［匿名加工とプライバシ保護］

④ 匿名加工・再識別コンテスト
―世界唯一の対戦型データ匿名加工コンテスト PWS Cup ―

小栗秀暢 | 富士通研究所

匿名加工・再識別コンテスト

匿名加工情報の作成方法は，個人情報保護委員会が作成したガイドラインで示されたものでは十分ではない．データの性質と使用目的に応じて，技術者が複数の匿名加工手法と安全性指標を組み合わせて作成する必要がある．本来ならば，データの用途に沿ったシナリオで匿名加工を行い，評価することが望ましい．しかし，その加工方法の多様さから，データの有用性と安全性を統一的な基準で計測することは困難であった．

このような課題に対して，本会コンピュータセキュリティ研究会 (CSEC) は，産学が共同してプライバシ保護技術の研究開発を活性化し，議論する場として，プライバシーワークショップ (PWS) を 2015 年から開催している．その中でも匿名加工技術の発展のために，毎年行われているのが，匿名加工・再識別コンテスト：PWS Cup である．匿名加工と再識別を両方行う対戦型のコンテストとして，現時点では世界でも唯一の試みである．

3 年目となった 2017 年度のコンテスト[1] の概要を表 -1 に示す．のべ 18 チーム，73 人の参加者が，同一のデータセット，かつ同じ有用性の基準によってさまざまな匿名加工処理を試み，有用性と安全性の総合値が最も優れた匿名加工データを作成することを目的として，その腕を競いあった．

■表 -1　PWS Cup 2017 開催概要

開催期間	9 月 11 日～ 10 月 23 日
のべ参加者数	73 人
参加チーム総数	18 チーム
匿名加工データ提出数	825 データ
再識別データ提出数	2,943 データ

コンテストの流れ

なぜ，PWS Cup では匿名加工と再識別を対戦形式で行うのか．それには，匿名加工処理の目的と攻撃方法を考える必要がある．

匿名加工処理とは，大雑把に考えると，データを棄損する処理である．たとえば，氏名と年齢を棄損させて仮 ID と年代に変更するような処理を行うことで，誰のデータか分からなくする．しかし，データを利用する側にしてみると，このような行為は分析の邪魔でしかない．

そこで，データ利用者と匿名加工者が協議した後，特定の個人が識別される可能性が高い要素だけを加工し，分析に必要な要素はなるべく元データのまま変更しないように処理を行う．それが匿名加工の本質的な要求である．

しかし，本当にデータから特定の個人が識別される要素が排除されているのだろうか．それを検証するために，匿名加工の研究では，攻撃手法と攻撃者が持つ知識量を仮定し，その範囲における安全性を保証する．その反面，攻撃者の想定が少し異なるだけで，アルゴリズムの安全性が比較できなくなるという課題があった．

そこで，PWS Cup では匿名加工フェイズと再識別フェイズを分離し，攻撃者の条件を統一化することで比較を可能とした．

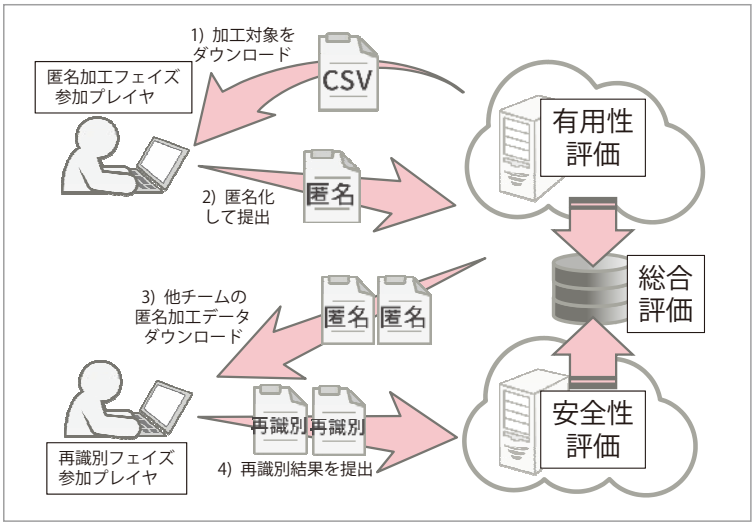
コンテストの流れを図 -1 に示す．まず，参加プレイヤは加工対象データをダウンロードする．2017

年度は UCI Machine Learning Repository にて公開されている，英国のあるオンラインショッピングサイトにおける購買履歴データ Online Retail Data Set[2] を採用した．

匿名加工フェイズでは，参加者は対象データをダウンロードした後に匿名加工し，データを評価システムに提出して有用性を評価する．2017 年度の有用性指標は購買履歴データを用いたレコメンドエンジンを開発するという想定に立ち，推薦結果精度を基準とした評価指標を設定した．

その後，再識別フェイズでは，各チームの匿名加工データを，元データとの関係性を示す対応表を削除した状態で他の参加者に配布する．互いの匿名加工データに対して，知識量が同一の形で再識別攻撃を行い，最終的な安全性を求める．コンテストとしての総合順位は有用性と安全性の和で定めた．

再識別者（攻撃者）は有用性の意味やデータ処理の目的を熟知していることから，安易な処理を行ったデータは簡単に再識別されてしまう．そこで有用性の値を操作し，ほかのチームが想定しない加工方法を考案して提出するなど，各チームが巧みに戦略を企てることが，対戦型コンテストの醍醐味である．



■図 -1　コンテストの流れ

コンテストのルール

PWS Cup の行われたこの 3 年間は，個人情報保護法の議論が活発化し，法律の成立から施行された期間でもある．その状況に対応し，実行委員会では，常に法律や社会の要請と学術的な課題を比較し，コンテストのルールと評価指標を定めてきた．

2015 年の PWS Cup では，ある個人がデータ内に 1 人しか存在しない「マスターデータ型」の匿名加工と再識別を行った．2016 年はデータに含まれる個人が複数個存在する「トランザクションデータ型（履歴データ型）」を利用して，より現実的なデータのユースケースに近づけた．

2017 年のコンテストは，さらにユースケースを検討し，毎月の購買データを第三者に提供することを考え，トランザクションデータに含まれる識別子を仮名化し，かつ仮名を複数個に分割可能なルールを設定した．

仮名の分割について図 -2 に示す．まず，元データは識別子，日付，商品 ID，単価，個数で構成されている購買履歴データである，それを，識別子と日付で分類した［表 A］を作成する．その後，元の識別子を「仮名」に変換して［表 B：仮名表］を生成する．攻撃者は，匿名加工データと，そこに含まれる仮名から，この仮名表を推定する．この処理を，本コンテストにおける「再識別」と定義した．

たとえば，購買履歴が多く，個人識別される可能性が高い Bob には B1 と B2 という分割された仮名を付与し，かつ 2011 年 2 月のデータを削除する．これによって，図 -2 に示されている 3 名は，2 つの仮名によって個人が識別される可能性を低減した 2 組のユーザ集合 {A1, B1}{B2, C1} に変換できる．

実際のコンテストでは，このような仮名表の工夫に加え，Alice と Bob の購買

商品を入れ替えるなど，有用性を下げつつも再識別されない工夫を行い，各参加者がその優劣を競いあった．本小特集では，2017 年度の優勝チームの加工詳細についても別記事で記載されているので参照されたい．

また，2017 年度のルールで最も議論となったのは仮名を分割した際に，1 カ月分の仮名だけが再識別された場合と，すべての期間が再識別された場合で，得られる得点に差をつけるべきか，という問題である．これは安全性の基準を，再識別に成功した数として考えるか，データの持つ機微性やプライバシ影響評価として考えるかの違いでもある．最終的には 12 カ月分すべての仮名を当てた場合に 1 人再識別されるというルールを採用した．この点は参加者からの意見も多く寄せられ，活発に議論された．今後のルール制定に活用したい．

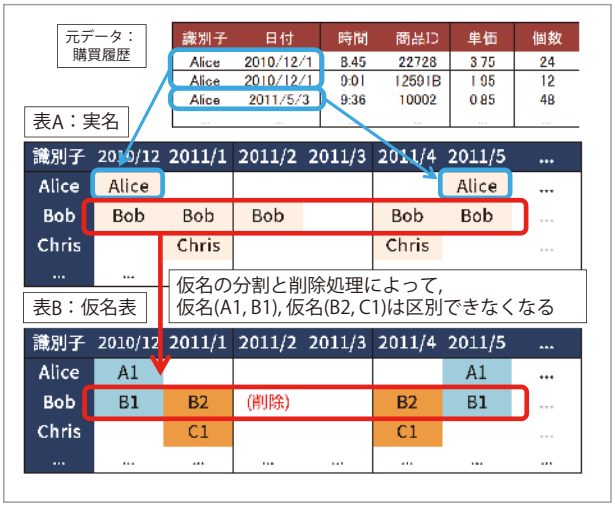
2017 年度のコンテスト結果

2017 年度のコンテストは，開催期間約 2 カ月の間に，オンラインでの「予備戦」，および PWS 会場での直接対戦である「本戦」の 2 回に分けて行われ，総合順位を定めた．コンテストを通じて合計 825 個の匿名加工データが提出され，その中から各チームで最も自信のあるデータを他の参加者に公開した．公開された匿名加工データに対して，他の参加者が仮名表の推定を行い，合計 2,943 個の再識別データが提出された．

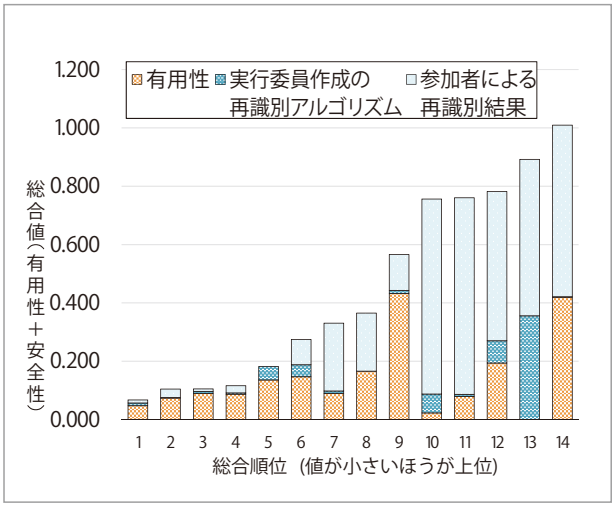
図 -3 は本戦における最終ランキングでの有用性と安全性の指標の分布である．グラフは有用性と安全性を示し，特に安全性は実行委員会が用意したサンプルの再識別アルゴリズムでの結果（青部分）と，再識別フェイズ後に他の参加者から攻撃された後の結果（薄青部分）に分かれている．薄青部分が大きいほど，他の参加者による攻撃によって安全性が大きく低下したことを示している．

参加者同士の再識別攻撃の状況を示したグラフが図 -4 である．円の大きさは各チームの最終的な安全性であり，大きい方が優れている．矢印の太さは再識別攻撃の成功率を示している．最終的には，他のチームからの再識別攻撃に耐え，他チームへの再識別攻撃に成功することで順位が上がる仕組みである．そのため，上位になるためには，他の参加者が想定しないような匿名加工アルゴリズムを考案し，かつ，他の参加者の匿名加工の方式を推定しなくてはいけない．

匿名加工の手法は多様であることから，あらゆるデータに対応する再識別アルゴリズムを作ることは



■図 -2　元データから仮名表を作成する流れ



■図 -3　本戦提出データの有用性と安全性

困難である．そのため，さまざまな想定を行った参加者が，多くの再識別アルゴリズムを試すことで，匿名加工データの安全性が徐々に明らかになってくる．

これらの順位やデータの詳細値は公式 Web ページ[☆1] を通じて，図 -5 のように有用性，安全性がグラフ化され，リアルタイムで公開された．

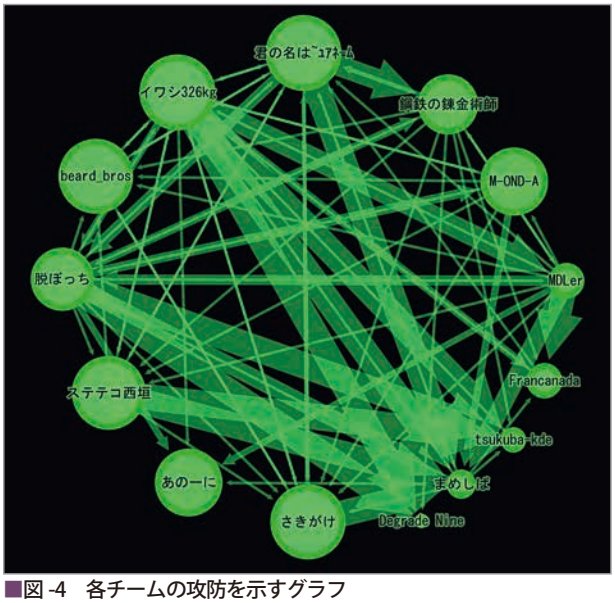
また，会場にて行われた本戦は，約 1 時間という限られた時間の中で匿名加工データを解釈し，他のチームの再識別を行う．会場では図 -6 に示すようなランキングの上下の動きがスクリーンに映し出された．そのため，チームの順位が変わるたびに会場から歓声が上がるなど，より対戦要素の強いイベントとなった．

当日の順位変動を参照すると，大きな順位の変動が発生するのは最初の 30 分くらいまでであり，その後はほとんどのチームの順位が固定されている．コンテストの上位チームは，確率的にしか個人が識別されないようにデータを加工している．そのため，再識別攻撃は一定の確率以上は成功せず，事前に用意してきた再識別アルゴリズムのアイディアが尽きた段階で，多くのチームの再識別結果が収束し，順位が固定されていくのが特徴的である．2017 年度のルールに則ると，攻撃時間を長く取っても成功率が大きく向上しない[3] ことが報告されている．

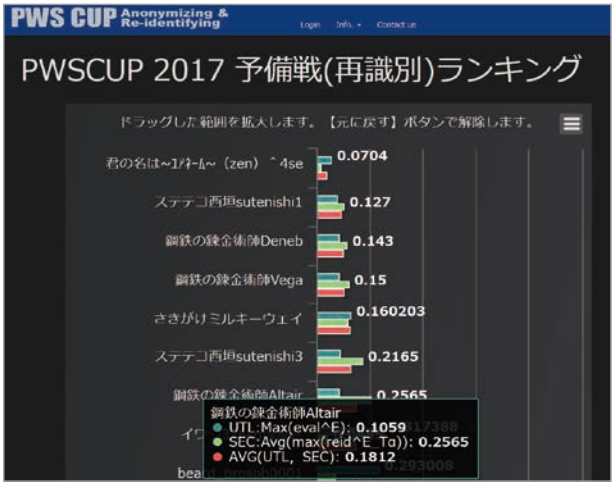
また，参加した各チームが得た匿名加工に関する知見が，コンテスト終了後に共有されることも PWS Cup の大きな意義である．2017 年度は再識別フェイズ後に，上位チームによるプレゼンテーションのセッションが設けられた．

セッションでは，個人情報保護委員会規則 19 条にて定められた匿名加工基準を参照し，コンテストルールに対して，どのように解釈したか，および，その解釈を匿名加工アルゴリズムに反映したかにつ

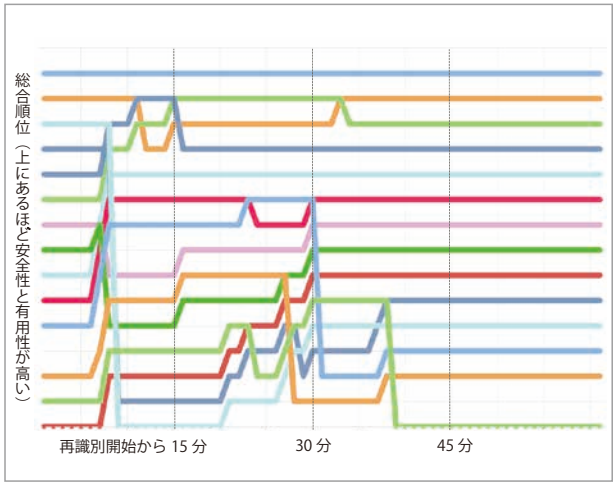
[☆1] https://pwscup.personal-data.biz



■図 -4　各チームの攻防を示すグラフ



■図 -5　Web サイトでの予備戦ランキング



■図 -6　会場で表示した順位変動図

いて，各チームから発表が行われ，議論が交わされた．図 -7 はその模様である．

各チームの加工方法は個人情報保護委員会にレポートとして提出し，各参加チームに向けてコメントをいただいた．このような活動は，匿名加工情報の扱いに悩む企業などにとっては，技術と知見を蓄積する良い機会であったと考える．

今後の展開

まず，2017 年度では国際化を実現し，台湾，カナダの両国の研究者に参加いただけた．特に台湾チームは総合 2 位を獲得する大健闘であった．来年度以降も国際化を進め，匿名加工データの国際的な安全性に関する議論が深まることを期待する．

コンテスト参加チームのすそ野が広がる一方，匿名加工技術の公開と共有という課題がある．現在，コンテストで使用したアルゴリズムの説明や作成した匿名加工データは，各チームから許諾を得たものだけが公開されており，利用できるものが制限されている．今後は学術利用が可能となるよう，より多く公開されることが望ましい．コンテストの意義の周知を強化するなど，運営方針の検討を続けていきたい．

過去に行われた PWS Cup を通じて，参加者は実行委員から与えられた有用性と安全性の基準を満たすための試行錯誤を行い，匿名加工データを生成する技術を磨いてきた．これらの活動はそのまますべてが実社会の匿名加工情報の生成に利用できるわけではない．しかし，現実における匿名加工処理は，データに含まれる属性値やその利用方法を総合的に判断して，最適な手法と指標を検討することが求められる．そこには，コンテストで得られた知見が役立つ場面が出てくると考える．

本コンテストを通じて，データの安全性に関する知識の共有と，利用要求に応じた加工処理を実践する人材の育成に寄与することができれば幸いである．

■図 -7　プレゼンテーションの模様

参考文献

1) 菊池浩明，小栗秀暢，中川裕志，野島　良，波多野卓磨，濱田浩気，村上隆夫，門田将徳，山岡裕司，山田　明，渡辺知恵美：PWSCUP 2017：長期間の履歴データの再識別リスクを競う，コンピュータセキュリティシンポジウム 2017 論文集 (2017).
2) Chen, D., Sain, S.-L. and Guo, K. : Data Mining for the Online Retail Industry : A Case Study of Rfm Model-based Customer Segmentation Using Data Mining, Journal of Database Marketing & Customer Strategy Management, Vol.19, No.3, pp.197-208 (2012).
3) 濱田浩気，岡田莉奈，小栗秀暢，菊池浩明，中川裕志，野島良，波多野卓磨，正木彰伍，渡辺知恵美：匿名加工アルゴリズムの公開・非公開による再識別容易性の比較，2018 年暗号と情報セキュリティシンポジウム (SCIS2018) 論文集，IEICE (2018).

(2018 年 1 月 29 日受付)

■小栗秀暢（正会員）　oguri.hidenobu@jp.fujitsu.com

1997 年早稲田大学第二文学部卒業．同年タイトー（株）にてゲーム／システム開発に従事．2007 年よりニフティ（株）にてデータ分析とプライバシ保護技術の研究開発を進める．2016 年に総合研究大学院大学 複合科学研究科 情報学専攻を修了．現在は（株）富士通研究所に勤務．博士（情報学）．