PWS : Privacy Workshop（プライバシーワークショップ）
PWS 2025 HP : https://www.iwsec.org/pws/2025/
PWS Cup 2025 HP : https://www.iwsec.org/pws/2025/cup25.html

PWS Cup 2025 について
第2版

2025年8月14日
情報処理学会 コンピュータセキュリティ研究会
PWS組織委員会
PWS2025実行委員会 Cup WG

PWS Cup（2015～）

- 個人データを安全に利活用するための匿名化とその攻撃の技術を競うコンテスト
  - 氏名を削除するだけ等の単純な匿名化では、個人が特定されてしまう場合があります
  - 参加チームのみなさまには、匿名化と攻撃の両方を行ってもらいます
  - 匿名性と有用性の両方を最大限高める匿名化技術を探求してください

元の個人データ（元データ）

氏名	性別	年齢	罹患歴1	・・・
岡山　一郎	男	27	腹痛	・・・
匿　名子	女	38	もやもや病	・・・
森　アミック	男	116	目まい	・・・
⋮	⋮	⋮	⋮	・・・

匿名化

個人特定（攻撃）

個人特定されないよう加工

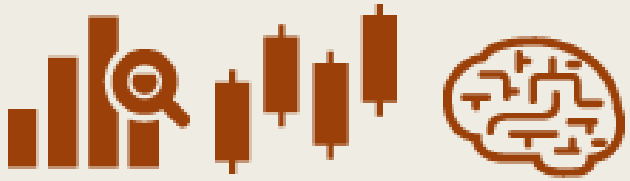
匿名化データ

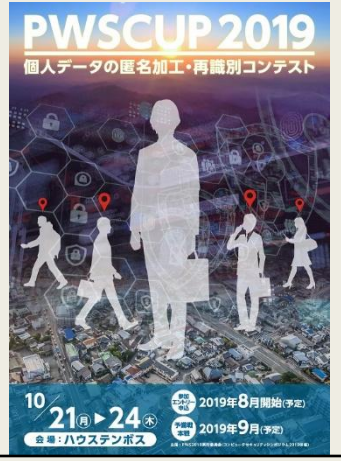
氏名	性別	年齢	罹患歴1	・・・
[redacted]	男	29	腹痛	・・・
[redacted]	女	38	指定難病	・・・
[redacted]	女	90以上	目まい	・・・
[redacted]	⋮	⋮	⋮	・・・

分析

元データと匿名化データの分析結果が近いほどよい（有用性が高い）

分析

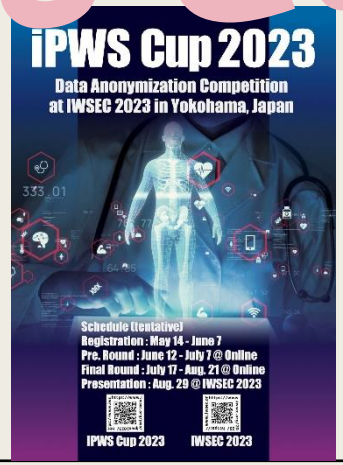




2015	2016	2017	2018	2019	2020
10/21-22 長崎 13チーム	10/11-12 秋田 15チーム	10/23-24 山形 14チーム	10/23-24 長野 14チーム	10/21-24 長崎 21チーム	10/26-29 online 20チーム

これまでの振り返り

祝 10周年



2021	2022	2023 i	2023	2024 i	2024
10/26-29 online 14チーム	10/24-27 熊本 15チーム	8/28 横浜 10チーム	10/30-11/2 福岡 15チーム	9/20 京都 10チーム	10/22-25 神戸 21チーム

PWS Cup 2025 の「４つの特徴」

1. リアリティの高い 架空の患者データ を用いて匿名化と医療分析を実施
   - Synthea　https://synthetichealth.github.io/synthea/
2. 匿名化データと 機械学習モデル を提出
   - 匿名化データから、基本統計や医療分析の有用性を競う
   - 機械学習モデルから、予測の正確性を競う
   - 匿名化データと機械学習モデルから、個人を特定されないようにする
3. 個人特定の攻撃として メンバーシップ推定攻撃 を採用
   - メンバーシップ推定：ある個人のデータが匿名化データや機械学習モデルに使われたかどうか
   - メンバーシップ推定できなければ個人特定もできない
4. １チーム5人まで（学生チームは責任者と指導者の追加OK）
   - 別チームと一緒に議論はOKですが、各チームのデータを教えあうのはNGとします
   - メンバー変更はできません

PWS Cup 参加のメリット

- 最新のデータプライバシー技術（匿名化技術・攻撃技術）を学べる、データ分析や機械学習に触れられる
  - サンプルコード（主にPython）を提供しますので、初心者でも気軽に参加できます
  - 今年は医療・ヘルスケアデータ分析（機械学習含む）がテーマです
- よい技術を創出して論文化、実用化、社会貢献
  - 個人情報保護委員会が毎年後援
- データプライバシーに関する産・学の専門家との交流機会
  - Cup WGメンバー内訳：産13名、学8名
- 入賞すれば → 対外アピール・組織内評価UP・賞状副賞贈呈！
- 【学生さん向け】卒論テーマ、ガクチカでアピール、就職先選択肢拡大(?)

スケジュール

8月6日(水) 18:00～　説明会@zoom
8月6日(水)～**9月15日(月)**：参加申込受付期間

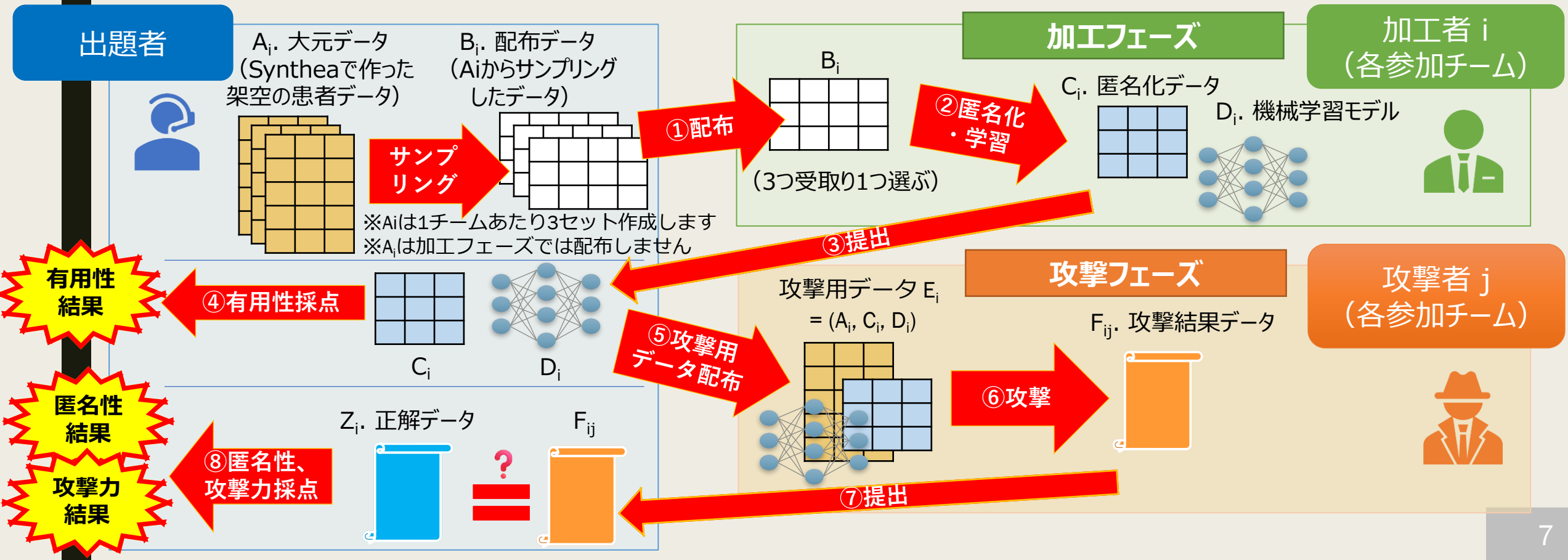
8月20日(水)9:00(JST)～9月1日(月)9:00(JST)
予備戦：匿名化フェーズ
9月4日(木)9:00(JST)～9月15日(月)9:00(JST)
予備戦：攻撃フェーズ

9月19日(金)9:00(JST)～10月3日(金)9:00(JST)
本戦：匿名化フェーズ
10月8日(水)9:00(JST)～10月21日(火)9:00(JST)
本戦：攻撃フェーズ

10月29日(水) 発表会・表彰式@岡山（CSS2025内イベント）

PWS Cup 2025 の基本的な流れ

- 全ての参加チームは「加工フェーズ」（匿名化フェーズ）と「攻撃フェーズ」の両方に参加
- 加工フェーズ：出題者から渡された(架空の)患者データから匿名化データと機械学習モデルを作成して提出
- 攻撃フェーズ：他チームの匿名化データと機械学習モデルを攻撃（メンバーシップ推定）して結果を提出
- 出題者は各チームの有用性、匿名性、および攻撃力の結果を発表



配布データ B_i のイメージ

※ 変更となる可能性があります
（予備戦と本戦で変わる可能性もあります）

受診回数 / 処置回数 / 投薬回数 / 予防接種回数 / アレルギー回数 / 医療機器使用回数 / 喘息歴 / 脳卒中歴 (TIA等含む) / 肥満 / 鬱病歴 / 収縮期血圧平均 (mmHg) / 拡張期血圧平均 (mmHg)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	GENDER	AGE	RACE	ETHNICITY	encounter_count	num_procedures	num_medications	num_immunizations	num_allergies	num_devices	asthma_flag	stroke_flag	obesity_flag	depression_flag	mean_systolic_bp	mean_diastolic_bp	mean_bmi	mean_weight
2	M	2	other	nonhispani	10	2	2	23			0	0	0	0	130.62	86.88		8.12
3	M	37	hawaiian	nonhispani	14	22	3	6	11	3	0	0	0	0	136	85.67	28.6	100.43
4	M	3	hawaiian	hispanic	14	12	3	25			0	0	0	0	139	87.4	36.25	9.03
5	M	28	white	nonhispani	8	49	2	7		2	0	0	0	0	117	92.5	36.5	71.5
6	M	30	other	nonhispani	14	54	5	9		2	0	0	0	0	123.75	74.5	26.18	88.2
7	M	41	asian	nonhispani	20	35	3	6		2	0	0	0	0	148	79.75	29	81.45
8	M	10	white	nonhispani	30	16	8	30	8	1	0	0	0	0	131.06	76.28	19.23	15.87
9	M	33	asian	nonhispani	22	72	24	11		1	0	1	0	0	141.08	82.67	26.89	80.56
10	F	36	asian	nonhispani	35	93	8	6		4	0	0	0	0	116.67	68.67	27.83	73.63
11	F	34	hawaiian	nonhispani	41	118	12	7		3	0	0	0	0	123.75	89	23.45	65.12
12	M	24	white	nonhispani	72	131	6	11	3	3	0	0	0	0	120.5	79.88	37.77	62.15
13	F	3	asian	nonhispani	12	3		26			0	0	0	0	124	81.18	27.48	8.66
14	F	52	native	nonhispani	32	104	28	13		3	0	1	1	0	123.55	78.45	28.1	69.7
15	M	80	other	nonhispani	44	151	11	11	3	7	0	0	1	1	125.7	79.9	27.4	104.4
16	F	70	white	nonhispani	40	127	13	15		16	0	0	1	0	120.91	75.27	27.8	73.4
17	M	8	hawaiian	nonhispani	26	45	6	35		3	0	0	0	0	97.94	79.18	47.24	13.69
18	F	66	native	nonhispani	88	198	87	15		5	0	1	1	0	129.25	83.5	29	92.18
19	F	68	white	nonhispani	109	181	52	14		2	0	1	1	0	121.89	84.11	27.6	68.6
20	M	31	asian	nonhispani	11	52	3	8		2	0	0	0	0	117	69.25	24.62	79.75

（参考）配布データ B_i の作り方　※変更可能性あり

- synthea をインストール
- synthea で M 人分のデータを生成（18種類の csv ファイルが作成されます）
  - M=100,000 の想定
  - *./run_synthea –p 100000 Massachusetts –exporter.format=csv*
    - 10万だとファイルサイズが非常に大きくなり時間もかかるので注意（分割生成推奨）
    - B_i ごとに地域（Massachusetts 等）の変更や混合により異なる分布のデータにする
      - （州, 地名）の組で 37,142 通りある
- 18種の各csvファイルにある同一キーで、同じ人のデータを結合・加工してデータ A_i を生成
  - 結合・加工方法は unified_synthea.py のソースコードを参照
  - M レコード（1人1レコード）の単一 csv ファイルデータ A_i が作成される
  - Ai は2種類の（州, 地名）のデータの組合わせ。どこのデータかは秘密とする
- A_i から N レコード抽出し、B_i（csvファイル）とする
  - N=10,000 の想定
  - 加工フェーズでは、B_i から N レコードの匿名化データ C_i と機械学習モデル D_i を作成
  - 攻撃フェーズでは、$E_i=(A_i,C_i,D_i)$ から、B_i の N レコードを当てる

（参考）synthea の csv ファイル情報

項番	ファイル名	説明
1	allergies.csv	患者のアレルギーデータ
2	careplans.csv	患者ケア計画データ（目標含む）
3	claims.csv	患者の請求データ
4	claims_transactions.csv	請求ごとの明細項目あたりの取引データ
5	conditions.csv	患者の状態または診断データ
6	devices.csv	患者が装着するデバイスのデータ
7	encounters.csv	患者の診察データ
8	imaging_studies.csv	患者の画像メタデータ
9	immunizations.csv	患者の予防接種データ
10	medications.csv	患者の投薬データ
11	observations.csv	バイタルサインや検査レポートのデータ
12	organizations.csv	病院を含むデータ提供機関のデータ
13	patients.csv	患者のデモグラフィックデータ
14	payer_transitions.csv	支払者移行データ（健康保険の変更など）
15	payers.csv	支払者組織のデータ
16	procedures.csv	手術を含む患者の処置データ
17	providers.csv	患者ケアを提供する医療従事者データ
18	supplies.csv	医療サービス提供に用いられる資材データ

有用性評価項目：基本統計と医療分析　※変更可能性あり

- 基本統計等（0～1に正規化（相関行列の値は-1～1））
  - 数値属性：平均、標準偏差、四分位数
  - カテゴリ属性（年齢をグループ化した属性を含む）：集計
  - カテゴリ属性×カテゴリ属性：クロス集計
  - 数値属性×数値属性：Pearson相関行列
  - カテゴリ属性×数値属性：カテゴリ属性の値毎の数値属性の平均、標準偏差、四分位数
- 医療分析
  - 喘息リスク因子の分析
    - asthma_flag（喘息歴の有無）を目的変数として、ロジスティック回帰で多変量解析。AUC、p値、オッズ比、95%信頼区間を算出し、0～1に正規化
  - 年齢群別にみる医療利用の分布差解析
    - 年齢を臨床カスタム区切りでビニングし、各医療指標に対してKruskal–Wallis検定を実施。数値安定なp値とともに、効果量（ε^2・η^2・順位η^2・Vargha–Delaney A）を算出

有用性評価項目：機械学習モデル　※変更可能性あり

- XGBoostを用いた脳卒中リスク予測
  - 脳卒中フラグ（stroke_flag）以外のデータを入力し、脳卒中リスクを予測する分類器を配布データ B_i から作成
    - 分類器データをjsonファイルとして提出
  - 分類器データの有用性評価軸は、テストデータを入力したときの脳卒中リスク予測結果と正解ラベルの一致率（=正解率）
    - 正解率は高い方がよい
    - 詳細は XGBoost の実行スクリプト xgbt.py 参照

得点

- 予備戦の得点×0.1+本戦の得点×0.9が高い順に順位を決定
- 匿名性の得点（方針）
  - 0～100点（マイナスは0点に補正）
  - 最もメンバーシップ推定に成功したチームの正解数×0.01を減点
  - 各レコードについて、より多くのチームに正解されるほどさらに減点（最大でLチームに正解されたレコードがある → L-1点減点）
    - 犠牲者を出さず、全員のプライバシーを守るように加工する必要がある
- 有用性の得点（方針）
  - 0～100点（小数点第3位を四捨五入）
  - 有用性評価項目で挙げた、基本統計、医療分析（2種）、機械学習の結果に基づき得点化（元のデータから得られる結果との差異が少ないほど得点が高い）
    - 基本統計、医療分析（2種）はそれぞれ各値を0～1に正規化し（相関係数は-1～1）、B_i, C_iそれぞれから得られる正規化値の差の最悪値を1から引いた値をベーススコア（マイナスは0に補正）とし、下記の満点値を乗算
    - 機械学習は、B_iから5,000行、(A_i-B_i)から5,000行抽出してテストデータとし、学習結果とテストデータ正解ラベルの一致数を0.0001倍した値に下記の満点値を乗算
    - 基本統計40点満点、医療分析それぞれ20点満点、機械学習20点満点
- 総合得点：匿名性の得点＋有用性の得点（0～200点）
- 攻撃力：総合得点の上位５チームに対する攻撃の得点を加算した値（0～500点）
  - 自分のチームの攻撃の得点は、他チームが自分のチームを攻撃した最高得点とする

サンプルデータ・サンプルコード

- https://github.com/pwscup/pwssite/tree/gh-pages/2025/sample を参照
- 随時追加や更新されますので、更新日時を確認して最新版を利用するようにしてください。
- 予備戦開始（8/20）後に追加または更新した場合はチーム代表者に連絡します。

表彰

- 総合1位～5位
  - 匿名性の得点＋有用性の得点が高かった順
  - 何位まで表彰するか、参加チーム数に応じて多少変動する可能性あり
- ベストアタック賞：攻撃力が最も高かったチーム
- ベストプレゼン賞：当日のプレゼンが最も優れていたチーム。複数の審査員で判定
- ベストデータサイエンティスト賞
  - 実際に今回の匿名化データを使って有用な分析手法を提案したチーム
  - 分析手法の独創性や実用性、匿名化データを使った分析の有用性等を総合的に評価
  - 当日のプレゼンで提案。発表するかどうかは任意
- 贈呈
  - 賞状：上記受賞チーム全て
  - 副賞（岡山に関する何か）：総合上位、ベストアタック、ベストプレゼンの各チーム

CodaBench

- 今年もコンペ用プラットフォーム CodaBench を利用します
- サイト作成中です
- 昨年のサイトをご参照ください
  https://www.codabench.org/competitions/3262/

参加方法

- PWS Cup 2025 HP https://www.iwsec.org/pws/2025/cup25.html の「参加申込ページをオープンしました」をクリックして参加申込ページから申込してください
  - ダイレクトURL https://forms.gle/inyw1whwWA7agX3D7

岡山でお会いしましょう！

https://www.iwsec.org/css/2025/outline.html