［差分プライバシ］

2 差分プライバシの基礎と動向

寺田雅之 | NTT ドコモ先進技術研究所

「その場しのぎのプライバシ保護」からの決別

差分プライバシ (differential privacy) は，日本ではまだあまり実用例を聞くことは多くないが，米国では Google や Apple などの IT 企業が採用を進めるのみならず，公的機関が大規模に活用する段階まで実用化が進んできている．

2019 年 10 月に米国の国勢調査局[☆1]が“A History of Census Privacy Protections”と題されたパンフレット[☆2]（図 -1）を公開した．これは米国での国勢調査におけるプライバシ保護の歴史をすごろくのような形で年表化したものだが，その 2010 年のところに「その場しのぎのプライバシ保護 (ad-hoc privacy protections) を使う最後の国勢調査」との記載がある．

米国では国勢調査は 10 年に一度実施されるので，次は 2020 年――つまり今年である．2010 年を最後に「その場しのぎのプライバシ保護」から決別し，次はどうするか．

このパンフレットによれば「2020 年の国勢調査データは差分プライバシにより守られるだろう (2020 Census data products will be protected using differential privacy)」と高らかに宣言されている（図 -2）．

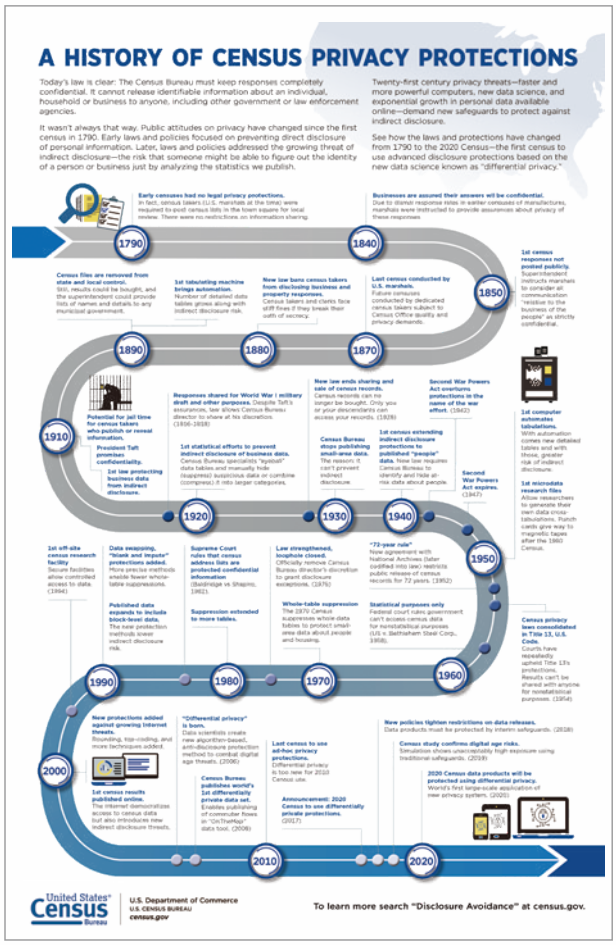

図 -1　米国国勢調査のプライバシ保護の歴史

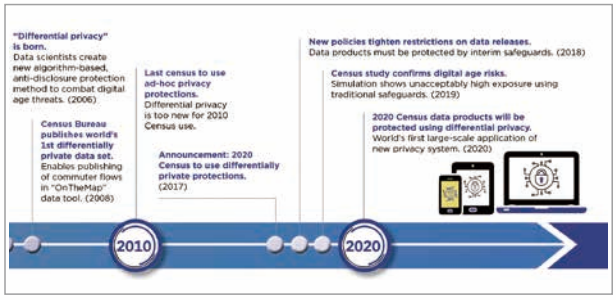

図 -2　2010 年以降を拡大

☆1 US Bureau of Census.「センサス局」と訳されることも多いが，本稿では同局の公式日本語サイトの表記にならい「国勢調査局」と記載する．

☆2 https://www.census.gov/library/visualizations/2019/comm/history-privacy-protection.html

なぜ差分プライバシか

米国国勢調査局は，なぜいままで自らが実施してきたプライバシ保護手段に対して「その場しのぎ(ad-hoc)」という言い方をしてまで差分プライバシを導入しようとしているのだろうか．その背景として，データの増加や計算機能力の向上によって（いままで現実的なリスクとして想定していなかった）プライバシ暴露への懸念が現実的になったこと，特にデータベース再構築(database reconstruction)と呼ばれる攻撃に対する脆弱性を無視できなくなってきたことが挙げられる[1]．

データベース再構築攻撃

データベース再構築攻撃とは，簡単に言えば，

- 複数の（それぞれ安全に見える）データを重ね合わせ，
- そこから導出される制約充足問題を解決する

ことによって，それらのデータに含まれる個人の情報を特定する攻撃である（図-3）．

この攻撃の強力なところは，一見して安全に見えるデータであっても，実際に攻撃を適用してみるとドミノ倒しのように多数の個人に関する情報が特定され得る（場合によってはすべての情報が特定されてしまう）ことにある．また，重ね合わせるデータの組合せが変われば導出される制約充足問題も変わるため，仮にある特定のデータの組合せがデータベース再構築に対して安全だったとしても，別のデータとの重ね合わせに対しても安全とは限らない．

この攻撃は計算量が大きい（NP困難とされる）制約充足の解決を必要とし，いままでは単なる理論的な可能性であるとして深刻に捉えられてこなかった．しかし，今日の計算機環境やSATソルバーなどの進化に伴い，米国国勢調査局のJ. M. Abowd氏はこの攻撃が「理論上のリスクから対策が求められる課題に変化した」☆3と表明している．

想定外といたちごっこ

これは，既知の攻撃やリスクに対しては安全なデータであっても「想定外」の新しい攻撃に対しては安全と言えないことを示している．

また，新しい攻撃が見つかって何らかの対策を施したとしても，次の「想定外」が見つかればさらに対策が必要となる．このような「いたちごっこ」をいつまでも繰り返しても安全を確信することはできない．また，攻撃への対策は何らかのデータの改変を伴うため，対策を重ねるたびにデータの有用性もどんどん低下することになる．

このいたちごっこから脱却するためには，（未知の攻撃も含めた）任意の攻撃に対して安全性を保証するようなプライバシ保護の枠組みが必要となる．

☆3 https://science.sciencemag.org/content/363/6423/114/tab-e-letters

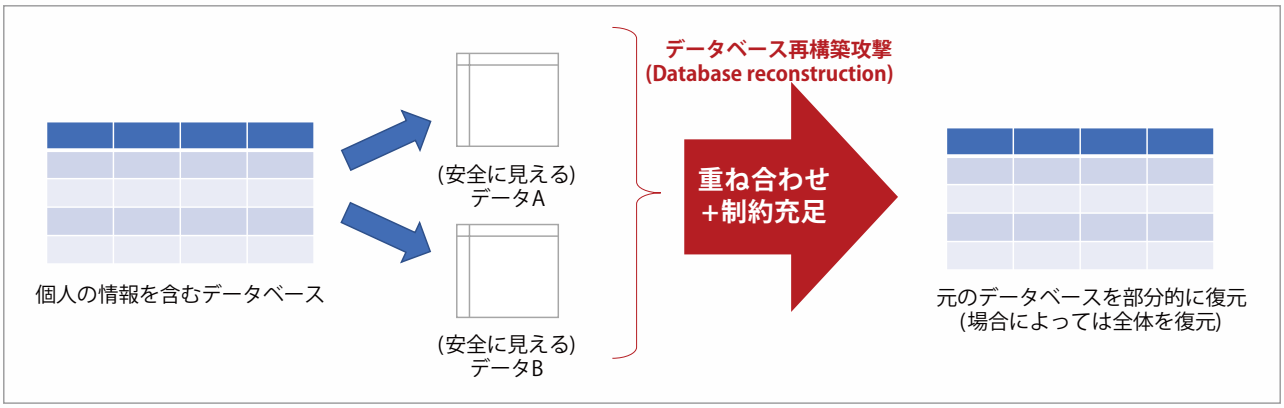

図-3　データベース再構築攻撃

差分プライバシの定義

差分プライバシは，この任意の攻撃に対する汎用的な（“ad-omnia”な）安全性を実現するためのプライバシ保護の枠組みであり，さまざまなプライバシ保護手段に対して統一的な安全性指標を与える．しばしば誤解されるが，差分プライバシ自体は**特定のプライバシ保護手段を表すものではない．**

差分プライバシを満たすプライバシ保護手段は「メカニズム」と呼ばれる．その代表例としてLaplace（ラプラス）メカニズムと呼ばれる手法がよく使われるが，Laplace メカニズムはあくまで差分プライバシを実現する手段の１つであって差分プライバシそのものではない．たとえばPRAM (post randomization) や幾何メカニズム (geometric mechanism) など，ほかにも差分プライバシを満たすメカニズムは数多く存在する．

差分プライバシは，これらのさまざまなプライバシ保護手段，すなわちメカニズムに対して統一的な安全性指標を提供する．この安全性指標は“ϵ”で表現され，以下の定義により与えられる．

定義 1. 任意の隣接したデータベース D_1 および D_2 ($D_1, D_2 \in \mathcal{D}$) に対し，ランダム化関数 (*randomized function*) $Q' : \mathcal{D} \to \mathcal{R}$ が下式を満たすとき，Q' は ϵ - 差分プライバシ（ϵ -*differential privacy*, 以下 ϵ -*DP* と略記する）を満たす．ただし，ここで S は Q' の出力空間 $\mathcal{R}$ の任意の部分空間である ($S \subseteq \mathcal{R}$).

$$\Pr[Q'(D_1) \in S] \leq e^{\epsilon} \cdot \Pr[Q'(D_2) \in S]. \qquad (1)$$

初めて見る人にとっては，そっとページを閉じたくなるような謎の定義だと思うが，後で直感的な説明を試みるので少しだけ我慢してほしい．

この定義において，ランダム化関数 Q' がそれぞれのメカニズムに相当する．ランダム化関数とは，計算結果に乱数ノイズを付与するなど，出力がなんらかのランダム性を持つ関数を表す[☆4]．

あるメカニズムが ϵ -DP を満たすとき，ϵ (≥ 0) の値が小さいほど安全性が高いとされる．$\epsilon = 0$ のときそのメカニズムは完全な安全性を持ち（ただし出力されたデータからは何の情報も得られない），$\epsilon = \infty$ ならば何の安全性も保証されない[☆5]．

差分プライバシの意味

さて，この差分プライバシの定義は何を意味するだろうか．一見しただけではそもそもプライバシ保護と何の関係があるかすら分かりにくい．そこで，以下に（なるべく）直感的な説明を試みる．

データベースとメカニズム

説明に先立って「データベース」と「メカニズム」を中心に用語を説明する．

データベースとは１つ以上のレコードから構成されるデータであり，それぞれのレコードは各個人に対応するものとする[☆6]．このデータベース (D とする）を加工し，なんらかの有益な情報を取り出すことを考える．

D から情報を取り出すための加工処理を問合せ (query) と呼び，Q と表記する．これには D から有益な情報を取り出すためのあらゆる処理が考えられる．たとえば平均や分散などの統計量の取得や，仮名化データの作成，クロス集計表やデータキューブなどの集計データの作成，D を学習データとした機械学習のモデル生成など，さまざまなデータ活用におけるデータの収集・加工プロセスは，すべて「問

☆4 つまり，差分プライバシを満たすメカニズムは原則として攪乱的 (perturbative) であると言える．

☆5 たとえば，一般に k- 匿名性を実現するためのアルゴリズムは差分プライバシを実現しない（$\epsilon = \infty$ となる）．これは，k- 匿名性はリンケージ攻撃以外（たとえばデータベース再構築攻撃）に対して安全性を保証しないことを反映している．

☆6 データベースが単一のレコードのみからなる（ある個人のデータしか含まない）とき，ここでの差分プライバシを特に局所（local）差分プライバシと呼ぶこともある．

合せ」として一般化して考えることができる．

ここで，問合せの出力 $Q(D)$ はデータ活用に有益な情報だけでなく，D に含まれる個々のレコードに関する情報をなんらかの形で含み得る．つまり，$Q(D)$ から個人のプライバシが暴露され得ることに注意が必要となる．

そこで，問合せによるプライバシの暴露を防ぎつつ有益な情報を得るために，$Q(D)$ をそのまま出力するのではなく，$Q(D)$ と似ているがプライバシ保護のための措置が施された $Q'(D)$ を出力することを考える．たとえば Q の出力の一部を確率的に変化させたり，Q の出力にノイズを加えたりして Q' を構成する．

この問合せ Q をプライバシ保護のために書き換えた Q' がメカニズムである（図 -4）．データ活用の観点からは，Q' の出力が持つ統計的性質が元の Q のそれをなるべく保持する☆7 ことが求められるが，あまり Q の出力と Q' の出力が似すぎているとプライバシが保護できない．つまりメカニズム Q' には有用性と安全性のトレードオフの関係が存在する．有用性については必要な統計的性質が定まれば定量的に評価できるが，Q' はどのような性質を持っていれば安全と言えるだろうか．

差分プライバシの定義が意味すること

メカニズム Q' の安全性について，定義 1 は「ϵ が十分に小さいとき，攻撃者はいかなる個人のプライバシも Q' の出力から確信を持って得ることはできない」ことを保証する．なぜこのようなことが言えるかについて，出題者と回答者の 2 人の間でのゲームを用いて考える．

このゲームにおいて，出題者は互いに隣接したデータベースである D_1 と D_2 を持ち，そのどちらかにメカニズム Q' を適用して出力 s を得る（どちらに適用したかは回答者に内緒である）．回答者は出題者から提示された s を見て，それが D_1 と D_2 のどちらから導出されたかを当てようとする（図 -5）．

ここで，データベースが互いに隣接するとは「1 つのレコードだけが違って，ほかのレコードはすべて同じ」ことを意味する．ここでは，たとえばデータベース D_1 に含まれているある 1 人（A さんとする）に関するレコードが D_2 では削除されており，その他のレコードは同一であるとする☆8．

また，Q' は問合せ Q を書き換えたものである．ここでは Q を「データベース中に含まれる，ある条件を満たすレコードの数」を数える問合せ（計数問合せ）とし，Q' はその出力に整数ノイズを加えてランダム化したものとする．

Q' はランダム化により確率的にふるまうため，$Q'(D_1)$ と $Q'(D_2)$ はいずれも確率変数となる．式 (1)

☆7 どのような統計的性質を保持すると有用であるかは応用による．

☆8 なお，隣接の定義として，このほかに「A さんのレコードだけが別の人のレコードにすげかえられている」とする場合もある．本来，どちらの定義を使うべきかはメカニズムによって使い分ける必要があるが，ここでの例（単一の計数問合せ）ではどちらの定義を使っても違いはない．

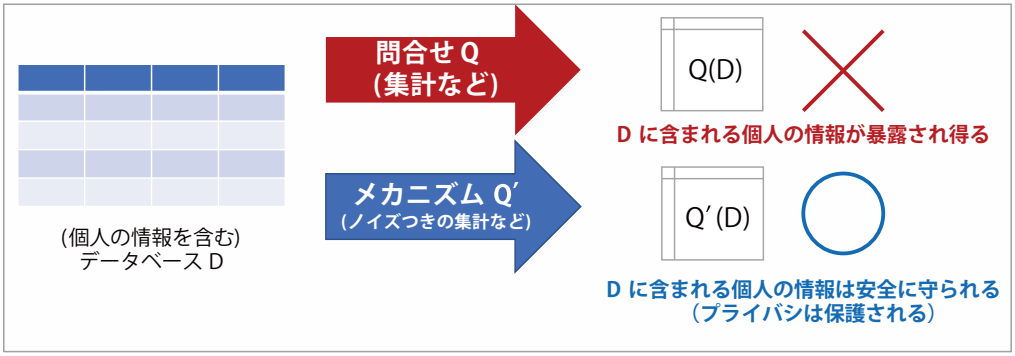

図 -4　問合せ Q とメカニズム Q′ の関係

は，$Q'(D_1)$ と $Q'(D_2)$ の分布が「ほとんど同じ」であること，すなわち任意の s に対して $\Pr[Q'(D_1)=s]$ と $\Pr[Q'(D_2)=s]$ の比が最大でも $e^{\epsilon}:1$ を超えないことを求める．このような性質を満たすノイズとしては，両側幾何分布に従う乱数や，Laplace 分布に従う乱数を（小数点以下を丸めて）離散化したものなどが挙げられる☆9．

このとき，ϵ が十分に小さければ，$Q'(D_1)=s$ となる確率と $Q'(D_2)=s$ の確率がほとんど同じになるので，回答者は s が D_1 と D_2 のどちらから導出されたのかを見分けようがない．ここで，（そもそも A さんの情報を含まない D_2 より得られた）$Q'(D_2)$ から A さんのプライバシが暴露されることはあり得ないため，それと見分けがつかない $Q'(D_1)$ から A さんのプライバシが暴露されることもない．したがって，A さんのプライバシは任意の攻撃から守られる．

より正確には，$\epsilon=0$ でない限り，上記の 2 つの確率の違いから，出力 s を得た回答者はそれが D_1 と D_2 のどちらに由来するかを推測することはできる．しかし，片方の確率が 0 となることはない☆10 ため，回答者はこれを確信することはできず，その推測結果にかならず過誤が発生し得る☆11．つまり出題者は回答者の推測に対して「それは決めつけだ」と否認する余地がある（否認可能性 (plausible deniability) が与えられる）．

D_1 と D_2 は（$\mathcal{D}$ 上の）「任意の」隣接したデータベースであるため，これはデータベースの中身がどのようなものであっても成立し，A さんではなく他のレコードに対応する人，つまり B さんでも C さんでも任意の人に関して同様に成立する．

すなわち，Q' が ϵ-DP を満たすとき，Q' は（$\mathcal{D}$ 上の）任意のデータベースに含まれるすべての人に関して上記の安全性を提供する．

差分プライバシの特徴

差分プライバシは，ϵ-DP を満たすメカニズムに対して，その実現方式にかかわらず，ϵ の値に応じた安全性を共通的に保証する．これは，異なるプライバシ保護方式の間で安全性を比較するための共通の物差しを与え，安全性を揃えた上で有用性を比較することを可能にする．また，合成定理 (com-

☆9 前者は幾何メカニズム，後者は Laplace メカニズム（に対して整数丸めという事後処理をしたもの）に相当する．

☆10 もしどちらかの確率が 0 になることを許すと式 (1) が成立しなくなる．「任意の隣接するデータベース」という条件から D_1 と D_2 を入れ替えても成立が求められることに注意．

☆11 どの程度「確信できない」かは，たとえば検定における検出力の上限（検出力が有意水準の e^{ϵ} 倍を超えることはない）として与えられる．

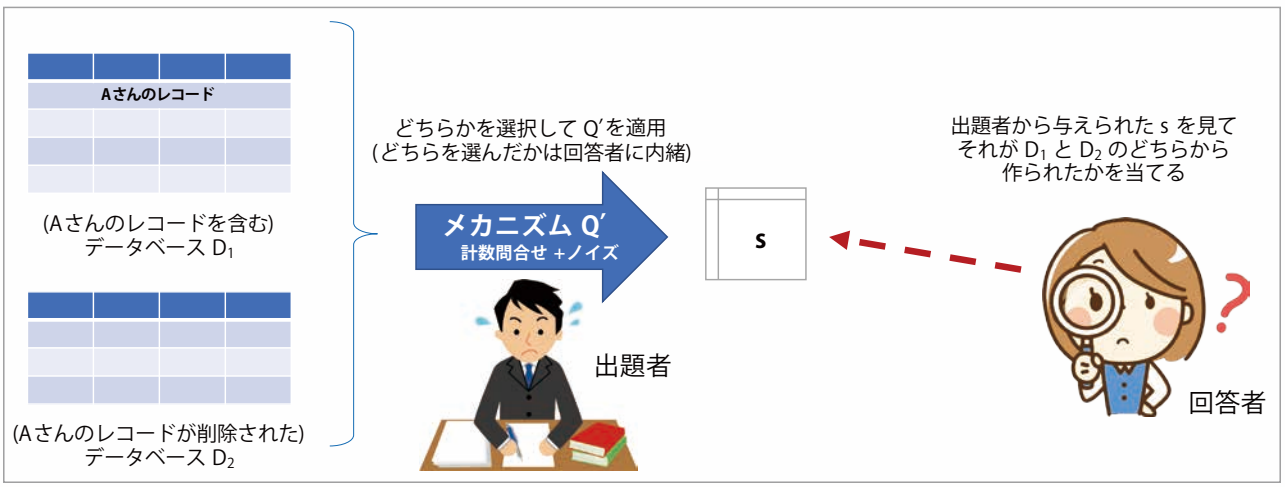

図 -5　ゲームの概要

position theorem)[☆12] と呼ばれる強力な定理により，差分プライバシを満たす新しいプライバシ保護方式を，既存の方式から組み合わせて構築できることを可能にする．

異なる方式間の安全性の比較

データベースからなんらかの情報を安全に取り出したいとする．それを実現するプライバシ保護方式が複数あるとき，どの方法を使うことが最も望ましいだろうか．差分プライバシは，この意思決定をするために必要となる，安全性に関する共通的な指標を与える．

あるデータベースに含まれるレコードを属性値の組合せごとに集計して分割表（クロス集計表）[☆13] を作成することを考える．たとえばある試験結果のデータベースから男女別の合否人数に関する集計結果をまとめたもの，つまり（男性，女性）×（合格，落第）の 4 つのセルにそれぞれ該当人数を記入したものが分割表に相当する．

安全な分割表を出力するための方式としては，分割表のそれぞれのセルの値に乱数ノイズを加える方法や，元のデータベースの一部を「男性→女性」「合格→落第」などとランダムに書き換えてから（普通に）集計する方法などがある．たとえば Laplace メカニズムは前者に相当し，PRAM は後者に相当する．さて，どちらがより安全に有用性が高いデータを出力できるだろうか？

このような問いに対し，差分プライバシは安全性指標である ϵ に基づいた比較を可能にする．つまり，それぞれの方式において ϵ という共通の物差しを使って安全性を揃えた上で，それぞれの方式の有用性を比較すれば，どの方式を用いるのが最適であるかを決めることができる[☆14]（図 -6）．

別の言い方をすれば，新たなプライバシ保護の手法を考案したとき，上記の定義に照らし合わせて ϵ の値を計算することができれば，その手法は ϵ の値に応じた安全性を持つことが保証される．つまり，考案した新たな手法について，安全性の基準を揃えた上で従来の手法に対するメリットやデメリットを比較することが可能になる[☆15]．

☆12 後述の並列合成定理との対比から，直列合成定理（sequential composition theorem）とも呼ばれる．
☆13 集計対象となる部分集合が互いに素となる集計表．
☆14 なお，有用性の指標を元の分割表との誤差としたとき，一般に Laplace メカニズムのほうが PRAM より有用性が高い（誤差が小さい）[2]．
☆15 これがないと「ぼくのかんがえたさいきょうのほうしき」が本当に最強かどうか比べようがないので，プライバシ技術の健全な発展のために実はけっこう重要な性質である．

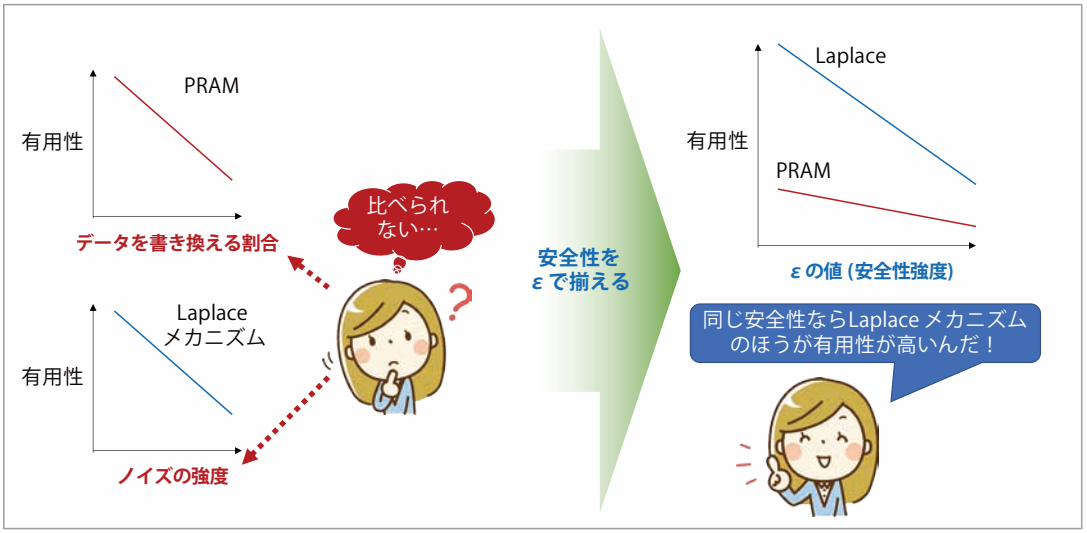

図 -6　安全性指標 ϵ を共通の物差しとして比較

合成定理

合成定理は，複数のメカニズムを合成したときの安全性を与える定理であり，以下で示される．

定理 1. それぞれ ϵ_i-*DP* を満たす n 個の問合せ Q'_i があり，Q' はそれらの Q'_i の列挙，つまり $Q'(D) = (Q'_1(D), Q'_2(D), \ldots, Q'_n(D))$ とする．このとき，Q' は $(\sum_{i=1}^{n} \epsilon_i)$-*DP* を満たす（図 -7）．

この定理は，複数のメカニズムを組み合わせて，新しい（より複雑な）差分プライバシを満たすメカニズムを構成することを可能にする．たとえば，ϵ_1-DP を満たすメカニズム Q'_1 と ϵ_2-DP を満たすメカニズム Q'_2 があるとする．このとき，$Q'(D) = f(Q'_1(D), Q'_2(D))$ として Q' が構成されるなら[☆16]，Q' は $(\epsilon_1 + \epsilon_2)$-DP を満たすことが保証される．

また，この定理は，差分プライバシを満たすメカニズムがデータベース再構築攻撃に対して一定の安全性を持つことを保証する．たとえば攻撃者がデータベース D から出力された $Q'_1(D)$ と $Q'_2(D)$ を得たとする．これらを重ね合わせて得られる任意の出力は，合成定理により $(\epsilon_1 + \epsilon_2)$-*DP* を満たすメカニズムの出力であるとみなせる．つまり，これらの重ね合わせによりどのような制約充足問題を得たとしても，$(\epsilon_1 + \epsilon_2)$-DP が与える安全性を超えて攻撃者が情報を得ることはない．

なお，合成定理の特殊な場合として，**定理 1** において Q'_i が適用されるレコードの集合が互いに素であるとき，Q' にはより強い安全性が与えられる．これを並列合成定理（parallel composition thorem）と呼び，具体的にはこのとき Q' は $(\max_i \epsilon_i)$-DP を満たす．

並列合成定理は，たとえば分割表を作成する際に，表の次元数（セル数）が増えても各セルに加えるノイズの強度は同じでよい（安全性は変わらない）ことを保証する．この性質は，たとえば国勢調査のような大規模な集計データのプライバシを保護するにあたって特に有用である．

☆16 f は任意の関数であるが，$Q'_1(D), Q'_2(D)$ のほかに D から導出された値を参照しないものとする．

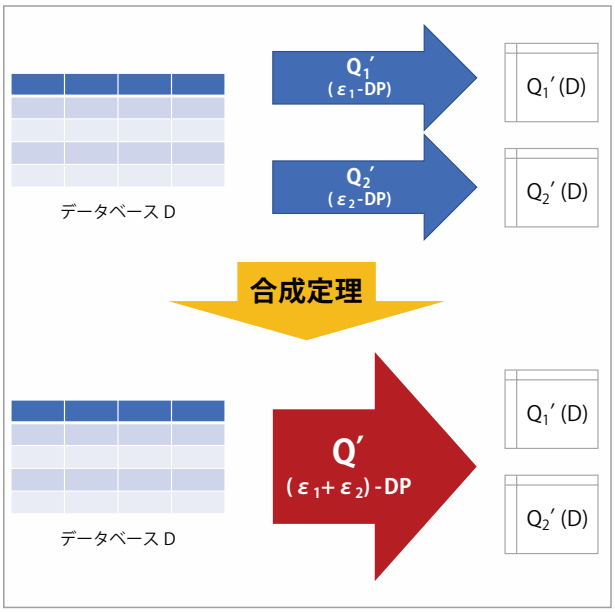

図 -7　合成定理

課題と今後の展望

差分プライバシはさまざまな有用な特徴を備え，その実現も簡単[☆17]であるが，まだ日本では普及が進んでいるとは言えない．何が導入を阻害しており，その解決には何が求められるのだろうか．

定義と ϵ の直感的理解の難しさ

まず 1 つに，定義 1 の直感的な理解の難しさが挙げられる．一見だけでこの定義が何を意味を持つことを理解するのは難しい（筆者自身も，最初に見たときはまったく分からなかった）．本稿が理解の一助となれば幸いであるし，今後さらに一般向けの解説が充実していくことが期待される．

また，このことにも関係するが，ϵ の値をいくつに設定すべきかが分かりにくいことも課題である．式 (1) を見ても ϵ の値がどの程度の安全性を意味するかは直感的に分かりにくい．また，ϵ がいくつで

☆17 たとえば Laplace メカニズムは，Python+NumPy なら一行で実装できる．

あれば十分に安全として社会的に認知されるかは，数式だけで定められるものではない．

ただし，冒頭で紹介した米国国勢調査局による差分プライバシの採用は，この ϵ の値の決定に関する問題への初めての大規模な取り組みと捉えることもできる．ϵ の値を決定するにあたっての考え方や具体的な値などについて，信頼できる公的機関による先行事例ができることによって状況が大きく変化していくことも考えられる．今後の動向に注目していきたい．

差分プライバシは厳しすぎる?

差分プライバシに対するよくある批判として，差分プライバシは厳しすぎる（データの有用性が不足する）というものがある．しかし，その理由が差分プライバシの定義が厳しすぎるためとは限らない．そもそもプライバシリスクが高すぎるデータを出力しようとしていたり，用いるメカニズムが適切ではなかったりすると，当然ながら有用なデータは得られない．

たとえば行動履歴データを匿名化して提供しようとする場合など，出力するデータが細かすぎると適切な ϵ を満たした上で高い有用性を持つ出力を得ることは困難である．しかし，このようなデータはそもそもプライバシ暴露のリスクがとても高いデータであり，差分プライバシは「適切に」そのリスクの高さを反映しているだけとも考えられる．差分プライバシを適用する以前に，安全性と有用性のトレードオフの観点から適切な粒度でデータを出力するように設計する，というプライバシ保護の鉄則を十分に検討することが重要である．

また，差分プライバシは安全性に関して統一的な保証を与えるが，その有用性はメカニズム次第である．差分プライバシを満たすメカニズムは無数に存在☆18し，それぞれ出力の統計的性質は異なる．つまり，応用ごとに適切なメカニズムは異なるものであり，不適切なメカニズムを用いると十分な有用性は得られない．たとえばPRAMはほとんどの問合せに適用可能な汎用性が高いメカニズムであるが，前述の通りこれを分割表の保護に使っても適切な ϵ の元に有用な出力を得ることは難しいだろう．

これまでの研究により，さまざまな応用に向けたメカニズムの提案や改善が進められている[3), 4)]．特に，近年では深層学習などの機械学習において差分プライバシに基づくプライバシ保護を実現する研究も活発になされている．差分プライバシの実用にあたっては，これらを参考に応用ごとに適したメカニズムを選択することが重要であるとともに，今後の技術の進展によるさらなるメカニズムの充実が期待される．

差分プライバシの先へ

ただし，定義1の要求が厳しすぎる側面がまったくないかというと，そうとも言い切れない．たとえば，あるメカニズムが任意の攻撃に対して一定の安全性を備えていても，それが ϵ として表せないケースも存在する．最後に，この ϵ では捉えきれない安全性に関する取り組みについて簡単に紹介する．

差分プライバシを実現するメカニズムとしてはLaplaceメカニズム（Laplaceノイズの加算）が代表的だが，より一般的な正規分布に従うノイズの加算（Gaussメカニズムと呼ばれる）では駄目なのだろうか．答えは駄目で，実際に定義1に照らして計算してみると $\epsilon = \infty$ となり，Gaussメカニズムは差分プライバシにおいて安全ではない．

これは，正規分布の裾のほうの極限遠点，つまり実際には値が発生することがあり得ないような領域で，式(1)における2つの確率の比が発散してしまうことによる．しかし，このようなほぼ発生しないことが明らかな（想定外の攻撃にはなり得ない）事象のために「安全ではない」としてしまうことは，安全性定義として厳しすぎる側面があるとも言える．

☆18 合成定理の存在から，任意のメカニズムの合成により新しいメカニズムを作り出すことができる．

(ϵ, δ)- 差分プライバシ

そこで，差分プライバシの変種として「ある一定以下の確率でなら，出力が差分プライバシを満たさないことを許容する」指標が提案されている．これを (ϵ, δ)- 差分プライバシ ((ϵ, δ)-DP) と呼び[☆19]．定義 1 における式 (1) を以下に置き換えたものとして定義される．

$$\Pr[Q'(D_1) \in S] \leq e^{\epsilon} \cdot \Pr[Q'(D_2) \in S] + \delta .$$

この式は式 (1) の右辺に δ を足したものであり，$\delta = 0$ のとき (ϵ, δ)-DP は ϵ-DP と等価となる．この定義も差分プライバシと似た安全性や合成定理を与えるが，$\delta > 0$ のとき，$\Pr[Q'(D_1) \in S] > 0$ かつ $\Pr[Q'(D_2) \in S] = 0$ となり得ることに注意したい．これは，メカニズムの出力値によっては，それが D_1 由来か D_2 由来かを攻撃者は決定的に知ることができてしまう（プライバシが決定的に暴露される）可能性があることを意味する[☆20]．

つまり，プライバシ保護において否認可能性を重視する立場からは，(ϵ, δ)-DP は安全性定義として逆に「ゆるすぎる」ところがあると言える．

レニー情報量に基づく定義

2016 年頃から議論されはじめた比較的新しい変種として，式 (1) の代わりにレニー情報量 (Rényi divergence) を用いて $Q'(D_1)$ と $Q'(D_2)$ の分布の近さとする定義が挙げられる（文献 5)，6）など）．具体的な安全性定義に少しずつ差異があるが，これらはいずれも決定的なプライバシ暴露の危険を排しつつ，Gauss メカニズムの安全性を定義可能にする点で共通している．また，これらの安全性定義の元では差分プライバシより効率良くメカニズムを合成できる（合成による安全性の低下が小さく抑えられる）という特徴を持つ．

ただし，これらの定義が与える安全性は差分プライバシと似て非なるものである．その解析は差分プライバシほどには進んでおらず，定義の解釈も差分プライバシよりさらに難しい（レニー情報量の概念の理解を必要とする）．そのため実用までの道程はまだ険しいと考えられるが，Gauss メカニズムの安全性を定義可能なことやメカニズム合成の効率が良いことは，高い有用性を備えた新しいメカニズムの構築に有効な性質である．プライバシ保護における，より高いレベルでの安全性と有用性のトレードオフの実現への期待から，今後の議論の進展に注目したい．

☆19 本来の差分プライバシと異なる（より弱い定義である）ことを明確にするために，(ε, δ) - 弱 (weak) 差分プライバシ，もしくは近似 (approximate) 差分プライバシとも呼ばれる．

☆20 なお，Gauss メカニズム自体は決定的なプライバシ暴露を起こさない．

参考文献

1) Garfinkel, S., Abowd, J. M. and Martindale, C. : Understanding Database Reconstruction Attacks on Public Data. ACM Queue, 16(5):28-53 (Oct. 2018).
2) 寺田，山口，本郷：匿名化個票開示への差分プライバシの適用，情報処理学会論文誌，58(9):1483-1500 (Sep. 2017).
3) Dwork, C. : Differential Privacy : A Survey of Results. In Proc. 5th Intl. Conf. Theory and Applications of Models of Computation, pp.1-19. Springer (2008).
4) Zhu, T., Li, G., Zhou, W. and Yu, P. S. : Differentially Private Data Publishing and Analysis : A Survey. IEEE Trans. Knowledge and Data Engineering, 29(8):1619-1638 (Aug. 2017).
5) Bun, M. and Steinke, T. : Concentrated Differential Privacy : Simplifications, Extensions, and Lower Bounds. In Theory of Cryptography, pp.635-658 (Nov. 2016).
6) Mironov, I. : Rényi Differential Privacy. In Proc. 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp.263-275 (Aug. 2017).

(2020 年 3 月 2 日受付)

■寺田雅之（正会員） teradam@nttdocomo.com

携帯電話ネットワークの運用データに基づく人口統計の作成と交通渋滞予測などの社会予測への応用，および大規模データのプライバシ保護に関する研究に従事．2017 ～ 2018 年度 CSEC 研究会主査．博士（工学）．