Computer Security Symposium 2019
21 - 24 October 2019

個人情報の結合可能性の評価方式と差分プライバシーを用いたデータ削除要求への対応手法

小栗 秀暢[†1] 山岡 裕司[†1] 鎌倉 健[†1]

概要：企業内における多くのパーソナルデータは，集計表や仮名表など，使用目的ごとに様々な形式に加工され，派生データとして利用される．多くの派生データは単独では個人を識別できなくとも，結合して元データを復元できる可能性がある．近年，サービス運営者には，ユーザからの削除要求に応じてパーソナルデータ中から特定のレコードを削除加工する義務が課されているが，派生データを削除する基準は曖昧であり，管理する手法が必要とされている．本稿では，派生データ間の属性ごとの結合可能性を計測し，グラフ構造でその関係性を管理する手法を提案する．その上で，派生データ間の結合可能性を経路として探索することで，パーソナルデータを再結合して復元できるリスクを計測する．また，探索した経路の中で，最も結合可能性の高い属性のみを差分プライバシーを用いてかく乱することで，派生データ群全体の復元可能性を減少させる手法について提案する．実験によって元情報に復元できないプライバシー保護指標の値域を求め，その効果を検証した．

キーワード：削除権，データ流通，仮名化，匿名加工

A management system on connectability of personal data, and erasure method using differential privacy

Hidenobu Oguri[†1] Yuji Yamaoka[†1] Ken Kamakura[†1]

Abstract: A lot of personal data in the company are processed into various formats for each purpose of use, such as aggregate tables, and are generally stored as derived data. Even if derived data cannot identify individuals by themselves, there is a possibility that the original data can be restored by combining to other derived data. In recent years, companies have been obligated to erase personal data appropriately according to user requests, but the criteria for how much of the derived data should be erased are ambiguous. In this paper, we propose a system to measure the connectability of derived data and clarify the relationship with graph structure. The risk that personal data can be restored is measured by searching the connectability of derived data as a route. In addition, we propose a method to reduce the overall restoration possibility by disturbing only the attribute with the highest connectability among the searched routes by using differential privacy. Experiments showed how to obtain index range at a level that cannot be restored to the original information, and verified the effect.

Keywords: Right to the erasure of personal data, Data distribution, Pseudonymization, Anonymization

1. はじめに

近年，企業や行政機関，医療施設などにおいて，パーソナルデータは業務の遂行に欠かせないものとなっている．多くのパーソナルデータは，機微情報や金融情報など，漏洩すると個人に対して大きな影響を与えるデータと，性別や年齢など，一般的に利用されているデータが混在しており，分析や利活用が難しい．そこで，多くの企業では，例えばクレジットカード等の金融情報は PCI DSS などの管理された領域に保存し，分析や売上集計などの目的に応じて，個別のレコードや属性のみを抽出，加工した「派生データ（Derived data）」として利用している．

この方式は，機微性の高い個人情報を安全に保管し，各個別のデータ利用を可能とする優れた方式であるが，多くの派生データが社内に散在することとなり，管理が困難である．派生データの多くは，安全性が検証されていない仮名化データや，集計データである．その利用に係る課題としては ①保管場所が一般事業領域であるため安全性が低い，②派生データの再結合により元データの復元が可能となる，などがある．この問題はセキュリティ面だけでなく，企業の法令対応の面からも大きな課題である．

2018 年の EU GDPR[1]施行に伴い，企業やサービスが保持するパーソナルデータに対する消去の要件が明確化された．具体的には消去権，忘れられる権利．又はデータの同意期限の終了による削除などへの対応である．これらの法令では原本となったマスターデータだけでなく，そのコピーについても追跡し，管理することが求められている．

また，日本 IT 団体連盟が認定している「情報銀行」の枠組み[2]においても「実効的な本人関与(コントローラビリティ)」は重要な要素であると規定されている．今後，情報銀行サービスが普及するに従い，日本国内においてもパーソナルデータの適切な削除について関心が高まるだろう．

†1 株式会社富士通研究所，
FUJITSU LABORATORIES LTD.

© 2019 Information Processing Society of Japan

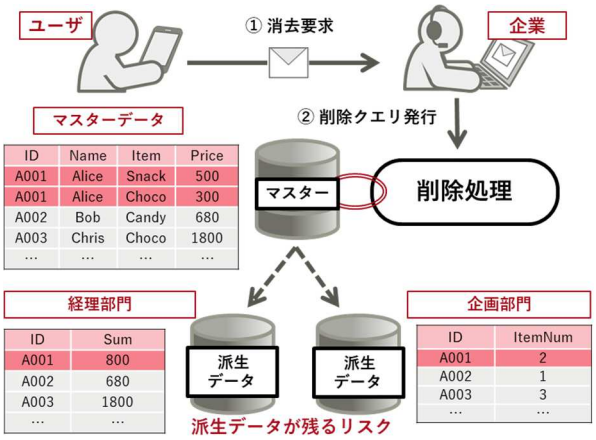

図 1 派生データが残るユースケース

しかし，あるユーザの求めに応じて，関連する全てのデータを削除する処理は実業務に影響が大きく，現実的ではない．例えば，図 1 のように派生データとして経理部門と企画部門にデータを提供する場合を考える．この場合，ある個人に関する派生データを全て消去することは，経理や事務的な手続きに支障が出る．そのため，実際には重要なデータの多くを残しておく必要がある．では，決済履歴を機械学習にかけて分析している企画部門のデータは全て消去するべきだろうか．純粋な売上分析であった場合，結果を業務ソフトウェアに投入している場合もある．データを削除することで業務ソフトウェアの不整合が発生する場合は処理するべきかなど，業務に必要なデータは，事業者ごとに異なる．

反面，それらの権限を悪用すると，社内の重要台帳を，個人の要求の名のもとに自由に書き換え可能となる．これによって，不正決算や技術的ミスの隠蔽など，企業の根幹をなす業務への影響が出る可能性がある．

そのため，多くの企業では自社の利益と法令上の義務を考慮してデータを残す，又は削除するという判断を行っている．しかし，データ証跡技術の進歩や，法令的な義務の厳格化などの要因によって，企業が保持しているパーソナルデータとその派生データから，個人の特定・識別に関わるデータを適切に削除し，業務に必要なデータと再結合されないように管理していることを示す技術が必要となると考える．

そこで本稿では，あるマスターとなるパーソナルデータを基準にして複数作成された派生データ間の属性の関係性を，グラフ構造によって管理し，元データを復元できるリスクを計測する手法を提案する．本方式は，パーソナルデータの結合リスクをノードとエッジの関係として表現できるため，最もデータの再結合リスクが高い属性を特定することができる．そこで，削除が必要な属性に対して差分プライバシーを用いてノイズを付与することで，個人のデータの復元リスクを減少させる手法を提案する．実験では，個人データを復元できない加工を行うため，プライバシー保護レベルを定式化する手法について検証し，実データにおいてプライバシー保護が可能となることを示した．

2. 従来研究

まず，パーソナルデータの結合と復元については，匿名化分野での研究が広く行われている．

Sweeny は投票者リスト（Public voter list）に存在する名前と，医療履歴データベースに含まれる Zip コード，誕生日，性別を準識別子として結合することで，マサチューセッツ州知事の病気に関する情報を得ることができた．また，同様の手法を用いることで，米国国民の 87 %を一意に識別することができることを報告した[3]．そこで同値類を作成することで，個人の再識別可能性を $1/k$（$k \geq 2$）まで減少させる k-匿名化が考案された．k-匿名性は個人の識別可能性を減少させるが，同値類を作成する際に元情報を大きく損なう可能性がある．そのため，最適なプライバシー保護と有用性を両立する k 値を定めることが困難である．

そこで，同値類を作成するのではなく，値に対してかく乱を加え，元データと匿名データの区別をつけにくくする手法が提案されている．その一つが差分プライバシーである．差分プライバシーとは，あるデータとたかだか 1 レコードだけが異なる別のデータを比較する際に，統計的に加えられたノイズを付与することでどちらかの判別ができないことを確率的に保証する手法である．

Dwark は，データに対して一定のラプラスノイズを付与することで，他のデータとの判別を不能とする ε-差分プライバシー[4]を提唱した．ある値の出現確率 $\Pr[p_D]$ に対して，加工を加えた後の確率 $\Pr[p_{D'}]$ が以下の関係にあるとき，ε-差分プライバシーと呼ぶ．

$$e^{-\varepsilon} \leq \frac{\Pr[p_D]}{\Pr[p_{D'}]} \leq e^{\varepsilon}$$

$$|\ \log(\Pr[p_D] \in S) - \log(\Pr[p_{D'}] \in S)\ | \leq \epsilon$$

仮説検定による解釈[5]によると，ε が 0.1-差分プライバシーを満たすとき，有意水準 5%で検出力 5.6%以上の検定を作ることができないとされている．

一般に ε-差分プライバシーを満たすには，ラプラス分布に沿ったノイズを加えることで実現される．まず，L1 感度 $\Delta\vec{f} = \max||\vec{f}(D_1) - \vec{f}(D_2)||_1$ （$||\ \ ||_1$ は L1 ノルム)を求め，プライバシー保護の最低単位を設定する．ε はこれに対して値の移動量を少なくするために与えられる．ε が小さい程元データとの距離が小さくなり，強いノイズが付与されることになる．

$$\sigma = \frac{\max||\vec{f}(D_1) - \vec{f}(D_2)||_1}{\varepsilon}$$

これに対して μ：出力するノイズ量の期待値を与えることで ε-差分プライバシーを達成することができる．

$$L_{p,\mu} = \begin{cases} if \quad U \leq 0.5 \ : \sigma \log_2 U + \mu \\ \text{otherwise}: \ \sigma \log_2 \ (\ 1 - U \ ) \ + \mu \end{cases}$$

ε-差分プライバシーは元データと無関係なラプラスノイズを付与することで元データと加工後のデータの結合可能性を減少させる．また，平均が 0 にほぼ近いラプラスノイズを付与することから，全体統計量や平均値など，分析に最低限必要な値が変化しない性質を持つ．しかし，安全性指標としての ε は，値が小さい程強いプライバシー保護レベルが高いが，k-匿名性の k 値と同じく，最適値を定める基準が存在せず，有用性とのバランスをとって ε の値を設定する手法が課題である．

また，グラフ構造に対する差分プライバシーを求める研究[6]もされている．しかしこのグラフ構造は SNS などの個人の挙動について表現するものであり，ある人と人のつながりが存在するかどうかを差分プライバシーによってかく乱する手法である．そのため，今回のような削除要求データを処理する際には利用できない．

また，差分プライバシーの考え方を拡張した局所差分プライバシー[7]が提案されている．局所差分プライバシーは，データを収集する事業者に対して，真の値を差分プライバシーによってかく乱する手法である．個々のユーザからデータ収集者にデータを送付する際に，端末内に同じ確率でラプラスノイズを付与する仕組みを搭載する．それによってユーザ個々の情報にはノイズが付与されているが，その平均や合計値には誤差が少ない状態が実現する．そのため，最終的な全体の統計情報しか利用しない事業者にとっては利便性が高い．本方式は，個人からのデータ削除要求が散発的に出現することから親和性が高い．

本研究では，散発的に増加するデータ削除要求に対して，対象となる属性をあらかじめ定めておき，かつデータごとに決められたプライバシー保護レベルでの差分プライバシーを満たすノイズを付与することで，派生データ全体における元データの復元可能性を低減する手法について提案する．

3. グラフ構造によるデータ管理手法

3.1 ユースケース

企業は図 2 に示すように，個人情報（マスターデータ）と，複数の派生データを保持している．その中で，特定の個人（複数である可能性もある）から，個人情報の削除要求が来たとする．

このような状況において，データを削除するという要求を満たし，派生データが再結合され，元データが復元されるリスクを低減する．かつ，データの削除項目を最低限にすることで事業者の負担を軽減する手法について検討する．

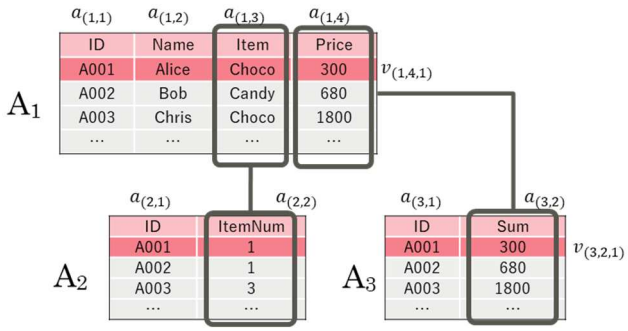

図 2 削除対象データの例

まず，派生データの種類は無数に存在しており，それら全ての加工方法を網羅することは困難である．しかし，多くの派生データにおいて，削除権の要請が出てくる可能性があるのは，個人の氏名や住所等の識別子を仮名に変更した，いわゆる仮名データである．仮名データは多くの定義においては個人情報と定義されているが，派生データとなった場合には，元情報との再結合が可能かを判定する必要がある．

本稿では，派生データとして利用されることの多い，1. 単純な仮名化データ，2. サンプリングされた仮名化データ，3. 識別子をキーとした集計データ，について主に述べる．それ以外のデータの基準については，データのユースケースによっても異なってくるため，別途検討する．

例えば，何らかの匿名化アルゴリズムによって処理されたデータについても検討する必要があるが，多くの匿名化アルゴリズムは，元データとの関係性について何らかの有用性指標を設定していることが多い．複数の属性をまとめた上で，匿名化アルゴリズムが用いている有用性指標を利用する方が現実的である．

3.2 結合可能性の評価

ある事業者が保持するデータベースには，マスターデータとデータを抽出，加工された派生データ $A = \{A_1, A_2, \ldots, A_n\}$ が存在する．A_n に含まれる属性は $a_n = \{a_{(n,1)}, a_{(n,2)}, \ldots, a_{(n,m)}\}$ とする．$a_{(n,m)}$ に含まれる値 $v_{(n,m)}$ と，異なる $a'_{(n',m')}$ に含まれる値 $v'_{(n',m')}$ を比較し，値の一致率を結合可能性と定義する．また，含まれる値が数値属性である場合は $v_{(n,m)}$ を，識別子を基準とした統計値に変更し，その一致率によって同様に処理するものとする．

定義 1：属性同士の結合可能性は $a_{(n,m)} \in A_n$ と $a'_{(n',m')}$ に含まれる値の Jaccard 係数の平均値を用いて示す．

$$R(a_{(n,m)}, a'_{(n',m')}) = \frac{1}{|m \cup m'|} \sum \frac{|v_{(n,m)} \cap v'_{(n',m')}|}{|v_{(n,m)} \cup v'_{(n',m')}|} > 0$$

定義 2：ただし $a_{(n,m)}$ と $a'_{(n',m')}$ が同じ元 $A_n = \{A_1, A_2, A_3\}$ に含まれる場合，$R(a_{(n,m)}, a'_{(n',m')}) = null$ とし，結合可能な状況を確認しない．

この値が大きい程，データ同士の結合可能性が高く，組み合わせた際に元データとして復元される可能性が高いデータと言える．

これによって派生データの全ての属性間の結合可能性を算出できるため，各属性をノード，属性間の結合可能性をエッジとして定義したグラフを作成する．このグラフの経路を探索することで，派生データを再結合した場合のリスクを計測できる．

3.3 処理手順

まず，調査対象データに含まれる属性同士の結合可能性の全組み合わせを調査し，表 L（図 3）を作成する．それをグラフ構造に示すことによって図 4 のように表現できる．

まず，探索の始点を設定する．本稿では目的を元データへの復元可能性に置いているため，元のデータと結合可能な識別子を復元可能なキーと考え，始点と設定する．

	a(1,1)	a(1,2)	a(1,3)	a(1,4)	a(2,1)	a(2,2)	a(3,1)	a(3,2)
a(1,1)	-	null	null	null	0	0	0	0
a(1,2)		-	null	null	0	0	0	0
a(1,3)			-	null	0	1.0	0	0
a(1,4)				-	0	0	0	1.0
a(2,1)					-	null	1.0	0
a(2,2)						-	0	0
a(3,1)							-	null
a(3,2)								-

図 3 結合可能性の組み合わせの表 L

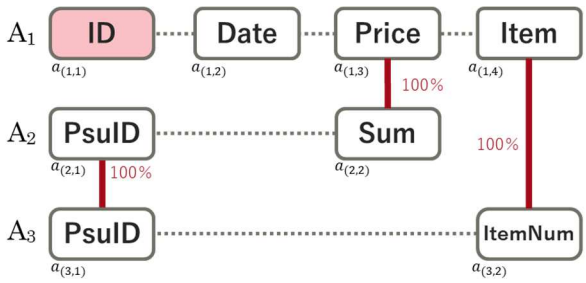

図 4 グラフ構造の例

消去できない属性を始点と定め，つながりがあるノードを探索し，結合可能経路としてノード履歴を記録する．

ノードリスト$H = (h_1, \ldots, h_l) =$

$[(a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(2,2)}, a_{(2,1)}, a_{(3,1)}, a_{(3,2)}, a_{(1,4)}),$

$(a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(1,4)}, a_{(3,2)}, a_{(3,1)}, a_{(2,1)}, a_{(2,2)}), \ldots]$

同時に各ノードをつなぐエッジの大きさ，即ち属性同士の結合可能性を，エッジの大きさとして記録する

探索済エッジ$P = (p_1, \ldots, p_l) =$

$[(-, null, null, 1.0, null, 1.0, null, 1.0),$

$(-, null, null, null, 1.0, null, 1.0, null, 1.0, null), \ldots]$

この探索済エッジPの合計値が，データ結合可能性の強さの総量であり，元データへの復元可能性である定義する．この結合可能性と復元可能性を用いてデータ削除処理の優先度を定める．

また，探索済エッジをそれぞれ検証することで，出現回数が多い，即ち結合可能性が高く，かつ多くの経路で利用されている，所謂ハブとなっている属性も判明する．これにより，レコードを削除するのではなく，結合可能性の高い属性のみを削除することで効果的に処理を完了できる．

しかし，データの削除処理はデータの有用性や事業の継続性という点で困難な場合も多い．そこで特定の属性との結合可能性を下げるため，匿名化や差分プライバシーの処理を加えることでデータの削除値数を最低限にし，業務への影響が少ない処理を提案する．

3.4 差分プライバシーを用いた結合可能性の低減処理

差分プライバシーは，個別処理で見ると元データへのノイズ付与を行うが，統計的にみるとほぼ平均が 0 のラプラスノイズを付与するため，平均値や合計値に大きな差がない．これは，マスターデータから派生データに加工し，機械学習などに定期的にデータを投入する場合などに優れた性質である．

また，削除処理を行う場合に，結合可能性が高い場合に強いノイズを加え，逆の場合は弱いノイズを与えることで，適応的なデータ処理が可能となる．それによって，元データに対する加工量が少なくて済む点も利点である．

そこで属性同士の結合可能性に応じてプライバシー保護レベルを変更する手法を提案する．

まず，ε-差分プライバシーでは，ε の値を小さくすることでノイズ付与量を大きくすることができる．実践的には L1 感度が 1 の場合，ε= 0.01～0.1 程度のノイズ付与量によってプライバシー保護がされると言われるが，その基準はデータの機微性や特徴によって異なる．

本稿では，データ同士の結合可能性 p_l が判明したとき，削除したことと同等のノイズ付与を行うため，ε をどのように導くべきかについて検討を行う

$p_l = (r_1, r_2, \ldots, r_l) = (-, null, null, 1.0, 0.5, 0.1, null)$ のときを考えよう．このデータにおいて最も結合可能性が高い 1.0 のノード（属性）については，強いノイズを付与する必要がある．逆に 0.1 の結合可能性のノードは，少ないノイズでも元データとの結合可能性を低下させることができる．

そこで結合可能性の逆数を使用して ε の値を定める．設定するべき $\varepsilon = n(1 - r_l)$ を係数としたラプラスノイズを付与し，ノイズ量の適正値を求める．

$$\sigma = \frac{\max\|\vec{f}(D_1) - \vec{f}(D_2)\|_1}{n\ (1 - r_l)}$$

ただし$r_l = 1$ の場合 $\varepsilon = z$ とする．これはゼロ除算を防ぐための極小さな係数である．また，調整係数として n を付与している．これは，結合可能性の範囲 $0 \le r_l \le 1$ に応じて対応する ε の範囲を定めるために用いる．この妥当な ε の値域を求める実験を次章で行う．

4. 実験

4.1 ユースケース

本実験では，あるサービス事業者にユーザからデータ削除要求が来た場合の処理を想定する．元となる購買データを処理して，派生データ 1 : Price の集計値，派生データ 2 丁目：購入アイテム数を作成した．元データを「削除できないデータ」と定義し，元データと紐づくことができる派生データの値を処理して，元データと派生データの結合可能性を排除することを目的とする．差分プライバシーノイズを集計値と購入回数に付与することによって元データとの結合可能性をなくし，かつ，その削除された利用者同士においても相対的に個人が識別されることを防ぐことを目的とする．

ここで，削除処理は実際には不定期に行われることに注意が必要である．そのため，あらかじめ全体の値の分布からノイズ付与レベルを定めておくことで，ローカル差分プライバシーによるメリットを受けることができるように業務を設計するための手法を検討する．

本実験では異なる 2 つの派生データに対して差分プライバシーをかけると仮定したとき，適切な ε の値域をどのように設定するかについて求める．

4.2 データセット

実験に使用するデータは Online Retail Data Set [8]より購買履歴データを取得し，ランダムに 100 名をサンプリングしたものを利用する．データセットの統計量を表 1，表 2，図 5 に示す．

表 1 統計量

Subject	Property
Record	m=10,480
User	n=100
Items	2,076

表 2 統計量

Subject	ItemNum	Sum
AVG	104.8	408.7
STDEV	203.1	1037.9
MAX	1729	9070.9
MIN	1	0.7

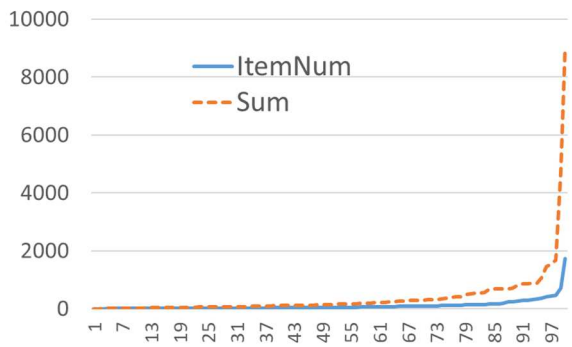

図 5 各データの分布

また，使用する属性は ID, Product name (Item) , Unit Price (Price) の 3 種類とする．このデータをマスターとし，派生データを 2 種類作成する．派生データ 1 はユーザ ID 毎に Price を集計したデータ ＝Sum とし，派生データ 2 はユーザ ID 毎に購入したアイテム数 ＝ ItemNum とする．この両方のデータは元データとの関連性を消去するため ID を仮名化し PsuID に変更している．図 6 にデータの関係性を示す．

数値データは統計値に変更された上で結合性の評価を行うため，元データと派生データの結合可能性は 100%であり，元データと派生データの両方にアクセス可能な管理者は，容易に再結合することができる．

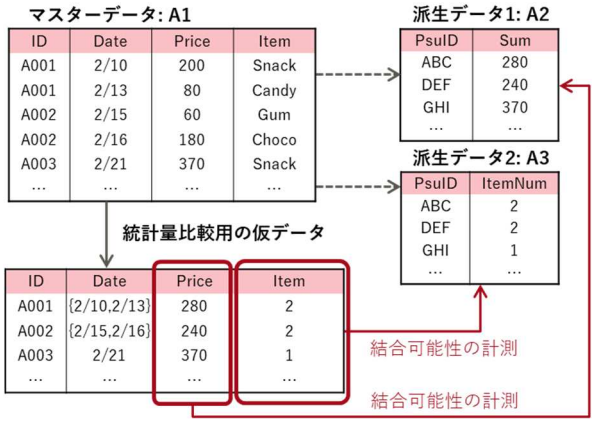

図 6 サンプルデータの結合性の例

4.3 関係性グラフの作成

ユースケースに沿ってデータ間の結合可能性を示すグラフを作成する．経路を探索すると，最も長い経路 $h_{\max} = [\, a_{(1,1)}, a_{(1,2)}, a_{(1,3)}, a_{(2,2)}, a_{(2,1)}, a_{(3,1)}, a_{(3,2)}, a_{(1,4)} \,]$ であり，その探索済エッジの最大値 $p_{\max} = [\, 0, null, null, 1.0, null, 1.0, null, 1.0, 0 \,]$，最大結合可能性 $|p_{\max}| = 3$ である．

この中で$[\, a_{(2,1)}, a_{(3,1)} \,]$間の結合可能性は，仮名の付け替えで対応した場合，必要な削除処理は$[\, a_{(1,3)}, a_{(2,2)} \,]$ $[\, a_{(3,2)}, a_{(1,4)} \,]$の 2 か所であり，この部分に対して差分プライバシーをかけた結果が，データを削除した場合と同じレベルの安全性を有していることを検証する．

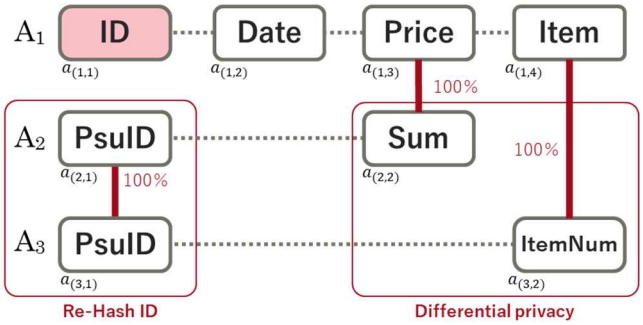

図 7 グラフ管理の例

4.4 実験手順

前節で述べたデータに対してデータ削除要求に対応する．このとき，削除要求に対応するのは 2 名とする．これは，差分プライバシーは，あるユーザと 1 レコードだけ異なる他のユーザについて，両者の区別がつかなくなることを求めているためである．

派生データ A_2, A_3 の結合可能性がある属性 $a_{(2,2)}$, $a_{(3,2)}$ を処理して，元データとの結合可能性をなくすことで対象データを削除したと同様の状態とする．そのためには，この 2 名を処理した後の値が差分プライバシーを満たすだけでなく，2 名の値の順序尺度が高い期待値で変更されなくてはいけない．このような値の加工と順序尺度での攻撃手法は，匿名加工・再識別コンテスト[9]等で使用されている．

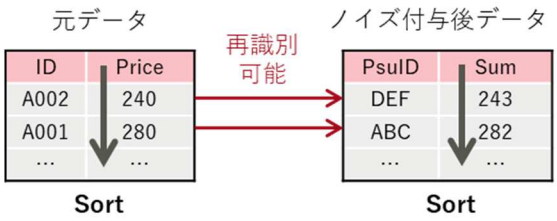

図 8　再識別されるノイズ量の例

図 8 に削除した 2 名の順序尺度が変更される場合を示す．あるユーザ A001，A002 の削除要求がされたとき，まずその 2 名の ID を仮名化した ID (PsuID) に変更する．その際に，差分プライバシーによってノイズを付与された A001，A002 の順番が変更されていない場合，高い確率で個人が特定される．

この考え方を元に，まずはデータ削除要件を満たすために最も強いノイズを付与する条件について検討する．最も強いノイズ量とは全てのデータ中から任意の 2 ユーザを抽出してノイズ付与した場合に，その両者がどちらであるかを完全に区分できない状態と考える．即ち，$a_{(3,2)}$ から抽出された 2 つの値 (x, y) が $x \neq y$，$x > y$，であったとき，差分プライバシーを適用した (x', y') について，$\Pr[x' \leqq y']$ (パターン①) の順番が完全にランダムになる状態を求める．2 値の大小の変化が目的であるため，2 項分布となり，期待値が 0.5 に近い程ランダム性が高くなる．

次にデータ削除要件の最も弱い条件を検討する．これはデータ削除要求が年間に n 件行われると仮定したとき，任意の 2 名の順番が $1/n$ 以上の確率で変更されることとする．即ち，全ての (x, y) の組み合わせの中で，ノイズを付与した際に 1 つも順番が変更されなかった率 $\Pr[\forall[x' \leqq y'] = \emptyset]$ (パターン②) を求めることで，任意のユーザ組において，x' と y'の区別がつかないレベルのノイズが 1 度以上発生したかを確認することができる．

例えば"Sum"の場合 $(\max(x), \min(y)) = (9070.9, 0.7)$ であるが，この x と y が判別できないレベルに加工されるには，最低でも合計で $\max(x) - \min(y) = 9070.2$ 以上のノイズが必要である．その量のノイズがパターン①の場合，確率 0.5 で発生しているレベルを検証し，パターン②の場合，n 回の施行の中で 1 回以上出現するレベルを検証する．

これにより削除要求に対するノイズ付与指標 ε の設定要件としてパターン①とパターン②間を値域として用いた場合に適切な削除処理が行われたと考える．

本実験では全 100 ユーザの中から任意の 2 名を抽出し，その 2 名の $a_{(2,2)}$ および $a_{(3,2)}$ に対して差分プライバシーを満たすノイズを付与する．そのため，抽出数（${}_nC_r$）として ${}_{100}C_2 = 4950$ 組を作成する．それぞれの組に対して，10000 回の削除要求が来たと仮定して ε 差分プライバシーを満たすノイズを付与する．そのパターン①と②の結果を計測することで，データを削除したと主張できる ε の値域を求める．

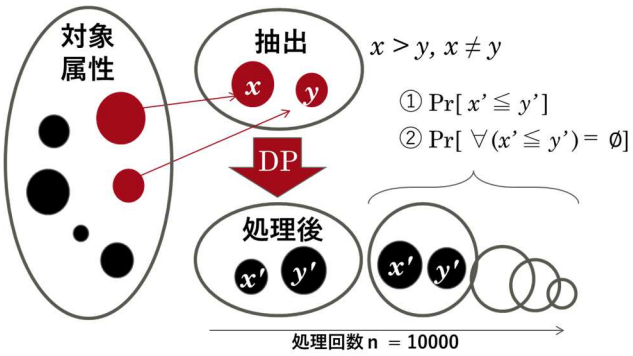

図 9 実験の概要

4.5 評価

実験では，ε 差分プライバシーの基準に基づき，L1 感度＝1 で ε の値を変更し，${}_nC_r = 4950$ パターン × 各 10000 回の施行の結果を示している．

図 10 に Sum の結果を示す．$\varepsilon = 10^{-3}$ のときにほぼ全てのユーザ組における $\Pr[\forall[x' \leqq y'] = \emptyset]$ の出現率が 0 になっている．ほぼ完全なランダムネスが保証される $\Pr[x' \leqq y'] = 0.5$ を達成するのは $\varepsilon = 10^{-5}$ からであり，それ以降は ε を小さくしてもプライバシー保護レベルに変化はない．即ち値域を $10^{-3} \leqq \varepsilon \leqq 10^{-5}$ とした場合，削除要求を満たしていると考える．

ItemNum は Sum より分散が小さいため，少ないノイズ量でもプライバシー保護が達成でき，$10^{-2} \leqq \varepsilon \leqq 10^{-4}$ 程度が適当であると確認できる．

データ利用側から考えると，例えば $(\max(x), \min(y))$ の順番が逆転するレベルのノイズ付与量はデータの利用性を大きく損なう．そのため，この値域を基準と考えた上で，データの利用性や機微性を含めて最終的に利用する ε の値域を設定することが望ましい．

また，削除要求が寄せられる回数も重要である．本実験

における処理回数 n とは，本データベースに何人から削除要求が寄せられるかの想定回数である．図 10，図 11 は処理 10000 回を実施した結果であるため，10000 人の削除要求が寄せられた場合の値域として有効である

注意点として，本実験のユースケースである 100 人のユーザ群に対して 10000 人から削除要求が寄せられることへの可否がある．本実験はデータセットから 100 名サンプリングして行ったものであることから，この 100 名への結果は元データ全体に対して削除要求が寄せられた場合の値域のシミュレーションであると認識している．

即ち，本実験を実サービスに適用する場合は，元となるデータベースの分布を正確に反映するサンプリングデータに対して，最終的な削除要求数の予測に基づいた試行回数 n によって実験を行うことで，適切な値域が導き出せる．

図 12，図 13 は、パターン②において，試行回数を 10 回～10000 回まで変更した場合における結果の変化量を示している．両方のパターンにおいて，試行回数を減らすことで，条件を満たす大きさのノイズが発生しない可能性が高まっている．

これにより，適切なノイズ量を得られる ε の値域を求めるためには，削除要求の想定回数 ＝ 試行回数 n の設定が必要であることが確認できる．

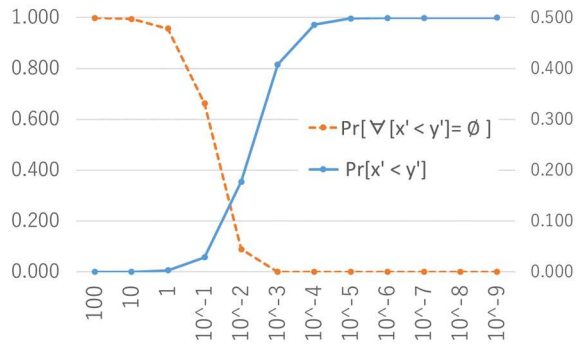

図 10 “Sum”の結果

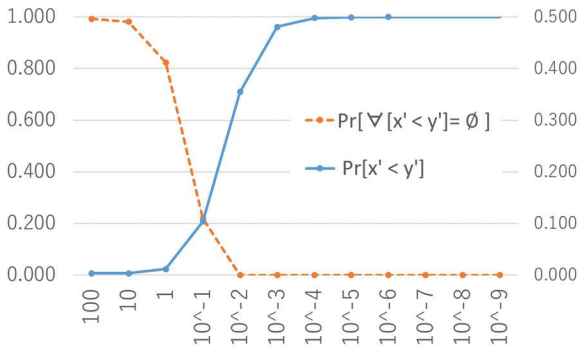

図 11 “ItemNum” の結果

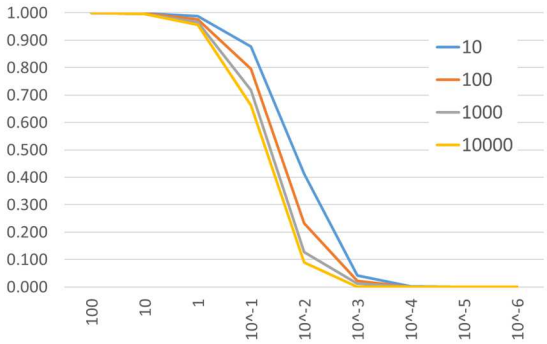

図 12 “Sum” の施行回数による変化

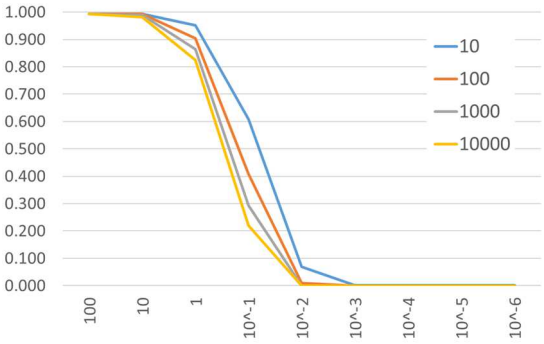

図 13 “ItemNum” の施行回数による変化

5. まとめ

本稿では，個人からの要求によって複数の派生データへの削除加工を行う場合に，派生データの属性同士の結合可能性を計測することで，グラフ構造でデータを管理する手法を提案した．また，そのグラフにおける経路を探索し，エッジの大きさとして結合可能性の集計を行うことで元データへの復元可能性を計測する手法を示した．

それによって．経路中に含まれる結合可能性が高いハブとなる属性を導き，特定の属性に対してのみ差分プライバシーを満たすノイズを付与する手法を提案した．しかし，ある個人のデータを削除したものと同様の効果を得るためのプライバシー保護指標の値域の設定方法が定まっていなかった．

実験によって，あるサービスに削除要求が来た場合を想定し，任意の 2 名の組を抽出してノイズを付与する際の最適なプライバシー保護指標 ε の値域を求めた．値域の定義として，完全なデータのランダムネスを保証する指標 $\Pr[x' < y']$を満たす位置をノイズ付与の最大値，削除要求に沿った試行回数において，データのランダム化が全てにおいて行われる可能性がある指標 $\Pr[\forall[x' < y'] = \emptyset]$ をノイズ付与の最小値と考え，ε の値を結合可能性の値から適応的に求める手法を示した．

しかし，削除対象となるユーザ数の見込みによって ε の値が変化するため，実験によって試行回数毎の最小値レベ

ルが変化することを検証し，実サービスに適用する際には削除要求数を想定するためのユースケース設定が重要であることを示した．

しかし，本方式はいくつか課題が残る．

まず，今回適用した差分プライバシーは非負制約を満たしていないため，売上金額に対してマイナスの値が存在するなど，使えない値が混在している．その制約を満たすと，差分プライバシーを満たさない，または平均値が大きく増加するなどの問題が発生するため，手法の改良が必要である．

また，本手法は多くのユーザに対して組み合わせを確認して ε の値を求める手法を示しているが，現実的にはサービスにおけるユーザ分布に従ったサンプリングを行って適切な人数による値域を求める必要がある．これらは今後の削除要求のユースケースなどに合わせて検討する必要がある．

参考文献

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) , (2016) .

[2] 情報信託機能の認定スキームの在り方に関する検討会, ”情報信託機能の認定に係る指針 ver1.0”, 総務省 経済産業省, (2018) .

[3] L.Sweeney, "k-anonymity: a model for protecting privacy", International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, pp.557-570, (2002) .

[4] Dwork, C., "Differential privacy", Automata, languages and programming, pp.1--12, (2006) .

[5] Wasserman, L., & Zhou, S., "A statistical framework for differential privacy", The Journal of the American Statistical Association, pp.375--389, (2010) .

[6] Chen, S. and Zhou, S., "Recursive mechanism: towards node differential privacy and unrestricted joins", Proceedings of the 2013 ACM SIGMOD International Conference on Management of Data, pp.653--664, (2013) .

[7] Rastogi, V., Hay, M., Miklau, G. and Suciu, D., "Relationship privacy: output perturbation for queries with joins", Proceedings of the twenty-eighth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, pp.107--116, (2009) .

[8] Chen, D., Sain, S.L. and Guo, K., "Data mining for the online retail industry: A case study of RFM model-based customer segmentation using data mining", Journal of Database Marketing & Customer Strategy Management, 19 (3) , pp.197-208, (2012) .

[9] KIKUCHI, H., YAMAGUCHI, T., HAMADA, K., YAMAOKA, Y., OGURI, H. and SAKUMA, J., "Study on Record Linkage of Anonymizied Data", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 101 (1) , pp.19--28, (2018) .