デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

個人データの保護と流通を目的とする匿名化と再識別コンテスト：PWS Cup

小栗 秀暢[1]　黒政 敦史[2]　中川 裕志[3,4]　菊池 浩明[4,5]　門田 将徳[3]

[1]富士通研究所　[2]富士通クラウドテクノロジーズ　[3]東京大学　[4]国立研究開発法人 理化学研究所　[5]明治大学

2017年5月30日に全面施行された改正個人情報保護法により「匿名加工情報」という新たな情報の類型が導入された．その作成に関する規則の解釈や技術的な知見の共有が求められている．2015年より行われている匿名加工・再識別コンテスト（PWS Cup）は，匿名加工技術の発展を目的とする対戦型コンテストである．2017年に行われたコンテストでは，政府が定めた規則への解釈を含め，データの有用性と安全性を総合的に評価する試みを実施した．本稿ではコンテストの概要と結果について紹介した上で，得られた知見について報告する．

1. はじめに

近年のデータ分析技術の進歩により，パーソナルデータを用いて，顧客の行動や属性に応じたサービスや，商品のレコメンドシステムなどに活用する企業が増加している．しかし，パーソナルデータの中には，個人が他人に知られたくない情報や，攻撃の標的になりやすい情報が含まれる場合がある．そこで，パーソナルデータから特定の個人が識別されるリスクを低減する，匿名加工技術が注目されている．

2017年5月30日に全面施行された改正個人情報保護法 [1]（以後，改正法とする）は，匿名加工情報という新たな情報の類型を定義した．匿名加工情報は，一定の条件の下で，本人の同意がなくても第三者提供や目的外利用が可能となる．これによって，業種業態を超えたデータの活用が進むことが期待されている．

改正法が定める個人情報保護委員会は，匿名加工情報の加工基準として，個人情報の保護に関する法律施行規則[2]（以後，規則とする），および，個人情報保護法ガイドライン匿名加工情報編[3]を公開し，技術的な基準を定めている．

しかし，匿名加工情報の実装方法は無数に存在しており，個人情報保護委員会などが作成したガイドラインや指針に示された情報だけでは不十分である．そのため，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．

また，それら個別のデータ処理は技術者の判断によって行われる部分も多いことから，個々の技術者に向けたアルゴリズムや加工事例の共有が必要である．しかし，匿名加工情報の加工に関する情報は，公開されている匿名加工情報の安全性を損ねる可能性があるため，改正法やガイドラインにおいて，安全に管理することが定められている．

これらの課題により，個々の技術者，研究者による匿名加工技術の向上を促す機会と，特定の匿名加工情報に依存しない技術共有の場が求められていた．

これらの課題に対し，情報処理学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ー保護技術の研究開発を活性化し，議論するため，2015年にプライバシーワークショップ（PWS）を発足した．

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）[4],[5],[6],[7]である．PWS Cupは，参加チームが匿名加工したデータを，他のチームが再識別するという対戦型コンテストとして，世界でも唯一の試みである．その概要を**表1**に示す．

表1　実施されたPWS Cupの概要
脚注：[4],[5],[6],[7],[10]

	2015年度[4]	2016年度[5]	2017年度[6,7]
募集ポスター			
開催期間	10/21,22	10/11,12	10/23,24
本戦参加チーム数（参加者数）	13チーム（20名）	15チーム（42名）	14チーム（43名）
データセット	擬似ミクロデータ	UCI Online Retail Data Set[10]	
個人数	8,333	400	500
履歴数	-	18,524	44,917
攻撃者モデル	最大知識攻撃者		部分知識攻撃者

まず，2015年に行われた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うため，独立行政法人統計センターが作成した擬似ミクロデータ[8]を用いて，攻撃者が元データの値すべてを保持している「最大知識攻撃者[9]」を想定したコンテストを実施した．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，より現実的なユースケースに近づけた．

2017年度のPWS Cup（以降PWS Cup2017）は，個人情報保護法の全面施行の直後に行われたことから，コンテストルールの中で，個人情報保護委員会規則を解釈して匿名加工を行うことを求めた．また，レコメンドエンジン向けに，毎月購買データを提供するという，より現実的なユースケースを設定した．

本稿では，このコンテストを通じて，技術的に明確にすることが困難な法律，規則，ガイドラインに対して，人間の解釈と処理アルゴリズムを組み合わせ，安全性と有用性の高い匿名加工方式を決めるという活動，および得られた知見について報告する．

2. コンテストのルール

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，参加チームに同一の知識（加工対象データ）を配布し，それぞれのチームが作成したデータに対して，他のチームが攻撃するという，対戦方式のコンテストを設計[4]した．その結果，異なる匿名加工アルゴリズムにおける安全性と有用性の比較が可能となった．

本稿では，コンテストのルールの制約にしたがってデータの安全性を高める処理を「匿名加工」と呼び，その結果出力されたデータを「匿名加工データ」とする．「匿名加工情報」は法律用語であるため区別して扱う．

PWS Cup2017では，匿名加工データの優劣を定めるため，A）匿名加工フェイズ，B）再識別フェイズ が実施され，1）安全性，2）有用性，3）個人情報保護委員会規則第19条への対応の3つの観点から評価して順位や賞を定めた．

2.1 コンテストの流れ

コンテストはA）匿名加工フェイズとB）再識別フェイズに区切って運営される．**図1**にPWS Cup2017におけるコンテストの流れを示す．

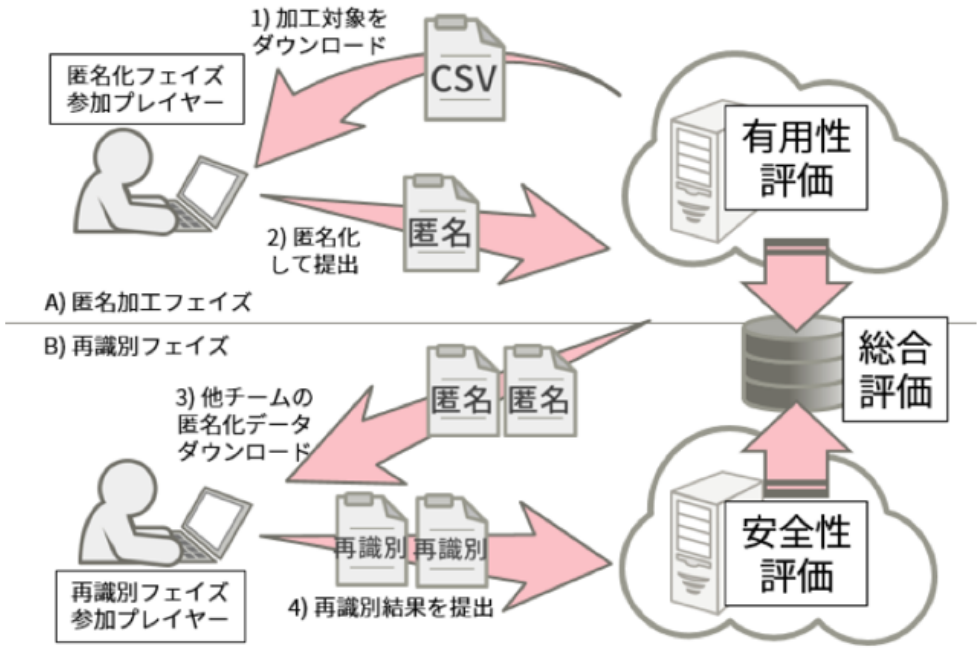

図1　匿名加工・再識別コンテストの流れ

A）匿名加工フェイズ では公式サイトからコンテストの対象データ（顧客マスターと購買履歴データ）をダウンロードし， 元情報との対応ができないよう加工した購買履歴データを作成する．このデータを評価システムに投入する際に，ルールにて定められた有用性評価が行われる．

B）再識別フェイズ では，匿名加工された購買履歴データに対して，評価システムが行番号のかく乱処理を施し，元情報との対応が分からない匿名加工データとして他のチームに公開される．参加チームは，再識別攻撃者として匿名加工データと元データを対照し，あるレコードが元データでは誰のレコードであったかを推定し，再識別結果を提出する，評価システムは，再識別結果を元情報と比較して，匿名加工データの安全性を決定する．最終的には有用性と安全性の評価の和によって総合評価が定まる．

2.2　コンテストルール概要

図2に本コンテストのルール概要を示す．コンテストの正式なルール，および解説はルール論文[6]，および公式Webサイト等で公開した資料[7]に詳述されているため，そちらを参照していただきたい．

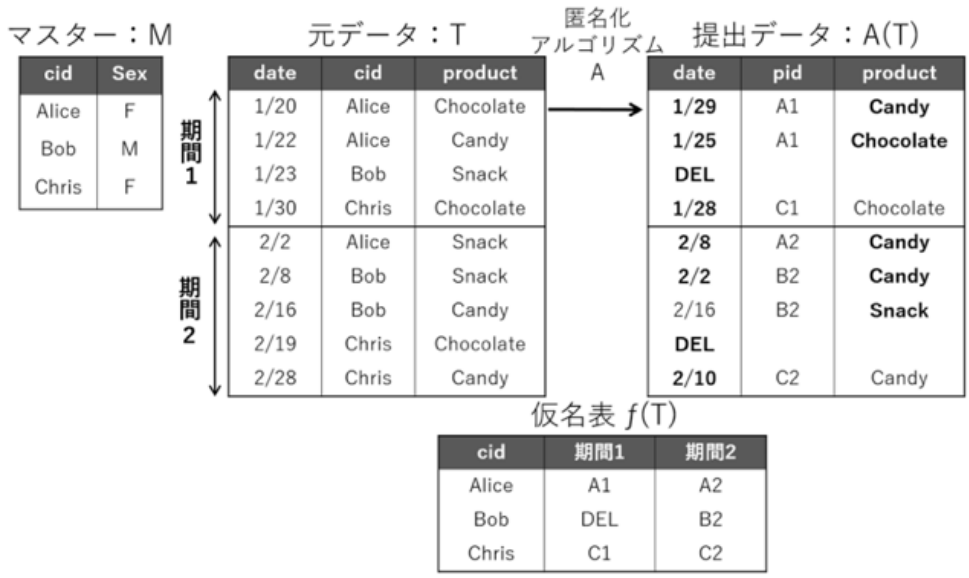

図2　匿名加工フェイズで利用するデータ概要

本コンテストでは，登録された個人情報である顧客マスターデータMと顧客が行った購買取引（トランザクション）の履歴を表す購買履歴データTを対象とする．MとTの間は，顧客識別子cidにより結び付けられている．たとえば，図2の顧客Aliceは，1月20日と22日に商品ChocolateとCandyをそれぞれ購入している．

この購買履歴がAliceのものであることが識別できないように，匿名加工アルゴリズムAにより加工したデータを提出データA（T）とする．A（T）は Tに対して顧客cidが仮名pidに振り替えられ，日付や商品のランダムな変更（摂動），レコード（行）削除などが行われる．たとえばAliceの1月20日のChocolateは，1月29日にCandyを購入したことに加工され，顧客Bobの履歴は識別されるリスクが高いと判断されて，削除（図の “DEL”で指定）されている．

このとき，A（T）の加工処理は期間単位で行うと想定して，期間を超えた変更はできないものとルールで定めた．この加工期間のルールについては2.4節にて述べる．

たとえば期間1である1月30日のChrisのChocolate購買履歴は，期間2である2月1日に変更することはできない．これによって，購買履歴データTから，顧客cidと月ごとに設定された仮名pidで構成される仮名表 f が作成される．この f を安全性を評価する基礎データとする．再識別フェイズの概要を**図3**に示す．参加プレイヤは，元情報の仮名表 f を推定し，推定仮名表 $\hat{f}$ を作成する．評価システムにおいて f と $\hat{f}$ を比較し，元情報との紐づけに成功した割合を安全性指標とする．

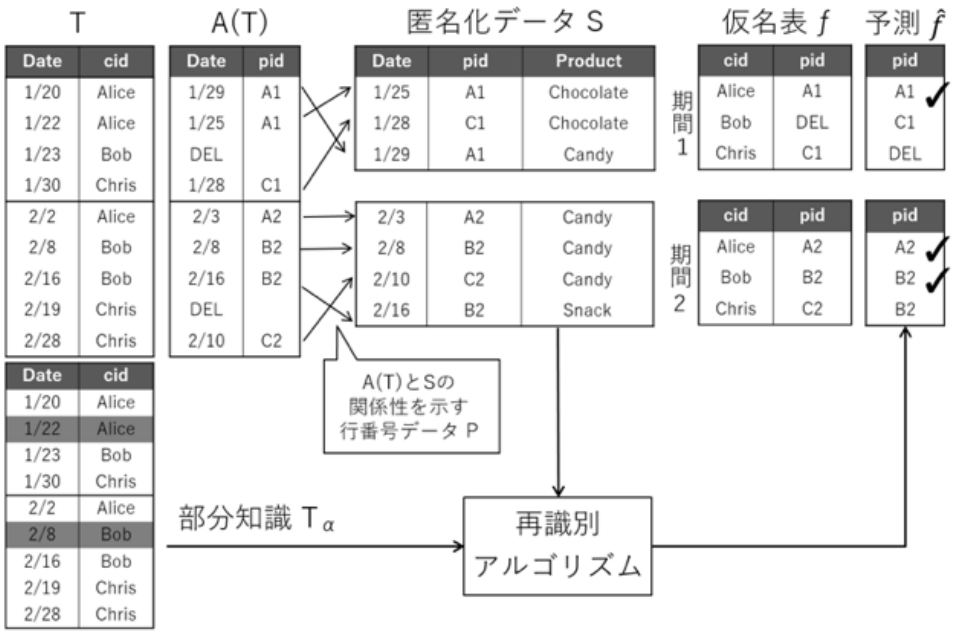

図3　再識別フェイズで取り扱うデータ概要

2.3　使用したデータセット

2017年度のコンテストでは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[10]をサンプリングして購買履歴データTを作成した．また，顧客マスターデータ Mは，Tに出現する顧客IDを元に，実行委員が生成した属性値[5]を使用した．それらデータ概要を**表2**，**表3**，**表4**に示す．

表2　Online Retail Data Set概要

項 目	値 域 , 値 数
Online Retail Data Set (購 買 履 歴 デ ー タ T)	レ コ ー ド 数　397,625
顧 客 マ ス タ ー デ ー タ M	顧 客 数　4,333

表3　購買履歴データT

属性名	値域，説明
CustomerID(顧客 ID)	M と接続する顧客 ID
InvoiceDate(購入日時)	2010/12/1 8:26 – 2011/12/9 12:50
StockCode(商品 ID)	商品数 3,663
UnitPrice(単価)	€0.01 – €38970
Quantity(購入数)	1 個 – 80995 個

表4　顧客マスターデータM

項目	値域，説明
CustomerID(顧客 ID)	T と接続する顧客 ID
Sex (性別)	(f, m) に区分
Generation(年代)	1930-1980 までの年代に抽象化
Country(国名)	United Kingdom, France, Germany, Others の 4 種類

2.4　再識別の定義と長期間履歴データの制御

2017年度のコンテストルールの特徴として，匿名加工データを作成する際に，個人識別性の高い長期間履歴データを制御する処理がある．これは，個人の履歴の途中で仮名IDを変更することによって履歴データを分割し，個人の識別可能性を低減させる処理である．

長期間履歴データの加工については，事務局レポート[11]においても記述があるが，その期間とリスクの関係性についての研究は少ない．そこで，2017年度のコンテストでは，定期的な仮ID変更が再識別攻撃に与える影響について観察することを目的の1つとした．

仮名の分割について**図4**に示す．まず，元データである購買履歴データを，識別子と日付（月）で分類した[表A：実名]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．この処理をコンテストにおける「再識別」と定義した．

図4　元データから仮名表を作成する流れ

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．これにより，図4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，各参加チームがその優劣を競いあった．

3. PWS Cup2017の評価指標

匿名加工データの評価指標には，有用性と安全性の両方の指標が必要である．たとえば，利用目的が明確には定まっておらず，有用性の評価基準が不明な場合を考えよう．データ処理者は安全性を高くすることに注力するため，あらゆる行と列の値を削除することが可能となる．結果として，何の意味も持たないデータになる恐れがある．加えて，匿名加工データから再識別されるリスクを完全に排除することはできないため，値をすべて削除したとしても【1/データの行数】の識別リスクが存在する．

すなわち匿名加工データの優劣を競うためには，そのデータの作成目的，または有用性としてデータのどの属性を何の用途に用いるか等の定義と加工制限が必要となる．

PWS Cup実行委員は，匿名加工データの利用方法を複数想定し，それらの条件を同時に満たすことを有用性の条件として指標を設計した．

3.1　有用性指標

表5にPWS Cup2017の有用性指標を示す[7]．有用性指標は商品推薦に用いるレコメンドエンジンの作成を目的としたデータ利用者を想定した指標（E1，E2，E3）と，時系列分析や価格変動の分析を目的としたデータ利用者を想定した指標（E4，E5）に大別される．また，過度なレコード消去を抑制するための指標としてE6を採用した．E1，E2，E3については3.2節にて詳述する．

表5　PWS Cup2017で採用された有用性指標

有用性指標	概要	作成者
E1-ItemCF-s	対問屋用のレコメンドエンジン作成のための有用性を評価	村上　隆夫 門田　将徳
E2-ItemCF-r	対小売店用のレコメンドエンジン作成のための有用性を評価	
E3-topk	購入した顧客数が最も多い上位 k 個の商品集合の差分を評価	
E4-diff-date	匿名加工前後の購入日の差の絶対値を評価	野島　良
E5-diff-price	匿名加工前後の単価の比率の和を評価	
E6-nrow	消去されたレコード(行)の割合を評価	小栗　秀暢

1つのコンテストにおいて，利用目的の異なる複数の有用性指標を設定することで，評価対象データが複数の用途に利用可能であることを示す．

また，2017年度のデータセットは，2016年度[5]と同じものを利用しているが，有用性や加工制限のルールが異なる．そのため，最終的なデータの生成方法とその結果がまったく異なるものになることにも留意されたい．

3.1.1　レコメンドエンジン作成を想定した有用性指標

本項では有用性指標E1，E2，E3について述べる．PWS Cup2017では，ある商品を買う人の併売商品を推薦するためのレコメンドエンジンの開発をデータ活用ターゲットの1つとして想定した．オリジナルのトランザクションデータTと，匿名加工トランザクションデータからそれぞれ商品同士の類似度行列を作成し，それらの距離によってレコメンドエンジンにおける有用性の評価を行った．

購買履歴データTの商品購入数の分布について**図5**に示す．それによると，合計購入数が12個，24個，36個，48個のとき，いわゆる「ダース買い」のときに，それぞれ【顧客×商品】の組合せ数が多く出現している．そこで，レコメンドエンジンの適用先としてダース単位以上で購入する「問屋」と，12個未満の商品を購入する「小売店」の2種類を設定した．

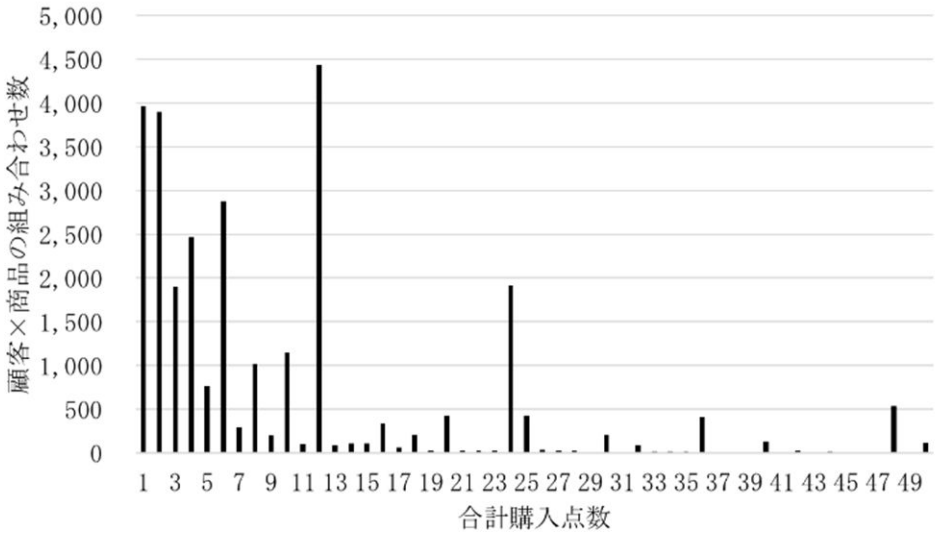

図5　合計購入数の分布

E1-ItemCF-sは，商品をダース以上で大量に購入する問屋をイメージした指標である．匿名加工前後で顧客と商品の組合せごとの合計購入点数が，12個以上の組合せを対象として類似度行列を作成し，それらの距離を評価する．反対に，E2-ItemCF-rは小売店を想定しており，合計購入点数が12個未満のものを対象として類似度行列を作成し，評価する．

また，E3-topkは問屋と小売店の両方で利用できる指標である．こちらは，購入した顧客数が最も多い上位k個の商品集合について類似度行列を作成し，匿名加工前後でその距離を評価した．

3.2　安全性指標としての再識別率の定義

2017年度のコンテストの安全性は，再識別フェイズにおける他の参加プレイヤからの再識別攻撃において再識別されたレコード数の最大値にて評価した．また，安全性にも複数の定義があり，実行委員の中で議論された．

最終的には，ある顧客についてすべての月の仮名を再識別された場合，1人のデータが再識別された，と定義した．この再識別ルールにおける一致率の定義とその課題については5.2節にて述べる．

3.3　匿名加工の規則に対応した加工方法の評価

PWS Cup2017では，以下の3つの賞を設定した．

1. 総合順位：有用性と安全性の和で定める．
2. 再識別賞：総合順位1位のチームに対して最も再識別に成功したチームを表彰する．
3. 匿名加工基準賞：国が求める匿名加工基準を正当に解釈し，匿名加工アルゴリズムに適用したことを評価する．

特に3. 匿名加工基準賞は，匿名加工に関する規則を解釈して行われた処理について評価するものである．本節では，その解釈のベースとなる規則とガイドライン，およびコンテストとの関係性について述べる．

3.3.1　関係する規則，ガイドライン

まず，匿名加工情報を作成するにあたって必要な法令について，**図6**を参照して述べる．

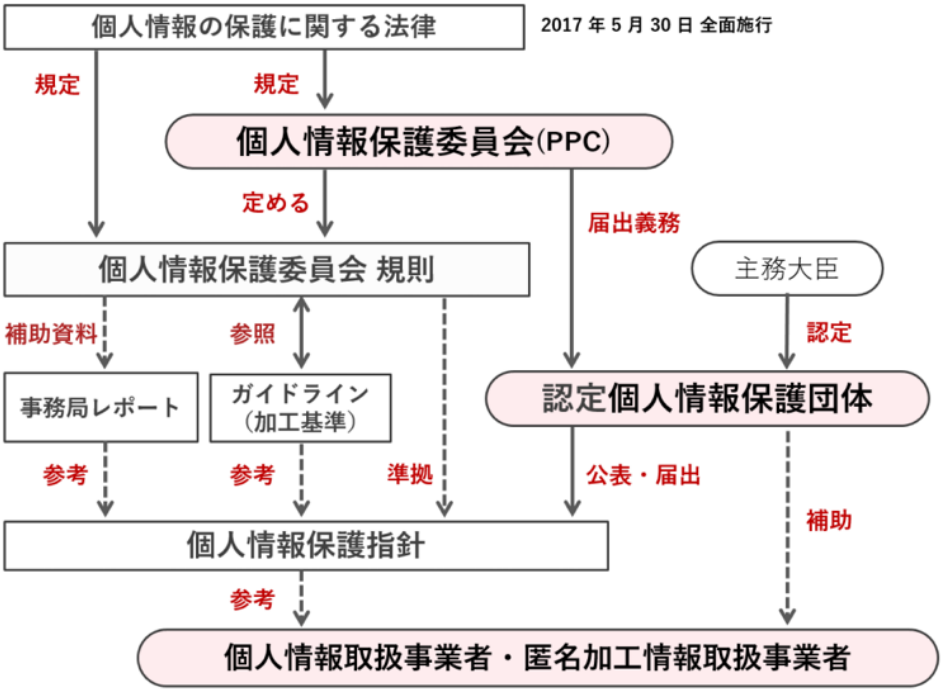

図6　匿名加工情報にかかわる規則，指針，ガイドライン等

改正法によって規定された個人情報保護委員会は，匿名加工情報の加工基準について「個人情報の保護に関する法律施行規則[2]」（以後，規則とする）に定め，個人情報保護法ガイドライン匿名加工情報編[3]（以降，ガイドラインとする），個人情報保護委員会事務局レポート[11]（以後，事務局レポートとする）を公開した．しかし，事業者が具体的にどのような加工を行うかについては，取り扱う個人情報の性質，取扱い実態等に応じて定めることが望ましい．そのため，主務大臣が認定する認定個人情報保護団体が作成する個人情報保護指針等の自主的なルールにゆだねることとしており，呼応して認定団体から指針が順次公開されている．

個人情報を適切に匿名加工情報にするためには，これらの規則，ガイドライン等を参照して適切な事例や加工方法を見つけ出し，必要な場合は，認定個人情報保護団体等に加工方法を確認することが求められる．

特に，これらの加工方法の基準として多くの指針に反映されているものに，規則第19条がある．以下に条文を紹介する．

> 規則第19条 法第36条第１項の個人情報保護委員会規則で定める基準は，次のとおりとする．
>
> （1） 個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（※）．
> （2） 個人情報に含まれる個人識別符号の全部を削除すること（※）．
> （3） 個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る）を削除すること（※）．
> （4） 特異な記述等を削除すること（※）．
> （5） 前各号に掲げる措置のほか，個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し，その結果を踏まえて適切な措置を講ずること．

（※当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）

このうち，規則19条の1号から3号までは，技術的な加工方法と対応しており，明確に判断できる場合が多い．しかし，4号と5号に関しては，それぞれのデータの持つ特徴や社会的な意義を含むことから，解釈の余地が生じる．

3.3.2　コンテストにおける規則，ガイドラインへの対応

PWS Cup2017のルールを作成する際，実行委員は規則19条との関係性について議論を行った．たとえば，4号における「特異な記述」などを，コンテストルールで縛り，一定以上の加工を行わないデータにデメリットを与えることが検討された．しかし，定量的な基準に落とし込むには，まだ国内における議論が足りないと判断し，各チームに解釈をゆだねることとした．

その代わり，PWS会場にて，有用性・安全性の総合点で上位10チームによる最終プレゼンテーションを行い，それぞれの解釈を報告する機会を設けた．その報告に対して，参加者，聴講者による投票を行い，最も得票数の多いチームに対して「匿名加工基準賞」を与え，表彰することを定めた．

これによって，匿名加工の技術として優れたデータだけでなく，技術者の解釈の妥当性を，多くのプライバシー研究者からの投票という形で検証することができた（**図7**）．

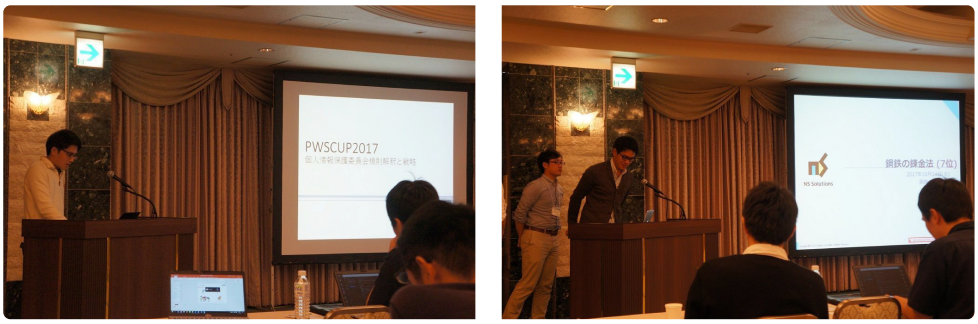

図7　会場におけるプレゼンテーションの模様

4．2017年度のコンテスト結果

4.1　総合順位と安全性・有用性の分布

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チームに公開した．公開された匿名加工データに対して，他の参加チーム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． 本稿ではその中から本戦にて実施された133個の匿名加工データと724個の再識別データの結果について述べる．

図8の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作成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チームから攻撃された後の結果（薄青部分）に分かれている．最終的な安全性は，サンプルアルゴリズムを含めた，他チームからのすべての再識別攻撃の成功率の最大値を採用した．

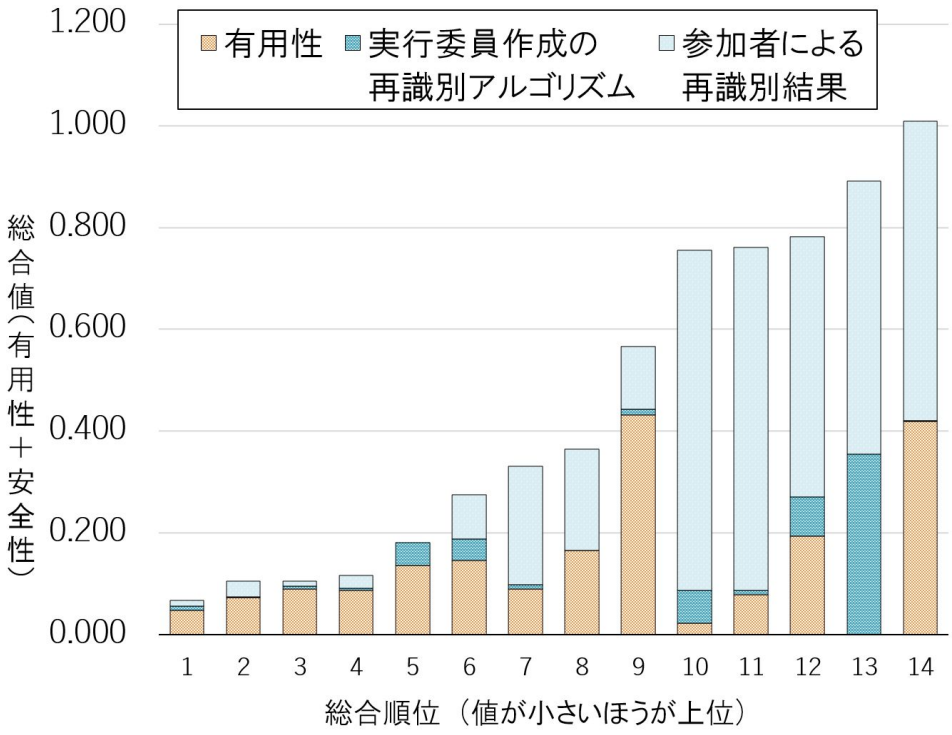

図8　本戦提出データの有用性と安全性

サンプルのアルゴリズムは，コンテスト開始前に実行委員会が想定した再識別攻撃しか防ぐことができないため，すぐに参加チームに対策されてしまう．しかし，他のチームからの再識別攻撃は，匿名加工アルゴリズムを推定して作成されたものであるため，より攻撃力が強い．図8のグラフでは，薄青部分が大きいほど，他の参加チーム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．

図8のデータから青と薄青部分だけを抽出したグラフが**図9**である．いくつかの匿名加工データは，実行委員会作成のアルゴリズムに対して，ほとんど再識別されないように加工されているが，他のチームからの再識別攻撃によって安全性を大きく落としていることが読み取れる．

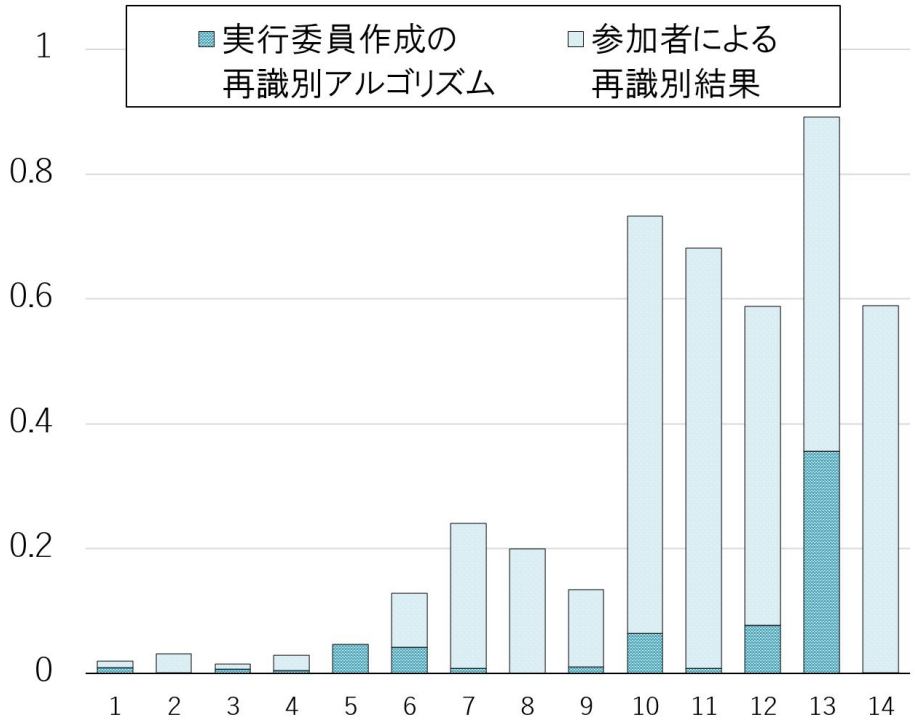

図9　本戦提出データの安全性

表6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．予選と本戦を通じて，最も有用性と安全性の和が小さかったチーム「君の名は～ユアネーム～」が総合優勝となった．

表6　上位10チームの有用性と安全性

順位	チーム名	データ名	有用性	安全性	平均値
1	君の名は~ユアネーム~	(rai)^4se	0.047600	0.019500	0.033550
2	beard_bros	final	0.073800	0.031000	0.052400
3	イワシ 326kg	生姜煮	0.089725	0.015500	0.052612
4	さきがけ	201710230241	0.087196	0.029000	0.058098
5	ステテコ西垣	AT__004	0.135743	0.046000	0.090871
6	M-OND-A	S	0.146653	0.128000	0.137327
7	鋼鉄の錬金術師	aaaa	0.090000	0.240500	0.165250
8	脱ぼっち	2m	0.166018	0.199000	0.182509
9	あのーに	201710220536	0.432556	0.133500	0.283028
10	tsukuba-kde	201710230951	0.022918	0.733000	0.377959

また，有用性と安全性の最終的な値は，指標群における最大値が採用される．そのため，各チームは何らかの指標に対する加工を最大値と設定して，その値に収束させる戦略を企てる．提出された匿名加工データの有用性指標の相関係数を**図10**に示す．

	E1	E2	E3	E4	E5	E6
E1	1.000					
E2	0.965	1.000				
E3	0.823	0.780	1.000			
E4	0.107	0.064	0.076	1.000		
E5	0.279	0.242	0.205	0.727	1.000	
E6	0.017	-0.029	-0.002	0.023	0.037	1.000

n = 133（本戦 匿名化フェイズ提出データ）

図10　本戦提出データにおける有用性指標の相関係数

これによると，有用性指標E1，E2，E3まではレコメンドエンジンに関係する指標であり相関係数が0.78以上と高い数値を示している．これらの指標で評価される属性が，商品ID，単価，購入数と共通であることから，どれか1つの指標を最大値とし，他の指標をその値に近似するレベルまで加工するためである．

また，有用性指標E4，E5は日付と価格の摂動量を表し，相関係数0.727とこちらも高い数値となっているが，その値はE1，E2，E3の指標との相関係数は低い．これは，レコメンドエンジンの指標群がデータ全体における集計値を用いている一方，E4，E5はトランザクションデータのレコードごとに紐づいた絶対値の差を示しており，両者の有用性を高めるための加工方法が異なるためであると考えられる．この指標の違いについては5.1節にて述べる．

これら，算出方法が異なる指標群を同時に満たした匿名加工データは，複数の分析手法を適用した場合でも，有用な結果が得られることが期待できる．

有用性，安全性の分布の例として，2017年度の優勝チーム「君の名は〜ユアネーム〜」の最終結果について**表7**，**表8**に示す．最終順位における有用性は，有用性指標E1-E6における最大値を採用するため，有用性指標群の最大値（最も悪い）であるE6-nrow（レコードを削除した行数）の値が使用された．その値に対応するようにE4（日付の誤差）E5（価格の誤差）の指標を，近似するレベルまで摂動していることが分かる．

表7　トップチームの有用性詳細

番号	有用性指標	値	最大値
1	E1-ItemCF-s	0.000727	
2	E2-ItemCF-r	0.005660	
3	E3-topk(1)	0.010000	
4	E3-topk(2)	0.006237	
5	E4-diff-date	0.047594	
6	E5-diff-price	0.047595	
7	E6-nrow	0.047600	○

表8　トップチームへの再識別攻撃成功率の詳細

No.	攻撃チーム	攻撃回数	部分知識25%	部分知識50%	部分知識75%	部分知識100%
1	さきがけ	3	**0.010**	0.012	0.012	**0.038**
2	イワシ 326kg	6	**0.010**	0.014	0.012	0.020
3	MDLer	2	0.006	0.006	0.006	0.030
4	beard_bros	4	0.000	**0.016**	**0.014**	0.016
5	脱ぼっち	8	0.000	0.010	0.010	0.024
6	鋼鉄の錬金術師	3	0.000	0.000	0.000	**0.038**
7	ステテコ西垣	3	**0.010**	0.010	0.008	0.010
8	Francanada	1	0.006	0.012	0.006	0.006
9	まめしば	1	0.000	0.000	0.000	0.000

最終順位における安全性は，他のチームから再識別攻撃された成功率の最大値の平均値を用いる．2017年度の再識別攻撃は，元の購買履歴データから一定割合をランダム抽出（25%，50%，75%，100%の4種類）した部分知識を用いて行われた．表8の攻撃成功率の詳細を見ると，部分知識（25%，50%，75%，100%）への再識別攻撃の成功率の最大値は，それぞれ（0.010，0.016，0.014，0.038）であり，その平均値0.0195が最終的な安全性の順位計算に用いられた．また，全データを通じた最大再識別リスクは0.0380であり，これは人数にして500人中19人が再識別された計算となる．

トップのチームが約4%の再識別成功率で終了したのに対し，50%以上再識別されたデータも5チームあり，上位と下位における安全性には大きな差がみられた．また，有用性が低いのに安全性が低いデータも存在しており，データの摂動量が，安全性に直結するわけではないことを示している．

参加チーム同士の再識別攻撃の状況を示したグラフが**図11**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，他の参加チーム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，他の参加チームの匿名加工の方式を推定しなくてはいけない．

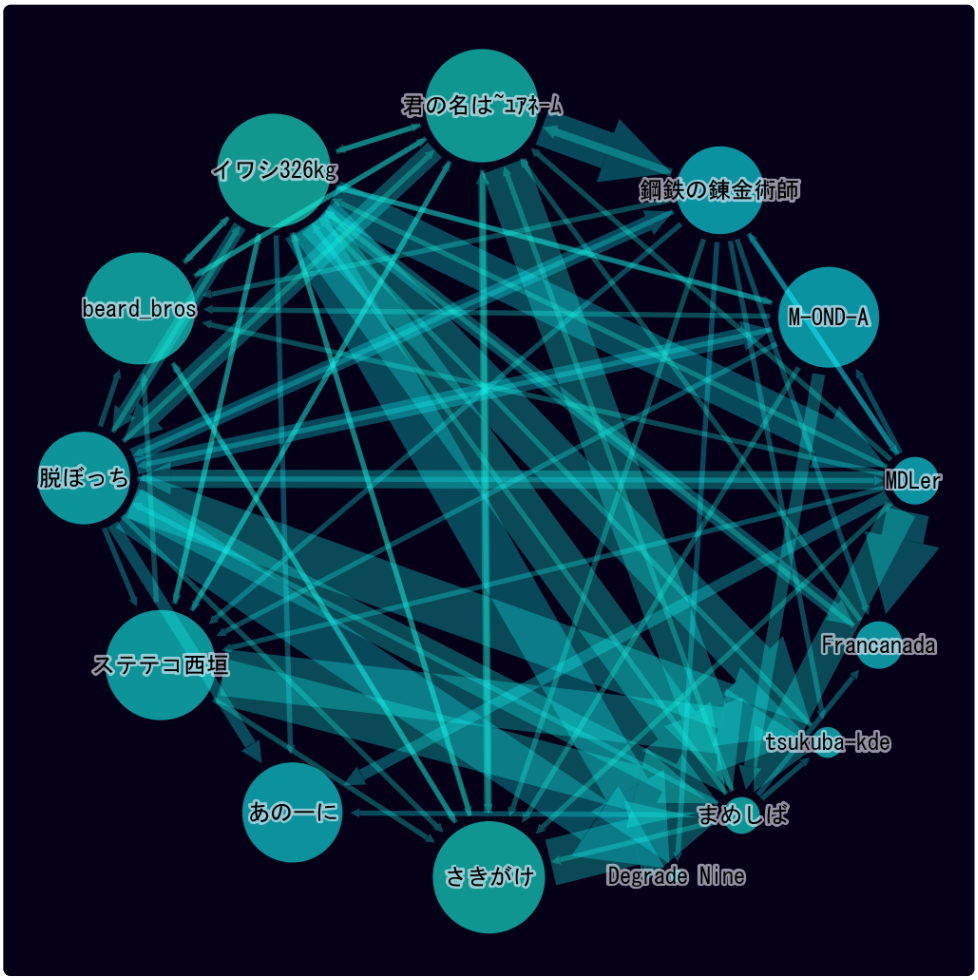

図11　各チームの攻防を示すグラフ

そのため，参加チームはさまざまな匿名加工を想定し，多くの再識別アルゴリズムを作成，その結果を検証する作業を，決められた期間の中で繰り返す．PWS Cupにおける安全性は，このような多くのチームによる安全性検証の繰り返しによって得られた結果だといえる．

4.2　コンテストの運営

これらの順位やデータの詳細は公式HP （https://pwscup.personal-data.biz）を通じて，**図12**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．予備戦はすべてオンライン参加が可能なため，2017年度は台湾，カナダのチームが参加している．

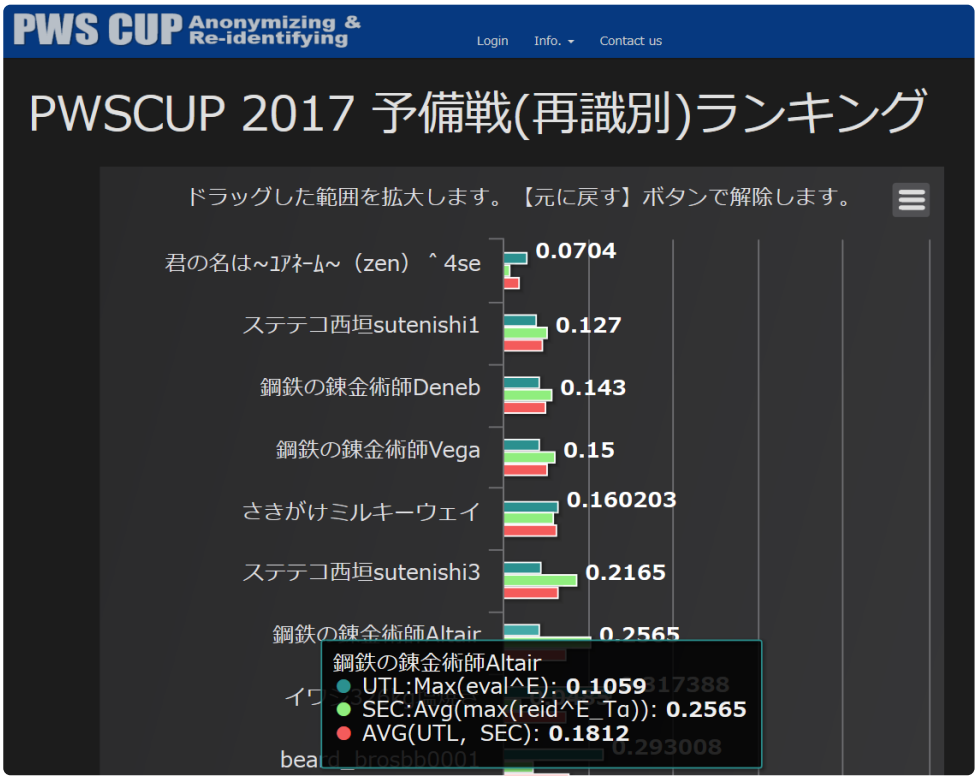

図12　Webサイトでの予備戦ランキング

また，PWS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，他のチームが提出した匿名加工データの再識別を行う．会場では**図13**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．会場の模様について**図14**に示す．

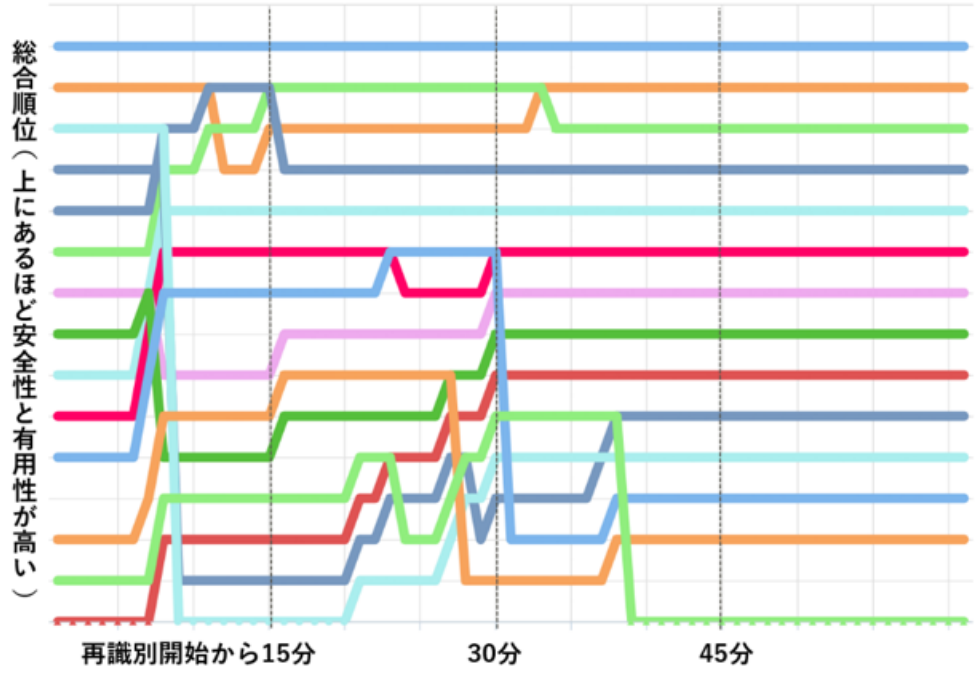

図13　会場で表示した順位変動図


図14　本戦会場の模様

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．コンテストの本戦まで進むと，上位チームは，確率的にしか個人が識別されないような匿名加工データを生成している．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ことが読み取れた．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[12]ことが報告されている．

4.3　再識別賞受賞チームにおける規則の解釈と措置

本節では，各参加チームによる規則第19条4号5号の解釈とそれに対して講じた措置の発表を行い，その結果「匿名加工基準賞」を得たチーム「M-OND-A」のよる発表内容を，匿名加工基準に対する解釈の一例として紹介する．

各号に対する解釈

4号は，レコードに含まれる一つひとつの値のうち，特異な記述と解釈した．今回のデータセットでは商品はすべて商品IDによって管理されており，商品によって社会通念上の特異性を判断することはできず，単価や数量にも極端な外れ値はなく，特異性はないと判断した．また，4号における「特異な記述」の有無は，母集団からのサンプリングの方法にも依存すると考えられる．

5号は，各顧客に関するレコードの集計値に現れる特異性だと解釈した．今回のデータセットであれば，購入した月のパターンや，各月の合計購入商品数，レコード数なども考慮の対象とした．

規則第19条とPWS Cup2017の比較

PWS Cup2017ではデータセットとユースケースのみならず，再識別条件も定義されており，それらのルールのもとで参加チームが技術を競い合うものである．それぞれの匿名化処理技術や再識別技術を客観的に評価するものとして，非常に意義のあるものであるが，その一方で，同じ方法で匿名化処理された実データを匿名加工情報として，流通させることは難しい．なぜなら，再識別条件やユースケースの定義は同じデータセットに対してもいくつか考えられるものがあり，規則第19条に対する措置はそれぞれ異なると考えられるためである．

これらの解釈は，あくまでも一例であり，他のチームにおいてはそれぞれの視点で措置を行ったことが報告された．その他のチームの解釈・措置については，別途Webサイトにて公表されている．今後の匿名加工基準の検討の参考となることを望む．

全チームの発表内容は事前のアンケート等でも確認され，その多くが個人情報保護委員会の担当者に届けられている．その個別のコメントについては公表できないが，それぞれの基準解釈については，明確に誤ったものではないことが，実行委員，各参加チームに伝えられている．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．

5. コンテスト結果に関する考察と議論

5.1 PWS Cup2017上位チームに特徴的な加工方法

本節では，筆者らが本戦のプレゼンテーションを聴講した結果，多くのチームで考えられた匿名加工の手法について概要を述べる．PWS Cup2017の総合優勝者である濱田らのアルゴリズム[12]も，別途参照いただきたい．

まず，3.2節で記述した通り，PWS Cup2017は再識別の定義が「年間を通してすべての仮名を特定された場合再識別されたとする」であったため，各顧客のトランザクションのうち，ある1つの月だけでも仮名を特定されなければ再識別には該当しない．

本戦参加14チームのうち上位9チームは，トランザクションデータの属性のうち，［購入日，単価］と［商品ID，数量］を切り離して加工を行った．その理由は，前者はトランザクションデータの行番号に紐づけられたまま有用性が評価され（E4，E5），後者は年間を通した統計値で評価される（E1，E2，E3）ためである．したがって，レコメンドエンジン型の指標で評価される［商品ID，数量］は，顧客と商品の組合せごとの合計購入点数を保持していれば，月や顧客IDを超えた加工を行ってもE1，E2，E3への評価には影響を与えない．

その点を考慮し，顧客ごとにE1，E2，E3の有用性に与える影響が最も小さい月のすべてのレコードに，それ以外の月とは別の仮名を付与することで，その月を分割した．

その上で，分割し別の仮名を付与したレコードが，本来の顧客の他のレコードと同一人物のものだと特定されないように，購入日や単価，さらにはレコード数，購入商品集合などの個人を特定され得る情報を撹乱した．

以上の手法によって，定義された有用性を高く保ちながら，再識別を防止するデータに加工することができた．

ここで，**表9**と**表10**を用いて有効な匿名加工手法について紹介する．表9と表10を比較すると，6行目のレコードに他の5つのレコードと異なる仮名が付与されている．

表9　トランザクションデータの例

	顧客 ID	購入日	商品 ID	単価	数量
1	12345	1/5	A400X	10.5	2
2	12345	1/23	B500C	2.5	14
3	12345	2/12	A400X	10.5	15
4	12345	2/14	A400X	10.5	3
5	12345	2/27	P230A	40.0	1
6	12345	3/9	B500C	2.5	5

表10　匿名加工したデータの例

	顧客 ID	購入日	商品 ID	単価	数量
1	**Ab4xd**	1/5	A400X	10.5	2
2	**Ab4xd**	1/23	B500C	2.5	**19**
3	**Ab4xd**	2/12	A400X	10.5	15
4	**Ab4xd**	2/14	A400X	10.5	3
5	**Ab4xd**	2/27	P230A	40.0	1
6	**BB89Q**	**3/20**	**P230A**	**40.0**	**20**

顧客ID「12345」による商品ID「B500C」の購買履歴が行番号2のレコードに集計され（数量を合計値に変換），購入日，商品ID，単価も異なる値に変更されている．

このように加工することで，顧客ID「12345」に関する1，2月のレコードは特定されても，3月のレコードは特定されず，今回のPWS Cup2017の再識別条件の定義のもとでは，顧客ID「12345」は再識別されないことになる．

5.2　再識別率の定義に関する議論

2017年度のルール制定において議論された点として，再識別率の定義がある．本節では再識別に関する考え方について，実行委員や参加者の間で交わされた議論の一部を紹介する

議論の要点は，ある個人を再識別するというコンテストにおいて，再識別された個人ごとにスコアの軽重を付けるべきかどうか，である．スコアの軽重とは，たとえば再識別されたユーザ1名に対して，購買金額が多い人の再識別スコアや，購買した月が多い人の再識別スコアを，大きく見積もるべきか，ということである．

まず，コンテストで利用されたデータセットの種類から，再識別の定義は，顧客マスタ，購買履歴データ，仮名表の3種類が存在することに留意されたい．それぞれの違いについて**表11**で述べる．

表11　検討された再識別定義の種類

種類	検討された再識別数の定義
マスターデータ (顧客マスター M)	再識別に成功したユニークなユーザ数： PWSCup2015，2016で採用した方式
トランザクションデータ (購買履歴データ T)	再識別されたレコード数： 購入した回数が多いユーザの再識別に成功するとスコアが高くなる．
	再識別されたレコード数*金額： 支払い金額が高いユーザの再識別に成功するとスコアが高くなる．
仮名表 f	セル数方式： （12か月×ユーザ数）のセルの中で何セルの再識別に成功したかを検証する．ただしユーザに応じて購入月のばらつきがあるため，最終データの調整が必要．
	Or方式： 12か月分の内のn か月（n>0）の仮名の再識別に成功した場合，1名の再識別に成功した，と定義する．
	And方式： 12か月分の全ての仮名の再識別に成功した場合，1名の再識別に成功した，と定義する．

過去のコンテストルールでは，主にユニークな顧客マスタを用いて再識別成功率の算定を行ってきた．その場合，プライバシー侵害された顧客はあくまで1名であり，そのスコアに軽重を付けない．これは事業者等においてパーソナルデータが漏洩した場合，その漏洩した人数に対して損害賠償等の対応を行う方式を模している．

しかし，パーソナルデータを漏洩されたユーザの観点から考えると，データの行数やそのデータの持つ意味のほうが重要と考えるかもしれない．たとえば，1ドルの商品を購入したという情報より，1万ドルの商品を購入したという情報の方が，個人が受ける影響や，その後の損害賠償等の処理額が大きくなるだろう．

このような，個人ごとのプライバシー侵害のレベルを評価するには，購買履歴データの値（たとえば購買総額や購買回数）を用いてデータの機微性とその影響を定義する必要がある．しかし，これらの値を一概に定義することはコンテストでは困難であり，2017年度は，購買履歴データのレコード数や属性までフォーカスした案は見送られた．

それに代わり，2017年度は1つの識別子に対して，複数の仮名を利用するルールを活用するため，仮名表による再識別率が提案された．しかし，その場合でも定義は複数存在する．その内，検討された代表的な方式は，セル数方式，Or型方式，And型方式である．

図15にセル数方式の再識別率の例を示す．再識別攻撃者が推定した仮名表と，元の仮名表を比較して，（ユーザ数×12カ月）のセル数のうち，何セルが再識別されたかを競うものである．これは再識別攻撃の成功数を正確に計測する手段ではあるが，その反面「何人のユーザの再識別に成功したのか」は判明しない．すなわち1人が12カ月分すべて再識別されたのか，それとも12人が1カ月ずつ再識別されたのか，判別ができない課題がある．

図15　セル数方式の再識別率の例

PWS Cup2017開始当初は，この指標が安全性指標として用いられていた．しかし，影響がある個人の数が明確に確認できない指標は，不完全であるという議論が実行委員の中でも発生したことから，開始から1週間程度でルールを変更し，コンテストを再スタートさせることになった．

しかし，再スタートするためのルール変更案に対しても多く議論がなされた．その代表例がAnd方式とOr方式である．

And方式は，12カ月すべての仮名が再識別された場合に，1人再識別されたものと定義する方式である．一方Or方式は12カ月のうちnカ月（n>0）以上再識別された場合に1人再識別されたものとする方式である．

図16にAnd方式の例を示す．本方式は12カ月すべての仮名を再識別する必要があるため，5.1節で示した結果データ全般について，全月のデータを守るのではなく，12カ月の中の1カ月だけを守る，という戦略が効果的に機能するという課題がある．

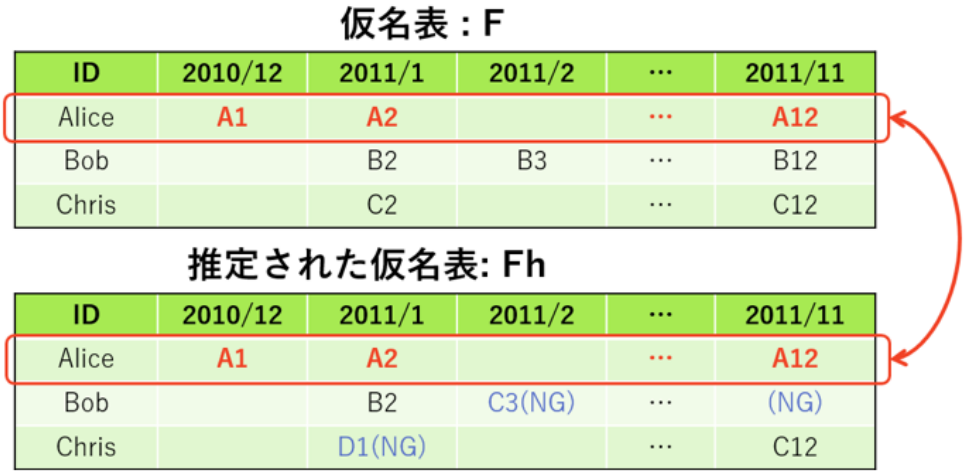

図16　And方式の再識別率の例

その反面，Or方式はnか月（n>0）分の仮名の再識別に成功した場合を想定するため，一般人にも分かりやすい指標である．しかし，その反面，nカ月という基準を定めることが困難である．

たとえば，3カ月分の仮名を当てた場合に1人が再識別された，と定義した場合を考えてみよう．購買履歴データには1カ月のみしか購入していないユーザがおり，その場合には，その他11カ月分のデータが存在しない．その場合は削除値（ルールでは”DEL”と表記する）を3個加えることで，高い確率で正解できてしまう課題がある．

また，このようなルールの制限によって，参加チームはその値に特化した加工を行う可能性が高くなる．それでは今年度の目的の1つでもある長期間の仮名分割による安全性検証が達成できない恐れがある．

セル数，Or方式，And方式と，それぞれ課題を総合的に判断した結果，12カ月分の仮名すべてに正解した場合が，最も明確なルールとなるため，And方式にルールが定まった．

4.1節で紹介した優勝チームのデータについて，再識別率をそれぞれ検証したところ，**表12**の結果を得た．And方式で19人再識別されたデータは，セル数に換算すると約53%の再識別率となる．また，その際に元となる識別子は1087の仮名まで分割された．この仮名の分割数と安全性の関係性2017年度の結果を用いた検証論文[13]が発表されており，基本的に分割数が多いほど安全性が高いことが検証されている．

表12　優勝データにおける再識別定義の違い

再識別定義	数値
And方式	0.038（19人/500人）
セル数方式	0.529（773セル/1460セル）
仮名分割数	500人　→　1087人

これらの数値をベースに，仮名分割された場合の再識別のあり方について技術的な議論の進展を期待する．

6. まとめ

個人情報保護法の改正によって匿名加工情報の枠組みが作られたが，法律，規則，ガイドライン等，多くの参考資料を解釈し，それを具体的な加工アルゴリズムに落とし込むことは困難である．特に規則19条4号「特異な記述等」，5号「個人情報データベース等の性質を勘案」などの個所は，個別の解釈を多分に含む可能性がある．しかし，改正法が求める匿名加工方法の安全管理義務などの影響から，研究や知見の共有が進んでいないのが現状である．

そのような状況に対して，PWS Cupはガイドラインが求める基準と技術的な要請などから，毎年新しいルールと評価指標を考案することで技術者・研究者の技術向上を図っている．

コンテストを経て得られた知見について以下にまとめる．

- 有用性の基準として採用されたレコメンドエンジンの精度は，安全性指標との関係性により，購入日，単価，商品ID，数量などの値を変更することで，大きく有用性を落とさずに安全性を高めることができた．
- 匿名加工データの再識別攻撃の成功率は，攻撃時間を長くすることで高まるが，匿名加工として確率的なかく乱や同値類化が適切になされている場合，一定時間を越えても安全性の値が大きく変化しない．
- 統一的な安全性指標として用いることができる再識別率という考え方は，顧客マスタ，購買履歴データ，仮名表で，それぞれ別の指標が提案された．それぞれの指標には利点と課題があり，すべてを1つの指標でカバーするのは困難である．
- 仮名の分割数の増加と安全性指標の検証は，今年度のデータおよびルールを用いた限りでは相関している．しかし，他のルールや有用性要件を変化させた場合の検証は行われておらず，今後の検討課題である．
- 規則19条における安全性の解釈を行い，その解釈をアルゴリズムに反映した場合でも，匿名加工データの安全性を高めることが可能であることが確認された．

これらの知見を含む，PWS Cup2017で考案された匿名加工技術や評価の手法は，異なる有用性，安全性の要件を持つ，他のデータにそのまま適用することは困難である．しかし，与えられた状況に応じて，最も有用性，安全性の高いデータを生成するという経験は，実際のデータ処理の現場でも効果を発揮するだろう．

コンテストを通じて，パーソナル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．

謝辞　本稿執筆にあたり，PWS実行委員の皆様，およびコンテスト参加チームの皆様より，多くのご支援をいただきました．厚く御礼申し上げます．

参考文献

1）個人情報の保護に関する法律および行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律（平成27年法律第65号）．
2）個人情報保護委員会：個人情報の保護に関する法律施行規則 (2017)，https://www.ppc.go.jp/files/pdf/290530_personal_commissionrules.pdf
3）個人情報保護委員会：個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）(2016)，http://www.ppc.go.jp/files/pdf/guidelines04.pdf
4）菊池浩明，山口高康，濱田浩気，山岡裕司，小栗秀暢，佐久間淳：匿名加工・再識別コンテストIce & Fireの設計，コンピュータセキュリティシンポジウム2015論文集，2015（3），pp.363-370 (2015)．
5）菊池浩明，小栗秀暢，野島　良，濱田浩気，村上隆夫，山岡裕司，山口高康，渡辺知恵美：PWS Cup: 履歴データを安全に匿名加工せよ，コンピュータセキュリティシンポジウム2016論文集，2016（2），pp.271-278 (2016)．
6）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：PWS Cup2017: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)．
7）PWS Cup 実行委員会：PWS Cup 2017 匿名加工・再識別コンテスト 競技ルール，Ver1.3 (2017)，https://pwscup.personal-data.biz/web/pws2017/index.php
8）秋山裕美，山口幸三，伊藤伸介，星野なおみ，後藤武彦：教育用擬似ミクロデータの開発とその利用～平成16年全国消費実態調査を例として～，統計センター製表技術参考資料，16，

pp.1-43 (2012).
9）Domingo-Ferrer, J., Ricci, S. and Soria-Comas, J. : Disclosure Risk Assessment via Record Linkage by a Maximum-knowledge Attacker, Privacy, Security and Trust（PST）, 2015 13th Annual Conference on, pp.28-35 (2015).
10）Chen, D., Sain, S. L. and Guo, L. : 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).
11）個人情報保護委員会：個人情報保護委員会事務局レポート：匿名加工情報「パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」(2017), https://www.ppc.go.jp/files/pdf/report_office.pdf
12）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 (2018).
13）菊池浩明：購買データの匿名加工について，第31回多値論理とその応用研究会（多値論理研究会） (2018).

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ー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）．

黒政敦史（正会員）kuromasa@fujitsu.com
1982年国立秋田工業専門学校卒業．富士通（株）を経て，2002年よりニフティ（株）にてISP事業，新規ビジネス開発を担当．2017年4月ニフティの分社化により富士通クラウドテクノロジーズ（株）に在籍．匿名化データを活用したビジネス開発を担当．（一社）情報法制研究所上席研究員，情報法制学会会員．

中川裕志（正会員）
1953年生．1975年東京大学卒業．1980年同大学大学院博士課程修了．横浜国立大学を経て，1999年より東京大学情報基盤センター教授．自然言語処理，統計的機械学習，プライバシー保護データマイニングの研究に従事．

菊池浩明（正会員）kikn@meiji.ac.jp
1990年明治大学院博士前期課程修了．1994年同博士（工学）．（株）富士通研究所，東海大学情報通信学部を経て，2013年より明治大学総合数理学部先端メディアサイエンス学科教授．1990年日本ファジィ学会奨励賞，1993年本会奨励賞，1996年SCIS論文賞，2010年本会JIP Outstanding Paper Award．2013年 IEEE AINA Best Paper Award．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM各会員．本会フェロー．

門田将徳（非会員）mntiottkdk.ry@gmail.com
2018年東京大学 大学院学際情報学府修了．

投稿受付：2018年2月15日

採録決定：2018年3月26日
編集担当：荒木拓也（日本電気（株））