# 海外における公的統計に対する攪乱的手法の新たな取り組み
## ―アメリカセンサス局による差分プライバシーの適用を中心に―

伊藤　伸介[†]

寺田　雅之[††]

赤塚　裕人[‡]

北井　宏昌[‡‡]

## Perturbative Methods for Official Statistics: Application of Differential Privacy by the U.S. Census Bureau

ITO Shinsuke
TERADA Masayuki
AKATSUKA Hiroto
KITAI Hiromasa

差分プライバシーの公的統計への適用可能性が、海外の統計作成部局において議論されている。アメリカセンサス局は、2020年人口センサスにおける統計表の作成・公表において、差分プライバシーの方法論の適用を進めてきた。それは、「データベース再構築攻撃」が、統計表に含まれる個体情報を特定化するリスクを高める意味で脅威になっているからである。一方、イギリス国家統計局やドイツ連邦統計局は、オーストラリア統計局のオンデマンド集計システムであるTableBuilderを参考にして、集計表の各セルにランダムなノイズを付与するcell key methodの実用性を追究している。本稿では、アメリカセンサス局による差分プライバシーの適用例を中心に、海外における公的統計に対する攪乱的手法の新たな取り組みについて議論する。欧米諸国におけるこうした海外事例は、わが国における公的統計の将来的な公表のあり方を議論する上での有力な参考事例になると思われる。

キーワード　差分プライバシー、データベース再構築攻撃、アメリカ人口センサス、cell key method

National Statistical Institutions in various countries are currently investigating the introduction of differential privacy. The U.S Census Bureau adopted the methodology of differential privacy to the creation and publication of statistical tables for the 2020 Population Census. The underlying reason is that “database reconstruction attacks” can increase the risk of individuals being identified based on information contained in the tables. The Office for National Statistics in the U.K. and German Federal Statistical Office are investigating the cell key method which adds random noise to each cell in a statistical table based on TableBuilder, the remote execution system developed in the Australian Bureau of Statistics. This paper discusses the introduction of perturbative methods for official statistics in countries other than Japan, mainly the current situation regarding the application of differential privacy by the U.S. Census Bureau. These examples from European countries and the United States provide an important reference for discussing the future publication of official statistics in Japan.

Keywords: Differential Privacy, Database Reconstruction Attack, U.S. Population Census, cell key method

[†] 中央大学経済学部　Email:ssitoh@tamacc.chuo-u.ac.jp
[††] (株)NTTドコモ　Email: teradam@nttdocomo.com
[‡] (株)NTTドコモ　Email: hiroto.akatsuka.fb@nttdocomo.com
[‡‡] (株)NTTドコモ　Email: hiromasa.kitai.us@nttdocomo.com

## 1. はじめに

情報工学の分野において議論されてきた差分プライバシー(differential privacy)の公的統計への適用可能性が、海外の統計作成部局において模索されている。例えば、アメリカセンサス局(以下「センサス局」と略称)は、アメリカ人口センサス(以下「センサス」と略称)における公表可能な統計表を作成するために、2020 年センサスにおいて差分プライバシーの本格的な適用を進めてきた。

Abowd(2018)によれば、統計作成部局は、地域区分が細かい統計表を作成・公表していることから、ミクロデータが公開されてない場合であっても、このような地域区分が詳細な公表された統計表を組み合わせることによって、個体を特定するリスクが高まることが指摘されている。センサス局内部では、こうした差分攻撃(differencing attack)に対する実証的な研究がなされてきた。このような特定化のリスクを回避するためには、統計表に含まれる結果数値の精度を考慮しながら、ノイズを付与することによって、安全な統計表を公表することが求められる。その場合、集計表のセルの度数に対してランダムノイズを付与することによって、集計表を提供するオーストラリア統計局の TableBulder のようなオンデマンド型のシステムも存在する(伊藤・谷道・小島(2018))。TableBulder の方法論を参考にした上で、イギリスやドイツでは、小地域レベルの集計表に対する攪乱的手法として cell key methods の可能性が追究されている。また、人口センサスの統計表を作成する元データに対して、スワッピング(data swapping)を適用したイギリス国家統計局の事例もある。それに対して、差分プライバシーの方法論を統計の実務レベルで全面的に導入しようとしているのがセンサス局であって、こうした動きは、ヨーロッパ諸国等の他国とは大きく異なる取り組みだと言える。

差分プライバシーはプライバシーの定義として妥当性を有しているだけでなく、統計作成部局においてデータの精度に関する評価基準が整備され、差分プライバシーの公的統計への適用が実用に耐えうるものになってきたことが指摘できる(伊藤・寺田(2020))。このことから、ノルウェー統計局等の欧米の統計作成部局でも、公的統計における差分プライバシーの可能性に対する注目が高まっている(Heldal et al.(2019))。また、わが国においても、例えば、寺田他(2015)によって考案された、差分プライバシーの方法論の国勢調査のメッシュデータに対する適用可能性に関して実証研究が進められてきた(Ito et al.(2019), 伊藤・寺田(2020))。

このように、海外では、一方では差分プライバシーの適用、他方では cell key method の適用可能性の検討という多様な方向で、公的統計への攪乱的手法の実用性が追究されている。本稿では、海外におけるこうした状況を踏まえた上で、センサス局における差分プライバシーの方法論の実用化に向けた取り組み状況を中心に、攪乱的手法の適用に関する展開方向を洞察する。

## 2. ヨーロッパ諸国における公的統計データへの攪乱的手法の適用状況

ヨーロッパ諸国では、各種の公的統計ミクロデータの作成・提供において様々な匿名化措置が施されてきた。匿名化措置が施された公的統計ミクロデータは、その秘匿性の程度によって、学術研究用の匿名化ミクロデータ(anonymized microdata)と一般公開型ミクロデータ(public use microdata)に類別される。前者は学術研究用ファイル(Scientific Use File = SUF)、後者は一般公開型ファイル(Public Use File = PUF)という形でヨーロッパ諸国において作成・提供されている(伊藤(2018))。また、ヨーロッパではオンデマンド集計システムを含むリモートエグゼキューションも展開されている。本節では、ヨーロッパ諸国における公的統計データに対する攪乱的手法の適用状況について概括する。

2.1 匿名化ミクロデータの作成に向けた攪乱的手法の適用状況

ヨーロッパでは、匿名化ミクロデータの作成のために、様々な攪乱的手法が用いられている。世帯・人口系のデータについては、イギリスの人口センサスを例に挙げると、学術研究用の匿名化ミクロデータの作成にあたって、元データとなる個票データにランダム・スワッピング(random data swapping)やターゲット・スワッピング(targeted data swapping)が採用されたことが指摘できる。さらに、教育用の公開型ミクロデータの作成においても、スワッピングを適用したことが知られている(伊藤(2020a))。また、オランダ統計局は、匿名化ミクロデータの作成において、PRAM(=Post Randomization Methods)を適用している(伊藤(2020b))。

事業所・企業系の統計調査における匿名化ミクロデータの作成事例は少ないが、イタリアやドイツでは、事業所・企業系の匿名化ミクロデータの作成の展開がされてきた。例えば、イタリアでは、イタリア国立統計研究所(ISTAT)において、2020 年現在、企業のイノベーション活動に関する統計調査である Community Innovation Survey(CIS)の匿名化ミクロデータが作成されている。CIS については、SUF や PUF が提供されている(伊藤・横溝(2021, 4 頁))。これらのミクロデータの作成においては、ミクロアグリゲーションが採用されていることから、事業所・企業系の匿名化ミクロデータにおける攪乱的手法の適用が指摘できる。

つぎに、ドイツにおいては、ドイツ連邦統計局が、事業所・企業系の統計調査を対象に、PUF や SUF だけでなく、教育目的のために秘匿の強度を上げた campus file(CF)の形で匿名化ミクロデータの作成を進めてきた。ドイツにおけるミクロデータの匿名性の考え方としては、「事実上の匿名性(factual anonymity)」[1]という概念があり、事実上の匿名性の概念に基づく事業所・企業系の匿名化ミクロデータの作成可能性が追究されてきた。具体的には、事業所・企業系のミクロデータを研究者が利用可能にすることを目指した「企業ミクロデータに関する事実上の匿名化」プロジェクト(Factual Anonymisation of Business Micro Data)( 2002 年～2005 年) (Lenz et al. (2006))において、SUF の作成にあたって、ミクロアグリゲーションやノイズ付加(加法ノイズ、乗法ノイズ)等の攪乱的手法の適用可能性が定量的に評価された。さらに、「企業パネルデータに関する事実上の匿名化」プロジェクト(Business Statistics Panel Data and Factual Anonymisation)(2006 年～2008 年) (Brandt et al. (2008))では、縦断的なリンケージによるパネルデータの作成のために、ミクロアグリゲーション、乗法ノイズ、多重代入法(multiple imputation)による検討がなされている(伊藤・横溝(2021))。

このように、ヨーロッパにおいて、公的統計ミクロデータに対する匿名化手法として、リコーディング等の非攪乱的手法だけでなく、ノイズ、スワッピング、さらにはミクロアグリゲーションといった攪乱的手法も採用されていることは注目に値する。

2.2　リモートエグゼキューションにおける攪乱的手法の適用

ヨーロッパ諸国では、個票データのアクセスサービスについては、オンサイト施設やリモートアクセス施設といったセキュアな環境での個票データの利用サービス、プログラム送付型のリモートエグゼキューションのような個票データに直接アクセスしない形での分析結果の提供等、多様な提供形態を指摘することができる[2]。

---

[1]「事実上の匿名性(factual anonymity)」とは、「著しく大きな時間，経費および労力の支出によって，当事者に関連づけることができない」ことである。事実上の匿名性の特徴については、濱砂(1999)を参照されたい。

[2] 例えば、オランダは、1998 年からオランダ統計局内部でのオンサイト施設による個票データの利用が開始された。また、2006 年からは、リモートアクセスによる個票データの利用が可能になっている。さらに、デンマークは、2001 年からリモートアクセスによる個票データの利用サービスが開始された。1988 年より運用されていたデンマーク統計局のオンサイト施設によるサービスは 2008 年に廃止され、現在はリモートアクセスのみによる個票データの利用が可能になっている(伊藤(2020b))。プログラム送付型のリモートエグゼキューションに関し

Eurostat では、Confidentiality on the fly と呼ばれるオンデマンド集計システムに基づくリモートエグゼキューション(リモート集計)が議論されてきた。オンデマンド集計システムにおいては、集計前の元データに攪乱的な手法を適用するのではなく、作成・提供される集計表に対して攪乱的な秘匿処理の方法が検討されてきた。例えばオーストラリア統計局の TableBuilder においては、個票データの各レコードにランダムに割り振られた値である record key に基づいて、出力される集計表の中のセルの数値に対応するノイズが算出され、そのセルに対してノイズが含まれた出力結果が自動的に付与されている(伊藤・谷道・小島(2018))。

さらに近年、分析結果のチェックの自動化が注目されており、例えば、イギリスやドイツでは、オンデマンド集計システムの展開として、オーストラリア統計局(ABS)の TableBuilder を参考にして、個別のレコードに割り当てられる乱数にしたがって、集計表の各セルにランダムなノイズを付与する cell key method の実用化が進められている。具体的には、TableBuilder の方法論を参考にした上で、ドイツ連邦統計局のオンデマンドシステムである genesis online[3] やイギリス国家統計局で現在開発が進められている Flexible Dissemination System においても、独自の cell key method の実用化が進められている(Office for National Statistics(2017))。この cell key method が、イギリスの 2021 年人口センサスにおける集計表の作成・公表に用いられることが計画されている[4]。

### 2.3 Cell Key Method の特徴

本節では、ドイツやイギリスで議論されている cell key method の特徴について述べる。図 1 は cell key method の概要を表示したものである。cell key method の手順は、①攪乱のルールを定める(ノイズ関数の設定)、②一様分布の乱数である record key を各レコードに追加する、③原データの集計を行う、④原データの集計と同時に record key も集計することによって、cell key の数値を算出する、⑤ノイズ関数(ONS の場合には、look up table(p table[5]とも呼ばれる))を用いてノイズの値を確定させた上で、元の集計値にノイズを付与する。図 1 を例に見ていくと、最初に、統計作成部局において統計実務の観点を踏まえた上で、ノイズに関する関数(あるいは p table)を設定する。つぎに、各レコードには record key を付与する。つぎに性別と年齢グループ別に集計すると、40～59 歳(年齢グループが B となる年齢階級)の男性の度数は 3 となる。同時に、同じ 40～59 歳で男性であるレコードに付与された record key の数値を総計することによって cell key が算出される。図 1 では 0.866+0.535+0.337=1.738 という数値が得られるが、cell key では、小数第 1 位以下の 0.738 が用いられることから、40～59 歳の男性の cell key 欄には小数第 2 位で四捨五入された 0.74 が入力される。この 0.74 と度数 3 に対応するノイズである「+1」が選定される。ゆえに、40～59 歳で男性の集計値については度数 3 にノイズとして 1 が追加され、該当する度数は 4 となる(Enderle and Giessing (2020))。

このノイズが付与された度数を集計した場合、例えば、全体の総計値や部分総計にも cell

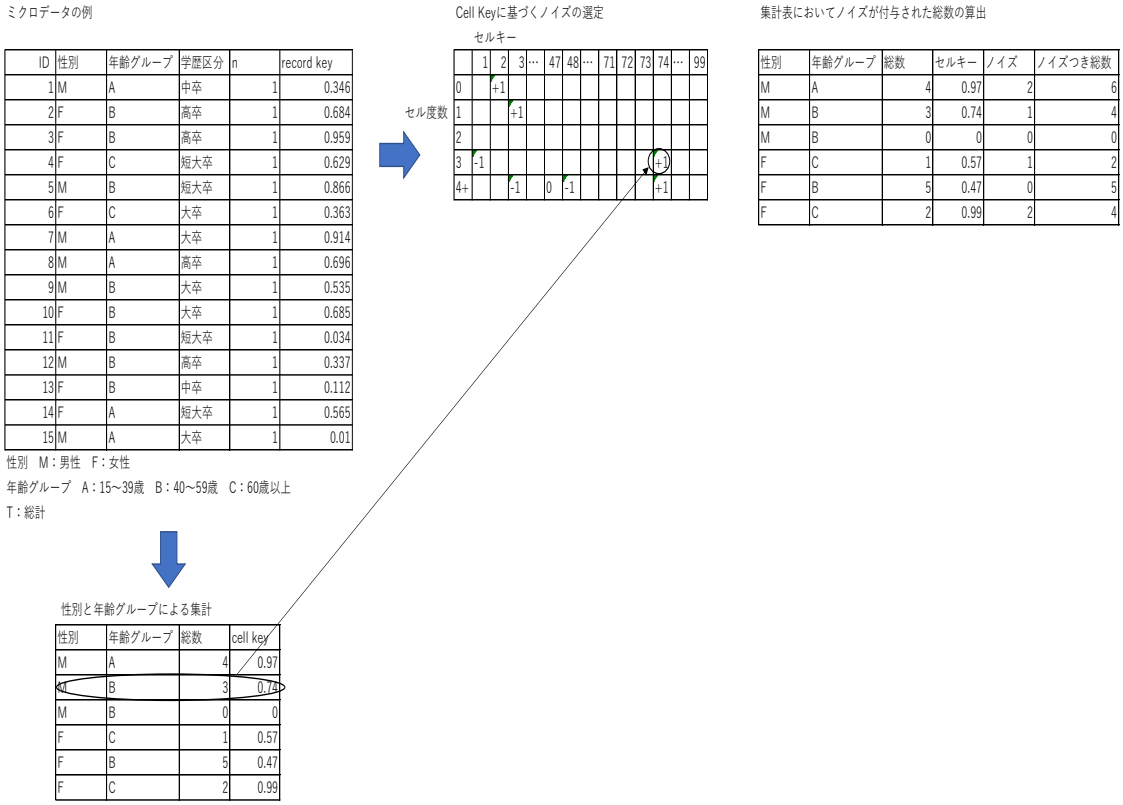
ては、ドイツ連邦統計局によるリモートエグゼキューションの利用サービスやノルウェー統計局が開発した microdata.no と呼ばれるリモートエグゼキューションの事例がある(伊藤(2020a))。

[3] genesis online は、ドイツ連邦統計局が運用するオンデマンド型のサービスであり、集計事項や分類区分を選択することによって加工された集計表をウェブ上で入手することが可能である。

[4] ドイツ連邦統計局の Sarah Giessing 氏によれば、新型コロナ感染症の影響で、2021 年に予定されていた人口センサスの実施が 1 年遅れることになったということである(2021 年 2 月 10 日時点)。その影響で、2021 年人口センサスへの適用が計画されていた cell key method を用いた genesis online は、2023 年末以降に稼働予定になっているということであった。

[5] 伊藤・谷道・小島(2018)は、TableBuilder における pTable に関して、①pTable の分布は 0 を基軸に左右対称であり、0 が付与されるケースもあること、②ノイズの最大値や最小値等、経験則に基づいて作成していることを指摘している(伊藤・谷道・小島(2018, p.201-204))。

図１　cell key method の適用のイメージ




| ID | 性別 | 年齢グループ | 学歴区分 | n | record key |
|---|---|---|---|---|---|
| 1 | M | A | 中卒 | 1 | 0.346 |
| 2 | F | B | 高卒 | 1 | 0.684 |
| 3 | F | B | 高卒 | 1 | 0.959 |
| 4 | F | C | 短大卒 | 1 | 0.629 |
| 5 | M | B | 短大卒 | 1 | 0.866 |
| 6 | F | C | 大卒 | 1 | 0.363 |
| 7 | M | A | 大卒 | 1 | 0.914 |
| 8 | M | A | 高卒 | 1 | 0.696 |
| 9 | M | B | 大卒 | 1 | 0.535 |
| 10 | F | B | 大卒 | 1 | 0.685 |
| 11 | F | B | 短大卒 | 1 | 0.034 |
| 12 | M | B | 高卒 | 1 | 0.337 |
| 13 | F | B | 中卒 | 1 | 0.112 |
| 14 | F | A | 短大卒 | 1 | 0.565 |
| 15 | M | A | 大卒 | 1 | 0.01 |

| | 1 | 2 | 3 | … | 47 | 48 | … | 71 | 72 | 73 | 74 | … | 99 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | +1 | | | | | | | | | | | |
| 1 | | | +1 | | | | | | | | | | |
| 2 | | | | | | | | | | | | | |
| 3 | -1 | | | | | | | | | | (+1) | | |
| 4+ | | | -1 | | 0 | -1 | | | | | +1 | | |

| 性別 | 年齢グループ | 総数 | セルキー | ノイズ | ノイズつき総数 |
|---|---|---|---|---|---|
| M | A | 4 | 0.97 | 2 | 6 |
| M | B | 3 | 0.74 | 1 | 4 |
| M | B | 0 | 0 | 0 | 0 |
| F | C | 1 | 0.57 | 1 | 2 |
| F | B | 5 | 0.47 | 0 | 5 |
| F | C | 2 | 0.99 | 2 | 4 |

| 性別 | 年齢グループ | 総数 | cell key |
|---|---|---|---|
| M | A | 4 | 0.97 |
| M | B | 3 | 0.74 |
| M | B | 0 | 0 |
| F | C | 1 | 0.57 |
| F | B | 5 | 0.47 |
| F | C | 2 | 0.99 |

出所　Enderle and Giessing (2020)をもとに一部加筆・修正

key method を適用すると、同時分布から算定される集計値が、周辺分布である部分総計や全体の総計値と一致しない場合が生じる。こうした状況に対して、ドイツ連邦統計局では、Controlled Tabular Adjustment (CTA)の適用が提唱されている(Enderle and Giessing (2020))。

## 3. アメリカにおける公的統計データの作成・公表に対する秘匿措置の動向[6]

アメリカでは、公的統計の分野において差分プライバシーの実用化に向けた議論が進展している。センサス局では、2020 年センサスの集計結果の公表およびミクロデータの作成に向けて、差分プライバシーを用いた公的統計の作成に関するプロジェクトを展開してきた。本節では、アメリカのセンサスのデータに対する差分プライバシーの適用状況を中心に、アメリカにおける匿名化されたセンサスのミクロデータに関する作成の動向および 2020 年センサスにおける統計表の作成・公表にあたっての秘匿措置の特徴を論じる。

### 3.1 匿名化されたセンサスのミクロデータに関する作成の動向

[6] 本節の執筆においては、下記のセンサス局の 2020 年センサスに関するウェブサイトに掲載されているセンサスに関するデータの公表や秘匿措置に関する資料を参照した。
https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/2020-das-development.html.

センサス局は、2010 年センサスまでの一般公開型ミクロデータサンプル(Public Use Microdata Sample=PUMS)の作成においては、個票データに含まれる個体情報の露見リスク(disclosure risk)を回避するために、「その場限りの(ad hoc)」秘匿措置を適用していた。センサス局が最初に PUMS を作成したのは、1960 年センサスであって、1962 年に公開された。全人口の 0.1%のサンプルが提供されている。PUMS を作成するための秘匿措置としては、直接的な識別子を削除すること、および提供可能な地域区分の人口規模を最低 25 万人以上にするという措置が取られた。1970 年センサスでも引き続き、直接的な識別子の削除と 25 万人以上という地域区分の人口規模のしきい値が設定された。つぎに、1980 年センサスの PUMS においては、直接的な識別子の削除だけでなく、所得額については 10 ドル単位の丸めと 75000 ドルをしきい値とするトップコーディング、さらに年齢について 90 歳をしきい値とするトップコーディングが適用された。また、地域区分に含まれる人口規模のしきい値が 25 万人から 10 万人に引き下げられている。さらに、1990 年センサスの PUMS の作成にあたっては、直接的な識別子の削除に加えて、居住地、勤務地、集合住宅(group quarters)、所得、年齢等、PUMS の秘匿性を確保するためのトップコーディングやリコーディングが多くの属性に採用された。トップコーディングの適用においては、全体の分布の上位 0.5%、非負である分布の上位 3%が、トップコーディングのしきい値としての基準になっており、その中でより高い数値がしきい値として選定されている。2000 年センサスの PUMS で用いられた秘匿措置の特徴は、センサス局が、直接的な識別子の削除、トップ・(ボトム)コーディングとリコーディングだけでなく、PUMS の作成のために用いられる公表統計表の元になる個票データに対して初めてスワッピングを適用したことである。それは、小地域レベルの統計表から個体が特定されないことを指向して採用されたが、PUMS 作成のための攪乱的な手法としても位置付けられうる。また、カテゴリカルな変数におけるすべての分類区分が最低 1 万人以上を代表するように区分の統合が行われるだけでなく、世帯人員が多い世帯については、ノイズが付与されている(McKenna(2019))。

そして、2010 年センサスにおいて PUMS の作成のために用いてきた方法は、情報の削除、トップ・ボトムコーディングといった非攪乱的手法による統計に含まれる情報の低減、およびノイズ付与、スワッピング、部分的な合成データ(synthetic data)の手法の適用を含む攪乱的手法であった。これらの手法を適切に組み合わせることによって、公表可能な統計表や PUMS として提供可能なレベルにまで特定化のリスクを低減していることが知られている(Zayatz(2007), Lauger et al.(2014))。さらには、センサス局は、2010 年センサスにおいても統計表の元になる個票データにおいてスワッピングを適用してきた(Zayatz(2007))。

それに対して、2020 年センサスの統計表(集計結果表)の作成・公表においては、「フォーマルな(定式化された、formal)」プライバシーの 1 つである、差分プライバシーの方法論が適用される。これは、個票データに適用された一連のクエリとしてモデル化したものである。この考え方に立って、差分プライバシーの公的統計への適用可能性が追究されるようになった。

### 3.2 2020 年センサスに向けた差分プライバシー適用に関する議論

センサス局は、センサス法(Title 13 of U. S. Code)第 9 条(a)(2)[7]に明記された法的根拠に基づき、公的統計データに対する秘匿処理を行ってきた。2020 年センサスにおいて差分プライバシーの方法論を採用したのは、Abowd(2018)が指摘する、集計表における「データベース再構

[7] センサス法(Title 13 of U. S. Code)第 9 条(a)(2)では、「商務省長官及びそれに属する局あるいは課のいかなる職員も」、「いかなる特定の事業所或いは個人から提供されたデータも識別できる形で公表すること」をしてはならないことが明記されている(石田(2000，p.31))。

築攻撃(database reconstruction attack)」に対応するためであった。データベース再構築攻撃とは、複数の集計結果表を組み合わせることによって、元となる個票データに含まれる個体情報を暴露することである(Dinir and Nissim(2003))。データベース再構築攻撃に用いられる集計結果表は、センサスの統計表に限らず、センサス以外のデータに基づく集計表を含みうる。こうしたデータベース再構築攻撃を回避するために、適切なεを決めた上で、ノイズを入れてクエリを返すという差分プライバシーの方法論(Dwork(2006))を公的統計に適用するための取り組みがセンサス局によってなされてきた。

センサス局は、統計実務上の経験も踏まえながら、2020年センサスに差分プライバシーを適用するための準備段階として、2010年センサスを用いた検証を行った。具体的には、全国レベルの性別、人種、年齢、世帯主との続き柄に関する様々な集計結果表を対象に、結果数値の精度を確保した上で公表することを可能にしつつ、安全性を確保するために、差分プライバシーの実用性に関する検証を進めてきた。検証に関する特徴は以下のとおりである。第１は、作成した統計表の公表によって消費されるプライバシー損失予算(privacy loss budget) ε[8]を管理しつつ、プライバシーの損失と精度のトレードオフの関係を勘案した上で、ε を決定することである。第2は、プライバシー損失予算εを設定した上で、州、郡、センサストラクト、およびセンサスブロックの各地域のレベルにおいて、プライバシー損失予算を割り当てることである(Garfinkel et al.(2019), Abowd et al.(2019))。

センサス局は、PL94-171 という人種と地域に関する統計表と SF1 と呼ばれる性別年齢別のサマリーファイルを対象に、2010 年センサスを用いて以下の手順で実験を行っている(Abowd(2018), Garfinkel et al. (2018))。最初に、全国レベルで集計を行い、数理的に最適化されたプライバシー損失予算εに基づいてノイズを付与し、構造的ゼロ(structural zeros)[9]を考慮した上で差分プライベートな統計表を作成する。つぎに、州のレベルで、構造的ゼロを考慮したクエリとして州レベルの統計表を作成する。これらの差分プライベートな統計表に対応する形で、州レベルの地域区分が付与された個人単位のミクロデータが設定される。同様に、郡、センサストラクト、センサスブロックの各レベルにおける統計表をそれぞれ作成した上で、それに対応する地域区分が擬似的に付与されたミクロデータを新たに構築する(伊藤・寺田(2020))。

センサス局による差分プライバシーの方法論の採用においては、ミネソタ人口研究センターの Steven Ruggles が、差分プライバシーが適用された人口センサスのデータの有用性に疑問を呈している(Ruggles et al. (2019))。それに対して、Hawes(2020)は、2020 年センサスに対するフォーマルなプライベートモデルの適用によって秘匿措置における透明性が示されたこと、さらにプライバシー損失予算の利用を通じてプライバシーとデータの精度のトレードオフの関係が明確に定量化されたことによって、データの利用者とプライバシーの支持者のいずれも、データの有用性とプライバシーの重要性に関して、オープンな形での議論が可能になったことを指摘している。このように、差分プライバシーの方法論の適用にあたって、センサスの作成者側と様々な立場の利用者側との間のデータの利活用をめぐる論争に対する解決策が、大きな課題となっている。なお、第4節で議論するアラバマ州とセンサス局との差分プライバシーの公的統計への適用をめぐる裁判もこうした論争の１つであって、この裁判を通じて、センサスの作成者側と利用者側の対立に関する論点およびその解決に向けた方

---

[8] 本稿では、privacy loss budget については、許容されるプライバシー損失の総量を予算に見立てて「プライバシー損失予算」という日本語訳にしている。

[9] 構造的ゼロとは、例えば、15 歳未満の者に対する子供の数や無業者における現職の就業期間のように、論理的に矛盾した内容であることから、該当するセルにゼロを入力することである。

向性が明確になったと言うことができる。

3.3 2020 年センサスに向けた差分プライバシーの適用に関する近況

つぎに、2020 年センサスに向けて、センサスの統計データ(以下「センサスデータ」)を対象に、センサス局が差分プライバシーの適用をどのような形で進めてきたかについて、近況を見ていくことにしたい。2019 年 10 月に、センサス局は、PL94-171 の統計表を対象に、2010 年センサスの回答結果を用いて差分プライバシーが適用された 2010 Demonstration Data Products と呼ばれるセンサスデータを作成・公表した。それは、2020 年センサスのために新たに整備された、差分プライバシーの方法論を適用した「露見回避システム(Disclosure Avoidance System、以下 DAS と略称)」が、公的統計データの精度に与える影響をデータの利用者に明示するためであった。この 2010 Demonstration Data Products の作成においては、スワッピングが適用されていない 2010 年センサスの原データ(the 2010 Census Edited File)を対象に、センサス局が差分プライバシーを適用することによって作成したミクロデータファイル(Microdata Detail File(MDF)と呼ばれる)が利用された(U.S. Cemsus Bureau(2019))。なお、センサス局は、2010 年におけるセンサスデータを用いて、データの利用者が精度検証を可能にするために、近似性に関する指標を新たに提示した。それは平均絶対誤差(MAE)や平均 2 乗誤差の平方根(RMSE)であって、これらの指標が、センサス局によって実施された 2020 年のセンサスデータの精度の検証にも用いられる。

MDF から作成した 2010 Demonstration Data Products と 2010 年センサスのスワッピング済みミクロデータ(the 2010 Census Hundred-percent Detailed File と呼ばれる)を用いて作成したセンサスデータの両方が、センサス局で公表されたことから、データの利用者は、差分プライバシーとスワッピングの手法がそれぞれ適用された 2 種類のセンサスデータの分布特性に関して、近似性の指標をもとに比較・検討を行うことができた。また、2 種類のセンサスデータによる精度の比較についてセンサス局へのフィードバックも可能になった。

さらに、センサス局は、2019 年 10 月 29 日に 2010 年センサスに差分プライバシーが適用された、検証用データである「プライバシー保護済ミクロデータファイル(Privacy-Protected Microdata Files =PPMFs)」の公開を開始した。それにあたって、センサス局は、DAS で用いられるパラメータ ε を設定した。このパラメータの設定については、以下の経緯をたどっている。2019 年 10 月に DAS を用いて作成した PPMFs の最初のヴァージョンでは、パラメータが、個人に関するデータについて ε=4.0、世帯に関するデータに関しては ε=0.5 にそれぞれ設定された。その後、2020 年 5 月、9 月、11 月に PPMFs がバージョンアップした上で公開されたが、プライバシー損失予算 ε の数値は保持されていた(Garfinkel (2022))。

しかしながら、2021 年 4 月に公開された PPMFs のパラメータは、ε=12.2 (個人に関するデータが ε=10.3、世帯単位のデータが ε=1.9)に変更された。この PPMFs におけるパラメータは、これまで公開されたヴァージョンの PPMFs とは大きく異なる特徴を備えている。それは、これまでの PPMFs がプライバシー損失予算 ε に基づいてラプラスノイズを統計表のセルに付与する差分プライバシーを適用したのに対して、2021 年 4 月時点の PPMFs では、Zero-Concentrated Differential Privacy (zCDP) (Bun and Steinke (2016)) が適用されていることである。zCDP の特徴として、ラプラス分布ではなく、ガウス分布を用いることが指摘できる。この zCDP の導入に関する詳細および ε の変更の影響については、第 4.4 節で議論する。

2021 年 4 月に PPMFs を公開した後に、データの利用者、専門家、利害関係者からフィードバックがなされた。これらのフィードバックを検討した後に、プライバシーや秘密保護等に関する政策的課題を議論し、意思決定を行うセンサス局内部の中核的な機関である Data Stewardship Executive Policy Committee(DSEP)によって、人種・民族別の人口数の精度改善の

ために TopDown アルゴリズムを修正することが承認された。それによって、差分プライバシーの方法論の適用に際し、アメリカインディアン/アラスカ先住民/ハワイ先住民(American Indian/Alaska Native/Native Hawaiian=AIANNH)の地域および準州地域の人口数とその人口社会的特性を直接算出できるように変更がなされた。具体的には、法的・政治的に分割される地域ごとに正確な統計数値の獲得を指向して、AIANNH およびその関連地域(38 州の合併した地域とセンサスの調査対象区域、12 州の市と町/タウンシップ）をその地理的な階層構造に合わせるように、差分プライバシーにおけるアルゴリズムが修正された。これについては「アメリカ投票権法(Voting Rights Act of 1965)」との関連が指摘される[10]。そして、最終版の PPMFs の作成にあたっては、2021 年 6 月 8 日に、全体のプライバシー損失予算として ε=19.61 が、DSEP によって設定された(個人に関するデータが ε=17.14、世帯単位のデータが ε=2.47)。

このようにセンサス局は、2020 年センサスの統計表の作成・公表にあたって、差分プライバシーの方法論の適用を進めてきた。なぜ、センサス局はこうした方法論を採用してきたのだろうか。次節では、アラバマ州がセンサス局を提訴した際の裁判記録を紹介することで、センサス局が差分プライバシーの方法論を統計実務で実用化してきた経緯を明らかにする。

## 4. 2020 年センサスへの差分プライバシーの適用に関するアラバマ州からの訴訟について

センサス局による 2020 年センサスへの差分プライバシーの適用に対しては、アメリカでも賛否両論の議論が巻き起こされた。特に、2021 年 3 月 10 日に提訴されたアラバマ州からの訴訟 (Alabama v. U.S. Dep't of Commerce[11], Case 3:21-CV-211) は、センサスという大規模な公的統計への差分プライバシー適用の是非について公開法廷で争われたという点で、アメリカだけにとどまらず、今後の公的統計における秘匿措置のあり方を考えるにあたって極めて資料性が高いものと考えられる。

以下、本訴訟の概要と流れを簡単に示すとともに、参考人意見書として提出された「データプライバシー専門家の意見書」(Calo et al. (2021)) における議論を中心として、本訴訟における 2020 年センサスへの差分プライバシー導入の是非に関する論点の概要を示す。

### 4.1 本訴訟の経緯

本訴訟は、2021 年 3 月 10 日にアラバマ州が Robert Aderholt 下院議員 (共和党) 等と連名で、アメリカ商務省に対して 2020 年センサスの結果公表の 3 月末への前倒しや、2020 年センサスへの差分プライバシーの適用の中止などを求めて提訴したことにより開始された (The State of Alabama et al. (2021))。本訴訟において原告は、新型コロナウイルス (COVID-19) の感染拡大を理由とした結果公表の遅延や、差分プライバシーの導入による集計結果の「歪曲 (skew)」は、2020 年センサスに基づく選挙区の区割りに悪影響を及ぼし、連邦法に違反するものであると主張している。

最終的に、本訴訟は 2021 年 6 月 29 日にほぼ全面的に原告が敗訴する形で判決が下され (Newsom et al. (2021))、それを受けて 2020 年センサスは差分プライバシーを適用した形で 2021 年 8 月 16 日に公表された。本訴訟の提訴から結審までの時系列的な流れは以下の通りである。

---

[10] 人種間の不平等の是正、さらにはマイノリティの選挙権行使およびマイノリティにおける代表の選出を保障することを指向したアメリカ投票権法(Voting Rights Act)が 1965 年に制定された。アメリカ投票権法とアメリカにおける選挙区画再編の動向については、例えば梅田(2008)を参照。

[11] 本訴訟は、センサス局が所属するアメリカ商務省 (Department of Commerce) を被告として提訴された。

3/10:　原告による提訴
3/26:　巡回裁判所での審理決定
4/13-26:　原告・被告および参考人からの意見陳述。
6/29:　判決および Newsom 判事による補足意見
9/9:　原告による提訴の取り下げ

4.2 本訴訟に関する裁判記録の概要

本訴訟における、原告の訴状 (Complaint)、被告の反論 (Opposition)、参考人意見書 (Amicus Brief) などの裁判記録は、様々な組織によりインターネット上に公開されている (たとえばブレナン司法センター[12]など)。それらの中でも、被告からの反論書や参考人からの意見書には、(技術的には非専門家である) 裁判官にもわかりやすいように、2020 年センサスへの差分プライバシーの導入の必要性に関する技術的背景や、差分プライバシーに関する「よくある誤解」への反論などの技術的な背景が論理的に説明されており、今後の公的統計において留意すべきリスクと、その対策としての差分プライバシーの位置付けを議論する上で大いに参考になると考えられる。

特に、以下 2 点の参考人意見書は、2020 年センサスへの差分プライバシーの導入や、それに対しての原告側からの批判に関し、その論点を専門家の立場から網羅的に論評したものである。

データプライバシー専門家の意見書 (Calo et al. (2021))

データプライバシーや暗号分野、および関連する機械学習、統計学、情報理論の各分野における 20 名の専門家から提出された意見書であり、差分プライバシーの提唱者である Dwork をはじめ、Canneti や Wasserman などセキュリティ分野や統計理論分野における第一線の研究者が提出者である「専門家」として名を連ねている。

電子プライバシー情報センターの意見書 (Electronic Privacy Information Center (2021))

プライバシー保護の分野において国際的に大きな影響力を持つ非営利団体である「電子プライバシー情報センター (Electronic Privacy Information Center, EPIC)」から提出された意見書である。EPIC は、個人のプライバシーや、それに関連する人権の保証に懸念を抱かせるような政策に対し、政府を提訴したり訴訟を支援したりすることも多いが、この訴訟では政府 (商務省) を擁護する形で意見書を提出している。

いずれも、プライバシー保護に関する専門的な知見に基づいて提出された意見書であり、大筋としては同様の主張がされていることから、本稿では「データプライバシー専門家の意見書」を中心として論点を概説する。

4.3 データプライバシー専門家の意見書について

前述の通り、この意見書はプライバシー保護分野、セキュリティ分野、統計分野などにおける第一線の研究者を中心とした、20 名の「データプライバシー専門家 (Data Privacy Experts)」の連名で提出されており、以下の 4 つの論点に関する議論から構成されている (Calo et al. (2021), Argument I-IV)。

論点 1:「再構築攻撃」の脅威に関する指摘[13] (Argument I)

[12] https://www.brennancenter.org/our-work/court-cases/alabama-v-us-dept-commerce.
[13] 原文は “Reconstruction attacks Are Real and Put the Confidentiality of Individuals Whose Data are Reflected in Statistical Disclosures at Serious Risk”と記載されている。

論点 2: センサスの秘匿手法を強化する必要性に関する指摘[14] (Argument II)
論点 3: 差分プライバシー自体と 2020 DAS との区別の必要性に関する指摘[15] (Argument III)
論点 4: 2020 DAS は統計的推定を用いていないことに関する指摘[16] (Argument IV)

論点 1 と論点 2 は対を成すものであり、現在までの計算機能力やアルゴリズムの進化を背景とした新たな攻撃 (再構築攻撃)に関してその脅威を指摘する (論点 1) とともに、それらの脅威に対処できるよう秘匿手法を進化させる必要性について指摘している (論点 2)。

また、論点 3 と論点 4 はいずれも原告側の技術的な誤解ないし理解不足と、それに伴って原告側の批判が根拠を欠くことを指摘するものである。特に、論点 3 は「差分プライバシー」自体とその実現手段 (2020 年センサスにおいては 2020 DAS) との違いについて原告側が混同している点の指摘であるが、この差分プライバシーと実現手段の混同は、差分プライバシーに関する「よくある誤解」の一つでもあることから、単に本訴訟における原告側の誤解を指摘するだけに留まらず、差分プライバシーに関する正しい理解の促進や啓発にあたっても参考になる議論であると考えられる。

なお、論点 4 は 2020 DAS で用いられたノイズ付与の手法が (原告が主張するような) 統計的推定 (statistical inference) には相当しないことの指摘であるが、これは 2020 DAS 固有の議論であることから、本稿では議論を割愛する。

以下、論点 1〜3 に関し、本意見書における指摘の内容を概観する。

4.3.1 論点 1 :「再構築攻撃」の脅威 (Argument I)

再構築攻撃 (reconstruction attack) とは、あるデータベースから生成された、(一見すると安全に見える) 複数のデータを重ね合わせることによって制約充足問題を構築し、その問題を解いて元のデータベースを復元することにより、それらのデータに含まれる個人のプライバシーを暴露する攻撃であり、データベース再構築攻撃とも呼ばれる (寺田 (2019)、Garfinkel (2019))。また、複数のデータベースの重ね合わせにより個人のプライバシーが暴露されやすくなることは、モザイク効果 (mosaic effect) とも呼ばれる (寺田 (2018)、The State of Oregon (2019), ORS 276A.350 (e))。

センサス局は、2020 年センサスへの差分プライバシーの導入の背景として、再構築攻撃に関する懸念を重要視している(Garfinkel (2019))。本意見書でもその判断を支持しており、再構築攻撃に関するリスクがプライバシーに対する現実的な脅威であることを以下の 4 点から議論している (Calo et al. (2021), Argument I, B-E)。

(1) センサス局の実験により、再構築攻撃は実際に危険なことが示された。
(2) 外部の研究者による別の実験でも、再構築攻撃の危険性が示されている。
(3) 再構築攻撃は、個体の再識別をもたらす。
(4) 再構築攻撃を介した個体の再識別は、現実的な脅威である。

以下、それぞれに関する本意見書による指摘について議論する。

(1) センサス局の実験により、再構築攻撃は実際に危険なことが示された。

---

[14] 原文は “Census Confidentiality Protections Must Evolve to Address Today’s Threats”
[15] 原文は “Distinguishing the Census Bureau’s 2020 Disclosure Avoidance System (2020 DAS) and Differential Privacy”
[16] 原文は ”The 2020 DAS Does Not Use Statistical Inference”

本意見書では、センサス局自身による 2010 年センサスの集計結果への再構築攻撃の適用実験において、実際にアメリカ国民の 46% (約 1.4 億人) の居住ブロック、性別、年代、人種、民族が復元された (年齢に 1 歳の誤差を許すと 71% が復元された) こと、およびその結果を一般に流通している市販データと照合することによって 5,200 万人が再識別されたことから、再構築攻撃によるプライバシー暴露が理論上の可能性ではなく現実の脅威であることを指摘している。

また、原告や、原告側参考人の Bambauer、原告側証人の Ruggles が再構築攻撃の脅威を軽視していることについて、Ruggles (2021) における分析が単純すぎて実際のリスクを過小評価している[17]として、その問題点を論じている。

(2) 外部の研究者による別の実験でも、再構築攻撃の危険性が示されている。

また、センサス局自身による過去のセンサスに対する実験だけでなく、その他の再構築攻撃によるプライバシー暴露に関する興味深い事例について二点紹介している。

- Aircloak 社による Diffix と呼ばれる商用システムは「フランスの公的機関 (CNIL) が GDPR レベルの匿名性を認定した」とされている (Cohen and Nissim (2020)) が、2018 年に Cohen と Nissim は再構築攻撃を実装した数百行のプログラムにより、一般的なノート PC を用いて数秒以内に全データレコードを完全に復元することに成功した。
- イスラエル中央統計局 (Israel Central Bureau of Statistics, CBS) が公表している 2011 年社会調査 (Social Survey) の統計表から、2014 年に大学生のグループが 14%のレコードを完全に復元することに成功し、その中にグループメンバーの一人に関するレコードが入っていることを確認した (その時点で攻撃を中止した)。

これらの実験結果は偶然のものとは言えず、統計作成部局が直面しつつある新しいリスクを証左するものとし、NASEM (National Academies of Sciences, Engineering, and Medicine)[18] の 2017 年のレポートによる、外部データの拡大や計算機能力の向上を背景として伝統的な手法がプライバシー漏洩を引き起こす懸念がますます高まっているとの指摘を引用している。

(3) 再構築攻撃は、個体の再識別をもたらす。

いわゆる「匿名化された ("anonymized"[19])」データからの再識別 (re-identification) の危険性は周知のこととなっており、特に再構築されたデータセットからの再識別は、一般に流通しているデータセットを用いて、よく知られた方法で容易に実行できることを指摘している。

以降、「匿名化された」はずのデータセットからの再識別に関し、さまざまな事例を引用するとともに、その危険性は、すでに議論の必要がない明白なこととしてプライバシー保護に関する学術界では結論づけられているとしている。

(4) 再構築攻撃を介した個体の再識別は、現実的な脅威である。

前述のセンサス局による (再構築攻撃の結果からの) 再識別の実験は、高校卒業レベルの技術 (eighteen-year-old techniques) と公開データのみを用いて実施されたものであり、センサス局が持つ秘密情報を一切使っていない (誰でもできる) ものであることを指摘している。

[17] Ruggles の主張は、簡単に言えば「ランダムに推測してもまぐれ当たりすることがある (ので、再構築攻撃は新たな脅威ではない)」というものである (Ruggles (2021, p.7))。
[18] 全米アカデミーズ (National Academies) とも呼ばれる。アメリカの議会令に根拠を持つ、政府とは独立した学術団体であり、科学、技術および医学の分野において専門的な知見から政府に助言する機能を有する。
[19] 原文においても "anonymized" と引用符を付けて記載されている。

また、この再構築攻撃を介した再識別が、安全保障上のリスクであることについて、たとえば Google, Facebook, Twitter などにより商用目的で収集されたデータとの照合による再識別や、(過去に発生した) アメリカ人事管理局 (Office of Personnel Management, OPM) への侵入により漏洩したデータとの照合による再識別が発生した際における安全保障上の脅威について議論している。

4.3.2 論点 2：センサスの秘匿手法を強化する必要性 (Argument II)

上記で示した再構築攻撃の脅威への対抗手段として、本意見書では現時点において有効な対策は差分プライバシーしか知られておらず[20]、差分プライバシーを 2020 年センサスに適用するとした DSEP の決定は賢明であったとしている (なお、EPIC の意見書でも同様の指摘がされている[21])。

これに加え、差分プライバシーは、センサス局が必要とするデータの有用性と安全性の両立という要件に関し、3 つの利点を与えるとしている。

- 差分プライバシーは未来 (における安全性) を保証する (future-proof)。Sweeney による再識別攻撃[22]や、Dinur と Nissim による再構築攻撃など、いままでも新たな攻撃は発見され続けてきており、今後もそれは続くと予想される。それらに対する保護を提供することはセンサス局にとって重要である。
- 差分プライバシーは攻撃者を問わない (adversary agnostic)。攻撃者がどのような動機や財力、計算能力、情報などを持っていたとしても安全性を提供する。
- 差分プライバシーは計測可能である (measurable)。データが分析されたり共有・結合されたりすることによるプライバシーの損失度合いを定量的に検証できる。

また、(原告側) 参考人である Bambauer による「センサス局は実際に予見可能な最大限のリスクに対して対策をすべきだ」という主張に対して、センサス局が攻撃者の能力や未知の攻撃を予見しきることは不可能であり、予見できなかった攻撃によるプライバシー損失は取り返しがつかないという観点から反論し、従来の経験的 (heuristic) な手法の限界について議論している。

4.3.3 論点 3：差分プライバシー自体と 2020 DAS との区別の必要性 (Argument III)

原告の訴状や原告側参考人の意見書の多くが、「差分プライバシー」そのものと、差分プライバシーに基づく実装の一つである 2020 DAS を混同していることを指摘している。

このような差分プライバシーとその実現方式との混同は、差分プライバシーに関する「よくある誤解」の一つである (寺田 (2018))。差分プライバシーは、ある方式が「どのくらい安全か」を測るための指標を与える数学的な定義であって、何か具体的なアルゴリズムや実装を指す言葉ではない。その一方で、差分プライバシーを満たす方式は多数存在し、2020 DAS はそのうちの一つを実装したものである。

本訴訟における原告側の差分プライバシーと 2020 DAS (ないし他の差分プライバシーの実現方式) との混同は、原告側の主張を理解困難なものとしており、本訴訟を担当した判事の

---

[20] 原文は “Differential privacy is the only known way to protect against reconstruction attacks.”。ただし、次節で議論する通り、差分プライバシーはプライバシーの安全性指標を与える数学的な定義であって、差分プライバシーを満たす手段は多数存在することに注意されたい。

[21] 原文は “Differential privacy is the only technique known to effectively protect against reidentification attacks.” (EPIC (2021), Argument II)。

[22] 再識別攻撃 (Sweeney (2002)) とは、郵便番号や年齢など、複数の属性 (準識別子) の組み合わせを用いることにより個人を再識別する攻撃を表す。

一人である Newsom 判事は、この原告側による差分プライバシーに関する主張の一貫性の欠如を判決時の補足意見で批判している (Newsom (2021))。

4.4 本訴訟における議論から得られる知見

本訴訟における議論は、単に公的統計への差分プライバシーの導入の是非だけに留まらず、公的統計に求められる安全性について様々な示唆を与えるものと考えられる。以下、それらのうち主要なものと思われる三点について議論する。

4.4.1 再構築攻撃の脅威に関する認識について

本訴訟における議論のうち、技術的な視点から最も興味深い論点は、「2020 年センサスにおいて、センサス局は差分プライバシーを適用する必然性は存在したのか？」である。論点 1 で議論した通り、センサス局は再構築攻撃を現実的かつ重大な脅威であるとみなしており、その対策として差分プライバシーの導入を決定している。また、「データプライバシー専門家」グループや EPIC も、それが唯一の有効な対策であるとして支持している。つまり、2020 年センサスにおける差分プライバシーの導入は、再構築攻撃という新たな脅威からプライバシーを保護するために強い必然性を持ってなされたものであるという観点に立っており、プライバシー保護技術に関する専門家もそれを支持している (データ利用側の専門家である Ruggles は、再構築攻撃は大した脅威ではないとの立場をとっているが、第 4.3.1 節 (1) での議論の通り、Ruggles (2021) の主張はデータ専門家の意見書で否定されている)。

その一方で、これまでわが国では賛成反対いずれの立場からも、ほとんど再構築攻撃については議論がされていないのが現状である。再構築攻撃は、技術的には「差分開示 (disclosure by differencing) 攻撃」の応用として位置付けられるが、その差分開示攻撃に関しても活発な議論の対象とはなっていない。アメリカとわが国では公的統計において公表される集計表の粒度が異なることや、民間データの流通の活発さに違いがあることなどから、アメリカで 2020 年センサスに再構築攻撃への対策が必要であったとしても、たとえばわが国の 2020 年国勢調査に同じことが当てはまるとは限らない。しかし、今後のオープンデータや DFFT (Data Free Flow with Trust) の促進によるデータ活用の活性化を考慮すると、わが国でも近い将来に同様の課題に直面することが予想される。今後のわが国において、データのさらなる活用を健全なプライバシー保護の元で進めていくためには、再構築攻撃などの新たなプライバシー暴露攻撃に関する研究や、その対処手段に関する検討が急務になると考えられる。

4.4.2 差分プライバシー導入の必要性について

また、論点 2 に関する議論で示した通り、再構築攻撃への対策として、データプライバシー専門家の意見書では、差分プライバシーの導入が現時点では唯一の手段であるとしている。これはかなり強い主張であるが、連名する 20 名の「データプライバシー専門家」の共通見解として示されたものであり、さらに EPIC の意見書でも同様の趣旨が記載されていることから、これはアメリカのプライバシー保護技術の専門家の間において、少なくとも特異な見解ではないことが推察される。

ただし、ここで論点 3 における議論、つまり「差分プライバシー」を満たす方式は一つではなく、多数存在することに留意が必要である。再構築攻撃の対策として差分プライバシーの導入が唯一の手段であったとしても、それを実現する方法は一つではない。たとえば、伝統的な手法の一つである PRAM (Post Randomization Methods) は、(その効率はともかくとして) 差分プライバシーを満たす手法の一つであることが知られており、その他にも攪乱的手

法であれば[23]差分プライバシーを満たす可能性がある。たとえば第 2 章で議論した、欧州を中心に検討が進められている cell key method など、統計分野で検討が進められている各種の攪乱的手法と差分プライバシーの関係や、それらの再構築攻撃に対する堅牢性は、今後の検討における方向性の一つとなると考えられる。

4.4.3 「未来の脅威」に対する安全性確保の必要性について

さらに、データプライバシー専門家の意見書は、プライバシーは一度暴露されると取り返しをつけられるものではないため、(再構築攻撃に限らず) 今後さらに新たな攻撃が発見されることを想定してプライバシーの保証を与えられること (future-proof) が重要であるとしている。伝統的な手法は、(差分プライバシーと異なり) 数理的な安全性の保証はなくとも、その長い適用の歴史がその妥当性を支えている。しかし、これは (再構築攻撃をはじめとする) 急速な進展を見せている攻撃手法に対する今日の安全性を保証するものではなく、さらに今度どのような新たな攻撃が発生しうるものであるかを「予見」することは困難である。この点について、意見書では「センサス局は (未来を予見する) 水晶玉を持っているわけではない (The Census Bureau has no crystal ball)」という表現で指摘している。

これらの指摘の通り、近年の計算機能力の向上やそれに伴う攻撃手法の進化や、データ活用の進展に伴う高次元大規模データへの要求の高まりは、経験的な手法でデータを保護し、最終的に人間が目で見て安全性を判断する、という伝統的な開示制御のプロセスを困難にしていくことが予想される。ただし、2020 DAS がこの問題を完全に解決できたかと言えば、実際のところはまだ「道半ば」であると評価すべきであろう。これは、2020 DAS で最終的に採用されたプライバシー損失予算 (ε) の値が、差分プライバシーにより (将来にわたっての) 数理的な安全性を与えるとは言い難い大きさとなったことに表れている。この点については次章でより具体的に議論する。

## 5. 2020 年センサスにおけるプライバシー損失予算 (ε) の妥当性をめぐって

差分プライバシーが与える安全性保証は、一般に ε で表される安全性パラメータにより定められ、これは 2020 年センサスにおいてプライバシー損失予算と呼ばれている。この ε の値を通じて、データの有用性 (出力に含まれるノイズの少なさ) と安全性 (数理的に保証されるプライバシー保護の度合い) のバランスを調整することが可能であり、ε が小さい値であるほど高い安全性が与えられ (その代わりにデータの有用性は低下する)、大きな値であるほどデータの有用性は向上する (その代わりに安全性は低下する)。ある安全性パラメータ ε の元で差分プライバシーの定義を満たすことを、「ε-差分プライバシー (ε-differential privacy, ε-DP)」を満たすと言う。

第 3 章で示した通り、2020 DAS におけるプライバシー損失予算 ε の値は、約 1 年半にわたる試験提供やそれに基づく DSEP の議論を通じて「調整」され、最終的には個人単位のデータについて ε = 17.14、世帯単位のデータについて ε = 2.47 という値が採用された。

ここで、世帯単位のデータで用いられた ε = 2.47 は、いわゆる「現実的な落としどころ」として評価できる範囲の値であると考えられるが、個人単位のデータにおける ε = 17.14 は一般的にはあまり安全とはみなされない値である[24]。以下、この点について考察を加える。

---

[23] 差分プライバシーは確率的な識別不可能性 (indistinguishability) を安全性の根拠として求めるため、決定的手法は差分プライバシーを満たすことが原理的に困難である。

[24] 安全性パラメータ ε が具体的にどのくらいの値であれば「安全」と呼べるかについては、データの性質や使い

まず、2020 DAS が採用している TopDown アルゴリズムは、単一のノイズによってデータを保護しているのではなく、複数のノイズの合成により保護が与えられることに留意が必要である。すなわち、2020 DAS における ε の値は、差分プライバシーの合成定理 (composition theorem)[25] を使って与えられており、実際には安全性マージンが存在する (単に ε＝17.14 として最適なノイズを加えるよりも高い安全性を持つ)。なお、この安全性マージンの存在は、純粋な差分プライバシー (ε-DP) のみでは表現不能であるが、これを定量的に安全性定義に組み込んだ差分プライバシーの拡張として「レニー情報量」に基づく安全性定義が提案されている (寺田 (2019))。

次に、センサス局は 2021 年 4 月の DSEP 以降、純粋な差分プライバシーに基づいて 2020 DAS を実行しているのではなく、上記のレニー情報量に基づく拡張の一つである zCDP (第 3 章参照) に基づいて安全性パラメータ (ρ で表される) を与えることによりデータを生成し、そこから zCDP と (ε, δ)-differential privacy ((ε, δ)-DP)[26] (Dwork et al. (2006)) の間に成立する数学的な関係を用いて ε の値を導出する、という複雑な手順を用いていることに留意する必要がある。具体的には、以下の手順により ε を与えている。

1. zCDP の安全性パラメータ $\rho$ に基づいてデータを生成する。なお、ここで個人単位のデータに対しては $\rho = 2.56$、世帯単位のデータに対しては $\rho = 0.07$ を用いている。
2. その後、zCDP と (ε, δ)-DP の関係における換算式を用いて ε の値を導出する。なお、この導出の際に $\delta$ の値を所与のものとして与える必要があるが、2020 DAS では $\delta = 10^{-10}$ を与えている。なお、これは「百億分の一 ($10^{-10}$) の確率で ε-DP が成立しない可能性を許容する」ことを意味する。

なお、zCDP は 2010 年代後半になり提唱された、差分プライバシーと比べてもさらに新しい概念であり、センサス局もこれまでその採用について特に言及することはなかった。それにもかかわらず、センサス局がなぜ (いわば唐突に) zCDP の採用を決定したかについて、その真意はこれまで公開された資料の中では十分に読み取れない (前述の裁判記録の中でも特に言及されていない)。ただし、当時の関連する状況からは、下記が背景にあると推察される。

1. DSEP での議論において、2020 DAS における少数民族 (AIANNH) に関する統計の精度について問題が提起され、試験を繰り返すうちに、その部分の精度を保つために消費するプライバシー損失予算が過大なものとなってきた。
2. 前述の通り、2020 DAS は差分プライバシーの合成定理に基づいて ε を与えるが、プライバシー予算が過大なものとなっていく中で、その安全性マージン (ある意味で「予算のムダ」とも言える) が無視できないものになってきた。
3. そこで、上記の合成定理による安全性マージンをより適切に取り扱うことができる差分プライバシーの拡張である zCDP に着目し、zCDP における合成定理に基づいて「安全性マージン」を圧縮した上で、プライバシー損失予算を配分することとした。つまり、通常の ε-DP における合成定理に基づく場合に比べ、(合成がより効率的に行えることに

方などによって異なるため一概には言い難いが、たとえば randomized response におけるランダムな回答の比率と、それにより与えられる ε との関係にあてはめると、ε が保証する安全性のレベルがどの程度かについて直感的に理解しやすい (寺田 (2018))。たとえば、ε＝2.47 は約 15%の確率でランダムな回答が返されることに相当し、ε＝17.14 は約 1,400 万分の一の確率でランダムな回答が返されることに相当する。

[25] 複数の差分プライバシーを満たす手段（メカニズムと呼ばれる）を合成して得られるメカニズムが、差分プライバシーを満たすことを保証する定理。合成後のメカニズムの ε の値は、(最悪でも) 合成元の各メカニズムにおける ε の値の総和となることが保証される。

[26] ある微小な確率で ε-DP が満たされないことを許容する差分プライバシーの拡張。δ＝0 のとき ε-DP と等価となる。

より) 同じプライバシー損失予算でより小さなノイズ強度を達成できるようにした。

したがって、2020 年センサスの安全性に関し、そのプライバシー損失予算 ε の値のみに基づいて議論することは、合成定理の適用による安全性マージンの存在や、zCDP における $\rho$ からの換算値として ε が導出されている (実際の安全性は $\rho$ によって与えられる) ことから、あまり適切ではない。また、この ε の値の大きさから、2020 年センサスが差分プライバシーの特長である「将来におけるプライバシーの保証 (future-proof)」を備えるかどうかについては疑わしく、その安全性については 2020 DAS のアルゴリズムに関する検証と議論を要すると考えられる。

このように、2020 年センサスにおける差分プライバシーの導入は、公的統計におけるプライバシー保護の方法論に大きな一石を投じていることは議論をまたないが、差分プライバシーに基づく数理的な安全性保証が限定的にしか与えられないなど、その特長を十分に享受しているとは言い難い。そのため、差分プライバシーの導入事例としては「道半ば」の不完全な形であるとも言え、今後の議論を通じた改善とさらなる進展が期待される。

## 6. むすびに代えて

本稿では、ヨーロッパにおける公的統計データへの攪乱的手法の適用の現状を述べただけでなく、センサス局における差分プライバシーの方法論の統計実務への導入やその後の差分プライバシーをめぐる裁判記録について論じることによって、攪乱的手法の適用に関する展開の方向を明らかにした。

センサス局の最近の動きで注目すべき点は、データベース再構築攻撃への対応を契機として、2010 年までの人口センサスまでの「その場限りの(ad hoc)」秘匿措置から転換したことである。そのために、2020 年センサスにおける露見回避システム(DAS)が開発された。これによって、統計実務において攪乱的方法を適用するための差分プライバシーの方法論の構築(TopDown アルゴリズム)と秘匿措置の基準が明示された。さらに、統計数値の秘匿性の観点だけでなく、データの利用者や利害関係者を踏まえた上で、統計数値の精度も考慮した形でパラメータ ε が設定されている。このようなセンサス局における事例は、わが国における公的統計の作成・公表のあり方を議論する上での有力な参考事例になると思われる。とくに、国勢調査の集計結果表では、市区町村レベルの地域でも度数の少ないセルに関する結果数値が公表されているが、このようなセルの結果数値の公表にあたっては、わが国におけるデータベース再構築攻撃の可能性に関する議論も今後求められるだろう。

ただし、このセンサス局によるドラスティックとも言える方向転換は、賛否両論の議論も巻き起こしている。その一例として、2020 年センサスへの差分プライバシーへの導入に関する、アラバマ州等を原告とした訴訟について概説するとともに、その主要な論点を示した。この訴訟は、筆者らが知る限り、差分プライバシーの公的統計への導入の是非が初めて公開裁判で争われたものであり、その裁判記録の資料性は高い。特に「データプライバシー専門家の意見書」は、2020 年センサスを取り巻くプライバシー上の脅威と、差分プライバシー導入の必要性について、第一線の研究者らによる最新の技術的知見に基づいて示されたものであり、今後の統計プライバシー保護のあり方を検討する上で重要な示唆を含むものと言える。

2020 年センサスにおけるプライバシー損失予算 ε の値は、DSEP での議論などに基づいて修正が重ねられ、最終的には個人に関するデータにおいて $\varepsilon = 17.14$、世帯単位のデータについて $\varepsilon = 2.47$ という値が採用された。特に個人に関するデータについて、これは一般的に安全と言い難い値であるが、2020 DAS における TopDown アルゴリズムは、差分プライバシーの合成法則の適用に伴う安全性マージンを持つことに留意が必要である。また、2020 年セン

サスは、実際には zCDP と呼ばれるレニー情報量に基づく差分プライバシーの拡張に基づいてプライバシーが保護されており、その安全性パラメータ $\rho$ からの換算式を用いてプライバシー損失予算 $\varepsilon$ が導出されている。つまり、2020 年センサスの作成においては、「純粋な」差分プライバシーを直接適用する代わりに、zCDP を介して差分プライバシーを満たす形を取っている。これらの理由から、その安全性に関して $\varepsilon$ の値のみに基づく一般性を持たせた議論を加えることは困難である。そのため、2020 年センサスにおいて、差分プライバシーの特長の一つである「将来におけるプライバシーの保証」が与えられているとは言い難く、その安全性については 2020 DAS に関する今後の検証と議論が待たれる。

2020 年センサスは、差分プライバシーを大規模な公的統計の作成と公開に適用した初めての事例であり、公的統計におけるプライバシー保護の方法論に大きな一石を投じていることは議論をまたない。その一方で、プライバシー損失予算 $\varepsilon$ の値に基づく数理的な安全性の保証は限定的なものに留まるなど、完璧なものとは言い難い。また、2020 年センサスの作成に用いられた 2020 DAS は、大規模な集計データに差分プライバシーを適用するにあたって優れた性質を持つ方式であるが、それが公的統計への差分プライバシーの適用手段として常に最適とも限らず、そのアルゴリズムにも改善の余地が大いに残されていると考えられる。また、2020 DAS で取られた手法 (TopDown アルゴリズム) の他にも、合成データに基づく手法や、機械学習技術を応用した手法など、統計の有用性とプライバシーに関する安全性をより高いレベルで両立させるための技術開発は様々なアプローチから進められている。それらの技術の進展や実用化の動向にも注目する必要があろう。

AI 技術や DX の進展に沿った形で、公的統計の様々な利活用が期待されている。このような公的統計データの利用をめぐる社会的な環境が急速に変容する中で、公的統計におけるプライバシー保護に対する技術的な措置が、社会的にも一層注目されている。その意味では、本稿で議論した差分プライバシーの方法論がわが国の公的統計において適用可能かどうかは、検討に値すると思われる。その一方で、統計実務の観点から見た場合、プライバシー損失予算 $\varepsilon$ の設定方法や $\varepsilon$ の公表の仕方、公的統計の利用者や調査対象者等の統計作成部局の外部に対する差分プライバシーについての対外的な説明のあり方等、検討すべき点は少なくない。今後のわが国におけるデータ活用の健全な形での進展に向け、これらの議論のさらなる活性化が求められる。

謝辞

本稿は、2021 年度統計関連学会連合大会における学会報告(2021 年 9 月 7 日)、および研究集会「大規模データの公開におけるプライバシー保護の理論と応用」での研究発表(2021 年 12 月 9 日)に基づいている。報告内容について貴重なコメントをしていただいた星野伸明先生(金沢大学教授)と槙田直木氏((独)統計センター統計技術・提供部長)に謝意を申し上げたい。また、2 名の匿名の査読者の方から数多くの丁寧なコメントをいただいたことによって、本稿の内容を大きく改善することができたことについても深謝したい。

参考文献

[1] 梅田久枝(2008)「アメリカの選挙区画再編に関する立法動向―選挙過程からの政治の排除―」『外国の立法』No. 236, pp.163-172.
[2] 石田晃(1999)「アメリカ、カナダにおけるミクロデータの現状について」，法政大学統計研究所『研究所報』No.25，pp.1-34.
[3] 伊藤伸介(2018) 「公的統計ミクロデータの利活用における匿名化措置のあり方について」『日本統計学会誌』第 47 巻第 2 号, pp.77-101.

[4] 伊藤伸介・谷道正太郎・小島健一(2018)「オーストラリアにおける公的統計の二次的利用について―オンデマンド集計システム TableBuilder を中心に―」,『経済学論纂(中央大学)』第 58 巻第 2 号，pp.187-208.
[5] 伊藤伸介(2020a) 「諸外国における公的統計と行政記録データの二次利用に関する展開方向」『経済学論纂(中央大学)』第 61 巻第 2 号，pp.1-16.
[6] 伊藤伸介(2020b)「デンマークとオランダにおける医療健康データの二次利用について」『日本統計学会誌』，第 50 巻第 1 号，pp. 109-138
[7] 伊藤伸介・寺田雅之(2020)「詳細な地域データにおける秘匿処理の適用可能性について」『日本統計学会誌』，第 50 巻第 1 号，pp. 139-166
[8] 伊藤伸介・横溝秀始(2021)「経済センサスのミクロデータを用いた匿名化手法の適用可能性に関する実証研究」総務省統計研究研修所『リサーチペーパー』第 49 号，pp.1-61.
[9] 寺田雅之・鈴木亮平・山口高康・本郷節之(2015)「大規模集計データへの差分プライバシの適用」『情報処理学会論文誌』，第 56 巻第 9 号, pp.1801-1816.
[10] 寺田雅之 (2018)「差分プライバシーとは何か」『システム/制御/情報』 第 63 巻第 2 号, システム制御情報学会, pp.58-63.
[11] 寺田雅之 (2019)「差分プライバシの基礎と動向」『情報処理』 第 61 巻第 6 号, 情報処理学会, pp.591-599.
[12] 濱砂敬郎(1999)「ドイツ連邦統計法におけるミクロデータ規定の匿名化措置」，法政大学統計研究所『研究所報』No.25，pp.69-99.
[13] Abowd, J. M. (2018) “Staring-down the Database Reconstruction Theorem”, Joint Statistical Meetings, Vancouver, BC, Canada.
[14] Abowd, J. and Schmutte, I. M. (2019) “An Economic Analysis of Privacy Protection and Statistical Accuracy as Social Choices”, *American Economic Review*, Vol.109, No.1, pp.171–202.
[15] Bun, M. and Steinke, T. (2016) “Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds”, *Theory of Cryptography 2016*, Lecture Notes in Computer Science, Vol. 9985, Springer, pp. 635-658.
[16] Brandt M., Lenz R., Rosemann M. (2008) “Anonymisation of Panel Enterprise Microdata – Survey of a German Project”, Domingo-Ferrer J., Saygın Y. (eds) *Privacy in Statistical Databases PSD 2008,* Lecture Notes in Computer Science, vol 5262 Springer, Berlin, Heidelberg.
[17] Calo, R., Canetti, R., Cohen, A., Dwork, C., Geambasu, R., Jha, S., Kohli, N., Korolova, A., Lei, J., Ligett, K., Mulligan, D. K., Reingold, O., Roth, A., Rothblum, G. N., Slavkovic, A., Smith, A., Talwar, K., Vadhan, S., Wasserman, L., Weitzner, D. J. (2021) “Amicus Brief of Data Privacy Experts”, Case 3:21-cv-00211-RAH-ECM-KCN.
[18] Cohen, A. and Nissim, K. (2020) “Linear Program Reconstruction in Practice”, *Journal of Privacy and Confidentiality*, Vol. 10, No. 1, pp.1-13.
[19] Dinur, I., and Nissim, K. (2003) “Revealing information while preserving privacy”, in *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, ACM, pp. 202–210.
[20] Dwork, C. (2006) *Differential privacy*. ICALP.
[21] Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I. and Naor, M., (2006) “Our Data, Ourselves: Privacy via Distributed Noise Generation”, *EUROCRYPT 2006*, pp. 486–503.
[22] Electronic Privacy Information Center (2021) “Brief of Amicus Curiae Electronic Privacy Information Center in Support of Defendants’ Response in Opposition to Plaintiffs’ Motion for Preliminary Injunction and Petition for Writ of Mandamus”, Case 3:21-cv-00211-RAH-ECM-

KCN.
[23] Enderle, T., Giessing, S., (2020) “Disclosure Control for German Census 2021- Methodology and Decision Process”, presented at Virtual Expert Group Meeting on SDC for Caribbean Census Tables Trinidad and Tobago.
[24] Garfinkel, S. Abowd, J. M., and Martindale, C. (2019) “Understanding Database Reconstruction Attack in Public Data”, *Communications of the ACM*, Vol. 62 No. 3, ACM, pp. 46-53.
[25] Garfinkel, S. (2022) “Differential Privacy and the 2020 US Census”, MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2022.
[26] Hawes, M. B., (2020) “Implementing Differential Privacy: Seven Lessons from the 2020 United States Census”, *Harvard Data Science Review*, Issue 2.2, Spring 2020.
[27] Heldal, J., Johansen, S., Risnes, Ø. (2019) “Instant Access to Microdata – microdata.no”, Paper presented at New Techniques and Technologies for Statistics 2019, Brussels.
[28] Ito, S. and Terada, M. (2019) “The Potential of Anonymization Method for Creating Detailed Geographical Data in Japan”, Paper Presented at Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality, The Hague, Netherlands, 2019, pp. 1–14.
[29] Lauger A., Wisniewski, B., McKenna, L. (2014) “Disclosure Avoidance Techniques at the U.S. Census Bureau: Current Practices and Research”, Research Report Series (Disclosure Avoidance #2014-02), U.S. Census Bureau, pp.1-13.
[30] Lenz R., Rosemann M., Vorgrimler D., Sturm R. (2006) “European Data Watch: Anonymising Business Micro Data – Results of a German Project”, Schmollers Jahrbuch : *Journal of Applied Social Science Studies / Zeitschrift für Wirtschafts- und Sozialwissenschaften*, Duncker & Humblot, Berlin, vol. 126(4), pp. 635-651.
[31] McKenna, L. (2019) “Research and Methodology Directorate: Disclosure Avoidance Techniques Used for the 1960 Through 2010 Decennial Censuses of Population and Housing Public Use Microdata Samples”, U.S. Census Bureau.
[32] Newsom, K. C. (2021) “Memorandum Opinion”, Case 3:21-cv-00211-RAH-ECM-KCN.
[33] Newsom, K. C., Marks, E. C., Huffaker, Jr., R. A. (2021) “Memorandum Opinion and Order”, Case 3:21-cv-00211-RAH-ECM-KCN.
[34] Office for National Statistics (2017) “Development of flexible dissemination for 2021 Census”.
[35] Ruggles, S., Fitch, C., Magnuson, D., Schroeder, J. (2019) “Differential Privacy and Census Data: Implications for Social and Economic Research”, AEA Papers and Proceedings 2019, 109, pp.403-408.
[36] Ruggles S. (2021) “Expert Report of Steven Ruggles”, Case 3:21-cv-00211-RAH-ECM-KCN.
[37] The State of Alabama, Aderholt, R., Green, W., and Williams, C. (2021) “Complaint for Declaratory and Injunctive Relief”, Case 3:21-cv-00211-RAH-KFP.
[38] The State of Oregon (2019) “2019 Oregon Revised Statutes”.
[39] Sweeney, L. (2002) “*k*-anonymity: A Model for Protecting Privacy”, *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, World Scientific Publishing, pp. 557-570.
[40] U.S. Census Bureau (2019) “Disclosure Avoidance System for the 2010 Demonstration Data Products: Design Specification”.
[41] Zayatz, L. (2007) “Disclosure Avoidance Practices and Research at the U.S. Census Bureau: An Update”, *Journal of Official Statistics*, Vol.23, No.2, pp.253-265.