国勢調査を対象にした差分プライバシーの実用性に関する検討
―Zero-Concentrated Differential Privacy (zCDP)に着目して―

伊藤　伸介 †
寺田　雅之 ††
加藤　駿典 ‡
松井　秀俊 ‡‡

A Study on the Practicality of Differential Privacy for Japanese Census Data: Focusing on Zero-Concentrated Differential Privacy (zCDP)

ITO Shinsuke
TERADA Masayuki
KATO Shunsuke
MATSUI Hidetoshi

アメリカセンサス局は、公的統計の作成・公開に差分プライバシーを適用するうえで、データの安全性を保ちつつ有用性を向上させるために、2020 年人口センサスの統計表と一般公開型ミクロデータの両方において zCDP (=Zero-Concentrated Differential Privacy)を導入した。わが国の公的統計においても、 zCDP が有効かどうかを実証的に明らかにすることは、統計実務においても有益であると考える。そこで、本稿では、アメリカにおけるプライバシー保護の取り組みを踏まえつつ、わが国の公的統計における zCDP の実用性を追究した。具体的には、令和 2 年国勢調査の個票データに、zCDP に基づく差分プライバシーの方法論を適用し、その有効性を検証した。本実験の結果、zCDP を適用する場合、パラメータの値の変化によって付与されるノイズの大きさが変動することから、Laplace ノイズと比較して、センサス局が適用した Gaussian ノイズが必ずしも有効とは言えないことが明らかになった。

キーワード: 差分プライバシー、アメリカ人口センサス、国勢調査、zCDP、Laplace ノイズ、Gaussian ノイズ

The U.S. Census Bureau has introduced zCDP (Zero-Concentrated Differential Privacy) in statistical tables from the 2020 Population Census as well as its public use microdata and with the objective of enhancing data usability while maintaining data security of official statistics. Demonstrating an effectiveness of zCDP also for Japan's official statistics would be beneficial for statistical practice. This paper explores the practicality of zCDP in Japan's official statistics, drawing on privacy protection efforts in the United States. Specifically, we applied a zCDP-based differential privacy methodology to individual data from the 2020 Population Census and verified its effectiveness. The results of our experiment show that when applying zCDP, the amount of noise added varies according to changes in parameter values. As a result, the Gaussian noise applied by the Census Bureau cannot necessarily be considered effective when compared to Laplace noise.

Keywords: differential privacy, U.S. Census, Japanese Population Census, zCDP, Laplace noise, Gaussian noise

† 中央大学経済学部　Email: ssitoh@tamacc.chuo-u.ac.jp
†† (株)NTT ドコモ/京都橘大学　Email: teradam@nttdocomo.com
‡ (独)統計センター/総務省統計研究研修所　Email: skato@nstac.go.jp
‡‡ 滋賀大学データサイエンス学部　E-mail: hmatsui@biwako.shiga-u.ac.jp

1. はじめに

近年、公的統計に対する差分プライバシー(differential privacy)の方法論の適用をめぐって、様々な議論が展開されている。例えば、アメリカでは、2001 年にアメリカセンサス局内部に設置された中核機関である DSEP(=Data Stewardship Executive Policy Committee)において、人口センサスを対象にしたプライバシー保護のための方法論として、差分プライバシーの方法論の適用可能性が検討されてきた。そして、2020 年人口センサスにおいて差分プライバシーの実現方式が適用されたノイズ付与済の統計データが、公表されている(伊藤他(2022), 伊藤・寺田(2023))。

アメリカセンサス局による人口センサスへの差分プライバシーの適用に関しては、ミネソタ人口研究センターの Steven Ruggles 教授らが、利用者の立場から差分プライベートなセンサスデータの有用性についての批判を行っている(Ruggles et al.(2019))。さらに、差分プライベートなセンサスデータの識別リスクに関しても、Muralidhar and Ruggles(2024)がそれに対する脆弱性を指摘している。それに対して、Hawes et al.(2025)は、人口センサスの作成者側から、公的統計の秘匿性(confidentiality)を担保するだけでなく，精度(accuracy)と利用可能性(availability)も勘案し、「公的統計の三重のトレードオフ（triple tradeoff of official statistics）」（Abowd and Hawes(2023)）の間でバランスを取ることの重要性を述べている(伊藤(2025))。

管見の限り、アメリカセンサス局の事例を除けば、公的統計の統計表の作成・公表において差分プライバシーの方法論が統計作成部局によって採用された例はないものと考える。一方で、海外の統計作成部局による差分プライバシーの適用可能性の検討状況を見ると、例えば、イギリス国家統計局(ONS)は、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が、結果数値の有用性を重視する観点から、人口センサスにおける差分プライバシーの適用は検討段階に留まっていることが知られている(伊藤・寺田(2023))。しかしながら、ONS において、近年差分プライバシーの方法論を適用した合成データの作成に関する研究が展開されているのは興味深いと言える(Daniel(2025))。

わが国ではこれまで、公的統計の個票データを用いて、攪乱的手法(perturbative methods)(加法ノイズ(additive noise)、データスワッピング(data swapping)、PRAM(=Post Randomization Methods)、ミクロアグリゲーション(microaggregation)等)の有効性に関する実証研究が行われてきた(伊藤他(2014), 伊藤・星野(2014), Ito et al.(2018), 伊藤(2019)等)。その一方で、わが国の統計データに対する高度な攪乱的手法として、国勢調査のメッシュ統計や個票データに基づいて作成された統計データへの差分プライバシーの適用可能性が検討され、差分プライバシーの実現方式の可能性が追究されてきた(伊藤・寺田(2020), 伊藤他(2024), 伊藤他(2025))。

本稿は、アメリカセンサス局が 2020 年人口センサスの統計データの公表にあたって採用した差分プライバシーの方法論が、わが国の公的統計に対しても適用可能かどうかを検証することを目的とする。そのために、令和 2 年国勢調査の調査票情報(個票データ)に基づき作成した統計表に対して複数の差分プライバシーの実現方式を適用した上で、その有効性について定量的に比較・検討するだけでなく、公的統計に対する差分プライバシーの方法論の実用性について考察を行う。

2. アメリカにおける人口センサスに対する差分プライバシーの適用状況

本節では、アメリカ人口センサス(以下「センサス」と略称)を対象にした、アメリカセンサス局(以下「センサス局」)による差分プライバシーの適用状況について述べることにしたい。

2.1　差分プライバシーの定義と解釈

差分プライバシーは、未知の攻撃を含む任意の攻撃に対する包括的（ad omnia）なプライバシー保護を実現することを目的としたプライバシー保護フレームワークであり、様々なプライバシー保護手法に対して、一貫したプライバシー損失予算（$\varepsilon \geq 0$）を定量的に提供する (Dwork et al. (2006a))[1]。この指標の値が低くなるほど、プライバシー保護のレベルは高くなる。

あるランダム化関数として表されるプライバシー保護手法 $M: D \to R$ が下記の定義 1 を満たすとき、M は ε-差分プライバシーを満たすと言われる。

定義 1: 隣接するデータベース D_1 と D_2 $(D_1, D_2 \in D)$ に対して、ランダム化関数 M は、以下の不等式を満たす場合、ε-差分プライバシーを満たす。ここで S は M の出力空間 R の任意の部分空間 $(S \subseteq R)$ である:

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

この定義の直観的な解釈は、個人 A に関するデータを含むデータベースD_1 に対してM を適用した結果が、個人 A に関するデータを含まないデータベースD_2 に対してM を適用した結果と区別不能である場合、M の出力は個人 A のプライバシーを侵害しないということである。また、ε の値が低いほど、前者の結果は後者と区別困難であり、これはプライバシー保護手法 M がより高い安全性を提供することを意味する。言い換えれば、ε は、M の出力によって失われるプライバシーの度合いを示す指標である。このため、ε はプライバシー損失またはプライバシー損失予算とも呼ばれる。

定義 1 が示すように、差分プライバシーは特定のプライバシー保護手法を指すのではなく、プライバシー保護手法が提供するデータセキュリティのレベルを定義する枠組みである。差分プライバシーに基づく個々のプライバシー保護手法（定義 1 における M）はメカニズムと呼ばれ、その代表的なものとして、出力結果に対して (ε などによって定まる) 所定のスケールの Laplace 分布に従うノイズを加える手法である、Laplace メカニズムが挙げられる (Dwork et al. (2006a))。また、PRAM などの従来の攪乱的手法の一部も、差分プライバシーを満たすメカニズムであることが知られている (Dwork and Roth (2014))。たとえば、d 次の属性を持ち n レコードからなる個票データに対し、属性 A_j $(j \in 1..d)$ に対応する維持確率を ρ_j として PRAM を適用するとき、これは下式で与えられる ε をプライバシー損失とした ε-差分プライバシーを満たす (寺田他 (2017a))。ここで $|A_j|$ は属性 A_j の濃度 (cardinality) を表す[2]。

$$\varepsilon = \sum_{j=1}^{d} \ln \frac{1 + (|A_j| - 1)\rho_j}{1 - \rho_j}.$$

2.2 近似差分プライバシー

---

[1] 決定論的手法では、$\varepsilon \to \infty$ となる（何の安全性も保証されない）。

[2] たとえば $A_j = \{$男性，女性，その他$\}$ であるとき、$|A_j| = 3$ となる。

近似差分プライバシー (approximate differential privacy) (Dwork et al. (2006b)) は、差分プライバシーの定義を緩和し、Mが差分プライバシーを満たすことに、ある確率で「失敗する」ことを許容する安全性指標であり、正規分布に従うノイズを加える手法である Gaussian メカニズム (Dwork et al. (2006a)) が差分プライバシー[3]の枠組みでは扱えない (ε の値が無限大となる) ことなどを背景として提案された。

その定義は差分プライバシーと近しいものであり、前節の差分プライバシーの定義 (定義 1) における条件式を下式に変更したものとして定義される。

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

メカニズム M がこれを満たすとき、(ε ,δ)-近似差分プライバシーを満たすと言われる[4]。なお、定義 1 における条件式を比較すると明らかなように、$\delta = 0$ のとき差分プライバシーの定義と完全に等しい。つまり、(ε ,0)-近似差分プライバシーは ε-差分プライバシーと等価であると言える。

近似差分プライバシーにおける δ の値は、「破滅的な失敗 (catastrophic failure)」が許容される確率と理解することができる。ここで、破滅的な失敗とは、プライバシーの確定的な暴露を表す。つまり、近似差分プライバシーにおいて、データベースに含まれる人のプライバシーは、確率 $(1-\delta)$ で ε-差分プライバシーにより守られるが、確率 δ で確定的に暴露されうることを示す (実際に暴露されうるかどうかは用いるメカニズムにより異なるが、少なくとも近似差分プライバシーの定義としてはそれを許容する)。そのため、近似差分プライバシーの適用にあたっては、(差分プライバシーと同様に) εの値を適切に定めるだけではなく、さらに δ の値を「十分に小さい[5]」値となるよう設定することが必要とされる。

2.3 アメリカにおけるセンサスデータへの差分プライバシーの適用

センサス局が公的統計に対して差分プライバシーの方法論を適用する契機となったのは、データベース再構築攻撃(database reconstruction attack)への懸念であった(Abowd (2018), Dinur and Nissim (2003))。この種の再構築攻撃では、(一見安全な)データベースから生成されたデータを重ね合わせ、制約充足問題を設定し、この問題を解いて元のデータベースを復元することで、データに含まれる個人のプライバシーを暴露する。センサス局は、2010 年のセンサスデータを対象に、データベース再構築攻撃に対処するための差分プライバシーの検討を実施し、これを基に、2020 年センサスの公表統計表に対して差分プライバシーを適用した。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 ε を設定し、TopDown アルゴリズム(TopDown algorithm=TDA)に基づく地域レベルでのプライバシー損失予算(privacy

[3] 近似差分プライバシーと対比するとき、定義 1 の差分プライバシーは「純粋な (pure)」差分プライバシーとも呼ばれる。

[4] 「近似」を省略し、単に「(ε,δ)-差分プライバシー」と呼ばれることもある。たとえば 2020 年アメリカセンサスにおける差分プライバシーの適用において、zCDP の導入以前の試験的なデータ提供では (純粋な) 差分プライバシーを満たすものであったが、(正式提供を含む) zCDP の導入以降は、実際には近似差分プライバシーに基づいて ε の値が表されている。

[5] 具体的にどの程度であれば「十分に小さい」と言えるかについては確たる定めはなく、多分に恣意性を有する (客体数を N としたとき、$\delta < 1/N$ と設定されることが多いが、絶対的なものではない)。このことから生じる問題については第 5 節で議論する。

loss budget)の割り当てに関する検証を実施した(Garfinkel et al. (2019), Garfinkel(2022))。その結果として、2021 年 6 月に公開された最終版のプライバシー保護済ミクロデータファイル(Privacy-Protected Microdata Files=PPMFs)の作成においては、DSEP によって、「露見回避システム(Disclosure Avoidance System)」における全体のプライバシー損失予算のパラメータは、$\varepsilon = 19.61$と設定された(伊藤他(2022))。

センサス局は、2020 年センサスを対象に、差分プライバシーの実現方式が適された各種のセンサスデータを公開している。2021 年 8 月に、統計表区画改定データ(PL94-171) が最初に公表された。2023 年 5 月～2024 年 9 月においては、年齢、性別、人種等の詳細な人口社会的な特性値と、住宅の所有関係　(housing occupancy)、居住歴(housing tenure) を含む住宅に関する特性値に関する集計データとして、複数の人口・住宅ファイル (Demographic and Housing Characteristics File) が公表されている(伊藤(2025))。さらに、2024 年に、一般公開型ミクロデータとして、差分プライベートである PPMFs が公開されるが、これは、合成データとしても位置付けられうる(伊藤他(2024))。

これらのセンサスに関する公表された統計表あるいは一般公開型ミクロデータについては、差分プライバシーの方法論が適用されているだけでなく、zero-concentrated differential privacy (zCDP, Bun and Steinke (2016)) によってプライバシー損失予算 (privacy loss budget) が割り当てられたことが指摘できる。次節では、zCDP の特徴に関して概説する。

2.4 zCDP の特徴

zCDP とは、2016 年に提案された差分プライバシーよりも新しい概念であって、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た上で、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。

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$\mathcal{M}\colon \mathcal{D} \to \mathcal{R}$ が下式を満たすとき、$\mathcal{M}$は ρ-zCDP を満たす。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 (Erven and Harremos (2014))。

zCDP は、(純粋な) 差分プライバシーでは安全性が与えられない (ε が無限大となる) Gaussian メカニズムの安全性を扱うことを可能にする。また、合成則 (composition theorem) の適用によって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。

また、ρ-zCDP を満たすメカニズムは、任意の $\delta > 0$ について (ε, δ)-近似差分プライバ

シーを満たすことが知られている。具体的には、δ をある値に定めたとき、下式を用いてρからεの値を求めることができる (Bun and Steinke (2016), 石岡・寺田(2024))。

$$\varepsilon = \rho + 2\sqrt{\rho log\left(\frac{1}{\delta}\right)}$$

ここで、上記の変換式において $\delta > 0$ であることが求められることに注意したい。つまり、zCDP を適用した場合、(純粋な) 差分プライバシーによる安全性保証を得ることはできず、近似差分プライバシーによる緩和された安全性保証に基づくことになる。

3. 国勢調査データを対象にした差分プライバシーの適用に関する比較検証

本節では、わが国の国勢調査を対象にした差分プライバシーの方法論の適用に関する実証実験の手順とその特徴について述べる。

3.1 わが国の公的統計を対象にした差分プライバシーの適用に関する先行研究

本実証実験では、伊藤他(2024)における実験の方法に基づいている。伊藤他(2024)は、平成27 年国勢調査の個票データを用いて、地域区分の粒度の異なる統計表に様々な各種の差分プライバシーの実現方式を適用した上で、その有用性を比較することによって、わが国の公的統計に対する差分プライバシーの適用可能性を検討した。本研究では、様々な差分プライバシーを適用した統計データの有用性を比較するための評価指標として、平均絶対誤差(MAE)と二乗平均平方根誤差(RMSE)を用いている。

伊藤他(2024)では、差分プライバシーの実現方式として 2 種類のアプローチが採られている。第 1 のアプローチはボトムアップ構成法であり、最小の地域区分の集計表からより上位の地域区分における集計表へとノイズ付加と最適化を段階的に適用する手法である。ボトムアップ構成法では、(Laplace メカニズムと同様に) それぞれの集計表における最小集計区分のセル値に対して Laplace ノイズを付加した後に、多次元ベクトル空間における単体への射影問題 (projection onto simplex) を解くことによって、セル値の総数 (総数制約) を保持しつつ、Laplace ノイズの付与により生じる負のセル値が除去される (非負制約が充足される) (寺田他(2017a),寺田他(2017b))。第 2 はトップダウン構成法であって、最上位の地域区分である統計表からより詳細な地域区分に対してノイズ付加と最適化を階層的に適用する手法である。具体的には第 1 に、全国のクロス表を総数制約として、ノイズ付加後の都道府県単位のクロス表に対して単体への射影を適用することによって、総数制約と非負制約 (これら 2 つの制約を合わせて単体制約と呼ぶ) を充足したプライバシー保護済みの都道府県単位のクロス表を算出する。第 2 に、上記で得られた (プライバシー保護済の) 都道府県単位のクロス表を総数制約として、ノイズ付加後の市区町村単位のクロス表に対して単体への射影を適用して、単体制約を充足したプライバシー保護済みの市区町村単位のクロス表を算定する。これらの過程を最小の地域区分である基本単位区までトップダウンの方向で再帰的に繰り返すことによって、総数制約を保持しつつ非負制約を充足したプライバシー保護済のクロス表

が得られる[6]。

伊藤他(2024)は、国勢調査データを用いた差分プライバシーの実証研究を行い、Laplace ノイズに基づくトップダウン法が適用された集計表の結果数値のノイズ付与前の集計表における数値からの MAE が、ボトムアップ法におけるそれよりも小さいことを明らかにした。本研究では、わが国におけるこれまでの差分プライバシーに関する実証研究の成果を踏まえ、センサス局によって導入された zCDP に着目した上で、わが国の国勢調査を対象に、差分プライバシーの実現方式の適用における zCDP の有効性について定量的な評価を行う。

3.2 実験に使用したデータ

本研究で使用したデータは、令和 2 年国勢調査の調査票情報(個票データ)である。本実験では、性別、年齢、労働力状態といった 3 変数を対象にしたあらゆるクロス集計表を異なる地域区分ごとに作成した。次に、集計表にノイズを付与するために、各種の差分プライバシーの実現方式を適用する。さらに、zCDP の有効性を検証するため、ε とδ の値を変化させた場合のノイズが付与された国勢調査データの有用性を比較・検討する。

3.3 実験の概要

本実験においては、令和 2 年国勢調査の個票データを用いて、性別、年齢と労働力状態の 3 つの変数をもとに、地域区分の粒度が異なる集計表を作成した上で、伊藤他 (2024) において優れた結果を得たトップダウン法に基づき、zCDP の導入による効果を検証した[7]。

本研究は、トップダウン法の内部において、異なる地域区分の粒度ごとに作成したクロス表にノイズを付与するにあたり、Laplace メカニズムを適用して Laplace ノイズを付与した場合と、zCDP に基づき Gaussian メカニズムを適用して正規ノイズを付与した場合との間で、それが有用性に及ぼす影響を比較・検証することにより、zCDP の導入が有効かどうかを明らかにすることを指向している。本実証実験では、都道府県、市区町村、町・字および基本単位区のそれぞれについて、2.4 節に示した zCDP における近似差分プライバシーへの換算式を用いてプライバシー損失予算 (ε) の条件を揃えた上で[8]、これらの両手法に基づき、性別(2 区分)と年齢(18 区分)の 2 変数、および性別、年齢と労働力状態(3 区分)の 3 変数に関するクロス表を作成し、その有用性に関する評価を行った。なお、性別、年齢と労働力状態に関する分類区分の詳細については、付図を参照されたい。

ここで、プライバシー損失予算 ε は、伊藤他(2024)と同様に、0.1、0.2、0.7、1.0、1.1、5、10、20 の 8 種類を設定した。また、zCDP における ρ からの ε の導出にあたって用いる δ の値としては、10^{-1}、10^{-2}、10^{-4} と10^{-8}の 4 種類を設定した。[9]

なお、各地域区分において作成したクロス表に含まれる統計数値に関する有用性の指標と

---

[6] トップダウン構成法では、それぞれの地域区分ごとにプライバシー損失予算を配分する必要があるが、伊藤他(2024)ではこれを均等に配分している。

[7] トップダウン構成法におけるプライバシー損失予算の配分は、伊藤他 (2024) と同様に各地域区分ごとに均等配分する。

[8] 具体的には、Laplace メカニズムを適用した場合における ε の値は、純粋な差分プライバシー ($\delta = 0$) としての安全性を保証するため、差分プライバシーにおける合成則に基づいて計量 (accounting) した。一方、Gaussian メカニズムにおける ε の値は、zCDP に基づき ρ の値を計量した上で、2.4 節に示した zCDP から (ε, δ)-近似差分プライバシーへの換算式により (δ の値ごとに) 求めている。

[9] なお、本実験における隣接 (第 2 章参照) の定義としては、加除 (add/remove) の関係 (2 つのデータベースD_1, D_2 の間で、1 つのレコードが追加または削除されている関係) を用いた。

しては、平均絶対誤差 (MAE)と二乗平均平方根誤差(RMSE)の誤差指標が用いられている。

4. 実験の結果と考察

図 1 は、性別と労働力状態の 2 変数を対象として作成した地域区分ごとのクロス集計表において、Laplace メカニズムを適用した場合と、Gaussian メカニズムをそれぞれ $\varepsilon = 1$ の条件下で適用した場合における誤差 (MAE) について、地域区分の粒度 (基本単位区、町・字、市区町村、都道府県) ごとに示したグラフである。ここで、Gaussian メカニズムで用いられる正規ノイズの強度が同じであっても (すなわち ρ の値が同じであっても)、設定するδの値によって得られる ε の値が異なることから、前節で示した 4 種類の δ を用いた結果をそれぞれ示した。また、グラフ中の破線は、それぞれの条件における、トップダウン構成法の理論的な誤差上界[10]を示す。

この結果が示す通り、Laplace メカニズムを用いた場合と Gaussian メカニズムを用いた場合のいずれであっても、上位の地域区分における誤差の増大が抑えられるというトップダウン構成法の効果が得られている。また、下位の地域区分であるほど、トップダウン構成法における非負制約によるノイズ軽減効果が得られやすい点についても同様である。

両メカニズムの比較においては、設定する δ の値によってどちらが優位であるかが異なり、δの値が大きいほど Gaussian メカニズムが優位となる結果を得た。具体的には、δ が10^{-1}と10^{-2}のときは Gaussian メカニズムによる誤差は Laplace メカニズムより小さく、10^{-4}と10^{-8}のときはその逆となる結果を得た。

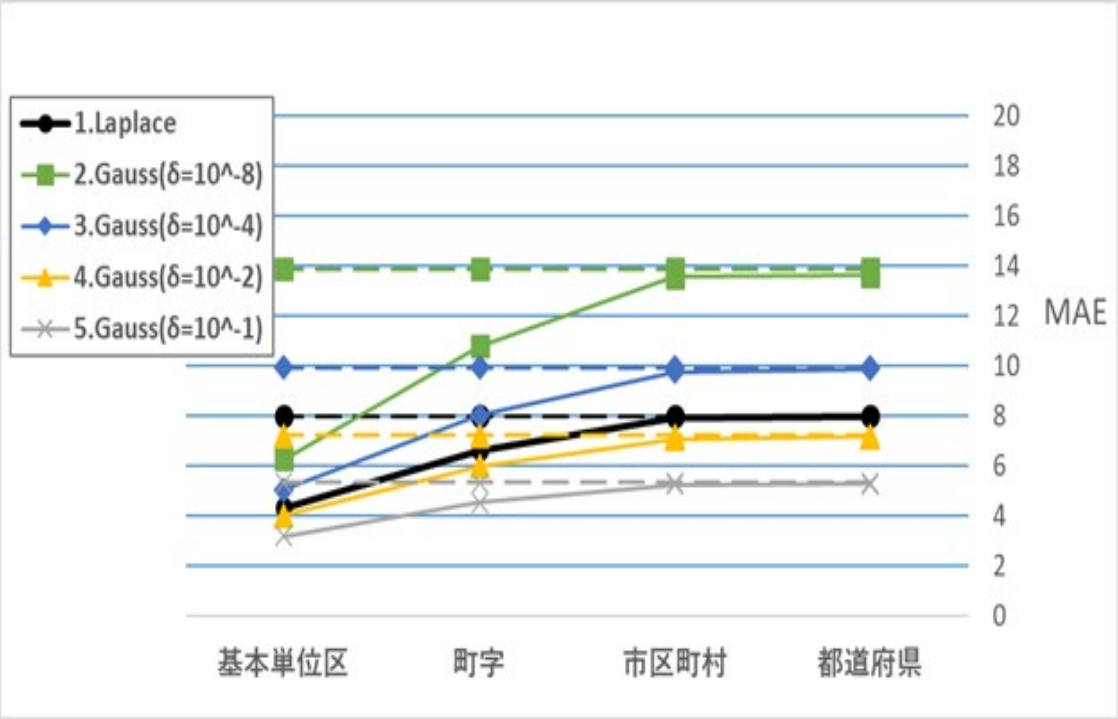
図 2 は、図 1 と同様の条件において、誤差指標として (MAE ではなく) RMSE を用いた場合の結果を示す。図 1 とほぼ同様であるが、定量的には若干ながら Gaussian メカニズムにより有利な結果を得ている。これは、それぞれのメカニズムにおいて用いられるノイズ分布の性質 (Laplace 分布は正規分布と比べて「裾が重い」分布である) と、RMSE が MAE と比べて大きな誤差の影響をより強く反映する評価指標であることによるものと考えられる。

図 3 と図 4 は、性別、年齢と労働力状態の 3 変数を対象として、同様に評価した結果を示し、図 3 は MAE を、図 4 は RMSE をそれぞれ誤差指標としている。全体的な傾向としては図 1 および図 2 と同様であるが、これらに比べて誤差の絶対値が小さくなっており、その傾向は下位の地域区分においてより顕著である。これは、2 変数のクロス集計表より 3 変数のクロス集計表のほうが各セルの値が相対的に小さくなり、そのスパース性も高まる (ゼロ値を持つセルの割合が増える) ことから、トップダウン構成法における非負制約によるノイズ軽減効果がより効果的に働くことによるものと考えられる。

図 5 から図 8 は、$\varepsilon = 0.1$ において図 1 から図 4 と同様な条件で評価した結果である。すなわち、図 5 と図 6 は性別と労働力状態の 2 変数のクロス集計表における MAE と RMSE を、図 7 と図 8 はそれらに年齢を加えた 3 変数のクロス集計表における MAE と RMSE をそれぞれ表す。その結果、ε の値を変動させても、誤差の絶対値が変化する以外には傾向に変わりはなく、これまでの図 1 から図 4 までを対象とした議論と符合する結果が得られた。なお、前節で示した通り、その他の ε の値を用いた実験も行ったが、同様の結果を示すのみであったため、本稿では具体的な図示は割愛する。

[10] トップダウン構成法での各階層において、単体制約の充足に伴う誤差の軽減がまったく行われないことを仮定した場合における誤差の理論値。

図 1 差分プライバシーの適用実験の結果,、性別×労働力状態、ε=1、MAE による比較



注 上図における破線は、それぞれの条件における理論的な誤差上界を表す(以下同様)。

図 2 差分プライバシーの適用実験の結果,、性別×労働力状態、ε=1、RMSE による比較

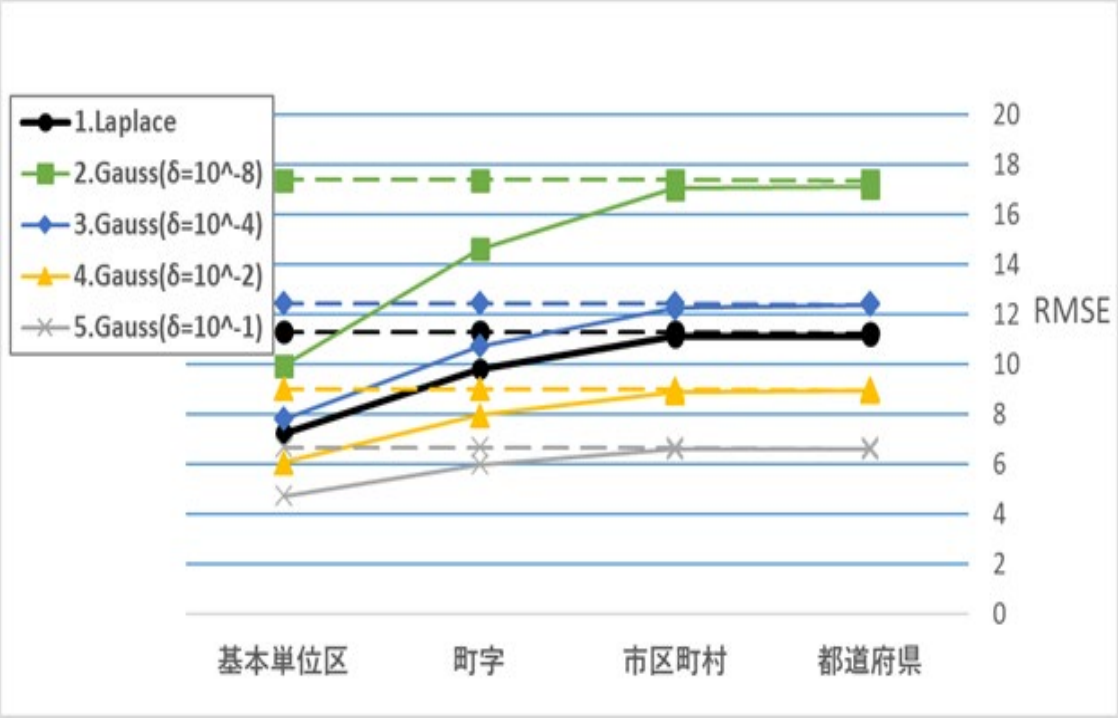


図 3 差分プライバシーの適用実験の結果,、性別×年齢×労働力状態、ε=1、MAE による比較

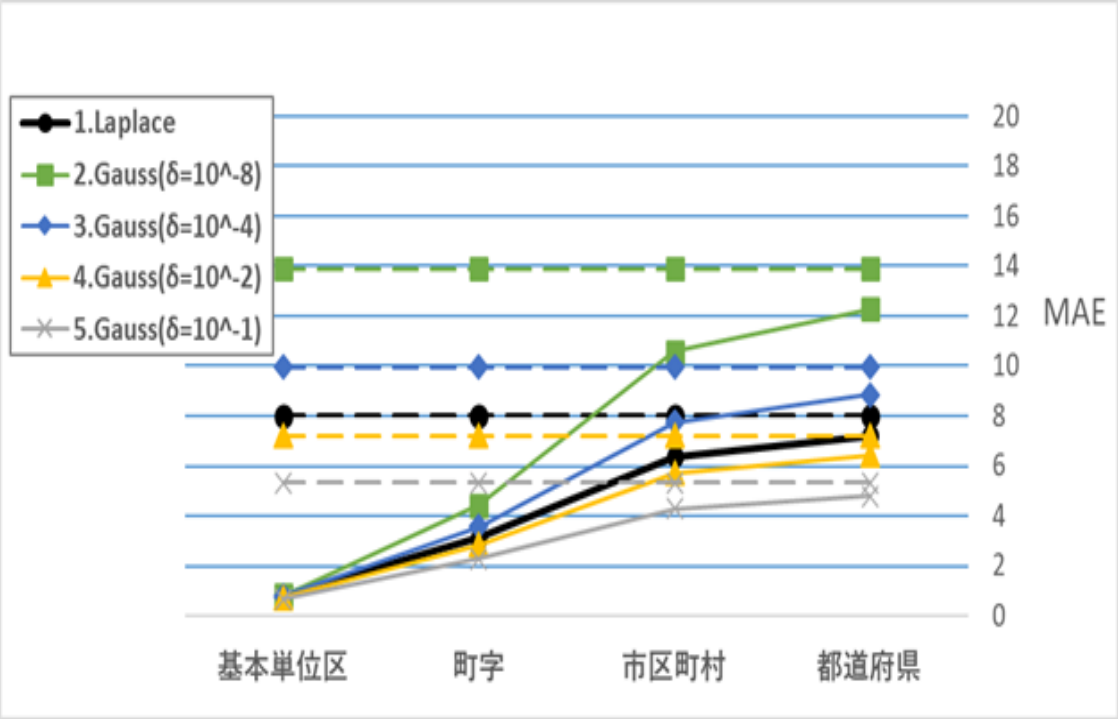


図 4 差分プライバシーの適用実験の結果,、性別×年齢×労働力状態、ε=1、RMSE による比較

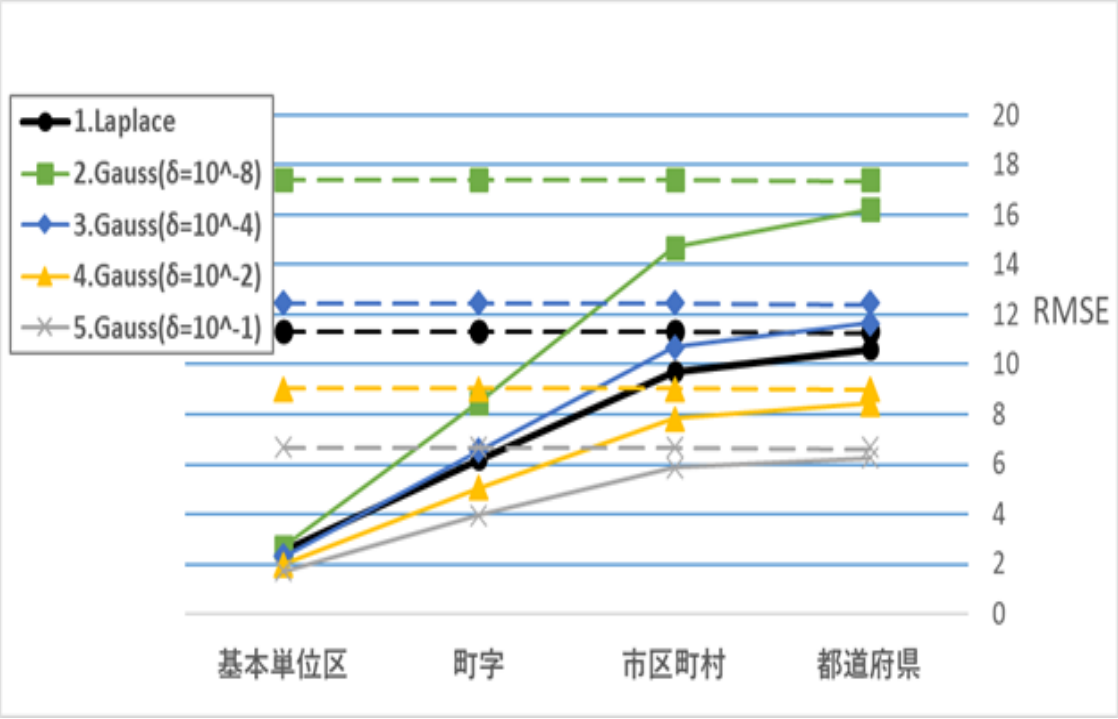


図 5 差分プライバシーの適用実験の結果,、性別×労働力状態、ε=0.1、MAE による比較

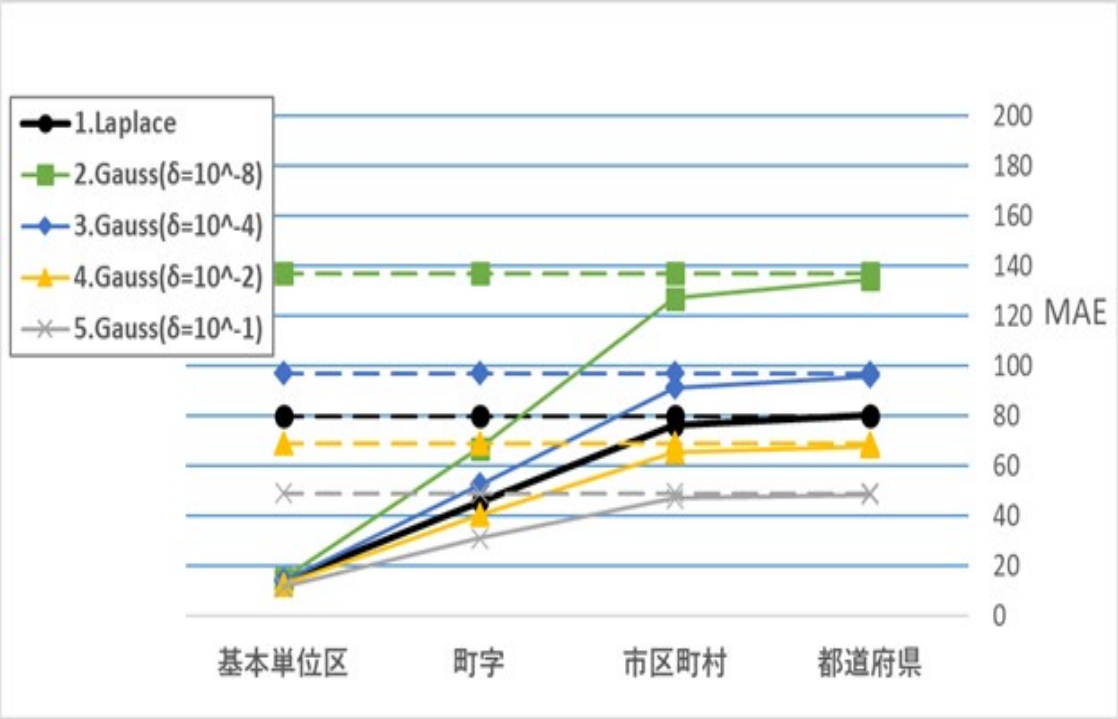


図 6 差分プライバシーの適用実験の結果,、性別×労働力状態、ε=0.1、RMSE による比較

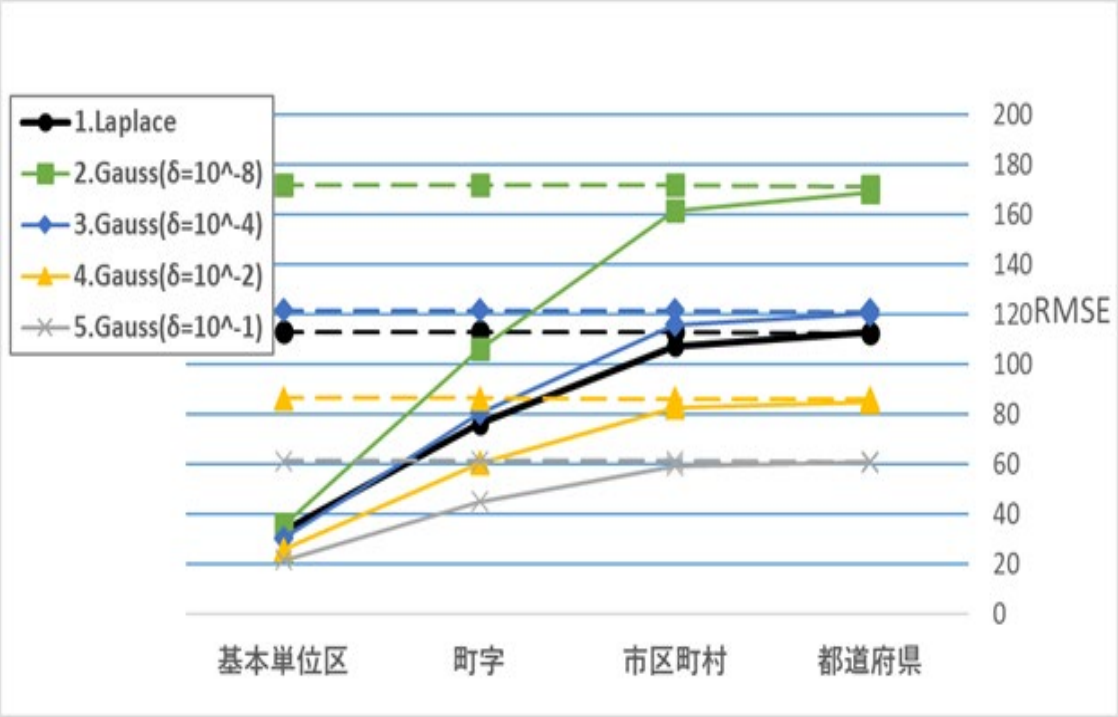


図 7 差分プライバシーの適用実験の結果,、性別×年齢×労働力状態、ε=0.1、MAE による比較

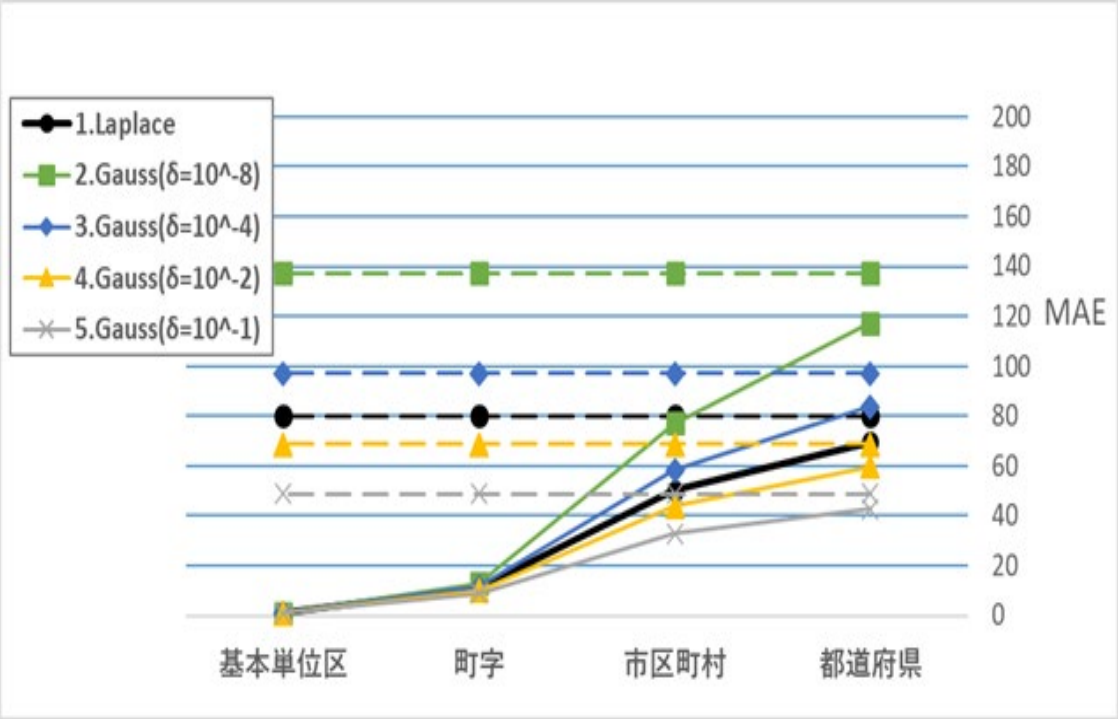
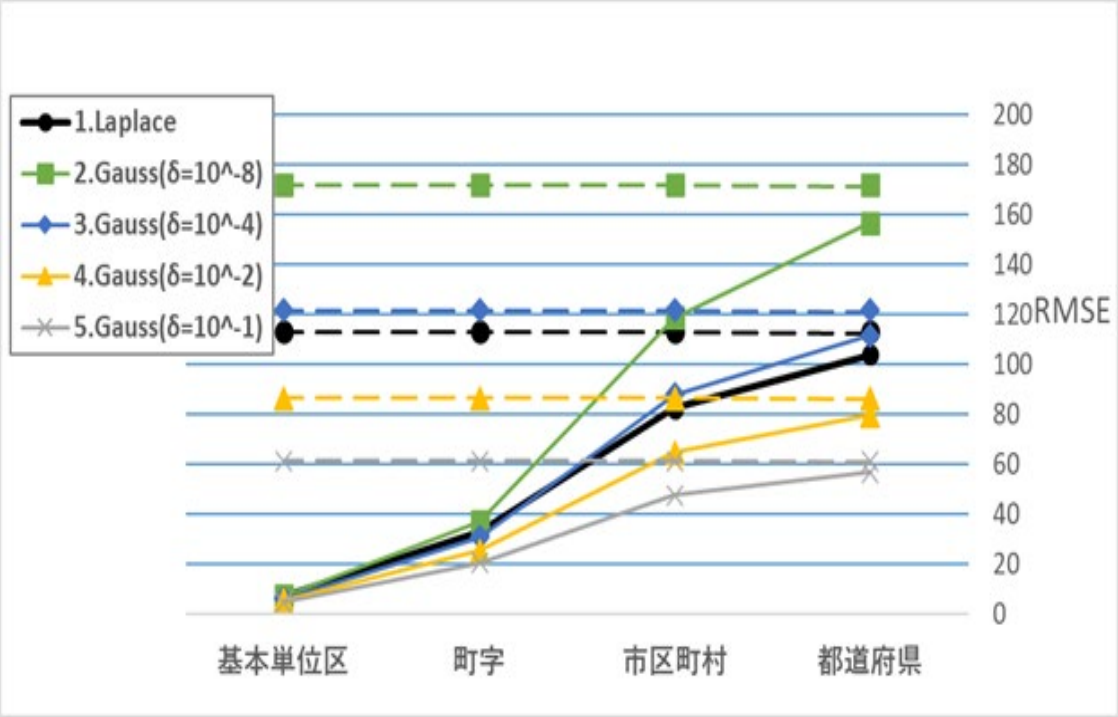


図 8 差分プライバシーの適用実験の結果,、性別×年齢×労働力状態、ε=0.1、RMSE による比較



5. zCDP の適用可能性に関する考察

第 4 節において得られた実験結果から、わが国の国勢調査への zCDP の適用可能性や、zCDP を適用する場合における留意事項について、2020 年センサスにおける適用結果や、メッシュ人口への zCDP の適用に関する先行研究 (石岡・寺田 (2024)、Ishioka and Terada (2025)) における実験結果などを参照しつつ議論する。

第 4 節の結果から、2020 年センサスで採用された、zCDP に基づく Gaussian メカニズムの導入は、少なくとも本実験の条件下においては、必ずしも Laplace メカニズムに対して優位とは言えず、設定する δ の値に依存して優位か否かが異なることが示された。さらに、本実験において Gaussian メカニズムのほうが優位な結果が得られた δ の値は、10^{-1} や 10^{-2} など、近似差分プライバシーにおいて一般的に用いられる値[11]を大きく上回るものであった。すなわち、Laplace メカニズムのほうが zCDP に基づく Gaussian メカニズムより誤差の観点で優位であったと言える。

なお、本実験における比較は、(純粋な) 差分プライバシー ($\delta = 0$) と近似差分プライバシー ($\delta > 0$) という、厳密には異なる安全性モデル間での比較となっている点（脚注 8 参照）に留意が必要である。もし Laplace メカニズムを用いた際のプライバシー損失 (ε) の計量において純粋な差分プライバシーに基づく安全性を放棄し、近似差分プライバシーにおける合成則 (advanced composition theorem) を適用して $\delta > 0$ を許容したならば、そのプライバシー損失はより小さく計算され、その結果、付与されるノイズも減少し有用性はさらに向上する。すなわち、本実験の (Laplace メカニズムにとって不利とも言える) 設定においてさえ、zCDP に基づく Gaussian メカニズムは Laplace メカニズムに対する優位性を示せなかったと言える。つまり、(1) 安全性について $\delta > 0$ を許容するという妥協をした上で、(2) その δ の値を非現実的なほど大きく設定しなければ、zCDP に基づく Gaussian メカニズムは有用性での優位を得られなかったことを示している。

この結論は、2020 年センサスにおける zCDP の導入効果とは異なるが、その理由として Laplace メカニズムの準最適性と、差分プライバシーと zCDP における合成則 (composition theorem) の適用効果の差異が挙げられる。Laplace メカニズムの準最適性により、(非負制約や整数制約などの) 制約条件を持たない単一の値に対して差分プライバシーを適用するときには、Laplace メカニズムがほぼ最適なメカニズムであるとされる[12]。その一方で、zCDP における合成則の適用によるプライバシー損失の増加は、差分プライバシーにおける増加より緩やかであることが知られている。すなわち、多数のメカニズムに対して合成則を適用する必要があるような複雑な状況であるほど、zCDP を導入したほうがプライバシー損失予算の消費が抑えられ、その結果として誤差の観点で有利となる。実際、本実験では基本単位区から都道府県までの 4 つの地域区分においてノイズを付与し、それらを合成しているため、合成則の適用対象数は 4 で抑えられていることに対し、2020 年センサスでは少数民族の人口分布における誤差の軽減などを目的として様々な区分でノイズを付与していることから、その適用対象数は 60 を上回る。この違いが、本実験と 2020 年センサスにおける zCDP の導入効

---

[11] 2.4 節で述べた通り、レコード数をNとしたとき、およそ$\delta < 1/N$ と設定されることが多い。本実験は国勢調査の個票データを対象としていることから、N は日本の総人口 (約1.2×10^8) に相当する。すなわち、δの値は 10^{-8} ないし 10^{-9} より小さくすることが「一般的」とされることになる。

[12] より厳密には Staircase メカニズムが最適であるとされ (Geng and Vismanath (2014))、さらに値域が整数であるという制約 (整数制約) の下では、幾何メカニズム (離散 Laplace メカニズムとも呼ばれる) が最適とされる (Ghosh et al. (2012))。ただし、いずれも Laplace 分布に類似した分布のノイズを加える手法であり、ε が十分に小さい条件下では Laplace メカニズムと大きな差異はない。

果の差異をもたらしたと考えられる。

これらの議論を踏まえると、わが国の国勢調査に差分プライバシーの方法論を導入するにあたっては、単純に 2020 年センサスに倣って zCDP を導入するべきとは言えず、実際に作成する集計表における集計区分のあり方や、(センサスデータで必要とされたような) 特殊な集計条件への対応の必要性などに基づき、そのメリットやデメリットを定量的に勘案した上で結論づけるべきと考えられる。たとえば、平成 22 年国勢調査のメッシュ人口への非負 Wavelet 法 (寺田他(2015)) および 2020 年センサスの手法 (Census TDA) の適用実験 (石岡・寺田(2024)) や、令和 2 年国勢調査のメッシュ人口への両手法の適用実験 (Ishioka and Terada(2025)) においては、メッシュ人口に対して非負 Wavelet 法と Census TDA を適用するにあたり、それぞれの内部でのノイズ付加において Laplace メカニズムを利用して差分プライバシーを得る場合と、Gaussian ノイズを用いて zCDP 経由で近似差分プライバシー得る場合について、本稿と同様に δ の値を変動させながら同一 ε 条件下での誤差の大きさについて比較評価している。その結果、いずれの手法を適用する場合であっても、狭い領域を対象とした場合 (合成則の適用回数が少ない) においては Laplace メカニズムが優位であり、広い領域を対象とした場合 (合成則の適用回数が多い) においては zCDP に基づく Gaussian メカニズムが優位となる結論を得ている。この結果はこれまでの議論と符合するものであり、有用性の観点からの zCDP の導入の是非は一概に結論づけられるものではなく、上記の通り個々の統計の性質ごとに定量的な判断の元に検討する必要があることを示唆している。

また、2.4 節で述べたように、zCDP を用いてプライバシー損失を計量した場合、(純粋な) 差分プライバシーではなく近似差分プライバシーによる安全性しか与えられないことにも留意が必要である。本実験における各種の結果が示した通り、ε が同一の条件下であっても、zCDP に基づく Gaussian メカニズムがもたらす誤差の程度は δ の値によって大きく異なる。しかし、この δの値が具体的にいくつであるべきかについて確たる基準はなく、その設定には多分に恣意性を含みうることから、近年の研究ではその点が「有害」として問題視されつつある (Gomez et al.(2025))。したがって、zCDP の導入を検討するにあたっては、δ の恣意性について慎重に検討した上でなんらかの基準を設けるか、もしくは δ に依存しない (近似差分プライバシーへの変換を経由しない) 安全性表現を導入する可能性などについて検討を進めることが求められる。

6. まとめ

本稿では、わが国の公的統計における差分プライバシーの方法論の適用可能性を追究するために、センサスデータの公表にあたってセンサス局で採用された zCDP に着目し、令和 2 年国勢調査の個票データを用いて作成した集計表をもとに、zCDP を適用した場合における各種の差分プライバシーの実現手法の有用性を比較・検討した。特に、これまで国勢調査を用いた差分プライバシーに関する実証研究で議論した統計数値に対する Laplace ベースのノイズの付与に対して、zCDP に基づく Gaussian ベースのノイズの適用の有効性を比較・検証した。

本研究の成果によれば、zCDP を適用した場合、δ の値によって付与されるノイズの値が変わることから、Laplace ベースのノイズと比較して、センサス局が適用した Gaussian ベースのノイズが必ずしも有効な手法であるとは言えないことが明らかになった。このことから、zCDP の導入にあたっては、対象となる公的統計データの特性に応じて、zCDP の有効性に関する定量的な検証結果をもとに検討することが求められよう。

こうした点を踏まえると、わが国における差分プライバシーの公的統計への適用可能性に

ついてはさらなる実証実験が必要になるが、これについては今後の検討課題としたい。

謝辞

本稿は、JST 経済安全保障重要技術育成プログラム【JPMJKP24U5】の支援を受けている。

参考文献

[1] 石岡卓将・寺田雅之 (2024)「大規模集計データへの zCDP の適用」Computer Security Symposium 2024, pp915-922.
[2] 伊藤伸介・村田磨理子・高野正博(2014)「ミクロデータにおける匿名化技法の有効性の検証―全国消費実態調査と家計調査を例に―」,『統計研究彙報』第 71 号，pp.83-124.
[3] 伊藤伸介・星野なおみ (2014) 「国勢調査ミクロデータを用いたスワッピングの有効性の検証」『統計学』107 号, pp.1-16.
[4] 伊藤伸介(2019)「公的統計データにおける秘匿性と有用性の評価のあり方に関する一考察―スワッピングを中心に」坂田幸繁編『公的統計情報―その利活用と展望』中央大学出版部，pp. 39-62.
[5] 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.
[6] 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.
[7] 伊藤伸介・寺田雅之 (2023)「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―」『統計研究彙報』，第 80 号，pp.117-136.
[8] 伊藤伸介・寺田雅之・加藤駿典 (2024)「公的統計に対する差分プライバシーの適用と有効性の評価に関する検討―国勢調査を例に―」『統計研究彙報』第 81 号，pp.69-88.
[9] 伊藤伸介・寺田雅之・加藤駿典・松井秀俊 (2025)「差分プライベートな国勢調査データの有用性に関する定量的な評価研究」『統計研究彙報』第 82 号，pp.101-120.
[10] 伊藤伸介(2025)「海外における公的大規模データの利活用の現状」『日本労働研究雑誌』No.779，pp.53-64.
[11] 寺田雅之・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.
[12] 寺田雅之・山口高康・本郷節之(2017a)「匿名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』第 58 巻第 9 号, pp.1483-1500.
[13] 寺田雅之・山口高康・本郷節之(2017b)「高次元大規模データへの差分プライバシー適用のための最適精緻化法」『SCIS2017 予稿集』3B3-5, pp.1-8.
[14] Abowd, J. M. (2018). Staring-down the database reconstruction theorem, Joint Statistical Meetings, Vancouver, BC, Canada.
[15] Abowd, J. M. and M. B. Hawes (2023) "21st Century Statistical Disclosure Limitation: Motivations and Challenges", Working Paper ced-wp-2023-002.
[16] 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.
[17] Daniel, O. (2025) "Is it really private if you can't explain it? A practical framework for

productonalising legally-compliant synthetic data in government", Paper Presented at UNECE Expert Meeting on Statistical Data Confidentiality 2025, Barcelona, Spain, pp.1-9.

[18] Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006a) "Calibrating Noise to Sensitivity in Private Data Analysis", Theory of Cryptography 2006, pp. 265-284.

[19] Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., and Naor, M. (2006b) "Our data, ourselves: privacy via distributed noise generation", EUROCRYPT 2006, pp. 486-503.

[20] Dwork, C. and Roth, A. (2014) "The Algorithmic Foundations of Differential Privacy", Foundations and Trends in Theoretical Computer Science, Vol 9, Nos. 3-4, pp. 211-407.

[21] 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.

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

[23] 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.

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

[25] Geng, Q. and Vismanath, P. (2014) "The Optimal Mechanism in Differential Privacy", *2014 IEEE International Symposium on Information Theory*, pp. 2371-2375.

[26] Gomez, J.F., Kulynych, B., Kaissis, G., Hayes, J., Balle, B., Honkela, A. (2025) "(ε, δ) Considered Harmful: Best Practices for Reporting Differential Privacy Guarantees.", in Proceedings of the 2025 Theory and Practice of Differential Privacy (TPDP 2025). Available at: arXiv:2503.10945 [cs.LG].

[27] Ghosh, A., Roughgarden, T., and Sundararajan, M. (2012) "Universally Utility-maximizing Privacy Mechanisms.", SIAM J. Comput., Vol. 41, No. 6, pp. 1673-1693.

[28] Hawes, M. B., E. M. Brassell, A. Caruso, R. Cumings-Menon, J. Devine, C. Dorius, D. Evans, K. Haase, M. C. Hedrick, S. H. Holan, C. D. Hollingsworth, E. B. Jensen, D. Kifer, A. Krause, P. Leclerc, J. Livsey, R. A. Rodríguez L. T. Rogers, M. Spence, V. Velkof, M. Walsh, J. Whitehorne, and S. A. Keller (2025) "Towards a Principled Framework for Disclosure Avoidance", Working Paper ced-wp-2024-005.

[29] Ishioka, T. and Terada, M. (2025) "Utility of the Non-Negative Wavelet Mechanism with Zero-Concentrated Differential Privacy", 20th International Workshop on Security (IWSEC2025), (to appear).

[30] Ito, S., Yoshitake, T., Kikuchi, R., and Akutsu, F. (2018) "Comparative Study of the Effectiveness of Perturbative Methods for Creating Official Microdata in Japan", *Proc. intl. conf. Privacy in Statistical Databases (PSD 2018)*, LNCS 11126, Springer, pp. 200–214.

[31] Muralidhar, K., Ruggles, S., (2024) "Escalation of Commitment: A Case Study of the United States Census Bureau Efforts to Implement Differential Privacy for the 2020 Decennial Census", Domingo-Ferrer, J. and Önen, M.(eds.) *International Conference, PSD 2024 Antibes Juan-les-Pins, France, September 25–27, 2024 Proceedings*, Springer, pp.393-402.

[32] 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.

付図　本実験で用いた変数の分類区分

1.　性別

性別	
1	男
2	女

2.　年齢

年齢	
1	0～4歳
2	5～9歳
3	10～14歳
4	15～19歳
5	20～24歳
6	25～29歳
7	30～34歳
8	35～39歳
9	40～44歳
10	45～49歳
11	50～54歳
12	55～59歳
13	60～64歳
14	65～69歳
15	70～74歳
16	75～79歳
17	80～84歳
18	85歳以上

3．労働力状態

労働力状態	
1	就業者
2	完全失業者
3	非労働力人口