IMES DISCUSSION PAPER SERIES

情報セキュリティ・シンポジウム（第24回）の模様：
データ活用とプライバシー保護の両立

Discussion Paper No. 2024-J-12

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

1. はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies：CITECS）は、2024 年 2 月 15 日、「データ活用とプライバシー保護の両立～プライバシー保護技術を正しく理解する～」をテーマとして、第 24 回情報セキュリティ・シンポジウムを開催した。

近年、多くの組織が、戦略的にデータ活用を推進しながら、デジタル・トランスフォーメーション（DX）や新たな価値創造に向けた取組みを強化している。また、複数の組織がデータを持ち寄ることによって、高度な統合分析を目指す動きへの関心も高まっている。このように各組織においてデータを取り扱う際、そうしたデータに「個人に関する情報」が含まれている場合には、プライバシーへの配慮が必要となる。

こうした観点から、本シンポジウムでは、専門家の方々から、さまざまなプライバシー保護技術の特徴や技術を組み合わせた場合の効果について、技術と法制度の両面から解説いただくとともに、プライバシー保護技術の利用に当たっての留意点などについてパネル・ディスカッションを行った。当日は、金融機関やフィンテック企業などの実務家、システム開発・運用に携わる技術者、研究者など約 200 名がオンラインで参加した。本稿では、以下に示したプログラムに沿って、3 つの講演とパネル・ディスカッションにおける議論の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

【第 24 回情報セキュリティ・シンポジウムのプログラム】

- 講演 1「プライバシー保護技術の動向～主要技術の概要と組み合わせ事例の紹介～」
  LINE ヤフー株式会社 プライバシー&トラストチーム リーダー　竹之内隆夫
- 講演 2「プライバシー保護技術の国内法制度における位置づけ」
  ひかり総合法律事務所 パートナー弁護士　板倉陽一郎
- 講演 3「業界横断の安全なデータ活用に基づく社会課題解決の試み」
  株式会社 NTT ドコモ クロステック開発部 担当部長 セキュリティプリンシパル
  寺田雅之

[1] 文中の講演者やパネリストの所属および肩書きは、シンポジウム開催時点のものである。また、本稿において示された意見はすべて発言者個人に属し、その所属する組織の公式見解を示すものではない。また、本シンポジウムでの講演の資料等については、日本銀行金融研究所のサイト（https://www.imes.boj.or.jp/jp/conference/citecs/24sympo/24sec_sympo.html）を参照されたい。

- パネル・ディスカッション「プライバシー保護技術の利用に当たっての留意点」
  ・パネリスト：竹之内隆夫、板倉陽一郎、寺田雅之、
  日本銀行金融研究所 企画役　菅　和聖
  ・モデレータ：日本銀行金融研究所 企画役　田村裕子

2. 講演 1「プライバシー保護技術の動向～主要技術の概要と組み合わせ事例の紹介～」

竹之内は、企業におけるプライバシー保護への取組状況、および、主要なプライバシー保護技術の概要と最近の活用トレンドについて、次のとおり講演した。

（1）プライバシー保護は経営戦略の一部に

プライバシー保護においては技術面の対応を要するが、それだけですべて対応できるものでもなく、技術者と非技術者の連携が極めて重要となる。こうした連携に当たっては、相手方の専門分野に関する知識がある程度必要になり、例えば非技術者においても、プライバシー保護技術について一定の知識を備えておくことが望ましい。

海外では、ユーザのプライバシーに対する意識の高まりを受けて、プライバシー保護を経営戦略として位置づけるとともに、プライバシーへ配慮する姿勢をブランド化する動きが増えてきている。こうしたブランド化によって、ユーザから個人データ[2]を収集しやすくなる効果も見込めるようである。個人データはデジタル化社会において重要であり、企業活動において個人データの安全な収集・活用は不可欠となっている。国内企業がこうしたグローバル企業と伍していくうえでは、企業間でのデータ連携もありうべき戦略の 1 つであろう。そのためにも、プライバシー保護技術は今後より一層重要になっていくと考えられる。

（2）プライバシー保護技術とその組み合わせ

プライバシー保護技術にはさまざまな種類がある。近年の主流は、①差分プライバシーを満たす手法、②連合学習、③秘密計算[3]の 3 つであり、これらは概念の異なるプライバシー保護技術である。やや抽象的に表現すると、①差分プ

[2] 本講演では、「個人データ」を、個人に関するデータという意味で用いる。法令上の用語・定義ではない点には注意されたい。
[3] 本講演では、秘密計算を、データを暗号化したまま計算する技術の総称として用いている。

ライバシーを満たす手法はデータを「ぼかす」、②連合学習はデータを「減らす」、③秘密計算はデータを「隔離する」ことを通じて、それぞれユーザのプライバシーを保護する技術である。

より具体的に表現するために、ユーザのデバイスからサーバに個人データを送信して個人データベースに蓄積し、当該サーバで個人データを集計・加工したのち、分析結果を分析者に送信する、という典型的なデータ処理のフローを想定してみる。このとき、①差分プライバシーを満たす手法は、ユーザのデバイスからサーバに送信される個人データ、または、サーバから分析者に送信される集計結果のデータに確率的なノイズを付与するなどしてデータを「ぼかす」ものである[4]。②連合学習は、ユーザのデバイス内で個人データを用いた機械学習モデルの更新を行い、更新情報だけをサーバに送信することで、共有される個人データの範囲を「減らす」ものである。③秘密計算（TEE＜Trusted Execution Environment＞を用いる場合）は、個人データをサーバの安全な領域に「隔離」してから処理するものであり、処理中のデータも保護できる。このように、これらのプライバシー保護技術は、データ保護の様態や安全性の性質が異なるため、それぞれ単体で用いられる場合もあるが、近年では、複数の技術を組み合わせることでプライバシー保護を強化する事例が増えてきている。

イ．差分プライバシー

差分プライバシーとは、個人データまたは個人データベースの集計結果にノイズを加えるなどしてデータを確率変数化する手法について、その安全性を統計的に評価する尺度である。例えば、あるユーザ A の個人データを含まない個人データベースと、これを含む個人データベースを用意し、それぞれのデータベースから得られる集計結果にノイズを加えることを考える。このとき、両者の集計結果を区別できる確率が無視できるほど小さければ、集計結果からユーザ A に関する情報が漏れていないとみなすことができる。こうした性質がユーザ A だけでなくすべてのユーザに対して成り立つのであれば、当該手法は差分プライバシーを満たすといえる。差分プライバシーの特長は、個人データベースの情報を除くいかなる知識（背景知識）を持つ攻撃者に対しても安全性を保証できる点にある。

---

[4] 差分プライバシーには、セントラル差分プライバシーとローカル差分プライバシーの 2 種類がある。前者は、個人データベースを集計加工した結果を分析者などに提供する際に、サーバ側で集計加工結果にノイズを付加するものである。後者は、ユーザのデバイスから個人データをサーバに提供する際に、デバイス側で個人データにノイズを付加するものである。

ロ．連合学習

一般的な機械学習では、各ユーザのデバイスから個人データを集め、それらを訓練データとして集約したものを機械学習モデルの訓練に用いる。この場合、各ユーザの個人データは、機械学習モデルの訓練を実施する主体に送信・開示されることとなる。これに対し、連合学習では、個人データをユーザのデバイスから外部に送信することなく、機械学習モデルの訓練が行われる。具体的には、ユーザのデバイス内で機械学習モデルが更新され、その更新情報を受け取ったサーバが機械学習モデルを生成する。ただし、近年の研究において、機械学習モデルの更新情報から個人データを復元できる可能性が指摘されていることを受けて、更新情報に差分プライバシーを満たす手法を適用するケースが増えてきている。

ハ．秘密計算

秘密計算とは、処理中のデータに機密性をもたせることを目的とする暗号技術の一種である。秘密計算を実現する方法には、暗号アルゴリズムの安全性に依拠する MPC（Multi-Party Computation）と、ハードウェアの安全性に依拠する TEE がある。TEE では、処理するプログラムが不正に改竄されていないことを確認する機能もあわせて提供する。なお、ユーザのデバイスから個人データをサーバに送信して集計するタスクに秘密計算を適用すれば、ローカル差分プライバシー[5]を適用する際に個人データに付加するノイズを小さくできるとの研究結果が報告されており、こうした組み合わせは、個人データの有用性とプライバシー保護のトレードオフの改善に有効であることがわかっている。

（3）プライバシー保護技術の組み合わせ事例

イ．LINE ヤフー社によるスタンプの自動推薦

モバイル・メッセージ・アプリ「LINE」で提供するスタンプ[6]には、ダウンロードして使用するタイプ以外に、「LINE スタンププレミアム」[7]というダウンロードしなくても使用できるサービスもある。このサービスでは 1,200 万個以上のスタンプを利用可能であるため、ユーザが自身の好みに適したスタンプを選択し

---

5 脚注 4 参照。

6 スタンプとは、テキスト・メッセージに挿入できるイラストをいう。通常は、アプリにダウンロードしたスタンプ一覧から、ユーザが送信したいスタンプを選択する。推薦機能を利用する場合には、ユーザがテキストで「ありがとう」と入力すると、「ありがとう」とタグ付けされたスタンプが候補として表示される。

7 https://store.line.me/stickers-premium/landing/ja

やすくするよう、ユーザへの推薦機能が重要となる。推薦に当たっては、まず、スタンプの入手履歴データを訓練データとした機械学習の手法により、推薦するスタンプの候補を絞りこむ。次に、各ユーザのスタンプの閲覧・送信履歴データをもとに機械学習を行い、推薦候補を並び替える。これら 2 つのタスクのうち推薦候補を並び替える処理において、サーバ（LINE ヤフー社）に送信するプライバシーに関する情報を「減らす」観点から連合学習を採用したうえで、さらに機械学習モデルの更新情報を差分プライバシーにより保護している[8]。

スタンプ推薦機能におけるプライバシー保護については、エンジニアや開発者向けに詳細な技術仕様を記載したホワイトペーパーを公表している[9]。これは、プライバシー保護に関する取組みは外部からみえにくいため、積極的な情報発信が必要との考えからである。また、公表に際しては、技術者と非技術者に対して、それぞれの立場の違いを意識して理解しやすい情報発信を心がけている。

ロ．他社の事例

Google 社では、多言語キーボード・アプリにおいて、連合学習と差分プライバシー、および秘密計算を組み合わせて適用することで、ユーザのキーボード利用に関するプライバシー保護を図っている[10]。具体的には、連合学習においてユーザ端末がサーバに送信するモデル更新情報は差分プライバシーで保護されるほか、サーバにおけるデータ処理には秘密計算が適用されている。

また、Apple 社と Google 社による企業間連携の事例として、COVID-19 に関するデータ集計において、秘密計算と差分プライバシーの組み合わせが使用された[11]。具体的には、ユーザのデバイスからサーバに送信される個人データは差分プライバシーで保護されたほか、iPhone ユーザと Android ユーザの個人データを集計する際には、秘密計算が応用された。これにより、Apple 社と Google 社は、互いにユーザ端末の特定や位置情報の取得などができない仕組みとなっている。

国内では、複数の金融機関が取引データを持ち寄り、連合学習と秘密計算を応用して、顧客のプライバシーに配慮しながら不正送金検知の精度を向上させる実証実験の事例がある[12]。

---

8 https://privacy.lycorp.co.jp/ja/acquisition/privacy_techs.html

9 https://s.yimg.jp/images/cdo/privacycenter/2023renewal/pdf/ja/line-differential-privacy-whitepaper-ver1.0.pdf

10 https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/

11 https://www.google.com/covid19/exposurenotifications/

12 https://www2.nict.go.jp/oihq/seeds/detail/0024.html

3. 講演 2：プライバシー保護技術の国内法制度における位置づけ

板倉は、プライバシー保護技術の 1 つである秘密計算のうち暗号処理を伴う方式に関し、個人情報保護法における取扱いの現状について、次のとおり講演した。

（1）プライバシー・バイ・デザイン

1990 年代に提唱された「プライバシー・バイ・デザイン」は、システムの企画・設計の段階からプライバシーを保護する施策を組み込む考え方である。この考え方は、プライバシー保護技術を事後的に適用するアプローチのみではプライバシー保護を達成できないのではないか、との問題意識から生まれた。近年、プライバシー保護技術の利用事例が増えてきたことから、技術で解決できる課題とそうでない課題が明確になりつつある。本講演では、プライバシー保護技術のうち近年注目を集めている秘密計算について、日本の個人情報保護法上の位置付けを整理したい。

（2）個人情報該当性

個人情報保護法が対象としているのは、「個人に関する情報」であることが前提となっている「個人情報」である。そのため、個人に関する情報に該当しなければ、個人情報保護法の規制下にはおかれない。秘密計算とは、データを秘匿したまま演算処理する技術のことであり、直感的には、秘密計算において処理中のデータは、個人に関する情報ではないようにも思われる。しかしながら、個人情報保護委員会において、個人に関する情報に該当するかは、暗号化等によって内容が秘匿されているか否かを問わない、という見解が示されていることを踏まえると、秘密計算における処理中のデータであっても、個人情報該当性は失われないという前提で議論せざるを得ない。

（3）安全管理措置

個人情報保護法第 23 条では、個人情報取扱業者に対して、個人情報を含むデータ（個人データ）に、適切に安全管理措置を施す義務を課している。この安全管理措置の一環として、情報の漏えい等を防止する手法がガイドラインで例示されているが、秘密計算は例示された手法には含まれていない。もっとも、秘密計算が、情報の漏えい等を防止し、または、情報が漏えいした場合の影響を最小限に抑制する技術であることに疑いの余地はない。実際、政府が公表する資料などからは、安全管理措置として秘密計算を推奨する姿勢を読み取ることができる。このため、適切に実装されていることを前提とすれば、秘密計算は

技術的安全管理措置の一部を構成すると考えてよい。

（4）監督官庁への通知義務の免除

個人情報保護法第 26 条（民間事業者の義務）および同 68 条（行政機関等の義務）では、個人情報取扱事業者に対して、取り扱う個人データが漏えいなどした場合に、個人情報保護委員会に報告し、本人に通知する義務が規定されている。ただし、同法の施行規則第 8 条では、情報の漏えい等が発生した場合であっても、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている個人データの場合については報告を要しない、とされている。秘密計算がこうした措置に該当するか否かについて、ガイドライン等に特段の記述は見当たらない。また、秘密計算は電子政府推奨暗号ではない。しかし、秘密計算は、CRYPTREC 暗号技術ガイドライン（高機能暗号）において取り上げられていることから、暗号化等の技術的措置に該当する場面があると整理する方向で検討が進んでいるともいえる。

（5）利用目的規制・第三者提供規制との関係

個人情報保護法上、個人情報取扱事業者には、個人情報の利用目的をできる限り特定する義務が定められているほか（第 17 条 1 項）、利用目的を公表していない場合には、速やかに利用目的を本人に通知する義務が定められている（第 21 条 1 項）。データを開示せずに計算結果だけが導き出されるという秘密計算の性質に着目すれば、秘密計算による計算結果の導出が利用目的規制の対象となるか否かについては、一考の余地があると考えられる。個人情報保護委員会が公表している Q&A では、個人情報に該当しない統計データは利用目的規制の対象とはならないほか、統計データの加工自体を利用目的とする必要はないとされている。そのため、単独の事業者によって行われる、秘密計算による計算結果の導出に当たっては、利用目的の特定は不要と理解することができる。

次に、個人データの第三者提供について考察する。個人情報保護法上、個人データの第三者提供には、あらかじめ本人の同意が必要とされている。秘密計算により秘匿化されたデータが組織の垣根を越えて交換されるケースでは、こうしたデータ交換が個人データの第三者提供に当たるか、という論点がある。この点、個人情報保護委員会は、準同型暗号を用いた秘密計算について、暗号化は安全管理措置の 1 つとして考慮されるべき要素ではあるが、個人情報該当性に影響するものではないとの見解を示している。当該見解は、秘密計算の過程で暗号化された個人データの個人情報該当性を示すものではあるが、秘密計算の過程における個人データの交換が第三者提供に該当するか否かについて正

面から回答していない。このように、現時点では、秘密計算において行われる、暗号化された個人データの組織を越えた交換については、第三者提供に該当しないとはいいきれないことには留意が必要である。

対照的に、仮名加工情報については、利用目的の柔軟な変更が許容されている。例えば、仮名加工情報については、共同利用が認められているほか、名寄せを伴う共同利用も排除されていない。もっとも、仮名加工情報を作成する前に仮 ID の作成方法に関する情報を他の事業者と共有する場合には、作成後、直ちに削除しなければならないとされている。いずれにせよ、秘密計算を利用する際には、仮名加工情報を対象とすることも一案であろう。

（6）海外の事例

2014 年、エストニアにおいて、政府機関等が保有する税情報と教育情報を結合し、大学生の留年と仕事量（アルバイト等）の相関関係を導出するのに秘密計算が用いられた事例がある。一般データ保護規則（GDPR：General Data Protection Regulation）施行前のエストニアの法律では、個人データの処理にはデータ保護機関による事前の許諾が必要であったが、秘密計算を用いた処理は個人データの「処理」に該当しないとして事前許諾は不要と判断された。

米国には連邦レベルでの包括的なデータ保護法は存在しないが、欧米間のデータ移動については、欧米間で合意されたデータ保護の枠組みである欧米プライバシー・シールドが適用されてきた。その後、米国に移転された個人データの米国国内法による保護が不十分であるとして、欧州連合（司法裁判所）は、欧米プライバシー・シールドについての十分性決定を無効とする決定を下したが、追加的措置が必要な場合があることを前提に、データ移転をすべて無効とはしなかった。この追加的措置の有効な手法の 1 つとして秘密計算が挙げられており、秘密計算が個人データの保護に資する技術として認められている。

日本と欧州は相互にデータ保護制度を認証している（欧州からの十分性認定、日本からの同等性の決定）ことから、海外の事例における GDPR の解釈は、日本法の解釈に当たっても参考になると思われる。

4. 講演 3：業界横断の安全なデータ活用に基づく社会課題解決の試み

寺田は、複数の企業がもつデータの秘匿性を維持し、プライバシーが保護された安全な統計情報の作成に関する実証実験の内容について、次のとおり講演した。

（1）統計データを「つくる」技術と「つかう」技術

NTT ドコモ社では、携帯電話ネットワークの運用データに基づき、日本全国を対象にエリアごとの人流を継続的に把握できる「モバイル空間統計」と呼ばれる統計データを提供している。降雨の状況から、川の水位上昇や堤防の越水可能性を予測できるように、モバイル空間統計を使えば、交通渋滞の発生や店舗売上の変動、感染症の拡大など、数時間先の社会の未来を予測できる可能性がある。

その一例に「AI 渋滞予知」[13]がある。モバイル空間統計と AI 技術を組み合わせて数時間先の渋滞予測データを提供することにより、人々は渋滞を回避しやすくなる。その結果、渋滞そのものの消失または緩和が期待される。

（2）統計データを「まもる」技術

健全なデータ活用には適切なプライバシー保護が必須であり、統計データを「まもる」技術は、データを「つくる」・「つかう」ための基盤となる。モバイル空間統計は、プライバシーが保護された安全な統計データに変換されていればこそ、多くの企業に提供して広く利用してもらうことができる。また、異なる組織がそれぞれ保有するデータを、プライバシーを保護したまま掛け合わせて安全な統計データに変換する技術が確立できれば、さらに有益な応用事例へと発展していくことも展望できる。そうした観点から開発した技術が「秘匿クロス統計技術」である。

（3）秘匿クロス統計技術

NTT ドコモ社では、2022 年 10 月、他社と共同で、差分プライバシーと秘密計算を組み合わせた「秘匿クロス統計技術」による企業横断データ活用の実証実験を開始した。秘匿クロス統計技術とは、複数の企業が、それぞれのデータの秘匿性を保ったまま、プライバシーが保護された安全な統計情報（クロス集計表）を出力する技術である。秘匿クロス統計の安全性要件は、(1) 出力されるデータが、適切にプライバシーが保護された統計情報であること、および、(2) それぞれの組織にとって、自らの不正がない限り、出力される統計情報以外に、自らのデータに関する情報が漏えいしないことである。

秘匿クロス統計技術は、①入力データの個人識別性を除去する「非識別化処理」、②秘匿共通集合濃度計算を用いて（暗号化された）クロス集計表を作成す

---

[13] 東京湾アクアライン上り線と、関越自動車道上り線（練馬～沼田間）の渋滞予測情報が、NEXCO 東日本の道路情報サイト「ドラぷら」から配信されている。

る「集計処理」、③暗号化された集計表に差分プライバシーを適用したうえで復号する「秘匿処理」の 3 つの処理で構成される。

複数企業が互いの情報を持ち寄ってクロス集計表を作る場合、共有 ID（仮名）を持たせたデータを平文のまま他社に渡してしまうと、特定の個人が識別されたり、プライバシーが暴露されたりする可能性が生じる。そこで、秘匿共通集合濃度計算を使用することによって、互いのデータを知られることなく計算の結果だけを得られるようにする。ここで、秘匿共通集合濃度計算は、集合 A と集合 B がそれぞれ異なる組織により保持されているときに、互いに集合の内容を明かさずに、共通集合の要素数 $|A \cap B|$ のみを計算する技術である。これは、準同型暗号を利用した秘密計算の一種であり、安全性要件（2）を満たすうえで重要な役割を果たす[14]。

次の課題は、最終成果物であるクロス統計表そのものの安全性である。秘匿共通集合濃度計算は、クロス集計表を作成する過程の安全性を保証するが、作成されたクロス集計表そのものの安全性を保証するものではない。実際、公表された複数のクロス統計表を手掛かりに、データベース再構築攻撃と呼ばれる攻撃によってプライバシー情報が漏えいする可能性がある。これは、あるデータベースから作成された複数の集計表を組み合わせることによって、元のデータベースの一部または全部を復元し、個人のプライバシーを暴露する攻撃である[15]。データベース再構築攻撃への対策には、差分プライバシーの枠組みが有効である。

秘匿クロス統計技術では、暗号化された状態のクロス集計表に対して差分プライバシーに基づくノイズ付与を行い、そのあと復号することとしている。これにより、安全なクロス集計表のみが平文で出力される。

（4）データベース再構築攻撃への対応

米国では、従前より、国勢調査における国民のプライバシー保護のあり方について議論が行われていた。そうしたなか、2010 年の国勢調査結果に対してデータベース再構築攻撃を適用したところ、46%の国民について、移住ブロック、性

---

14 この方式以外にも、秘密分散に基づく方式がある。秘密分散とは、秘密情報を n 個のシェアと呼ばれるデータに分割し、そのうちの k 個以上を集めれば秘密情報を復元することができるというデータの分散保管技術である。秘密分散では、その性質上、自分以外の組織が結託した場合には秘密情報が復元されうる（$n > k$ の場合）。秘密分散に基づく方式は安全性要件（2）を満たさないため、実証実験での利用は見送られた。

15 直感的には、複数の統計表を組み合わせて、虫食い算や数独パズルのような制約充足問題を作り、これを解くことで元データを復元する攻撃が挙げられる。

別、年代、人種、民族が復元されてしまうことが判明した。また、1 歳の年齢誤差を許容した場合には、71%の国民についての情報が復元可能であったとの結果が報告された。復元されたデータは、個人を特定できるものではなかったが、その後、一般に入手可能な市販データと照合するによって、約 5,200 万人分（米国民の約 17%）の個人を特定できることが判明した。

米国センサス局では、データベース再構築攻撃のリスクは、理論上のリスクから対策が求められる課題へと変質したとして、2020 年の国勢調査から差分プライバシーの導入を決定した。差分プライバシーは、さまざまなプライバシー保護技術に対する統一的な安全性の尺度である。この尺度は、データベースから出力される情報から、データベースに含まれる特定個人に関するプライバシー情報の流出量の最大値を測るものである。

（5）まとめ

秘匿クロス統計を用いて 2022 年から 2023 年にかけて実施した実証実験では、異業種間でのデータ連携において、プライバシーを技術的に安全に保護しながら有益な社会価値を創出できることを確認できた。今後、さらに実績を重ねることにより、新たなデータ分析の方法論を確立し、得られた知見を広く社会に還元していきたい。安全な統計データの作成方法を確立することは容易ではないが、これを実現することで、有益な社会価値の創出が進んでいくと期待している。

5. パネル・ディスカッション

（1）関係者間におけるコミュニケーションの重要性

プライバシー保護技術は、安全性の基準やデータ処理プロセスの異なるフェーズで適用されるものが混在しているため、ユースケースに照らした技術の選択やそれらの組合せが難しい。こうした観点から、**田村**（モデレータ）は、各組織が顧客のプライバシー保護の取組みを行う際の留意点について、パネリストに意見を求めた。

竹之内は、関係者間のコミュニケーションの重要性を指摘した。具体的には、顧客のプライバシー保護に当たっては、ビジネス側と技術者側のコミュニケーションが必須であるとしたうえで、顧客に価値を提供するためにはどのようなデータが必要かを明確にし、ユーザのプライバシーを保護する方法について話し合うことが重要である、との見解を示した。

寺田は、収集するデータの粒度に関する留意点について意見を述べた。そもそも細かすぎるデータを安全にすることは極めて難しいとしたうえで、ビジネス側には技術的な制約への理解が必要であるほか、ビジネス側から細かいデータの出力を求めた場合であっても、実際には、そこまでの細かいデータが不要であるケースや、むしろ粗いデータの方がサンプル数を増やせてより品質のよい結果が得られるケースもあることを紹介した。また、プライバシー保護の観点からは、まずは粗いデータで分析を行い、徐々にブレークダウンしていくというアプローチが有用ではないか、との見方を示した。

板倉は、データの取扱いにおいては、個人情報保護法を遵守するための対応と、技術的なリスクを想定した対応の両方が必要であると指摘した。そのうえで、両者は観点が異なるため、両方に対応するためには、関係者に広く相談する必要があるとして、関係者間でのコミュニケーションの重要性を指摘した。

菅は、プライバシー保護技術にはさまざまな方式があり、安全性の概念と強度、保護の範囲がそれぞれ異なると指摘した。そのうえで、プライバシー保護に当たっては、データのライフサイクルでの安全性評価が必要であり、残余リスクを洗い出して関係者間で共有し、リスクを受容することも含めて対応方法を検討することが重要である、との見解を示した。

（2）プライバシー保護に関する取組みを公表することの重要性

田村は、国内においても、プライバシー保護技術の活用事例が増えてきていることについて、今後、同技術をより一層普及させていくには、どういったことに留意すべきか、各パネリストに問うた。

竹之内は、プライバシー保護技術の効果は社外からは見えにくいため、プライバシー保護技術を実際には適用していないのに、適用しているように偽装することができてしまうことの問題点を指摘した。そのうえで、今のところこうした偽装への有効な対策はなく、コミュニティー間での情報連携によって対応するほかないとの見解を示した。また、プライバシー保護に関する情報収集には、専門家が多く集まる学会の場を積極的に利用していくことも有用であり、そうなっていくことが望まれる、と述べた。

寺田は、竹之内と同様、プライバシー保護に関しては、実際には安全でなくても安全であると主張できてしまう点に留意が必要である、と述べた。実際、プライバシー保護のために相応のコストをかけて対応している企業と、単に偽装しているだけの企業の見分けがつきにくいことを指摘したうえで、第三者による検証制度の構築が課題であるとの見解を示した。この点、「IT セキュリティ評価及び認証制度」といった第三者による評価・認定制度を利用するといった

アイデアもあるが、プライバシー保護分野についての活用事例はなく、コストの面でも課題があるだろうと述べた。

板倉は、情報開示の重要性について指摘した。すなわち、個人情報保護法では、安全管理のために講じた措置の公表等が義務化されており、こうした公表物は、企業の安全管理措置に対する姿勢の評価にも活用されている実情を紹介した。そのうえで、プライバシー保護への対応についても同様であり、外から見えにくいからこそ、企業の取り組み姿勢を積極的に公表していくことが重要である、との見解を示した。また、一般向けのプレスリリースでは、技術的な内容まで説明することは難しく、それにより誤解が生じるリスクがあるとしたうえで、技術的な内容については別途詳細版を公表することが望ましい、との見解を示した。

（3）セキュリティ・パラメータの設定

プライバシー保護技術には、それぞれにプライバシー保護の程度を評価するためのパラメータが存在する。**田村**は、こうしたパラメータについて、どの程度の数値であれば十分に安全であるといった何らかの目安はあるのか、と各パネリストに質問した。

竹之内は、プライバシー保護におけるデータの安全性は、有用性とのトレードオフの関係にあるため、どの程度の安全性を確保すれば十分といった数値基準を提示するのは難しい、との見解を示した。そのうえで、LINE スタンプのオンライン・サービスを例に挙げ、まだユーザ数が少なかった当初は、データの有用性確保の観点から、差分プライバシーのノイズを少なくせざるを得なかったと述べた。それと同時に、同取組みが「ただちにプライバシーの向上にはつながるものではありません」と公表したことを紹介した。そして、現在も、データの有用性とプライバシー保護の両立のあり方に向けて検討を進めている段階であり、望ましいセキュリティ・パラメータはどの程度かといった数字を提供できる段階にはない、と述べた。

寺田は、*k*-匿名化[16]を例に取り上げ、データベース再構築攻撃に対して安全な方式ではないため、十分な安全性を確保できる k は一般には存在しないとの見解を示した。また、差分プライバシーのセキュリティ・パラメータ[17]については、

---

16 *k*-匿名化とは、同じ属性をもつ値が *k* 個以上になるようにデータを加工することで、*k* 人未満へのデータの絞り込みを困難にする方法である。

17 ε は、2 つのデータベースから得られる集計結果にノイズを加えたとき、これらを区別することができる程度を表すパラメータであり、ε の値が小さいほど安全性が高いとされる。

例えばεが 1 より小さければ十分にプライバシーを保護できているだろうとの相場観はあるものの、社会的なコンセンサスが形成されているわけではないため、今後、関係者間での議論が深まることが期待される、と述べた。

菅は、研究分野では、差分プライバシーがプライバシー保護技術の安全性を示すスタンダードになりつつあることを紹介した。そのうえで、寺田と同様、*k*-匿名化といったプライバシー保護技術は、外部の情報と突合したときの安全性を十分に考慮したものではないことから、現実的な脅威への対策とはなりにくい点には留意が必要である、との見解を示した。

板倉は、匿名加工情報は第三者への提供が認められていることから、第三者に提供しても問題がないような加工処理が求められると指摘した。そのうえで、多くの企業は、個人情報委員会が提示している例を参考に対応しているが、事例集に掲載されている手法を単純に適用しただけでは、実際のリスクに照らして安全なデータになっているとはいい切れないことに留意が必要である、と述べた。

（4）差分プライバシー

差分プライバシーについては、外部にある情報と突合した場合にもプライバシー保護が可能という点で相対的に安全性が高いことから、今後利用が増えていくことが想定されている。そうしたもとで、**田村**は、差分プライバシーを利用するうえでの留意点について、各パネリストに意見を求めた。

竹之内は、データにノイズを付加さえすれば、一定の差分プライバシーは確保されるが、データの有用性を維持しつつプライバシーを保護するには、高いスキルが必要であると指摘した。

菅は、感染症アプリの例に照らすと、高機能なプライバシー保護の実現には、差分プライバシーを他の技術と組み合わせて使用することが必要である、との見解を示した。また、金融機関における不正検知の例では、監査可能性とプライバシー保護という相反する性質の両立が求められるし、医療分野の例では、データにノイズを加えてしまうとデータに価値がなくなることがあると指摘したうえで、ユースケースに応じたプライバシー保護技術が必要であり、差分プライバシーさえあれば十分ということではない、と述べた。

寺田は、差分プライバシー等のプライバシー保護技術は、データに含まれるプライバシー情報の秘匿性を保つ技術であることから、情報セキュリティ技術の一部と位置付けることもできる、と説明した。そのうえで、差分プライバシーの場合、プライバシー情報は秘匿するが、それ以外の情報は開示できるという

性質を持つことが求められるため、既存の暗号技術とは安全性の定義が異なるものの、これまでセキュリティ分野で蓄積されてきた知見がプライバシー保護技術の分野でも活用されていくことが期待される、と述べた。

（5）個人情報保護法とプライバシー保護技術

個人情報保護法では、特定の個人を識別することができないように個人情報を加工したものであれば、本人の同意を得ずに第三者に提供することが可能とされている。また、個人との対応関係が排斥された統計データは個人情報でなくなることから、個人情報保護法の規制下にはおかれない。こうしたもとで、**田村**は、個人情報保護法を踏まえたデータの加工技術とプライバシー保護技術の関係について、各パネリストに見解を問うた。

菅は、差分プライバシーの発想は、個人に関する情報の流出量を制限することで確定的な暴露を回避するというものであり、個人情報保護法におけるプライバシー保護とはコンセプトが大きく異なるのではないか、と述べた。

板倉は、個人情報保護法では、*k*-匿名性（*k* は 2 以上）を満たすように加工された個人データは、匿名加工情報に該当する、と説明した。それは、個人情報保護法上、仮名加工情報や匿名加工情報については、元の個人データと照合してはいけないとの義務が課せられているうえに、*k*-匿名性を有するデータであれば、個人の特定が難しいと考えられるためである、と述べた。そのうえで、個人データを集計加工して得られる統計データは、個人に関する情報ではなく、匿名加工情報でもないとすると、もはや個人情報保護法の範囲外であって法的制約はないが、技術的には、他の個人データとの照合などによって個人が特定される可能性は排除できないことから、今後の法改正によって見直しが行われる可能性はある、との見解を示した。

寺田は、特定の個人との対応関係が排斥された統計データは「個人情報」ではなくなることに関連して、差分プライバシーは、統計データなどから個人に関する情報が確定的に暴露されるのを防止する枠組みであり、個人情報ではない形に加工する技術として有益である、と説明した。

さらに、**板倉**は、現在の個人情報保護法では、差分プライバシーが適用されていたとしても、個人データの一部が少しでも外部に出てしまえば、仮にそれが当たり障りのないものであっても個人情報の漏えいに該当するが、今後の検討次第で、規制を緩和することも考えられるのではないか、との見解を示した。

（6）人材育成

シンポジウム参加者から、企業における人材育成のあり方について質問がよせられた。

寺田は、人材育成には教師となる専門家が必要であるが、国内においてプライバシー保護技術の専門家はまだ少ないこともあって、現時点において企業内での育成は難しいのではないか、との見解を示した。そのうえで、まずは大学等でプライバシー保護技術の基礎を学べるようになることが望ましいが、そうしたカリキュラムをもつ大学は多くないことから、企業のニーズにあわせたカリキュラム構成を大学側に働きかけることは一案となり得る、と述べた。

これに対して、**萱**は、データ・アナリストやデータベースのスペシャリストらがプライバシー保護についても勉強していく、というのが人材育成の近道ではないか、との見解を示した。また、大学での座学と、実社会において実際にユーザのプライバシーを保護することとの間には大きなギャップがあると想像されるため、企業で実戦経験を積むことが重要である、と述べた。

以　上