「プライバシー保護データマイニング」特集号 解　説

プライバシー保護データ流通のための匿名化手法

小栗　秀暢*

1. はじめに

近年のITの進歩に伴い，多くの企業や公的機関ではパーソナルデータを蓄積し，機械学習やデータマイニングなどの手法でデータ利活用を行っている．

しかし，それらの技術は分析対象となる学習データが多量に必要であり，一つの機関のデータでは分析目的が達成できない場合がある．そこで，公的機関や異なる機関が保持するデータを流通させ，サービス開発や事業の最適化などに活用するニーズが高まっている．

2017年の改正個人情報保護法の全面施行により，匿名加工情報という情報の類型が示された．これはパーソナルデータから特定の個人が識別される要素を排除したデータを，簡易的な手続きで第三者提供可能とする枠組みを認めたものである．

このような，パーソナルデータから個人のプライバシー侵害が発生する要素を排除して利用者に提供する技術として「プライバシー保護データパブリッシング(PPDP :Privacy Preserving Data Publishing)」がある．これはいわゆる，パーソナルデータに匿名化技術を適用した**「匿名データ」**を流通させる技術であり,「出力プライバシー(Output privacy)」ともよばれる．

PPDPでは，公開するデータの安全性基準と，その利活用の目的に沿った加工をバランスよく成立させることを目的としている．しかし，個人のプライバシー侵害が発生する条件とその攻撃者は多様であり，パーソナルデータを安全な形に加工する技術と，その安全性指標は，必ずしも明白ではない．

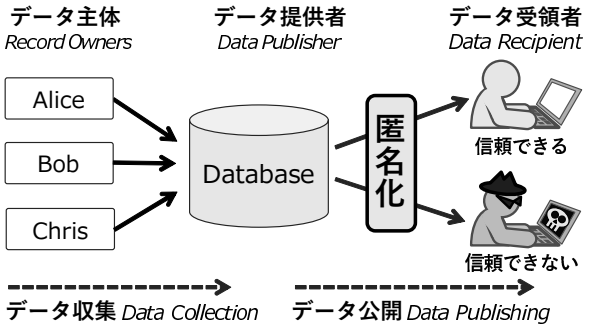
本稿では，PPDPに関連する技術要素，および攻撃者モデルと安全性指標，アルゴリズムについて解説し，その実現に向けた課題についてまとめる

2. データ定義

2.1 PPDPの攻撃者モデル

まず，PPDPにおける攻撃者モデルと用語の定義について記す．第1図にFungらがまとめた攻撃者モデル[1]を示す．

PPDPは収集したパーソナルデータを外部のデータ利用者に提供するモデルを基本とする．データ提供者(Data Publisher)は，データ主体(Record Owners)から収集したデータを匿名化し，データ受領者(Data Recipient)に提供する．その後，信頼できないデータ受領者が入手した匿名データから個人を攻撃するモデルを想定している．



第1図　PPDPにおける攻撃者モデル

本モデルにおいて，データ提供者はデータ主体との契約に基づいて正当にデータを処理しており，信頼できるプレイヤーとして考える．逆に，データ受領者が信頼できるか否かを区分する術は存在しないため，すべてを信頼できないプレイヤーと定義する．そのため，PPDPはすべてのデータ受領者に匿名データを提供してもデータ主体の安全が保証されるという，制約条件を伴った匿名化技術によって実施される．

2.2 パーソナルデータと匿名データ

まず，パーソナルデータとは，ある人間の属性や行動に関するデータ全般を指す．個人情報とはパーソナルデータに含まれる記述などによって，特定の個人を識別できるものを指す．本稿では加工対象はパーソナルデータとする．

それに対して，匿名データの定義は明確ではない．日本の個人情報保護法における匿名加工情報は**「個人情報保護委員会規則で定める基準に従い，個人情報を加工して特定の個人を識別することができないようにするとともに，当該個人情報を復元することができないようにしたものをいう（三十六条）」**と定義されており，ガイドラインが公開されている．しかし，これは法律としての定義であり，技術的な定義ではない．

また，欧州連合におけるデータ保護のアドバイザリー

* 株式会社 富士通研究所
Key Words: privacy preserving data publishing, PPDP, anonymisation, de-identification.

機関である第 29 条作業部会は「匿名化技術に関する意見書 [2]」にて，以下のように定義している．

(1) 個人を識別すること (single out) は可能か
(2) 個人に関する記録と紐付けることは可能か
(3) 個人を推定することは可能か

これらの基準に合わせて匿名化技術を選定することが必要とされるが「完全な技術は存在しないため，一つの手法に依存しないこと」を求めている．

また，英訳についても，文献によっては，Anonymised-data と De-identification を使い分けている場合があり，注意が必要である．

本稿での匿名データとは，パーソナルデータを加工し，**3** 章以降にて解説するいずれかの安全性指標を満たしたデータ，と広く定義する．

2.3 特定と識別

まず，パーソナルデータを利用してプライバシー侵害を可能とする方法として**「特定」**と**「識別」** がある．

「特定」は「ある情報が誰の情報であるかがわかる」ことである．具体的には，ある個人情報などが攻撃者の手に渡ったとき，氏名や住所，所属組織などから，その人物の社会的な状況が判明するデータである．物理的に個人への接触が可能となることから，強盗や詐欺などの強いプライバシー侵害を誘発する可能性がある．

つぎに「識別」は，社会的に誰であるかが判明しない場合でも「あるパーソナルデータ中において，その 1 名が存在することが判明する」ことである．シングルアウトともよばれる．インターネット企業などでは，本名を知らなくとも，管理 ID，メールアドレス，Cookie 情報など，個人を識別できる情報によって，ある嗜好をもつグループへの広告表示やメール配信などの形でアクセス可能となる．そのため，データ受領者が利益を追求するために，取得した匿名データを再識別して目的外利用する，というモチベーションが生まれやすい．

匿名化によるプライバシー保護は，この「特定」「識別」リスクを抑制することが主目的とされる．

2.4 パーソナルデータに含まれる要素

第 2 図にパーソナルデータと匿名データを構成する要素の定義を示す．

まず，パーソナルデータとは**「属性 (Attribute)」**と**「属性値 (Value)」**としてテーブルの形で表現される，データ主体に関する情報であり，あるデータ主体 1 名の情報を 1 レコードとして表現する．パーソナルデータには氏名や住民番号などの，直接識別子 (Explicit-Identifier) が含まれ，他のユーザと区別される．

匿名データでは，直接識別子は削除され，代わりに仮名 ID (Pseudonymized-Identifier) が振られる場合が多い．このパーソナルデータにおける直接識別子を仮名 ID に変換させただけのデータを「仮名データ」とよぶ．多くの情報セキュリティガイドラインにおいて，仮名データは匿名データとみなされないため，区分が必要である．

第 2 図 匿名データにおけるデータ定義例

2.5 匿名データに含まれる属性

つぎに，匿名データに含まれる属性について記す．

単一の属性ではユーザを特定できないが，複数組み合わせるとユーザを特定できる可能性のある属性を**「準識別子 (QID :Quasi-Identifier)」**とよぶ．第 2 図の例では 性別={ 男，女 } が該当する．このデータの準識別子が複数重なり，男，20 才，東京，..... などのように組み合わせられることで個人が識別される可能性が高まる．

また，準識別子には**観察可能性 (Observability)** の条件が付加されている．観察可能性の定義は難しいが，たとえば，一般的な知人や友人レベルならば知っている情報を指す．たとえば，性別や身長などについては，知人であれば，正確な値は解らなくとも「170cm くらいの男性」程度の知識をもっている．そのような属性は「観察可能性がある」ために，準識別子として区分することが多い．この観察可能性の設定が「攻撃者知識」に相当する．

また，複数のレコードにおいて，準識別子に同じ値をもつ群を**等価クラス (Equivalence Class)** または同値類とよぶ．第 2 図においては，準識別子として { 男，女 } の二種類が存在し，それぞれが 2 レコードずつの等価クラスをもつ，といえる．

そして，データ主体を特定・識別された状態で公開されることが望ましくない属性を**「センシティブ属性 (SA : Sensitive Attribute)」**とよぶ．準識別子とは異なり，センシティブ属性には一般的に観察可能性がない，または非常に観察可能性が少ないものと考える．第 2 図では，症状={ 骨折，風邪，ガン } をセンシティブ属性と設定しているが，これはあくまでも想定する攻撃者知識であり，データの管理状況やガイドラインなどに応じて，属性の設定は常に変化する．

最後に，その他の属性である．これは観察可能性がなく，本人の行動や嗜好にも関係しない属性などを指す．第 2 図では例として管理サーバ番号を示した．これは本人の属性情報ではなく，仮に漏洩しても，本人特定に結び付くリスクは非常に少ないと判断できる．

2.6 匿名データを作成する目的

データ分析の分野では，準識別子は分析対象における説明変数 (Explanatory variable) や特徴量であり，センシティブ属性はその目的変数 (Target variable) と考えることができる．個人のプライバシーに配慮して準識別子やセンシティブ属性を大きく加工することは，最終的な統計量の誤差が発生することを意味するため，データ受領者にとって好ましくない．一般的に「有用性の高い匿名データ」とは，元データと比較して，値の変化量が少ないデータを指す．

しかし，一般的な統計調査においてでさえも，すべての値を分析対象として利用するのではない．たとえば年齢属性を 5 才刻み，10 才刻みなどに一般化するなど，データ組合せ数（次元）の削減手法が多く用いられている．

あらかじめ，データ受領者が 10 才刻みで顧客を分析することがわかっていれば，個人が識別される可能性が高い 1 才刻みのデータを使う必要はない．データ中の値が抽象化され，個人の識別性が低いデータでも，分析目的を達成できるならば，それはデータ受領者，データ提供者，データ主体のすべてのプレイヤーにメリットのある選択である．

安全性と有用性の関係は一般にトレードオフであるが，事前にデータ受領者の利用目的と攻撃者定義を詳細化することで，その有用性損失量をコントロールできる．そのため，多様なデータの利用方法に合わせた安全性指標と匿名加工手法が提案されている．

3. 匿名データへの攻撃モデル

3.1 リスク測定

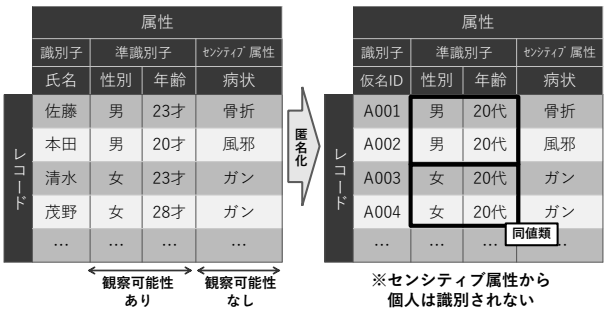
匿名データは信頼できないデータ受領者に提供される前提で作成されるため，データ主体について知識をもつデータ受領者から攻撃される可能性は否定できない．

Emam は匿名データ提供時に，以下の四つの起こりそうな攻撃のリスク測定を行う手法を提案している [3].

(1) 故意による再特定の試み：データ受領者がデータの再特定を試みる動機×再特定の成功率
(2) 故意でない再特定の試み：データ受領者がデータ主体の知人である可能性×再特定の成功率
(3) データ侵害：データ受領者がデータを紛失する可能性×再特定の成功率
(4) 公開データ：再特定の成功率

同書では「再特定」の成功率と記載されているが，文脈としては「特定の個人を識別」する成功率を指している．上記の (1)〜(4) までのリスクを算出したうえで，その最大値を漏洩リスクと定義し，リスクに応じてデータの提供可否を定める．

これらのすべての確率は (4) 再特定の成功率が基本となっている．そこで，次節から匿名データに含まれる特定の個人を識別するための攻撃モデルと，それを回避する安全性指標について記す．



第 3 図　レコード結合を防止する 2-匿名化の例

3.2 攻撃モデル

匿名データに対して行われる攻撃モデルについて，Fung[1] は 4 種類を定義し，それぞれに対応する安全性指標をまとめている．

レコード結合 (Record linkage) は，最も多く発生する攻撃モデルである．パーソナルデータにおける識別子，準識別子を用いて，ユーザの一意絞込み（シングルアウト）が発生する．それによって個人が識別され，公開してはならないセンシティブ情報が漏洩する．

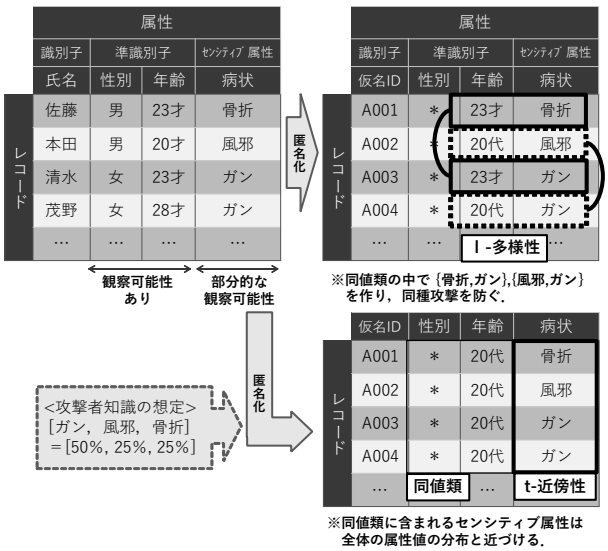
Sweeny は, [4] において，投票者リスト (Public voter list) に存在する名前と，医療履歴データベースに含まれる Zip コード，誕生日，性別を準識別子として結合することで，マサチューセッツ州知事の病気に関する情報を得ることができた．また，同様の手法を用いることで，米国国民の 87%を一意に識別することができることを報告した．

準識別子の組合せによって一意に絞込みされたデータを基点として，その人物のセンシティブ属性が判明するというプライバシー侵害が発生する．

そこで，第 3 図に示すように，パーソナルデータに含まれる準識別子を，より抽象的な概念に変更し，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 [4]．図中では，{ 男，20 代 }，{ 女，20 代 } の同値類が 2 個存在することで，2-匿名化を満たし，個人の識別可能性を 1/2 に低減させている．

また，k-匿名化は集合化や抽象化処理に着目し，ある個人に対する再識別確率という指標から生成されたため，データのかく乱やスワッピング処理などのデータ全体に対する確率調整処理を想定していない．そこでユーザを $1/k$ 以上の確信度に絞り込むことができないことを保証する指標として，**Pk-匿名性**が提案されている [5]．Pk-匿名性では，匿名化前と匿名化後のテーブルと値域，および匿名化手法とその確率変数を与えられた攻撃者を想定し，任意の個人が再識別される確率を $1/k$ 以下になるように加工したことを示す指標である．

属性結合 (Attribute linkage) は，攻撃者が準識別子とセンシティブ属性の関係を用いてプライバシーを侵害する攻撃である．属性結合による攻撃手法は**同種攻撃**



第 4 図　属性結合を防止する処理の例

と**背景知識攻撃**が知られている．

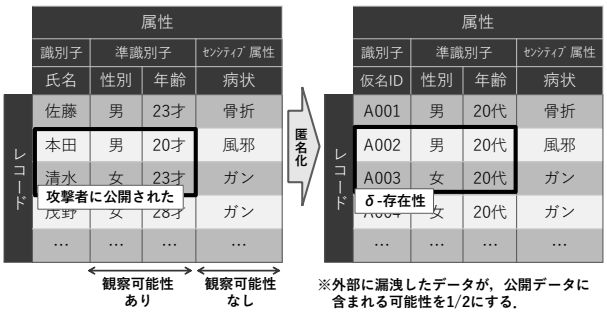
同種攻撃は属性値を抽象化した場合でも，その属性に含まれる内容が単一である場合に，センシティブ属性が推定される攻撃である．第 3 図では {女，20 代} の同値類を作成して 2-匿名性に加工したが「観察可能性ありの準識別子」と「観察可能性なしのセンシティブ属性」が同値類になっていることで，攻撃者は「女性で 20 代ならば，全員ガンである」と確信できる．これによって k-匿名化されているデータからでも，20 代女性に対してガン患者向けの広告を表示するなどの攻撃が可能である．

この解決手段として **l-多様性** [6] が知られている．第 4 図に l-多様性の状態を示す．ここでは性別の準識別子を削除し，年齢のみの準識別子を作成することで，2-匿名性かつ 2-多様性を満たすように加工した．

しかし，この攻撃者が，たとえばこのデータベース中に存在するセンシティブ属性の分布を知っている場合，同値類の偏りから値が知られてしまう場合がある．

背景知識攻撃は，準識別子とセンシティブ属性の組合せ，または属性値の出現数や分布の特性などから，センシティブ属性の値を知られてしまう攻撃である．解決手段として，元情報の属性値の出現数の分散と匿名化後の分散の差分を t 以下に抑制する，**t-近傍性** [7] が知られている．第 4 図の右下表では属性値の分布を知っている攻撃者知識に対応し，同値類に含まれるセンシティブ属性の出現率を $[50\%, 25\%, 25\%]$ とした．しかし，分布を同一にするために性別属性を削除しており，データの有用性が下がっている．

属性結合攻撃を防止する l-多様性や t-近傍性は，センシティブ属性を残すためにほかの準識別子を大きく加工する．そのため，安全性を強く設定すると元情報との乖離が大きくなる．また，その結果として守られるプライバシーの性質も，レコード結合における「特定」「識別」とは異なり，値が「推定」されるものである．センシティブ属性が推定された場合，レコード結合攻撃と組み合わさることで，強いプライバシー侵害が発生する可能性がある．



第 5 図　テーブル結合を防止する処理例

テーブル結合 (Table linkage) は，元となるパーソナルデータのレコードの一部が，過去に何らかの方法で攻撃者に公開されていた場合に，その知識を用いて匿名データから個人を再識別する攻撃である．第 5 図では本田と清水のレコードについて，外部に提供した事実がある場合を想定している．

δ-存在性 (δ-Presence)[8] は，このような公開データによる匿名性の漏れが発生する可能性を低減させる指標である．k-匿名化されたデータ中のレコードについて，過去に公開されたレコードが含まれる確率を δ %以下にすることで安全性を高める．

たとえば第 5 図の場合，A002 と A003 が攻撃者に知られている．その状態で右表の匿名データを作成する場合，過去に公開されたデータが占める割合は $\frac{|\{A002, A003\}|}{|\{A001, A002, A003, A004\}|} = \frac{1}{2}$ であり，すなわち (1/2)-存在性 である．

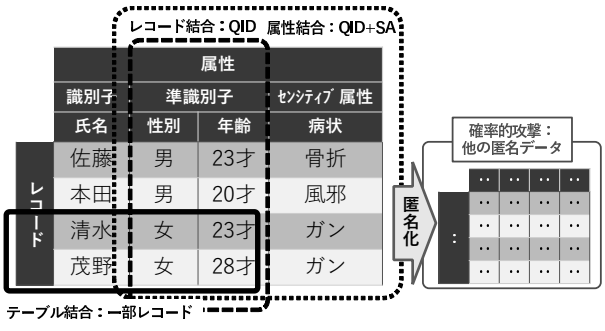
この処理によって攻撃者知識と対照される可能性を減少させてから，k-匿名化などの処理を行う．第 5 図の場合，{男，20 才}{女，23 才} が存在することが知られているため，2-匿名化して個人の識別性を低減させている．

確率的攻撃 (Probabilistic Attack) は，パーソナルデータにおけるレコードや属性値を用いるのではなく，過去に公開されたデータとの統計的差異を用いて行う．たとえば，定期的に提供した複数の匿名データについて，複数のデータの統計的差異を検証することで，変化した個人を識別する攻撃であり，差分プライバシーともよばれる．これは差分プライバシーの解説を参照いただきたい．

3.3　攻撃者知識に依存しないリスク低減処理

匿名データを作成する際には，公開する準識別子とセンシティブ属性を決定した後に，データ提供者がもつ攻撃のモチベーションと，それぞれの属性がどの程度の観察可能性を有しているかを想定して **3.1** 節にて述べた総合的なリスク評価を行う．

たとえば，攻撃者（データ受領者）がデータ主体の家



第 6 図　攻撃モデルと想定する攻撃者知識

族である場合には，非常に機微な情報を知っていると考えるが，攻撃する動機が少ないことも確かである．逆に海外から攻撃を受けた場合は，攻撃する動機は非常に高いが，知識は少ないと考えられる．

ある程度の攻撃者の設定とそのモチベーションが設定できた後に，前項までに述べた攻撃モデルを参考に，攻撃者の保持する元情報の種類を想定する．

第 6 図にて，各攻撃モデルにおける攻撃者知識について整理する．攻撃者が，準識別子を利用して個人を識別するのがレコード結合，準識別子とセンシティブ属性の関係によって値を推定するのが属性結合，元データを一部分知っている場合の攻撃がテーブル結合，同等のアルゴリズムで出力された，異なる匿名データを保持している場合は確率的攻撃，と分類することができる．

これらの攻撃モデルは，攻撃者が「元情報をどこまで知っているか」または「観察可能性があるか」などの条件設定によって，元情報を部分的に保持するという前提に立った，部分知識型モデルである．

しかし，これらの攻撃者知識を正確に想定することは困難である．また，作成時に定めた観察可能性は，その後も同じ安全性が維持されるという保証はない．

Emam は匿名データ作成後の，データ主体による自己開示の危険性について述べている [3]．匿名データの安全性はほかのデータ主体との識別不能性 (Indistinguishability) に依存しているため，あるデータ主体が属性を公開すると，類似した属性をもち（かつ，データ公開を望まない）ほかのデータ主体の情報が推定されるリスクが増加する．

このような，匿名データ作成後の部分的なデータ開示などのリスクに備えるため，観察可能性の想定に依存しない匿名化手法が必要とされる．例として，サンプリングと最大知識攻撃者モデルによる安全性検証方式がある．

サンプリングは元データをそのまま匿名化するのではなく，一定率の抽出を行い，データ主体が公開データに存在する確率自体を低下させる手法である．とくに医療や公共などの悉皆性のあるデータにおいて有効であり，ほかの匿名化手法と組み合わせて利用することで，より効果的に個人のプライバシーが保護される．

また，データ自体の安全性を検証する手法として Domingo によって**最大知識攻撃者モデル** (Maximum-knowledge attacker)[9] が提唱されている．このモデルにおいて攻撃者は，元データのすべての行・列の値，および匿名加工に用いたアルゴリズムの知識も保持している．この状態において匿名データを元情報と接続する攻撃を行い，その成功率を安全性と定義する．

このような強い攻撃者モデルは，それ以外の多くの部分知識型の匿名化指標・アルゴリズムが想定した前提を無視する形で行われるが，その反面，あらゆる匿名データを同一の条件で評価することができる利点がある．

これは，日本において匿名データを**提供元基準**で評価する，という考え方とも類似している．提供元基準とは，匿名データを作成したデータ提供者自体が，元のデータに戻せないことを求めるように匿名化するという安全管理措置の考え方である．

データ提供者は元データを保持しているが，匿名データと元データを接続する対照表を廃棄した後に，匿名データと元データとの再識別（ID の再紐づけ）に成功する確率を算出できれば，ほかの部分知識型攻撃の成功リスクはそれ以下であると定義できる．

しかし，最大知識攻撃者を想定した再識別攻撃は，データの種類や方式などに応じて変化するため，コンテストなどのルールが明確な範囲の中では成立する [11] が，実際のデータ利活用の現場において機能するかについては実証されておらず，今後の研究課題である．

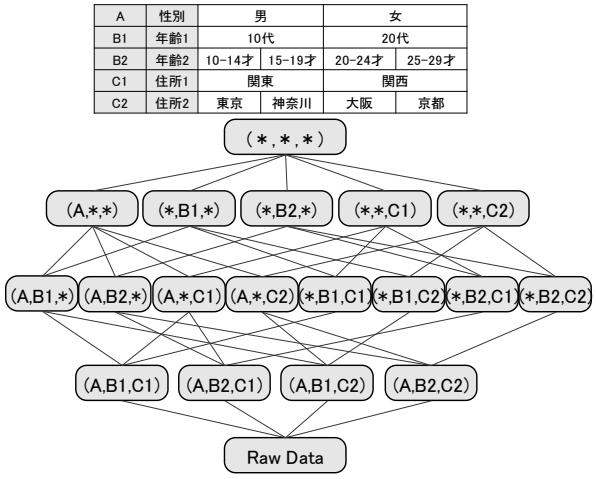
4. 匿名化アルゴリズム

3 章で詳述した攻撃者に対して匿名化を行うためのアルゴリズムについて記す．匿名化のアルゴリズムは，それぞれ利点や向いているデータ形式が異なるため，用途に応じて使い分ける必要がある．

まず，匿名化アルゴリズムは**大域的符号化 (Global recoding)** と**局所的符号化 (Local recoding)** に区分される．一般に大域的符号化とは，同じ属性値に対して一律に同処理を施す手法である．反対に局所的符号化は，同じ属性値であっても異なる処理を施す．たとえば，GPS 情報を匿名化する際に，出力結果を一律に都道府県レベルなどにそろえる場合は大域的，人口密度などによってクラスタや GPS メッシュのサイズを変更するなどの処理を局所的とよぶ．

また，属性値の書き換え方法として**一般化** (Generalization) と**かく乱** (Randomization) が存在する．一般化は値に対して，部分的な削除，桁の丸め，一般化階層木を適用するなどの手法で情報をぼやかし，同値類を作成することで k-匿名性などを実現する処理である．値を消去する**抑制**，および，概念の**集合化**をする処理（ [東京，神奈川]=[{ 東京，神奈川 }，{ 東京，神奈川 }] など）も大きくは一般化の一部と考えることができる．

逆にかく乱は，値に対してノイズ，スワップ，順列変更などの処理を加えることで元情報との接続性を失わせ，安全性を高める処理である．



第 7 図 格子構造 (Lattice Structure) の例

一般化とかく乱は使用に適した属性が異なっており，一般化はカテゴリー属性に向き，かく乱は数値属性に向いている．それぞれ，単一の属性を処理するものと，複数の属性を同時に処理するアルゴリズムがあるが，複数属性を同時に処理するものは指数的に処理回数が増加するため，最適な k-匿名化は NP 困難 [10] である．そこで，処理を効率化するアルゴリズムが多く提案されている．

4.1 k-匿名化アルゴリズム

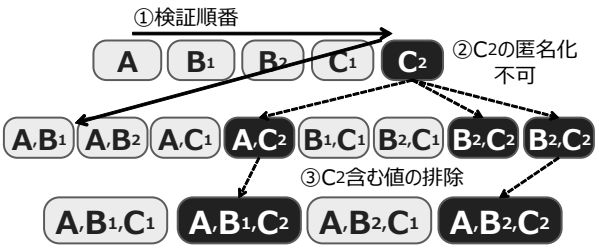
k-匿名化の代表的なアルゴリズムについて解説する．k-匿名化では，ある準識別子の属性値を一般化して，より抽象的な値に変更し，その結果，同じ準識別子をもつレコードが少なくとも k 個 ($k \geq 2$) 以上になるように書き換える．しかし，書き換えた結果が求めた安全性を満たさない場合，さらに抽象度の高い候補に書き換える処理を繰り返す．

本稿では，一般化を行うアルゴリズムについて大域的と局所的に行う例を示す．

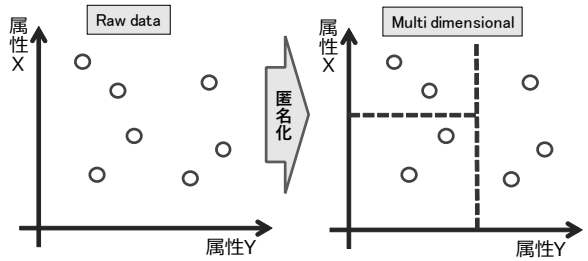
まず，大域的に行う場合に必要となる，属性の組合せの準備について示す．一般化階層を用いて k-匿名化処理を行う場合，第 7 図に示すような，属性の全組合せで格子構造 (Lattice Structure)[12] を作成し，それぞれ生成されるクラスタの最小サイズが，k-匿名性における k 値以上であるかを検証する．この検証作業は，属性の組合せ（次元）が大きいほど複雑になるため，検証回数が増加する．

また，組合せによっては，分析対象の削除や過度な変更が発生し，データ利用目的が損なわれる場合がある．そのため，使用する一般化階層はデータ利用者とあらかじめ協議し，利用可能なデータ区分になるよう調整する．最も抽象化した状態を＊（値の抑制）と考えて最上層に置き，最下層は元データとする．その間にデータ利用者が求める属性の変更候補を，概念が抽象的な順に並べて構築するのが一般的である．

Incognito[12] 方式は，大域的符号化の一般的な手法として知られている．構築した格子構造から，トップダウン型で属性の抽象化候補を探索し，属性値を抽象的な値に変換して匿名化を行う．第 8 図にてその概念図を示す．まず，最も情報量が少ない属性から順に値を変更していき，該当データが匿名性基準を満たすかの検証を行う．その際に，仮に C_2 が匿名性を満たさないことが検証された場合，C_2 を含む組合せを検証候補から排除し，探索する組合せ数を減少させる．



第 8 図 Incognito 方式による検証量削減方式の例



第 9 図 Mondorian における次元分割の例

つぎに，局所的な手法として，多次元分割手法を紹介する．**Mondrian**[13] は多次元の属性を分割することで匿名化を行う手法であり，m 個の属性をもつデータの k-匿名化を，m 次元における空間分割の最適化命題と考える．その概念図を第 9 図にて示す．Raw Data から開始し，属性値 X と Y の 2 軸に対して，すべての値が k-匿名性を満たすまで分割線を増加させ，データを詳細に区分していく．

複数の属性に対応する匿名化アルゴリズムとして Incognito と Mondrian を例として挙げたが，これらを含む多次元型の匿名化手法は，属性を組み合わせるごとに情報が詳細になり，匿名性を維持するのが困難となる．そのため，さらに強い抽象化や分割処理を施すことで情報の有用度が下がる，「次元の呪い」[14] という性質を有している．

そのため，最終的な分析目的の達成に必要なデータ以外を排除し，最小のデータ量で匿名化できるよう，データ受領者と合意することが最も重要である．

5. 課題とまとめ

本稿では，PPDP に関連する用語と技術の定義について述べ，関連する匿名化アルゴリズムについて解説した．これらの技術は，データ公開の安全性を高めるために一

定の効果があるが，すべてのプライバシー侵害に対して効果があるわけではない．

現代社会では，あるデータ主体のパーソナルデータは多くの機関・企業に保管されており，個人が意図しない企業に対しても，本当は開示されたくない内容が共有されている可能性がある．そのため，攻撃者知識の設定はますます困難となっており，現状では加工事例に基づくノウハウレベルで設定・運用がされている．このような攻撃者知識設定の定式化は今後の課題である．

また，世界的に見るとパーソナルデータに対する厳密な保護と管理に対する要求が強まっており，データ主体との適切な契約に基づいて匿名化の範囲を定めることが重要になってきている．

今後も，データ分析技術は向上し，プライバシー侵害事件も多様に変化するだろう．PPDP に求められるのは，技術としての正確性だけではなく，データ主体とデータ受領者が安心して利用できるように加工手法を公開・共有するなど，信頼性を向上させる手法である．

今後，匿名化技術を使用する企業の信頼性をベースとして，データの有用性と安全性のバランスを実現する研究が進展することを期待する．

(2018 年 8 月 23 日受付)

参 考 文 献

[1] B. Fung, K. Wang, R. Chen and P. S. Yu: Privacy-preserving data publishing: A survey of recent developments; *ACM Computing Surveys (CSUR)*, Vol. 42, No. 4, p. 14 (2010)

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY: Opinion 05/2014 on Anonymisation Techniques; *European Commission* (2014)

[3] K. E. Emam and L. Arbuckle: データ匿名化手法　ヘルスデータ事例に学ぶ個人情報保護, オライリー・ジャパン (2015)

[4] L. Sweeney: *k*-anonymity: A model for protecting privacy; *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, pp. 557–570 (2002)

[5] 五十嵐, 千田, 高橋: *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 2009(CSS2009) 論文集, pp. 1–6 (2011)

[6] A. Machanavajjhala, D. Kifer, J. Gehrke and M. Venkitasubramaniam: l-diversity: Privacy beyond *k*-anonymity; *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Vol. 1, No. 1, p. 3 (2007)

[7] N. Li, T. Li and S. Venkatasubramanian: t-closeness: Privacy beyond *k*-anonymity and l-diversity; *Data Engineering, ICDE 2007, IEEE 23rd International Conference on*, pp. 106–115 (2007)

[8] M. E. Nergiz, M. Atzori and C. Clifton: Hiding the presence of individuals from shared databases; *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, pp.665–676 (2007)

[9] J. D. Ferrer, S. Ricci and J. S. Comas: Disclosure risk assessment via record linkage by a maximum-knowledge attacker; *Privacy, Security and Trust (PST), 2015 13th Annual Conference on*, pp. 28–35 (2015)

[10] A. Meyerson and R. Williams: On the complexity of optimal k-anonymity; *Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, pp. 223–228 (2004)

[11] 菊池, 小栗, 野島, 濱田, 村上, 山岡, 山口, 渡辺: PWS-CUP: 履歴データを安全に匿名加工せよ; コンピュータセキュリティシンポジウム 2016 論文集, Vol. 2016, No. 2, pp. 271–278 (2016)

[12] K. LeFevre, D. J. DeWitt and R. Ramakrishnan: Incognito: Efficient full-domain *k*-anonymity; *Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data*, pp. 49–60 (2005)

[13] K. LeFevre, D. J. DeWitt and R. Ramakrishnan: Mondrian multidimensional *k*-anonymity; *Data Engineering, ICDE'06, Proceedings of the 22nd International Conference on*, pp. 25–25 (2006)

[14] C. C. Aggarwal: On *k*-anonymity and the curse of dimensionality; *Proceedings of the 31st International Conference on Very Large Data Bases*, pp. 901–909 (2005)

著 者 略 歴

小栗（おぐり）　秀暢（ひでのぶ）

1973 年生．1997 年早稲田大学第二文学部卒業．同年タイトー株式会社入社，2007 年よりニフティ株式会社にてデータ分析，プライバシー保護技術に関する研究開発業務に従事．2016 年に総合研究大学院大学複合科学研究科 情報学専攻修了．現在は富士通研究所に勤務．博士（情報学）．