PWS Cup 2024 & iPWS Cup 2024
ルール説明 Ver 1.1

Ver 1.1 2024年7月23日
Ver 1.0 2024年7月12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
PWS2024実行委員会 Cup WG

※ PWS : Privacy Workshop（プライバシーワークショップ）
※ PWS2024 HP → https://www.iwsec.org/pws/2024/

PWS Cup & iPWS Cup

※ iPWS Cup：PWS Cup の国際版

- 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
  - 単純な匿名化では、個人が特定されたり、機微な情報が復元される場合があります
  - 参加チームのみなさんには、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方法を探求してください
- 対戦形式：**Ice**（匿名化） vs. **Fire**（攻撃）

元の個人データ（元データ）

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

匿名化

個人特定・復元（攻撃）

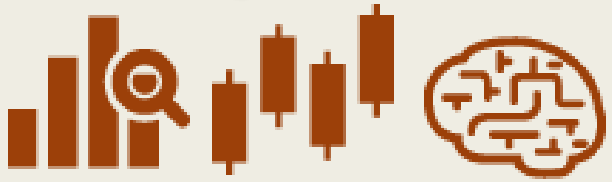
個人特定・元データ復元されないよう加工

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

分析

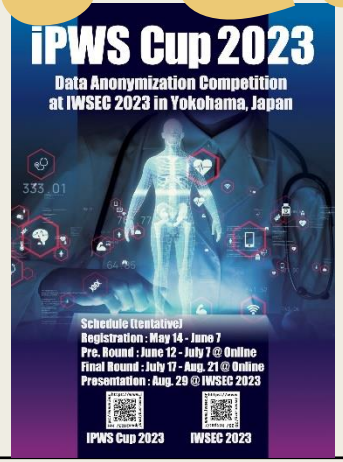


元データと匿名化データの分析結果が近いほどよい（有用性が高い）

これまでの振り返り

祝 10周年

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



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 ??チーム	10/22-25 神戸 ??チーム

PWS Cup & iPWS Cup（補足）

- PWS Cup 20XX（2015～）
  - サンプルコード（Pythonが多い）があるので、初心者でも気軽に参加できます
  - データ分析とセキュリティ・プライバシーに興味がある方に特にお勧めです
  - 入賞チームには賞状・副賞贈呈！
  - 主催：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 PWS2024実行委員会 Cup WG
- iPWS Cup 20XX（2023～）
  - PWS Cup の国際版です（2023年は国内6チーム、海外4チーム参加）
  - 良くも悪くも英語に触れる機会が増えます
  - ルールは基本的に PWS Cup と同じです
  - 今年は PWS Cup 2024 と同一テーマで、時期も PWS Cup と同じです
  - PWS Cup と両方の参加がお得です（推奨）
    - 入賞のチャンスが増えます（iPWS Cup では入賞チームに賞金(VISA Gift Card)・賞状・副賞贈呈します）
    - ルールは基本的に同じなので、両方参加しても手間はあまり増えません
    - 各チーム1名は CSS2024（国内シンポジウム）と IWSEC2024（国際会議）に参加登録が必要です

スケジュール

PWS Cup 2024
https://www.iwsec.org/pws/2024/cup24.html

iPWS Cup 2024
https://www.iwsec.org/pws/ipws2024/

7月12日(金) 16:00～　説明会@zoom
7月12日(金)～7月24日(水)：エントリー期間（各HP参照）

7月26日(金)9:00(JST)～8月13日(火)9:00(JST)
予備戦：匿名化フェーズ
8月16日(金)9:00(JST)～9月3日(火)9:00(JST)
予備戦：攻撃フェーズ

9月10日(火)9:00(JST)～9月25日(水)9:00(JST)
本戦：匿名化フェーズ
10月1日(火)9:00(JST)～10月16日(水)9:00(JST)
本戦：攻撃フェーズ

10月22日(火)～10月25日(金)
のうち１日
発表会・表彰式
@神戸（CSS2024内イベント）

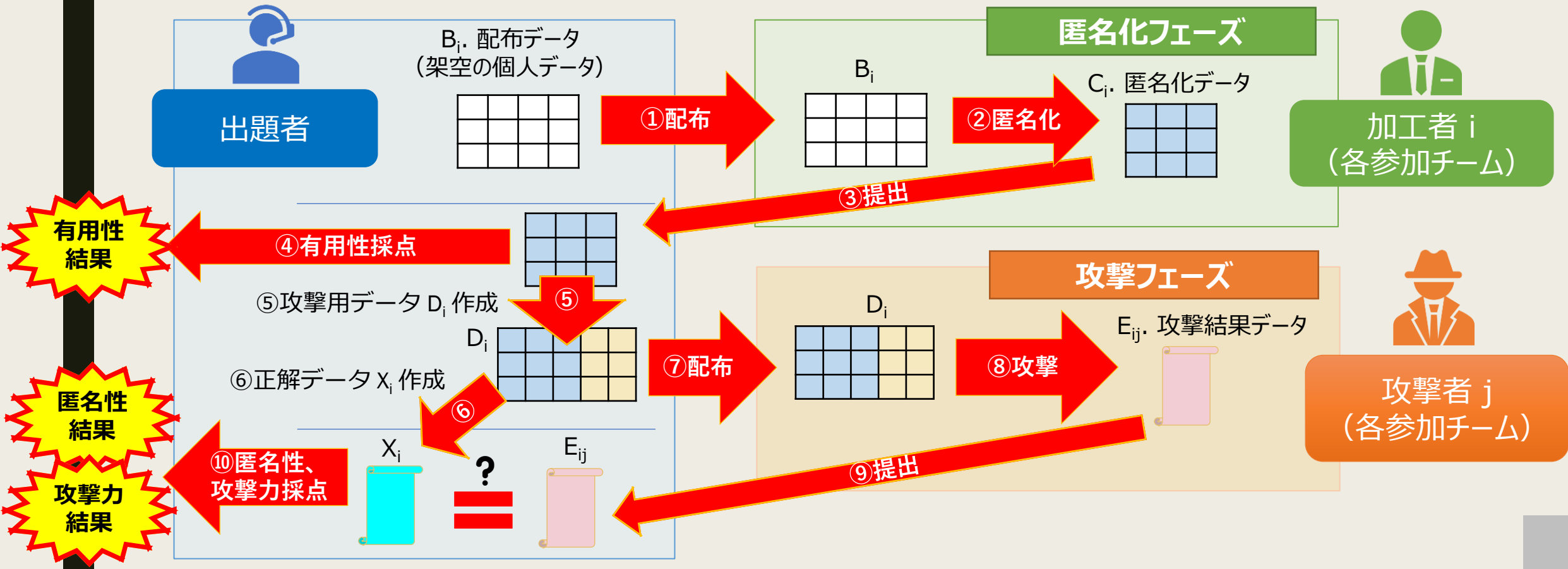
7月26日(金)9:00(JST)～8月17日(土)9:00(JST)
本戦：匿名化フェーズ
8月20日(火)9:00(JST)～9月10日(火)9:00(JST)
本戦：攻撃フェーズ

9月20日(金)
発表会・表彰式
@京都 (IWSEC2024併設イベント)

IWSEC2024 https://www.iwsec.org/2024/
CSS2024 https://www.iwsec.org/css/2024/

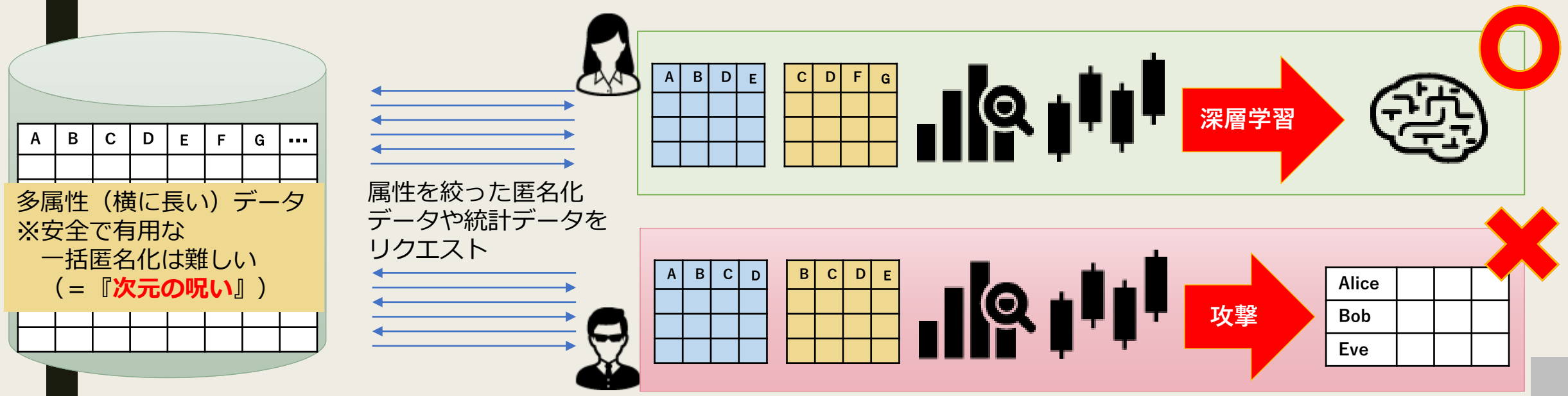
基本的な流れ

- 全ての参加チームは「匿名化フェーズ」と「攻撃フェーズ」の両方に参加
- 匿名化フェーズ：出題者から渡された（架空の）個人データを匿名化して提出
- 攻撃フェーズ：他チームの匿名化データの攻撃結果を提出
- 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



PWS Cup 2024 & iPWS Cup 2024 のテーマ

- 昨今問題となっている「データベース（DB）再構築攻撃」に対して安全なデータ群を作成
  - DB再構築攻撃：ある DB から都度必要な属性のみ抽出して加工・提供される匿名化データや統計データを組み合わせて、DB 内のデータを不正に復元する攻撃
- 映画レビューデータ MovieLens https://grouplens.org/datasets/movielens/ を用いて、DB再構築攻撃や個人特定攻撃を防ぎつつ、有用性の高い匿名化データを作成する
  - Netflix 問題 https://www.anonify.layerx.co.jp/post/differential-privacy のように、単純な匿名化では別のデータと突き合わせて個人特定されてしまう恐れがある



利用するデータ

- 映画レビューデータセット MovieLens https://grouplens.org/datasets/movielens/ の MovieLens 1M Dataset (Released 2/2003)
  - movies.dat
    - Movie ID, Title, Genres
    - 3,952作品、18ジャンル (Action, Adventure, Animation, …) [複数選択可]
  - ratings.dat
    - User ID, Movie ID, Rating (1 – 5), Timestamp
    - 6,040ユーザ、1,000,209レコード
    - 全ユーザが20作品以上は Rating を付けている (最大2,314作品)
  - users.dat
    - User ID と基本属性（Gender(M/F), Age, Occupation, ZIP-code）
    - Ageは7種：1(Under 18), 18(18-24), 25(25-34), 35(35-44), 45(45-49), 50(50-55), 56(56+)
    - Occupationは21種：0(other or not specified), 1(academic/educator), …, 20(writer)
    - ZIP-codeは5桁：米国では1桁目は州のグループ、2-3桁目は区域、4-5桁目は配達先グループ

利用するデータ（続き）

- MovieLens 1M Dataset を扱い易くするため以下の加工を行う
  - ジャンルに "Fantasy" を含む作品のみ抽出
    - 46作品、4,850人視聴
  - 属性は以下の51種
    - User ID（架空の氏名に変換予定）
    - 基本属性：Gender (M/F), Age (7種), Occupation (21種), ZIP-code(3桁目まで)
    - 46作品それぞれの Rating (1～5)　※視聴なしは0とする
  - 1人1レコードの単一 csv ファイルにする（51列のデータ）
  - 5作品以上Ratingをつけている1,920レコードを抽出
  - 以上の加工を施したデータを "**元データ A**" として公開する
    - 元データ A = "A.csv" を公開
- **配布データ B_i** は、各チーム別々のデータとなるよう、元データ A から作成された合成データとする
  - 他チームの配布データの中身は分からないようにする
  - レコード数を1,920から10,000に増やす（架空の1万人データ）
    - 配布データ Bi サンプル = "sampleBi.csv" を公開
  - 配布データは元データと分布が大きく異なるので注意
  - 公平性のため、B_i は各チームが選べるようにする

ジャンル	映画数	視聴者数
Action	402	6,012
Adventure	234	5,894
Animation	71	4,808
Children's	179	5,283
Comedy	938	6,031
Crime	171	5,662
Documentary	90	2,243
Drama	1,168	6,037
Fantasy	46	4,850
Film-Noir	33	4,150
Horror	251	5,300
Musical	84	4,754
Mystery	83	5,133
Romance	367	5,961
Sci-Fi	220	5,911
Thriller	375	5,989
War	139	5,769
Western	56	4,100

元データ A のイメージ

Movie ID（46個の映画作品ID）

51列

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	User ID	Gender	Age	Occupatic	ZIP-code	2	56	247	260	653	673	810	885	1009	1073	1097	1126	1525	1654	1702	1750	1881	1920	1967	2(
2	0	M	1	0	296	0	3	4	5	1	5	4	5	3	2	5	0	5	4	2	5	4	4	2	
3	1	M	18	19	390	3	3	5	5	1	0	4	0	5	0	1	2	0	0	0	5	1	3	3	
4	2	M	25	15	27	3	0	4	5	0	0	1	2	1	3	2	4	1	0	1	1	0	2	4	
5	3	F	1	2	316	4	3	1	5	5	0	0	5	3	1	4	1	3	3	0	5	4	4	0	
6	4	M	45	9	725	4	1	0	1	5	4	0	0	1	4	1	1	0	0	4	2	2	2	0	
7	5	F	18	8	968	4	2	3	1	3	1	2	1	1	3	4	2	3	3	2	5	5	0	0	
8	6	M	50	9	45	2	4	4	3	2	0	2	0	3	5	0	2	2	5	0	1	5	1	5	
9	7	M	50	14	517	2	3	3	4	0	2	0	4	4	1	1	0	4	1	5	2	2	3	4	
10	8	M	18	14	525	2	1	5	3	4	1	0	4	2	1	4	2	4	0	2	1	5	0	4	
11	9	M	18	14	530	0	0	1	2	4	3	0	5	0	1	5	5	0	5	5	1	2	0	2	
12	10	M	25	10	695	2	1	4	2	0	3	4	3	0	2	0	0	5	1	0	3	3	4	1	
13	11	M	56	3	378	4	1	0	1	5	3	0	1	4	2	1	0	1	2	1	1	3	2	2	
14	12	M	18	12	20	1	0	5	2	3	0	2	3	1	5	0	1	4	2	5	5	0	4	2	
15	13	M	25	1	886	0	1	2	0	1	4	0	1	4	4	2	2	5	1	5	4	2	3	2	
16	14	F	18	14	829	1	1	4	5	3	0	4	4	5	5	2	0	2	3	5	1	0	4	2	
17	15	M	18	15	910	4	1	4	4	5	0	3	3	2	0	2	0	0	3	3	0	4	1	3	
18	16	M	50	1	596	2	2	5	2	0	0	4	4	1	5	4	5	0	5	0	2	0	0	5	
19	17	M	35	16	947	1	0	3	2	3	0	0	5	1	2	5	3	0	4	2	3	1	4	2	
20	18	F	25	10	888	4	1	0	5	0	1	1	2	4	1	3	1	1	3	5	4	0	3	1	
21	19	M	18	20	546	0	2	4	2	3	2	0	4	5	2	3	1	5	2	4	1	3	2	3	
22	20	F	1	10	715	5	1	1	3	5	1	0	3	3	1	0	3	2	5	3	2	0	1	4	

1,920行（ヘッダ行除く）

“Fantasy” 映画作品一覧

ID	Title	Genres	View
2	Jumanji (1995)	Adventure|Children's|Fantasy	701
56	Kids of the Round Table (1995)	Adventure|Children's|Fantasy	9
247	Heavenly Creatures (1994)	Drama|Fantasy|Romance|Thriller	477
260	Star Wars, Episode IV - A New Hope (1977)	Action|Adventure|Fantasy|Sci-Fi	2991
653	Dragonheart (1996)	Action|Adventure|Fantasy	612
673	Space Jam (1996)	Adventure|Animation|Children's|Comedy|Fantasy	563
810	Kazaam (1996)	Children's|Comedy|Fantasy	120
885	Bogus (1996)	Children's|Drama|Fantasy	43
1009	Escape to Witch Mountain (1975)	Adventure|Children's|Fantasy	291
1073	Willy Wonka and the Chocolate Factory (1971)	Adventure|Children's|Comedy|Fantasy	1313
1097	E.T. the Extra-Terrestrial (1982)	Children's|Drama|Fantasy|Sci-Fi	2269
1126	Drop Dead Fred (1991)	Comedy|Fantasy	317
1525	Warriors of Virtue (1997)	Action|Adventure|Children's|Fantasy	44
1654	FairyTale, A True Story (1997)	Children's|Drama|Fantasy	87
1702	Flubber (1997)	Children's|Comedy|Fantasy	302
1750	Star Kid (1997)	Adventure|Children's|Fantasy|Sci-Fi	63
1881	Quest for Camelot (1998)	Adventure|Animation|Children's|Fantasy	68
1920	Small Soldiers (1998)	Animation|Children's|Fantasy|War	364
1967	Labyrinth (1986)	Adventure|Children's|Fantasy	554
2017	Babes in Toyland (1961)	Children's|Fantasy|Musical	162
2021	Dune (1984)	Fantasy|Sci-Fi	789
2043	Darby O'Gill and the Little People (1959)	Adventure|Children's|Fantasy	158
2086	One Magic Christmas (1985)	Drama|Fantasy	29
2087	Peter Pan (1953)	Animation|Children's|Fantasy|Musical	594
2093	Return to Oz (1985)	Adventure|Children's|Fantasy|Sci-Fi	276
2100	Splash (1984)	Comedy|Fantasy|Romance	1163
2105	Tron (1982)	Action|Adventure|Fantasy|Sci-Fi	970
2138	Watership Down (1978)	Animation|Children's|Drama|Fantasy	305
2143	Legend (1985)	Adventure|Fantasy|Romance	355
2174	Beetlejuice (1988)	Comedy|Fantasy	1495
2193	Willow (1988)	Action|Adventure|Fantasy	802
2253	Toys (1992)	Action|Comedy|Fantasy	440
2399	Santa Claus, The Movie (1985)	Adventure|Children's|Fantasy	223
2628	Star Wars, Episode I - The Phantom Menace (1999)	Action|Adventure|Fantasy|Sci-Fi	2250
2797	Big (1988)	Comedy|Fantasy	1491
2872	Excalibur (1981)	Action|Drama|Fantasy|Romance	742
2968	Time Bandits (1981)	Adventure|Fantasy|Sci-Fi	1010
3393	Date with an Angel (1987)	Comedy|Fantasy	51
3438	Teenage Mutant Ninja Turtles (1990)	Action|Children's|Fantasy	534
3439	Teenage Mutant Ninja Turtles II, The Secret of the Ooze (1991)	Action|Children's|Fantasy	251
3440	Teenage Mutant Ninja Turtles III (1993)	Action|Children's|Fantasy	188
3466	Heart and Souls (1993)	Comedy|Fantasy	219
3479	Ladyhawke (1985)	Adventure|Fantasy|Romance	542
3489	Hook (1991)	Adventure|Fantasy	722
3877	Supergirl (1984)	Action|Adventure|Fantasy	182
3889	Highlander, Endgame (2000)	Action|Adventure|Fantasy	135

配布データ B_i（合成データ）の作成方法と配布方法

- PrivBayes https://github.com/DataResponsibly/DataSynthesizer/blob/master/DataSynthesizer/lib/PrivBayes.py を用いて、元データ A から合成データを100個作成（データID 00～99）
- 各合成データのハッシュ値 (SHA256) をデータIDとともに開示
- 各チーム、好きなデータIDを３つ選ぶ
  - 重複した場合は、出題者が一チームを選び（早く提出した順の予定）、残りのチームは直後（99の直後は00とする）の空きデータIDに変更
- 全チーム重複なくデータIDが３つ決まったら、出題者がそのデータIDに対応した３個の合成データを配布データ1,2,3として各チームに配布
- 各チームは必要に応じてハッシュ値から配布データ1,2,3の integrity をチェック
- 各チームは配布データ1,2,3から匿名化しやすいデータを自由に１つを選び、それを B_i とし、B_i のデータIDを匿名化データと一緒に提出 → 当該データIDは開示される

【匿名化フェーズ】加工者 i の処理

1. 配布データ B_i から、以下の10パターンの属性の組のサブセットデータ $B_i^{(0)}$～$B_i^{(9)}$ を抽出する
   - 出題者が csv ファイルとして $B_i^{(0)}$～$B_i^{(9)}$ を配布予定
   - 基本属性：Gender, Age, Occupation, ZIP-code

   0. 基本属性, "Action" 作品（260, 653, 1525, 2105, 2193, 2253, 2628, 2872, 3438, 3439, 3440, 3877, 3889）
   1. 基本属性, "Adventure" 作品（2, 56, 260, 653, 673, 1009, 1073, 1525, 1750, 1881, 1967, 2043, 2093, 2105, 2143, 2193, 2399, 2628, 2968, 3479, 3489, 3877, 3889）
   2. 基本属性, "Animation" 作品（673, 1881, 1920, 2087, 2138）
   3. 基本属性, "Children's" 作品（2, 56, 673, 810, 885, 1009, 1073, 1097, 1525, 1654, 1702, 1750, 1881, 1920, 1967, 2017, 2043, 2087, 2093, 2138, 2399, 3438, 3439, 3440）
   4. 基本属性, "Comedy" 作品（673, 810, 1073, 1126, 1702, 2100, 2174, 2253, 2797, 3393, 3466）
   5. 基本属性, "Drama" 作品（247, 885, 1097, 1654, 2086, 2138, 2872）
   6. 基本属性, "Romance" 作品（247, 2100, 2143, 2872, 3479）
   7. 基本属性, "Sci-Fi" 作品（260, 1097, 1750, 2021, 2093, 2105, 2628, 2968）
   8. 基本属性, "Musical" and "Thriller" and "War" 作品（247, 1920, 2017, 2087）
   9. 基本属性, View Top 10 作品（260, 1097, 2628, 2174, 2797, 1073, 2100, 2968, 2105, 2193）

2. 上記の $B_i^{(0)}$～$B_i^{(9)}$ 各々について、以下の加工を自由に行い匿名化データ $C_i^{(0)}$～$C_i^{(9)}$ として提出する
   - レコードシャッフル（複数の行を選び、行ごと値を入れ替え）、スワッピング（同じ列の二つのデータを入れ替え）
   - リコーディング（例：値域が {1,18,25,35,45,50,56} のAgeについて、Age=18のデータを一律1に置き換え）
   - ランダム化（例：Ageの値をドメイン内のランダムな値に置き換え）

【匿名化フェーズ】有用性とサンプル匿名性

- 加工者 i は、$B_i^{(0)}$～$B_i^{(9)}$ に対し、以下の「有用性」と「サンプル匿名性」のスコアがなるべく高くなるような匿名化データ $C_i^{(0)}$～$C_i^{(9)}$ を作成する
  - 「匿名性」のスコアは攻撃フェーズが終わらないと算出できないため、代わりにサンプル匿名性を導入
- **有用性**： $B_i^{(0)}$～$B_i^{(9)}$, $C_i^{(0)}$～$C_i^{(9)}$ について、基本属性×RatingとRating×Ratingの全パターンの2重クロス集計表を作り、$(B_i^{(j)}, C_i^{(j)})$ (j=0,1, … ,9) のクロス集計表の MAE (Mean Absolute Error) の最悪値 MAE_{worst} を用いて、有用性スコアを $(1\text{-}MAE_{worst})\times 100$ とする（0～100点）
- **サンプル匿名性**：21頁記載のサンプル攻撃コードの攻撃成功率 $SampAtk_{succ}$ を用いて、サンプル匿名性スコアを $(1\text{-}SampAtk_{succ})\times 100$ とする（0～100点）
  - サンプル匿名性が高くても匿名性が高いとは限らないが、コンテスト盛り上げのため匿名化フェーズで開示

$B_i^{(0)}$ の Gender × Movie 260 のクロス集計表（$a_{*,*}$は度数）

	0	1	2	3	4	5
F	$a_{F,0}$	$a_{F,1}$	$a_{F,2}$	$a_{F,3}$	$a_{F,4}$	$a_{F,5}$
M	$a_{M,0}$	$a_{M,1}$	$a_{M,2}$	$a_{M,3}$	$a_{M,4}$	$a_{M,5}$

$C_i^{(0)}$ の Gender × Movie 260 のクロス集計表（$b_{*,*}$は度数）

	0	1	2	3	4	5
F	$b_{F,0}$	$b_{F,1}$	$b_{F,2}$	$b_{F,3}$	$b_{F,4}$	$b_{F,5}$
M	$b_{M,0}$	$b_{M,1}$	$b_{M,2}$	$b_{M,3}$	$b_{M,4}$	$b_{M,5}$

$B_i^{(0)}$と$C_i^{(0)}$の Gender×Movie 260のクロス集計表のMAEを意味する

$$MAE_{(0),Gender,260} = \frac{1}{20000}\sum_{i=0}^{5}\left(\left|a_{F,i}-b_{F,i}\right|+\left|a_{M,i}-b_{M,i}\right|\right)$$

【攻撃フェーズ】出題者の処理

- 各チームの元データ B_i からランダムに50レコード選ぶ
- User ID & 基本属性 (Gender, Age, Occupation, ZIP-code) と46作品の Ratings を切り離し（前者を基本属性データ、後者をRatingsデータと呼ぶ）、Ratingsデータの全レコードをランダムシャッフルする
- Ratingsデータの各レコードについて、ランダムに1か所選び黒塗りする（黒塗りはアスタリスク '*' 表示）
- 各チームの匿名化データ $C_i^{(0)}$～$C_i^{(9)}$ および上記の基本属性データと加工されたRatingsデータ（ランダムシャッフル＋黒塗り）の一式を攻撃用データ D_i とし、攻撃者 j に送る

元データ B_i からランダムに選んだ50レコード

基本属性データ | Ratingsデータ

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	User ID	Gender	Age	Occupatic	ZIP-code	2	56	247	260	653	673	810	885
2	0	M	1	0	296	0	3	4	5	1	5	4	5
3	1	M	18	19	390	3	3	5	5	1	0	4	0
4	2	M	25	15	27	3	0	4	5	0	0	1	2
5	3	F	1	2	316	4	3	1	5	5	0	0	5
6	4	M	45	9	725	4	1	0	1	5	4	0	0
7	5	F	18	8	968	4	2	3	1	3	1	2	1
8	6	M	50	9	45	2	4	4	3	2	0	2	0
9	7	M	50	14	517	2	3	3	4	0	2	0	4
10	8	M	18	14	525	2	1	5	3	4	1	0	4
11	9	M	18	14	530	0	0	1	2	4	3	0	5
12	10	M	25	10	695	2	1	4	2	0	3	4	3

Ratingsデータのレコードをランダムシャッフルし、
各行1列ランダムに黒塗り

基本属性データ

	A	B	C	D	E
1	User ID	Gender	Age	Occupatic	ZIP-code
2	0	M	1	0	296
3	1	M	18	19	390
4	2	M	25	15	27
5	3	F	1	2	316
6	4	M	45	9	725
7	5	F	18	8	968
8	6	M	50	9	45
9	7	M	50	14	517
10	8	M	18	14	525
11	9	M	18	14	530
12	10	M	25	10	695

?

加工されたRatingsデータ

2	56	247	260	653	673	810	885
2	4	■	3	2	0	2	0
4	3	1	5	5	■	0	5
3	3	5	■	1	0	4	0
2	1	5	3	4	1	0	■
0	3	4	5	■	5	4	5
0	0	■	2	4	3	0	5
4	■	3	1	3	1	2	1
■	3	3	4	0	2	0	4
3	0	4	5	0	0	■	2
4	1	0	1	■	4	0	0

【攻撃フェーズ】攻撃者 j の処理

- 個人特定攻撃：ランダムシャッフルしたレコードの番号を当てる（0～50点）
- DB再構築攻撃：50か所の黒塗り部分の値を復元する（0～50点）
- 加工者 i に対する攻撃結果データ E_{ij} として、以下に基づく50行2列の csv ファイルを提出する
  - 1列目のk行目には、D_i のRatingsデータのk行目（先頭は0行目でヘッダ行）が、D_i の基本属性の何行目に対応するか（すなわちk行目のRatingsデータはどのユーザのデータか）推定して記入（個人特定攻撃）
  - 2列目のk行目には、D_i のRatingsデータのk行目（先頭は0行目でヘッダ行）の黒塗り部分の値を推定して記入（DB再構築攻撃）
- 攻撃結果データ E_{1j}, E_{2j}, E_{3j}, … を一つの csv ファイル（Nチーム参加の場合、50行×2N列のテーブル）にまとめて提出
  - (2i-1)列目はi番目のチームの個人特定攻撃結果、2i列目はi番目のチームのDB再構築攻撃結果となる
  - 自分のチームの攻撃結果の列は空欄としてください
- 3回まで提出できる（すなわち3回攻撃できる）※最後に3回の攻撃結果の何れかを選び最終提出となる

元データ B_i からランダムに選んだ50レコード

基本属性データ

	A	B	C	D	E
1	User ID	Gender	Age	Occupatic	ZIP-code
2	0	M	1	0	296
3	1	M	18	19	390
4	2	M	25	15	27
5	3	F	1	2	316
6	4	M	45	9	725
7	5	F	18	8	968
8	6	M	50	9	45
9	7	M	50	14	517
10	8	M	18	14	525
11	9	M	18	14	530
12	10	M	25	10	695

Ratingsデータ

	F	G	H	I	J	K	L	M
1	2	56	247	260	653	673	810	885
2	0	3	4	5	1	5	4	5
3	3	3	5	5	1	0	4	0
4	3	0	4	5	0	0	1	2
5	4	3	1	5	5	0	0	5
6	4	1	0	1	5	4	0	0
7	4	2	3	1	3	1	2	1
8	2	4	4	3	2	0	2	0
9	2	3	3	4	0	2	0	4
10	2	1	5	3	4	1	0	4
11	0	0	1	2	4	3	0	5
12	2	1	4	2	0	3	4	3

Ratingsデータのレコードをランダムシャッフルし、
各行1列ランダムに黒塗り

基本属性データ

	A	B	C	D	E
1	User ID	Gender	Age	Occupatic	ZIP-code
2	0	M	1	0	296
3	1	M	18	19	390
4	2	M	25	15	27
5	3	F	1	2	316
6	4	M	45	9	725
7	5	F	18	8	968
8	6	M	50	9	45
9	7	M	50	14	517
10	8	M	18	14	525
11	9	M	18	14	530
12	10	M	25	10	695

?

加工されたRatingsデータ

2	56	247	260	653	673	810	885
2	4		3	2	0	2	0
4	3	1	5	5		0	5
3	3	5		1	0	4	0
2	1	5	3	4	1	0	
0	3	4	5		5	4	5
0	0		2	4	3	0	5
4		3	1	3	1	2	1
	3	3	4	0	2	0	4
3	0	4	5	0	0		2
4	1	0	1		4	0	0

【攻撃フェーズ】得点

- **匿名性**：他チームの攻撃（個人特定＋DB再構築）の最高得点を100から引いた値を匿名性スコアとする（0～100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

以下、再掲

- 個人特定攻撃：ランダムシャッフルしたレコードの番号を当てる（0～50点）
- DB再構築攻撃：50か所の黒塗り部分の値を復元する（0～50点）
- 匿名化フェーズで決まる得点
  - **有用性**： $B_i^{(0)}$～$B_i^{(9)}$, $C_i^{(0)}$～$C_i^{(9)}$ について、基本属性×RatingとRating×Ratingの全パターンの2重クロス集計表を作り、$(B_i^{(j)}, C_i^{(j)})$ (j=0,1, ... ,9) のクロス集計表の MAE (Mean Absolute Error) の最悪値 MAE_{worst} を用いて、有用性スコアを $(1\text{-}MAE_{worst})\times100$ とする（0～100点）
  - **サンプル匿名性**：21頁記載のサンプル攻撃コードの攻撃成功数 $SampAtk_{succ}$ を用いて、サンプル匿名性スコアを $100\text{-}SampAtk_{succ}$ とする（0～100点）
    - サンプル匿名性が高くても匿名性が高いとは限らないが、コンテスト盛り上げのため匿名化フェーズで開示

表彰

- 総合1位～5位
  - 匿名性スコア＋有用性スコアが高かった順
  - 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
- ベストデータサイエンティスト賞（仮称）
  - 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、および匿名化データを使った分析の有用性などを総合的に評価
  - 当日のプレゼンで提案。発表するかどうかは任意

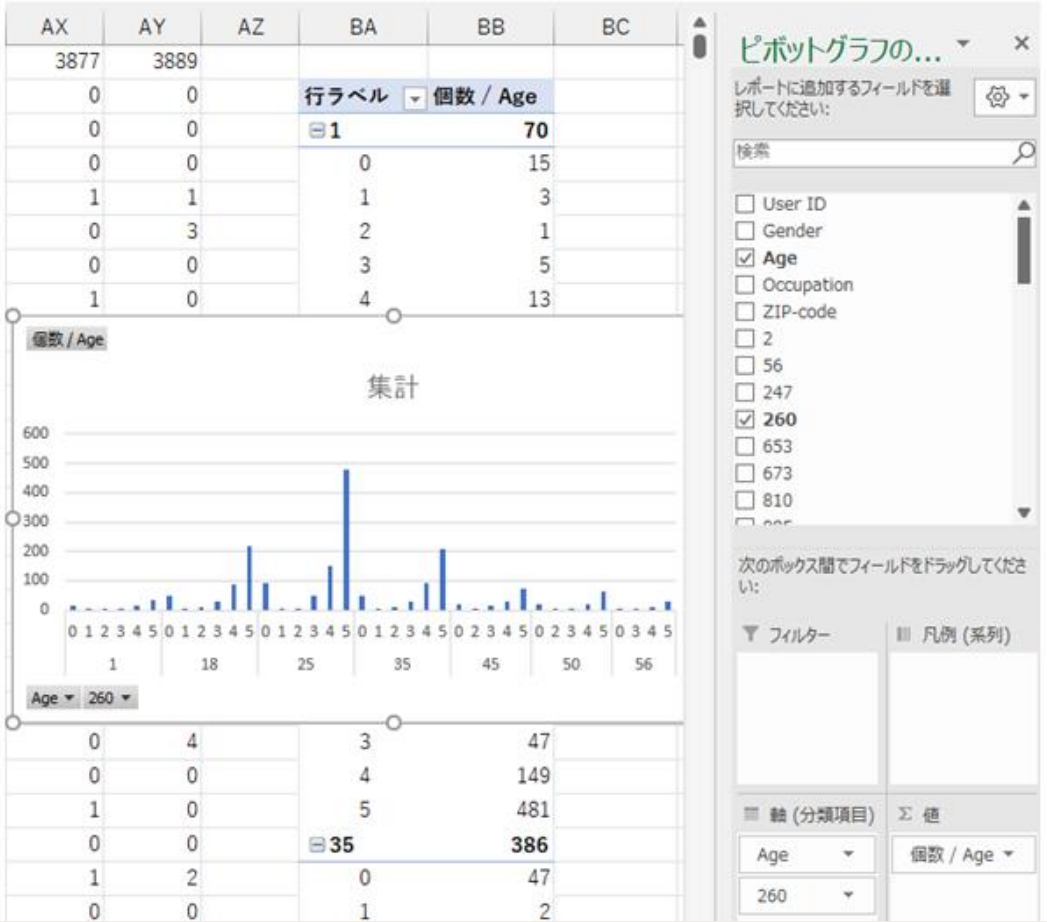
- 贈呈
  - 賞状：上記受賞チーム全て
  - 副賞（京都／神戸にまつわる何か）：総合上位、ベストアタック、ベストプレゼンの各チーム
  - 賞金（VISA Gift Card 総額10万円）※iPWS Cup のみ：総合上位、ベストアタックの各チーム

サンプルデータ

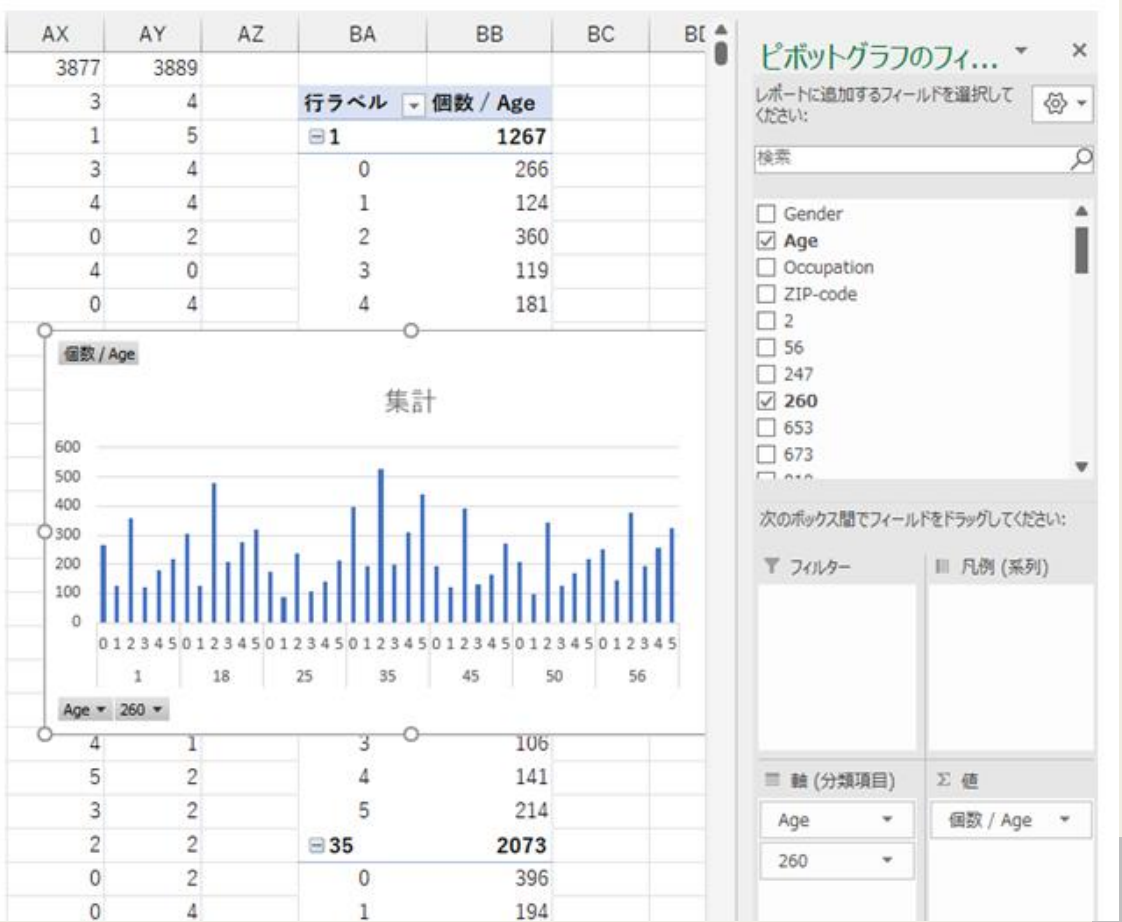
	A	B	C	D	E	F	G	H	I	J
1	Name	Gender	Age	Occupatic	ZIP-code	2	56	247	260	653
2	Waylan Kirton	M	25	8	794	0	3	4	3	5
3	Jamal Seamon	M	50	8	322	0	4	0	3	2
4	Garvy Abyss	M	35	8	975	3	1	3	2	3
5	Arline Morales	F	1	9	140	4	0	5	4	5
6	Babbie Lorroway	F	1	3	942	1	2	1	2	0
7	Corissa Parham	F	56	11	180	0	3	1	0	4

- Bi のサンプルデータ（sampleBi.csv）
  - 元データ A から作った10,000行51列の合成データ（先頭のヘッダ行を入れると10,001行）

元データ A の Age x Movie 260 (Star Wars Episode IV) の分布（クロス集計）



配布データサンプル Bi の Age x Movie 260 (Star Wars Episode IV) の分布（クロス集計）



サンプルコード（Python）

- 匿名化
  - ランダムシャッフル（sampleRandomShuffle.py）
    - csv ファイルを読み込み、行データの順序をランダムに置き換える
    - ただし1行目（ヘッダ行）は置き換えない
  - スワッピング（swapping.py）
    - csvファイルを読み込み、属性名（複数可）と回数nを指定し、指定した属性のデータをランダムに２つ選んで値を入れ替える（これをn回繰り返す）
  - リコーディング（recoding.py）
    - csvファイルを読み込み、属性名（一つのみ）、変更前の値、変更後の値を指定し、変更前の値を変更後の値に一括変換する
    - （変更前の値が変更後の値に統合されるため、一般化と同様の加工とみなせる。ただしクロス集計表のMAEの値が大きくなることに注意）
  - ランダム化（samleRandomization.py）
    - csv ファイルを読み込み、指定した属性のデータをランダム化する
    - 例えば属性Aのデータを選んだとき、属性Aのドメインから要素を１つランダムに選んで置き換える

サンプルコード（Python）

- 攻撃（sampleAttack.py）
  - 個人特定攻撃とDB再構築攻撃を行う
  - 個人特定攻撃
    - 攻撃対象となるUser ID＆基本属性の50レコード (a)、Ratings 50レコード (b)、および$C_i^{(0)}$～$C_i^{(9)}$ を読み込み、$C_i^{(0)}$～$C_i^{(9)}$ の同じ行番号のレコードを連結（T）し（重複する属性は適当に一つ選択）、bの各レコードについて、User IDを除いたaの各レコードを連結し、Tの各行とのハミング距離を求め、最小のハミング距離となったaの行番号を出力する
      - Ratings 50レコードの各行は1列だけ黒塗り（アスタリスク ‘*’ 表示）されているので注意
  - DB再構築攻撃
    - 攻撃対象となるUser ID ＆基本属性の50レコード、Ratings 50レコード、および$C_i^{(0)}$～$C_i^{(9)}$ を読み込み、sampleIdentificationAttack.pyで求めた、$C_i^{(0)}$～$C_i^{(9)}$ の最小ハミング距離の総和が最小となる$C_i^{(0)}$～$C_i^{(9)}$ のレコードのデータを出力する
      - Ratings 50レコードの各行は1列だけ黒塗り（アスタリスク ‘*’ 表示）されているので注意
  - 個人特定攻撃の結果は1列目に、DB再構築攻撃の結果は2列目に記されたcsvファイルを出力する

管理用コード（参加チームも利用可能）

- 得点計算
  - 有用性（utilityScore.py）
    - 元データ B_i と匿名化データ $C_i^{(0)}$～$C_i^{(9)}$を入力し、基本属性×Rating、Rating×Ratingの全ての2重クロス集計のMAEを計算し、その最悪値 MAE_{worst} (0～1) を用いて有用性スコア $S_{\mathrm{util},i} = (1 - \mathrm{MAE}_{\mathrm{worst}}) \times 100$ を計算して出力する
  - 攻撃（attackScore.py）
    - 攻撃結果データ E_{ij} と正解データ X_i を入力し、一致している個数を攻撃スコアとして出力
      - E_{ij} と X_i はともに50行2列のデータ
    - 全チーム分の攻撃結果データを一つのcsvファイルにまとめ、一括で攻撃スコアを出せるようにする
  - サンプル匿名性（sampleAnonymity.py）
    - 攻撃用データ D_i と正解データ X_i を入力し、sampleIdenticationAttack.py と sampleDBReconstructionAttack.py を実行して攻撃結果データ E_{ij} を求め、attackScore.py の出力 $\mathrm{SampAtk}_{\mathrm{succ}}$（0～100） を用いて匿名性のスコア $S_{\mathrm{anon},i} = 100 - \mathrm{SampAtk}_{\mathrm{succ}}$ を計算して出力する
- チェッカー
  - C_i（checkCi.py）
    - 匿名化データ Ci の形式が正しいかチェックする
  - 元データ B_i 、攻撃用データ D_i 、攻撃結果データ E_{ij} 、正解データ X_i のチェッカーも順次作成予定
  - ハッシュ値生成（genHash.py）
- テーブル操作
  - B_iから$B_i^{(0)}$～$B_i^{(9)}$を作成（split.py）

参加方法

- PWS Cup 2024 HP https://www.iwsec.org/pws/2024/cup24.html の「参加方法」を参照
- CodaBench というコンペ用プラットフォームを利用します

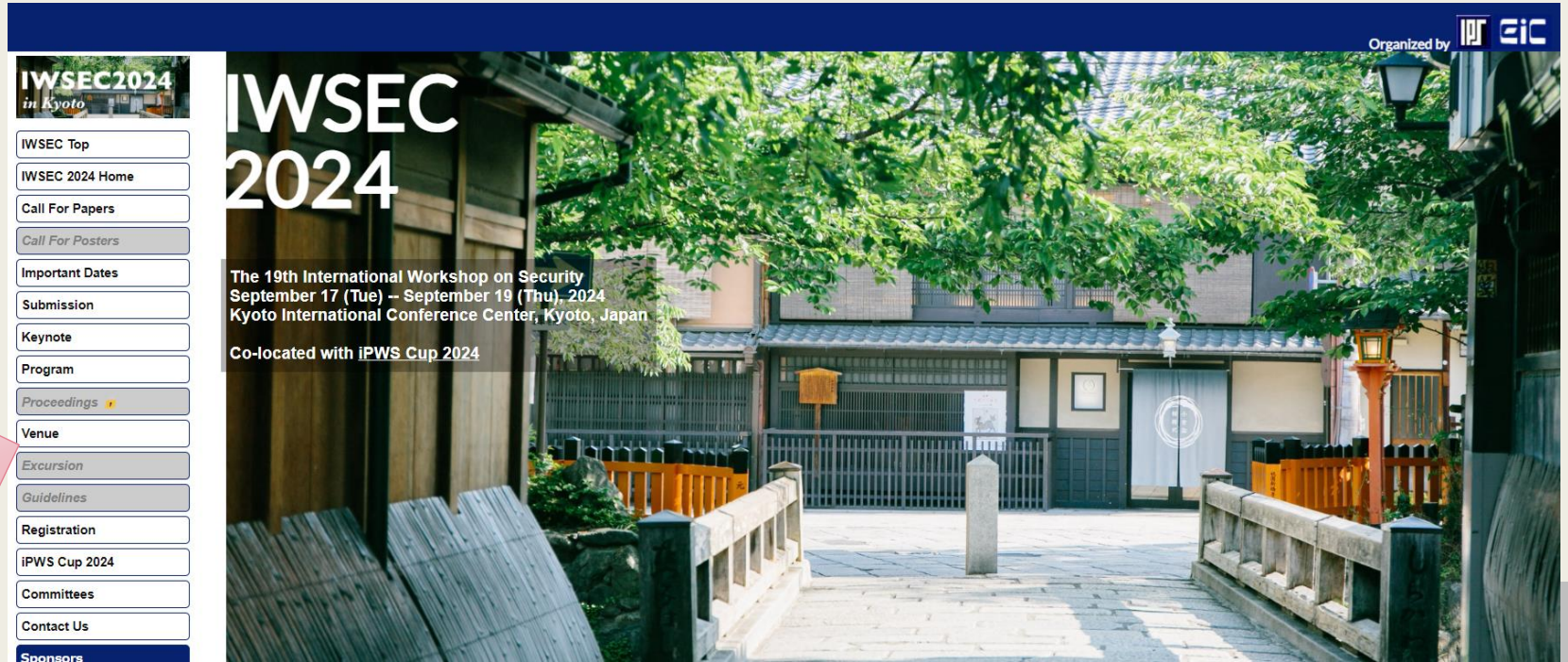
Attack Phase Result

#	User	Entries	Date of Last Entry	Team Name	Attack Score	Privacy Scores after the attack								
					Attack Score	Team 1	Team 2	Team 3	Team 4	Team 5	Team 6	Team 7	Team 8	Team 9	Team 10
1	Hikaru	13	08/21/23	08: THREE	0.3044 (1)	0.9800 (1)	0.0000 (1)	0.4600 (1)	0.9500 (1)	0.9500 (1)	0.8667 (2)	0.8833 (4)	- (9)	0.4100 (1)	0.7600 (2)
2	kchida	11	08/17/23	04: Gunmataro116luxuary	0.2911 (2)	0.9800 (1)	0.0267 (3)	0.4667 (2)	- (9)	0.9533 (2)	0.8433 (1)	0.8833 (4)	0.8900 (1)	0.5533 (6)	0.7833 (4)

iPWS Cup 2023 の画面例

神戸・京都でお会いしましょう！

2024年10月22～25日
神戸国際会議場
https://www.iwsec.org/css/2024/



2024年9月17～20日
国立京都国際会館
https://www.iwsec.org/2024/