿名化データのレコードのうちある個人のレコードがどれであるかということに関する知識の正確さを測る指標

Group 5) ある指定されたデータベースと匿名化データを見ることによって客観的に得られる，この匿名化データにある個人の情報が含まれている確率に関する知識の正確さを測る指標

攻撃モデルによる分類 [11] や，基本的なプライバシ保護目的指標である k-匿名性との関係による分類 [22]，入力プライバシと出力プライバシによる分類 [33] に基づくものはあるが，各プライバシ保護目的指標がそもそも何を測ろうとしているか，という視点での分類はこれまで行われておらず，この視点で分類することは本研究の貢献の 1 つである．たとえば ϵ-差分プライバシも，個人のセンシティブ属性値を保護することを目的としているが，高いプライバシ保護レベルを設定したとしても，センシティブ属性値がほぼ確実に判明することもありうる．

このように，プライバシを保護するといっても，センシティブ属性値が高い精度で判明するのを防ぐことを対象としていないプライバシ保護目的指標も多数存在するため，何を対象として何を測る指標であるのかの視点で分類・整理することは，プライバシ保護目的指標を実際に利用する際には重要である．

以下に，各グループの考え方がどのように異なるかを直観的に把握するための例を示す．

Example1 「年収が 10 万円以上か？」というセンシティブ属性があったとする．これは多くの人が「YES」となることは明らかであり，実際に，あるデータ保有者が保有するデータベースでもそうであったとする（しかしながら当然，「NO」となる人も存在しており，保護すべき属性であると考えられる）．しかし，ほぼ確実に「YES」であるとデータ利用者に判明すると，プライバシが保護されていないと考えるのが Group 1 のプライバシ保護目的指標である．一方 Group 2 や Group 3 では，ほぼ確実に「YES」だとデータ利用者に判明しても，それをプライバシが保護されていないとは見なさない．

Example2 ある会社の 9 割の社員の年収が 3,000 万円であったとする．しかしこの情報は一般には公開されておらず，データ利用者も知識を持っていない．しかし，業種や社員数，国内の平均年収分布等の情報から，データ利用者はその会社の平均年収を 400 万円だと推測していたとする．このとき，事前知識は 400 万円となる．ここで，Alex が当該会社で働いていることをデータ利用者は知っていたとする．この会社の年収を匿名化した後のデータベースから，その会社の平均年収も Alex の年収も高い精度でほぼ 3,000 万円であることがデータ利用者に判明したとする．年収をセンシティブ属性と考えると，Group 3 ではプライバシが保護されていないと考える．なぜなら，事前知識と事後知識の差が大きいためである．Group 2 では，プライ

表 2 生データ
Table 2 Raw data.

Name	Age	Job	Disease
Alex	41	Artist	HIV
Becky	41	Writer	Hay fever
Carl	50	Artist	Asthma
Diana	51	Nurse	Tight shoulders

バシが保護されていないとは考えない．なぜなら，データベースにおけるセンシティブ属性値の相対度数分布から客観的に得られる知識と，Alex のセンシティブ属性値に関する知識がほぼ同じであるからである．一方，正確な値が判明しているため，Group 1 ではプライバシが保護されていないと考える．

2.2 本研究で調査対象とする指標

本研究では，Group 1 から l-多様性，Group 2 から ϵ-差分プライバシ，Group 3 から γ-amplification を選定し，詳細な分析を行うこととした．それぞれの指標を選定した理由は，多くの研究論文が発表されているためである．

また，プライバシ保護目的指標として提案はされていないが，近年指摘されている「濡れ衣問題」についてもあわせて分析を行う．濡れ衣問題とは，匿名化後のデータを見ることによって，ある個人がある属性値を持っていると高い確信度を持って「誤って」判断される問題のことである．たとえば，Alex はある時刻に A 大学にいたとする．しかし，匿名化後のデータを見ることによって，Alex は確率 0.9 で B 消費者金融店舗にいて，確率 0.1 で A 大学にいたと客観的に判断されたとする．このとき，Alex は本来は消費者金融店舗にいたわけではないが，濡れ衣として，そこにいたと誤って判断されてしまうことになる．このとき，消費者金融店舗にいたと考えられる確率を「濡れ衣問題に係る誤った確信度」と本論文では呼ぶことにする．

以下，各プライバシ保護目的指標を説明するうえで，共通の例を利用する．データ保有者が保有する生データを**表 2** に示す．データ利用者は Alex がこのデータに含まれていることを知っている，と想定する．データ利用者に生データが提供されると，Alex が HIV であることを一意に特定できてしまう．名前を削除すると（**表 3**），Alex は上 4 レコードのいずれかに存在することしか分からない．したがって，HIV，Hay fever（花粉症），Asthma（喘息），Tight shoulders（肩こり）である確率がそれぞれ 25%であることのみが分かる．

しかしもしデータ利用者が Alex の年齢（41 歳）と職業（Artist）を知っている場合，名前を削除したデータから，Alex が HIV である確率が 100%であるということが分かる．なぜなら，年齢が 41 歳でありかつ職業が Artist であるレコードはただ 1 つしかないためである．

表 3 識別子（Name）を削除したデータ
Table 3 Data without its explicit identifier (Name).

Age	Job	Disease
41	Artist	HIV
41	Writer	Hay fever
50	Artist	Asthma
51	Nurse	Tight shoulders

表 4 l-多様性による匿名化例（$l = 2$）
Table 4 Anonymization ex. of l-Diversity ($l = 2$).

Age	Job	Disease
41	*	HIV
41	*	Hay fever
50-51	Artist	Asthma
50-51	Artist	Tight shoulders

2.2.1 *l*-多様性

Machanavajjhala らが提案した l-多様性（l-Diversity）[16] は，k-匿名性 [21], [23] を拡張した指標である．l-多様性の指標には，Distinct l-多様性，Entropy l-多様性，Recursive (c, l)-多様性等，いくつかのバリエーションがあるが，本論文では Entropy l-多様性を採用する．Entropy l-多様性は，これらの中でも強力かつ保守的な指標である [15]．本論文では，Entropy l-多様性を単に l-多様性と記述する．

保護する必要のない属性のうち，他の公開情報等と組み合わせることによって個人を特定できる属性を準識別子（QID: Quasi-Identifier）と呼ぶ．居住地の郵便番号，年齢，職業等を QID と考えることが多い．この QID の値がすべて同じレコードの集合を QID グループと呼ぶ．またセンシティブ属性値としてとりうる値の集合を S とおく．ある QID グループ q^* において，あるセンシティブ属性値 $s \in S$ が出現する回数を $n_{(q^*,s)}$ とおく．

このとき l-多様性は以下のように定義される．

Definition4（*l*-多様性） データベース D の各 QID グループにおいて，

$$-\sum_{s \in S} p_{(q^*,s)} \log(p_{(q^*,s)}) \geq \log(l) \quad \text{where } p_{(q^*,s)} = \frac{n_{(q^*,s)}}{\sum_{s' \in S} n_{(q^*,s')}} \tag{1}$$

が満たされるとき，D は l-多様性を満たす．

パラメータ l の値が増加するほど，プライバシ保護レベルは向上する．

l-多様性に基づき，パラメータを $l = 2$ に設定した場合における匿名化例を**表 4** に示す．このとき，データ利用者が Alex の年齢（41 歳）および職業（Artist）を知っていたとしても，Alex に相当するレコードが 1 番目のレコードか 2 番目のレコードか分からない．したがって，Alex の病名として HIV と Hay fever の 2 種類がありうるため，表 3 と比べて表 4 は，各個人の病名を保護することができている．

2.2.2 ϵ-差分プライバシ

ϵ-差分プライバシ（ϵ-Differential Privacy）[8] という指標が近年特にさかんに研究されている．この指標は最も強力なプライバシ定義の 1 つだといわれることもあり [19]，直観的には，ある 1 人の個人がいてもいなくても匿名化の出力にほとんど差がない，ということを要求する．

以下に ϵ-差分プライバシを定義する．

Definition5（ϵ-差分プライバシ） たかだか 1 レコードのみ異なるデータベース D_1 および D_2 を考える．ランダム機構 $\mathcal{R}$ を確率的アルゴリズムとする．また，$Range(\mathcal{R})$ を，$\mathcal{R}$ が出力する可能性のある値の集合とし，$S \subseteq Range(\mathcal{R})$ とすると，

$$\Pr[\mathcal{R}(D_1) \in S] \leq e^{\epsilon} \Pr[\mathcal{R}(D_2) \in S] \tag{2}$$

が満たされるとき，ランダム機構 $\mathcal{R}$ は ϵ-差分プライバシを与える．

パラメータ ϵ の値が増加するほど，プライバシ保護レベルは低下する．

文献 [9] ではラプラス分布に従って生成されたノイズを加算することによって ϵ-差分プライバシを実現する手法が提案されており，多くの研究がこの Laplace mechanism を採用している．Laplace mechanism は以下のように実現される．

Definition6（Laplace Mechanism） たかだか 1 レコードのみ異なるデータベース D_1 および D_2 を考える．d を非負整数とし，関数 $f : \mathcal{D} \rightarrow \mathbb{R}^d$ において，すべての D_1 および D_2 について，

$$\Delta f = \max_{D_1, D_2} ||f(D_1) - f(D_2)||_1 \tag{3}$$

が成り立つとき，この Δf を f の global sensitivity と定義する．このとき，データベース D に対して $f(D) + RandomValue(Lap(0, \Delta f/\epsilon))$ を返すランダム機構 $\mathcal{R}$ は，ϵ-差分プライバシを実現する．

ここで $Lap(0, \Delta f/\epsilon)$ は，平均 0，尺度指数 σ が $\Delta f/\epsilon$ であるラプラス分布を表し，$RandomValue$ は引数の確率分布から生成した乱数を返す関数である．また，集計値である場合は，$\Delta f = 1$ である [1] から $\sigma = 1/\epsilon$ となる．

ϵ-差分プライバシの指標に基づき，プライバシ保護レベルを $\epsilon = 1$ に設定した場合における匿名化例を**表 5** に示す[*1]．年齢・職業と病名の各組合せについて，それぞれ何人がデータに含まれているかを「# of persons」の列に設定している．ここで，ϵ の値の大きさに応じて非決定的に計算される誤差を加算している．たとえば，41 歳，Artist で HIV の個人は 1 人いるが，誤差 0.8 が加算されて，表 5 には 1.8 と設定されている．一方，41 歳，Artist で Hay fever の個人は 1 人いるが，誤差 −0.1 が加算されて，表 5 には 0.9 と設定されている．

表 5 ϵ-差分プライバシによる匿名化例（$\epsilon = 1$）
Table 5 Anonymization ex. of ϵ-Differential Privacy ($\epsilon = 1$).

Age×Job	Disease	# of persons
41×Artist	HIV	1.8
41×Artist	Hay fever	0.9
41×Artist	Asthma	0.3
41×Artist	Tight shoulders	0.9
...	...	...

さらに，ϵ-差分プライバシが，表 1 において Group 1 に属さない（ϵ-差分プライバシにおいて高いプライバシ保護レベルで匿名化されても，個人のセンシティブ属性値が高い確率で特定される状況がありうる）例を以下に示す．あるデータベース D には，年収の分布が登録されている．年収は，「100 万円未満」「100 万円以上 200 万円未満」「200 万円以上 300 万円未満」...「1000 万円以上」のようにカテゴリ分けされている．データベース D には全部で 10,000 人の年収が登録されており，そのうち 9,600 人が「300 万円以上 400 万円未満」であったとする．多くの研究が，高いプライバシ保護レベルを実現する値として $\epsilon = 0.01$ から $\epsilon = 0.5$ 程度に設定している [1], [28], [29], [31]．ここではよりプライバシ保護レベルが高い方の値である $\epsilon = 0.01$ を考える．このとき，「300 万円以上 400 万円未満」の値である「9,600 人」を匿名化すると，およそ 95%の確率で 9,900 人から 9,300 人のいずれかの値をとる[*2]．つまりデータ利用者は，データベース D に含まれている各個人の年収はおよそ 9 割以上の確率で，「300 万円以上 400 万円未満」であると判断することが可能となる．

このように，匿名化対象となるデータベース D に含まれるセンシティブ属性値が偏っている場合は，各個人のセンシティブ属性値は高い精度で判明する．しかしながら，ϵ-差分プライバシを利用し，かつ ϵ の値や匿名化対象のレコード数が上記例のような状況においては，たとえ偶然だとしても，D における他の多数の個人も同じ値を保有しているのだから，センシティブ属性値が高い精度で判明しても問題ではない，ということになる．

2.2.3 γ-amplification

データ利用者における事前知識と事後知識の差に着目した指標として，ρ_1-to-ρ_2 プライバシ [10] が提案されている．ここでいう事前知識および事後知識は，あるターゲットとなる個人のセンシティブ属性値に関する知識のことを指す．

Definition7（ρ_1-to-ρ_2 プライバシ） データ利用者が認識している，ある個人があるセンシティブ属性値 Q を持

[*1] ϵ-差分プライバシは，データ利用者がデータ保有者にクエリを投げた際に誤差を与えて回答するという，インタラクティブなモデルが想定されることが多い．しかし，本論文では，他の指標との比較のため，匿名化したデータをデータ利用者に提供するシナリオに統一して説明する．

[*2] 確率分布を引数にとってその確率密度関数を返す関数を PDF とおくと，$\int_{x=-300}^{300} PDF(Lap(0, 1/0.01)) \approx 0.95$ となる．

つ確率（事前確率）と，このデータ利用者が匿名化データを見た後に更新される，当該個人が当該センシティブ属性値 Q を持つ確率（事後確率）を考える．事前確率が ρ_1 以下である場合に，事後確率が ρ_2 以上となるとき，upward ρ_1-to-ρ_2 プライバシが保護されていない，と定義される．逆に，事前確率が ρ_2 以上である場合に，事後確率が ρ_1 以下となるとき，downward ρ_2-to-ρ_1 プライバシが保護されていないと定義され，upward ρ_1-to-ρ_2 プライバシおよび downward ρ_2-to-ρ_1 プライバシの両方が保護されているとき，ρ_1-to-ρ_2 プライバシが保護されていると定義される．

たとえば病名のデータでは，日本人の有病率（ある一時点の患者数を観察人口で除した値）を事前確率と考えることができる．仮に，HIV の有病率を 0.01%とおくと，任意の人が HIV にかかっているかどうかの事前確率は 0.01%であると考えることができる．一方，表 3 を見ると，Alex が HIV にかかっている確率は 25%となるため，0.0002-to-0.3 プライバシは満たされるが，0.0001-to-0.2 プライバシは満たされない，という状況となる．事前確率が 0.1%のときに事後確率をどこまで許容するか，事前確率が 1%のときに事後確率をどこまで許容するか，というように，事前確率の大きさごとに許容できる事後確率を決定する必要があり，プライバシ保護レベルの設定および管理が煩雑となってしまう．そこで，0 より大きい値を持つパラメータ γ を用意し，事前知識がとりうる値それぞれについて事後確率を設定しなくても，事前知識と事後知識の差が大きくなりすぎることがないよう制約を設けることができる．

γ-amplification は以下のように定義される．

Definition8（γ-amplification） データ利用者が認識している，ある個人があるセンシティブ属性値 Q を持つ確率（事前確率）を ρ_1 とおく．このデータ利用者が匿名化データを見た後に更新される，当該個人が当該センシティブ属性値 Q を持つ確率（事後確率）を ρ_2 とおく．以下の式が満たされるとき，γ-amplification が満たされる．

$$\gamma \leq \frac{\rho_2}{\rho_1} \times \frac{1-\rho_1}{1-\rho_2} \tag{4}$$

パラメータ γ の値が増加するほど，プライバシ保護レベルは低下する．

たとえば，ある個人がセンシティブ属性値 Q を持つ確率が，データ利用者の事前知識として 5%であったとする．この場合，$\gamma = 10$ であると，データ利用者の事後知識において，当該個人がセンシティブ属性値 Q を持つ確率は最大約 35%に抑えられる．一方，$\gamma = 100$ であると，データ利用者の事後知識において当該個人がセンシティブ属性値 Q を持つ確率は最大約 84%となる．

γ-amplification の指標に基づき，プライバシ保護レベルを $\gamma = 101$ に設定した場合における匿名化例を**表 6** に示す．データ利用者の事前知識として，HIV，Hay fever，Asthma，Tight shoulders の日本人における有病率がそれぞれ 0.01%，30%，5%，30%であると認識しているものとする．また，生データに含まれる患者の有病率も，この有病率と等しいと想定しているものとする．表 6 を見ると，HIV である確率が 1%となっており，データ利用者の事前知識である 0.01%との差が 100 倍ある．定義 8 より，γ の値が 101 のとき，この差はちょうど許容されている．同様に，他の病気についても，$\gamma = 101$ のとき，この事前知識と事後知識の差は許容されている計算になる．

表 6 γ-amplificaiton による匿名化例（$\gamma = 101$）
Table 6 Anonymization ex. of γ-Amplification ($\gamma = 101$).

Age×Job	Disease	Probabiliby
41×Artist	HIV	1%
41×Artist	Hay fever	25%
41×Artist	Asthma	30%
41×Artist	Tight shoulders	20%
41×Artist	...	...
...	...	...

3. アンケート概要

集計値（どの属性値（群）を持った人が何人存在するか）を，データ保有者がデータ利用者に提供するシナリオを想定した．集計値の計算は最も基本的な分析の 1 つであり，プライバシ保護データマイニングにおける多くの既存研究がアプリケーション例として取り上げているためである [1], [2], [6], [26], [29].

また各個人は，自分のデータを匿名化データに含めてよいかどうかを選択することができることとした．これは，本人の求めに応じて個人データを第三者に提供することを停止することができる仕組みが用意されることが想定されるためである．匿名化データに含めてよいかどうかについて，「まったく問題なく同意できる」「多少は嫌だが同意できる」「かなり嫌だが同意できる」「かなり悩ましいが同意できない」「多少は悩ましいが同意できない」「まったく同意できない」の 6 つの選択肢から選択させるようにした．

プライバシ保護データマイニングの多くの研究が，病名を対象とした匿名化を例にあげていることから，アンケート回答者が病院に通っており，通院している人の年齢とその病名を，匿名化したうえで地方自治体に提供するというシナリオを作成した．

プライバシ保護レベルが一定である場合に状況によって個人の感じ方が変わるか，また，プライバシ保護レベルを変動させた場合に想定どおりに個人の感じ方が変わるかどうかを調査するため，2 つのプライバシ保護目的指標におけるプライバシ保護レベルを固定して残り 1 つのプライバシ保護レベルを変動させたり，3 つすべてのプライバシ保護レベルを固定してプライバシ保護レベルに依存しない状況を変動させたりして，アンケートの設問を作成した．

20 代～60 代，男女それぞれ 40 人ずつ，計 400 人に対し

表 7 アンケート説明文
Table 7 Description of the questionnaire.

全国の地方自治体（市町村）には、地域医療データシステムを設立する動きがあります。このシステムには、住民が治療している病気や症状の傾向などについての情報が集められています。自治体はこのような情報を把握し、どの病気を治療する施設や医師団を自治体内に充実させればよいか、医療機関と介護施設との連携を強化するためにどのような支援をすればよいか、などの問題に効果的・効率的に取り組むことができると考えています。
あなたが住むところの自治体でも、外部機関に委託しつつ、地域医療データシステムの整備を進めています。このデータシステムには既に、あなたの自治体内に住む全住民の「名前」、「現住所」、「年齢」、「これまでに通院したことがある病院の名前」に関する情報が入っています。
あなたが住むところの自治体は、さらにこのデータシステムを充実させるため、自治体の中に存在する各病院に対して、「通院している人の年齢と、その病名」に関するデータ提供への協力を求めています。協力する各病院は、以下のような形式で自治体にデータを提供します。
（例）
15 歳の通院患者数：150 人
上の 15 歳の 150 人分のデータのうち、風邪で通院した患者数：99〜101 人
上の 15 歳の 150 人分のデータのうち、風邪以外の病気で通院した患者数：49〜51 人

あなたが通っている地元の病院 A にも、自治体は上記のようなデータ提供への協力を求めてきました。病院 A は自治体に協力するつもりです。
今日、あなたが病院 A に行ったところ、「あなたのデータを病院 A から自治体に提供するデータのうちの 1 人分として入れてもいいかどうか？」と聞かれました。あなたが同意すれば、病院 A から自治体に提供される「あなたと同じ年齢で病院 A に通院している患者数」や、「あなたと同じ病気で病院 A に通院している患者数」などのデータの 1 人分に、あなたのデータが入ることになります。
ただ、あなたはデータ提供に同意しないこともできます。あなたが同意しなければ、病院 A は、あなたの分のデータが含まれない統計データを自治体に提供することになります。
上の文をよく読んでいただけたでしょうか？文中の「あなた」が置かれた立場をよく理解できた、と思った人はアンケートの質問に進んでください。

表 8 設問の設定（BA は喘息，MS は多発性硬化症，HF は花粉症，MH は偏頭痛を表す）
Table 8 Setting of items.

設問番号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
l の値	0.88	0.88	0.88	0.64	0.88	1.22	0.64	0.88	0.92	1.22	1.22	1.22	1.60	1.22	0.64
ϵ の値	∞	∞	∞	∞	∞	∞	∞	6.0	12.0	12.0	12.0	12.0	12.0	2.0	2.0
γ の値	345	4.03	345	39996	345	9999	39996	345	9354	9354	17.77	2.18	9354	9999	39996
回答者の病名	HIV	BA	MS	HF	MH	HIV	HIV	HIV	HIV	HIV	MH	HF	HIV	HIV	HIV

てアンケート調査を行った．アンケート回答者に提示したアンケート説明文を**表 7** に示す．

各設問における，具体的な各プライバシ保護目的指標のプライバシ保護レベルの値と，回答者個人の属性値を整理したものを**表 8** に示す．また，各調査目的と設問との関係を**表 9** に示す．プライバシ保護レベルを上昇させると「プライバシがより保護されている」と感じる人が増加することが期待されるが，本当に既存のプライバシ保護目的指標が，そのような特徴を持つかどうかを調査することが本研究の主な目的である．したがって比較検討すべき点として，表 9 に示すとおり，ϵ-差分プライバシにおける ϵ の値，γ-amplification における γ の値，l-多様性における l の値，それぞれの値を変動させたときに，回答結果にどのような違いが出るかを調査する．それぞれ表 9 の設問集合の列に，どの設問を見ることでこの調査が可能であるかを示している．各設問における各指標のパラメータ値は表 8 に示しているとおりである．また，回答者個人の病名が回答結果に大きな影響を与える可能性があると考えられるため，回答者個人の属性値が与える影響も調査する．さらに，

表 9 調査目的と設問の関係
Table 9 Relationship between purpose and items.

調査目的 （以下が回答に与える影響を調査）	設問集合
回答者個人の属性値	{1,3,5}, {4,7}
l-多様性における l の値	{1,6}, {6,8}, {9,10,13}
ϵ-差分プライバシにおける ϵ の値	{1,8}, {6,10,14}, {7,15}
γ-amplification における γ の値	{1,7}, {2,3}, {10,11,12}
濡れ衣問題に係る誤った確信度	{4,7}

2.2 節で紹介した濡れ衣問題についても近年問題であると指摘されていることから，今回の調査観点に含めた．

アンケートの各設問を**表 10** および**表 11** に示す．アンケート調査においては，設問を表示する順序がアンケート結果に与える影響を低減させるために，1〜7 をセット A，8〜15 をセット B とし，セット A 内，セット B 内でそれぞれアンケート回答者に見せる設問の順序をローテーションして表示した．また，半分の回答者にはセット A を先に見せ，残り半分の回答者にはセット B を先に見せた．

表 10 アンケート設問（1/2）
Table 10 Items of the questionnaire (1/2).

設問 1 あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ） あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、HIV にかかっている患者数：1 人 上の 30 人分のデータの中で、偏頭痛にかかっている患者数：9 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：19 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：1 人 –
設問 2 あなたがかかっている病気の名前： 喘息 あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、喘息にかかっている患者数：1 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：19 人 上の 30 人分のデータの中で、偏頭痛にかかっている患者数：9 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：1 人 –
設問 3 あなたがかかっている病気の名前： 多発性硬化症 あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：1 人 上の 30 人分のデータの中で、偏頭痛にかかっている患者数：9 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：19 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：1 人 –
設問 4 あなたがかかっている病気の名前： 花粉症 あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：3 人 上の 30 人分のデータの中で、HIV にかかっている患者数：24 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：3 人 –
設問 5 あなたがかかっている病気の名前： 偏頭痛 あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、偏頭痛にかかっている患者数：9 人 上の 30 人分のデータの中で、HIV にかかっている患者数：1 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：19 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：1 人 –
設問 6 あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ） あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、HIV にかかっている患者数：15 人 上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：6 人 上の 30 人分のデータの中で、白血病にかかっている患者数：6 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：3 人 –
設問 7 あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ） あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、HIV にかかっている患者数：24 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：3 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：3 人 –
設問 8 あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ） あなたが同意した場合に、自治体に提供される統計データ – あなたと同じ年齢の患者数：30 人 上の 30 人分のデータの中で、HIV にかかっている患者数：0〜2 人 上の 30 人分のデータの中で、偏頭痛にかかっている患者数：8〜10 人 上の 30 人分のデータの中で、花粉症にかかっている患者数：18〜20 人 上の 30 人分のデータの中で、その他の病気にかかっている患者数：0〜2 人 –

表 11 アンケート設問（2/2）
Table 11 Items of the questionnaire (2/2).

設問 9
あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ）
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、HIV にかかっている患者数：14〜15 人
上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：13〜14 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜3 人
–

設問 10
あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ）
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、HIV にかかっている患者数：14〜15 人
上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：6〜7 人
上の 30 人分のデータの中で、白血病にかかっている患者数：6〜7 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜3 人
–

設問 11
あなたがかかっている病気の名前： 偏頭痛
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、偏頭痛にかかっている患者数：14〜15 人
上の 30 人分のデータの中で、喘息にかかっている患者数：6〜7 人
上の 30 人分のデータの中で、食物アレルギーにかかっている患者数：6〜7 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜3 人
–

設問 12
あなたがかかっている病気の名前： 花粉症
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、花粉症にかかっている患者数：14〜15 人
上の 30 人分のデータの中で、腰痛にかかっている患者数：6〜7 人
上の 30 人分のデータの中で、肩こりにかかっている患者数：6〜7 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜3 人
–

設問 13
あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ）
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、HIV にかかっている患者数：14〜15 人
上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：2〜3 人
上の 30 人分のデータの中で、白血病にかかっている患者数：2〜3 人
上の 30 人分のデータの中で、結核にかかっている患者数：2〜3 人
上の 30 人分のデータの中で、もやもや病にかかっている患者数：2〜3 人
上の 30 人分のデータの中で、メニエール病にかかっている患者数：2〜3 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜3 人
–

設問 14
あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ）
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、HIV にかかっている患者数：12〜18 人
上の 30 人分のデータの中で、多発性硬化症にかかっている患者数：3〜9 人
上の 30 人分のデータの中で、白血病にかかっている患者数：3〜9 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：0〜6 人
–

設問 15
あなたがかかっている病気の名前： 後天性免疫不全症候群（通称、HIV およびエイズ）
あなたが同意した場合に、自治体に提供される統計データ
–
あなたと同じ年齢の患者数：30 人
上の 30 人分のデータの中で、HIV にかかっている患者数：23〜25 人
上の 30 人分のデータの中で、花粉症にかかっている患者数：2〜4 人
上の 30 人分のデータの中で、その他の病気にかかっている患者数：2〜4 人
–

4. プライバシ保護目的指標ごとの調整

ϵ-差分プライバシでは，0 より大きい値を持つ ϵ の値をどのように変えても，その値が ∞ でない限りは，表 5 のように匿名化される可能性がある．しかし，ϵ の値によってこのように匿名化される確率が異なる．匿名化された結果だけをアンケート回答者に見せて，それがどういう意味を持つかを数学的に説明することは困難であるため，4.1 節に示すように工夫して提示した．

また，γ-amplification ではデータ利用者の事前知識を明確にする必要がある．今回は病名であるため，日本における有病率を事前に調べておき，それを事前知識とした．詳細を 4.2 節に示す．

4.1 ϵ-差分プライバシ

本来は，表 5 に示したように，非決定的に求められた誤差を真の値に追加する．ここで，誤差は 0 から $\pm\infty$ までありうる．本来はアンケート回答者に確率分布の概念を理解してもらうことが適切である．しかし，実際にそれを行うのは困難であり，理解が容易となるように，以下の工夫を行った．

真の値が v であるとする．パラメータ ϵ が与えられた場合，平均 0，尺度母数 $\Delta f/\epsilon$ であるラプラス分布に基づいて計算される値を追加することになる．匿名化後の値 v^* は

$$v^* = v + RandomValue(Lap(0, \Delta f/\epsilon)) \quad (5)$$

となる．

$\Delta f = 1$ であるとき，およそ 95%の確率で匿名化後の値は $v \pm 2.996/\epsilon$ の範囲内の値となる．そのうえ，匿名化データを受け取ったデータ利用者にとっては，加えられる誤差の値が何であるかは分からない．データ利用者にとっては，ϵ-差分プライバシに基づいて匿名化された値が v^* であることが分かったとき，真の値 v は，およそ 95%の確率で $v^* \pm 2.996/\epsilon$ の範囲に収まっているということが分かる．

一方で，信頼区間を設定した検定では，95%信頼区間をおいているものが多い．

本論文ではこの分析に基づき，パラメータ ϵ が与えられたとき，ϵ-差分プライバシに基づいて匿名化を行った値 v^* は，$v \pm 3 \times 2/\epsilon$ の範囲のいずれかの値をとる（$\pm 3 \times 2/\epsilon$ の誤差を与える）と見なしてアンケートを行った．

なお集計値に対して差分プライバシを適用する手法は他にも提案されている．たとえば Acs ら [1] は，集計値に対してフーリエ変換をまず実行し，その結果に対して Exponential mechanism [17] を適用することで，差分プライバシを実現している．同じプライバシ保護目的指標・同じプライバシ保護レベルを設定した場合，本研究で採用した Laplace mechanism よりも，集計値に与える誤差が小さくなり，結果としてデータ利用者の有効性が向上する．Acs ら以外にも多数のアルゴリズムが提案されているが，本論文では，プライバシ保護目的指標・プライバシ保護レベルと状況の差異によってアンケート回答者の感じ方がどう変わるかについて研究を行うことに重点をおき，同じプライバシ保護目的指標を採用しているがアルゴリズムが違う場合にアンケート回答者の感じ方がどう変わるかについては将来課題とする．

4.2 γ-amplification

有病率が低い病名の集合（HIV，多発性硬化症，白血病，結核，もやもや病，メニエール），中程度の集合（偏頭痛，喘息，食物アレルギー），高い集合（花粉症，肩こり，腰痛）に分けて，それぞれ事前確率が低い，中程度，高いものとして取り扱った．事前に広く文献調査を行い，各集合内の病気における有病率をおおむね一定に設定している．

5. アンケート結果

アンケート結果を**図 1** に示す．

「まったく問題なく同意」の割合を**許諾率**と呼ぶことにする．

本章ではまず，アンケート対象者の病名を変えたときに，どのように許諾率が変動するかについて分析を行う．次に，各プライバシ保護レベルが許諾率に与える影響を分析する．最後に，濡れ衣問題について議論を行う．

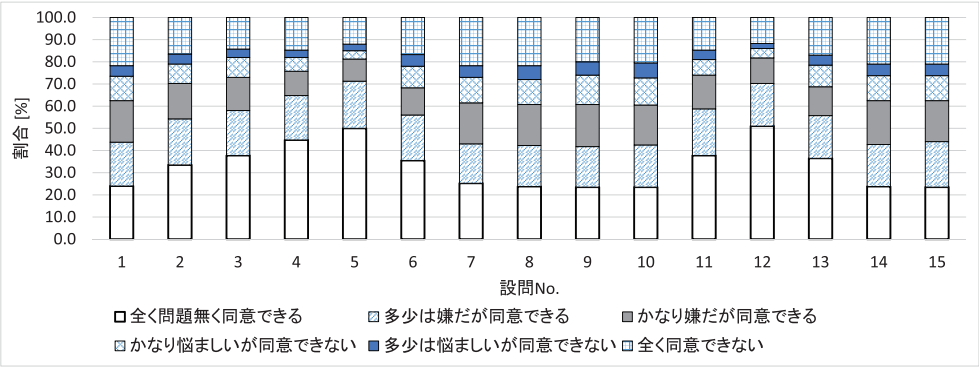


図 1 アンケート結果
Fig. 1 Results of the questionnaire.

5.1 自分の病名の影響

まず，アンケート対象者の病名を変えたときに，どのように許諾率が変動するのかについて分析を行った．設問 1，3，5 の集合は，3 つのプライバシ保護レベルを一定にし，アンケート対象者の病名のみを変えている．設問 4，7 の集合も同様である．結果を**図 2** に示す．

図 2 (a) は設問 1，3，5 についての結果を表している．いずれの指標もプライバシ保護レベルを変えていないことにより，アンケート対象者の許諾率がこれらの設問で変わらないことが期待された．しかしながら許諾率は 24.0%，37.8%，50.0%に増加しており（カイ二乗検定により有意差が認められた（$p < 0.005$））．自分のセンシティブ属性値が何であるかということが，個人の感じ方に大きな影響を与えていると考えられる．図 2 (b) は設問 4，7 についての結果を表している．これらの設問もプライバシ保護レベルを変えていないが，許諾率は 25.3%から 44.8%に増加している（カイ二乗検定により有意差が認められた（$p < 0.005$））．

5.2 各指標のプライバシ保護レベルの影響

各指標に関する分析結果を**図 3** に示す．横軸については，右側にいくほどプライバシ保護レベルが高くなるよう設定している．

5.2.1 l-多様性

l-多様性に関する分析結果を図 3 (a) に示す．

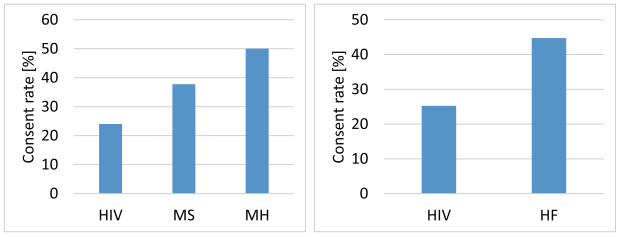
設問 9，設問 10，設問 13 は，ϵ-差分プライバシと γ-amplification のプライバシ保護レベルを一定にし，自分の病名も一定にし，l-多様性のパラメータ l を増加させた（プライバシ保護レベルを向上させた）．許諾率は 23.5%，23.5%，36.5%の順に増加しており，l の値が想定どおり許諾率に影響を与えることが確認できた（設問 9 または設問 10 と，設問 13 との間には，カイ二乗検定により有意差が認められた（$p < 0.005$））．

設問 1 と設問 6 についても，自分の病名を一定にし，l-多様性のパラメータ l を増加させた（プライバシ保護レベルを向上させた）．ただし，γ-amplification のプライバシ保護レベルは低下している．このときも，許諾率は 24%から 35.5%に増加しており，l の値が想定どおり許諾率に影響を与えることが確認できた（カイ二乗検定により有意差が認められた（$p < 0.005$））．設問 8 と設問 6 についても同様であり，l の値が想定どおり許諾率に影響を与えることが確認できた（カイ二乗検定により有意差が認められた（$p < 0.005$））．

5.2.2 ϵ-差分プライバシ

ϵ-差分プライバシに関する分析結果を図 3 (b) に示す．なお，ϵ-差分プライバシについては，ϵ の値が ∞ となっている設問が複数ある．本来は図示できない値であるが，便宜的に，図上ではおよそ ϵ の値が 100 のところに，∞ のときの結果を載せている．

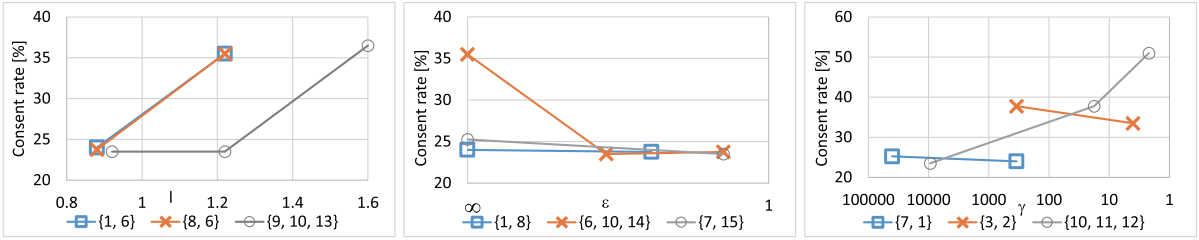
設問 1 と設問 8，および，設問 7 と設問 15 はそれぞれ，ϵ-差分プライバシのパラメータ ϵ を ∞ から 6 や 2 に変えており，プライバシ保護レベルが上昇している．ϵ-差分プライバシは，「ある個人のデータがあってもなくても匿名化データがほとんど変わらない」ことを目的としていると説明されることが多い．たとえば HIV 患者数が 10 人である状況を考える．パラメータ ϵ が ∞ である場合，この 10 という数字がそのままデータ利用者に提供される．つまり，ϵ-差分プライバシを指標として用いている場合，まったく匿名化されていない（まったくプライバシが保護されていない）状態である．一方，真の値から ±1 の誤差が与えられている設問に関しては，「ある個人のデータがあってもなくても匿名化データがほとんど変わらない」ということがある程度満たされていると考えられる．しかし，アンケート調査の結果から，想定とは逆に，有意差は認められないものの，プライバシ保護レベルが上昇するほうが許諾率は



(a) Result on items 1,3,5　　(b) Result on items 4,7

図 2 自分の病名と許諾率の関係

Fig. 2 Relationship between consensus rate and disease name.



(a) l-Diversity　　(b) ϵ-Differential Privacy　　(c) γ-amplification

図 3 許諾率の結果（凡例は設問番号の集合を表す）

Fig. 3 Results of consent rate (Each legend represents a set of item numbers).

低下するという結果となった．

設問 6，設問 10，設問 14 は，l-多様性と γ-amplification のプライバシ保護レベルを一定にし，ϵ-差分プライバシのパラメータ ϵ の値を減少させた（プライバシ保護レベルを向上させた）．割合は 35.5%，23.5%，23.8%となり，プライバシ保護レベルを上げるほど，許諾率が減少するという，想定外の結果となった（設問 6 と，設問 10 および設問 14 との間には，カイ二乗検定により有意差が認められた（$p < 0.005$））．

5.2.3 γ-amplification

γ-amplification に関する分析結果を図 3 (c) に示す．

設問 2 と設問 3 においては，γ-amplification のプライバシ保護レベルを変動させ，l-多様性と ϵ-差分プライバシのプライバシ保護レベルを固定した．γ-amplification については設問 3 のほうがプライバシ保護レベルが低い．しかし，許諾率は 33.5%と 37.8%となり，ほぼ変わらないという結果となった．

設問 1 と設問 7 は，HIV の患者数を変え，HIV の割合は 1/30 と 24/30 で大きく異なっている．したがって γ-amplification のプライバシ保護レベルは大きく低下している．しかし，許諾率はほとんど同じ結果となった．

設問 10，設問 11，設問 12 は，ϵ-差分プライバシと l-多様性のプライバシ保護レベルを一定にし，γ-amplification のパラメータ γ の値を減少させ（プライバシ保護レベルを向上させ），それにともない，自分の病名を変えた．許諾率は 23.5%，37.8%，51.0%の順に増加している．一方で，設問 1 と設問 5 で，すべてのプライバシ保護レベルを一定にして，自分の病名を HIV から偏頭痛に変えただけで，許諾率が 24.0%から 50.0%に増加していることを考慮すると，γ-amplification のプライバシ保護レベルのみで，許諾率に影響を与えているとはいえない．

5.2.4 濡れ衣問題の影響

設問 4 と設問 7 は，HIV が 24/30 と多い．HIV の割合が多いため，たとえ自分の病名が花粉症であったとしても，データ利用者から，「HIV の可能性が高い」と誤解されうる．しかしながら，自分が HIV なら許諾率は 25.3%，花粉症なら許諾率は 44.8%であり，HIV の割合は関係なく，自分が何の病気であるかの影響が大きいことが分かる．したがって，このような「濡れ衣」の問題は，実際には個人の感じ方にあまり影響を与えない可能性があることが分かった．

5.3 分析のまとめ

γ-amplification は，プライバシ保護レベルを上昇させるほどプライバシが保護されていると感じるユーザ数が増える場合とほとんど変わらない場合があった．回答者の病名が HIV 以外の場合に限定すると，プライバシ保護レベルを上昇させても許諾率にはほとんど影響がなかった．さらに，ϵ-差分プライバシについては，プライバシ保護レベルを向上させるほど，許諾率が低下する場合があるという想定外の結果になった．一方，l-多様性についてはそのプライバシ保護レベルを高い値に設定することで，許諾率が増加した．ただし，自治体に提供されるデータ内に含まれる病名数や，自分と同じ病気の患者数等にも依存することが考えられるため，この結論から l-多様性という指標が，プライバシ保護実現指標であると結論付けることはできない．どのような状況のときに，プライバシ保護レベルを向上させると許諾率が向上するという関係が得られるか，状況を洗い出して今後調査していく必要がある．

またこれら 3 指標すべてに共通して，そのプライバシ保護レベルを変えることよりも，「自分の属性値」が許諾率に与える影響のほうが強いことが分かった．また，匿名化データから自分の病名を誤解されうる「濡れ衣」問題について，本アンケート調査においてはあまり個人の感じ方に影響を与えない可能性があることが分かった．

6. 考察

6.1 プライバシ保護レベルの変動が与える許諾率への影響

プライバシ保護レベルを向上させても，許諾率がほとんど変動しない場合や，逆に許諾率が低下する場合があることが分かった．これはいくつかの可能性が考えられる．1 つは，このようなプライバシ保護目的指標が，実際にはプライバシを測定できない可能性があるということである．もう 1 つは，アンケート回答者に，リスクについての知識がなかったためである可能性がある．

特に ϵ-差分プライバシについては，誤差が大きくなるほど個人の病名が特定される可能性が低いために，誤差の大きい設問のほうが許諾率が増加するだろうという予想をしていたが，誤差の値が 0 のときが最も許諾率が高かった．したがって，ϵ-差分プライバシが，実際にはプライバシを計測できない指標である可能性がある．少なくとも，「アンケート回答者に，差分プライバシのプライバシ保護レベルを上げることによってどのようなリスクが軽減されるのかの具体的な説明を行わない場合は，プライバシ保護レベルを上げるほど許諾率が低下する場合がある」という特徴が ϵ-差分プライバシにはあると考えられる．

しかし，回答者が，誤差が大きくなるほど個人の病名が特定される可能性が低くなる，という知識を持っていなかっただけであり，知識を持っていれば逆の結果となった可能性もある．人間は曖昧な条件が示されたときに消極的な判断を行うことが既存研究によって示されている [4]．アンケート回答者に提示された誤差の値の大きさがこの曖昧さにつながり，消極的な判断につながった可能性がある．

したがって自分の属性値が特定されてしまうリスクについては，数学的な理解を求めることは困難ではあるが，適切に説明する必要があると考えられる．また，匿名化データに自分のデータが含まれているかどうかが分かってしま

うリスク等，センシティブ属性値が特定される以外のリスクもある．将来課題として，どのリスクを説明し，どのリスクは説明しないのか，個人の感じ方に関わる要因を抽出する必要があると考えられる．

6.2 自分の属性値による許諾率の変化

既存のプライバシ保護目的指標の多くは，自分の属性値に依存せずにプライバシ保護レベルが決定される．今回対象とした3指標もすべて，自分の属性値に依存せずにプライバシ保護レベルが算出される．同じプライバシ保護レベルが設定されていたとしても，自分の属性値によって感じ方が大きく変わることにより，次に述べる問題が発生する．

自分の情報が含まれることを許諾するかどうかの判断基準が，各個人の属性値に依存しないのであれば，データ利用者側は匿名化データから正しく統計的な分析を行うことができる．しかし，自分の属性値によって，自分のデータが匿名化データに含まれてよいかどうかの判断が変わる場合，匿名化データから得られる情報が，真の情報とかけ離れてしまう恐れがある．

たとえば，ある特定の病気Aにかかっている個人は，自分のデータが匿名化データに含まれることを許諾せず，それ以外の病気にかかっている個人は許諾する，という状況を考える．このとき病気Aについては，匿名化データを作成する時点で，極端に偏ったサンプリングが行われていることになる．プライバシ保護データマイニングの研究分野では，データの有効性をできるだけ損なわない匿名化手法が数多く提案されているが，基になるデータがすでに真実から乖離している場合は，匿名化手法がどれだけ洗練されたとしても，データ利用者は誤った分析結果しか得られない．

したがって，属性値ごとに許諾率がどう変わるかを何らかの方法で断定する必要がある．少なくとも，属性値ごとに許諾率が大きく変わることを認識したうえで，匿名化データを取り扱う必要がある．

6.3 新しくプライバシ保護目的指標を提案する際の課題

プライバシ保護データマイニングの分野では，研究者が新しくプライバシ保護問題を提起し，それを解決する指標および匿名化アルゴリズムが提案されることが多い．プライバシという，人の感じ方に大きく影響を受ける分野でありながら，人の感じ方を調査したうえで新しい指標やアルゴリズムを提案している研究はほとんど存在しない．各研究者が主張するプライバシ保護問題が実社会において本当に問題となりうるかどうかは，実際にアンケート調査を行う等，人々がそれをどう感じるかを把握しなければ分からないため，少人数規模であっても感じ方に関する調査を行うことが必要であると考えられる．

7. おわりに

プライバシ保護データマイニングに関する研究がさかんに行われており，どれだけプライバシが保護されているかを計測する指標が数多く提案されている．プライバシは人々の心理に関わる問題でありながら，これまで，提案されている指標のパラメータを変えると感じ方がどう変わるかについて数百人規模で調査した例はない．対象とする属性の種類（年収，病名，年齢等）やデータ利用者（民間企業，大学，公的機関等）といった要因も大きな影響を与えると考えられるが，既存研究で頻繁に例題として取り上げられている病名を対象とし，公的機関をデータ利用者に設定した本研究は，プライバシ保護レベルによって変わる感じ方の調査として重要な第一歩となると考えている．

謝辞 本研究はJSPS科研費24300005，26330081，26870201の助成を受けたものです．

参考文献

[1] Acs, G., Castelluccia, C. and Chen, R.: Differentially Private Histogram Publishing through Lossy Compression, *Proc. IEEE ICDM*, pp.1–10 (2012).
[2] Agrawal, R., Srikant, R. and Thomas, D.: Privacy preserving OLAP, *Proc. ACM SIGMOD*, pp.251–262 (2005).
[3] Blum, A., Ligett, K. and Roth, A.: A learning theory approach to noninteractive database privacy, *Journal of the ACM*, Vol.60, No.2, pp.12:1–12:25 (2013).
[4] Camerer, C. and Weber, M.: Recent developments in modeling preferences: Uncertainty and ambiguity, *Journal of Risk and Uncertainty*, Vol.5, No.4, pp.325–370 (1992).
[5] Chawla, S., Dwork, C., McSherry, F., Smith, A. and Wee, H.: Toward Privacy in Public Databases, *Proc. Theory of Cryptography Conference* (*TCC*), pp.363–385 (2005).
[6] Chaytor, R. and Wang, K.: Small domain randomization: same privacy, more utility, *Proc. VLDB Endow.*, Vol.3, No.1-2, pp.608–618 (2010).
[7] Chi-Wing, R., Li, J., Fu, A.W.-C. and Wang, K.: (α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing, *Proc. ACM KDD*, pp.754–759 (2006).
[8] Dwork, C.: Differential Privacy, *Automata, Languages and Programming*, Lecture Notes in Computer Science, Vol.4052, pp.1–12, Springer (2006).
[9] Dwork, C., McSherry, F., Nissim, K. and Smith, A.: Calibrating Noise to Sensitivity in Private Data Analysis, *Proc. Theory of Cryptography* (*TCC*), pp.265–284 (2006).
[10] Evfimievski, A., Gehrke, J. and Srikant, R.: Limiting privacy breaches in privacy preserving data mining, *Proc. ACM PODS*, pp.211–222 (2003).
[11] Fung, B.C.M., Wang, K., Chen, R. and Yu, P.S.: Privacy-preserving data publishing: A survey of recent developments, *ACM Computing Surveys*, Vol.42, No.4, pp.1–53 (online), DOI: 10.1145/1749603.1749605 (2010).
[12] LeFevre, K., DeWitt, D. and Ramakrishnan, R.: Mondrian Multidimensional K-Anonymity, *Proc. IEEE*

ICDE, pp.25–25 (2006).
[13] LeFevre, K., DeWitt, D.J. and Ramakrishnan, R.: Workload-aware anonymization techniques for large-scale datasets, *ACM Trans. Database Systems*, Vol.33, No.3, pp.1–47 (2008).
[14] Li, J., Tao, Y. and Xiao, X.: Preservation of proximity privacy in publishing numerical sensitive data, *Proc. ACM SIGMOD*, pp.473–486 (2008).
[15] Li, N., Li, T. and Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity, *Proc. IEEE ICDE*, pp.106–115 (2007).
[16] Machanavajjhala, A., Gehrke, J., Kifer, D. and Venkitasubramaniam, M.: l-diversity: Privacy Beyond k-Anonymity, *Proc. IEEE ICDE*, pp.24:1–24:12 (2006).
[17] McSherry, F. and Talwar, K.: Mechanism Design via Differential Privacy, *Proc. IEEE FOCS*, pp.94–103 (2007).
[18] Nergiz, M.E., Atzori, M. and Clifton, C.: Hiding the presence of individuals from shared databases, *Proc. ACM SIGMOD*, pp.665–676 (2007).
[19] Nikolov, A., Talwar, K. and Zhang, L.: The geometry of differential privacy: the sparse and approximate cases, *Proc. ACM STOC*, pp.351–360 (2013).
[20] Rastogi, V., Suciu, D. and Hong, S.: The boundary between privacy and utility in data publishing, *Proc. VLDB*, pp.531–542 (2007).
[21] Samarati, P.: Protecting respondents' identities in microdata release, *IEEE Trans. Knowl. Data Eng.*, Vol.13, No.6, pp.1010–1027 (2001).
[22] Shabtai, A., Elovici, Y. and Rokach, L.: A Survey of Data Leakage Detection and Prevention Solutions, *SpringerBriefs in Computer Science*, Vol.2002, Springer (2012).
[23] 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).
[24] Wang, K. and Fung, B.C.M.: Anonymizing sequential releases, *Proc. ACM KDD*, pp.414–423 (2006).
[25] Wu, S., Wang, X., Wang, S., Zhang, Z. and Tung, A.K.: K-Anonymity for Crowdsourcing Database, *IEEE Trans. Knowledge and Data Engineering*, Vol.26, No.9, pp.2207–2221 (2014).
[26] Xiao, X. and Tao, Y.: Anatomy: simple and effective privacy preservation, *Proc. VLDB*, pp.139–150 (2006).
[27] Xiao, X. and Tao, Y.: m-invariance: Towards Privacy Preserving Re-Publication of Dynamic Datasets, *Proc. ACM SIGMOD*, pp.689–700 (2007).
[28] Xiao, X., Wang, G. and Gehrke, J.: Differential privacy via wavelet transforms (2010).
[29] Xu, J., Zhang, Z., Xiao, X., Yang, Y., Yu, G. and Winslett, M.: Differentially private histogram publication, *The VLDB Journal*, Vol.22, No.6, pp.797–822 (2013).
[30] Zhang, Q., Koudas, N., Srivastava, D. and Yu, T.: Aggregate Query Answering on Anonymized Tables, *Proc. IEEE ICDE*, pp.116–125 (2007).
[31] Zhang, X. and Meng, X.: Discovering top-k patterns with differential privacy-an accurate approach, *Frontiers of Computer Science*, Vol.8, No.5, pp.816–827 (2014).
[32] 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，コンピュータセキュリティシンポジウム（CSS），pp.1–6 (2009).
[33] 佐久間淳，高橋克巳：クラウドストレージにおける個人情報の利活用とプライバシー保護，情報処理，Vol.52, No.6, pp.706–715 (2011).
[34] 清　雄一，大須賀昭彦：誤差を考慮した位置匿名化手法の提案，電子情報通信学会論文誌，Vol.J97-D, No.5, pp.964–974 (2014).

清 雄一　（正会員）

1981 年生．2009 年東京大学大学院情報理工学系研究科博士後期課程修了．同年（株）三菱総合研究所入社．同社情報技術研究センター，金融ソリューション本部等に所属．2013 年より電気通信大学助教，現在に至る．分散コンピューティング，セキュリティ，プライバシ保護技術等の研究に従事．電子情報通信学会，IEEE Computer Society 各会員．

稲葉 緑　（正会員）

2005 年名古屋大学大学院環境学研究科修了，同年より（独）交通安全環境研究所自動車安全研究領域非常勤研究員，電気通信大学大学院情報システム学研究科助教を経て，現在，JR 東日本研究開発センター安全研究所研究員．人間の感情を考慮した情報の提供方法，ICT 利用による安全教育等の研究に従事．日本心理学会，計測自動制御学会，自動車技術会等の会員．博士（心理学）．

大須賀 昭彦　（正会員）

1958 年生．1981 年上智大学理工学部数学科卒業．同年（株）東芝入社．同社研究開発センター，ソフトウェア技術センター等に所属．1985～1989 年（財）新世代コンピュータ技術開発機構（ICOT）出向．2007 年より電気通信大学大学院情報システム学研究科教授．2012 年より国立情報学研究所客員教授兼任．工学博士（早稲田大学）．主としてソフトウェアのためのフォーマルメソッド，エージェント技術の研究に従事．1986 年度情報処理学会論文賞受賞．IEEE Computer Society Japan Chapter Chair，人工知能学会理事，日本ソフトウェア科学会理事を歴任．電子情報通信学会，人工知能学会，日本ソフトウェア科学会，IEEE Computer Society 各会員．