
公募企画

公募企画ワークショップ9

パーソナルデータの利活用のための情報処理技術の方向性について

2017年11月22日(水) 08:45 ～ 10:45 G会場 (10F 会議室1006-1007)

[3-G-1-PS9-5] 「第3回プライバシーワークショップ」開催報告

千田 浩司（日本電信電話（株））

今年10月23～25日に行なわれる「第3回プライバシーワークショップ（PWS2017）」の開催報告を行う。

PWSは、情報処理学会コンピュータセキュリティ研究会の主催で2015年から、パーソナルデータの利活用とプライバシー保護を両立させる技術や基準の発展を目指し、学術機関や現場の技術者等との間で議論・交流を行う場として継続的な活動を行っている。PWS2015では、匿名化処理とそのアタックの技術を競うコンテスト「PWS Cup」や、「現場で求められるプライバシー保護」と題して医療情報の研究者も含めた学際的な議論が活発に行われた。PWS2016では、PWS Cupの開催や、企画セッションとして「プライバシーを保護したゲノム利用の現状と課題」と題したパネル討論等が行われた。パネル討論では、ゲノム利用とプライバシーに関する専門家が集まり、ゲノム利用においてどのようなプライバシーリスクがあるのか、技術的な対策はどこまで進んでいるのか、そして法制度の整備状況など多岐に渡り理解を深めた。一般講演においても、ゲノム利用とプライバシーに関する話題が多く見られ、関心の高さが伺える。

今年のPWS2017では、基準が具体化されつつある匿名加工情報をより強く反映させたPWS Cupの開催、そして欧米で本格的な議論が進みつつある、パーソナルデータ利活用におけるプライバシーリスクとその技術対策を踏まえた討論、さらにはパーソナルデータをセキュアに「名寄せ」して横断的な利活用を行うための技術や基準の構築に向けた検討が行われる予定である。特にパーソナルデータのセキュアな名寄せは、2017年4月に成立した次世代医療基盤法の下でパーソナルデータを扱う上での重要な要件となることが想定される。

PWSでは、セキュリティやプライバシー保護が様々な分野で重要なファクターであることを踏まえ、学際的な取り組みを積極的に企画している。今後も医療情報とセキュリティ・プライバシー保護の接点で議論を深めていきたい。

パーソナルデータの利活用のための情報処理技術の方向性について

木村 映善^{*1}、藤村 明子^{*2}、美馬 正司^{*3}、菊池 浩明^{*4}、千田 浩司^{*2}、佐久間 淳^{*5}

^{*1} 愛媛大学大学院 医学系研究科、^{*2} 日本電信電話株式会社 NTT セキュアプラットフォーム研究所、
^{*3} 株式会社 日立コンサルティング、^{*4} 明治大学 総合数理学部、^{*5} 筑波大学大学院 システム情報工学研究科

Trend of personal data utilization and personal data protection technologies for the secondary usage of health data

Kimura Eizen^{*1}, Fujimura Akiko^{*2}, Mima Tadashi^{*3}, Kikuchi Hiroaki^{*4}, Chida Koji^{*2}, Sakuma Jun^{*5}

^{*1} Dept. Medical Informatics of Medical School of Ehime University, ^{*2} NTT Secure Platform Laboratories, NTT Corporation, ^{*3} Hitachi Consulting Co., Ltd., ^{*4} School of Interdisciplinary Mathematical Sciences, Meiji University, ^{*5} Department of Computer Science, University of Tsukuba

The revised Personal Information Protection Law takes effect in May of this year, and the ethical guidelines on clinical research and epidemiological research were revised. Meanwhile, when using data beyond the scope of the original research or providing data to a third party, it is required to satisfy the five requirements on anonymization by the Personal Information Protection Commission. However, detailed technical standards for anonymization that can deal with these five requirements have not yet been determined. Also, since anonymization is inevitable to deteriorate the quality of data, there is also a demand for a secret computing technique to calculate statistics etc. while encrypting data. We will introduce domestic the trends related to anonymous processing under the revised Personal Information Protection Act and the topics concerning certified anonymous processing medical information operators, the activities of the workshop of JAMIA to developing technical standards for anonymization of health data, the guideline on photo data utilization and statistical analysis of medical data using homomorphic encryption.

Keywords: personal data, the Act on the Protection of Personal Information, privacy, secondary use, genome medicine

1. はじめに

今年の 5 月に改正個人情報保護法が施行され、臨床研究・疫学研究に関する倫理指針も現実的な運用ができるかたちに改定された。一方で、当初の研究範囲を超えてデータを利用したり、第三者にデータを提供したりする場合は、個人情報保護委員会における匿名化の 5 要件を充足することが求められている。しかし、この 5 要件に対応できる匿名加工処理の詳細な技術的基準は未だに定まっていない。また、匿名化によりデータの品質の低下は不可避であるため、データを暗号化したまま統計量等を計算する秘密計算技術への需要もあるが、こちらについても医療情報システムの安全管理に関するガイドラインを始めとして、諸ガイドラインにおける位置づけが明確になっていないために、導入の広がりを見せていない。その中で、来年中に施行予定の次世代医療基盤法が今年 4 月に成立し、認定事業者のありかたについての議論が急速に進められている。我々は、一昨年沖縄の医療情報学連合大会にて匿名化やリスク評価に関する国内外事例を紹介し、医療分野におけるパーソナルデータの行方について議論した。そして、昨年は、パーソナルデータの利活用に関するガイドラインに関して主に技術的見地からその可能性と課題について論じた。今年は、これらの議論を引き継ぐ。まず、改正個人情報保護法下の匿名加工に関する国内動向および認定匿名加工医療情報作成事業者に関する動向について紹介する。そして、医療分野における匿名加工の技術的基準の策定を視野にいれた医療情報学会課題研究会の活動内容について報告する。一方で、個人情報を含むデータ利用事例としてカメラ画像利活用に関するガイドライン、準同型暗号を用いた医療データの統計解析について紹介する。最後に、一層のデータ利活用のために必要な技術、及びその

技術利用を推進するための制度設計、ガイドラインのありかたについて意見交換する。

2. 匿名加工情報に関する国内動向

2017 年 5 月 30 日に改正個人情報保護法が完全施行された。匿名加工情報に関するルールについて、「個人情報の保護に関する法律施行規則」「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)」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、そして各認定個人情報保護団体指針、という複数の法令やガイドライン類で構成され、匿名加工情報の加工基準と各種義務など必要最低限の事項が一通り定められた。今後は、匿名加工情報制度の実務環境の整備の重要性が各分野で増していくことが予測される。

医療情報分野においては、従前より個人情報保護法と医療情報の関係で2次利用上の「匿名化」をめぐる措置が懸案事項であった。いわゆる「連結可能匿名化」と「連結不可能匿名化」が独自の概念であったことから、医療情報分野の研究を阻害せず、かつ個人情報保護法と整合性を取る「匿名化」をどのように制度設計するかということが重要課題だった。

このたび同 5 月 12 日に「医療分野の研究開発に資するための匿名加工医療情報に関する法律(次世代医療基盤法)」が公布された。同法は医療機関と認定匿名加工医療情報作成事業者の連携の下、医療情報の研究開発目的に本人の医療情報を匿名加工するしくみを制度化したものである。公布から 1 年以内の施行を前に政令以下ガイドラインやドキュメント類が検討中であるが、これとあわせて医療情報分野特有の背景に照らした実務上の環境整備が急務となっている。

本講演では、改正個人情報保護法の匿名加工情報制度を背景に、改正前から改正後の流れを解説し、新たな次世代

医療基盤法によりもたらされる医療情報分野の利活用の可能性や積み残しのおそれがある法的課題についても言及する。

3. 認定匿名加工医療情報作成事業者の動向

2017年5月30日に施行された改正個人情報保護法に医療情報を含む「要配慮個人情報」が規定され、プライバシー保護が進む一方、これまでの医療分野の研究(特に学術以外)が阻害されることが危惧されていた。このような背景を踏まえ「医療分野の研究開発に資するための匿名加工医療情報に関する法律」(以下、次世代医療基盤法)が第193回通常国会に法案として提出され、2017年5月12日に公布された。

次世代医療基盤法は、健康・医療に関する先端的研究開発及び新産業創出を促進し、もって健康長寿社会の形成に資することを目的としており、医療機関等においてあらかじめ本人に通知し、本人が提供を拒否しない場合、認定匿名加工医療情報作成事業者(以下、認定事業者)に医療情報を提供できるとしている。認定事業者は取得した医療情報を適切な匿名加工を行った後、医療分野の研究開発の用に供することができる。次世代医療基盤法については、公布から1年以内に施行されることになっており、施行に向けて、基本方針や政令等の検討が進められているが、その内容や検討状況については十分に明らかになっていない。

そこで、公開情報等を基に次世代医療基盤法の概要について整理を行うとともに、関連事業の状況等を踏まえ、認定事業者に関する動向について解説を行う。具体的には、事業の全体の枠組み、医療情報の範囲、認定事業者の認定基準、医療情報の収集の方法、匿名加工の基準、求められる安全管理措置等について整理する。匿名加工については、改正個人情報保護法の施行規則19条を基本とすることが想定されるものの、医療情報ならではの観点について検討する。さらに、国内外の類似事例、施策等を踏まえて、今後、次世代医療基盤法の施行に向けて、想定される論点等をまとめる。

4 匿名加工の技術的ガイドライン策定にむけて

個人情報保護法下において、第三者提供をする場合は原則的に事前に同意を取得しておくこと、またデータの取得経緯、提供の記録・管理が求められている。医療分野の研究開発に資するための匿名加工医療情報に関する法律(次世代医療基盤法)は、オプトアウトについて患者に丁寧な説明を実施することを前提として、にデータ収集をすることを可能にする制度環境を整備し、その結果得られた匿名加工された医療情報の安心・適正な利用を通じて、健康・医療に関する先端的研究開発及び新産業創出を促進し、健康社会の形成に貢献することを意図したものである。認定匿名加工医療情報作成事業者(以下、認定事業者)は高い情報セキュリティと運用管理技術を背景として適切なデータ管理を行い、十分な匿名加工技術を有するなどの一定基準を満たし、医療情報等の管理や利活用のための匿名化を適正かつ確実に行うことが出来る者として国に認定されるものである。次世代医療基盤法中において、「医療情報及び匿名加工医療情報について、適正な規格の整備をおこなうものとし、その整備は「国際的動向、医療分野の研究開発の進展等に応じて行う」とされている。また、匿名加工医療情報作成事業を行う者(認定事業者)は、主務大臣の認定を受けるにあたり、様々な書類を提出しなければならないが、その書類の中に「医療情報の整理の方法」「医療情報の加工の方法」が含まれている。

しかしながら、この匿名加工の方法及び認定に関して詳細な技術的な基準を含めた規格は現時点では存在しない。そ

こで、医療情報学会内に「匿名加工に求められる技術要件の研究会」と称する課題研究会を発足させた。この課題研究会の立ち位置と、検討してきた策定する匿名加工技術に関する基準、方向性について解説する。

5 カメラ画像利活用ガイドブックについて

IoT 機器の普及に伴い、我々の生活空間を多くのカメラが撮影し、生活者の意図を検知したサービスの向上やビッグデータとしての活用が始められようとしている。病床においても、転倒リスクのある患者の起床や移動を検出したり、睡眠時無呼吸症候群を抱える患者を遠隔モニタリングする応用が考えられる。カメラ画像に対する期待が膨らむその一方で、患者のプライバシー侵害や望まない形でデータが利用されてしまう不安が懸念されている。特に、2017年5月30日に完全施行された改正個人情報保護法の下では、顔画像を機械可読とした特徴量情報も個人番号と同様の個人識別符号に分類され、厳密な安全管理措置が求められるようになった。

そこで、カメラ画像を利活用する事業者に対して、配慮事項を整理して生活者の不安を取り除いた利活用を進めるために、IoT 推進コンソーシアム(総務省、経済産業省)では、2017年1月31日に、「カメラ画像利活用ガイドブック」を策定した。本ガイドブックでは、カメラ画像の活用を検討している幾つかの事業者のユースケースから、1. (店舗内等)カメラ画像からの性別、年齢などの属性推定、2. (店舗内カメラ等による)動線データ、行動履歴、3. (駅などの公共空間における)人物の識別とカウント、4. (車外カメラ等からの)道路、混雑度識別、5. (駅などの公共空間での)滞留状況把握などのいくつかの具体的な適用ケースについて、必要と考えられる配慮事項を整理している。本講演では、本ガイドブックの内容を紹介し、カメラ画像が個人情報となる得る条件などを整理する。医療分野におけるカメラ画像の活用における留意点を報告する。

6 準同型暗号を用いた医療データの統計解析

完全準同型暗号とは入力情報を暗号化したまま任意の関数の計算を可能にする性質を持つ暗号系の総称である。完全準同型暗号を実現する具体的な方式は長らく発見されなかったが、Gentry によって 2009 年に初めて実現可能な方式が提案された。提案当初の完全準同型暗号は暗号文や鍵が極めて多くの記憶容量を必要とする上に、実用的な時間で計算可能な乗算の回数が限られるなど、多くの制約があったが、その後の研究開発によって、完全準同型暗号が必要とする計算時間と記憶容量は飛躍的に改善されつつある。完全準同型暗号を活用することで、プライバシーを損なうことなく、組織の壁を超えた統計解析が実現されつつある。

完全準同型暗号の応用の一つとして、医療情報や遺伝情報を用いた統計解析があげられる。昨今成立した次世代医療基盤法は、各医療機関に散在している医療データを代理機関に収集し、それを個人毎にリンケージし、それぞれの情報が特定の個人と結びつかないように匿名加工した上で研究機関や医療機関に提供し、もって医療の高度化や医学研究の発展につなげることを主旨とする。次世代医療基盤法に基づく医療情報利活用の仕組みは極めて有用な医療データを産み出しうるが、代理機関には識別情報が付与された大量の医療データが集積されることから、極めて高いレベルのセキュリティが要求される。講演では準同型暗号を用いた統計解析を紹介するとともに、代理機関における高いレベルのセキュリティを確保する手段としての準同型暗号の利用可能性について議論する。