

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—

2025年9月9日

(独)統計センター / 総務省統計研究研修所 加藤 駿典

中央大学経済学部 伊藤 伸介

NTTドコモ / 京都橘大学工学部 寺田 雅之

滋賀大学データサイエンス学部 松井 秀俊

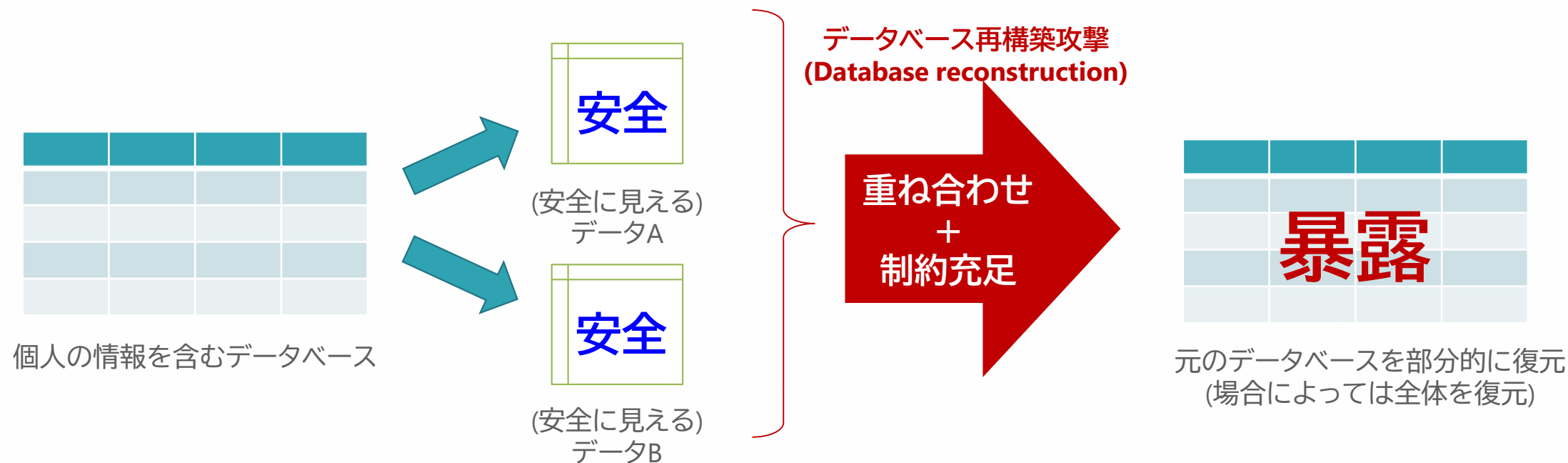
本報告の内容は個人的見解を示すものであり、
統計センターの見解を示すものではありません。

公的統計をつくる 活かす 支える

- アメリカセンサス局は、プライバシーに関する懸念を2010年センサス以前から持っていた。
- 2001年にセンサス局内部に設置されたDSEP(=Data Stewardship Executive Policy Committee)は、2010年センサスまで適用していたスワッピングとは異なる新たな方法論について、2020年人口センサスに向けて模索していた。
- **データベース再構築攻撃(Database Reconstruction Attack)**が現実的な脅威として指摘された(Abowd, 2018)。
- その対策として、**差分プライバシー(Differential Privacy)**の適用が検討される。(Jamin, 2021)

【データベース再構築攻撃 (Dinur and Nissim, 2003)】

あるデータベースから生成された (一見して安全に見える) 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、データに含まれる**個人のプライバシーを暴露**する攻撃。



アメリカセンサス局は、

- 2020年の人口センサスに向けて、2010年人口センサス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た。
- その際、実現方式として**TopDownアルゴリズム**を用いて、**プライバシー損失予算 ϵ** の調整を行った (Garfinkel et al., 2019)
- 最終的に、 **$\epsilon = 19.61$** に設定されたプライバシー保護済マイクロデータファイル(**PPMFs**)が公開された(2021年6月)。

↓(2020年センサスを対象として)

- 2021年8月に、差分プライバシーを適用した統計表区画改定データ(PL94-171)を公表した。
- 2024年に、一般公開型マイクロデータとして、差分プライバシーを適用したPPMFsを公開した。

- 2023年5月～2024年9月には、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、居住歴を含む住宅に関する特性値に関する集計データである、**人口・住宅ファイル (Demographic and Housing Characteristics File)** の公表に際して、差分プライバシーが適用された (伊藤, 2025)。
- なお、2020年9月以降では、差分プライバシー適用に際して、その拡張技術である **zero-Concentrated Differential Privacy (zCDP)** (Bun and Steinke, 2016) によってプライバシー保証がなされている。

本報告のモチベーション

- 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「zCDP」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、統計実務において有益であると考ええる。

本報告の目的

- 本報告では、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の実用性を模索する。
- 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、その有効性を検証する。

プライバシー保護における「安全性指標」を与える枠組み

- 特定のプライバシー保護方式を指す言葉ではない。
- 差分プライバシーを実現するプライバシー保護方式は数多く存在。
(集計値やデータにノイズを付加する方法が一般的)
- 様々な方式の安全性を統一的に測る指標として、プライバシー損失予算 (privacy loss budget) “ ϵ ” を与える(値が小さいほど安全)。

任意の攻撃能力や背景知識を持つ攻撃者に対する安全性

「想定外」の攻撃に対する堅牢性 (どんな AI ができても安全)

→ 任意のデータの組み合わせに対する再構築攻撃にも安全

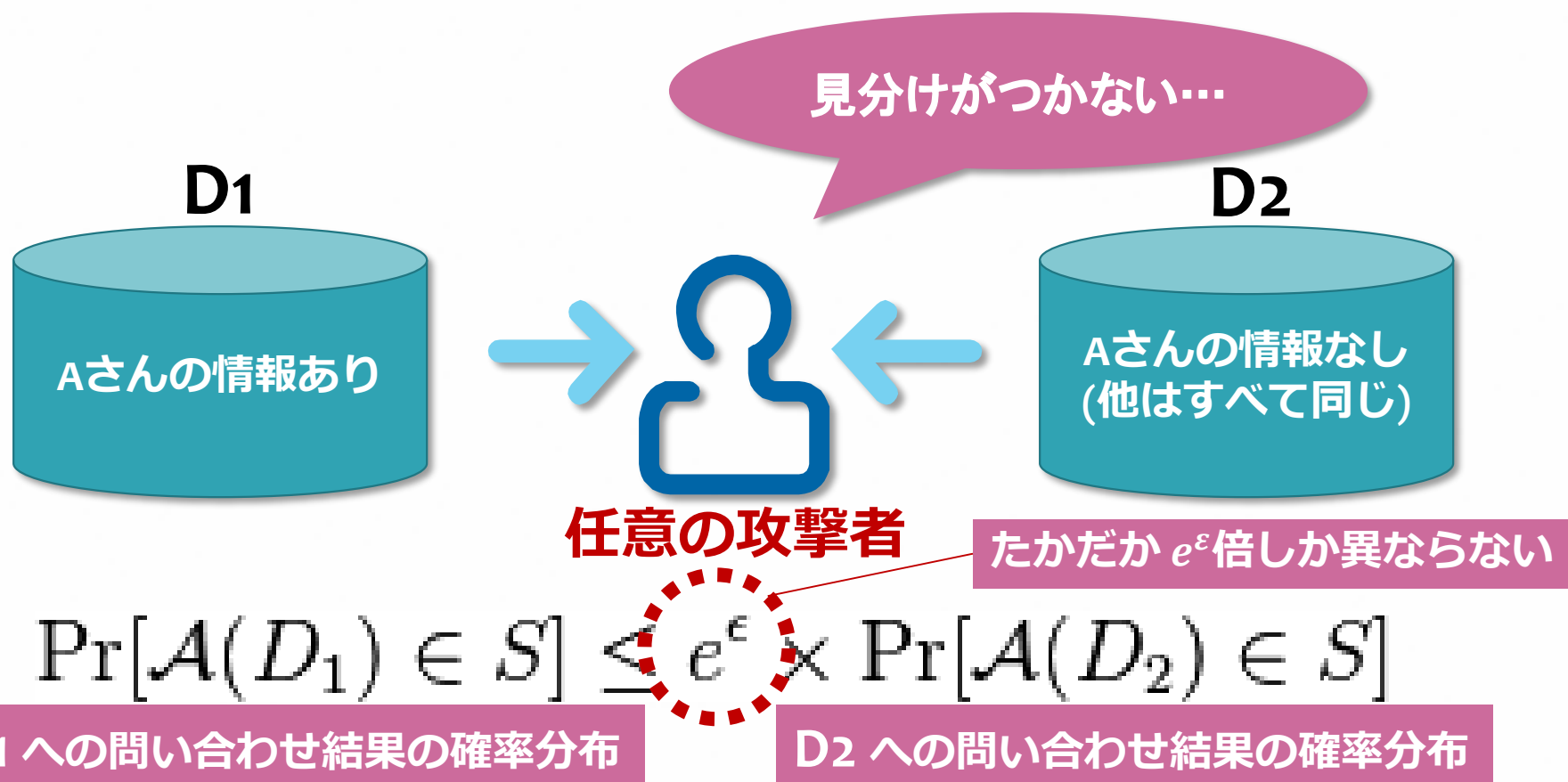
【定義】

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 $\mathcal{A}: \mathcal{D} \rightarrow \mathcal{R}$ が下記を満たすとき、 $\mathcal{A}$ は ϵ -差分プライバシーを満たす。

ただし、ここで S は $\mathcal{A}$ の出力空間 $\mathcal{R}$ の任意の部分集合である ($S \subseteq \mathcal{R}$)。

$$\Pr[\mathcal{A}(D_1) \in S] \leq e^\epsilon \times \Pr[\mathcal{A}(D_2) \in S]$$

Aさんの情報が**入っている**DBへの問い合わせ結果と、
Aさんの情報が**入っていない**DBへの問い合わせ結果が**区別できない**なら、
この問い合わせにより **Aさんのプライバシーが漏れることはない。**
⇒差分プライバシーを満たす



zCDPは、

- 差分プライバシーの拡張的な枠組み
- レニー情報量 (Rényi divergence) を用いて、以下定義の通り、 $\mathcal{A}(D_1)$ と $\mathcal{A}(D_2)$ の分布の近さを評価して、安全性指標“ ρ ”を定める。

【定義】

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 $\mathcal{A}: \mathcal{D} \rightarrow \mathcal{R}$ が下式を満たすとき、 $\mathcal{A}$ は ρ -zCDP を満たす。

$$D_\alpha(\mathcal{A}(D_1) \parallel \mathcal{A}(D_2)) \leq \rho \alpha$$

ただし、ここで $D_\alpha(\mathcal{A}(D_1) \parallel \mathcal{A}(D_2))$ は $\mathcal{A}(D_1)$ の分布と $\mathcal{A}(D_2)$ の分布との間の α -レニー情報量 (α -Rényi divergence) である。

【 ρ から ε への変換 (Bun and Steinke (2016), 石岡・寺田 (2024))】

- ρ -zCDPを満たす方式は、任意の $\delta > 0$ に対して、 (ε, δ) -近似差分プライバシーという安全性を満たすことができる。
- そのため、 ρ と δ の組合せにより、(純粋な)差分プライバシーと比較可能な ε への変換が可能となる。

- 変換式:

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

(δ : 出力結果が差分プライバシーを満たせない確率)

- $\alpha \in (1, \infty)$ 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、 $\alpha \rightarrow 1$ のとき KL-divergence (D_{KL}) に対して、 $\alpha \rightarrow \infty$ のとき max-divergence (D_∞) に対してそれぞれ漸近する (Erven and Harremoës (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。

- 伊藤他(2024)は、平成27年国勢調査の個票データを用いて、地理的区分が異なる統計表に各種の差分プライバシーの実現方式を適用した場合の有用性の評価を行った。
- 伊藤他(2025)は、令和2年国勢調査の個票データから作成した統計表を用いて、生態学的誤謬(ecological fallacy)の観点から有用性の検証を行った。
- いずれも(純粹な)差分プライバシーに基づき検証した。
- 評価指標として、**平均絶対誤差 (Mean Absolute Error=MAE)**を用いて有用性を評価した。

- 国勢調査への差分プライバシーの適用に際しては、ノイズの付加に加えて、それによって生じる統計表上の矛盾(例:負の人口値や表間の不整合)を解消するための「**精緻化**」も必要となる。
- そこで**実現方式**としては、主に以下の2種類が考えられる。

ボトムアップ構成法

- ノイズ付加と精緻化を最下位の地域区分の集計表に適用
- たたみ上げにより上位の集計表を作成

トップダウン構成法

- ノイズ付加と精緻化を全国表から「トップダウン」の方向に階層的に適用
- 2020年アメリカセンサスもこのアプローチを採用 (もう少し複雑)

⇒伊藤他(2024)では、トップダウン構成法が最も有効な実現方式であることが実証的に示された。

【使用するデータ】

令和2年国勢調査の個票データ (調査票情報)

【方法・目的】

- 性別、年齢、労働力状態の3つの変数を対象に、地域区分の粒度が異なる小地域別の集計表を作成し、差分プライバシーの実現方式を適用する。
- その上でzCDPの有効性を明らかにするために、 ϵ と δ の数値を変えた場合の有用性について検証を行う。
- その際、純粋な差分プライバシー (pure-DP) を与えるLaplaceノイズを用いる方法と、近似的な差分プライバシー (zCDP) を与えるGaussianノイズを用いる方法の比較も行う。

【実験条件】

①集計表の種類 (15種類)

②実現方式

(a) ボトムアップ構成法, (b) トップダウン構成法, (c) Laplaceメカニズム

③ノイズの種類

(a) Laplaceノイズ (pure-DP), (b) Gaussianノイズ (zCDP)

④プライバシー損失予算

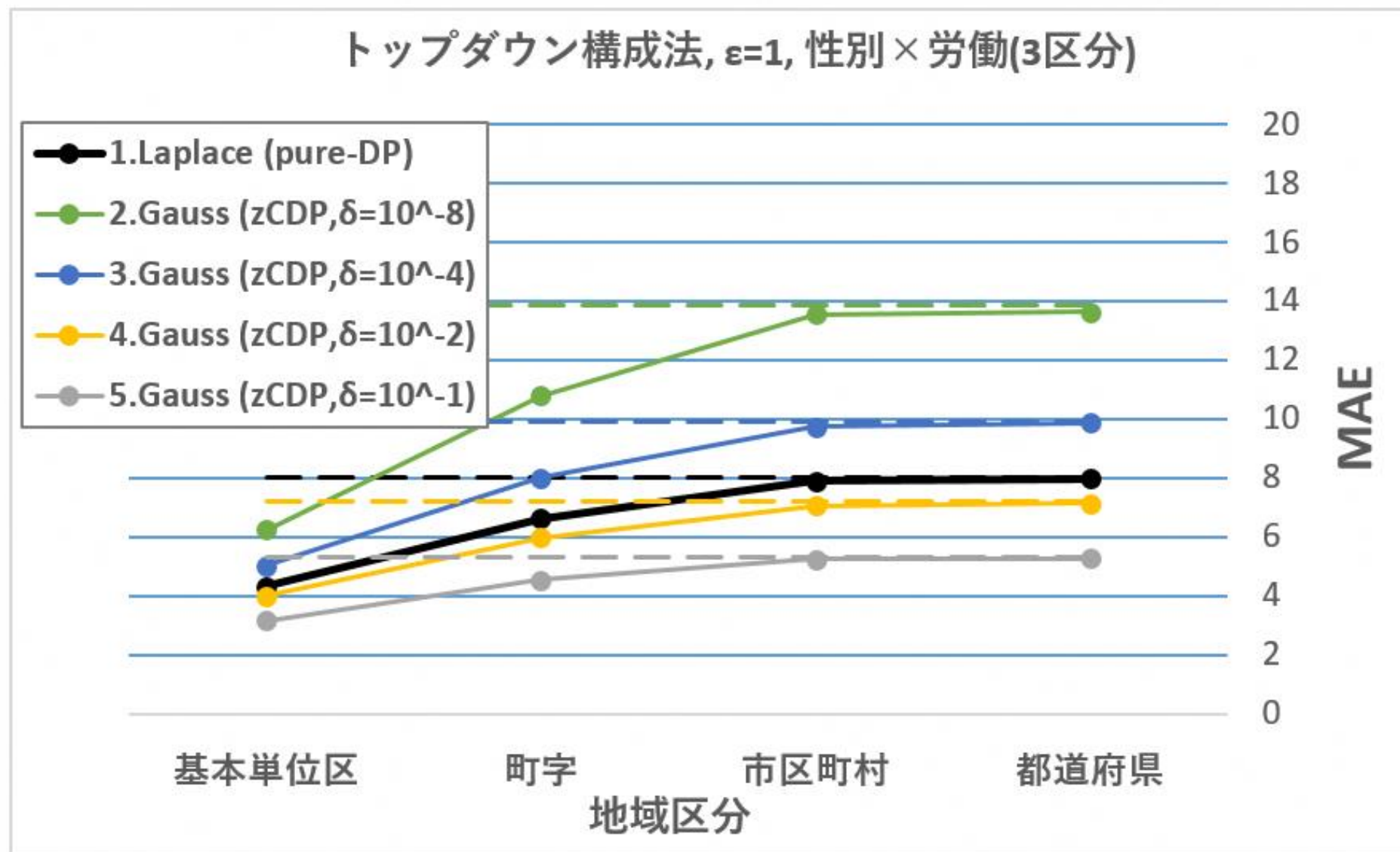
$\epsilon=0.1, 0.2, 0.7, 1, 1.1, 5, 10, 20$ ($\delta=10^{-1}, 10^{-2}, 10^{-4}, 10^{-8}$)

【有用性の評価方法】

4種類の地域区分

(a)都道府県、(b)市区町村、(c)町・字、(d)基本単位区

ごとに、MAEとRMSEを算出した。



注 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。
隣接の定義は公開n条件とした。

- 本実験では、Laplaceノイズベース (pure-DP) とGaussianノイズベース (zCDP) で実現方式を比較した結果、いずれもトップダウン構成法が良い結果をもたらすことが確認された。
- これにより、zCDPを用いた場合でも、**トップダウン構成法の有用性の高さが保持**されることが確認された。
- 本実験結果から、pure-DPを与えるLaplaceノイズベースの方法と比較して、**近似的な差分プライバシー (zCDP) を与えるGaussianノイズベースの方法が、必ずしも有用性が高いとは言えない**(δ の値によって優劣が異なる)ことが確認された。
⇒ ϵ の値を固定すると、 δ の値によって必要なノイズの大きさが変わる(δ が小さいほど大きなノイズが必要となる)。

- 差分プライバシーの適用に関して、zCDPはより有効に作用するのか
⇒常に有効に作用するとは言えない。
- センサス局が採用したzCDPはベストな方法であったのか？
⇒米国センサスでの集計条件においては有効であったとされている。ただ、わが国の国勢調査の個票データを用いた本実験の条件では、有効とは言い難い結果が得られた。そのため、zCDP を採用すべきか否かは、集計の対象や条件ごとにそれぞれ判断する必要があると考えられる。
- δ によって必要なノイズが変化するが、 δ はどの程度の値なら良いのか？
⇒一般には $1/N$ (N は対象となるレコード数。国勢調査であれば総人口) 以下であることが望ましいとされるが、理論的根拠に乏しい (恣意性を多分に持つ) ことから近年では批判もある (Gomez et al. (2025) など)。そのため、 δ に依存しないノイズの決定手法などの研究動向を注視する必要があると考える。

- 本報告では、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、差分プライバシーの方法論の適用可能性を追究することに加え、zCDPの有効性について検証した。
- その結果、zCDPを適用する場合、 δ の値によって付与されるノイズの大きさが変わることから、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わかった。
- ではなぜ、アメリカセンサスにおいては**Gaussian**ノイズを用いるzCDPが有効に作用したのか。理由としては、以下が考えられる。
 - **zCDP**は、複数のクエリを組み合わせた複雑な出力において、安全性を適切に計算できることが大きな利点。
 - アメリカセンサスでは、人種や少数民族の扱いなどの特有の複雑さに対応するため、出力が複雑化した（そこで、**zCDP**の利点が発揮された）。
- 公的統計への差分プライバシー適用については、実証実験によるさらなる検討がもとめられる。

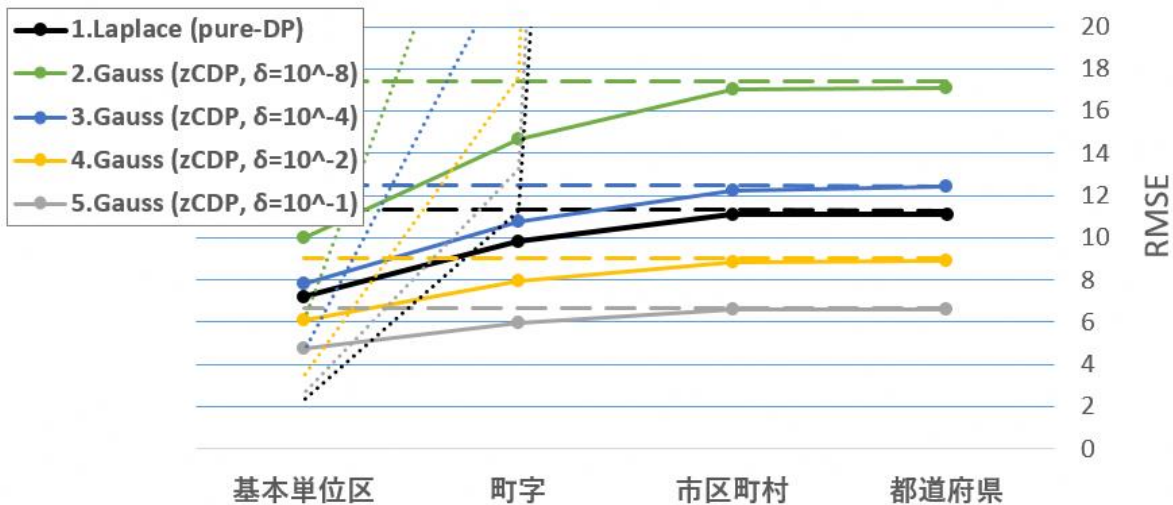
- 石岡卓将・寺田雅之(2024)「大規模集計データへのzCDPの適用」Computer Security Symposium 2024, pp915-922.
- 伊藤伸介・寺田雅之・赤塚裕人・北井宏昌 (2022) 「海外における公的統計に対する攪乱的手法の新たな取り組み—アメリカセンサス局による差分プライバシーの適用を中心に—」『統計研究彙報』第79号, pp.131-150.
- 伊藤伸介・寺田雅之 (2023)「海外における公的統計に関するプライバシー保護の現状—アメリカとイギリスの事例をもとに—」『統計研究彙報』, 第80号, pp.117-136.
- 伊藤伸介・寺田雅之・加藤駿典 (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.
- 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.
- 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.
- 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.
- Dwork, C. (2006) *Differential privacy*. ICALP.
- 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.
- Erven, T.v. and Harremos, P. (2014) "Rényi Divergence and Kullback-Leibler Divergence", *IEEE Trans. Information Theory* 60 (7), pp. 3797–3820.
- 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.
- 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].

謝辞

本研究は、JST経済安全保障重要技術育成プログラム【JPMJKP24U5】の支援を受けたものです。

【RMSE】

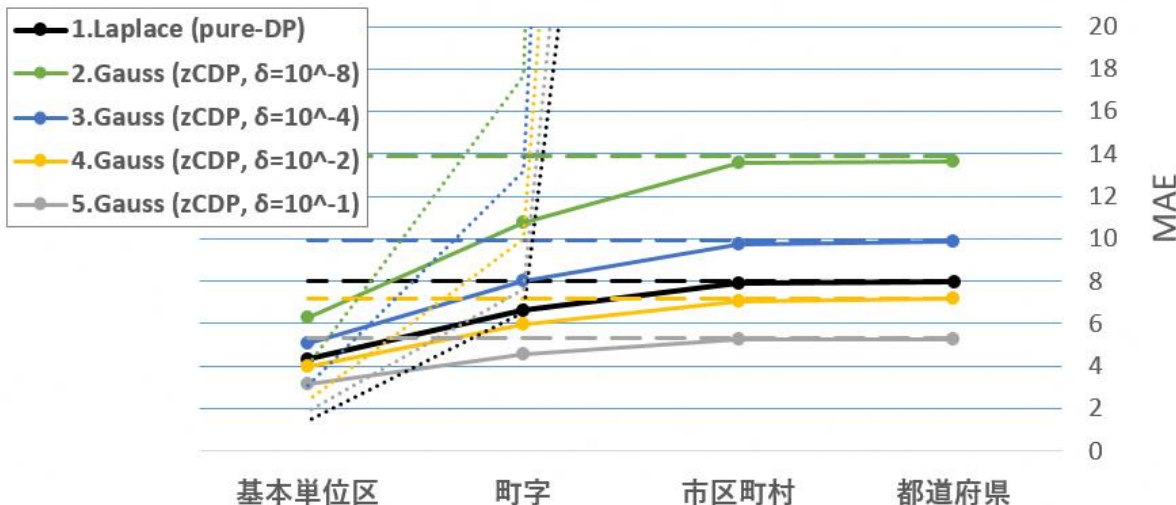
トップダウン構成法, 公開n, $\epsilon=1$, 性別×労働(3区分)



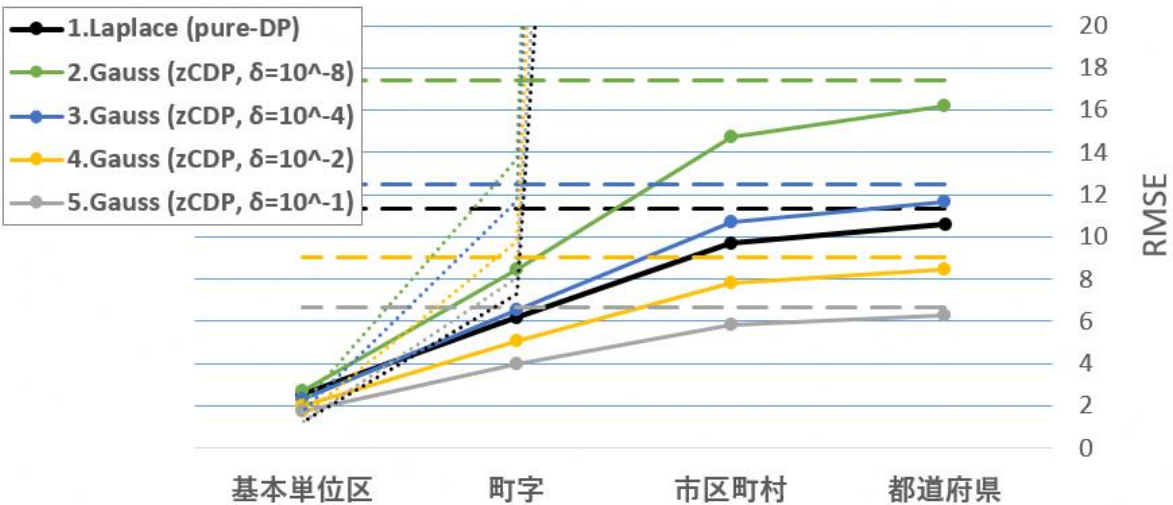
【MAE】

注 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。
点線は、ボトムアップ構成法の実験結果

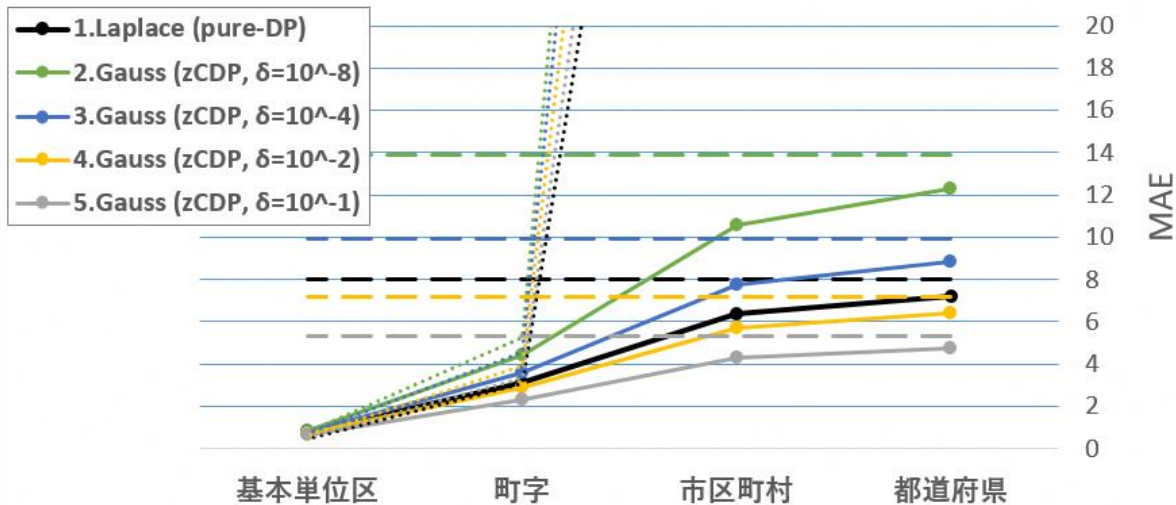
トップダウン構成法, 公開n, $\epsilon=1$, 性別×労働(3区分)



トップダウン構成法, 公開n, $\epsilon=1$, 性別×年齢(18区分)×労働(3区分)



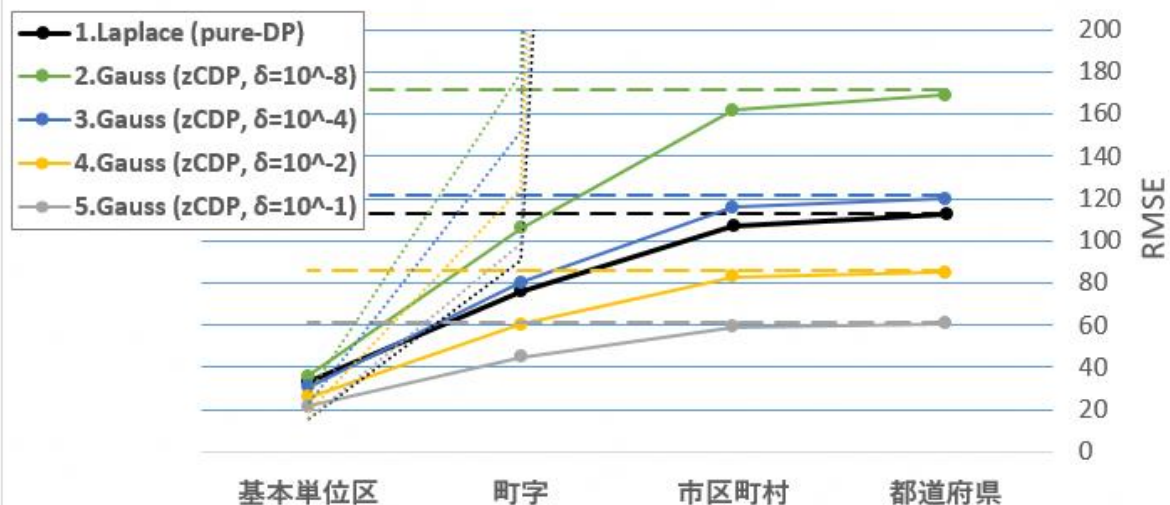
トップダウン構成法, 公開n, $\epsilon=1$, 性別×年齢(18区分)×労働(3区分)



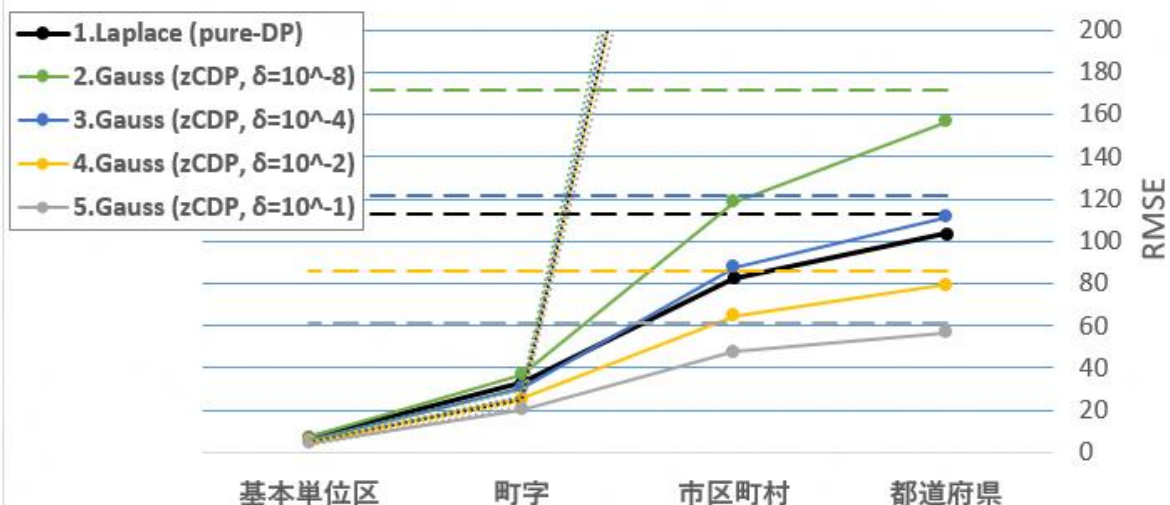
【補足資料】実験結果の一例($\epsilon=0.1$)

【RMSE】

トップダウン構成法, 公開 n , $\epsilon=0.1$, 性別×労働(3区分)



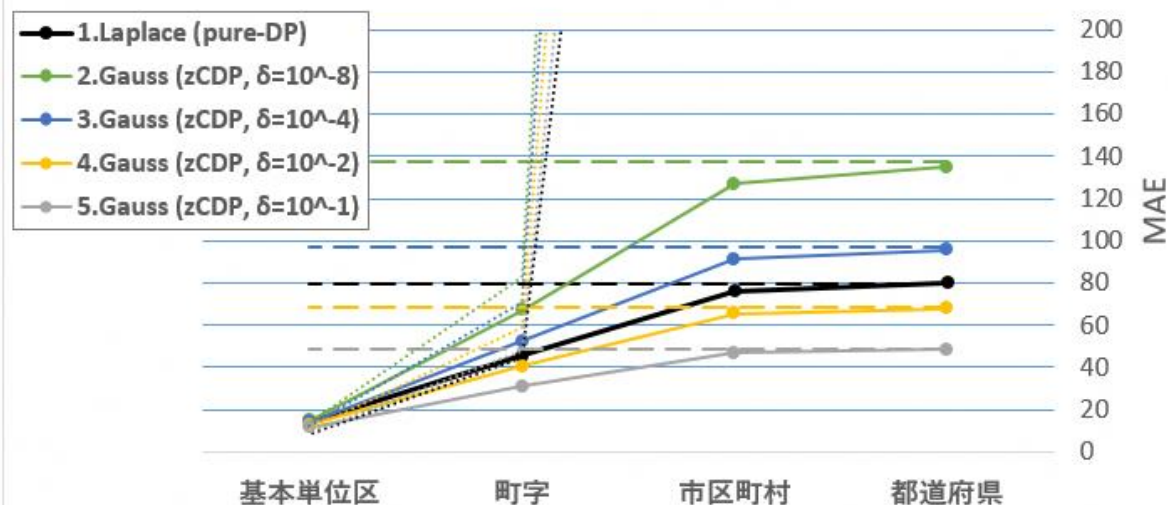
トップダウン構成法, 公開 n , $\epsilon=0.1$, 性別×年齢(18区分)×労働(3区分)



【MAE】

注 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。
点線は、ボトムアップ構成法の実験結果

トップダウン構成法, 公開 n , $\epsilon=0.1$, 性別×労働(3区分)



トップダウン構成法, 公開 n , $\epsilon=0.1$, 性別×年齢(18区分)×労働(3区分)

