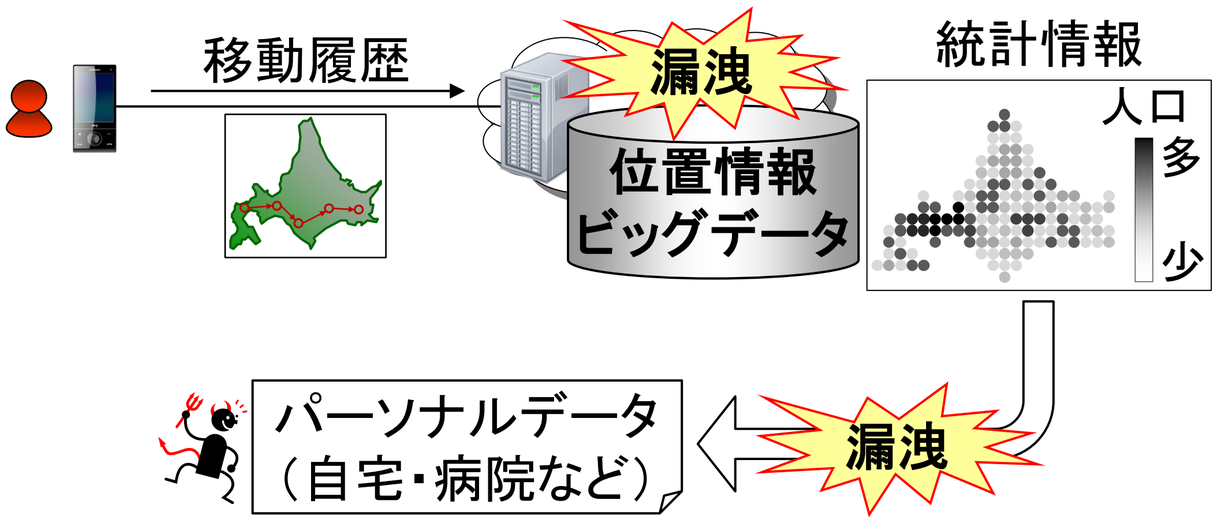
2024年5月24日　統計数理研究所　オープンハウス

差分プライバシーと統計解析への応用

村上　隆夫　　学際統計数理研究系　准教授

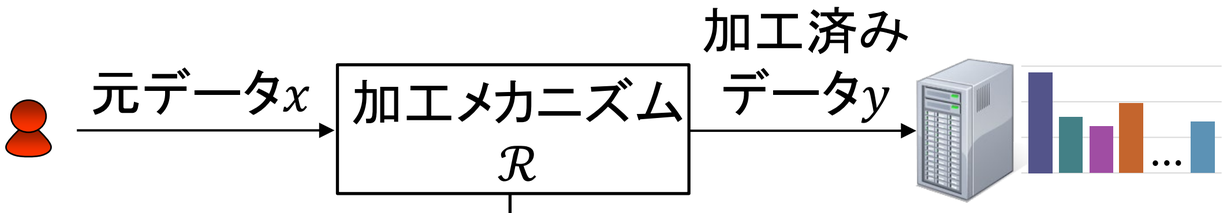
1. プライバシー問題

- IoTなどの普及に伴い、パーソナルデータの統計解析（例：人気スポットの分析）への期待が高まっている
- 一方、プライバシーの問題が懸念されている



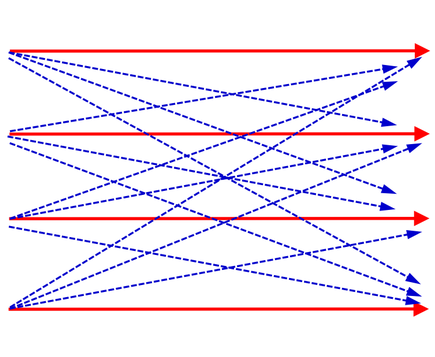
2. 差分プライバシー

- プライバシー保護技術の安全性指標のデファクト標準
- 近年、ユーザが自分で加工を行う「局所型差分プライバシー」（**LDP**: Local Differential Privacy）が実用化
- 例：GoogleがChromeの起動ページをLDPで解析



例

入力値 $x_1, x_2, \vdots, x_k$　　出力値 $y_1, y_2, \vdots, y_k$

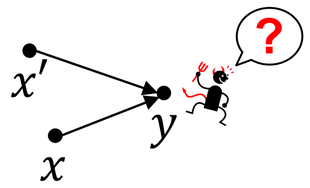


$$p_1 = \frac{e^{\varepsilon}}{k + e^{\varepsilon} - 1}$$

$$p_2 = \frac{1}{k + e^{\varepsilon} - 1}$$

定義（ε-LDP）

あらゆる元データ$x, x' \in \mathcal{X}$（$\mathcal{X}$: 定義域）と加工済みデータ$y \in \mathcal{Y}$（$\mathcal{Y}$: 値域）に対して



$$\Pr(y|x) \leq e^{\varepsilon} \Pr(y|x')$$

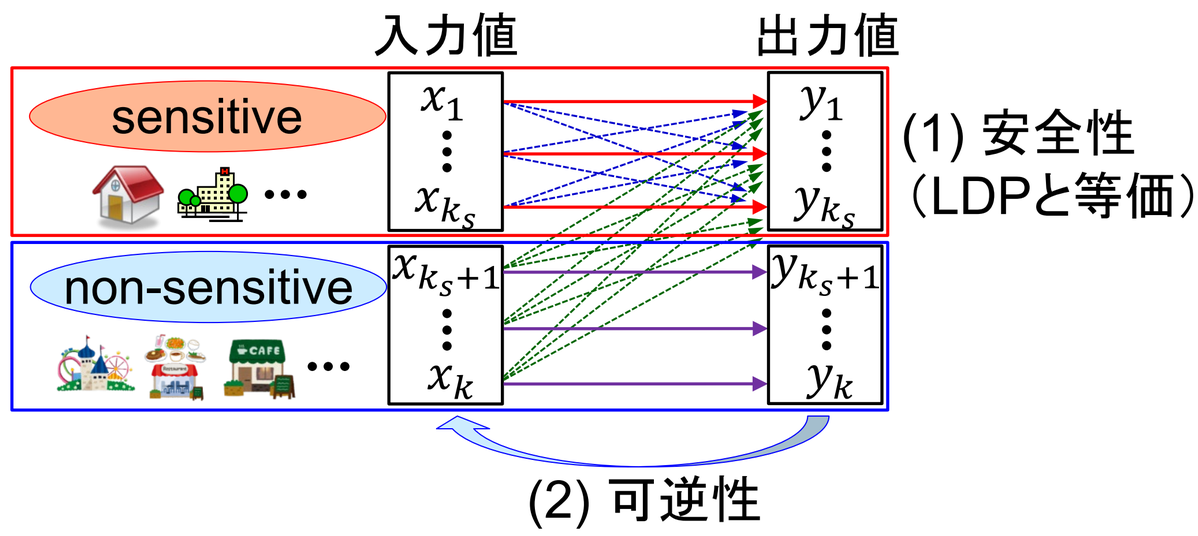
が成立するとき，加工メカニズム$\mathcal{R}$は**ε-LDP**を満たす
（ε: privacy budget）

直感的解釈

εが小さいとき（例：0～1）、$\Pr(y|x)$と$\Pr(y|x')$が近い
→ 攻撃者がyを見ても、入力値が分からない（安全）

3. LDPの有用性改善[1]

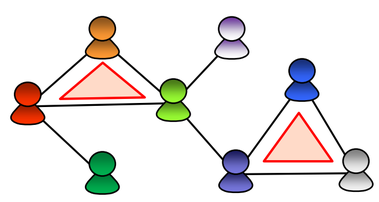
- 新しい安全性指標：**ULDP（Utility-Optimized LDP）**
  - sensitiveな入力値に対しては、LDPと等価な安全性を保証（安全性）
  - non-sensitiveな出力値からは対応する元データに戻せる（可逆性）→ ノイズ量の削減



- **GoogleがChromeに実装したLDPメカニズムの有用性（分布推定精度）を大幅向上**

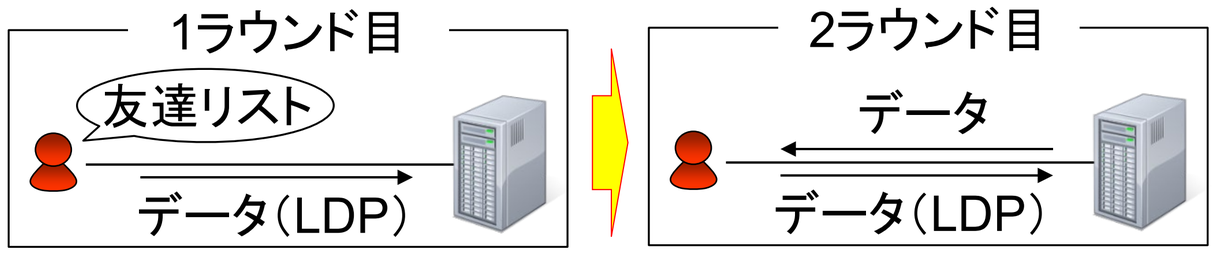
4. LDPに基づくグラフ統計解析[2]

- グラフ統計（部分グラフ数）
  - 「友達の友達が友達である確率」$= 3 \times \frac{\#\text{triangles}}{\#2\text{-stars}}$
    → 友達推薦の有効性が分かる
  - 但し、秘密の友達情報（edge）の漏洩は防ぎたい



Shape	Name	Count
△	Triangle	2
2-star	2-star	15
3-star	3-star	6

- LDPに基づくグラフ統計解析
  - k-starsに対しては1ラウンド、trianglesに対しては2ラウンドのLDPメカニズムを提案



- **k-starsは提案が最適、trianglesは2ラウンドでMSE（平均二乗誤差）が大幅に減る**ことを証明

MSE (n: ユーザ数, d_{max}: 最大次数 ($\ll n$))

	1ラウンド		2ラウンド
	下限	上限	上限
k-stars	$\boldsymbol{\Omega(nd_{max}^{2k-2})}$ =	$\boldsymbol{O(nd_{max}^{2k-2})}$	-
triangles	$\boldsymbol{\Omega(nd_{max}^{2})}$	$O(n^4)$	$\boldsymbol{O(nd_{max}^{3})}$

[1] Takao Murakami, Yusuke Kawamoto, “Utility-Optimized Local Differential Privacy Mechanisms for Distribution Estimation,” Proc. USENIX Security, 2019.
[2] Jacob Imola*, Takao Murakami*, Kamalika Chaudhuri (*: equal contribution), “Locally Differentially Private Analysis of Graph Statistics,” Proc. USENIX Security, 2021.