海外における公的統計に関するプライバシー保護の現状
―アメリカとイギリスの事例をもとに―

伊藤　伸介†

寺田　雅之††

Privacy Protection for Official Statistics in Foreign Countries: Examples from the United States and the United Kingdom

ITO Shinsuke
TERADA Masayuki

海外における公的統計データに対するプライバシー保護をめぐる議論は、多様な様相を呈している。アメリカセンサス局は、公表された人口センサスから「データベース再構築攻撃」によって個体情報が特定されるリスクへの対応策として、2020 年人口センサスにおいて、Top down アルゴリズムによる差分プライバシーの方法論を適用した。それは、人口センサスの公表統計表における利害関係者や一部の利用者の反応を勘案しつつも、アメリカセンサス局がその秘匿性を担保する観点から採用した方法論であった。一方、イギリス国家統計局は、集計表の各セルにランダムなノイズを付与する cell key method を適用することによって、人口センサスの多次元統計表をオンデマンドで提供することを進めている。さらに、イギリス国家統計局は、2021 年人口センサスで利用者のニーズと攻撃者のシナリオを考慮した上で、複数のミクロデータファイルの作成を計画している。本稿では、アメリカとイギリスを例として、公的統計に対するプライバシー保護の現状について議論するとともに、その動向を比較・検討することによって、公的統計における将来的な方向性を洞察する。アメリカとイギリスにおけるプライバシー保護の最近の動向は、わが国における公的統計を対象にした統計表の公表やミクロデータの作成・提供を議論する上での有益な参考事例になると考えられる。

キーワード: 差分プライバシー、JASON レポート、cell key method、ターゲット・スワッピング

Privacy protection for official statistical data is implemented differently in different countries. The U.S. Census Bureau has adopted the methodology of differential privacy using top-down algorithm in order to avoid identification risks associated with “database reconstruction attack” for statistical tables starting with the 2020 Population Census. The U.S. Census Bureau applied this methodology of differential privacy to statistical tables from the Population Census while aiming to maintain data confidentiality of the statistical tables in question. In the UK, the Office for National Statistics (ONS) has plans to disseminate flexible multivariate statistical tables created using the cell key method in which random noise is added to each cell of statistical tables. In addition, the ONS plans to create microdata files that reflect user’s needs for Census microdata but also possible attacks by intruders. This paper discusses the actual situation of privacy protection for official statistics, and outlines future trends by comparing the developments in privacy protection in the U.S. and UK. Privacy protection in the U.S. and UK also provide useful reference for discussing the future publication and dissemination of microdata files for official statistics in Japan.

Keywords: Differential Privacy, JASON report, cell key method, targeted data swapping

† 中央大学経済学部　Email:ssitoh@tamacc.chuo-u.ac.jp
†† (株)NTT ドコモ　Email: teradam@nttdocomo.com

1. はじめに

諸外国では、公的統計データに対するプライバシー保護のあり方が多様な様相を呈している。例えば、アメリカ合衆国(以下「アメリカ」と略称)においては、アメリカセンサス局 (以下「センサス局」と略称) が、「フォーマルな(formal)」プライバシーの 1 つである、差分プライバシー (differential privacy, Dwork (2006)) の方法論に関して、2020 年のアメリカ人口センサス(以下「2020 年センサス」と呼称)の公表統計表への適用を図ってきた。そのため、センサス局は、2010 年のアメリカ人口センサス(以下「2010 年センサス」と呼称)を用いて差分プライバシーの実用性に関する検証を行ってきた。具体的には、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 を設定し、地域のレベルにおけるプライバシー損失予算の割り当て(TopDown アルゴリズム)に関する検証を進めてきた(Garfinkel et al.(2019), 伊藤他(2022))。

それに対して、ヨーロッパ諸国、とくにイギリスにおける公的統計のプライバシー保護をめぐる最近の動きについては、以下の注目すべき点を指摘することができる。第 1 は、攻撃者(侵入者、intruder)のシナリオ(戦略、scenario)を想定し、露見リスク(disclosure risk)の定量的な評価も踏まえた上で[1]、公的統計の匿名化されたミクロデータの作成・提供が展開されていることである。第 2 は、イギリスの 2021 年センサスにおいては、攪乱的な秘匿処理の手法、とりわけ cell key method の実用化に向けた追究を行っていることである。第 3 は、欧州統計局(Eurostat)が、差分プライバシーの方法論の人口センサスへの適用可能性を追究していることから、イギリスにおいても、統計作成部局において差分プライバシーの検討がなされてきたが、2021 年の人口センサスでは、差分プライバシーの採用が見送られたことである。

このように、アメリカとイギリスでは、公的統計を含む大規模データのプライバシー保護について異なる様相を呈している。そこで本稿では、アメリカとイギリスにおける公的統計データを含む大規模データに対するプライバシー保護の最近の動向に焦点を当て、その特徴とさらなる方向性について論じることにしたい。

2. アメリカセンサス局における公的統計データの秘匿措置に関する最新動向[2]

アメリカセンサス局は、2020 年センサスにおいて秘匿措置の考え方を大幅に刷新し、これまでの人口センサスで実施してきた慣用的な手法 (セル秘匿やスワッピングなど) による個別的 (ad hoc) な秘匿措置の適用から、差分プライバシーに基づくフォーマルなプライバシー (formal privacy) の実現へと移行した。本節では、2020 年センサスへの差分プライバシー導入の背景や、その実現手法および実現までの流れについて概観する。

2.1 2020 年センサスへの差分プライバシー導入の背景

2020 年センサスにおける差分プライバシー導入の背景として、オープンデータ化に伴う「モザイク効果」のプライバシーリスクが無視できないものとなり、「再構築攻撃」に関する評価実験を通じてその脅威が定量的に確認されたことが指摘できる。

---

[1] イギリスにおけるシナリオに基づく露見リスクの定量的な評価の特徴については、伊藤(2011)を参照。

[2] 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人口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

モザイク効果 (mosaic effect) とは、「個々のデータセット単体では安全であっても、他のデータセットと組み合わせると（個人の再識別などの）プライバシー暴露を引き起こしうる」という事象を指す言葉である。その存在自体は潜在的なリスクとして 1970 年代から知られていた(Smith et al. (1996)) が、近年の計算機環境の進化やオープンデータ化の進展に伴い、現実的な脅威として注目されるようになってきた。

アメリカのオープンデータ政策において、モザイク効果によるプライバシーリスクはデータの公開時に考慮すべき事項として明示的に位置付けられている。2013 年 5 月、アメリカ行政管理予算局 (Office of Management and Budget) は「オープンデータ政策」に関する覚書 (Burwell et al. (2013)) において、各政府機関は「モザイク効果」がもたらすプライバシーリスクを考慮しなければならないとし、そのために必要な分析は、必要に応じて他の専門機関などの助けを借りつつも、最終的には各機関の責任において実施すべきとした。

また、「再構築攻撃 (reconstruction attack)[3] 」(Dinur and Nissim (2003)) は、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手法であり、モザイク効果によるプライバシーリスクを具体的なプライバシー攻撃手段に適用したものと言える。また、データの重ね合わせを通じてプライバシーを暴露するという観点からは、統計的開示制御 (statistical disclosure control) の分野で指摘される攻撃リスクの一つである「差分による開示 (disclosure by differencing, Hundepool et al. (2012))」も再構築攻撃の一種とみなすことができる。

センサス局は、これらの脅威に鑑み、2010 年センサスの集計表に対して再構築攻撃を実験的に適用し、その脅威を定量的に分析した。その結論として、これまでの (スワッピングなどの) 慣用的な秘匿措置では、すでにプライバシーが十分に保護できなくなっていることが明らかになった。以下にその結果の一部を示す (Abowd (2021))。

- 2010 年センサスの集計表への再構築攻撃の適用により、アメリカ国民の 46%（約 1.44 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）。
- その復元結果を一般に入手可能な市販データと照合することにより、約 5,200 万人分のレコードについて再識別（個人特定）された。これは、アメリカ国民の約 17%に相当する。

再構築攻撃による新たな脅威の発見は、既知の攻撃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。再構築攻撃においては、重ね合わせるデータの組み合わせが変われば導出される制約充足問題も変わるため、ある特定のデータの組み合わせが再構築攻撃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。

これは、少なくとも再構築攻撃によるプライバシー暴露のリスクを考慮すると、既知の攻撃に対して安全と言えるだけでは不十分であり、未知の攻撃も含めた安全性を考慮する必要があることを意味しており、センサス局が 2020 年センサスにおいて差分プライバシーに基づくフォーマルなプライバシー保護を必要とした技術的な背景として指摘できる。

差分プライバシーは、未知の攻撃を含めた任意の攻撃に対する「包括的 (ad omnia)」な安全性 (Dwork (2007)) を実現することを目的としたプライバシー保護の枠組みであり、様々なプライバシー保護手段に対して統一的な安全性指標を定量的に与える。この指標は $\varepsilon\ (\geq 0)$ で表され、その値が小さいほど安全性が高いことを示す[4]。

あるプライバシー保護手段$\mathcal{M}$のプライバシー損失がε以下であることが保証されるとき、

[3] データベース再構築（database reconstruction）攻撃とも呼ばれる。

[4] なお、決定論的手法に対しては $\varepsilon \to \infty$ となる（安全性が与えられない）。

$\mathcal{M}$は ε-差分プライバシーを満たすと呼び、より厳密には以下の通り定義される。

定義１　任意の隣接したデータベース D_1 と D_2 $(D_1, D_2 \in \mathcal{D})$ に対し、ランダム化関数 $\mathcal{M}: \mathcal{D} \to \mathcal{R}$ が下式を満たすとき、$\mathcal{M}$ は ε-差分プライバシー (ε-differential privacy) を満たす。ただし、ここでSは $\mathcal{M}$ の出力空間 $\mathcal{R}$ の任意の部分空間である $(S \subseteq \mathcal{R})$。

$$Pr[\mathcal{M}(D_1) \in S] \leq e^{\varepsilon} \cdot Pr[\mathcal{M}(D_2) \in S].$$

この定義は、直感的には「A さんのデータが含まれるデータベース D_1 への $\mathcal{M}$ の適用結果と、A さんのデータが含まれないデータベース D_2 への $\mathcal{M}$ の適用結果との見分けがつかなければ、$\mathcal{M}$ の出力がA さんのプライバシーを侵すことはない」と解釈でき、ε が小さいほど「見分けがつきにくい」、つまりプライバシーが強固に保護されることを意味する (寺田 (2019))。

逆に言えば、εは「$\mathcal{M}$の出力によりプライバシーがどれだけ損なわれるか」を示す指標であるとも言える。この性質から、εは「プライバシー損失（privacy loss)」もしくは「プライバシー損失予算（— budget)」とも呼ばれる。

2.2 2020 年センサスにおける露見回避システム (2020 DAS) の実現方式

アメリカの人口センサスにおいて、集計表からのプライバシーの暴露を防ぐためのデータ加工システムは露見回避システム（disclosure avoidance system, DAS）と呼ばれ、たとえば 2020 年センサスの露見回避システムは 2020 DAS と呼称される。2020 DAS の特徴として、トップダウンアルゴリズムと呼ばれるセンサス局により新規開発された差分プライバシーの実現方式を備えること、および (2020 年 9 月以降は) zCDP と呼ばれる「レニー情報量」に基づく安全性指標を通じて差分プライバシーが保証されていることが挙げられる。

2020 DAS における差分プライバシーの実現方法は、Laplace メカニズムなどの一般的な差分プライバシーの実現方法とは異なる。これは、単に集計値に対して Laplace メカニズムを適用 (Laplace ノイズを付与) すると、マイナスの人口を持つ地域 (たとえば人口が -2 人のブロックなど) が発生したり、ノイズによる誤差の積み上がりによって、郡 (county) や州 (state) などの上位の集計単位における人口の誤差が過大になったりする問題が発生するためである (寺田他 (2015))。

上記の問題を解決し、人口センサスの集計結果に望まれる性質を保ちつつ差分プライバシーを保証するために、センサス局は「トップダウンアルゴリズム (top down algorithm, TDA)」と名付けられた手法を開発し、2020 DAS に実装した。この手法は、アメリカ全体→州→郡→…→センサスブロックの順に (つまりトップダウンに)、ノイズの付与と上位の集計結果との矛盾の解消（事後処理）を繰り返すことにより、前述のマイナスの人口やノイズによる誤差の積み上がりなどの問題を解決する[5]。また、法的に正確な値の公表が求められる数値 (invariants) との矛盾も併せて解消するなど、制度的な要請も充足するよう設計されている (US Census Bureau (2021b))。

また、2020 DAS は、もともと定義 1 で示した「純粋な」差分プライバシー (pure DP) を保証するものとして設計された。しかし、2020 年 9 月から、DAS は差分プライバシーを直接的に保証するのではなく、zero-concentrated differential privacy (zCDP, Bun and Steinke (2016)) と

[5] わが国の国勢調査に基づくメッシュ人口統計に対し、類似した考え方に基づき、ウェーブレット変換を用いて「トップダウンに」上位の集計結果 (より粗いメッシュの部分和) との矛盾や非負制約の逸脱を解決する、差分プライバシーの実現方式と適用結果が報告されている (寺田他 (2015),伊藤・寺田 (2020))。

呼ばれる差分プライバシーの亜種を保証した上で、zCDP における安全性指標 (ρ)と差分プライバシーの安全性指標 (ε) との間に成立する換算式を用いて、DAS のプライバシー損失予算を計算する、という変則的な形で差分プライバシーを保証している[6]。

zCDP は差分プライバシーよりもさらに新しい概念 (2016 年に提案) であり、定義 1 の代わりにレニー情報量（Rényi divergence）を用いて $\mathcal{M}(D_1)$と $\mathcal{M}(D_2)$の分布の近さを定義し、これに基づいて安全性指標 $\rho\ (\geq 0)$ を定める。zCDP は、安全性指標 ρ を用いて以下の通り定義される[7]。

定義 2 任意の隣接したデータベースD_1とD_2 $(D_1, D_2 \in \mathcal{D})$、および任意の $\alpha \in (1, \infty)$ に対し、ランダム化関数$\mathcal{M}: \mathcal{D} \to \mathcal{R}$ が下式を満たすとき、$\mathcal{M}$は ρ-zCDP を満たす。ただし、ここで $\mathrm{D}_\alpha(\mathcal{M}(D_1)||\mathcal{M}(D_2))$ は $\mathcal{M}(D_1)$ の分布と $\mathcal{M}(D_2)$ の分布との間の α-レニー情報量 (α-Rényi divergence) である。

$$\mathrm{D}_\alpha(\mathcal{M}(D_1)||\mathcal{M}(D_2)) \leq \rho\alpha$$

$\alpha \in (1, \infty)$ において、α-レニー情報量とは、確率分布間の差異を測る尺度の一種であり、$\alpha \to 1$ のとき KL-divergence (D_{KL}) に対して、$\alpha \to \infty$ のとき max-divergence (D_∞) に対してそれぞれ漸近する[8] (Erven and Harremos (2014))。これは、Laplace ノイズより分布の裾が軽いガウスノイズを効率的に扱うことを可能とし、複数のメカニズムを組み合わせたときの安全性をより適切に（安全性マージンを大きく取ることなく）計算可能とするなど、データの有用性確保に有利な効果を与える。

その一方、zCDP の安全性指標であるρの値が持つ意味は、差分プライバシーの安全性指標ε以上に解釈が難しい。また、センサス局は、2020 年センサスに差分プライバシーを導入すると説明してきており、zCDP について言及することはなかった。そこで、zCDP の安全性指標 ρ そのものをプライバシー損失予算とするのではなく、上記の通り換算式を用いて ρ から ε を計算し、これを 2020 DAS のプライバシー損失予算としている。

2.3 ステークホルダープロセスを通じたプライバシー損失予算の決定

2020 年センサスへの差分プライバシーの適用にあたり、センサス局は「ステークホルダープロセス」を通じてアルゴリズムの改善とプライバシー損失予算の決定を行った。これは、2010 年センサスの個票データに対して 2020 DAS（のプロトタイプシステム）を適用したテストデータ (demonstration data) を作成し、その提供を受けたデータ利用者からのフィードバックを 2020 DAS に反映する、というプロセスの繰り返しとして実施された。

最初のプロトタイプ試験にあたる 2018 年 11 月の 2018 E2E Census Test DAS ではプライバシー損失予算として $\varepsilon = 0.25$ というかなり「安全側に倒した」値が用いられた。その後、2019 年 10 月のテストデータにおいて $\varepsilon = 6.0$ が採用された[9]後、2020 年 5 月～11 月のテス

---

[6] 厳密には、(ε, δ)-近似差分プライバシーと呼ばれる別の亜種を保証している。ただし、(ε, δ)-近似差分プライバシーは $\delta = 0$ において（純粋な）差分プライバシーと等価であり、センサス局は $\delta = 10^{-10}$ という十分に小さい値を用いているため、実務的にはその違いはほとんど無視できる。

[7] 正確には、zCDP にはパラメータが 1 つの定義 (ρ-zCDP) と 2 つの定義 ((ξ, ρ)-zCDP) が存在するが、本稿では簡単のため前者のみを与える。なお、2020 年センサスでも前者を用いている。

[8] なお、差分プライバシーは隣接するデータベースからの出力分布間の max-divergence の上界としても定義できることから、定義 2 の式において $\alpha \to \infty$ とし、右辺を定数 (ε) とすると定義 1 と等価になる。

[9] 本稿でのプライバシー損失予算の推移に関する記載は JASON (2022) によるが、文献によりゆらぎがあることに

トデータでは、さまざまなアルゴリズムの改善（前述の zCDP の導入も含む）を重ねつつ、いずれも $\varepsilon = 4.5$ が採用され、最終的にこの値に収束することが推測された。

しかし、ステークホルダープロセスの最後にあたる 2021 年 4 月に $\varepsilon = 4.5$ と $\varepsilon = 12.2$ の２種類のテストデータが提供され、2021 年 6 月には個人単位のデータについて $\varepsilon = 17.14$、世帯単位のデータについて $\varepsilon = 2.47$（合計 19.61）という値にまでプライバシー損失予算を引き上げることが決定された。この値に基づき、2020 年センサスによる区画改定データ (PL94-171) は 2021 年 8 月 16 日に公表されている。

3. 2020 年センサスへの差分プライバシー導入に対する議論

2020 年センサスにおける、差分プライバシーに基づく「フォーマルな安全性」の適用は、アメリカにおいても賛否両論を巻き起こした。本節ではそれらの反響や議論について、差分プライバシー導入の必要性、統計データの有用性、プライバシー損失予算の妥当性、の 3 種類の観点から概括して議論する。

3.1 差分プライバシー導入の必要性に関する議論

前述の通り、2013 年以降のアメリカのオープンデータ政策ではモザイク効果によるプライバシーリスクへの考慮が明示的に求められるようになり、さらに再構築攻撃に関する評価実験を通じて 2010 年センサスにおける伝統的な秘匿手法の脆弱性が定量的に判明したことから、センサス局にとって 2020 年センサスでのこれらへの対応は必然であったと考えられる。たとえば US Census Bureau (2021a) において、センサス局は 2020 年センサスへのセル秘匿 (suppression) やスワッピングの適用可能性について明確に “No”と否定している。

これに対する反論として、たとえば Ruggles (2021) は独自の攻撃評価を通じ、自らの実験において再識別の成功率が低いものであったことから、センサス局は再構築攻撃のリスクを過大評価している、と主張している。しかし、評価の際に用いた攻撃手法が稚拙であれば、当然ながらその成功率も低いものになる。したがって、ある評価において攻撃成功率が低かったことをもって、その安全性を主張することはできない。前述のデータプライバシー専門家の意見書においても、Ruggles (2021) による評価結果は分析手法が単純すぎて実際のリスクを過小評価しているとして批判されている。また、Cohen et al. (2022) は、TDA の選挙区割りへの影響に関する評価 (後述) の一環で、アリゾナ州ナバホ (Navajo) 郡の 2010 年センサスデータから、元の個票を完全に再構築したとしている。

また、再構築攻撃への対抗手段としてセンサス局は差分プライバシーを導入したが、それ以外の手段は存在しなかっただろうか。これについて、センサス局は差分プライバシー以外に有効な方法論は知られていないとしており、この見解は、アラバマ州との裁判におけるデータプライバシー専門家の意見書 (Calo et al. (2021)) や EPIC の意見書 (Electronic Privacy Information Center (2021)) でも支持されている。

3.2 統計データの有用性に関する議論

データの有用性確保とプライバシーの保護はトレードオフの関係にある。2020 DAS における TDA の適用によるノイズの付与が、どの程度データの有用性に影響を与えるかについ

留意が必要である。Garfinkel (2022) は 2019 年 10 月のテストデータでは $\varepsilon = 4.5$ を採用したとしており、伊藤他 (2022) はこれに従って議論されている。

て、特に選挙区割りにおける一票の価値の保証[10]や、ゲリマンダリング[11]対策などの観点から注視された。

2020 年センサスで (差分プライバシーを適用した上で) 最初に公表されたデータは PL94-171 と呼ばれる区画改定データであり、これは選挙区割りに用いられる重要なデータである。そのため、PL94-171 への差分プライバシーによる正確性への影響は、アメリカ各州の州政府や州議会による関心の対象となり、いくつかの州はステークホルダープロセスにおいて、センサス局に対して区割りへの影響への配慮や改善を求める書簡を送付している。

ただし、選挙区割りに関しては、差分プライバシーの導入による影響は実際のところ実務的には限定的であるとの評価がなされている。Cohen et al. (2022) は、選挙区割りへの影響に対する定量的な評価として、テキサス州とアリゾナ州のいくつかの郡 (county) を対象として、2010 年センサスのデータに基づき、2010 年センサスデータをそのまま用いた場合と、$\varepsilon = 1$ の条件下[12]で TDA を適用した場合とを比較評価した。その結果、適切な方法で区割りをすれば一票の価値に対する影響はほぼ無視できることや、TDA の適用により導入される誤差は、他の原因による既知の誤差よりもかなり小さく、検出できるグループレベルの偏りは、既知の過少カウントパターンよりもはるかに微妙であることが、少なくとも評価対象の地域に関しては結論づけられるとしている。

3.3 プライバシー損失予算の妥当性に関する議論

2020 年センサスの PL94-171 におけるプライバシー損失予算 ε の値は、ステークホルダープロセスにおけるほとんどのテストデータにおいては $\varepsilon = 4.5$ が採用されてきたが、その最終局面において大幅に増加し、最終的に $\varepsilon = 19.61$ に決定された。この値について、センサス局からの諮問を受けたアメリカの科学者グループである JASON は、差分プライバシーによる数理的な安全性保証を享受するには不十分な（高過ぎる）値であるとしている(JASON (2022))。

2020 年センサスにおいて、プライバシー損失予算がここまで大きくなった理由としては、技術的な要因と社会的な要因の双方が指摘される。まず、技術的な要因としては、PL94-171 が数多くの属性を持つ「細かい」集計表であり、データの安全性と有用性のトレードオフを検討するにあたって厳しい条件をもたらすことが指摘される。JASON (2022) は、センサスブロック単位での属性ごとの集計値の公表中止など、作成する集計表の粒度を粗くすることをセンサス局に対して推奨している。

その一方、社会的な要因としては、当時のアメリカの政治的な背景により、プライバシー保護団体などのプライバシー保護を重視するステークホルダーが十分に関与できなかったことなどが指摘されている (Garfinkel (2022))。JASON (2022) も、ステークホルダープロセスの重要性に関しては評価しつつ、2020 年センサスにおける進め方は安全性の低下に歯止めが効きにくいとしている。

また、このプライバシー損失予算の急激な増加は、2021 年 3 月に提訴されたアラバマ州に

[10] アメリカでは「一人一票 (“One Person, One Vote”)」の判例があり、市議会のような小さな選挙区から、議会のような大きな選挙区まで、選挙区全体の人口バランスを取ることが求められている。

[11] ある政党にとって有利となるように、恣意的に選挙区割りを実施すること。選挙区ごとのマイノリティの割合が問題になることが多いことから、人種別の人口の正しさが重要となる。

[12] 最終的に採用された ε の値より大幅に小さい値であることに注意。

よる 2020 年センサスへの差分プライバシーの適用差し止めを求めた訴訟[13] (*Alabama v. U.S.Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021)) の係争中に実施されたことにも注目すべきであろう。本訴訟において、原告側は差分プライバシーに対する誤認や知識不足から十分な論拠を示すことができず[14]、2021 年 6 月 29 日にほぼ全面的な原告敗訴の形で判決が下された (Newsom et al. (2021))[15]。センサス局自身は 2021 年のプライバシー損失予算の急激な増加と本訴訟との関係について特に言及していないが、この訴訟にはアメリカ投票権法に関連した政治的な動機も指摘される (Percival and Dennie (2021)) ことから、もしこの訴訟や、その背景となった当時のアメリカにおける政治的混乱がなければ、プライバシー損失予算は異なる値となった可能性も考えられるだろう。

なお、$\varepsilon = 19.61$ というプライバシー損失予算の値をどう解釈すべきかについて、2020 DAS は zCDP から DP への換算式を通じて間接的にこの値を得ていることに留意が必要である。この換算式は厳密 (tight) ではなく、実際より安全性を過小評価する性質を持つ。JASON (2022) の分析においても、実効真陽性率 (Effective TPR) の観点で（正式版の）2020 DAS の安全性を評価したところ、純粋な差分プライバシーにおける $\varepsilon = 6.0$ 未満に相当するとの結果を得ている。ただし、この分析も完全なものではなく、より正確な評価には差分プライバシーにおける安全性マージンの存在 (寺田 (2018)) や、前述の invariants による影響なども含めて検討する必要があると考えられ、今後のさらなる議論が望まれる。

4. イギリス国家統計局における公的統計データの作成・提供と秘匿措置に関する最近の動向

ヨーロッパ諸国では、法制度的かつ統計技術的な側面から様々な秘匿措置を施した上で、公的統計データの作成・提供が進められてきた。イギリスについて見れば、イギリス国家統計局(Office for National Statistics=ONS、以下「ONS」と呼称)が、人口センサスを中心にオープンデータとしての各種の統計表を公表するだけでなく、公的統計ミクロデータの作成・提供を行ってきた。イギリスにおける統計表の作成・提供の最近の動きとして注目すべき点は、2 節で議論されたデータベース再構築攻撃への対応策として、イギリスでも攪乱的手法を用いた秘匿処理をより積極的に適用する方向に向かっているだけでなく(Spicer(2020))、利用者のニーズに応じる形でオンデマンド型の集計による統計表の作成・公表が展開されていることである。

一方、公的統計ミクロデータの利用サービスについては、ONS に設置されている Secure Research Service(SRS)におけるオンサイト施設で公的統計の個票データの利用が可能であるが、アメリカとは異なり、個票データの利用に関しては、大学の研究室からのリモートアクセスも、広範に展開されてきたことが特徴的だと言える(伊藤(2016))。また、公的統計の匿名化されたミクロデータに関しては、各種の匿名化技法を適用することによって、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)

---

[13] 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、（センサス局が属する）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。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、連邦法に違反すると主張した (State of Alabama et al. (2021))。

[14] 原告側の差分プライバシーに関する主張の一貫性の欠如は、判決時における判事補足意見でも強く批判されている (Newsom (2021))。

[15] 最終的に、本訴訟は 9 月 9 日の原告取り下げにより結審している。

が作成されてきたが(伊藤(2018))、イギリスの場合、前者については、公的統計や社会調査を対象としたライセンス(End User Licence)を必要とするタイプのミクロデータ（以下「ライセンス型ミクロデータ」と呼称）、後者に関しては、人口センサスの教育用の一般公開型ファイル(Public Use File)が提供されてきた(伊藤(2020))。本節では、イギリスを例に、公的統計データの作成・提供、およびそのために講じられる秘匿措置の最近の動向について概括する。

4.1 2021 年人口センサスにおける cell key method と targeted data swapping の実用化の追究

ヨーロッパ諸国では、匿名化ミクロデータを作成するために、非攪乱的手法だけでなく、攪乱的手法も用いられてきた(伊藤(2018), 伊藤(2020))。イギリスにおいては、人口センサスの匿名化ミクロデータの作成において、ONS が攪乱的手法の１つであるスワッピングを採用した。具体的には、元データとなる個票データに対して、2001 年人口センサスではランダム・スワッピング(random data swapping)、2011 年人口センサスにおいては、ターゲット・スワッピング(targeted data swapping)を適用する方法が採られてきた。また、教育用の一般公開型ミクロデータの作成においても、スワッピングが適用されたことが知られている(伊藤(2020))。

ヨーロッパ諸国においては、近年オンデマンド集計システムに対する社会的な関心が高まっている。例えば、Eurostat は、オーストラリア統計局の TableBuilder(伊藤他(2018))を参考にして、攪乱的手法としての cell key method を用いたオンデマンド集計システム Confidentiality on the fly の開発に取り組んできた。

cell key method は、オンデマンドで作成された集計表の各セルに対してランダムにノイズを付与する手法であり、次のような特徴を備えている(伊藤他(2022))。第１は、各セルに攪乱を行うためのルールとして、セルに含まれる度数の区分と後述する cell key と呼ばれる数値群がクロスされたノイズに関する表である p table を予め設定することである。第２は、cell key の元になる record key と呼ばれる一様分布の乱数を集計前の各個体レコードに付与していることである。第３は、特定の変数群を対象に個体レコードを集計するだけでなく、個体レコードに付与される record key の集計も同時に行うことによって、集計表に含まれるセルの度数に対応する cell key の数値を算出していることである。第４は、求められた各セルの度数と該当する cell key の数値から p table で対応するノイズの値を特定し、そのノイズを元の集計値のセルに含まれる度数に付加した上で集計表の提供を行っていることである。

こうしたターゲット・スワッピングと cell key method の実用化の動きに対して、欧州委員会(European Commission)は、2021 年人口センサスデータの作成・公表において適用すべき攪乱的手法として、ターゲット・スワッピングと cell key method を推奨した。それを受ける形で、ヨーロッパでは、Eurostat の資金援助によって 2016 年において実施されたプロジェクト「ヨーロッパ統計システムにおけるセンサスデータに関する調和化された保護措置(Harmonised Protection of Census Data in the ESS)」およびその後継のプロジェクトによって、cell key method の実装化が進められている[16]。

ターゲット・スワッピングと cell key method を組み合わせることによって秘匿処理が施されたデータにおける有用性と秘匿性に関しては、Eurostat が定量的な評価を行っている。具体的には、スワッピングおよび cell key method の処理のステップについて SAS によるプログラムを実行した上で、ターゲット・スワッピングと cell key method の有効性の検証を行っている。なお、これらの検証結果については、有用性の評価に関する結果のみが公表されてい

[16] 具体的には、オランダ統計局が開発した集計表の秘匿処理用のツールである τ-Argus において、現在 cell key method のプログラムが搭載されている。また、オープンソースのソフトウェアである R においても、集計表の秘匿処理を行うための cellKey package と呼ばれるプログラムの利用が可能になっている(de Wolf(2021))。

る[17]。

ONS は、公的統計に対する cell key method の適用可能性を追究してきた(Office for National Statistics(2017))。そして ONS は、2021 年人口センサスの統計表の作成・公表に関する計画として、基本的な人口社会的な属性に関する統計表には、集計計画で策定された(ready-made)統計表を作成・公表するものの、多次元の集計表に関しては、「オンデマンド型公表システム(Flexible Dissemination System)」[18]の下で、集計項目の数やそれに含まれるカテゴリー数を利用者が選択し、オンデマンドで提供する計画であることを発表した(2022 年 3 月時点)[19]。

図 1 は、オンデマンド型公表システムのイメージ図を示したものである。最初に、原データに対してターゲット・スワッピングが適用される。このスワッピング済みデータがオンデマンド型公表システムにおいて多次元統計表を作成・公表するための元データとなる。利用者がオンライン上で変数を選択することによって、それらの変数を集計項目とする統計表が作成されるが、cell key method に基づいて、統計表の全てのセルにはノイズが付与される。その後の秘匿処理として注目すべき点は、オンデマンド型公表システムには、作成された統計表から個体情報が露見されないような自動化された露見チェック(automated disclosure check)の仕組みが備わっていることである。自動化された露見チェックのプロセスにおいては、集計された統計表の中に、①極端にスパース(sparce)な統計数値(当該度数は 1 でそれ以外のセルがゼロになるような数値)が存在するか、②統計表に含まれるセルの度数が個別の属性値あるいは集団の属性値と対応関係にあるために、個体の属性値が漏洩されるか(属性漏洩(attribute disclosure))、③統計表の中に個体の特定につながる度数 1 となるセルが発見されるか(個体識別漏洩(identity disclosure))が、主たる露見チェックの対象となる(Blanchred(2019))。秘匿性の観点から提供可能と判断されれば、このチェック済みの統計表を利用者はダウンロードすることが可能になる。しかしながら、露見リスクの観点から作成された統計表の公表が困難と判断されれば、変数の分類区分や地域の区分の統合を行った上で、再度集計が実行されるか、あるいは利用者はオーダーメイドの集計表(commissioned table)を ONS に依頼することを選択する。このように、オンデマンド型公表システムでは、ターゲット・スワッピングと cell key method だけでなく、秘匿に関するルールに基づく自動化された露見チェックが用いられることによって、利用者が求める統計表に対して弾力的に秘匿処理を施した上で公表可能な統計表を作成・提供していることが、2011 年までのイギリス人口センサスの統計表とは大きく異なる点だと言える。

オンデマンド型公表システムの実用化にあたっては、ターゲット・スワッピングについてはスワッピング率、cell key method に関しては p-table におけるノイズの数値の設定が事前に求められる。cell key method におけるパラメータの設定にあたっては、データの有用性を重視する形での攪乱(“a light touch cell key perturbation”)が指摘されている。また、オンデマンドで統計表が提供される前の自動化された露見チェックに関しても、差分攻撃(differencing)の

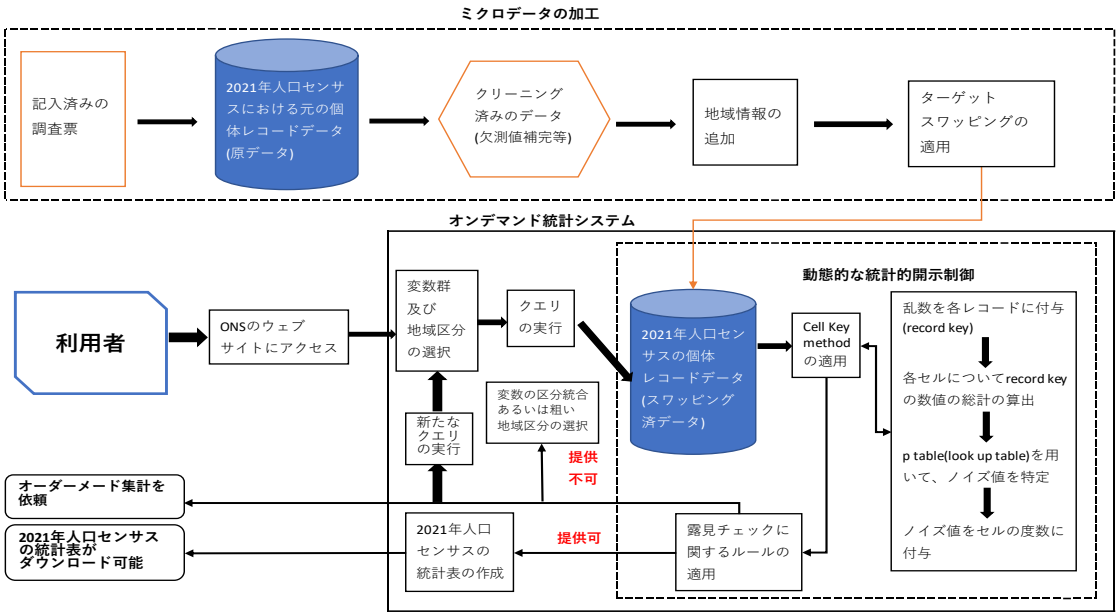
---

[17] 以下の報告書を参照。
Harmonised protection of census data in the ESS
https://ec.europa.eu/eurostat/cros/system/files/how_to_test_methods_for_protecting_census_data_0.pdf

[18] ONS は、オンデマンド型公表システムの開発において、Cantabular 社との委託契約を締結し、Cantabular 社によるオンデマンドの統計表における秘匿処理のためのシステム開発およびそれに関する技術的な支援を受けている(Thompson(2022))。なお、Cantabular 社のよるオンデマンド型公表システムの研究開発の状況については、以下の URL を参照。
Modernising statistical data dissemination with the Office for National Statistics in the United Kingdom
https://sensiblecode.io/resources/case-study-ons.pdf

[19] オンデマンド型公表システムにおいては、詳細な地域レベル(Output Area)の統計表の提供も可能になっている。

図１　オンデマンド型公表システムのイメージ



出所　https://unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.41/2017/Meeting-Geneva-Oct/Day3_1000_UK_UNECE_ONS_Flexible_dissemination_for_2021_Census.pdf をもとに筆者が作成。

リスクを想定した上で露見のチェックに関するルールが検討されてきた(Spicer(2020))。

このように、ONS は、2021 年人口センサスにおいて、過去の人口センサスでも用いてきたスワッピングに加えて、Eurostat 等で検討を進めてきた cell key method を新たに採用する形で、オンデマンド型の統計表の作成に関する新たな可能性を提示していると言える。

4.2 イギリスによる人口センサスの統計数値に対する差分プライバシーの可能性の検討

近年ヨーロッパにおいても、差分プライバシーの適用可能性に関する議論が展開されている。Eurostat は、欧州委員会によって人口センサスの適用に推奨された cell key method だけでなく、差分プライバシーについても、人口センサスの統計数値に対する攪乱的手法の適用可能性の検討を行ってきた(Bach (2022))。Eurostat では差分プライバシーを適用する上で、秘匿性と有用性の両面から、適用可能なノイズの範囲について検証している。具体的には、「厳密な(strict)」ε -差分プライバシーを適用してノイズの設定に対して制限を設けない(unbounded)場合と「緩やかな(relaxed)」(ε,δ)-近似差分プライバシーを適用してノイズの設定に制限がある(bounded)場合の両方で、定量的な評価を行っている。

Bach (2022)は、差分プライバシーは特定の統計表に依拠しない形で、個体情報の特定化のリスクを定量化に評価する上で有益な基準であることから、各種の匿名化技法におけるリスクの水準を定量的に比較することが可能であることを指摘している。また、差分プライバシーは、オンデマンドで得られる統計数値(flexible output)に対して求められる自動的なノイズの設定においてもリスク評価のための基準を与えることも論じている。

統計表における集計項目が増大するにしたがって、差分プライバシーによってセルの結果数値に付与されるノイズをより細かく設定することが求められるから、それは過大な秘匿処理が生じる可能性がある。そのことは、利用者にとって有用性の低下をもたらす。このことから、集計項目が事前に定められている詳細な統計表(complex static output)に対するノイズの設定については、取り扱いに留意する必要があることも指摘されている。

イギリスにおいても、ONS が内部で差分プライバシーの適用可能性に関する検討を行ってきた。具体的には、死亡のデータを用いて、①各種の統計表にプライバシー予算 ε を割り当てて、度数表のセルに直接ノイズを付与する方法や、②センサス局で検討されてきた方法を参考にした上で「トップダウン法(“top down method”)」についての実験が行われてきた(Dove(2021))。しかしながら、検証結果では、構造的ゼロ(structural zero)を含むセルや度数が小さなセルに差分プライバシーを適用した結果、負の数値が生成され、それをゼロに置き換えることによるバイアスが生じることが確認された。こうしたことから、ONS では、人口センサスにおける差分プライバシーの適用は、結果数値の有用性を重視する観点から、現時点ではあくまで検討の段階に過ぎないことが指摘される。

4.3 イギリスにおける人口センサスのミクロデータの提供について

イギリスでは、オンデマンド型公表システムの整備だけでなく、利用者のニーズに踏まえた形で複数のチャネルでミクロデータが提供されている(伊藤(2020))。そこで、本節では、ONS が現在準備を進めている 2021 年センサスのミクロデータに関する作成の方向を概括する。

2021 年人口センサスにおいては、ミクロデータの提供形態として、1991 年、2001 年と 2011 年のセンサスと同様に、複数のタイプのミクロデータファイルの作成・提供が計画されている[20]。第 1 のファイルは、Public-access sample と呼ばれる一般公開型ミクロデータである。このファイルは、個人を対象に最大で 1%のサンプルが抽出され、地方(region)レベルの地域区分が利用可能となっており、約 20 の変数を含んでいる。また、2011 年の教育用の一般公開型ミクロデータと同様に、ONS のウェブサイトから入手することが可能である。

第 2 のファイルは、Safeguarded microdata sample と呼ばれるライセンスが必要な匿名化ミクロデータであって、学術研究目的で UKDS から入手することが可能である。これについては 3 種類のミクロデータファイルの作成が計画されている。第 1 は、Safeguarded individual region sample というライセンス型ミクロデータであり、個人を対象に最大で 5%のサンプルが抽出され、地方レベルの地域区分が利用可能となっている。また、約 120 の変数が細かな分類区分で利用することができる。第 2 は、Safeguarded individual grouped local authority sample というライセンス型ミクロデータであって、個人を対象に最大で 5%のサンプルが抽出される。統合された地方自治体レベルの詳細な地域区分が利用できるが、ファイルに含まれる約 120 の変数は、Safeguarded individual region sample と比較して、より粗い区分でのみ利用可能になっている。第 3 は、Safeguarded household sample と呼ばれる階層構造を持つライセンス型ミクロデータであり、2021 年人口センサスで新たに作成・提供されるファイルとなっている。このファイルについては、世帯を対象に最大で 5%のサンプルが抽出され、地方レベルの地域区分が利用可能になっているだけでなく、粗い分類区分を持つ約 50 の変数が含まれている。階層的なファイル構造を有することから、個人に関する変数は制限されており、世帯に関する変数が設定されている。また、職業はファイルから削除されているが、その代わりに社会経済分類(National Economic Classification)と産業が利用可能になっている。

第 3 のファイルが、Secure microdata samples と呼ばれる一部のサンプルが抽出された個票

[20] 本節では、以下のサイトに基づいて論じている。なお、イギリス人口センサスに関する匿名化されたミクロデータの作成の経緯については、1991 年センサスに関しては森(2000)や伊藤(2011)、2001 年センサスについては伊藤(2011)を参照。なお、2011 年センサスも踏まえた形でのイギリスのミクロデータの提供状況に関しては伊藤(2020)も参照されたい。
Microdata Samples
https://www.ons.gov.uk/census/censustransformationprogramme/census2021outputs/2021dataproducts/microdata

データである。これについては、2011 年センサスと同様に、2 種類のファイルが存在する。第 1 は、Secure individual file と呼ばれる個票データであって、個人を対象に最大で 10%のサンプルが抽出され、地方自治体レベルの地域区分が利用可能である。これについては、約 200 の変数が含まれている。第 2 は、Secure household file と呼称される個票データであって、世帯を対象に最大 10%のサンプルが抽出されている。また、Secure individual file と同様に、地方自治体レベルの地域区分が含まれており、約 200 の変数が利用可能である。これらの Secure microdata samples については、「承認された研究者(approved researcher)」[21]あるいは「認定された研究者(accredited researcher)」のみが、SRS のオンサイト施設のようなセキュアな環境でアクセスすることができる。なお、Secure microdata samples においては、他のデータとのリンケージを行うための個体識別情報は除外されている。しかしながら、「認定された研究者」が、学術研究目的のために、ONS に対して学術研究プロジェクトとしてのリンケージによる人口センサスの個票データの利用申請を行い、ONS がその申請を容認した場合には、リンケージが可能な ID を付与された非識別データ(deidendified data)を SRS の内部で利用することができる。

なお、2021 年センサスで新たに作成されるミクロデータファイルには、ミネソタ大学が提供している、海外の人口センサスを対象にした「統合された一般公開型ミクロデータ(Integrated Public Use Microdata Series=IPUMS)」プロジェクト用のミクロデータファイル(IPUMS sample)も含まれる。このファイルは、個人を対象に最大で 1%のサンプルが抽出され、地方レベルの地域区分が利用可能である。現在、IPUMS International において利用可能なイギリスのミクロデータファイルは、学術研究目的に対して利用可能な 1991 年と 2001 年の人口センサスの匿名化標本データ(Samples of Anonymised Records)である[22]。したがって、ONS は、IPUMS sample についても、ライセンス型ミクロデータとしての作成を計画していることが推察される。

このように、2021 年センサスでも、2011 年センサスと同様に、①一般公開型ファイル、②ライセンス型ミクロデータ、③個票データという 3 種類のミクロデータが作成・提供される方向になっている。その中で、①と②の匿名化されたミクロデータに関しては、攻撃者のシナリオを想定し、それに対応したキー変数を選定した上で、匿名化措置が適用されているということができる。

4.4 攻撃者のシナリオに基づく公的統計ミクロデータの作成・提供[23]

イギリスの場合、公的統計の匿名化されたミクロデータを作成・提供を行うにあたって、統計作成部局が、攻撃者による個体情報の特定に関する複数のシナリオを想定した上で、提供用のミクロデータの作成を行っていることが特徴だと言える。ONS は、以下の 3 つのシナリオを想定している。

シナリオ 1　　公開されているデータセットを利用すること

シナリオ 2　　特異な属性の組み合わせを有している等、悪意がないような形で個体が偶発

---

[21] 承認された研究者については、伊藤(2016)を参照。

[22] 例えば、IPUMS International でウェブサイトにおいて情報提供している 2001 年人口センサスの匿名化標本データ(Samples of Anonymised Microdata)の概要については、以下のサイトを参照。
https://international.ipums.org/international-action/sample_details/country/uk#tab_uk2001a

[23] 本節の執筆にあたっては、以下のウェブサイトを参照した。
Policy for Social Survey Microdata
https://www.ons.gov.uk/methodology/methodologytopicsandstatisticalconcepts/disclosurecontrol/policyforsocialsurveymicrodata

的に特定されること(偶発的な個体特定(spontaneous recognition))
シナリオ 3　　個人に関する私的な情報を持っており、詮索好きの隣人(nosy neighbour)がいること

上記の 3 つのシナリオの中で、ONS はシナリオ 1 とシナリオ 2 を特に重要視している。シナリオ 1 は、公開されているデータセットを用いて、匿名化されたミクロデータとのマッチングを実行することであって、個体識別による露見(identification disclosure)のリスクや個体情報に含まれるセンシティブな属性に関する漏洩(属性漏洩、attribute disclosure)のリスクが想定される。そのため、個体識別による露見リスクや属性漏洩を制御するための匿名化技法の適用が求められる。また、シナリオ 2 の偶発的な個体特定とは、珍しい属性の組み合わせを持つ個体が、データの利用者によって、偶発的に母集団の中で特定されることである(Duncan et al.(2011, p.35))。公開されている情報を利用して、ミクロデータの中に特定の個人や企業が存在することを意図せざる形で攻撃者が把握する可能性がある。具体的には、回答者が特異な属性を有している、あるいは特定の個人が一般に知られていたり、ある企業が攻撃者によって認識されていたりする場合であって、攻撃者が悪意を持って個体の特定化を行わなかったとしても、偶発的な個体特定が発生することが指摘できる。なお、偶発的な個体特定について、攻撃者が使用する変数の例としては、個人の場合、名前、年齢、性別、結婚状態、所得、職業、住所と民族グループが、企業の場合、産業と所在地がそれぞれ指摘されている。

ONS は、こうした攻撃者によるシナリオを想定するだけでなく、露見リスクを有するレコードを探索し、該当するレコード群あるいは属性群に対して攪乱的手法を含む各種の匿名化技法を適用した上で、匿名化されたミクロデータの作成・提供を行っている。例えば、世帯・人口系の統計調査を対象にした場合、匿名化されたミクロデータの作成は、つぎの 5 つのステップによって行われる。①選定された変数群に関する集計表を作成し、母集団か標本で度数 1 を含むセルや特異な変数値の組み合わせによって発見される度数の小さなセルの分布特性を確認する。②①のステップで該当するセルが存在する場合に、対象となる変数やレコードに対して、変数やレコードの削除(data suppression)、リコーディング(recoding)、スワッピング(data swapping)といった匿名化技法を適用する。③②のステップで作成した匿名化されたミクロデータから、選定された変数群をもとに再度集計表の作成を行う。その場合、露見の可能性があるセルがなければ④のステップに進むが、露見リスクが確認されるのであれば、さらなる匿名化措置を講じる。④攻撃者によるマッチングの検証(intruder testing)を実行する。⑤提供用のミクロデータに対して要求されるライセンス(利用者に制限が課せられたライセンスかオープンライセンス)を踏まえた形で、匿名化されたミクロデータの提供・公開を行う。なお、④のステップで、マッチングの成功件数が数多く存在する場合には、⑤に進む前に、②から④のステップが繰り返される。

攻撃者に関してどのようなシナリオを想定するかによって、また、どのような利用目的を想定して匿名化されたミクロデータを作成するかによって、匿名化の対象となるキー変数(あるいは準識別子)や適用される匿名化技法も異なる。「社会調査のミクロデータに関する露見制御のためのガイダンス―事例研究(GSS/GSR Disclosure Control Guidance for Microdata Produced from Social Surveys – Case Studies)」では、ミクロデータに対して匿名化技法を適用した事例が紹介されている。その 1 つは、資産調査(The Wealth and Assets Survey)のライセンス型ミクロデータの作成に関するものである。この調査は、ONS がイングランド、ウェールズとスコットランドを対象に、ライフコースにおける家計資産の変動を把握するための縦断調査であって、このミクロデータの提供は 2012 年より開始された。現在は「承認された研究者」の資格を有する研究者に対してのみ、UKDS(=UK Data Service)を通じて、ミクロデータの利用が可能になっている。しかしながら、承認された研究者の申請資格を有しない海外の

研究者からも、資産調査に関するミクロデータの利用に対するニーズがあることから、ライセンス型ミクロデータについても作成が進められた。

ONS は、資産調査のライセンス型ミクロデータの作成にあたって、攻撃者のシナリオとして、(1)公開されているデータセットの利用と(2)偶発的な個体特定を想定した。さらに、①資産調査が、約 3 万のサンプルサイズを有する縦断的な世帯・人口系の統計調査であること、②資産に関する変数群においては極端な外れ値があることを考慮した上で、秘匿処理の方法について検討を行った。なお、個体識別リスクを定量的に評価するためのキー変数として、地域、出生国、民族、宗教、性同一性(Sexual identity)、年齢、世帯人数、職業といった変数が選定されている。

ライセンス型ミクロデータを作成するために、①世帯人数 10 人以上の世帯の削除、②80 歳以上の年齢のトップコーディング、③家計資産に関する変数に対する秘匿処理が適用された。③に関しては、該当するすべての変数に対するトップコーディングの適用が、ライセンス型ミクロデータの作成に関するガイダンス(Government Statistical Service (2014a))においては求められるものの、資産に関する変数の利用者のニーズの高さに配慮するために、研究において相対的に重要度が低い変数を削除することで、金融資産に関する変数に対する秘匿処理を行わないという措置がなされている。また、追加的な秘匿処理として、①地域情報の削除、②出生国、民族、宗教、性同一性といったセンシティブで観察可能な変数の削除、③年齢や職業におけるリコーディング、④資産に関する変数についての外れ値への対応も行われている。

5. アメリカとイギリスにおける公的統計のプライバシー保護の比較・検討

これまで、アメリカとイギリスを例に、公的統計データにおけるプライバシー保護の現状について見てきた。アメリカでは、センサス局が、公表されたセンサスの結果数値から「データベース再構築攻撃」によって個体情報が特定されるリスクへの対応策として、2020 年センサスにおいて、Top down アルゴリズムに基づく差分プライバシーの方法論を適用した。センサス局が採用した差分プライバシーは、センサス局が公表する統計表に対する利害関係者や一部の利用者の反応を勘案しつつも、人口センサスの公表統計表の秘匿性を担保する観点から追究されたものであった。そこで、本稿の第 2 節と第 3 節では、最初に、差分プライバシーの方法論の導入に至った社会的背景と統計技術的な課題を述べた上で、2010 年センサスの個票データを用いた Top down アルゴリズムによるテストデータの作成とその有用性の検証を議論した。つぎに、差分プライバシーの設定におけるプライバシー損失予算 ε の数値の設定をめぐるセンサス局と利用者側との議論に関する論点を整理した。さらに、アメリカにおいて選挙区割りのためにセンサスデータが必要なことから、アラバマ州による差分プライバシー適用の差し止め訴訟を含む政治的社会的な反応を論じるだけでなく、JASON レポートにおいてプライバシー損失予算 ε の妥当性について議論している。

それに対して、第 4 節では、欧州委員会の勧告に応じる形で、イギリスの ONS が、2021 年の人口センサスで展開している、ターゲット・スワッピングと cell key method を用いて、オンデマンドな形で人口センサスの多次元統計表の提供を可能にする「オンデマンド公表システム」の概要を述べた。また、2021 年センサスを対象に、利用者のニーズと攻撃者のシナリオを考慮する形で、個票データ、匿名化ミクロデータおよび一般公開型ミクロデータの複数のミクロデータファイルの作成・提供を計画していることを明らかにした。統計作成部局が、利用目的を問わないオープンな統計表だけでなく、学術研究利用で提供される個票データやライセンス型ミクロデータ、さらには教育利用を指向した一般公開型ファイルを含む多

様な提供形態を備えているのは、ヨーロッパにおける公的統計データの提供の特徴と言える。

アメリカとイギリスの人口センサスの作成・公表の動きには、いくつかの共通点があると考えられる。第 1 の点は、前回の 10 年前の人口センサスとは、作成・公表の方向性を大きく転換させたことである。第 2 節で議論したように、アメリカでは、2010 年センサスの公表統計表およびミクロデータの提供まで実施してきた伝統的な匿名化措置の方針を変更し、差分プライバシーの方法論の導入を進めた。それは、センサス局内部の中核機関である Data Stewardship Executive Policy Committee(DSEP)[24]を中心に、人口センサスのデータにおけるプライバシー保護について問題意識を共有し、センサス局内部におけるセンサスデータを用いた実証研究も含め、周到な準備を行ってきた結果だと考えられる。また、イギリスでも、ONS は、2011 年センサスまでとは異なり、2021 年センサスにおいて集計計画に基づいて集計項目が定められた統計表を公表するだけでなく、利用者が選択した変数が集計項目として設定された統計表を作成・提供する、オンデマンド公表システムも新たに進めてきた。その背景として、ONS では、2021 年センサスデータの作成・公表において、取得容易性(Accessibility)、柔軟性(Flexibility)および即時性(Timeliness)という 3 つの考え方を重視する方向に転換したことを指摘することができる(Spicer(2020))。その意味では、ONS のオンデマンド公表システムは、その 3 つの考え方が具現化されたシステムだと言える。

第 2 の点は、統計表や元になるミクロデータに対して、攪乱的な秘匿処理を行うだけでなく、プライバシー保護に関わるパラメータについて公開可能な情報を公表する方向に変化してきたことである。これまでの人口センサスに関する統計表の公表や匿名化されたミクロデータの作成・提供において、スワッピング率のような個体情報の特定につながる可能性のある情報は公表されなかった。しかしながら、アメリカでは、2020 年センサスにおける差分プライバシーの導入にあたって、テストデータである「プライバシー保護済ミクロデータファイル(Privacy-Protected Microdata Files =PPMFs)」を公開するだけでなく、パラメータ ε に関する情報も公表することによって、差分プライバシーの方法論の適用について利用者からのフィードバックを得ることを可能にした。また、イギリスにおいても、2021 年センサスにおいて透明性を高める方向に転換し、これまで公開しなかった秘匿処理に関する情報を可能な範囲で公表する方向に進んでいる[25]。具体的には、「オンデマンド集計システム」で用いられる自動化された露見チェックのパラメータは公表される予定になっている。しかしながら、p-table における record key やターゲット・スワッピングにおけるスワッピング率は公表されないことになっている。

---

[24] DSEP は、2001 年にセンサス局内部に設立され、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。DSEP の任務は、センサス局がアメリカ国民及びアメリカ経済に関するデータを効率的かつ合理的に収集・利用することを保証することであって、そのために、データの収集過程全体にわたって回答者のプライバシーとデータの秘匿情報を保護することが求められる。したがって、センサス局がセンサス法(the Title 13 of the U.S. Code)、プライバシー保護法(the Privacy Act)や他の適用可能な法令によって課される法的・倫理的な報告義務を遂行することへの責任を負うことが、DSEP によって保証される。

なお、DSEP を支援する(センサス局内部の)機関としては、以下のような委員会が存在する。

・開示評価委員会(Disclosure Review Board)
・プライバシー政策・研究委員会(Privacy Policy and Research Committee)
・データ統合政策委員会(Data Integration Policy Committee)
・データ管理委員会(Data Management Committee)
・医療保険の携行性と責任に関する法律(HIPPA)に関するプライバシー保護委員会(Health Insurance Portability and Accountability Act Privacy Board)

[25] 以下の資料を参照。
Transparency of SDC methods and parameter
https://uksa.statisticsauthority.gov.uk/wp-content/uploads/2022/02/EAP168-Statistical-Disclosure-Control-for-Census.pdf

一方、アメリカとイギリスで大きく異なっているのは、差分プライバシーの導入の是非に関してである。それは、アメリカとイギリスで対象となっている統計表の作成目的の違いにも起因する。センサス局は、人種と地域に関する詳細な統計表(PL94-171)を作成・公表するために、モザイク効果や再構築攻撃などを通じた個人識別の脅威に対して現実的な対策を必要とした。その一方で、アメリカのオープンデータ政策の方針により、モザイク効果などのプライバシー問題には配慮しつつ、データは可能な限りオープンにすることが求められた。Calo et al. (2021) や Electronic Privacy Information Center (2021) が示す通り、再構築攻撃に対して有効な対策は差分プライバシー以外に知られていないことから、2020 年センサスにおける差分プライバシーの導入はセンサス局にとって必然だったと言える。差分プライバシーの導入にあたっては、センサス局は既存の差分プライバシーの実現方式を単に適用するのではなく、アメリカの人口センサスに適した差分プライバシーの実現手法である TDA を独自で新たに技術開発するとともに、ステークホルダープロセスを通じた外部とのコミュニケーションのために、テスト用データの作成と利用者からの意見のフィードバックを繰り返した。さらに、ステークホルダープロセスの過程において、単にプライバシー損失予算の増減を調整するに留まらず、zCDP の導入などを含む大幅なアルゴリズムの改善とシステムの改修を実施している。2020 年センサスの予算総額は約 142 億ドル[26] (約 2 兆円[27]) にのぼり、これらの差分プライバシーの導入に向けた技術開発と社会対話を実現するにあたっての費用的な裏付けになったと考えられる。

それに対して、イギリスでは、差分プライバシーの適用可能性の検討が ONS 内部で行われてきたものの、統計表の結果数値における有用性に対する懸念から、差分プライバシーの適用は、あくまで検討段階に留まっており、差分プライバシーは 2021 年センサスには導入されなかった。なお、オンデマンド集計で作成される統計表に差分プライバシーを適用しようとした場合、利用者のニーズにしたがってクエリが繰り返される場合を想定すると、プライバシー予算が大きく消費されるため、公表される統計表に対するプライバシーの保護が担保できない可能性がある。このことが、2021 年センサスにおいて差分プライバシーの採用を見送った一因であることが考えられる。その一方で、ONS がオンデマンド公表システムにおいて、統計表における結果数値の有用性を重視する観点から cell key method を採用したと捉えることもできる。ただし、cell key method については、差分プライバシーに相当するような理論的な観点からの安全性は保証されていないように思われる。ゆえに、オンデマンド公表システムで統計表を提供する前に、自動化された露見チェックが秘匿性を担保する上で重要な機能を果たしていると言える。

6. まとめ

本稿は、アメリカとイギリスの事例をもとに、公的統計のプライバシーに関する最近の動向を洞察した上で、公的統計に対するプライバシー保護の方向性に関する比較・検討を行った。センサス局と ONS はいずれも、公的統計、とくに人口センサスの統計表の作成・公表におけるプライバシー保護について大きな展開を見せているが、その展開の方向性に関しては顕著な違いが確認された。

アメリカにおけるセンサスへの差分プライバシーの全面的な導入は、公的統計におけるプ

---

[26] 2021 年 6 月のアメリカ会計検査院報告 (Government Accountability Office (2021)) による。COVID-19 対策のための追加費用約 11 億ドルを含む。世帯あたりの費用は約 96 ドル。

[27] 1 ドル ＝140 円で換算。

ライバシー保護の考え方に関する、大きな転換点と捉えられるだろう。TDA の新規開発・導入や zCDP の導入など、センサス局が持つ高い技術開発力が惜しみなく投入され、野心的かつ積極的な技術の導入がなされることによって、人口センサスへの差分プライバシーの全面的な導入が実現した。ただし、その導入は平坦な過程ではなかった。例えば、一部のデータ利用者によるノイズへの忌避感、さらには当時のアメリカの政治状況、とりわけトランプ政権の大統領選挙敗北直後の状況におけるセンサス局への訴訟も、アメリカにおける差分プライバシーの適用を容易ならざるものとし、その結果として、プライバシー損失予算 (ε) の大幅な増大がもたらされた。

こうした状況であったが、アメリカにおける人口センサスの統計表に対する差分プライバシーの導入は、アメリカの公的統計の作成のためになされる秘匿処理に関するエポックメイキングな事象ということができる。その意味では、2025 年の American Community Survey (ACS) における秘匿処理も注目すべきと言えよう。

イギリスでは、人口センサスの統計表の公表のために、ヨーロッパで先行して、攪乱的な秘匿処理の技法である cell key method が適用されたオンデマンド集計システムが実用化されつつあることが注目すべき点だと言える。しかしながら、cell key method によって攪乱が施された統計表の中のセルに含まれる結果数値の安全性が、どのような形で保証されているかについては、さらなる確認・検討が求められる。ヨーロッパにおいては、Eurostat だけでなくイギリスも差分プライバシーの方法論の実用性に対する調査研究を進めていることから、将来的には、ヨーロッパにおける公表統計表の作成や公的統計ミクロデータの作成・提供において差分プライバシーの方法論が適用される可能性もある。例えば、ノルウェー統計局のように公的統計の二次利用に対する差分プライバシーへの関心が高い統計作成部局もあることから[28]、イギリスを含むヨーロッパにおける差分プライバシーの動向についても、今後さらに注視していきたい。

謝辞

本稿は、2022 年度統計関連学会連合大会における学会報告(2022 年 9 月 8 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中川裕志先生(理化学研究所)と星野伸明先生(金沢大学)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き、本稿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] 伊藤伸介(2011)「わが国におけるミクロデータの新たな展開可能性について―イギリスにおける地域分析用ミクロデータを例に―」，明海大学『経済学論集』Vol.23, No.3, pp.36-54.

[2] 伊藤伸介(2016)「政府統計における個票データの提供と秘密保護について―イギリスを例に―」，『経済学論纂(中央大学)』第 56 巻第 5・6 合併号，pp.1-19.

[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.

[28] 例えば、Heldal et al.(2019)を参照。

[5] 伊藤伸介(2020) 「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・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.
[7] 伊藤伸介・寺田雅之・赤塚裕人・北井宏昌(2022)「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―」『統計研究彙報』第 79 号，pp.131-150.
[8] 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.
[9] 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.
[10] 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.
[11] 森博美(2000)「イギリスにおけるミクロデータの提供」松田芳郎・濱砂敬郎・森博美編『講座ミクロ統計分析①統計調査制度とミクロ統計の開示』日本評論社, pp.48-83.
[12] Abowd, J. M. (2021) “Supplemental Declaration of John M. Abowd.”, *Alabama v. U.S. Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).
[13] Bach, F. (2022) “Differential Privacy and Noisy Confidentiality Concepts for European Population Statistics”, *Journal of Survey Statistics and Methodology* (**10**), pp.642-687.
[14] Blanchard S., “The Methodological Challenges of Protecting Outputs from a Flexible Dissemination System”, Survey Methodology Bulletin 79, pp. 1-15.
[15] Bun, M. and Steinke, T. (2016) “Concentrated Differential Privacy: Simplifications, Extensions, and Lower Bounds”*, Theory of Cryptography 2016*, LNC 9985, Springer, pp. 635-658.
[16] Burwell, S. M., VanRoekel, S., Park, T., and Mancini, D. J. (2013) *Open Data Policy – Managing Information as an Asset*, Memorandum M-13-13. Office of Management and Budget, Executive Office of the President, U.S.
[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”, *Alabama v. U.S. Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).
[18] Cohen, A., Duchin, M., Matthews, J.N., and Suwal, B. (2022) “Private Numbers in Public Policy: Census, Differential Privacy, and Redistricting.” *Harvard Data Science Review*, Special Issue 2, MIT Press.
[19] de Wolf, P. P. (2021) “The Cell Key Method in τ-ARGUS”, Paper Presented at NTTS-2021, pp.1-5.
[20] Dinur, I., and Nissim, K. (2003) “Revealing information while preserving privacy”, *Proc. 22nd ACM SIGMOD-SIGACT-SIGART symp. Principles of database systems*, ACM, pp. 202–210.
[21] Dove, I. (2021) “Applying differential privacy protection to ONS mortality data, pilot study”.
[22] Duncan, G. T., Elliot, M., Salazar-González, J-J.(2011) *Statistical Confidentiality*, Springer.
[23] Dwork, C. (2006) “Differential privacy”, *Proc. 33rd intl. conf. Automata, Languages and Programming*, LNCS 4052, Springer, pp. 1-12.
[24] Dwork, C. (2007) “An Ad Omnia Approach to Defining and Achieving Private Data Analysis”, *Proc. 1st intl. conf. Privacy, security, and trust in KDD*, pp. 1-13.
[25] 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", *Alabama v. U.S. Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).

[26] Erven, T.v. and Harremos, P. (2014) "Rényi Divergence and Kullback-Leibler Divergence", *IEEE Trans. Information Theory* 60 (7), pp. 3797–3820.

[27] 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.

[28] Garfinkel, S. (2022) "Differential Privacy and the 2020 US Census", MIT Case Studies in Social and Ethical Responsibilities of Computing, Winter 2022.

[29] Government Accountability Office, U.S. (2021) "2020 Census: Innovations Helped with Implementation, but Bureau Can Do More to Realize Future Benefits", Report to Congressional Addressee, GAO-21-478.

[30] Government Statistical Service (2014a) "GSS/GSR Disclosure Control Guidance for Microdata Produced from Social Surveys"

[31] Government Statistical Service (2014b) "GSS/GSR Disclosure Control Guidance for Microdata Produced from Social Surveys – Case Studies"

[32] Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E. S., Spice, K., de Wolf, P.-P. (2012) *Statistical Disclosure Control*, John Wiley & Sons.

[33] Heldal, J., Johansen, S., Risnes, Ø. (2019) "Instant Access to Microdata – microdata.no", Paper presented at New Techniques and Technologies for Statistics 2019, Brussels.

[34] JASON (2020) *Formal Privacy Methods for the 2020 Census*, JASON Report, JSR-19-2F, The MITRE Corporation.

[35] JASON (2022) *Consistency of Data Products and Formal Privacy Methods for the 2020 Census*, JASON Report, JSR-21-02, The MITRE Corporation.

[36] Newsom, K. C. (2021) "Memorandum Opinion", *Alabama v. U.S. Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).

[37] Newsom, K. C., Marks, E. C., Huffaker, Jr., R. A. (2021) "Memorandum Opinion and Order", *Alabama v. U.S.Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).

[38] Office for National Statistics (2017) "Development of flexible dissemination for 2021 Census".

[39] Percival, K. and Dennie, M. (2021) "The State of Census Lawsuits on the Eve of Key Data Releases", Analysis & Opinion, Brennan Center for Justice.

[40] Ruggles, S. (2021) "Expert Report of Steven Ruggles", *Alabama v. U.S. Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).

[41] Spicer, K. (2020) "Statistical Disclosure Control (SDC) for 2021 UK Census"

[42] Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke (1996) "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20(2): 167-196.

[43] The State of Alabama, Aderholt, R., Green, W., and Williams, C. (2021) "Complaint for Declaratory and Injunctive Relief", *Alabama v. U.S.Dep't of Commerce*, 546 F. Supp. 3d 1057 (M.D. Ala. 2021).

[44] Thompson, M. "Flexible Dissemination Software for the 2021 England & Wales Census", presented at the International Association for Official Statistics Conference 2022, Statistics Poland.

[45] U.S. Census Bureau (2021a) "Comparing Differential Privacy with Older Disclosure Avoidance Methods", Census Fact Sheets, D-FS-GP-EN-050.

[46] U.S. Census Bureau (2021b) *Disclosure Avoidance for the 2020 Census: An Introduction*, U.S. Government Publishing Office.