プライバシーを保護した
放射線疫学調査システム

†佐藤智貴　†菊池浩明　‡佐久間淳

†東海大学大学院工学研究科

‡筑波大学システム情報工学研究科

研究背景

- 放射線の人体への影響
  - **疫学調査**が重要

［事件］ニュース

ブログに書く | 引用ブログ（15件） | Tweet 152 | メッセ | 印刷

【放射能漏れ】

人体への影響は？　放射線１００ミリシーベルトから健康被害

2011.3.15 19:57 （1/2ページ）

福島第１原発から周辺自治体へ拡散する恐れが出ている放射性物質。３号機付近で毎時４００ミリシーベルトの高い強度の放射線が確認されており、

産経ニュース 2011.3/15

放射線疫学調査

組織A

名前	年齢	累積線量
佐藤	20	12
菊池	30	51
佐久間	30	33

組織B

名前	死因
田中	肺がん
佐藤	外因死
鈴木	肺がん

組織A：放射線事業従事者中央登録センター
組織B：厚生労働省(死亡テープ)
　　地域がんセンター(がん患者カルテ)

放射線疫学調査

組織A

名前	年齢	累積線量
佐藤	20	12
菊池	30	51
佐久間	30	33

組織B

名前	死因
田中	肺がん
佐藤	外因死
鈴木	肺がん

組織A：放射線事業従事者中央登録センター
組織B：厚生労働省(死亡テープ)
　　地域がんセンター(がん患者カルテ)

既存の疫学調査の問題点

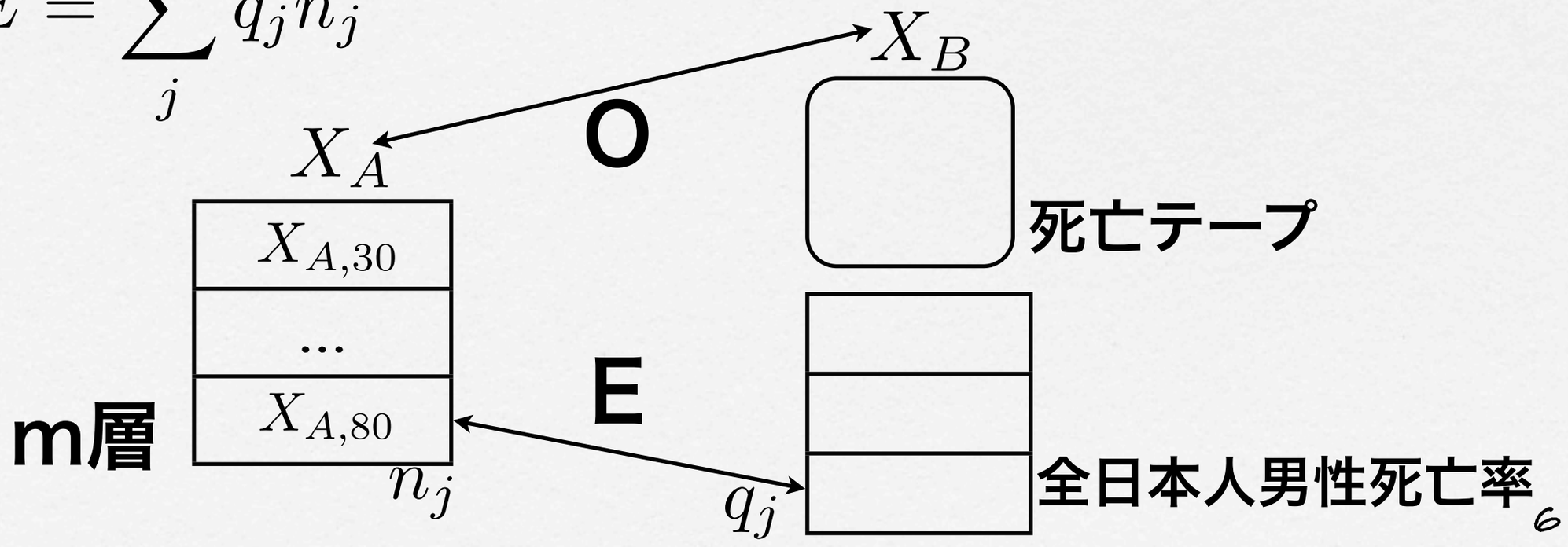
- 特殊な法律が必要
  - 行政機関の保有する電子計算機処理に係る個人情報保護の法律
- 従事者の同意が必要
  - 12,410人が拒否
- 情報の粒度や鮮度が不十分

目的

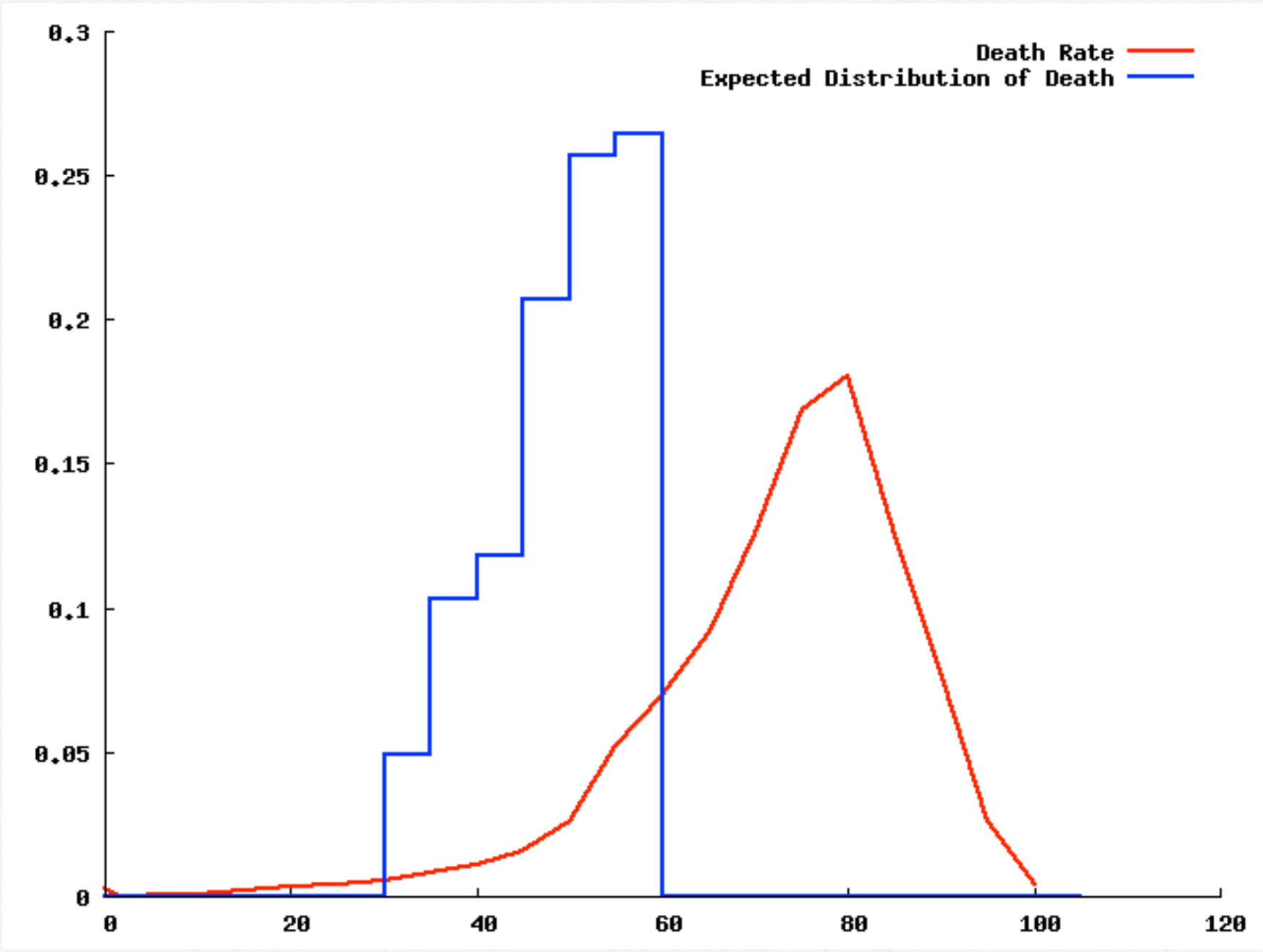
プライバシーを保護した疫学調査

疫学調査の方法

- **O(Observed)：観察死亡数**
  - $O = |X_A \cap X_B|$
- **E(Expected)：期待死亡数**
  - $E = \sum_{j}^{m} q_j n_j$



期待死亡率


Death Rate
Expected Distribution of Death
0.3
0.25
0.2
0.15
0.1
0.05
0
0
20
40
60
80
100
120

疫学調査の目的

X_A における死亡率や，がん罹患率
が標準的な期待死亡率に対して
有意な差があるか判定

表 1　表 3.3-1 死因別標準化死亡比 (SMR)
(前向き観察、最短潜伏期;0 年、年齢、暦年を調整)(文献[1] より引用)

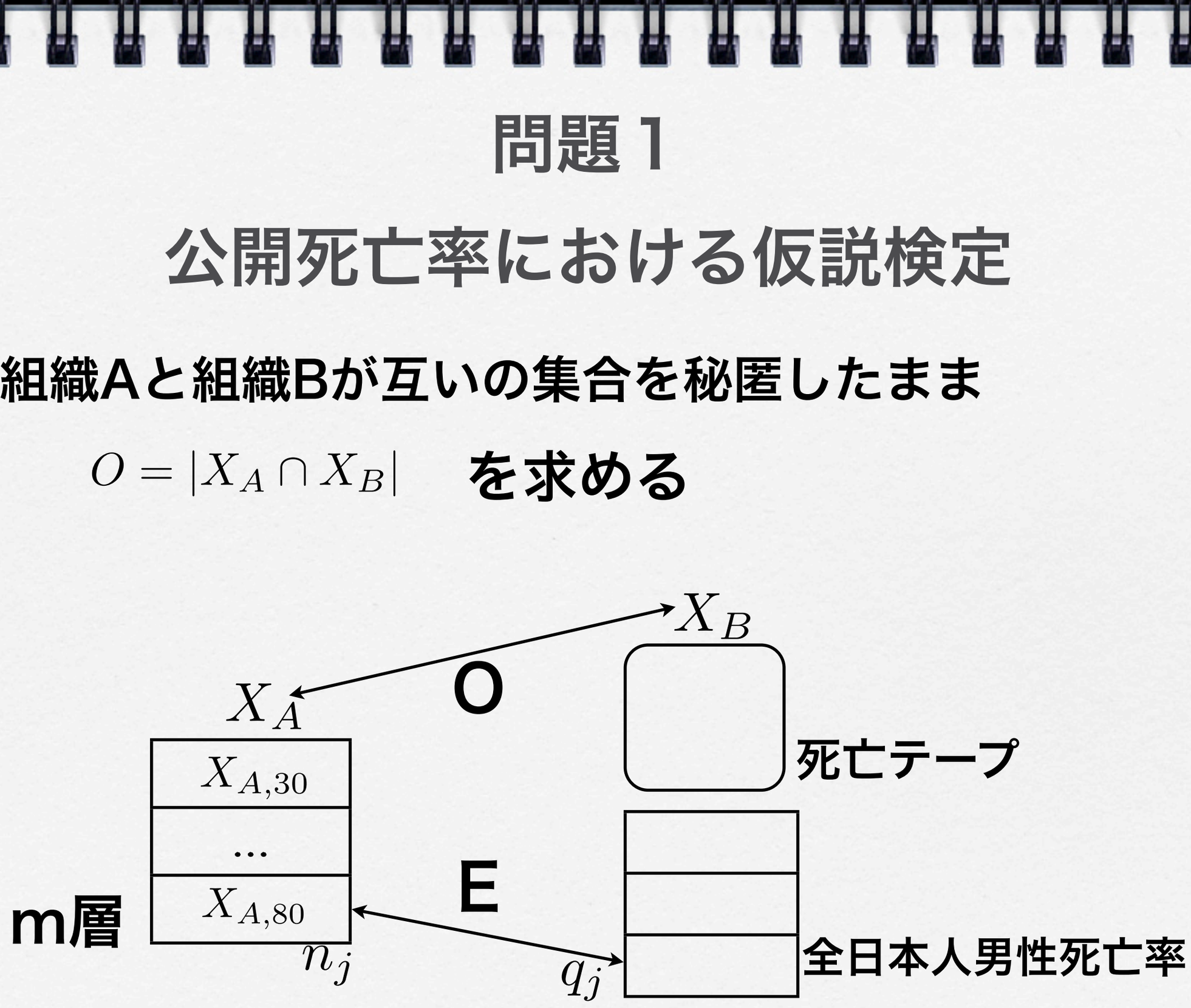
死因	観察死亡数	期待死亡数	SMR	95%信頼区間	両側検定結果 p 値
全死因$^{\star 1}$	14,224	14,086.9	1.01	(0.99 - 1.03)	0.250
食道	326	312.1	1.04	(0.93 - 1.16)	0.449
胃	1,002	989.4	1.01	(0.95 - 1.08)	0.700
肺	1,208	1,117.8	1.08	(1.02 - 1.14)	0.007

問題１

公開死亡率における仮説検定

組織Aと組織Bが互いの集合を秘匿したまま

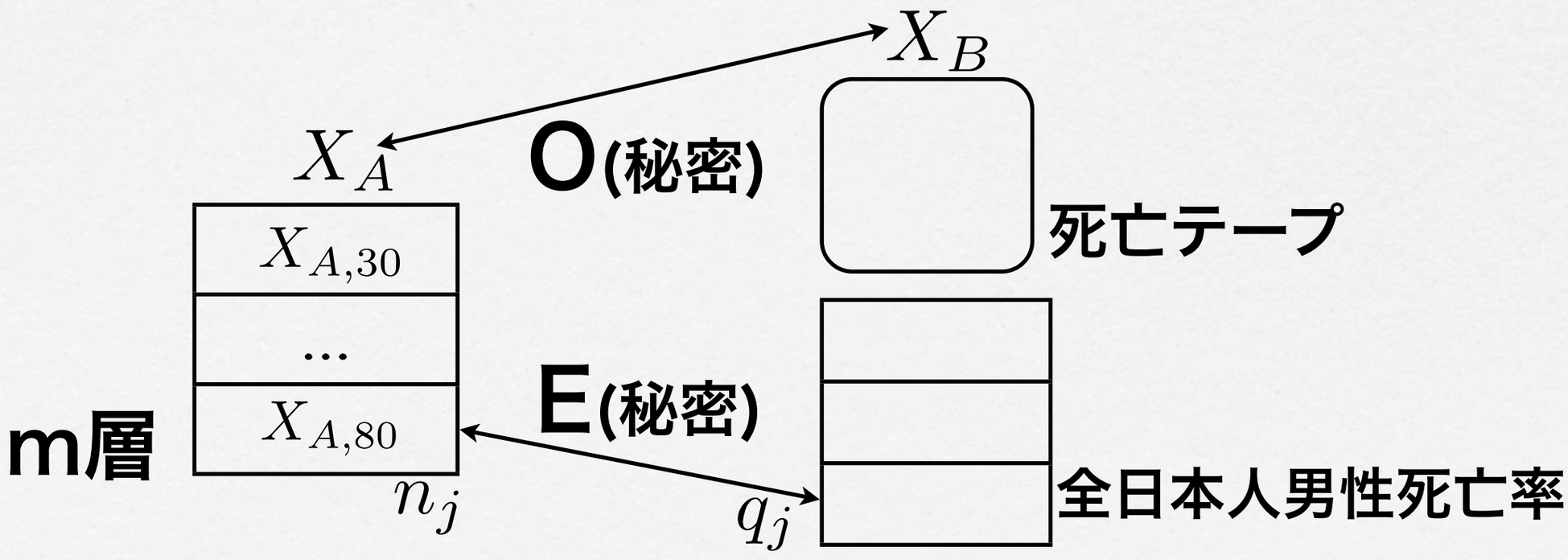
$O = |X_A \cap X_B|$　**を求める**



問題2

秘密死亡率における仮説検定

未知の疾病等，死亡率や罹患率を**公開できない**場合
OとEを秘密にしつつ，**有意な差**があるか判断



有意差があるかの判定

$$Z = \frac{|O - E| - 0.5}{\sqrt{E}} > Z(a/2)$$

$$z^2 = \frac{O^2}{E} - 2O + E$$

公開される情報

$X_A \cap X_B$	O	E	Z
従来	○	○	○	○
問題１	×	○	○	○
問題２	×	×	×	○

○：公開

×：秘密

問題1への提案プロトコル

- 可換一方向性関数(AES03)

可換一方向性関数 - 入出力

入力：集合 $X = \{x_1, \ldots, x_{n_A}\}$**を持つA**

$Y = \{y_1, \ldots, y_{n_B}\}$**を持つB**

出力： $|X \cap Y|$ **を求める**

可換一方向性関数

A

乱数2

$$X_A = \{3, 4, 6, 7\}$$

B

乱数3

$$X_B = \{2, 3, 5, 6\}$$

可換一方向性関数

A

乱数2

$$X_A = \{3, 4, 6, 7\}$$
$$X_A^2 = \{9, 16, 36, 49\}$$

B

乱数3

$$X_B = \{2, 3, 5, 6\}$$
$$X_B^3 = \{8, 27, 125, 216\}$$

可換一方向性関数

A

乱数2

$$X_A = \{3, 4, 6, 7\}$$

$$X_B^3 = \{8, 27, 125, 216\}$$

B

乱数3

$$X_B = \{2, 3, 5, 6\}$$

$$X_A^2 = \{9, 16, 36, 49\}$$

可換一方向性関数

A

乱数2

$$X_A = \{3, 4, 6, 7\}$$

$$X_B^3 = \{8, 27, 125, 216\}$$

B

乱数3

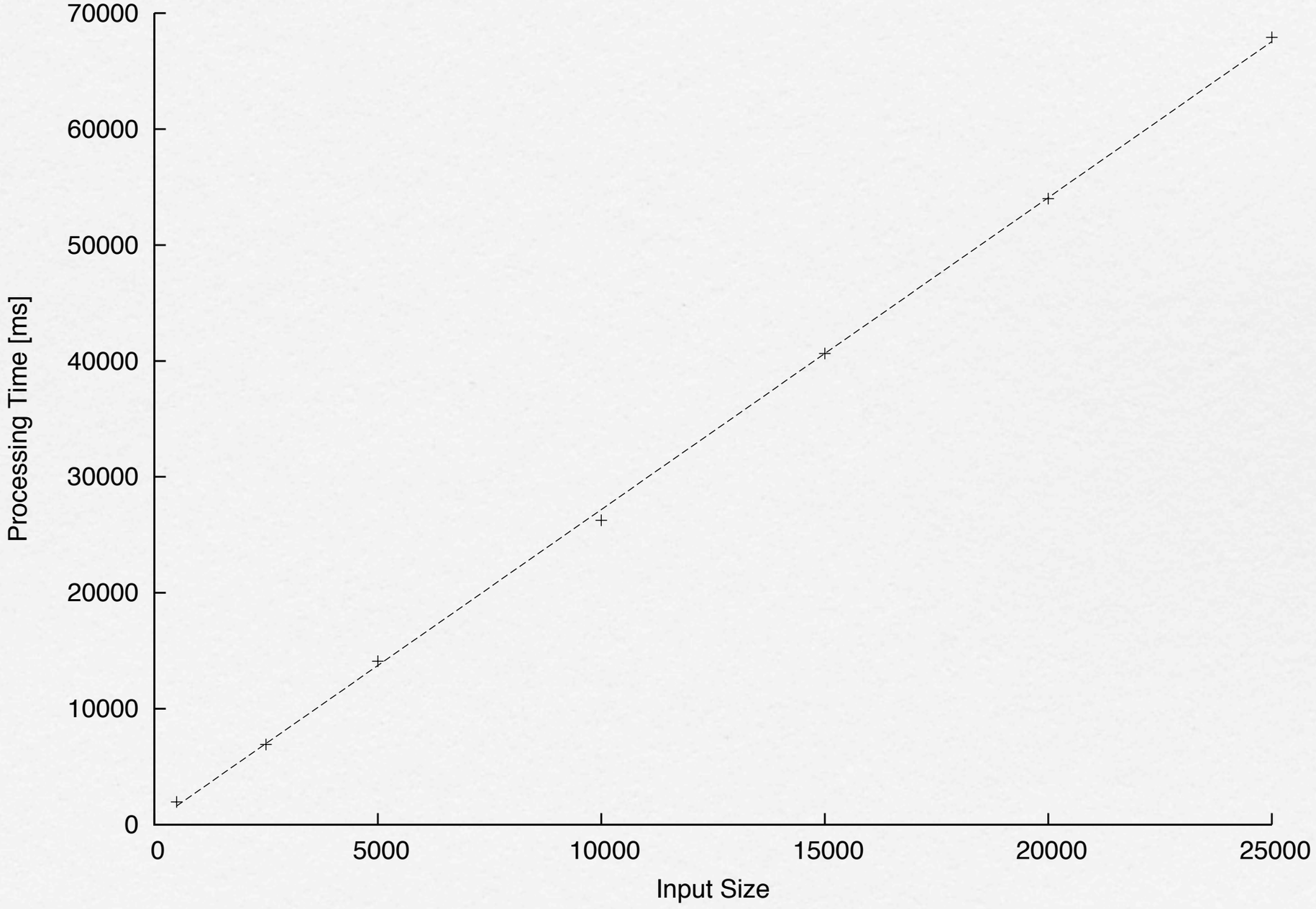
$$X_B = \{2, 3, 5, 6\}$$

$$X_A^2 = \{9, 16, 36, 49\}$$

$$(X_A^2)^3 = \{729, 4096, 46656, 117649\}$$

$$(X_B^3)^2 = \{64, 729, 15625, 46656\}$$

試験実装したプログラムの処理時間



問題2への提案プロトコル

- セキュア内積プロトコル(VC02)

VC02 - 入出力

入力：Aliceはn次元ベクトル $x = (x_1, \ldots, x_n)$
Bobはn次元ベクトル $y = (y_1, \ldots, y_n)$ を持つ

出力：AliceとBobは $s_A + s_B = x \cdot y$
となるような s_A と s_B を得る

VC02

pk:準同型暗号で
作った公開鍵

s_B :ランダム

A

B

pk

$E(x_1), \ldots, E(x_n)$

VC02

pk:準同型暗号で
作った公開鍵

s_B :ランダム

A

B

pk

$E(x_1), \ldots, E(x_n)$

VC02

pk:準同型暗号で
作った公開鍵

s_B :ランダム

A

B

pk

$$E(x_1), \ldots, E(x_n)$$

$$c = E(x_1)^{y_1} \ldots E(x_n)^{y_n} / E(s_B)$$

VC02

pk:準同型暗号で
作った公開鍵

s_B :ランダム

A

B

pk

$E(x_1), \ldots, E(x_n)$

$c = E(x_1)^{y_1} \ldots E(x_n)^{y_n} / E(s_B)$

VC02

pk:準同型暗号で
作った公開鍵

s_B :ランダム

A

B

pk

$E(x_1), \ldots, E(x_n)$

$$c = E(x_1)^{y_1} \ldots E(x_n)^{y_n} / E(s_B)$$

$$D(c) = x_1 y_1 + \ldots + x_n y_n - s_B = s_A$$

提案方式２

$$z^2 = \frac{O^2}{E} - 2O + E$$

$$z^2 = \frac{{s_A}^2 + 2(w_A + w_B) + {s_B}^2}{t_A + t_B} - 2(s_A + s_B) + (t_A + t_B)$$

提案方式２

$$z^2 = \frac{O^2}{E} - 2O + E$$

$$z^2 = \frac{{s_A}^2 + 2(w_A + w_B) + {s_B}^2}{t_A + t_B} - 2(s_A + s_B) + (t_A + t_B)$$

A

$${s_A}^2, s_A, t_A, w_A$$

B

$${s_B}^2, s_B, t_B, w_B$$

暗号プロトコルの比較

	AES03	VC02	FNP04
要素の同定可能	yes	no	yes
入力	集合	ベクトル	集合
処理性能	$O(n)$	$O(N)$	$O(n^2)$
パフォーマンス	360件/s	10件/s	-
提案方式２への利用	no	yes	no

まとめ

- 被験者のプライバシー保護と，より詳細な調査が必要であるという矛盾した問題に対して，暗号プロトコルの適用を提案し，試験実装に基づいて実現可能であることを示した.
- 今後の課題
  - 試験実装したプログラムの高速化
  - 提案方式２の試験実装