

PWSCUP2020

匿名メンバシップ
推定コンテスト

*Anonymity
against
Membership
Inference*
Contest

AMIC

10/26-29
月 木

参加エントリー申込

2020年8月7日(金)
~2020年8月26日(水)

予備戦

2020年8月27日(木)
~2020年9月18日(金)

本戦

2020年9月24日(木)
~2020年10月20日(火)

会場 オンライン開催

主催 PWS2020実行委員会

(コンピュータセキュリティシンポジウム2020に併催)

PWS Cup 2020 “AMIC” 振り返り

2021/3/12

PWS2021Meetup

千田浩司

(PWSCUP2020実行委員会副委員長)

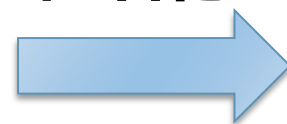
PWS Cup (2015~)

- ▶ パーソナルデータを使いやすく安全に匿名化する効果的な方法の探求のため、匿名化とその攻撃の技術を競うコンテスト
- ▶ 攻防戦：Ice (匿名化) vs. Fire (攻撃)

元のデータ

氏名	性別	年齢	罹患歴1	...
神戸 一郎	男	27	腹痛	...
匿名子	女	32	風邪	...
森 アミック	男	56	目まい	...
⋮	⋮	⋮	⋮	⋮

匿名化



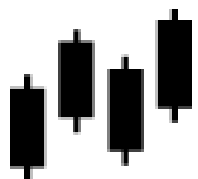
再識別
(攻撃)

匿名化データ

氏名	性別	年齢	罹患歴1	...
	男	27	腹痛	...
	女	32	風邪	...
	男	56	目まい	...
	⋮	⋮	⋮	⋮

再識別されな
いように加工

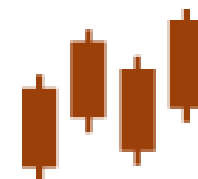
分析



有用性



分析



これまでの PWS Cup

- ▶ 様々なデータで実施
- ▶ 安全性(匿名性)指標や有用性指標も改善/変更

	2015	2016	2017	2018	2019
データセット	疑似マイクロデータ (世帯消費額)	UCI Dataset "Online Retail" (購買履歴)			位置情報
安全性指標		レコード リンケージ			レコードリンケージ、 トレース推定



PWSCUP2020

匿名メンバシップ
推定コンテスト

Anonymity
against
Membership
Inference
Contest

AMIC

PWS Cup 2020 “AMIC”

- ▶ “Synthetic Data” (擬似データ/合成データ) に着目
 - ▶ 匿名化の手段として
 - ▶ より有用性の高いデータが作れるかも
 - ▶ 特に最近では機械学習分野で注目されている
- ▶ データリンケージ → **メンバシップ推定**
 - ▶ 擬似データに適用できる安全性指標
 - ▶ 匿名化データにAさんが含まれているかどうか
- ▶ AI・機械学習分野の難関国際会議NeurIPS2020でも類似ルール of 匿名化技術コンペが開催

10/26-29
月 木

参加エントリー申込
2020年8月7日(金) ~2020年8月26日(水)
予備戦
2020年8月27日(木) ~2020年9月18日(金)
本戦
2020年9月24日(木) ~2020年10月20日(火)

会場 オンライン開催

主催 PWS2020実行委員会

(コンピュータセキュリティシンポジウム2020に併催)

	2015	2016	2017	2018	2019	2020
データセット	疑似マイクロデータ (世帯消費額)	UCI Dataset “Online Retail” (購買履歴)			位置情報	米国センサスデータの 疑似データ
安全性指標		レコード リンケージ			レコードリンケージ、ト レース推定	メンバシッ プ推定

PWS2020実行委員会 Cup WG メンバ

- ▶ 千田 浩司 (NTT)
- ▶ 荒井 ひろみ (理研)
- ▶ 井口 誠 (Kii)
- ▶ 小栗 秀暢 (富士通研)
- ▶ 菊池 浩明 (明治大)
- ▶ 黒政 敦史 (FJCT)
- ▶ 中川 裕志 (理研)
- ▶ 中村 優一 (早稲田大)
- ▶ 西山 賢志郎 (BizReach)
- ▶ 野島 良 (NICT)
- ▶ 長谷川 聡 (NTT)
- ▶ 波多野 卓磨 (NSSOL)
- ▶ 濱田 浩気 (NTT)
- ▶ 古川 諒 (NEC)
- ▶ 村上 隆夫 (産総研)
- ▶ 山岡 裕司 (富士通研)
- ▶ 山田 明 (KDDI総研)
- ▶ 渡辺 知恵美 (筑波技術大)

- PWS2021実行委員は絶賛募集中です！
- ご興味がありましたら、千田または上記メンバにお気軽にお問い合わせください

PWS Cup 2020 参加チーム (20チーム)

No.	チーム名	所属
02	Brown DP	非公開
03	鋼鉄の錬金術師	日鉄ソリューションズ株式会社
04	Yichi	非公開
05	小熊軟糖 🍬	非公開
06	たけのこ半島	非公開
07	JOSE2	三菱電機株式会社
08	サイコロ	非公開
11	SynIPA	UQAM
12	ホンワカインコ	非公開
13	🍓🍓🍓	株式会社ミクシィ

No.	チーム名	所属
14	ステテコ大木	静岡大学大木研究室
15	ステテコ西垣	静岡大学西垣研究室
16	ステテコ菊池	明治大学大学院
17	匿工野郎A チーム	非公開
18	天然水	筑波大学
19	docomo freshers	非公開
21	wakanalie	非公開
22	初ぼっち	非公開
23	テレぼっち	Kii株式会社
27	M.AI	非公開

AMIC で用いた米国センサスデータ

- ▶ **Census Income Data Set** <https://archive.ics.uci.edu/ml/datasets/census+income>
- ▶ 機械学習の試用を想定した15属性の訓練用データ32,561レコード、テスト用データ16,281レコード
- ▶ 出題者が用意した擬似データ生成手法を用いて、**重複レコードの無い10万レコードの擬似データ**を生成
 - ▶ 重複を含む100万レコードの擬似データを生成してから、重複を削除し、10万レコードをランダムサンプリング
- ▶ 属性値の数・分布や重複度等を考慮し、以下の**9属性を用いる** ($73 \times 8 \times 16 \times 7 \times 14 \times 6 \times 2 \times 99 \times 2 = 2,175,731,712$ 通り)

age: continuous. [17-90]

workclass(8): Private, Self-emp-not-inc, Self-emp-inc, Federal-gov, Local-gov, State-gov, Without-pay, Never-worked.

education(16): Bachelors, Some-college, 11th, HS-grad, Prof-school, Assoc-acdm, Assoc-voc, 9th, 7th-8th, 12th, Masters, 1st-4th, 10th, Doctorate, 5th-6th, Preschool.

marital-status(7): Married-civ-spouse, Divorced, Never-married, Separated, Widowed, Married-spouse-absent, Married-AF-spouse.

occupation(14): Tech-support, Craft-repair, Other-service, Sales, Exec-managerial, Prof-specialty, Handlers-cleaners, Machine-op-inspct, Adm-clerical, Farming-fishing, Transport-moving, Priv-house-serv, Protective-serv, Armed-Forces.

relationship(6): Wife, Own-child, Husband, Not-in-family, Other-relative, Unmarried.

sex(2): Female, Male.

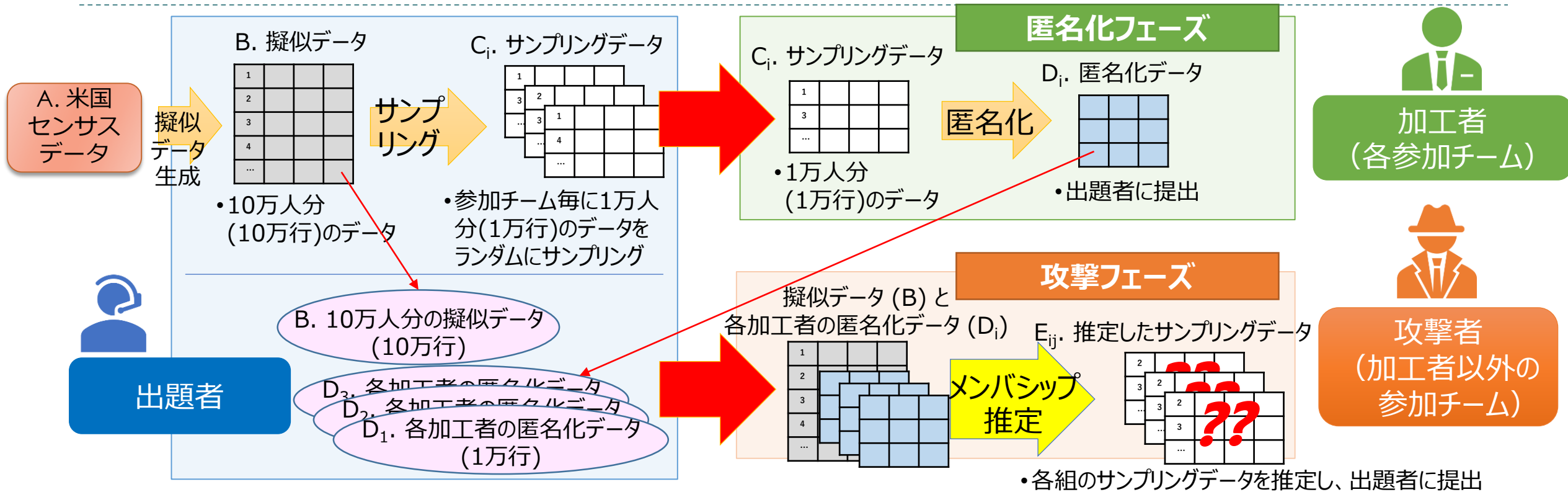
hours-per-week: continuous. [1-99]

income(2): >50K, <=50K

ヘッダ→
(今回はヘッダ
行を除いたファイル
を扱う)

age	workclass	education	marital-status	occupation	relationship	sex	hours-per-week	income
39	State-gov	Bachelors	Never-married	Adm-clerical	Not-in-family	Male	40	<=50K
50	Self-emp-not-inc	Bachelors	Married-civ-spouse	Exec-managerial	Husband	Male	13	>50K
38	Private	HS-grad	Divorced	Handlers-cleaners	Not-in-family	Male	40	<=50K
53	Private	11th	Married-civ-spouse	Handlers-cleaners	Husband	Male	40	<=50K
28	Private	Bachelors	Married-civ-spouse	Prof-specialty	Wife	Female	40	>50K
...

AMIC の全体像










- ▶ 匿名化の手段：擬似データ生成を含め、ほぼ任意の手段でOK (いくつかサンプルコードを用意)
- ▶ メンバシップ推定：擬似データ B と各匿名化データ D_i から、各サンプルングデータ C_i を推定
- ▶ 勝敗 (概略)
 - ▶ 匿名化部門：全攻撃者のメンバーシップ推定の最大成功確率が低いほど上位
 - ▶ 攻撃部門：匿名化部門の上位チームに対してメンバーシップ推定の成功確率が高いほど上位
 - ▶ 総合部門：上記各部門の順位から決定。3位まで表彰

有用性基準

- ▶ サンプルデータを用いた分析結果と、匿名化データを用いた分析結果を比較
- ▶ **匿名化データが以下の有用性基準を満たさなければ失格 (提出前にテストコードでセルフチェック可能)**
- ▶ 予備戦
 - ▶ ヒストグラム：全ての属性について、誤差が1%以下
 - ▶ 分散共分散：全ての二属性の分散共分散行列の各行について、各要素の誤差の総和が 2.5 以下
 - ▶ 決定木分析：目的変数="relationship(Husband or Not)", "income" として、F-尺度の誤差が何れも15%以下
- ▶ 本戦
 - ▶ ヒストグラム：全ての属性について、**誤差が3%以下**
 - ▶ **相関係数**：全ての二属性について、**誤差が10%以下**
 - ▶ 決定木分析：目的変数="relationship(Husband or Not)", "income" として、**F-尺度の誤差が何れも5%以下**

age	workclass	education	marital-status	occupation	relationship	sex	hours-per-week	income
39	State-gov	Bachelors	Never-married	Adm-clerical	Not-in-family	Male	40	<=50K
50	Self-emp-not-inc	Bachelors	Married-civ-spouse	Exec-managerial	Husband	Male	13	>50K
38	Private	HS-grad	Divorced	Handlers-cleaners	Not-in-family	Male	40	<=50K
53	Private	11th	Married-civ-spouse	Handlers-cleaners	Husband	Male	40	<=50K
28	Private	Bachelors	Married-civ-spouse	Prof-specialty	Wife	Female	40	>50K
...

本戦 結果： 攻防戦

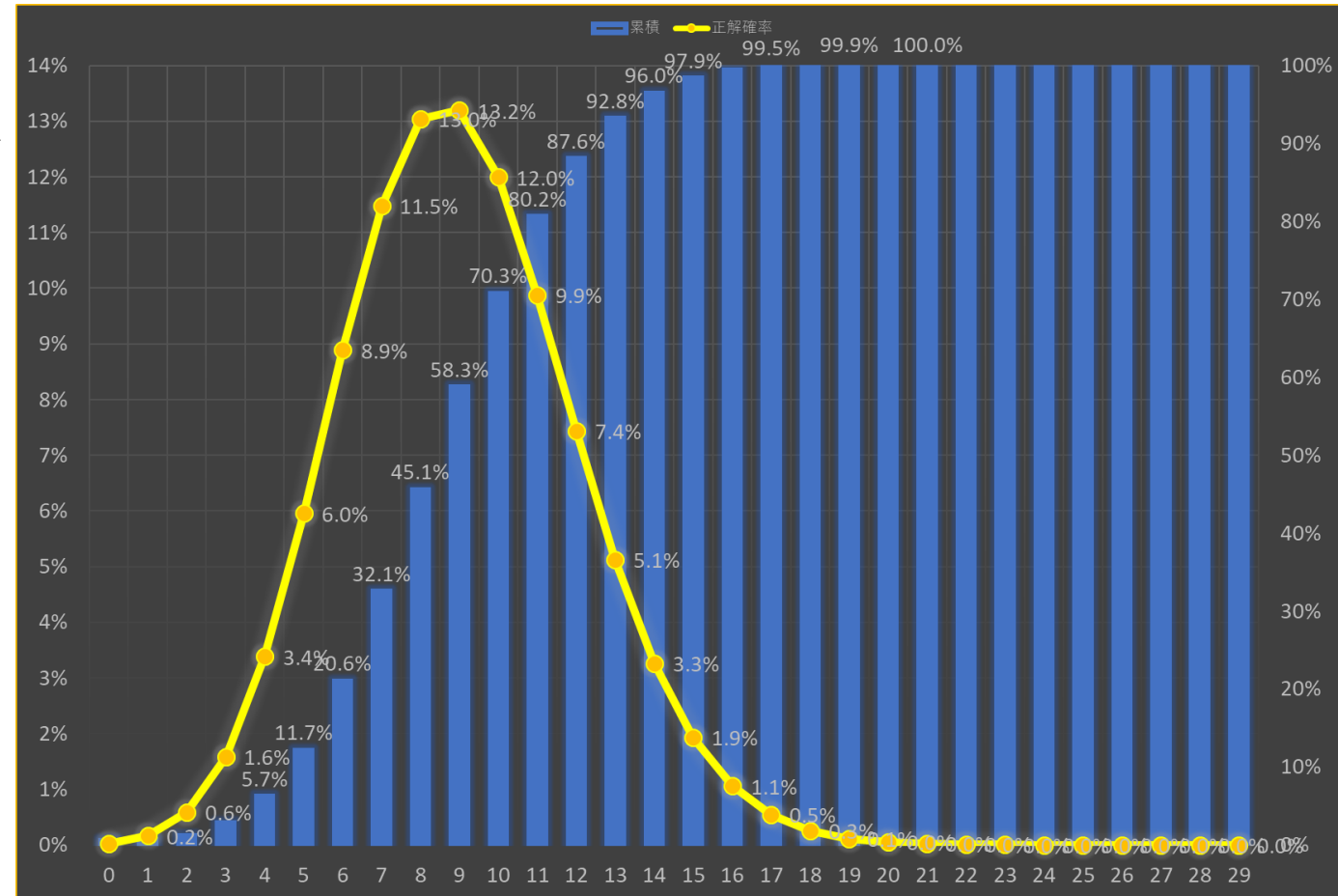
		 1		 3		Anonymizer										 2		 4	
		03	06	07	08	11	12	13	14	15	16	17	18	19	21	22	23	27	
attack.py		0	11	10	0	0	0	0	0	31	0	0	2	97	8	0	11	13	
Attacker	 03		12	5	8	9	2	97	18	65	13	6	11	100	5	11	37	13	
	04	7	12	8	7	4	9	15	14	7	8	8	9	7	10	9	11	13	
	06	11		16	13	12	13	10	13	4	5	14	14	10	14	15	14	7	
	 07	12	12		15	48	2	86	74	89	9	12	14	100	73	96	91	15	
	08	9	13	8		26	2	91	18	20	11	12	10	100	21	33	28	16	
	11	8	12	16	9		19	65	16	24	10	12	8	68	11	35	34	7	
	12	9	12	19	4	13		96	27	13	10	13	11	90	19	16	12	15	
	13	9	4	10	9	14	8		15	15	9	11	14	96	11	36	26		
	 14	11	15	12		8	8	11		10	12	11	11	97	12	9	14	8	
	15	10	5	77	10	26	29	36	78		6	11	9	100	70	86	8	13	
	16	4	10	8	11	36	9	87	25	50		9	8	99	13	19	61	12	
	17	10	7	7	19	53	59	96	25	49	9		15	90	39	82	61	14	
	18	11	9	5	10	7	20	9	9	5	7	17		4	11	7	10	6	
	19	9	9	9	12	11	3	78	8	17	7	7	16		14	15	26	7	
	21	11	8	60	13	9	18	21	52	41	13	12	6	96		88	48	13	
22	11	8	9	4	13	21	10	19	7	10	11	12	92	10		17	13		
23	11	6	9	6	15	47	52	18	11	8	12	9	100	7	23		11		

どれくらい当たる？

- ▶ 匿名化データがランダムであれば、メンバーシップ推定の成功確率は超幾何分布に従う

- ▶ 期待値は10 (100個中10個的中)
- ▶ 10個程度しか当てられなければかなり匿名性が高い
- ▶ 14個以上当てる確率は7.1%
- ▶ 最大成功確率

- ▶ 予備戦匿名化1位：15 / 100
- ▶ 予備戦匿名化2位：16 / 100
- ▶ 予備戦匿名化3位：16 / 100
- ▶ 予備戦匿名化4位：16 / 100
- ▶ 予備戦匿名化5位：25 / 100
- ▶ 予備戦匿名化6位：44 / 100
- ▶ 予備戦匿名化7位：51 / 100



どれくらい当たる？

- ▶ 匿名化データがランダムであれば、メンバーシップ推定の成功確率は超幾何分布に従う

- ▶ 期待値は10 (100個中10個的中)
- ▶ 10個程度しか当てられなければかなり匿名性が高い
- ▶ 14個以上当てる確率は7.1%
- ▶ 最大成功確率

- ▶ 本戦匿名化1位：12 / 100

- ▶ 本戦匿名化2位：13 / 100

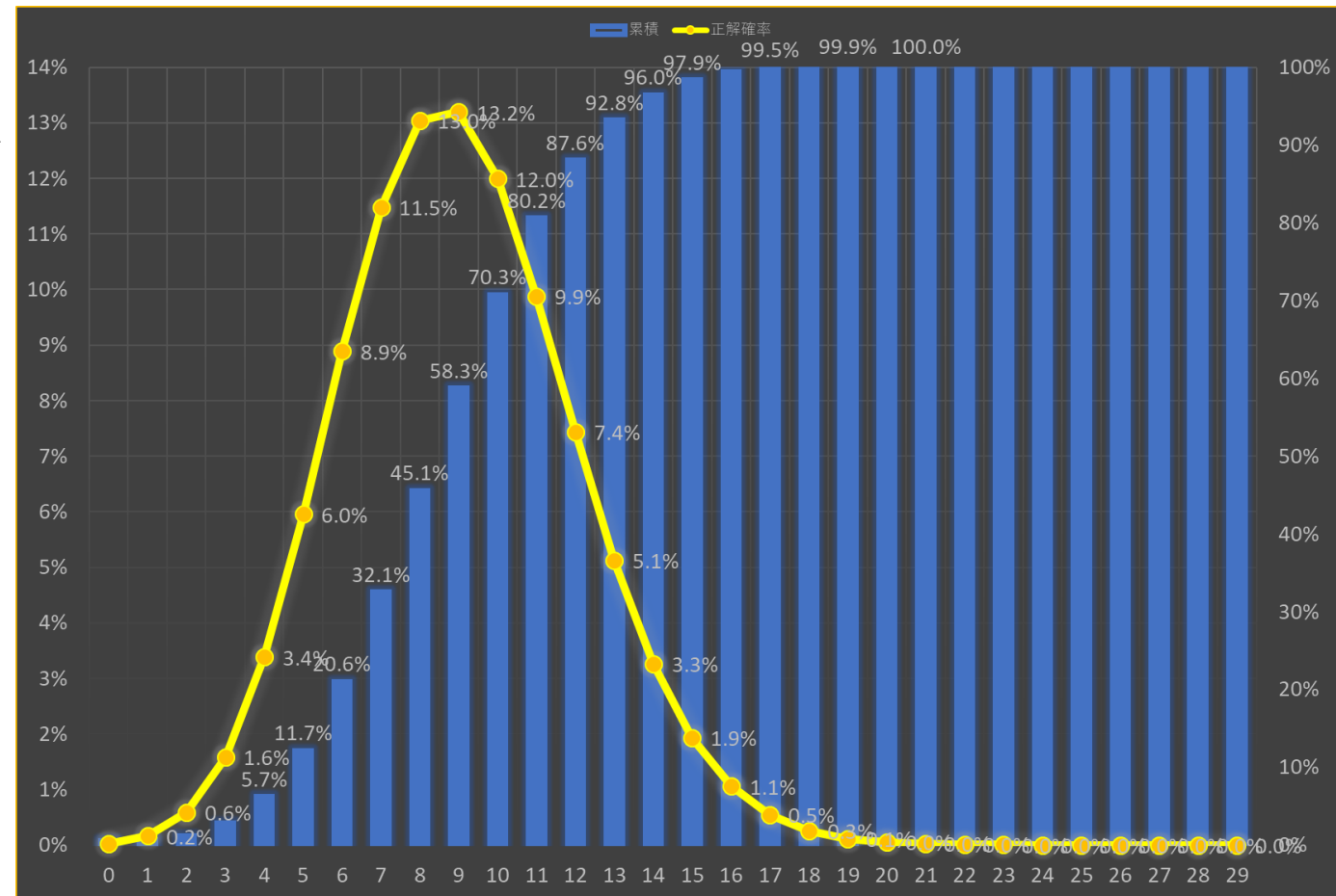
- ▶ 本戦匿名化3位：15 / 100

- ▶ 本戦匿名化4位：16 / 100

- ▶ 予備戦匿名化5位：16 / 100

- ▶ 予備戦匿名化6位：17 / 100

- ▶ 予備戦匿名化7位：19 / 100

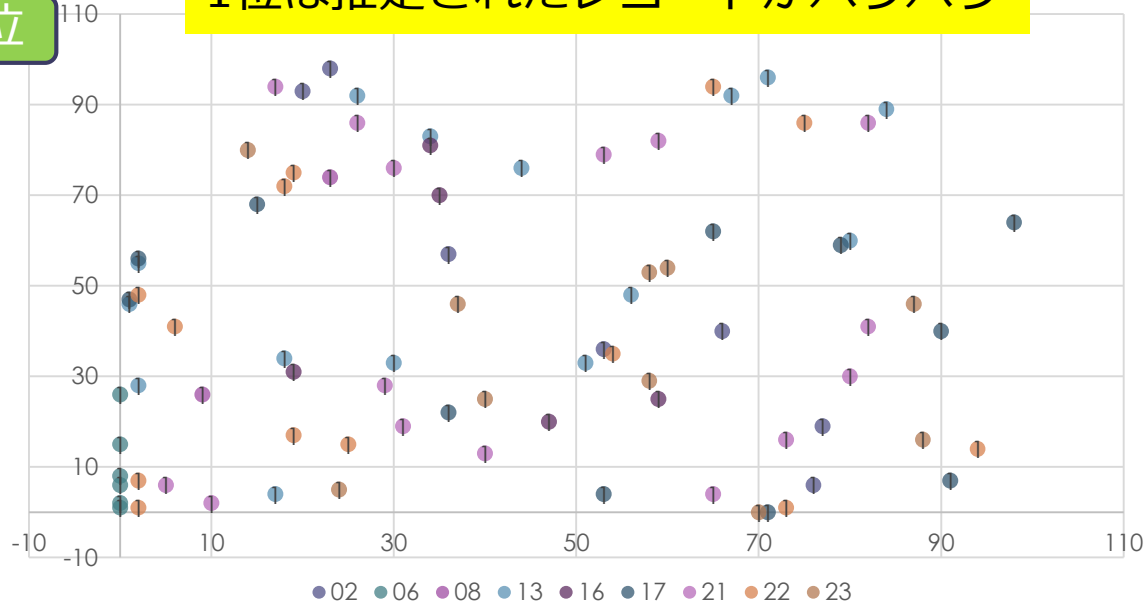


- ▶ 予備戦匿名化8位：53 / 100

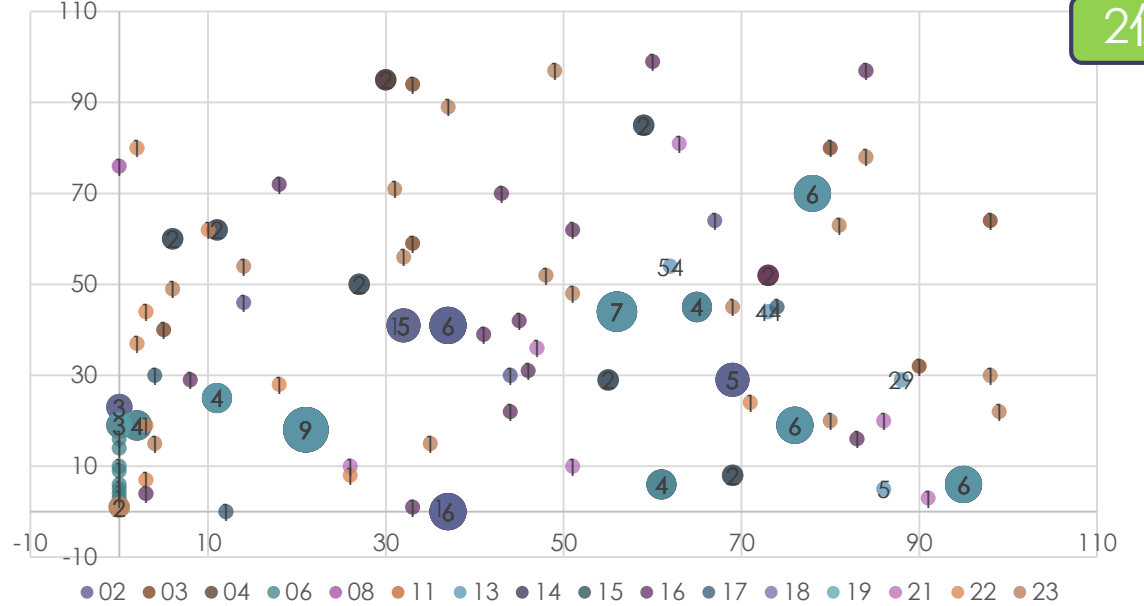
予備戦の匿名化部門上位の傾向 (参考)

1位

1位は推定されたレコードがバラバラ

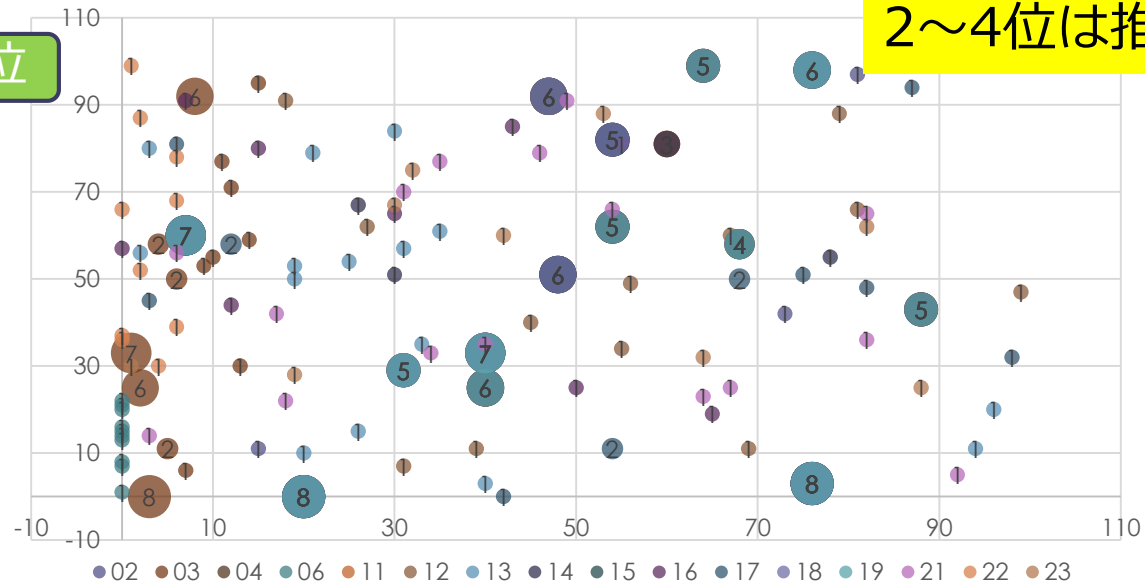


2位

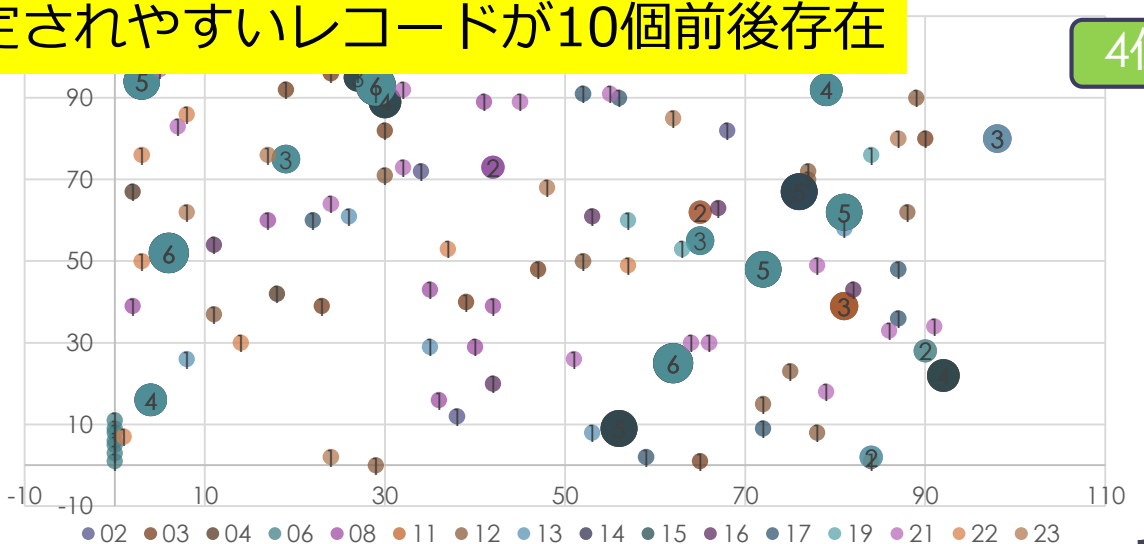


3位

2~4位は推定されやすいレコードが10個前後存在

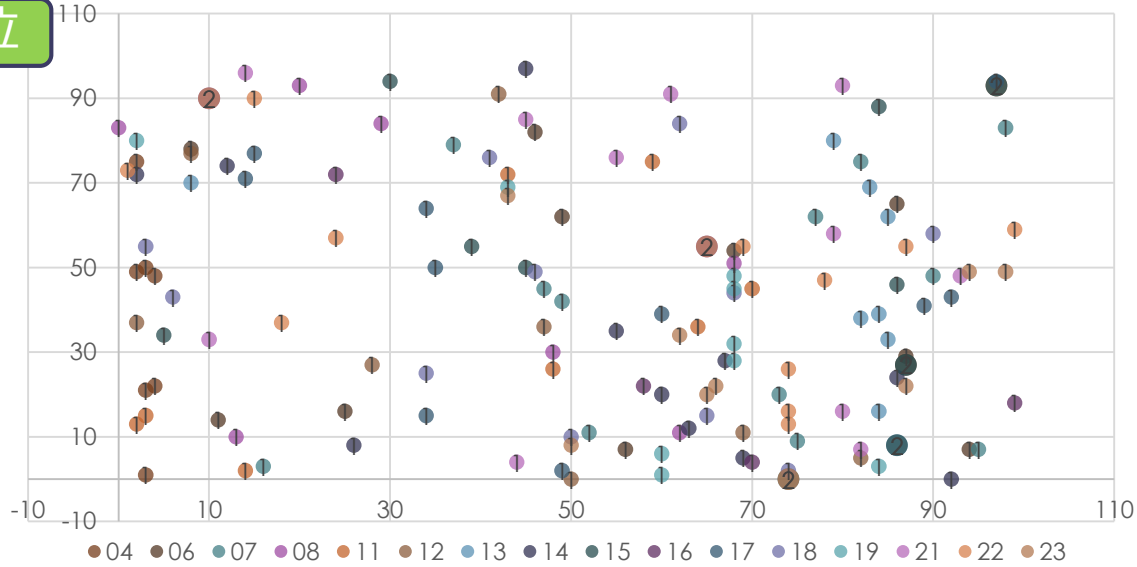


4位

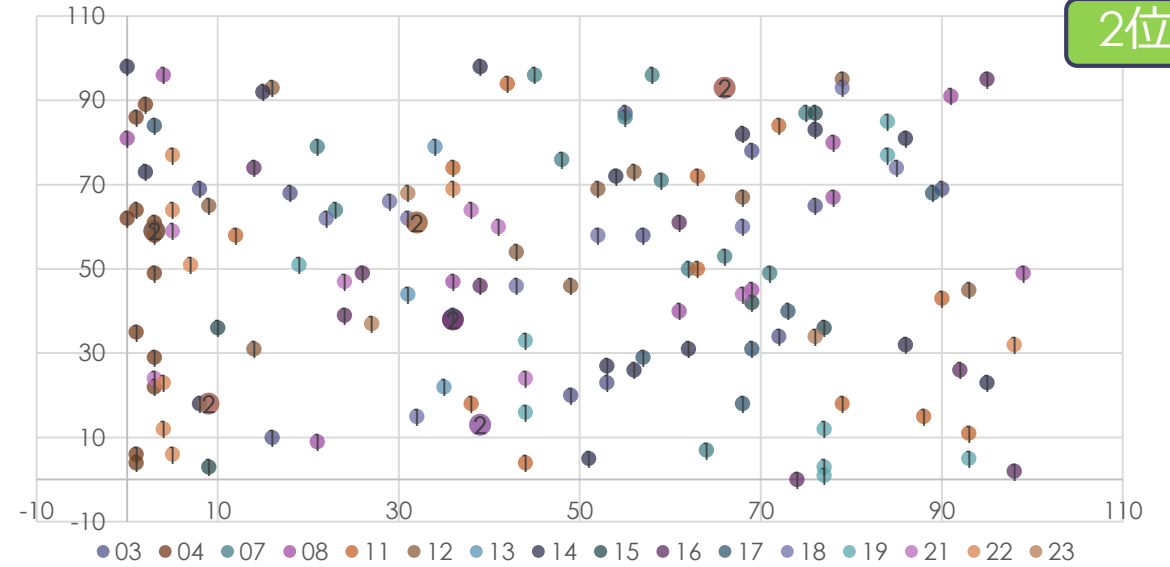


本戦の匿名化部門上位の傾向 (参考)

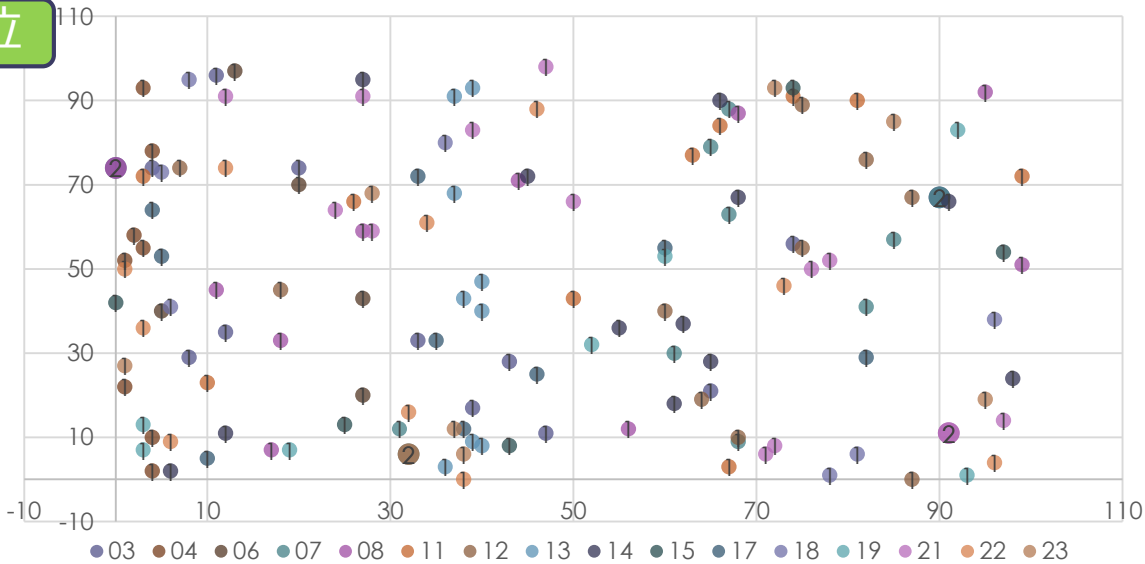
1位



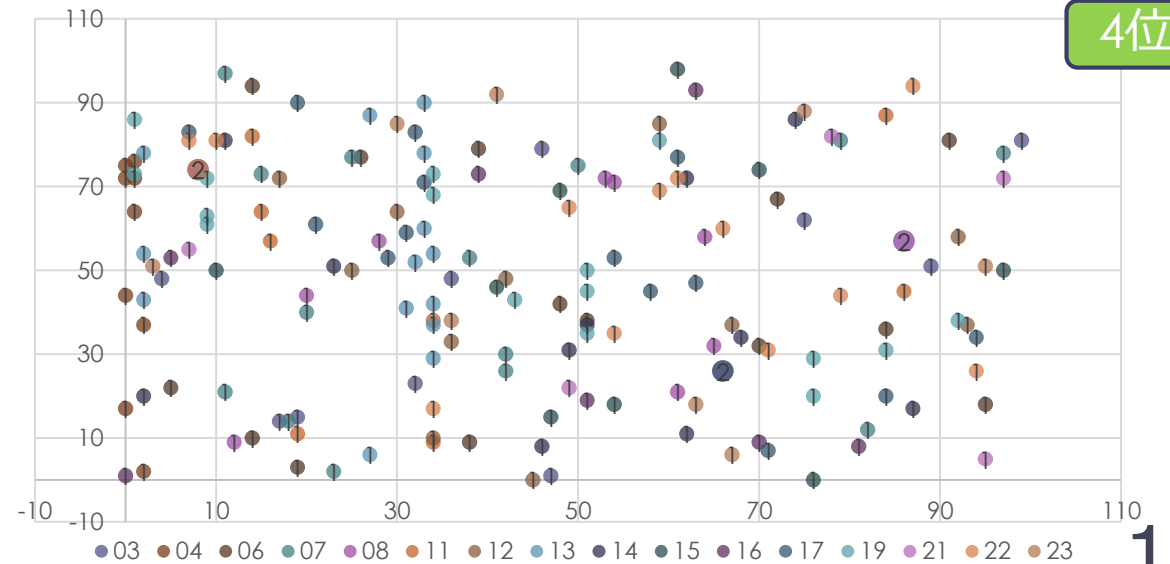
2位



3位



4位



おわりに

- ▶ 厳しい有用性基準でも、匿名性の高い擬似データを作れる可能性を示した
 - ▶ 従来よりも、より使いやすい匿名化データを作成できる可能性
- ▶ 擬似データ生成の新しいアイデアも生まれた
 - ▶ 焼きなまし法、深層学習ベースなど
 - ▶ 個票から生成する方法、統計量から生成する方法
- ▶ 攻撃手法も洗練
 - ▶ サンプルコードは完全一致攻撃と単純な距離ベースの攻撃
 - ▶ 高度な攻撃に進化
- ▶ 今後の方向性（(私)案）
 - ▶ 理論的に安全性を保証できる擬似データ生成の研究
 - ▶ 攻撃手法を蓄積して匿名性基準とする研究
 - ▶ 擬似データと統計情報・匿名加工情報との関係性の研究