

卒業研究発表会

2023/02/17

# 非対称な利得を考慮した プライバシー保護手法の提案

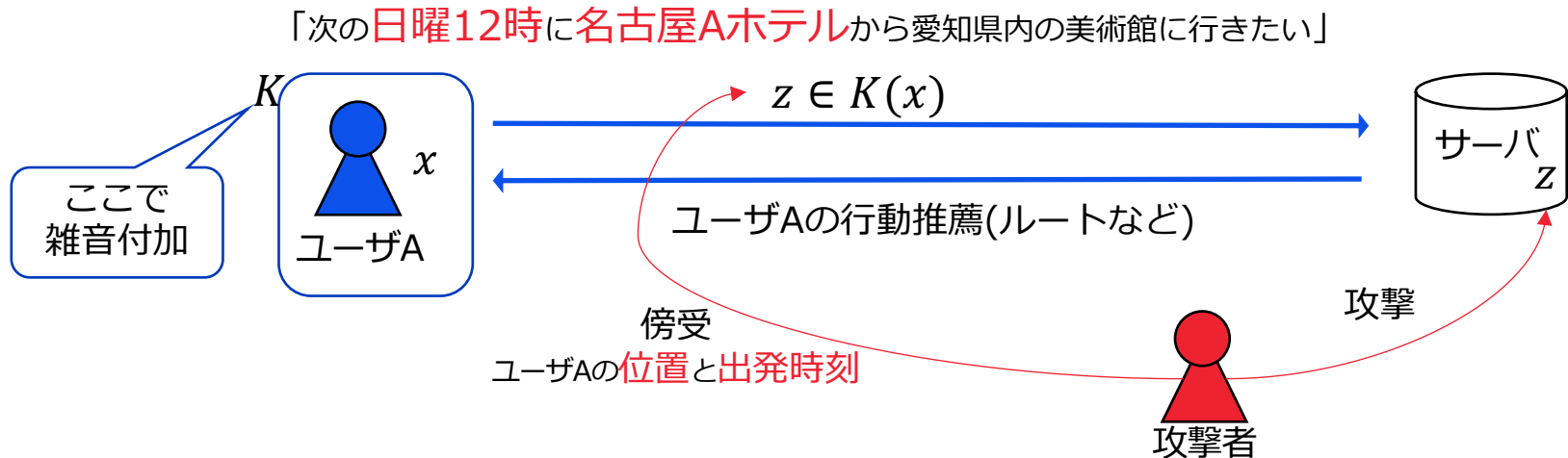
関研究室 4年

脇田侑輝

# 研究の背景：位置情報サービスにおけるプライバシー保護

ユーザの希望に応じて行動推薦を行うシステム<sup>†</sup>を考える

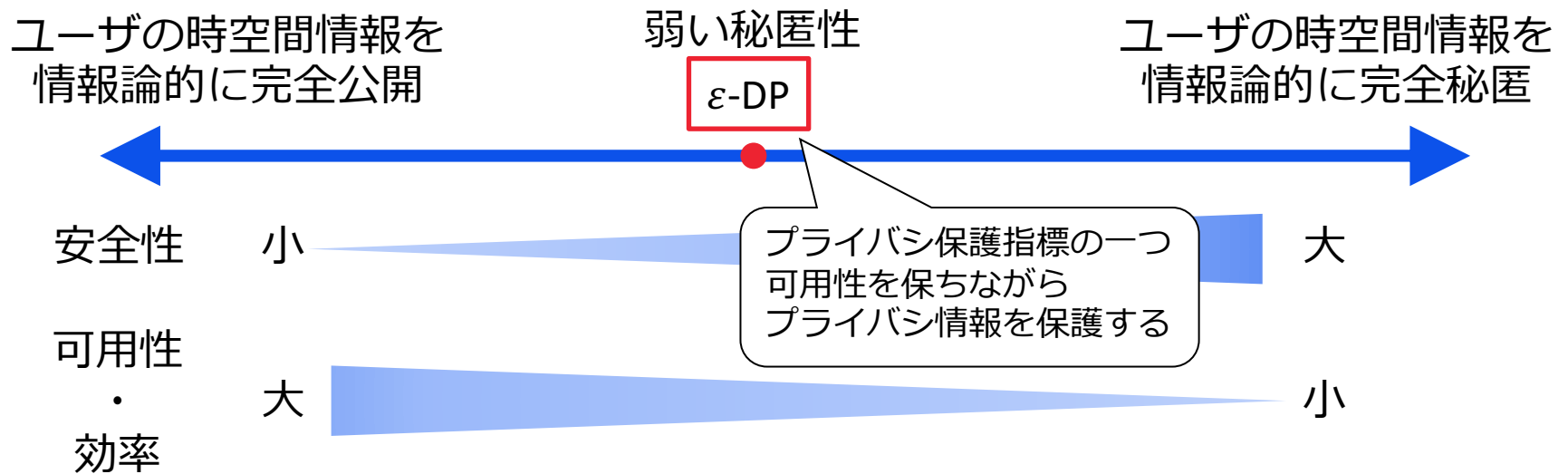
デジタルツインの行動推薦システムにて



通信内容もサーバ自体も攻撃されることを前提として、  
サービスの利得劣化を抑えつつユーザの時空間プライバシー情報を保護したい

<sup>†</sup> 奈良先端大・安本研究室「スマートシティの研究」 <http://ubi-lab.naist.jp/ja/>

# $\epsilon$ -差分プライバシー ( $\epsilon$ -differential privacy, $\epsilon$ -DP)<sup>[Dw06]</sup>



## $\epsilon$ -DPを満たして位置情報を保護する先行研究

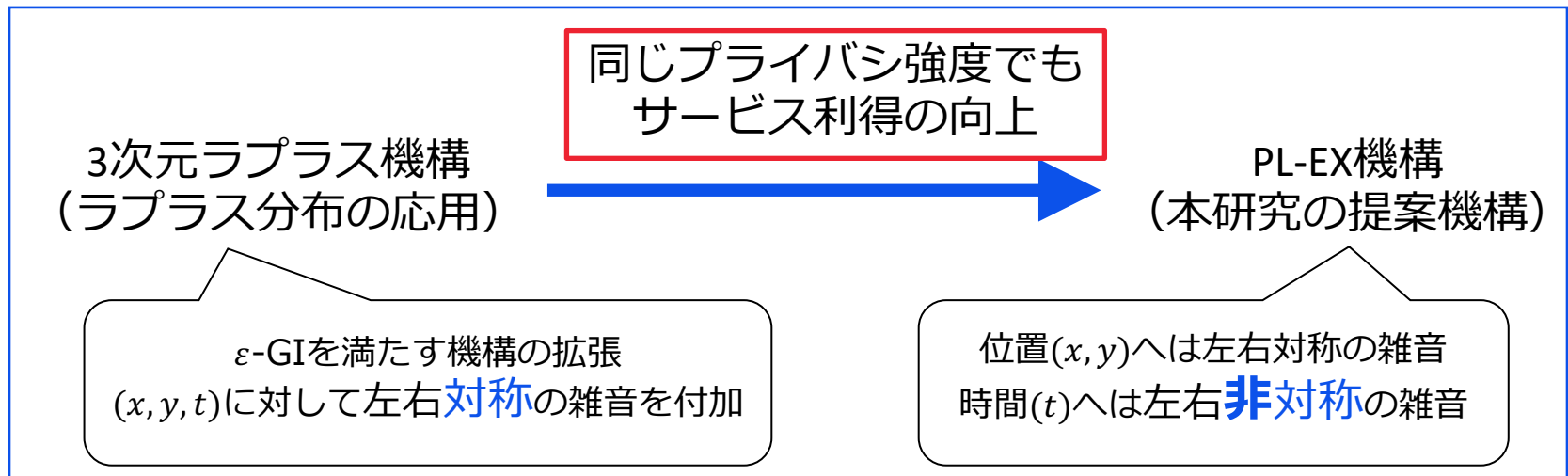
$\epsilon$ -**地理的識別不能性** ( $\epsilon$ -Geo-indistinguishability,  $\epsilon$ -GI)<sup>[ABCP13]</sup> という定義.

位置  $(x, y)$  に雑音付加して **ユーザの現在地点を曖昧化** することで  $\epsilon$ -GI を満たす.

[Dw06] C. Dwork, Differential privacy, ICALP 2006, LNCS 4052, 1-12.

[ABCP13] M. E. Andres, N. E. Bordenabe, K. Chatzikokolakis and C. Palamidessi, Geo-indistinguishability: Differential privacy for location-based systems, ACM CCS 2013.

$\epsilon$ -GIを満たす機構を，単純に時空間の3次元に拡張するのは容易  
しかし，雑音付加によるサービス利得の劣化が  
時間軸に対して対称でない場合に対応できない



## 研究成果

- $\epsilon$ -GIを拡張した指標  $\epsilon$ -時空間識別不能性 ( $\epsilon$ -spatio-temporal indistinguishability,  $\epsilon$ -STI)を提案した.
- 非対称な雑音機構として知られる指数機構を用いて  $\epsilon$ -STIを満たし時間の非対称性に対応した機構を構成した.

# $\varepsilon$ -時空間識別不能性 ( $\varepsilon$ -STI) の定義

$\varepsilon$ -GI<sup>[ABCP13]</sup>を3次元に拡張して以下を定義した.

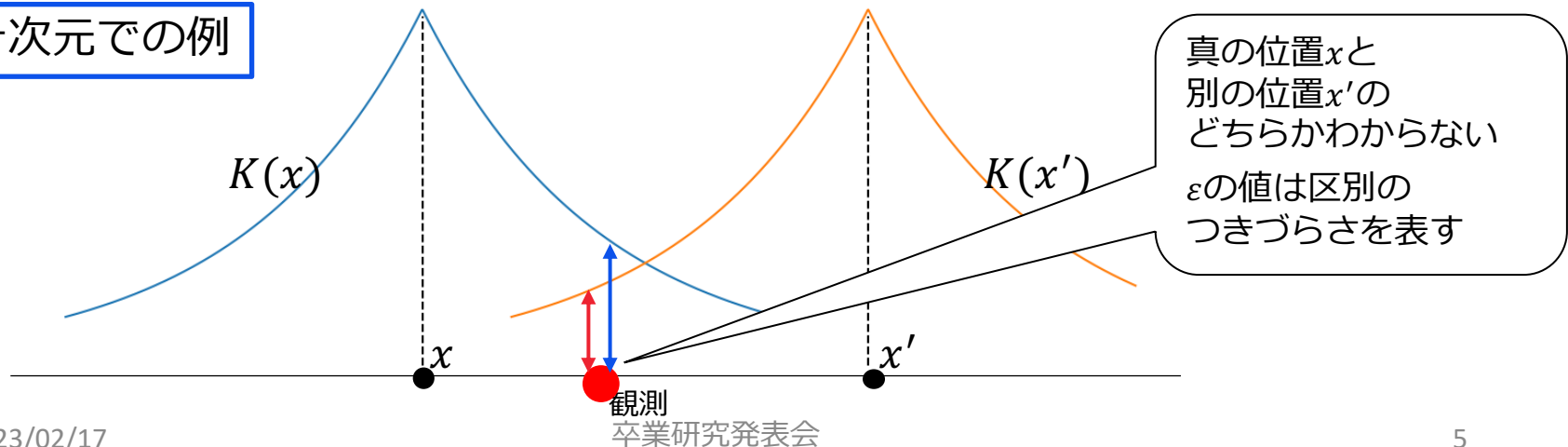
## 定義3.1 ( $\varepsilon$ -STI)

雑音付加機構 $K$ が任意の2点 $x, x' \in \mathbb{R}^3$ に対して, 以下を満たすとき $K$ は $\varepsilon$ -時空間識別不能性( $\varepsilon$ -spatio temporal indistinguishability,  $\varepsilon$ -STI)を満たすという.

$$d_{\mathcal{P}}(K(x), K(x')) \leq \varepsilon d(x, x')$$

- $\varepsilon (\geq 0)$ : プライバシ保護強度 ( $\varepsilon$ が小さいほど強い)
- $d(x, x')$ :  $x$ と $x'$ の3次元ユークリッド距離
- $d_{\mathcal{P}}(\sigma_1, \sigma_2)$ : 確率分布 $\sigma_1$ と $\sigma_2$ のある種の距離

## 一次元での例



次のような機構 $PL-EX$ を提案する.

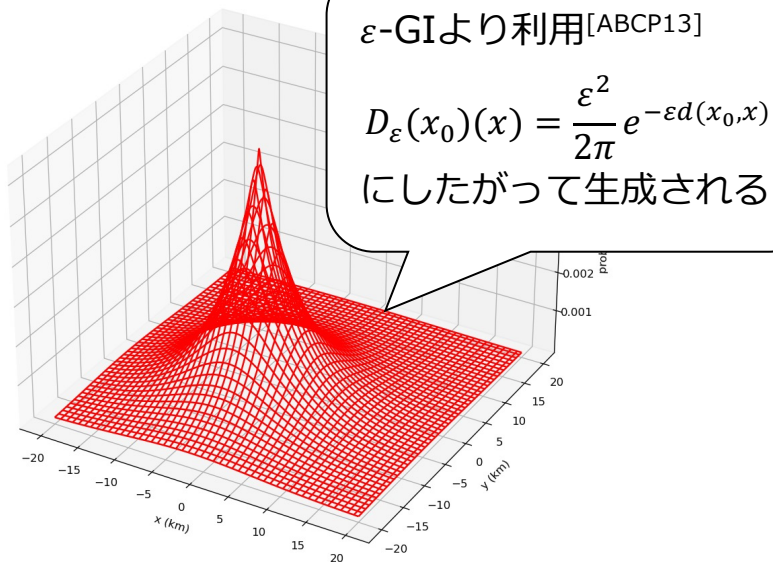
定義:  $PL-EX$ 機構

保護したい時空間データ $(x, y, t)$ に対して,

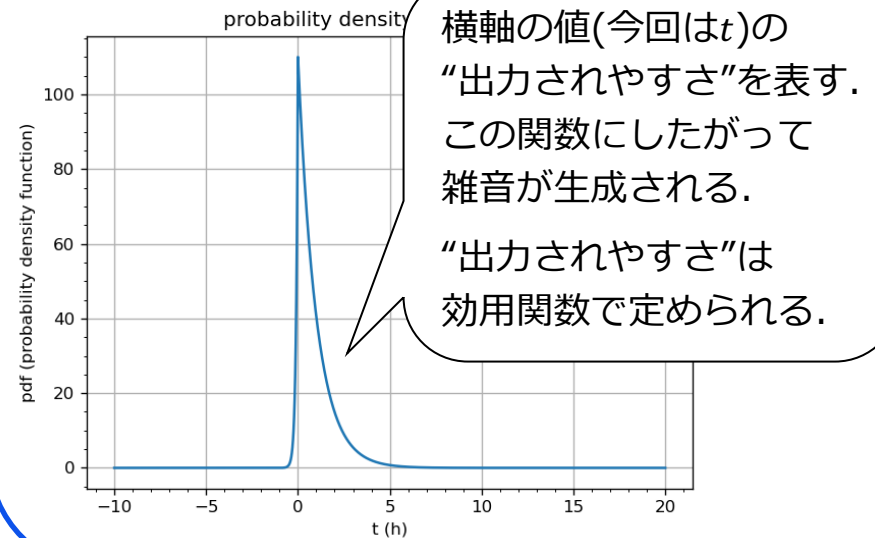
$$PL-EX((x, y, t)) = (PL(x, y), EXP(t))$$

ここで,  $PL$ : 平面ラプラス機構,  $EXP$ : 指数機構である.

## 平面ラプラス機構



## 指数機構



# PL-EX機構のパラメータについて

PL-EX機構は複数の機構の組み合わせである.

位置( $x, y$ )に平面ラプラス機構(PL) :  $D_{\varepsilon_{xy}}$ を,  
時間( $t$ )に指数機構(EXP) :  $M_E(\varepsilon_t, u, \mathbb{O})$ を適用する.  
以下の合成定理より,  $\varepsilon$ -STIが満たされる(ここで  $\varepsilon = \varepsilon_{xy} + \varepsilon_t$ ).

## $\varepsilon$ -DPの合成定理<sup>[DR14]</sup>

それぞれ $\varepsilon_i$ -DPを満たす $n$ 個の問い合わせ $Q_i$ がある( $i \in [n]$ ).  
任意のデータベース $D$ に対する $n$ 個の問い合わせは,  
 $Q = (Q_1(D), Q_2(D), \dots, Q_n(D))$ となり, これは $\sum_{i=1}^n \varepsilon_i$ -DPを満たす

[DR14] C. Dwork and A. Roth, The algorithmic foundations of differential privacy, Foundations and Trends in Theoretical Computer Science, Vol. 9, Nos 3-4, pp.42-44, 2014.

# ケーススタディの説明

## シナリオ

名古屋市内的あるユーザが現在地から閉館までに施設に到着できるか検証

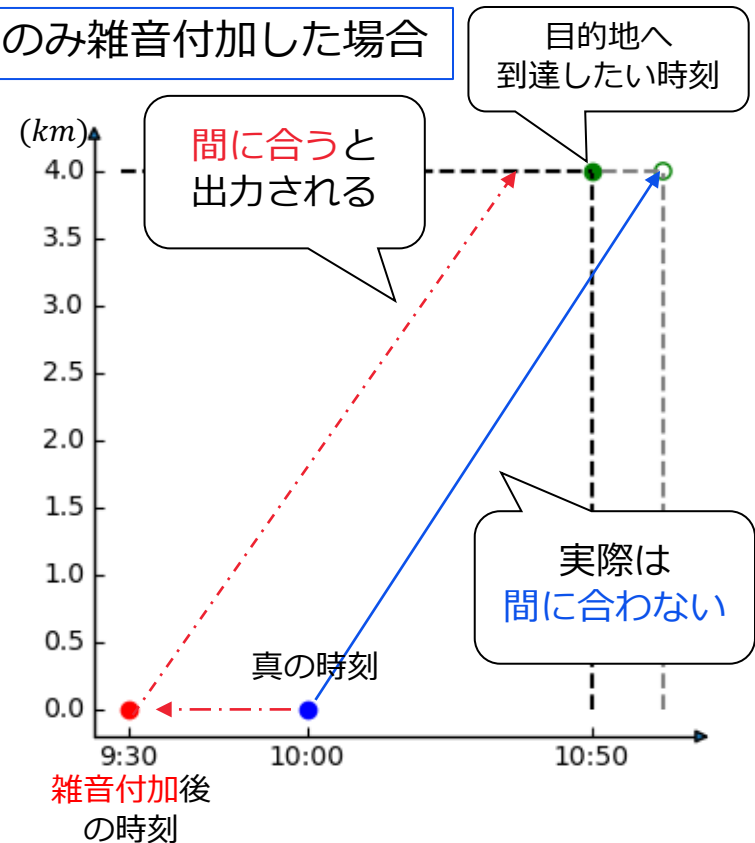
### 主な条件

- ユーザの移動速度は $4 \text{ km/h}$ .
- 実際には「間に合わない」地点へ「間に合う」と出力することは避けたい(サービス利得が劣化する)

### 実験内容

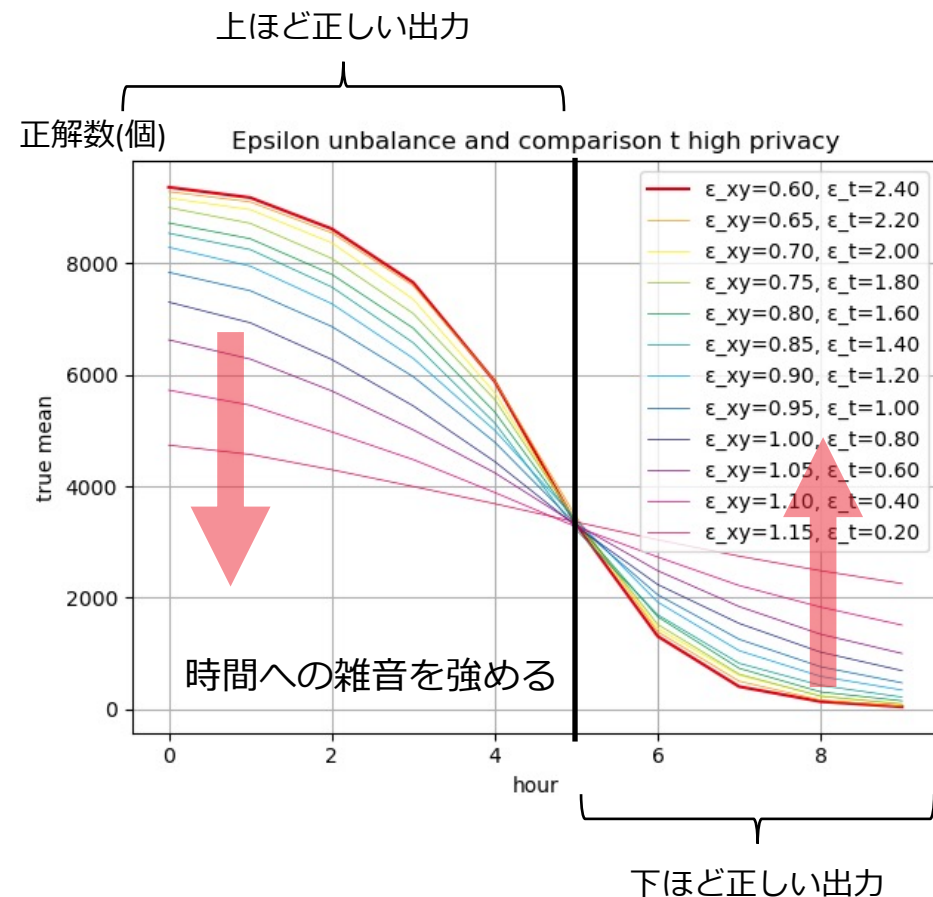
- 位置と時間へ付加する雑音の強度が出力精度に与える影響を確認
- 重み付き $F$ 値を利用して指数機構を評価

時間にのみ雑音付加した場合





# 実験1: 位置と時間へ付加する雑音の強度



左図: 雑音の総和を一定にして,  
相対的に時間への雑音を強めていった結果

## 結果

位置と時間へ付加する雑音は  
同じ強度のものが最も良い

この傾向は,  
位置への雑音を強めた場合も同様

赤いグラフ: 位置と時間に同じ強度の雑音を付加  
 $\epsilon = 1.2, (\epsilon_{xy} = 0.6, \epsilon_t = 2.4)$

## 実験2: 重み付きF値による指数機構の評価(1/2)

### 重み付きF値( $F_\beta$ 値)

適合率と再現率の重み付き調和平均

$$F_\beta = (1 + \beta^2) \cdot \frac{\text{適合率} \cdot \text{再現率}}{(\beta^2 \cdot \text{適合率}) + \text{再現率}} (\leq 1)$$

$\beta$ は適合率と比較して再現率を重視する度合い。

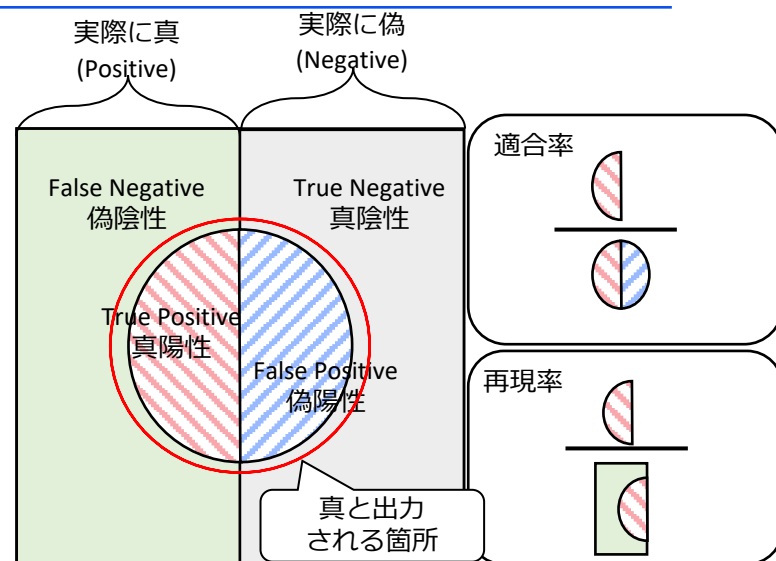
実際は「間に合わない」施設に  
「間に合う」と出力したくない

→FNを小さくしたい

→再現率を重視する(大きい $\beta$ )

$\beta$ を大きくしていくと

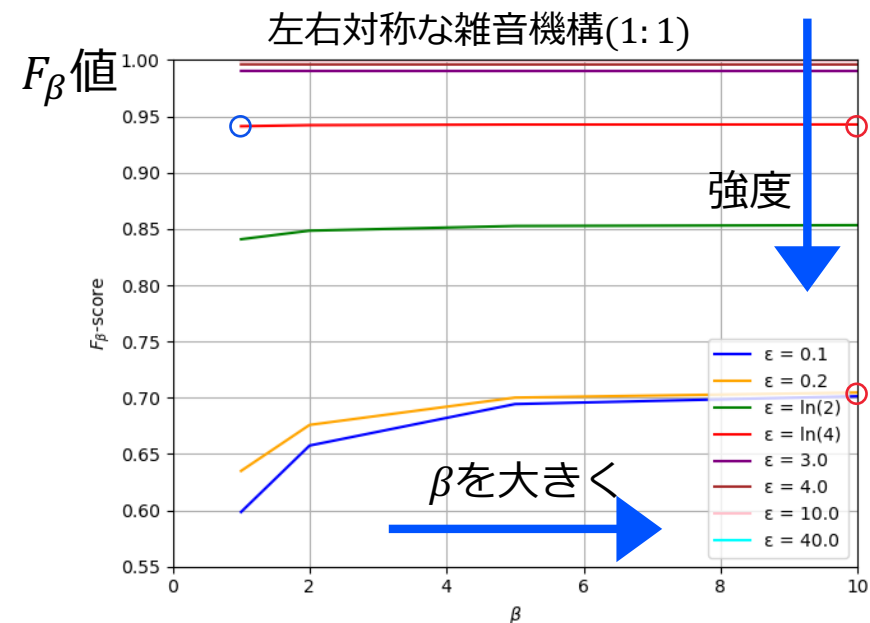
$F_\beta$ が1に近づくのが好ましい



$$\text{適合率} = \frac{TP}{TP+FP}, \quad \text{再現率} = \frac{TP}{TP+FN}$$

	実際	出力
True Positive(TP)	間に合わない	間に合わない
False Positive(FP)	間に合う	間に合わない
True Negative(TN)	間に合う	間に合う
False Negative(FN)	間に合わない	間に合う

## 実験2: 重み付き $F$ 値による指数機構の評価(2/2)

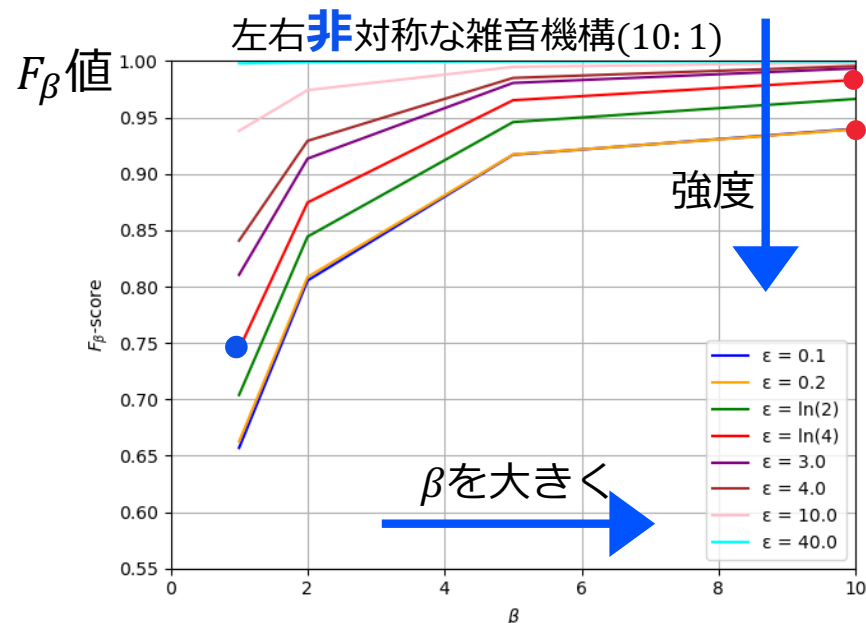


$F_\beta$ の値  
( $\epsilon = 0.2$ のとき)

	1:1	1:10
$\beta = 10$	0.71	<b>0.94</b>
$\beta = 1.0$	0.64	0.66

$F_\beta$ の値  
( $\epsilon = \ln 4$ のとき)

	1:1	1:10
$\beta = 10$	0.94	<b>0.99</b>
$\beta = 1.0$	0.94	<b>0.75</b>



- $\beta$ が大きい（再現率を重視）場合  
左右非対称なものは $F_\beta$ 値が大きい
- 一方で,  $\beta = 1.0$ の場合は  
 $\epsilon$ が大きいとき(強度小),  
左右非対称なものは $F_\beta$ 値が低い

$\varepsilon$ -STIを位置と時間の3次元で実現させる時

位置と時間のバランスをとり、

双方に同じプライバシー強度の雑音を付加することが有効だと考えられる。

指数機構の効用関数の選び方

サービスの利得劣化を抑えるために、状況に応じて時間に付加する雑音を左右非対称なものにするのが有効だと考えられる。

## ■ 研究の目的

スマートシティでの行動推薦システムにおいて  
ユーザの時空間プライバシー情報を保護する機構を作る

## ■ 研究方法

- $\epsilon$ -GIをさらに3次元に拡張した指標 $\epsilon$ -時空間識別不能性を提案する.
- 非対称な雑音機構として知られる指数機構を用いて  
 $\epsilon$ -STIを満たしプライバシー情報を保護する機構を構成する.
- 簡単なケーススタディを行い, プライバシ保護とサービス利得の  
トレードオフを評価する.

## ■ 研究成果

- 位置と時間へは同じ強度のプライバシーを実現するのが良い.
- 実際に「間に合わない」施設へ「間に合う」と出力されることを避ける  
(サービス利得劣化を防ぐ) ためには, 左右非対称の雑音を時間へ付加  
するのが良い.




# 今後の課題

---

1. 位置情報も非対称であるとした場合への拡張
2. プライバシ保護強度 $\epsilon$ の値の適切な値の調査
3. 行動推薦システムとして機能させるための,  
実際の公共交通機関などを利用した場合の経路曖昧化<sup>[ASY18]</sup>への応用

[ASY18]浅田真帆, 曹洋, 吉川正俊. Geo 識別不能性を用いた経路端点の曖昧化. 日本データベース学会和文論文誌, Vol. 16-J, p. 19, 2018





---

Q.  $\varepsilon$ の値をいくつにすれば十分安全と言えるのか？

$\varepsilon$ はプライバシー強度を表すという前提，それ以上は具体的な応用場面次第  
研究室のM2の先輩がゲーム理論で，問題を解決する研究を行っている

Q. 雑音が強すぎて使い物にならないのではないのか？

本研究「与えられた $\varepsilon$ に対して $\varepsilon$ -STIを満たす→プライバシー保護される」

ある意味でどのような攻撃も想定内であるため，

雑音が強すぎて可用性が低いという事実がある

→F値等でどの程度使い物にならないのかを数値評価してみようという動機  
づけになった

Q. 位置情報にも非対称な雑音をかけるべきではないか？

2次元以上のデータにどのように指数機構を適用するのか検討が必要である  
実現できれば，プライバシーと利得との高いトレードオフが得られる





---

Q. どんな雑音機構を使っているかは攻撃者は既知か？

既知.

指数機構においては偏りが利用されることも含めてパラメータ $\varepsilon$ で強度を調整する

Q. 実装において数値計算の誤差を考慮しているか？

今回はしていない

先行研究( $\varepsilon$ -GI)では詳細な数値計算誤差解析と補正を行っているので参考にして改良したい

Q. シナリオが単純なので機構のPDFから解析的に利得を計算できないか？

今後複雑なシナリオで評価する場合の準備という意味もあって数値でシミュレーションで評価した

安本研究所の行動推薦システム(奈良県の観光地)を利用させていただいて、より実用的なデータで実験を行いたい

## 補足1: 指数機構の定義

( $\mathbb{D}$  : 実データ値の集合,  $\mathbb{O}$  : 観測値の集合)

効用関数  $u : \mathbb{D} \times \mathbb{O} \rightarrow \mathbb{R}$

$u(x, z)$  は, 実データ  $x \in \mathbb{D}$  に対して  $z \in \mathbb{O}$  が観測される望ましさを表す

定義  $u$  を効用関数とする. 指数機構  $\mathcal{M}_E(\varepsilon, u, \mathbb{O})$  は, データ値  $x$  に対して

$e^{\frac{\varepsilon u(x, r)}{2\Delta u}}$  に比例する確率で要素  $r \in \mathbb{O}$  を選択して出力する.

ここで  $\Delta u$  は効用関数の感度 (効用関数の最大変化率)

性質 指数機構  $\mathcal{M}_E(\varepsilon, u, \mathbb{O})$  は  $\varepsilon$ -DP を満たす [MT07].

$$\Delta u \equiv \max_{r \in \mathcal{R}} \max_{x, y: \|x - y\|_1 \leq 1} |u(x, r) - u(y, r)|$$

効用関数の決定方法には明確な指針が存在しない

→ 本研究ではシナリオに合わせてどのようなものが適当であるかを検証した

[MT07] F. McSherry, K. Talwar, Mechanism design via differential privacy, FOCS 2007.

## 補足2: 指数機構の効用関数の例(1/2)

実際の時刻を $t(=0)$ , 雑音付加後の時刻を $t'$ として効用関数 $u(t, t')$ を次のように定める.

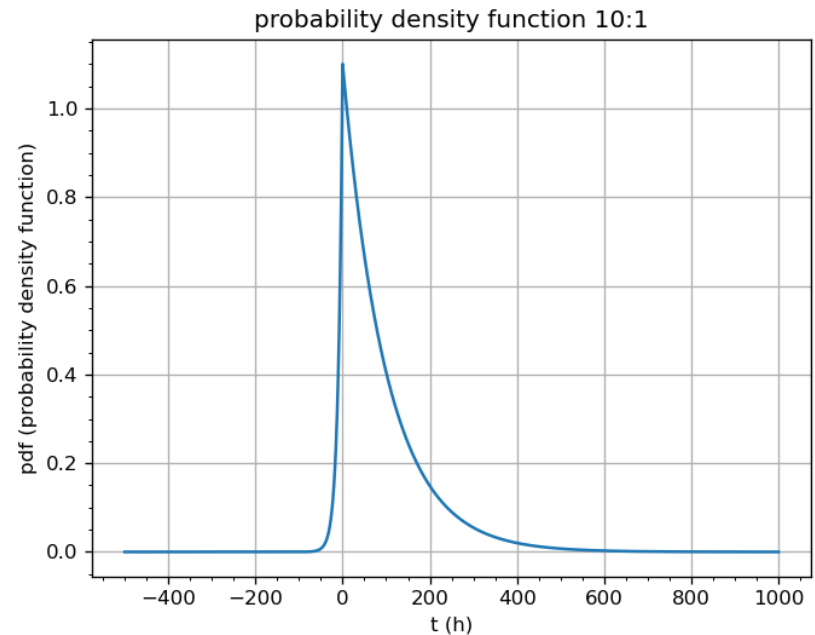
$$u(0, t') = \begin{cases} 10t' & (t' \leq 0) \\ -t' & (t' > 0) \end{cases}$$

ここで $\Delta u = 10$ である.

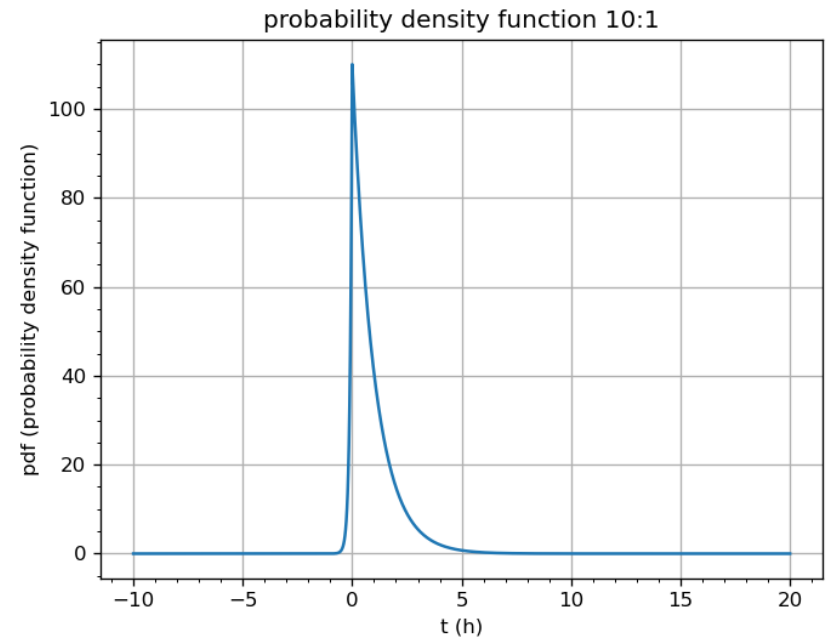
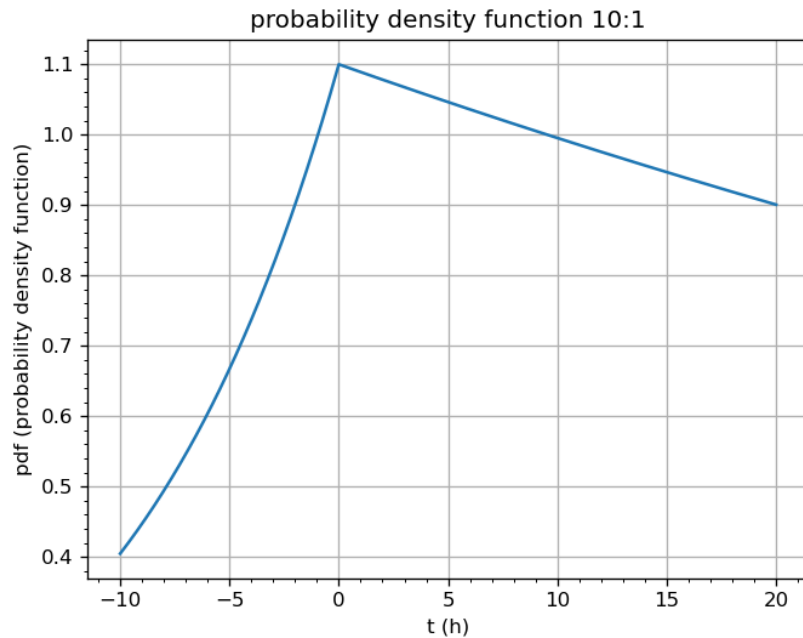
よって指数機構の確率密度関数(pdf) は次のようになる.

$$pdf = \begin{cases} \frac{\varepsilon}{22} e^{\frac{\varepsilon}{2} t'} & (t' \leq 0) \\ \frac{\varepsilon}{22} e^{-\frac{\varepsilon}{22} t'} & (t' > 0) \end{cases}$$

右図は $\varepsilon = 0.2$ としたときのpdfの様子である.



## 補足2: 指数機構の効用関数の例(2/2)



$\varepsilon$ でコントロールできる

効用関数の傾きの比はどちらも10 : 1

左側が $\varepsilon = 0.2$

右側が $\varepsilon = 20$

## 補足3: 複数回のクエリについて

### $\varepsilon$ -DPの合成定理<sup>[DR14]</sup> (再掲)

それぞれ $\varepsilon_i$ -DPを満たす $n$ 個の問い合わせ $Q_i$ がある( $i \in [n]$ ).  
任意のデータベース $D$ に対する $n$ 個の問い合わせは,  
 $Q = (Q_1(D), Q_2(D), \dots, Q_n(D))$ となり, これは $\sum_{i=1}^n \varepsilon_i$ -DPを満たす

クエリを複数回行う (または繰り返す) ことで  
プライバシー強度は弱まって行くことは避けられない.

( $\varepsilon$ の値は大きくなって行くため.  $\varepsilon = \infty$ ではプライバシーが保護されない)

## 補足4: $\varepsilon$ -地理的識別不能性( $\varepsilon$ -geo indistinguishability, $\varepsilon$ -GI)

定義: 機構  $K: \mathbb{R}^2 \rightarrow D(\mathbb{R}^2)$  が任意の2点  $x, x' \in \mathbb{R}^2$  に対して,

$$d_{\mathcal{P}}(K(x), K(x')) \leq \varepsilon d(x, x')$$

を満たすとき,  $K$  は  $\varepsilon$ -GI を満たすという

- 機構  $K$ : 与えられた位置  $x \in \mathbb{R}^2$  に対して位置の確率密度を返す関数
- $\varepsilon (\geq 0)$ : プライバシ保護強度 ( $\varepsilon$  が小さいほど強い)
- $d(x, x')$ :  $x$  と  $x'$  の3次元ユークリッド距離
- $d_{\mathcal{P}}(\sigma_1, \sigma_2)$ : 確率分布  $\sigma_1$  と  $\sigma_2$  のある種の距離

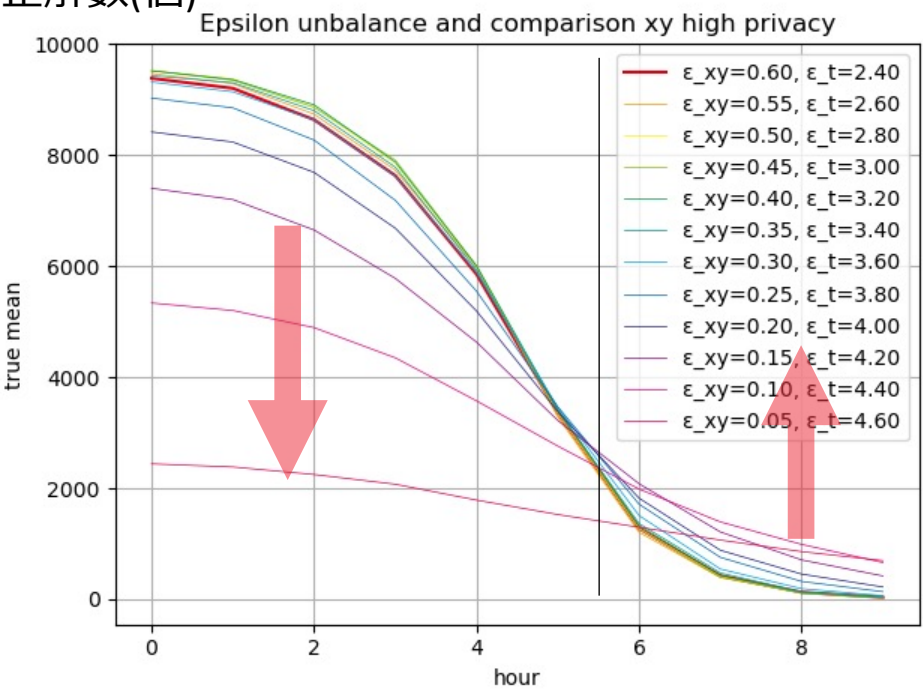
ユーザが位置  $x$  に  $\pi(x)$  の確率で存在すると攻撃者が知っている時  $\pi(x)$  が一様分布であれば,  $\varepsilon$ -STI の定義は以下と等価になる.

任意の2点  $x, x' \in \mathbb{R}^3, Z \subseteq \mathbb{R}^3$  に対して,

$$\ln \frac{K(x)(Z)}{K(x')(Z)} \leq \varepsilon d(x, x')$$

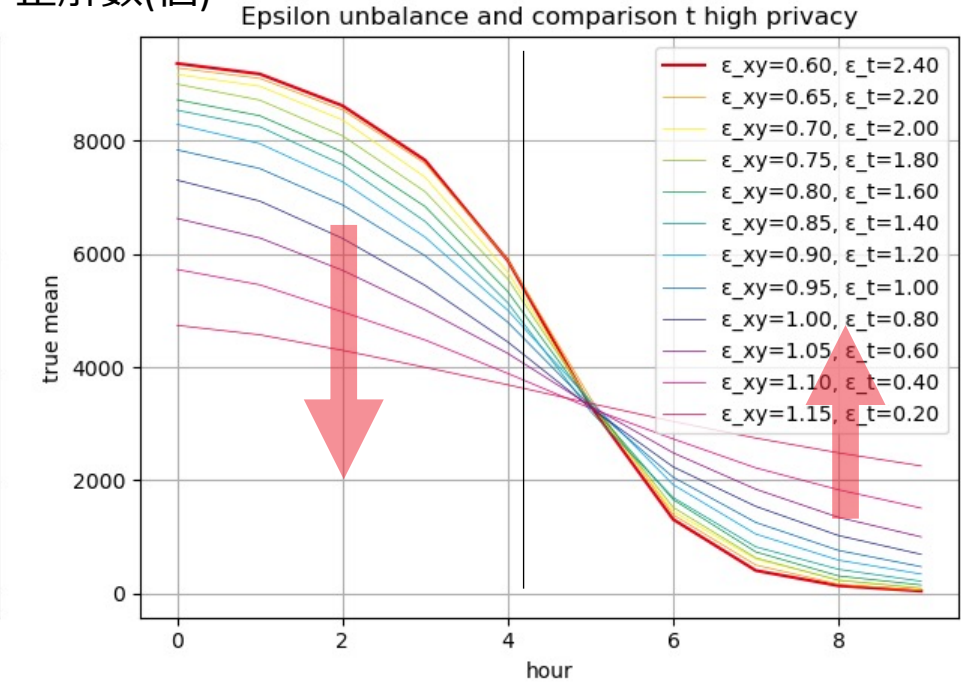
# 補足5: 実験結果の詳細 雑音付加バランス

正解数(個)



位置への雑音を強める

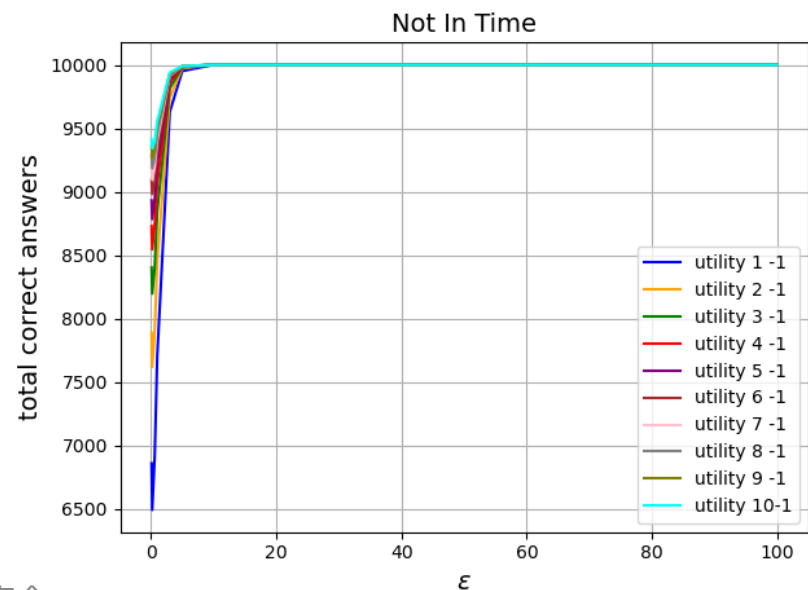
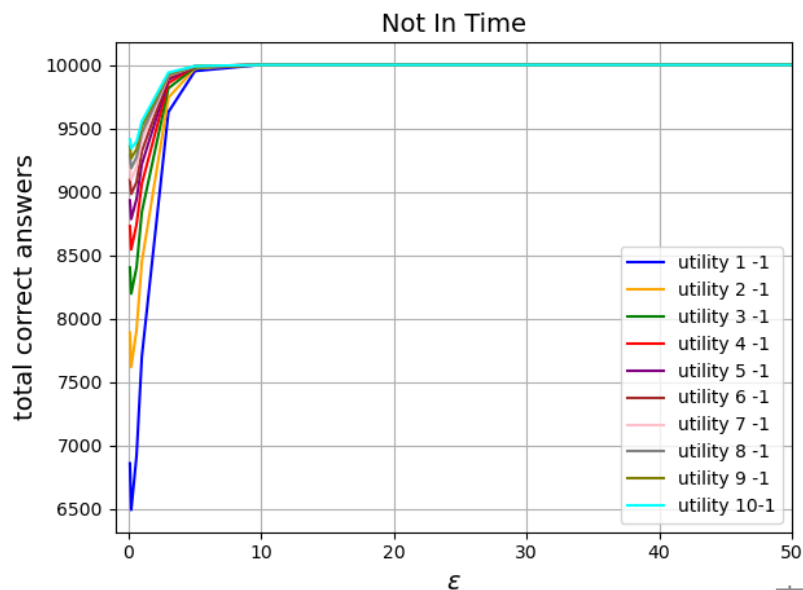
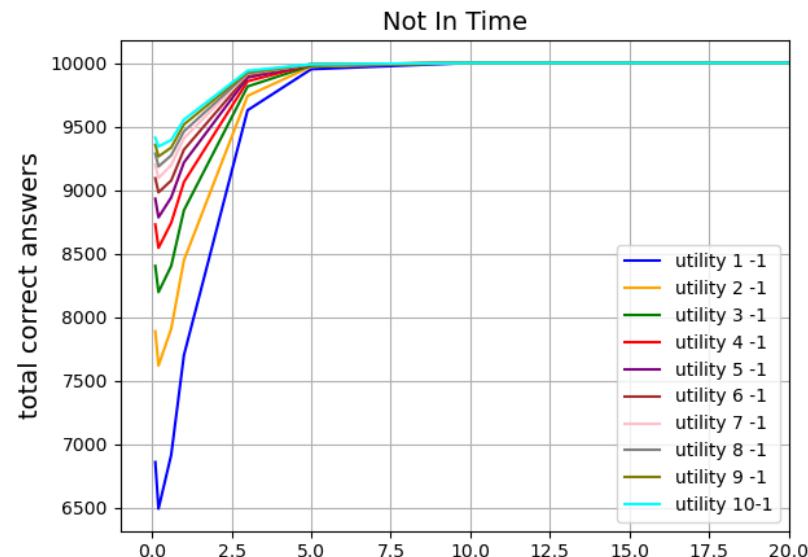
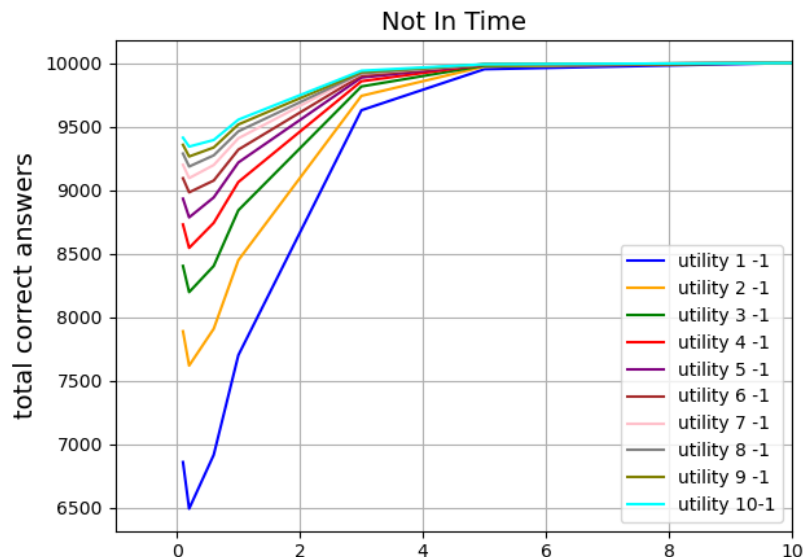
正解数(個)



時刻への雑音を強める



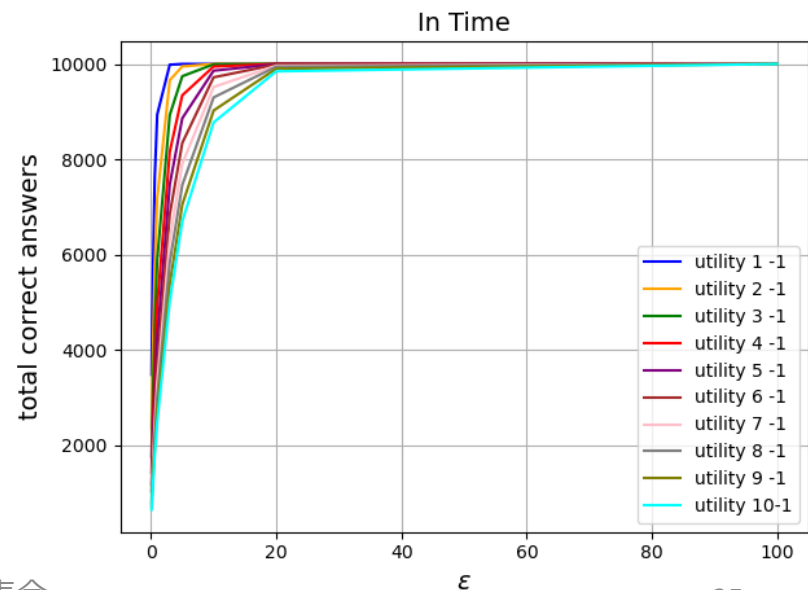
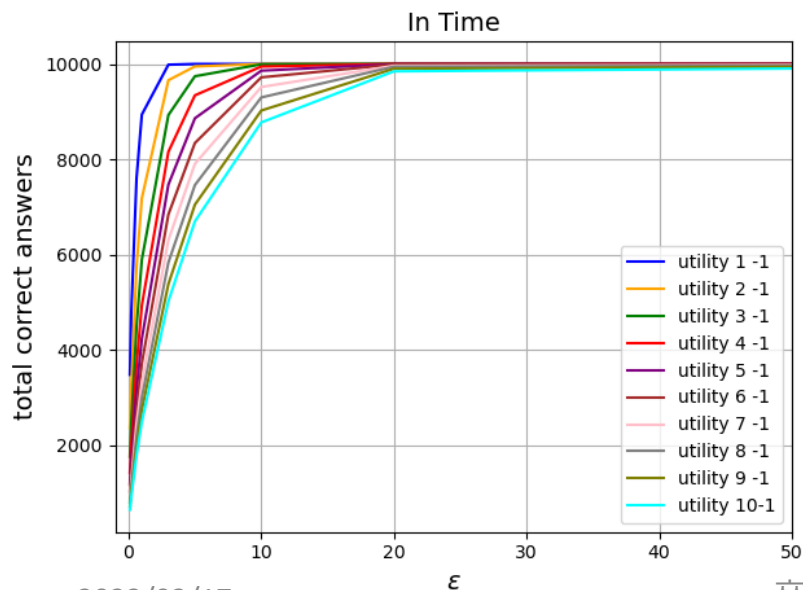
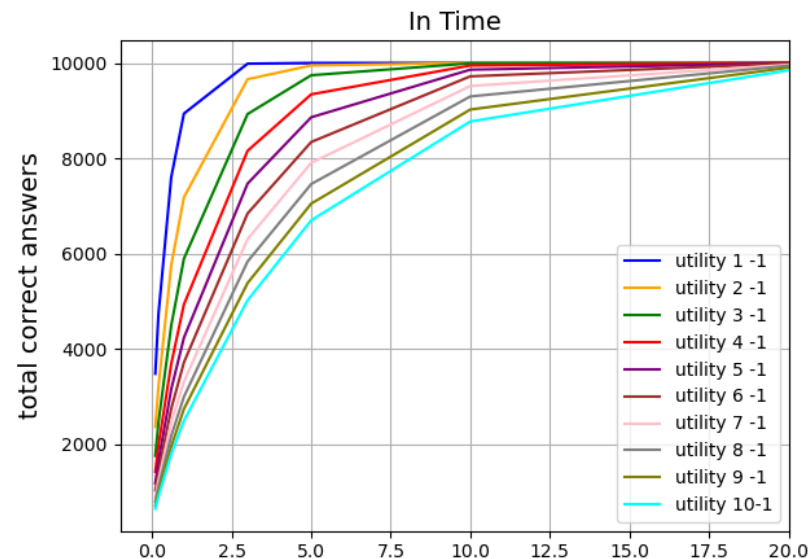
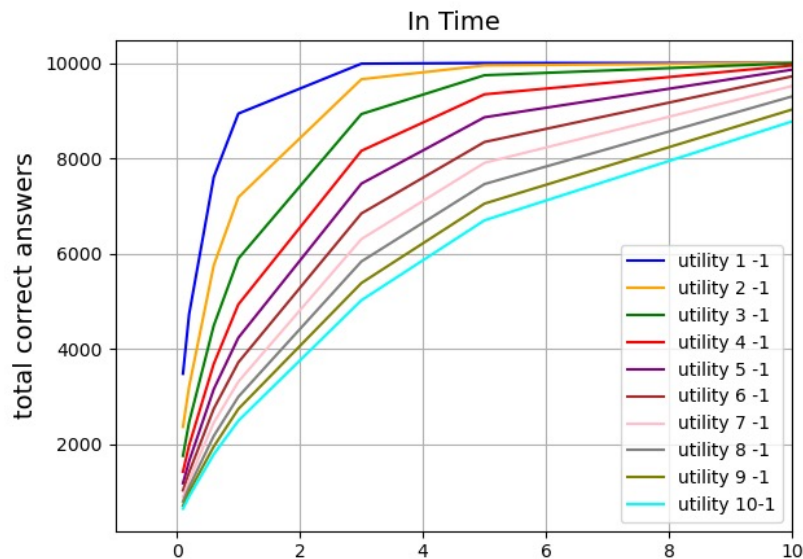
## 補足6: 実験結果の詳細 効用関数と出力精度 Not In Time







## 補足7: 実験結果の詳細 効用関数と出力精度 In Time



## 補足8: 効用関数と出力精度 (表)

	(4, 0, 17)	(8, 0, 17)	(12, 0, 17)	(16, 0, 17)
$\varepsilon = 0.1$	(3559, 6441)	(3518, 6482)	(3460, 6540)	(3361, 6639)
$\varepsilon = 0.2$	(5185, 4815)	(5002, 4998)	(4733, 5267)	(4342, 5658)
$\varepsilon = \ln(2)$	(9275, 725)	(8804, 1196)	(7969, 2031)	(6640, 3360)
$\varepsilon = \ln(4)$	(9963, 37)	(9858, 142)	(9490, 510)	(8145, 1855)
$\varepsilon = 3.0$	(10000, 0)	(10000, 0)	(9985, 15)	(9624, 376)
$\varepsilon = 4.0$	(10000, 0)	(10000, 0)	(9998, 2)	(9857, 143)
$\varepsilon = 10$	(10000, 0)	(10000, 0)	(10000, 0)	(10000, 0)
$\varepsilon = 40$	(10000, 0)	(10000, 0)	(10000, 0)	(10000, 0)

	(24, 0, 17)	(28, 0, 17)	(32, 0, 17)	(36, 0, 17)
$\varepsilon = 0.1$	(3119, 6881)	(2992, 7008)	(2860, 7140)	(2713, 7287)
$\varepsilon = 0.2$	(3513, 6487)	(3109, 6891)	(2696, 7304)	(2318, 7682)
$\varepsilon = \ln(2)$	(2874, 7126)	(1579, 8421)	(819, 9181)	(436, 9564)
$\varepsilon = \ln(4)$	(1652, 8348)	(446, 9554)	(122, 9878)	(24, 9976)
$\varepsilon = 3.0$	(373, 9627)	(17, 9983)	(0, 10000)	(0, 10000)
$\varepsilon = 4.0$	(144, 9856)	(1, 9999)	(0, 10000)	(0, 10000)
$\varepsilon = 10$	(0, 10000)	(0, 10000)	(0, 10000)	(0, 10000)
$\varepsilon = 40$	(0, 10000)	(0, 10000)	(0, 10000)	(0, 10000)

効用関数の傾きの比 1:1

	(4, 0, 17)	(8, 0, 17)	(12, 0, 17)	(16, 0, 17)
$\varepsilon = 0.1$	(659, 9341)	(658, 9342)	(645, 9355)	(629, 9371)
$\varepsilon = 0.2$	(984, 9016)	(938, 9062)	(891, 9109)	(811, 9189)
$\varepsilon = \ln(2)$	(2764, 7236)	(2404, 7596)	(1922, 8078)	(1393, 8607)
$\varepsilon = \ln(4)$	(4642, 5358)	(3950, 6050)	(3052, 6948)	(2020, 7980)
$\varepsilon = 3.0$	(7287, 2713)	(6344, 3656)	(5006, 4994)	(3217, 6783)
$\varepsilon = 4.0$	(8230, 1770)	(7314, 2686)	(5950, 4050)	(3937, 6063)
$\varepsilon = 10$	(9850, 150)	(9548, 452)	(8808, 1192)	(6704, 3296)
$\varepsilon = 40$	(10000, 0)	(10000, 0)	(9999, 1)	(9850, 150)

	(24, 0, 17)	(28, 0, 17)	(32, 0, 17)	(36, 0, 17)
$\varepsilon = 0.1$	(571, 9429)	(541, 9459)	(513, 9487)	(487, 9513)
$\varepsilon = 0.2$	(644, 9356)	(567, 9433)	(494, 9506)	(412, 9588)
$\varepsilon = \ln(2)$	(519, 9481)	(290, 9710)	(149, 9851)	(78, 9922)
$\varepsilon = \ln(4)$	(298, 9702)	(80, 9920)	(13, 9987)	(4, 9996)
$\varepsilon = 3.0$	(66, 9934)	(4, 9996)	(0, 10000)	(0, 10000)
$\varepsilon = 4.0$	(20, 9980)	(0, 10000)	(0, 10000)	(0, 10000)
$\varepsilon = 10$	(0, 10000)	(0, 10000)	(0, 10000)	(0, 10000)
$\varepsilon = 40$	(0, 10000)	(0, 10000)	(0, 10000)	(0, 10000)

効用関数の傾きの比 10:1



## 補足9: $F_\beta$ 値 (1/2)

	$\varepsilon = 0.1$	$\varepsilon = 0.2$	$\varepsilon = \ln(2)$	$\varepsilon = \ln(4)$	$\varepsilon = 3.0$	$\varepsilon = 4.0$	$\varepsilon = 10.0$	$\varepsilon = 40.0$
$\beta = 1.0$	0.599801	0.636664	0.840449	0.940374	0.990238	0.996375	1.0	1.0
$\beta = 2.0$	0.660299	0.678234	0.850479	0.942486	0.990245	0.996375	1.0	1.0
$\beta = 5.0$	0.698220	0.702948	0.855980	0.943628	0.990249	0.996375	1.0	1.0
$\beta = 10.0$	0.705383	0.707506	0.856960	0.943830	0.990250	0.996375	1.0	1.0
$\beta = 100.0$	0.707874	0.709084	0.857297	0.943899	0.990250	0.996375	1.0	1.0

表 4.5: 効用関数の傾きの比 1:1 の  $F_\beta$  値

	$\varepsilon = 0.1$	$\varepsilon = 0.2$	$\varepsilon = \ln(2)$	$\varepsilon = \ln(4)$	$\varepsilon = 3.0$	$\varepsilon = 4.0$	$\varepsilon = 10.0$	$\varepsilon = 40.0$
$\beta = 1.0$	0.657224	0.663108	0.705352	0.747680	0.814266	0.845699	0.940181	0.998116
$\beta = 2.0$	0.805110	0.808571	0.845276	0.876446	0.915507	0.931722	0.975182	0.999246
$\beta = 5.0$	0.916108	0.916872	0.946363	0.966029	0.981196	0.985710	0.995130	0.999855
$\beta = 10.0$	0.938996	0.939111	0.966806	0.983808	0.993803	0.995913	0.998742	0.999963
$\beta = 100.0$	0.947116	0.946994	0.974026	0.990061	0.998205	0.999464	0.999987	1.000000

表 4.8: 効用関数の傾きの比 10:1 の  $F_\beta$  値

## 補足9: $F_\beta$ 値 (2/2) – 条件を厳しくした状態

	$\varepsilon = 0.1$	$\varepsilon = 0.2$	$\varepsilon = \ln(2)$	$\varepsilon = \ln(4)$	$\varepsilon = 3.0$	$\varepsilon = 4.0$	$\varepsilon = 10.0$	$\varepsilon = 40.0$
$\beta = 1.0$	0.579441	0.569818	0.621458	0.711678	0.842013	0.886062	0.972568	0.999842
$\beta = 2.0$	0.635212	0.604463	0.631455	0.716658	0.843334	0.886854	0.972417	0.999817
$\beta = 5.0$	0.669933	0.624923	0.636972	0.719368	0.844047	0.887282	0.972336	0.999803
$\beta = 10.0$	0.676470	0.628685	0.637958	0.719850	0.844173	0.887357	0.972322	0.999801
$\beta = 100.0$	0.678743	0.629987	0.638297	0.720015	0.844216	0.887383	0.972317	0.999800

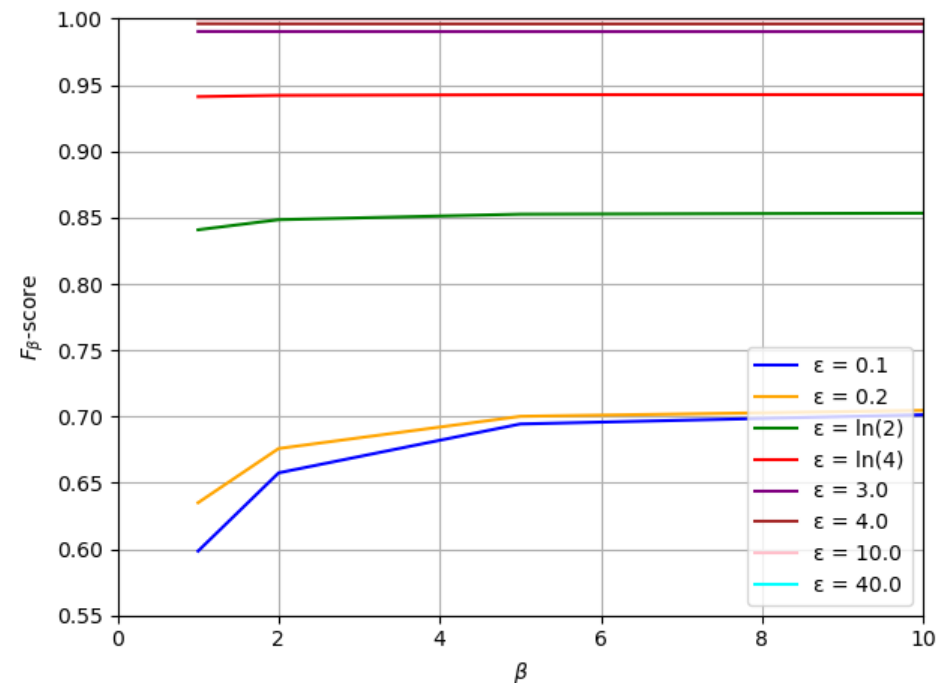
表 4.9: 効用関数の傾きの比 1:1 の  $F_\beta$  値

	$\varepsilon = 0.1$	$\varepsilon = 0.2$	$\varepsilon = \ln(2)$	$\varepsilon = \ln(4)$	$\varepsilon = 3.0$	$\varepsilon = 4.0$	$\varepsilon = 10.0$	$\varepsilon = 40.0$
$\beta = 1.0$	0.652712	0.652160	0.661946	0.678038	0.707791	0.722644	0.786523	0.925989
$\beta = 2.0$	0.798332	0.793854	0.799424	0.815883	0.844562	0.856937	0.899536	0.969011
$\beta = 5.0$	0.907330	0.899032	0.900082	0.916177	0.942644	0.952222	0.974970	0.993874
$\beta = 10.0$	0.929775	0.920597	0.920576	0.936531	0.962405	0.971317	0.989643	0.998404
$\beta = 100.0$	0.937735	0.928238	0.927825	0.943726	0.969378	0.978048	0.994781	0.999967

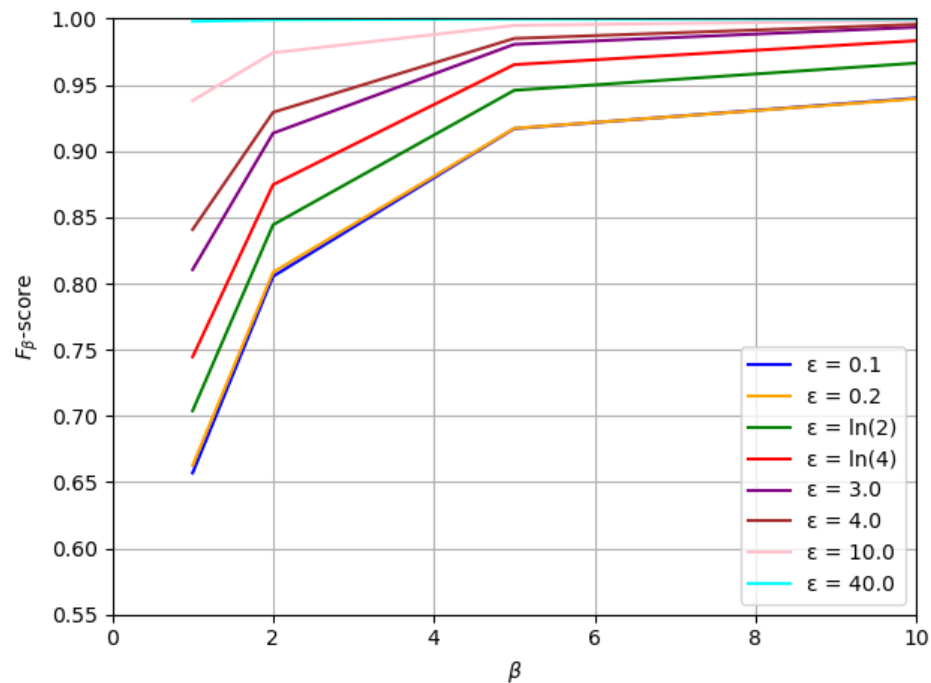
表 4.10: 効用関数の傾きの比 10:1 の  $F_\beta$  値



## 補足10: $F_\beta$ 値(グラフ) (1/2)



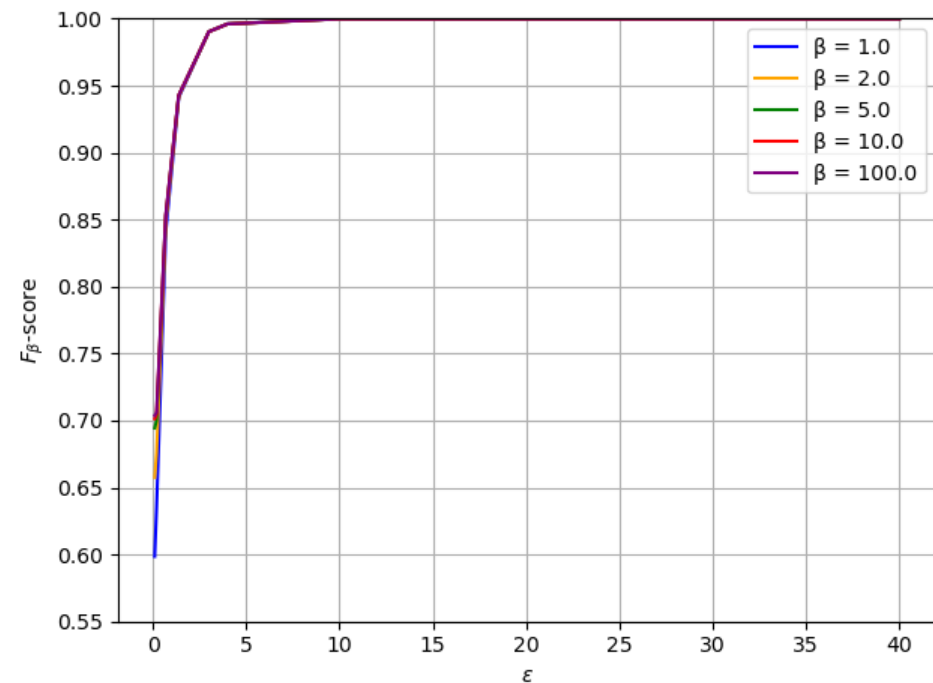
効用関数の傾きの比1:1



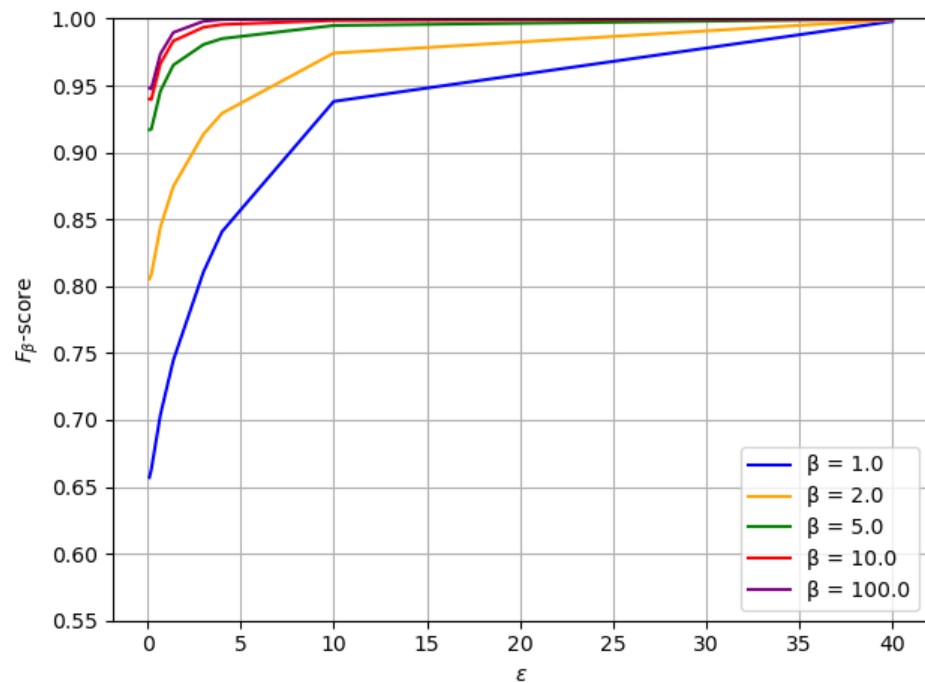
効用関数の傾きの比10:1



## 補足10: $F_\beta$ 値(グラフ) (2/2)

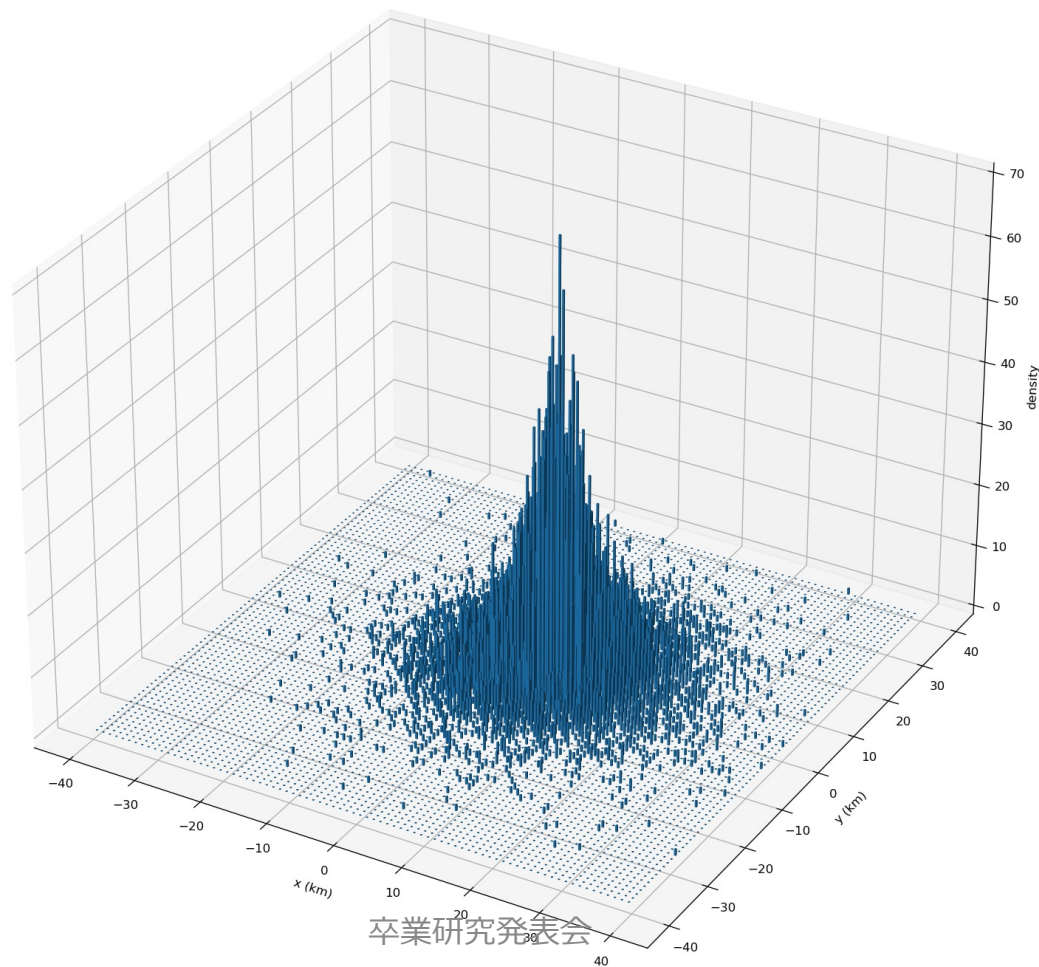


効用関数の傾きの比1:1



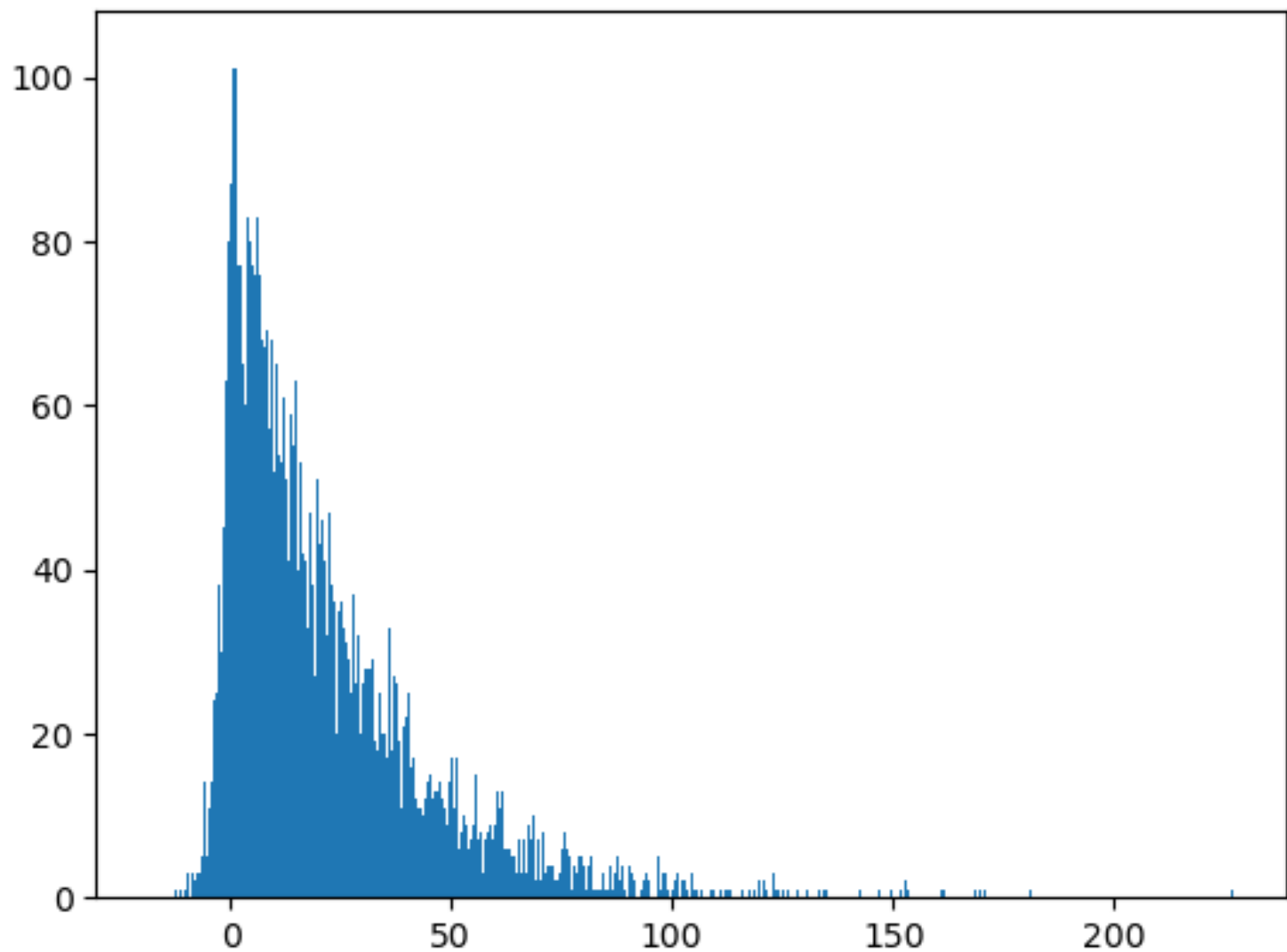
効用関数の傾きの比10:1

# 補足11: 平面ラプラス分布の実装



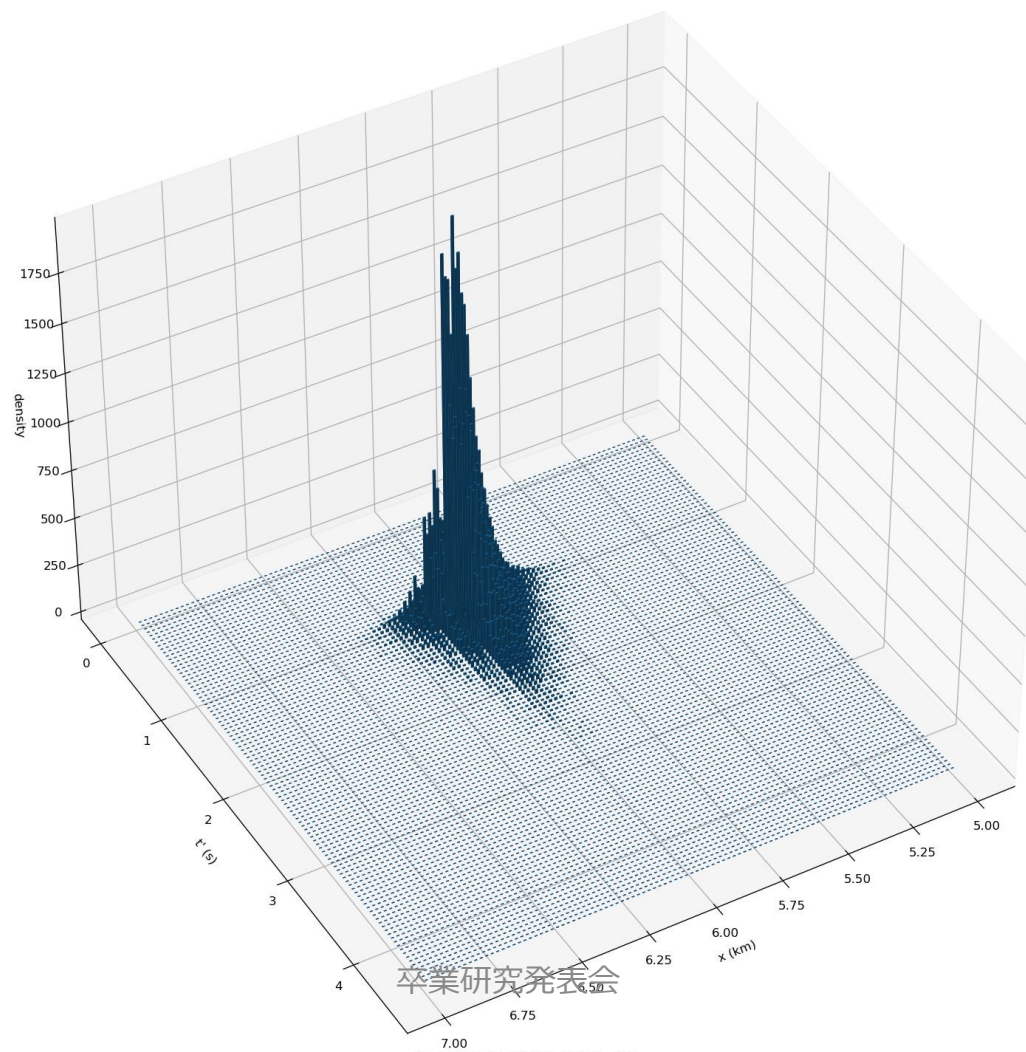


## 補足11': 指数機構の実装





## 補足12: $PL - EX$ 機構の実装 ( $x, t$ )



## 補足13: 実装したアルゴリズム

入力 :  $(x, y, t)$ ...実際のユーザの位置情報 /  $\varepsilon$ ...プライバシー強度の変数

出力 :  $(x', y', t')$ ...雑音が付加された位置情報

1.  $[0: 2\pi)$ の範囲で一様分布にしたがった $\theta$ を出力
2.  $[0: 1)$ の範囲で一様分布にしたがった $p_{xy}$ を出力※.  
機構にしたがって $r$ を作る
3.  $(x', y')$ に $(x, y) + \langle r\cos(\theta), r\sin(\theta) \rangle$ を代入する
4.  $[0: 1)$ の範囲で一様分布にしたがった $p_t$ を出力.  
機構にしたがって $T$ を作る
5.  $t'$ に $t + T$ を代入する
6.  $(x', y', t')$ を返す

※[ABCP13]の論文のうち, 単純な平面ラプラスノイズの付加機構を活用

[ABCP13] M. E. Andres, N. E. Bordenabe, K. Chatzikokolakis and C. Palamidessi, Geo-indistinguishability: Differential privacy for location-based systems, ACM CCS 2013.

## 補足14: 実験の準備

2つの機構を合成するためには、 $\varepsilon$ の単位の整合性を取る必要があり  
 $\varepsilon$ はその雑音を付加する対象の次元の逆の次元をもつ<sup>[ABCP13]</sup>.  
そのため、本研究ではユーザの移動速度( $v$  km/h)を利用して以下に示す.

### $\varepsilon$ の制約

$$\varepsilon = \varepsilon_{xy} + \varepsilon_t / v = \text{一定}$$

### 結果の取得方法

一様乱数値を10,000個用意して真の時空間情報にPL-EX機構を適用する.  
その後、各地点に対して到達できるかどうかを  
雑音付加された10,000個の点に対して行う.

これを各地点に対して100回ずつ行い、結果の平均を出力値とする.