データ利活用のための
プライバシー保護技術

統計数理研究所
南 和宏

2024年5月24日

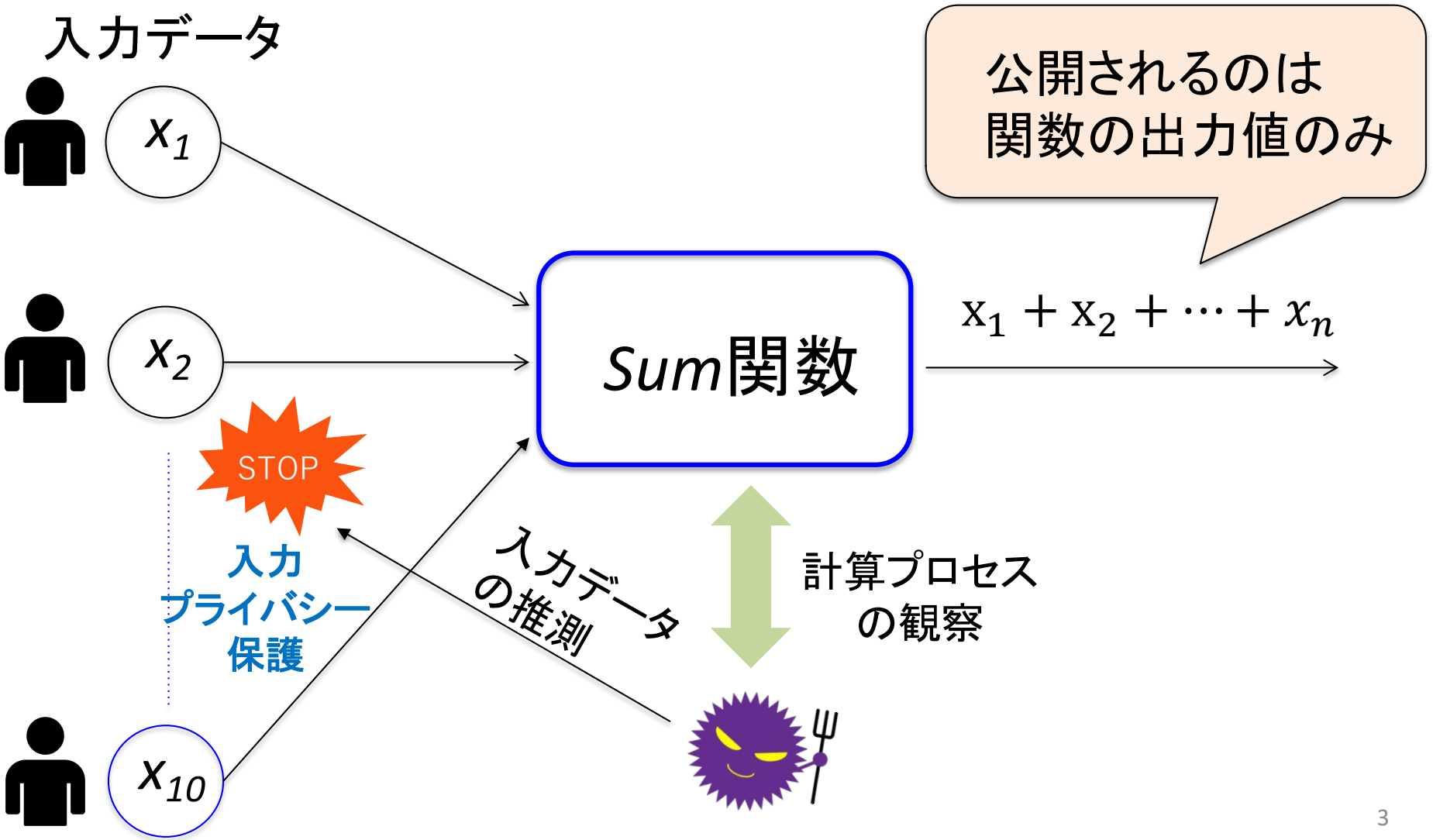
統計数理研究所オープンハウス2024公開講演会

本日の内容

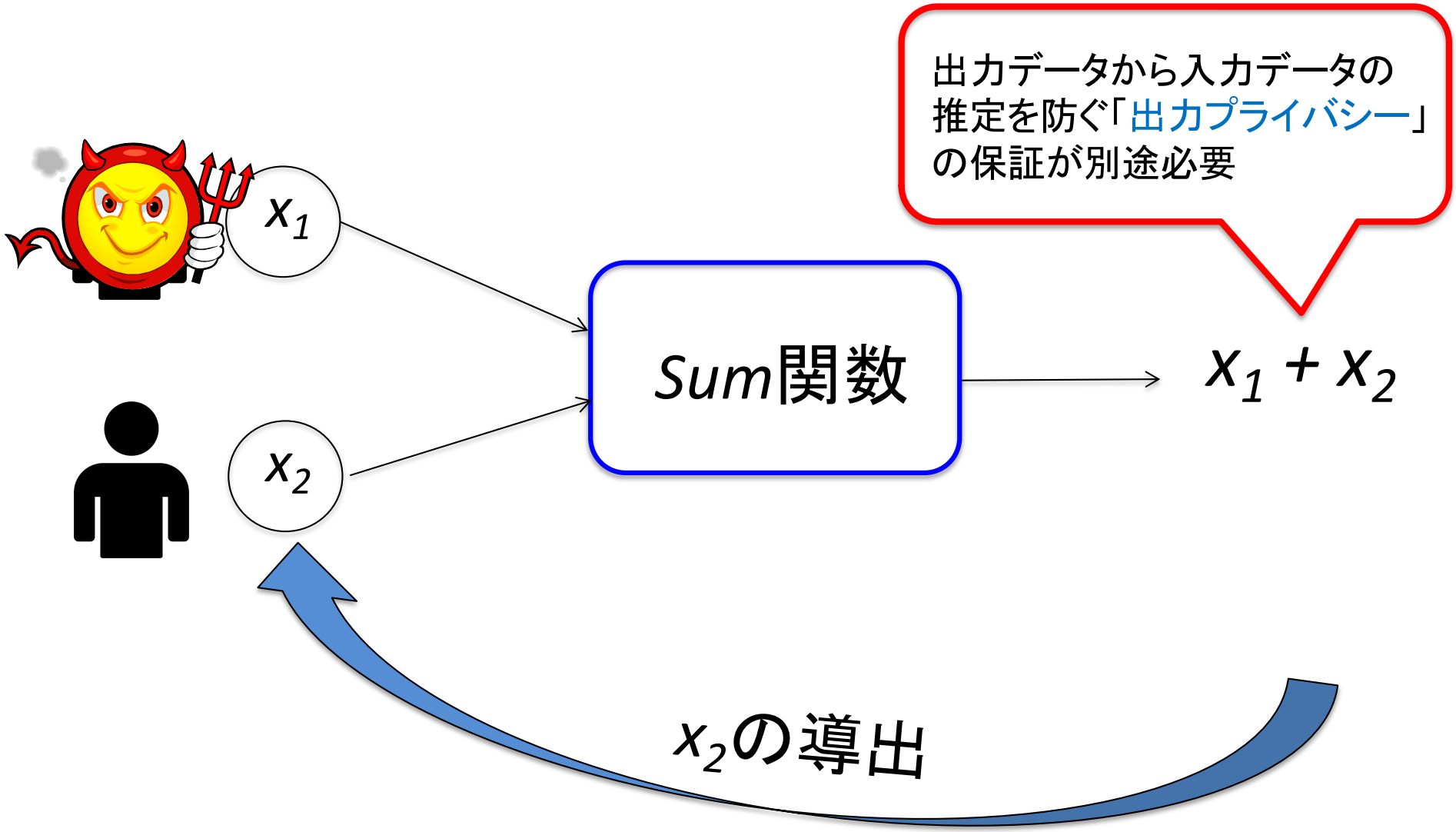
- データ利活用における出力プライバシー
- 統計開示抑制と安全性ルール
- 統計表の表セル秘匿処理とマッチング攻撃
- 今後の方向性

秘密計算による入力プライバシー保護

- 入力データの機密性を保証しつつ関数$f(x)$を計算



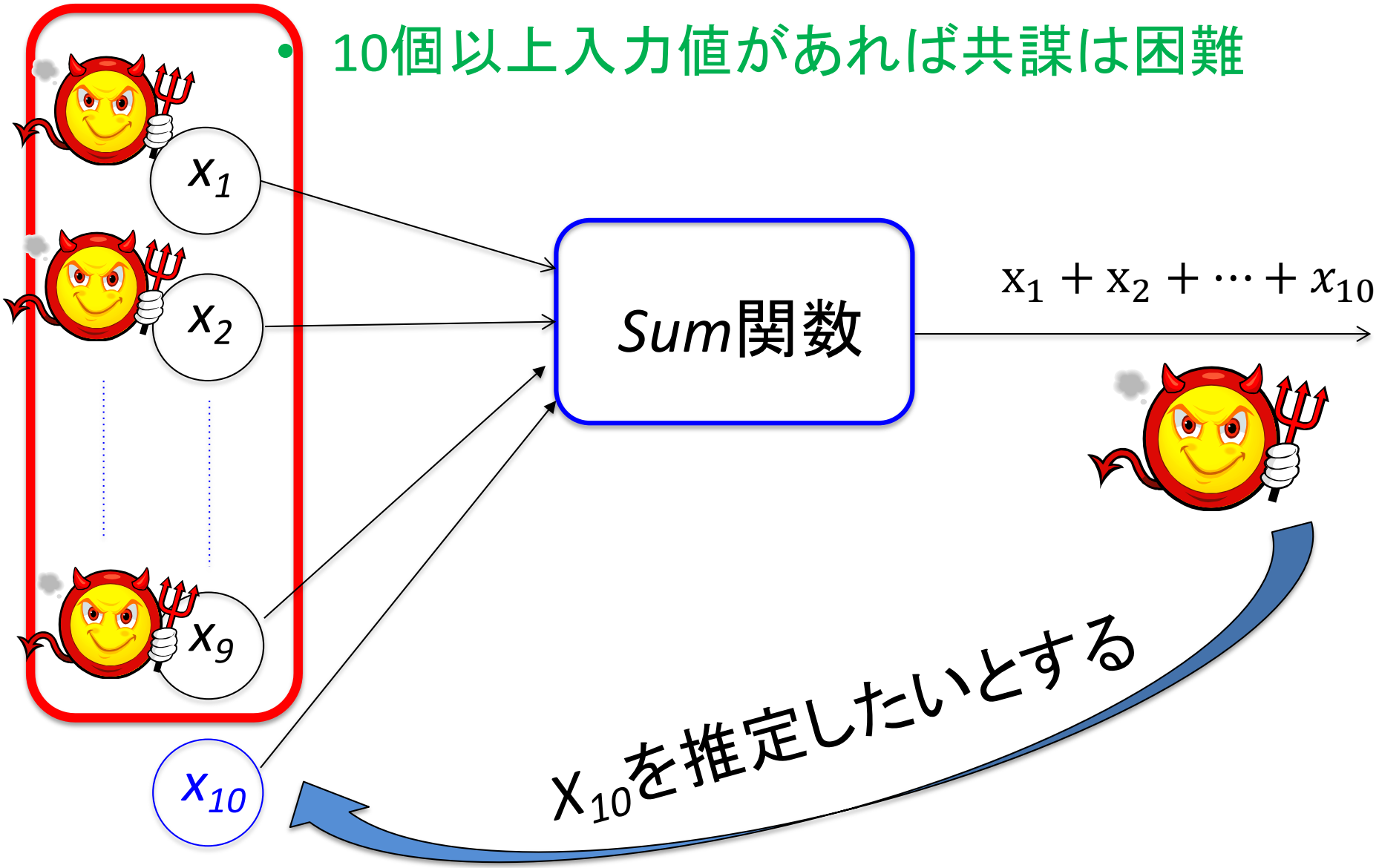
もしデータ提供者が二人だったら。。



統計開示制御 (Statistical Disclosure Control) による出力プライバシー保護

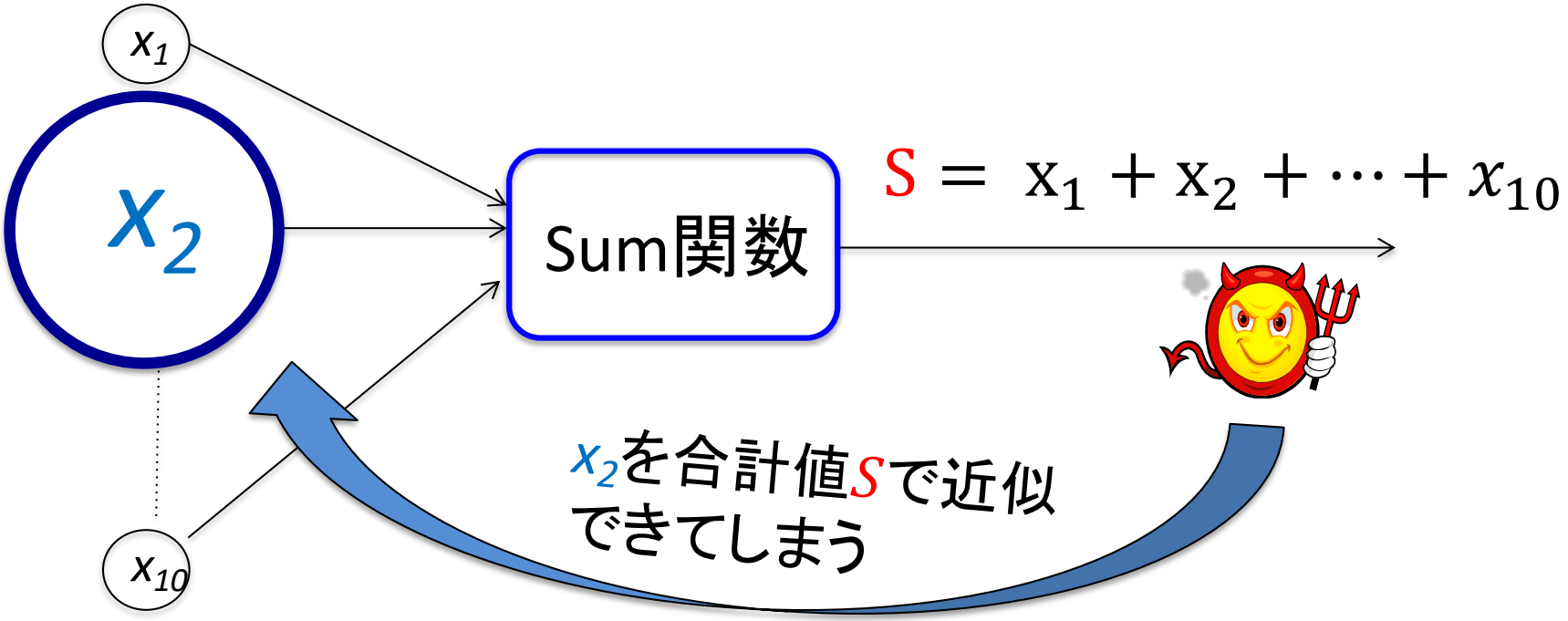
- 統計量の開示から入力データが推定されるリスクを抑制する方法論
- 公開するデータを修正、削除することで、統計開示のリスクを減少させる
- しかし公開するデータをあまり劣化させると、データが活用できない
  - 一般には機密情報の保護を拘束条件として、情報の有用性の最大化を目指す最適化問題として定式化される

客体10の原則


９人の共謀
が必要
10個以上入力値があれば共謀は困難
x_1
x_2
x_9
x_{10}
Sum関数
$x_1 + x_2 + \cdots + x_{10}$
x_{10}を推定したいとする

占有性の原則

- 入力データが多数あっても、一つの入力値が突出しておおきくてはいけない（例：70%以上）



統計表の統計開示抑制

- 統計表は最も基本的な記述統計
- 国が行う公的調査から多くの統計表が一般に公開されている
- 表の各セル値に
  - 最小度数ルール
  - 占有性ルール

  を適用し、安全性を確認

外部者による攻撃

度数分布表

職種

地域	P_1	P_2	P_3	P_4	P_5	合計
M_1	20	15	30	20	10	95
M_2	72	20	1	30	10	133
M_3	38	38	15	40	2	133
合計	130	73	46	90	22	361

集計表

	P_1	P_2	P_3	P_4	P_5	合計
M_1	360	450	720	400	360	2290
M_2	1440	540	22	570	320	2892
M_3	722	1178	375	800	363	3438
合計	2522	2168	1117	1770	1043	8620

収入の合計

内部者(調査対象者)による攻撃

度数分布表

職種

地域	P_1	P_2	P_3	P_4		
M_1	20	15	30	20		
M_2	72	20	1	30	10	133
M_3	38	38	15	40	2	133
合計	130	73	46	90	22	361

自分の属性は知っている

自分の収入を引けば
もう一人の収入が分かる

集計表

					P_5	合計
M_1	360	450	720	900	360	2290
M_2	1440	540	22	570	320	2892
M_3	722	1178	375	800	363	3438
合計	2522	2168	1117	1770	1043	8620

収入の合計

行計、列計の関係式から値が復元されてしまうのを防ぐためには2次秘匿が必要

集計表

	P_1	P_2	P_3	合計
M_1	20	24	28	72
M_2	38	38	40	116
M_3	40	39	42	121
合計	98	101	110	309

1次秘匿

NA (Not Available)

	P_1	P_2	P_3	合計
M_1	20	24	28	72
M_2	38	38	NA	116
M_3	40	39	42	121
合計	98	101	110	309

表の各セルに[illegible]小度数ルール、[illegible]適用

占有性ルールを侵害

2次秘匿

	P_1	P_2	P_3	合計
M_1	NA	24	NA	72
M_2	NA	38	NA	116
M_3	40	39	42	121
合計	98	101	110	309

この秘匿処理は安全か？

	B1	B2	B3	B4	計
A1	7	10	60	13	90
A2	11	60	12	60	143
A3	60	11	60	12	143
A4	14	60	13	60	147
計	92	141	145	145	523

↓

	B1	B2	B3	B4	計
A1	x_1	x_2	60	x_3	90
A2	x_4	60	x_5	60	143
A3	60	x_6	60	x_7	143
A4	x_8	60	x_9	60	147
計	92	141	145	145	523

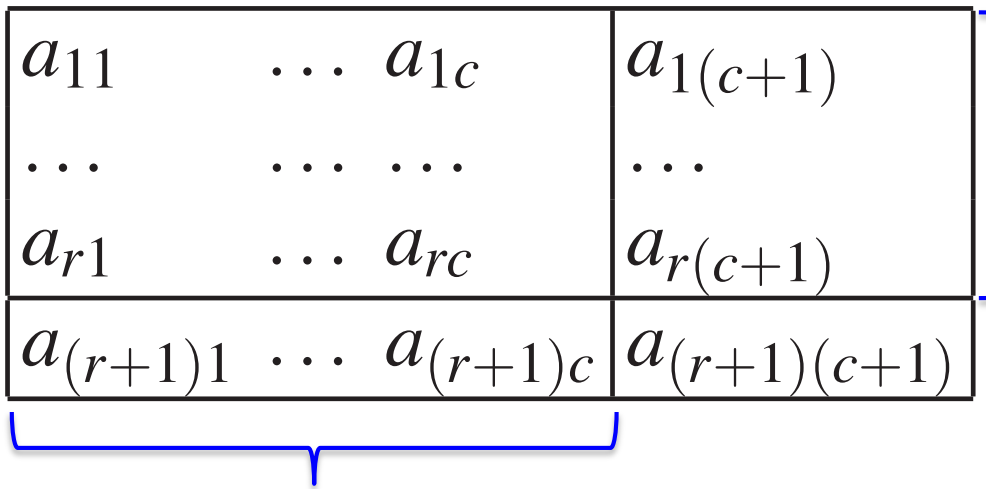
x_1は特定される

$$
\begin{array}{rrrrr}
 & x_1 + x_2 + x_3 & & & = 30 \\
 & x_2 & & + x_6 & = 21 \\
- & & x_3 & + x_7 & = 25 \\
\hline
 & x_1 & - & - x_6 - x_7 & = -16 \\
 & & & & \\
+ & & & x_6 + x_7 & = 23 \\
\hline
\end{array}
$$

$x_1 = 7$

行計、列計の関係式から秘匿セルの値が復元される

- *r*行*c*列の表には *(r+c)*個の線形制約条件が存在



$$\sum_{j=1}^{c} a_{ij} = a_{i(c+1)} \quad i = 1, \ldots, r$$

$$\sum_{i=1}^{c} a_{ij} = a_{(r+1)j} \quad j = 1, \ldots, c$$

安全性の検証には線形計画法の問題を解く必要がある

秘匿セルの取りうる値の範囲が十分広いことが安全性の要件

- 秘匿セル変数の可能範囲（*秘匿インターバル*）の幅*w*の長さがしきい値 *t*（*度数分布表では10*）以上であること

	P_1	P_2	P_3	合計
M_1	x_{11}	24	x_{13}	72
M_2	x_{21}	38	x_{23}	116
M_3	40	39	42	121
合計	98	101	110	309

1. 最小値問題

$$a_{23} = \min x_{23}$$

拘束条件:

$$\begin{aligned} x_{11} + x_{13} &= 72 - 24 \\ x_{21} + x_{23} &= 116 - 38 \\ x_{11} + x_{21} &= 98 - 40 \\ x_{13} + x_{23} &= 110 - 42 \\ (x_{11}, x_{13}, x_{21}, x_{23}) &\geq 0 \end{aligned}$$

and

2. 最大値問題

$$\overline{a_{23}} = \max x_{23}$$

拘束条件:

$$\begin{aligned} x_{11} + x_{13} &= 72 - 24 \\ x_{21} + x_{23} &= 116 - 38 \\ x_{11} + x_{21} &= 98 - 40 \\ x_{13} + x_{23} &= 110 - 42 \\ (x_{11}, x_{13}, x_{21}, x_{23}) &\geq 0. \end{aligned}$$

⇒ *秘匿インターバル* $w = \max x_{23} - \min x_{23} = 68 - 20 = 48 > 10$

表セル秘匿問題

- 秘匿パターン　$y_i \in \{0,1\} \quad i = 1, \ldots, n$

10	NA
5	80

(0,1,0,0)

- 目的関数: 秘匿セル数

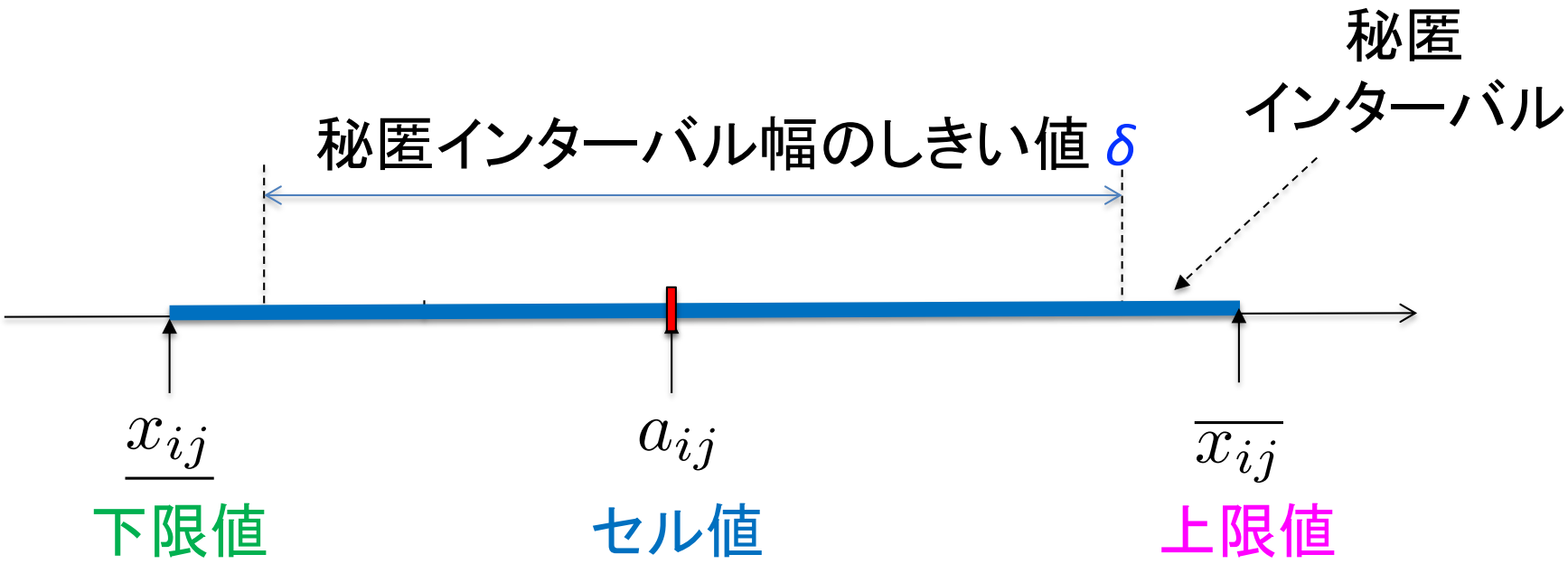
$$\sum_{i=1}^{n} y_i$$

最小化を目指す

- 拘束条件: 各1次秘匿セル値の機密性保護

秘匿インターバルの要件

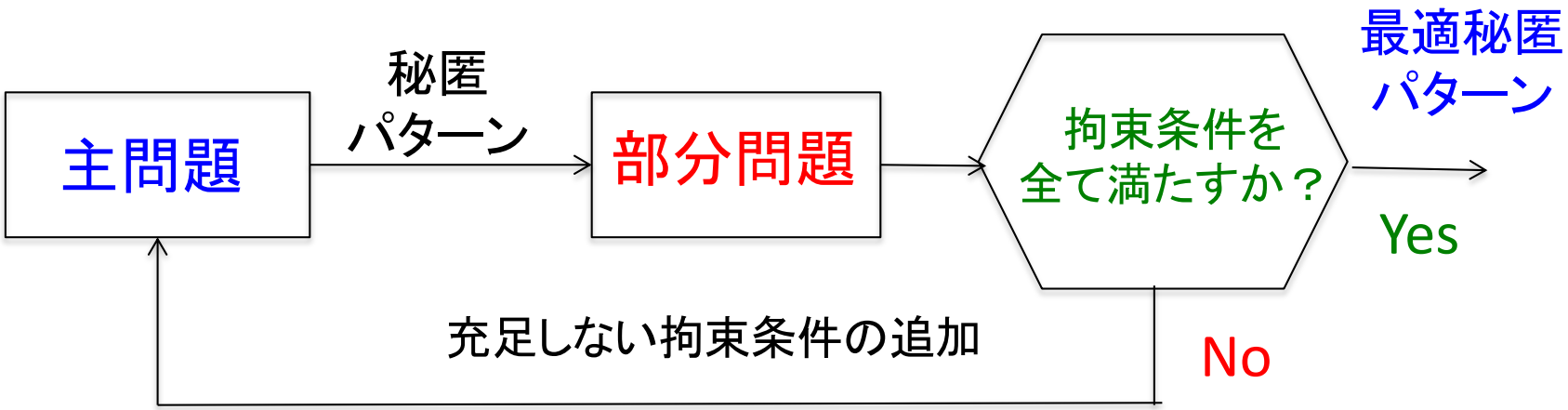
秘匿インターバルの幅 $w = \overline{x_{ij}} - \underline{x_{ij}} > \delta$



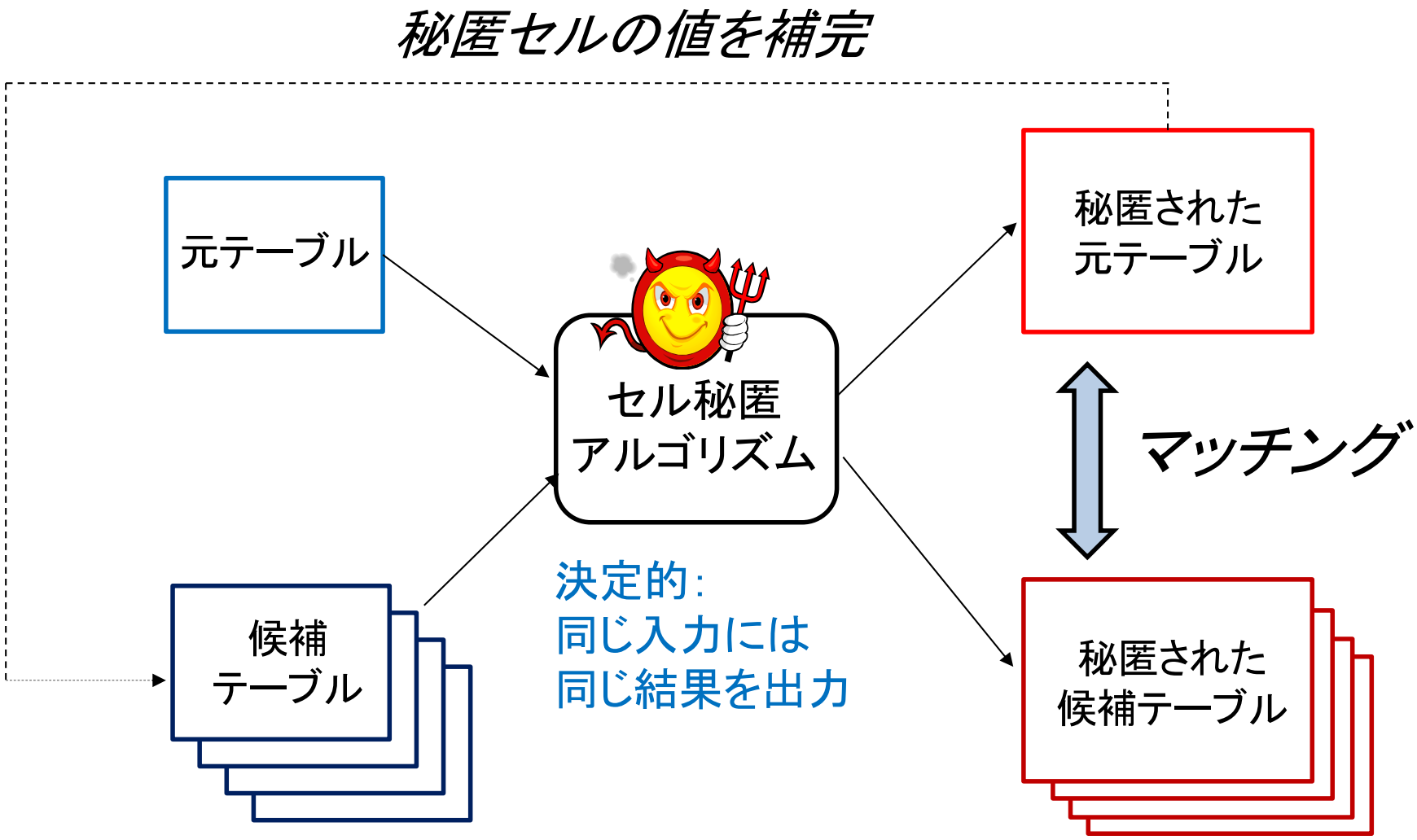
行計、列計の線形式を満足する値の範囲

Benders分割アルゴリズムによる効率的な実装

- 主問題と部分問題に分割
  - 主問題：秘匿パターンの最適化
  - 部分問題：各秘匿セルの拘束条件のチェック
- 最適化問題は*NP*困難であるが、大部分の表データを効率的に実行
- アルゴリズムが終了した場合は、*最適解を保証*



ただし、秘匿アルゴリズムが攻撃者の手に渡るとマッチング攻撃が可能



秘匿パターンが再現できた候補テーブルの値のみが真の候補値！

秘匿セルの候補値の列挙

- 秘匿セルの候補値ベクトルx は行計、列計に関する線形の拘束条件を満たす

$$Ax = b$$

- 行列Aの零空間N(A)は

$$N(A) = \{y \in \mathcal{Z}^n \mid Ay = 0\}$$

- $Ax = b$ の解の集合S は

$$S = \{v + y \mid Av = b \wedge y \in N(A)\}$$

例：秘匿セル候補値の列挙

	P_1	P_2	P_3	P_4	Sum
M_1	15	15	12	10	52
M_2	19	x_1	13	x_2	55
M_3	8	8	11	14	41
M_4	9	x_3	26	x_4	44
Sum	51	46	62	33	192

秘匿テーブル

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 23 \\ 9 \\ 23 \\ 9. \end{bmatrix}$$

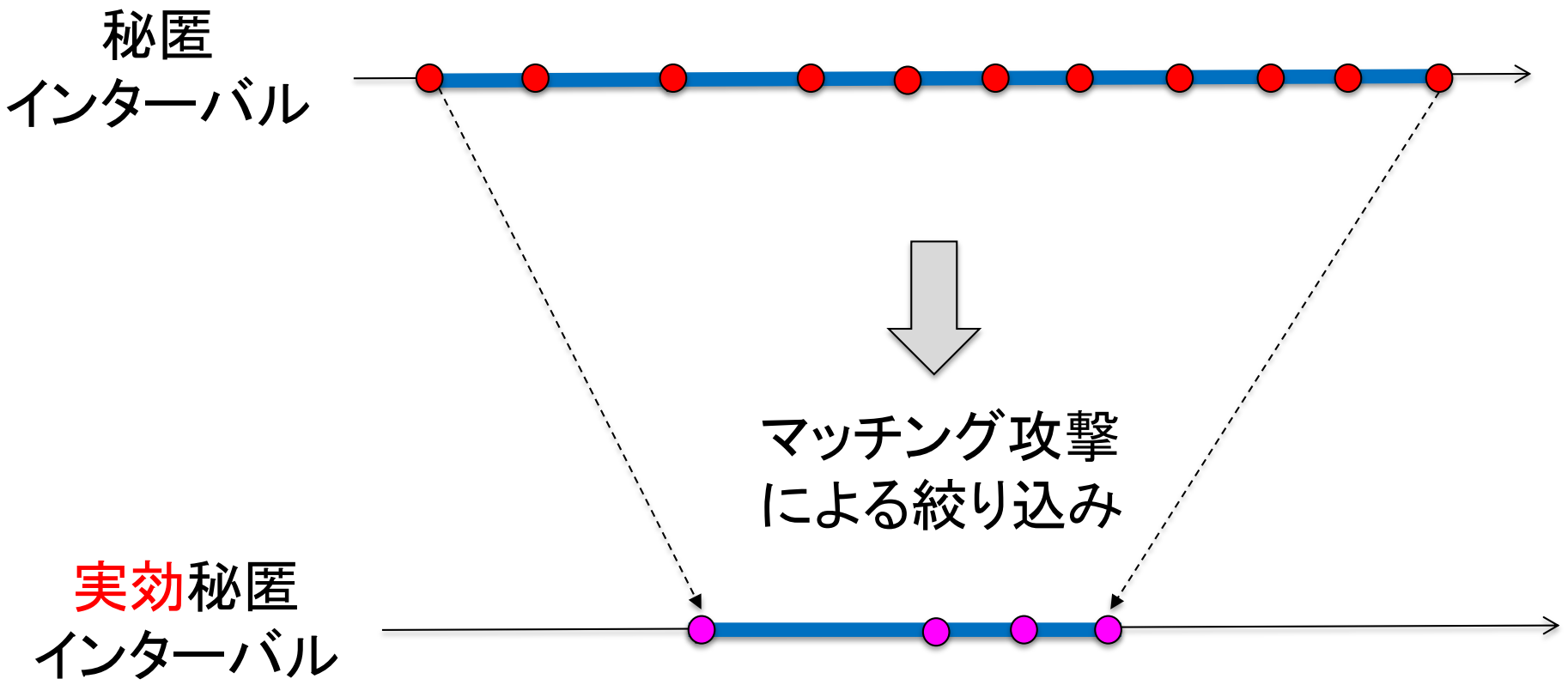
Ax = b

解集合

$$S = \left\{ \underbrace{\begin{bmatrix} 14 & 9 & 9 & 0 \end{bmatrix}^T}_{} + k \underbrace{\begin{bmatrix} 1 & -1 & -1 & 1 \end{bmatrix}^T}_{} \mid \quad k \in \mathcal{Z} \quad \wedge \quad 0 \leq k \leq 9 \right\}$$

Ax=b の特定の解　　零空間*N(A)*（この例では1次元）

秘匿インターバルの絞り込み



評価実験

Q:マッチング攻撃で秘匿インターバルの条件が侵害される一次秘匿セルの割合はどの程度か？

- セル数: 16, 25, 36, 49の2次元の度数分布表をランダムに各50個生成
  - セル値は平均15, 標準偏差10の正規分布から抽出
- セル秘匿アルゴリズムで2次秘匿テーブルを作成
  - 度数しきい値: 5
  - 秘匿インターバルのしきい値:8
- 同じセル秘匿アルゴリズムによるマッチング攻撃を実施

マッチング攻撃で安全要件（秘匿インターバルの最小幅）が破られた1次秘匿セル数

表セル数	一次秘匿セル数	安全でない一次秘匿セル数	安全でない一次秘匿セルの割合
16 (4×4)	104	48	46%
25 (5×5)	170	117	69%
36 (6×6)	230	190	83%
49 (7×7)	271	226	83%

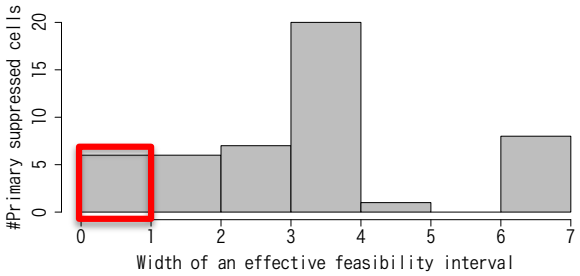
零空間の次元別の安全でない1次秘匿セルの割合

- 零空間の次元が小さいほど、候補となるテーブルが少なく、秘匿インターバルの絞り込みが大きい

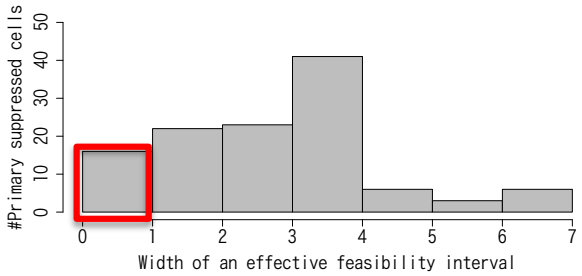
#Cells in a table	Dimension of the null space			
	1	2	3	4
16	0.83	0.42	0.17	
25	1.00	0.71	0.57	0.83
36	1.00	0.87	0.78	0.82
49		0.81	0.89	0.73
Total	0.88	0.73	0.75	0.77

絞り込まれた秘匿インターバルの分布

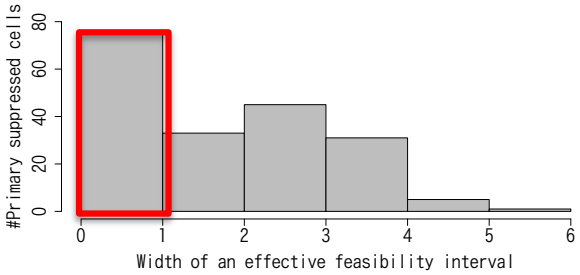
#Cells in a table	Width of an effective feasibility interval	#Unsafe cells
16	0	6
	1	6
	2	7
	3	20
	4	1
	5	0
	6	4
	7	4
25	0	16
	1	22
	2	23
	3	41
	4	6
	5	3
	6	5
	7	1
36	0	75
	1	33
	2	45
	3	31
	4	5
	5	0
	6	1
	7	0
49	0	92
	1	33
	2	28
	3	57
	4	4
	5	4
	6	5
	7	3



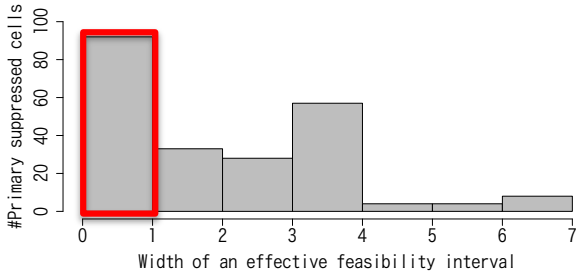
(a) Tables with 16 cells



(b) Tables with 25 cells



(c) Tables with 36 cells



(d) Tables with 49 cells

まとめ

- 統計開示抑制は出力プライバシー保護を目的とする
- 統計量が特定の入力に依存しないことを目指す安全性ルールに経験的に定めている
  - 最小度数ルール、占有性ルール
- 「決定論的」なセル秘匿処理には秘匿パターンの再現性確認によるマッチング攻撃が存在
  - 実証実験では現実的な脅威であることを確認
- 今後の方向性
  - ➢ 秘匿処理への確率的なランダム性の導入
    - ノイズ付加、ランダムサンプリング等
  - ➢ 攻撃者に関する仮定の緩和
    - 例：９人の共謀は不可能

自分以外のデータ提供者が全員共謀している場合に入力データの機密性を保証する安全性指標は？