PWS CUP 匿名加工・再識別コンテスト “*Ice and Fire*”

競技ルール Ver. 1.03

本コンテストには次の部門がある.

(1) 匿名加工コンテスト部門.

(2) 再識別コンテスト部門.

(3) 疑似データの生成コンテスト.

(1), (2), (3)は独立に応募可能. 例えば, (1)と(2)の両方, (1)のみという参加も可能.

- 使用するソフトウェアや OS には制限を加えない. 参加者は自分の実験環境を会場に持参する. ネットワークに繋いでもよい.

本ルールの記号やアルゴリズムの詳細は, 次の文献にて与えられている.

[1] 菊池, 山口, 濱田, 山岡, 小栗, 佐久間, 「匿名加工・再識別コンテスト Ice & Fire の設計」, プライバシーワークショップ 2015.

[2] 擬似ミクロデータ（簡易データ), データレイアウト及び符号表, 2011.（統計センター http://www.nstac.go.jp/services/giji/GIJI_2004zensho_s_layout_code.xls）

[3] 擬似ミクロデータ（大規模データ), データレイアウト及び符号表, 2011.（統計センター http://www.nstac.go.jp/services/giji/GIJI_2004zensho_layout_code.xls）

コンテスト(1), (2)のルールは次の通り. なお, 以下のルールは原則的に予備戦を想定した暫定的なものである. 本戦では, 本ルール(Ver. 0.1)や評価方法などを変更することがある.

1. （プレイヤー）匿名加工者, 再識別者, 審判員の 3 者が係る.
2. （匿名加工者） 匿名加工者は, 個人データ X を与えられ, 匿名加工データ Y と行番号データ I^Y を生成する. 再識別者に Y を, 審判員に Y と I^Y を提出する.
3. （再識別者）再識別者は, 個人データ X を参照して, 匿名加工データ Y から推定した推定行番号データ I^E を審判員に提出する.
4. （匿名加工の勝者）最も有用性が高く, 最も安全な匿名加工データを提出した匿名加工者を勝者とする. 有用性 50%と安全性 50%を総合して, 勝者を決定する.
5. （再識別者の勝者）最も多くの匿名加工データを正しく再識別した再識別者を, 勝者とする. Y と対応する I^Y と等しい I^E のレコードの数をその Y の E による再識別レコード数と呼ぶ. 再識別を行った全匿名加工データについての再識別レコード総数により, 評

価を行う．

6. （有用性の定義）匿名加工データ Y の有用性は，有用性指標 $U_1,\ldots,U_6$ の平均順位

$$\frac{1}{6}\sum_{i=1}^{6} Rank(U_i)$$

とする．ただし，Rank(U)は指標 U における全匿名加工データにおける順位(指標によって定められた順位付けによって決める)，有用性指標は，[1]で定める次の指標（いずれも値が小さいほど良い）とする．

U_1 = MeanMAE, SA={14,…,25}についての平均絶対誤差

U_2 = crossMeanA, B A={7, 8, 9} (性別,年齢,就業), B=15(消費支出)のクロス集計値の平均絶対誤差

U_3 = crossCntA,B 同クロス集計数の平均絶対誤差

U_4 = corMAE SA={14,…,25}についての全相関係数の平均絶対誤差

U_5 = IL 匿名加工データの各値の平均絶対誤差

U_6 = nrow 個人データと匿名加工データのレコード数の差（の絶対値）

7. （安全性の定義）匿名加工データ Y の安全性は，対応する行番号データ I^Y について定義される安全性指標 $S_1,S_2,..$と再識別アルゴリズム $E_1,E_2,..$についての再識別率 $re\text{-}id^{E1}$, $re\text{-}id^{E2}$,…から，

$$\frac{1}{4}\sum_{i=1}^{2} Rank(S_i) + \frac{1}{2} Rank(\max_j re\text{-}id^{E_j})$$

と定める．ここで，安全性指標 S_1, S_2 は，k-匿名性指標に対応する k-anony(X)とその平均値 k-anonyMean(X)を用いる．その順位 Rank(S)は，S の値が大きいほど良い順位とする．再識別率の順位 Rank(re-id)は，再識別率が小さいほど良い順位とする．また，匿名加工フェーズにおいては，次の再識別アルゴリズム[1]を用いる．

E_1 = IdRand QI={1,…,13}が同じレコードの中からランダムにレコードを識別

E_2 = IdSA QI={1,…,13}が同じレコードの中から，SA={15} (消費支出)について識別

E_3 = Sort SA={14,…, 25}の総和でソートする

E_4 = SA21 SA={21}だけで最小距離を持つレコードを識別

再識別フェーズにおいては，再識別者に用いられた再識別アルゴリズムの再識別率を更に追加して評価する．勝者の決定では，再識別フェーズの評価値を用いる．

8. （総合評価）予備戦 30%と本戦 70%で総合評価を行う．本戦の評価には，用いたアルゴリズムに関するプレゼンテーションに基づく評価を含む．

9. （匿名加工者の禁止事項）匿名加工者の次の行為を禁じる．なお，次の行為はいずれもシステムに拒絶されるため，その行為が理由で失格になるようなことは起きない．

(1) チームで 3 個を超える匿名加工データを提出すること．(ただし，匿名加工データの提出期間中は，提出済みの匿名加工データの削除および再提出が可能である．)

(2) 行番号データ I^Y が一意でない（同じ行番号データを複数用いてはならない．ただ

し，全行番号を含める必要はなく，いわゆる行削除は認める）

(3) 不正な形式の行番号データを提出すること．（行番号データの形式は，各行に行番号（1, 2, ...）１つを記載したテキストファイルである．）

(4) 擬似ミクロデータの仕様[2]に従わないデータを提出すること．（列の入れ替えを行っても良いが，それが[2]に従って解釈出来ることが必要．従って，列の削除は禁じる．なお，予備戦システム，本戦システムでは投稿データの形式チェックを行うので，それを通過すれば形式には適合しているとみなされる）

(5) 匿名加工データ Y に負の値を含むこと．

10. （再識別者の禁止事項）再識別者の次の行為を禁じる．

(1) 匿名加工者と結託すること（行番号データなどを教えてもらうこと）．ただし，再識別者が匿名加工者でもある時は，自分のデータを再識別することは認める．

(2) 不正な形式の推定行番号データ，あるいは Y の行数と異なる推定行番号データ I^E を提出すること．（ただし，I^E は一意でなくてもよい．推定行番号データの形式は行番号データの形式と同じで，各行に行番号（1, 2, ...）１つを記載したテキストファイルである．なお，この行為はシステムに拒絶されるため，この行為が理由で失格になるようなことは起きない）

(3) 同一の匿名加工データに対し推定行番号データを 2 回以上提出すること（すなわち，再識別は各データについて１回のみである．その推定結果を第三者に伝えてはならない．なお，この行為はシステムに拒絶されるため，この行為が理由で失格になるようなことは起きない）

11. （審判員の禁止事項）審判員の次の行為を禁じる．

(1) 匿名加工者や再識別者と結託すること（審判員の特権により知った情報（行番号データなど）を教えること）．

(2) PWS CUP 実行委員会委員として，匿名加工者や再識別者がそれを知ることでコンテストで有利になるような情報を非公開にすること

(3) コンテスト参加者として匿名加工者や再識別者を兼ねる場合，データ提出受付期間中に審判員の特権を使うこと（他チームの行番号データなどを知ること）　以上の禁止行為が守られている条件の下で，PWS CUP 実行委員会委員のコンテストへの参加を認める．

12. (本戦の個人データ)

(1) 本戦での個人データ X には，2 列目（世帯人員）と 3 列目（有業人員）以外は擬似ミクロデータ（簡易データ）[2]と同様のデータレイアウトと符号表を用いる．すなわち，属性 14 項目と消費支出などの属性 11 項目の合計 25 列，8333 行のデータである．2 列目（世帯人員）と 3 列目（有業人員）は擬似ミクロデータ（大

規模データ）[3]の符号表を用いる.

(2) X の 15 列から 25 列目(Youto)は，擬似ミクロデータ（大規模データ）[3]の中の支出 149 項目と収入 34 項目から 11 項目を当日ランダムに選ぶ.

(3) X のレコードは擬似ミクロデータ（大規模データ）[3]の 32,027 行の中から 8,333 行を当日ランダムに選ぶ.

13. (本戦の安全性定義)

(1) 予備戦の安全性定義(第 7 項)で用いた再識別アルゴリズムに, 次の E_5 を追加する.

E_5 = AYA　（Anti Yamaoka-Attacker）

入力： 匿名加工データ Y と対応する行番号データ I^Y

I^E = (IdSA, SA21 などにより推定した行番号データ)

出力: $i_i^{AYA} = \begin{cases} i_i^Y & \text{if } \left|X_{i_i^E} - Y_i\right| < \left|X_{i_i^Y} - Y_i\right| \\ * & \text{otherwise} \end{cases}$

ただし，ここで * は i^{Y_i}と異なる値とする．また，|x|は x の 14 列から 25 列目からなる 12 次元のベクトルの各属性での最大値と最小値で正規化した平均絶対誤差 MAE とする. (すなわち AYA 推定アルゴリズムだけは，匿名加工者に提出された行番号データ I^Yを攻撃に使うことが許されており，推定した行番号データ i^{E_i} が i^{Y_i}よりも MAE が近い場合には正しく推定できたものとして i^{Y_i}を，そうでない場合は i^{Y_i}と異なる値を，再識別レコードとして出力する．従って，論文[1] 3.5 節で述べられている「山岡攻撃」を行うと再識別率が高くなり，安全性が下がる．)

(2) 自分のチームが提出した匿名加工データに対する再識別の結果は評価しない．匿名加工データの安全性にも, 再識別者の再識別レコード総数にもカウントしない.

(3) 再識別者の勝者は第 5 項を補正し，再識別レコード総数を，自分のチームが提出したもの以外の匿名加工データの数で割った値により，評価を行う．補正の理由は，チームが提出した匿名加工データ数によって有利／不利にならないようにするためである（補正しないと，匿名加工データの提出数が少ないチームが有利になってしまう).

(4) 上記以外は，予備戦の安全性（第 7 項）と同様に評価する.

14. (本戦の有用性定義)

(1) U_2 (crossMean), U_3(crossCnt)における，A={1, 2, 3, 4, 5, 6} (世帯区分，世帯人員, 有業人員, 住居の構造, 住居の建て方, 住居の所有関係)，B=15 とする．B のデータが表す消費項目は，第 12 項でランダムに決められる.

(2) 上記以外は，予備戦の有用性（第 6 項）と同様に評価する.

15. （本戦の総合評価）

(1) A = 30* (N + 1 – 予備戦順位（本戦辞退者除く）)/N　（ここで，N=コンテスト参加者数)

B = 2/3 * (最終プレゼンテーション平均合計評価値)　（30 点満点）

C = 50 * (N + 1 – 本戦順位)/N

とする．（A+B+C = 100 点満点，A と C は匿名加工部門，再識別部門のそれぞれについて評価する）

(2) チームあたり 3 つ提出した匿名加工データの評価は，それらの最高位とする．

(3) 予備戦優勝者は A について決定する．

(4) 匿名加工部門優勝者 “Best Ice” は A と C の匿名加工部門の総和で決定する．

(5) 再識別部門優勝者 “Best Fire” は A と C の再識別部門の総和で決定する．

(6) 疑似データ生成部門優勝者 “Best Synthesizer” は B のみで決定する．

(7) 総合優勝者 “Best PWS CUP” は A,B,C の総和で決定する．

16. （本戦の禁止事項）

(1) 匿名加工者の提出する匿名加工データ Y が従うべき仕様も，第 12 項と同様に 2 列目と 3 列目だけは[3]で，その他の列は[2]とする（第 9 項(4)の変更）．

(2) 上記以外は，予備戦と同一（第 9,10 項）とする．

コンテスト(3)のルールは次の通り．

1. （疑似データの生成の評価）疑似データの生成をどのように行ったかをプレゼンテーションしてもらい，その技術力，独創力，実現可能性の観点で評価を行う．

2015 年 10 月 15 日 Ver 1.03
2015 年 9 月 15 日 Ver 1.02
2015 年 8 月 24 日 Ver 1.01
2015 年 8 月 20 日 Ver 1.0
PWS CUP 実行委員会