- 18時開始です
- 録画します（後日視聴できるようにします）
- AI議事録（AI Companion）を使います
- 字幕機能を使います

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

2025年8月6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

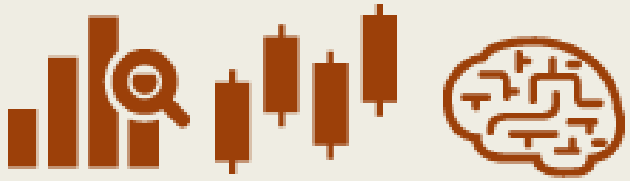
匿名化データ

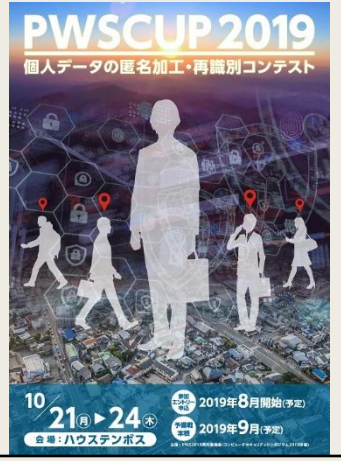
氏名	性別	年齢	罹患歴1	・・・
[redacted]	男	29	腹痛	・・・
[redacted]	女	38	指定難病	・・・
[redacted]	女	90以上	目まい	・・・
[redacted]	⋮	⋮	⋮	・・・

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

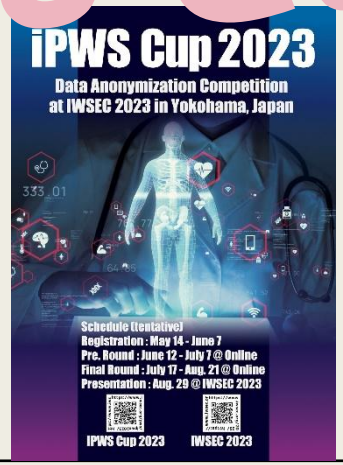




2015	2016	2017	2018	2019	2020
10/21-22 長崎 13チーム	10/11-12 秋田 15チーム	10/23-24 山形 14チーム	10/23-24 長野 14チーム	10/21-24 長崎 21チーム	10/26-29 online 20チーム

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
   - Aさん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）

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

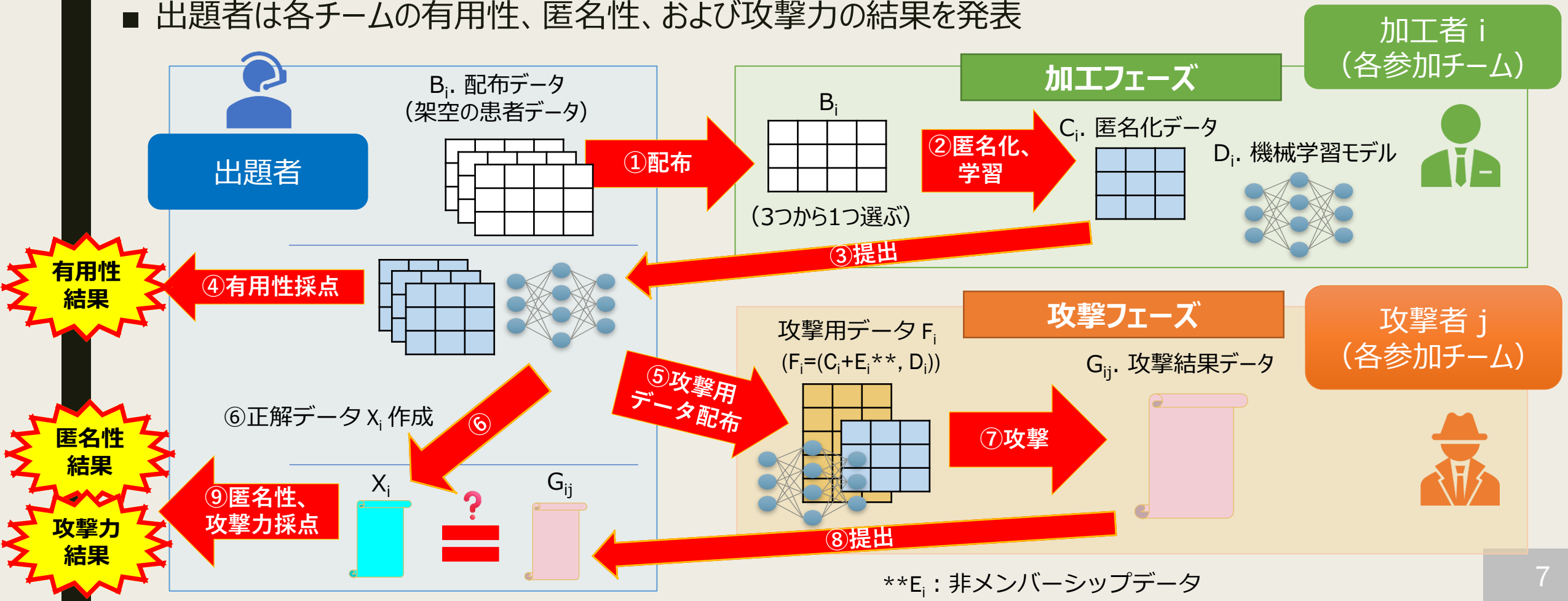
8月20日(水)9:00(JST)～9月1日(月)9:00(JST)
予備戦：匿名化フェーズ
9月4日(木)9:00(JST)～9月15日(月)9:00(JST)
予備戦：攻撃フェーズ

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）

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	gender	ethnicity	marital_status	race	income_level	age	encounter_count	num_procedures	num_medications	num_immunizations	num_allergies	num_devices	asthma_flag	obesity_flag	depression_flag	mean_respiratory_rate	mean_oxygen_saturation	mean_height	mean_weight
2	M	hispanic		white	4185	6	17	22	2	33		1	0	0	0	14.27		83.31	21.08
3	M	nonhispanic	M	white	32965	44	18	43	4	9		1	0	0	0	14.50		173.30	83.78
4	M	nonhispanic	D	white	677085	43	15	42	3	10		2	0	0	0	13.80		174.80	86.52
5	F	nonhispanic		white	43589	2	14	4	5	24	10		0	0	0	14.78		66.00	28.50
6	F	nonhispanic	M	white	79791	34	16	38	3	7	2	2	0	0	0	15.00		165.50	79.90
7	F	nonhispanic		black	49450	55	33	109	5	10		1	0	0	0	14.33		164.62	55.91
8	F	nonhispanic	M	white	92038	52	34	71	14	13	2	3	0	1	0	14.17		161.90	75.10
9	F	nonhispanic		white	138398	19	22	88	5	17		7	0	0	0	13.90		152.24	41.90
10	M	nonhispanic	M	white	137567	56	21	60	4	13		1	0	1	0	14.63		169.40	84.01
11	M	nonhispanic	M	white	21855	44	20	70	2	9		9	0	0	0	14.56	79.5	175.00	88.90
12	F	nonhispanic	S	white	199848	53	28	72	6	13	1	4	0	0	0	14.25		159.90	70.90
13	M	hispanic	S	white	14125	57	21	93	23	12		5	0	1	0	14.11		170.60	79.90
14	M	nonhispanic	M	white	74201	37	24	79	4	10		5	0	0	0	14.86	80.1	170.00	75.77
15	M	nonhispanic	S	white	109480	35	21	96	4	8		8	0	0	0	13.80		179.60	87.94
16	M	nonhispanic		white	143691	0	2	2		2			0	0	0	14.50		58.50	3.88
17	M	nonhispanic		white	75159	1	6	3		17			0	0	0	14.00		62.17	45.14
18	F	nonhispanic	M	white	47774	49	80	115	11	12	4	5	0	1	0	13.50		158.50	71.53
19	F	hispanic	M	white	170893	53	60	146	4	13		1	0	0	0	13.86		160.30	71.50
20	F	nonhispanic	S	white	1356	62	37	156	15	11		5	0	0	0	14.20		169.00	75.10
21	F	nonhispanic		other	88499	1	5	2		17			0	0	0	13.40		60.66	47.94
22	M	nonhispanic	M	white	71555	34	34	129	36	11		6	0	0	0	14.36		173.10	81.11
23	F	nonhispanic	M	white	39700	40	56	231	33	13	6	7	0	1	0	13.60		162.00	76.11
24	F	nonhispanic	S	white	82077	57	55	145	21	13	2	4	0	1	0	13.94		152.60	67.49
25	M	hispanic		white	112745	9	23	19	4	35			0	0	0	13.82		92.35	39.63

（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
- 18種類のcsvファイルを同一キーで結合して加工
  - unified_synthea.py（後日公開）参照
  - Mレコード（1人1レコード）の単一csvファイルが作成される
- MレコードからNレコード抽出し、B_i（csvファイル）とする
  - N=10,000 の想定
  - 攻撃フェーズでは、Mレコードの単一csvファイルと、B_i から作られたNレコードの匿名化データと機械学習モデルから、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
  - 各属性の集計値、平均、分散、四分位数
  - 複数属性のクロス集計値、共分散行列
- 医療分析
  - 肥満とバイタル値の関係
    - 性別（gender）ごとに、肥満かどうか（obesity_flag）で2群に分け、身長（mean_height）、体重（mean_weight）、呼吸数（mean_respiratory_rate）、酸素飽和度（mean_oxygen_saturation）でp値、t値を導出
  - 年齢と診療回数・医療利用の相関分析
    - 年齢（age）と診療回数（encounter_count）、投薬種類数（num_medications）、医療処置件数（num_procedures）、予防接種回数（num_immunizations）、医療機器装着・使用回数（num_devices）についてピアソン相関係数とp値およびスピアマン順位相関のp値を導出
  - 喘息患者の要因分析（ロジスティック回帰）
    - 喘息の有無（asthma_flag）を目的変数、性別（gender）、民族（ethnicity）、婚姻状態（marital_status）、人種（race）、収入レベル（income_level）、年齢（age）、肥満フラグ（obesity_flag）を説明変数とし、オッズ比とp値を導出

有用性評価項目：機械学習モデル　※変更可能性あり

- XGBoostを用いた肥満分類
  - 肥満フラグ（obesity_flag）以外のデータを入力し、肥満かどうか分類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肥満フラグの正解率と各属性の特徴量重要度（正規化した値）
    - 正解率は高い方がよく、重要度はBiからそのまま作成した分類器の結果に近い方がよい
    - XGBoostの実行スクリプト xgbt.py（後日公開）参照（下表は出力例）
    - テストデータは、B_i を含むMレコードから抽出

Accuracy (正解率): 0.8405		
特徴量名	Gain	正規化重要度
Age	7.6046	0.3318
mean_weight	1.8915	0.0825
race_white	1.7479	0.0763
marital_status_D	1.4435	0.0630
mean_height	1.2723	0.0555
gender_F	0.9756	0.0426
・・・	・・・	・・・

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
  - 最もメンバーシップ推定に成功したチームの正解率×100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
  - 有用性評価項目で挙げた、基本統計、医療分析、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）
- 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

サンプルコード

- 近日中に公開予定です…

- 公開予定のサンプルコード
  - 匿名化データ作成コード
  - 機械学習モデル作成コード
  - メンバーシップ推定攻撃コード（匿名化データ用）
  - メンバーシップ推定攻撃コード（機械学習モデル用）
  - 有用性評価コード
  - 基本統計処理コード
  - 医療分析コード
  - 機械学習分類コード

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