2.4.3 データ・コンテンツのセキュリティー

（1）研究開発領域の定義

個人情報や機密情報の収集、流通、管理、解析などの過程において、セキュリティーやプライバシーを保護する技術全般を扱う研究開発領域である。第三者の攻撃からの保護であるセキュリティーに対し、プライバシーは他人に知られたくない私事でありそれをコントロールする基本的人権である。情報自体の保護に加え、その適正な取り扱いも重要である。セキュリティー・プライバシー保護対策の代表的な技術には、①個人を識別不能にする匿名化技術、②プライベートなデータを暗号化したままで任意の計算を実行する秘匿計算技術、③プライバシーを保護した上でデータマイニングを実施する技術、④抽出された知識からプライベート情報が漏えいしないように精度を落としたりノイズを加えたりする差分プライバシー技術がある。

（2）キーワード

匿名化、秘匿計算、秘密計算、プライバシー保護データマイニング、差分プライバシー、準同型暗号、秘密分散、秘匿回路計算、コグニティブセキュリティー

（3）研究開発領域の概要

［本領域の意義］

「パーソナルデータは、インターネットにおける新しい石油である」と評されるように、パーソナルデータの活用はインターネット経済の発展における中心的役割を果たす。その一方で、データ活用におけるプライバシー保護への要求は、欧州連合における一般データ保護規則（GDPR：General Data Protection Regulation）の適用開始を契機に高まる一方である。データ活用とプライバシー保護は、相反する方向に作用するデータ経済の両輪であり、データ活用を妨げないセキュリティー、およびプライバシー保護技術の確立は、データ経済の発展に不可欠な技術的課題である。

［研究開発の動向］

❶ これまでの研究開発の流れとトレンド

多くの企業が顧客の情報や購買履歴などを管理して、ビジネスに活用する動きが加速している。いわゆるビッグデータと呼ばれる、大規模で機械的に収集される多量のデータが、あらゆる分野で注目を集めている。その一方で、データの活用から生じるセキュリティーやプライバシーの課題が浮き上がってきた。例えば、アクセス制限の不備によって約450万人分ものYahoo! BB登録者の個人情報が漏えいした2004年の事件や、日本年金機構に対し外部からの標的型攻撃メールが送られ、年金管理システムに保管されていた125万人分の個人情報が漏えいしたという2015年の事件が記憶に新しい。2019年には、2億6,700万人以上のFacebookユーザーのユーザーID、電話番号、名前が、パスワードやその他の認証なしにオンライン上で閲覧可能な状態に置かれていたとの報告[1)]があった。さらに近年では、技術の発展によって膨大な情報が非常に速いスピードで拡散されるようになった結果、フェイクニュースやフェイク動画と呼ばれる、悪意・扇動意識を持った思考誘導の情報操作が起きるようになり、社会的な問題になってきている。

このようなデータ・コンテンツへのセキュリティー・プライバシー保護対策のため、取り組まれている代表的な技術として、匿名化技術、秘匿計算（秘密計算と呼ばれることもある）技術、プライバシー保護データマイニング技術、および差分プライバシー技術について紹介する。なお、フェイクニュースやフェイク動画

に関する動向や対策については、「2.1.5 意思決定・合意形成支援」も参照されたい。

・匿名化技術

匿名化技術は、データとデータ主体（あるいは所有者）との間の相関を取り除く技術である。パーソナルデータの収集において、姓名などの識別子を削除しただけでは、上記の相関は完全には取り除けず、他の属性情報・履歴情報を束ねて見ることで個人が特定され得るリスクがある。このようなリスクを定式化し、低減するための考え方として k-匿名性[2)] がよく知られている。具体的には、表形式データについて、パーソナルデータの属性値の組み合わせが同じであるデータが、パーソナルデータ集合中に k 個以上存在している状態が、k-匿名性が成立した状態である。データの正確性は犠牲になるが、パーソナルデータを改変することで、k-匿名性を成立させ、個人特定を困難にする。その後、k-匿名性を基礎概念として、匿名化対象を表形式データからグラフや時系列データに拡張する研究や、k-匿名性モデルにおいて十分にプライバシーを保護できない状況下におけるより強力な匿名性定義の研究などが進められてきた（l-多様性、t-近似性など）。個人情報保護法による匿名加工情報の実装において実務上重要な技術である。

・秘匿計算技術

秘匿計算（マルチパーティー・コンピュテーション， MPC：Multi-Party Computation）技術は、互いに開示できない情報を持つ複数のグループが、それらの情報を利用した計算について、計算結果以外の情報を一切開示することなく、計算可能にする技術である。安全な秘匿計算のためのプロトコルは、1980年代から研究が開始された。近年では、理論的には成熟しつつあり、実用的な時間で動作する秘匿計算を実行するための汎用コンパイラーが開発され、専門家でなくても秘匿計算を利用したシステム開発を行うことが可能になりつつある。代表的なシステムソフトウェアには、EMP-toolkit、Obliv-C、ObliVM、SCALE-MAMBA（SPDZ）、Sharemind、ABYなどが知られる[3)]。また、秘匿計算の応用事例も徐々に登場している。例えば閾値暗号は、秘密鍵を複数の情報に分割し、暗号上の操作（復号や署名など）の分散実行を可能にする暗号であるが、この鍵情報の保管に秘匿計算を利用することで鍵の盗難や流出に対するリスクを低減する技術の実用化への取り組みが盛んである。暗号通貨の署名鍵の保護にも同様の手法の利用が期待され、具体的にはUnbound Tech.[4)]、Sepior[5)]、Curv[6)] などのセキュリティー企業の取り組みがある。

・プライバシー保護データマイニング技術

プライバシー保護データマイニング（PPDM：Privacy Preserving Data Mining）技術は、利用者のプライバシーを保護しながらビッグデータの活用を実現する技術である。

PPDM研究の原点は、2000年に発表された二つの同名の論文「Privacy Preserving Data Mining」である。一つは、公開鍵と秘密鍵のペアからなる公開鍵暗号方式を用いる暗号学的アプローチによるもの[7)]で、もう一方はランダムなデータを入力に加えてマイニング処理を行うランダム化アプローチによるもの[8)]であった。両論文のアプローチは異なるが、対象は両者ともプライバシー保護を考慮した決定木学習（与えられたデータから決定木と呼ばれる木構造のグラフを生成する手法）を実行するものであったことは、興味深い事実として知られる。この二つの論文を出発点として、PPDMに関して盛んに研究が行われるようになった。

PPDMの主な要素技術としては、暗号化したまま加算や乗算の演算が可能な準同型暗号があり、加算

が可能なPaillier暗号[9]や乗算が可能なRSA暗号[10]が知られる。これらの要素技術の研究開発や安全性評価は2000年代にはほぼ完成していて実現可能性は確認されているが、暗号化にかかる計算コストが大きく、広い実用化のレベルには至っていない。この技術的な困難さを改良するために、加法、乗法の両方の演算が可能な完全準同型暗号などの暗号要素技術の改良が重ねられている。

・差分プライバシー技術

差分プライバシー技術は、データ収集者が信頼できる場合に、データ収集者が公開した統計情報から個人に関する情報が推測されることを防ぐ技術である[11]。ただし、（3）❶に記載したFacebookの事例が示すように、多額のセキュリティー投資をしているプラットフォーマーでさえも、完全に信頼できるとはいえない。この問題を解決するために、個人がデータを提供する際にプライバシー保護処理を行い、その個人に関する情報が推測されることを防ぐことを保証する、局所差分プライバシー（LDP：Local Differential Privacy）が提案されるようになった[12]。

基本的な統計処理の流れを考える。データは個人が保持しており、そのデータを個人から収集者へ提供する。収集者は収集した個人データに対して統計処理を行い、それを解析者へ公開する。この流れの中で、差分プライバシーにおいては、収集者が解析結果を解析者に公開するときに個人データが漏えいしないようにプライバシー保護処理を行う。ただ、収集者は生の個人データを閲覧することができるため、個人が収集者を信頼できる必要がある。一方、局所差分プライバシーでは、個人がデータを提供する際、つまり収集者が個人データを収集する際にプライバシー保護処理を行い、個人のデータが漏えいしないようにする。従って、信頼できない収集者に対する個人データの漏えいも防ぐことができる。

このように、局所差分プライバシーでは、個人から収集者への提供データにノイズを加えて、元のデータが推測できないようにするとともに、収集者はノイズが入った提供データを用いて所望の統計処理を行う。従って、データセット全体で見たときには、差分プライバシーと比べて多くのノイズが加えられるため、実用性が低下しやすく、適用範囲が広いとはいえない。しかし、仕組みの単純さとプライバシー保証の強力さのために、多くのユーザーから情報を収集するGAFA（Google、Amazon、Facebook、Apple）を含むプラットフォーマーは、局所差分プライバシーを利用したデータ収集を取り入れ始めている。

❷ 海外・国内政策動向

個人データの取り扱いに関する研究は、欧州においては2018年から施行されたGDPRに大きく影響されたといえる。 GDPRの一つの大きな特徴は、IPアドレスやCookieなどのインターネットで利用される識別子を含む情報も、個人情報として取り扱うこととなったことにある。このことは、Web経由で個人のデータを暗黙的に収集してきた事業者に多くの影響を与えた。またGDPRは、個人情報を取り扱うサービスやシステムについて、設計段階でデータ保護が組み込まれ、利用者が明示的に設定しなくても、十分なプライバシー保護が初期状態で設定されていることを要求する（設計段階、および初期状態におけるプライバシー）。この設計思想は、プライバシー・バイ・デザインの影響を受けたものである。

さらにGDPRは、プロファイリングを含む個人に対しての自動化された意思決定について、分析する側に透明性の確保（プロファイリングしている事実を知らせること、およびプロファイリングの方法やその影響について説明すること）などを求めるとともに、利用者はこのような自動化された意思決定を受けない権利を有するものとした。「プロファイリング」とは、「個人の特定の側面を評価するために、個人データを自動的に処理すること」であり、特に個人の業務実績、経済状況、健康、個人的嗜好、興味、信頼、行動、

所在、または移動など、個人について重要な判断を伴う分析・予測やそれを提供するシステムとそのロジックについて、透明性の確保と説明責任を求めるとともに、そのような決定を受け入れない権利があることを定めている。

我が国においても、個人情報保護法が2020年6月に改正され、事業者が保有する個人データの利用停止・消去の権利や漏えい報告の義務化、仮名化の導入、罰金の強化・課徴金の導入などについて盛り込まれた。 GDPRの規定も意識した改正であると考えられる。また2018年5月、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）の施行や、同年6月に総務省および経済産業省がとりまとめを行なった「情報信託機能の認定に係る指針ver1.014」によって、認定された事業者によるデータ収集や利活用ができるようになってきた。今後の安心・安全なデータ利活用のため、データ・コンテンツに関するセキュリティー、およびプライバシー保護技術がますます重要になってきている[13)]。

（4）注目動向

［新展開・技術トピックス］

プライバシーや個人情報保護に関する注目トピックとして、AIシステムによる人種、性別、健康、宗教などによる差別の問題が挙げられる。 AIの入力データにこれらの情報が含まれる場合には、プライバシー・個人情報保護の問題となるが、AIによる出力や決定がこれらの情報と相関する場合には、差別の問題となる。差別配慮型のAIの学習は、人工知能分野においてはホットトピックである。またGDPRでは、AIがどのように自分の情報を使用するかの決定権を個人が持つことを保証するよう求めており、AIによる決定のロジックに透明性があることが必要とされている。深層学習を始めとしてAIによる決定は帰納的であり、決定のロジックが説明不可能であることが多い。AIによる決定を、演繹的・説明可能にするための研究もここ数年盛んになってきている。

またコンテンツの不正使用や操作に関して、敵対的生成ネットワーク（GAN：Generative Adversarial Networks）が注目されている。GANの発展により、写実的、かつ実在しない顔や物体の画像・音声・映像のバリエーションを無限に生成可能となったことから、GANを利用した実在の人物を模した偽の演説動画（例えば、DeepFake）などを生成できるようになった。写実性のある動画像や音声が、真正性の保証には利用できなくなるなどの弊害が予想されている。

［注目すべき国内外のプロジェクト］

❶ 戦略的創造研究推進事業におけるプロジェクト（JST）

JSTの戦略的創造研究推進事業CREST「イノベーション創発に資する人工知能基盤技術の創出と統合化」研究領域においては、「プライバシー保護データ解析技術の社会実装」研究課題が実施されている。個人情報や企業の機密情報などのあらゆる機微情報を、安全性を保ったまま任意のデータ処理に適用可能とするプライバシー保護データ解析技術を創出することを目的としている。2016年度にスモールフェーズの研究を開始し、2019年度からは加速フェーズへと移行し社会実装に向けた研究が進められている。

さらに、2020年度には文部科学省において「信頼されるAI」という戦略目標が決定された。達成目標の一つとしてデータの信頼性確保及び意思決定・合意形成支援技術の創出があり、フェイクニュースやフェイク動画、データ改ざんなどを検知し対処する技術などが想定される研究として挙げられている。当該戦略目標の下、CREST「信頼されるAIシステム」や、さきがけ「信頼されるAI」、ACT-X「AI活用で挑む学問の革新と創成」研究領域が設立された。

❷ コグニティブセキュリティー関連プロジェクト（米国国防高等研究計画局（DARPA））

フェイクニュースに見られるように、悪意を持ったオンラインやオフラインでの誘導・干渉によって人々の思考や行動に影響を与える問題は、コグニティブセキュリティー（Cognitive Security）と呼ばれる分野の中心課題の一つである。「2.4.2 サイバーセキュリティー」で紹介した、ソーシャルエンジニアリング攻撃もこれに含まれる。これらの問題は、個人から国家まで幅広い影響を与えており、近年注目を集めるようになった。 DARPAでは、画像・動画の改ざんやフェイクの検知、ソーシャルエンジニアリングの検知・防御などに関するさまざまな研究開発プロジェクトを推進している（詳細は、「2.1.5 意思決定・合意形成支援」参照）。

（5）科学技術的課題

❶ AI セキュリティー・プライバシー

データ解析に関わる個人情報の問題は、これまでは取得・収集データ（入力データ）の扱いにフォーカスされてきたが、AI技術の発展により、取得・収集された個人データを用いて学習したAIの出力データの扱いにも、配慮が必要となりつつある。例えば、AIの出力データが引き起こす差別やプライバシー侵害、個人を識別する情報（顔認証や指紋認証データ、顔画像・動画、音声など）の偽造、マルチメディア情報の偽造などである。従来の情報処理技術でも同様のことは可能であったが、これまでは生成にはコストと人手を要した。AIの利用によって、このような情報が極めて低コストで、無尽蔵に生成できるようになった。さらには、人間が執筆したテキストと遜色ないテキストを自動生成できる文章生成言語モデルGPT-3（Generative Pre-trained Transformer 3）[14] が登場した。このような技術の悪用による、犯罪や名誉毀損、扇動などが危惧される。現実の情報とAIによる生成情報の管理・識別は、今後の課題である。

また、人工知能の学習には大量の情報が必要であり、特に個人情報や個人の行動履歴を入力とする場合には、大量の個人情報の適切な収集と管理にコストがかかる。さらにGDPRをはじめとする法令上の規制から、個人情報の収集は必要最小限度に留めることが求められている。これによって、個人情報の収集が可能であったとしてもなるべく収集量を少なくする、情報の提供者である個人の手元に情報を留める、などの対策をとりつつ、高度なAIを学習させる技術が注目されつつある。具体的には、既存のAIを少量の情報のみを用いて別の目的のAIに転換する転移学習、少量の情報を基に、その情報の特徴を踏まえ類似情報を大量に生成するGAN、個人の手元に情報を留め、情報そのものではなく学習の手がかりになる情報（学習モデルの勾配）のみを収集してAIを学習させる連合学習（Federated Learning）などである。これらの技術は本来個人情報保護とは無関係に機械学習技術として発展してきた技術であるが、GDPRの発足とともに、個人情報保護を目的とした利用技術に発展していく可能性がある。さらに、これらの技術と局所差分プライバシーや秘密計算の併用も、発展の余地がある。

❷ 局所差分プライバシーと対話モデル

局所差分プライバシーには、個人データを提供するユーザーやデータ収集者の間のやり取りの制限を定めた対話可能性という概念が理論解析において必要となる。ユーザーが一斉にデータをランダム化し、収集者がそれらの処理済みデータを一旦収集してから統計処理を行うモデルを非対話的モデル、ユーザーがデータをランダム化する際にユーザーと収集者全員に共有された乱数を活用できるモデルを公開コインモデルと呼ぶ。公開コインモデルはユーザー負担の増加が少ないが、非対話モデルに比べて大きな精度の向上が見られる場合があり、前に紹介したGoogleやAppleの事例で利用されている。ユーザー一人ずつ逐次

的にデータの収集を行う逐次的対話モデルや、同じユーザーに対して何回もデータ収集を行うことが可能な完全対話モデルは、プライバシーに配慮した機械学習を行うための対話モデルとして盛んに研究が行われている。加えて局所差分プライバシーにおいては、極めて多くのユーザーからのデータ収集がプロセスに含まれること、ユーザーはスマートフォンなど限られた計算能力と限られた通信帯域しか持たないデバイスを通じてデータ提供を行うこと、などの事情から、サンプル複雑度に加えて、ユーザーサイドにおける送信データ生成に要する時間やデータ提供時の通信量なども合わせて議論の対象となる。スマートフォンやIoTなど実際にデータ収集に利用されるデバイスやインフラに合わせたデータ収集スキームと理論解析は、未解決課題である。

（6）その他の課題

❶ 法規制

我が国の個人情報保護法は、入力データとしての個人情報を保護するために必要な措置や、その措置を緩和するための手続き（匿名加工情報・仮名加工情報）を定めているが、急速に進展する人工知能などのデータ利用技術や秘密計算技術にキャッチアップできているとは言い難い。データ活用とデータ保護技術に関して、法制度は「だれもが理解できる範囲」の技術しか想定していない。世界的なAI開発競争の波に乗り遅れないためにも、発展的な個人情報保護技術の利用を促進するための工夫が必要である。例えば、用途や範囲を限定した上で、既存の規制にとらわれることなく新たな技術の実証を行える場を導入することなどを検討できる可能性がある。日本政府からは、データ活用の在り方、AI技術活用の在り方について、それぞれ「データ戦略タスクフォース　第一次とりまとめ」[15]が2020年12月に、「AI戦略 2019　～人・産業・地域・政府全てにAI～」[16]が2019年6月に公表されたところであり、議論の活性化が期待される。

❷ 産学連携

産学連携は一昔前に比べれば活発になり、特に企業が所持するデータを利用した研究は盛んになった。一方で産学官の人材の行き来は欧米・中国に比べ活発ではなく、産は産、学は学、あるいは産から学への一方通行に限られる。クロスアポイントメント制度や時限付きで、アカデミアの人材が積極的にインダストリーの中で活躍できるような事例が増加してゆけば良い効果が生まれる可能性がある。

❸ 人材育成

日本における本分野のトップ国際会議での存在感は非常に小さい。トップ国際会議での発表には粘り強く精密な実験と精緻な議論を行う必要があるが、そもそも博士課程を目指す学生が減少する中、アカデミアでは目先の成果を追い求め、チームで息の長い研究を行う体力が失われている。また産業界では、研究成果を広くオープンにするなど人材を引き寄せ発展を促す戦略をとっていない場合も多い。研究者を目指す学生を手厚く支援し、キャリアプランを充実化させ、研究開発に取り組みたいと思う若い研究者を地道に増やすこと、また流行の分野に大型予算を配分するだけでなく、基礎的な成果にも分け隔てなく継続的に中規模の予算を多方面に配分することが必要である。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・暗号理論の基礎研究に従事する研究者は多く、論文も多く出ているが、統計的プライバシー、AIセキュリティー・プライバシーについては、取り組む研究者の数も少なく存在感が薄い。
	応用研究・開発	○	→	・企業による秘密計算実装の提供などが行われているが、応用分野における先進的なプロジェクトは少ない。
米国	基礎研究	◎	↗	・多くの学術論文が発表されている。いずれの研究領域においても、コアとなる理論的アイデアはほとんど米国の大学・企業の研究者から提案されている。
	応用研究・開発	◎	↗	・局所差分プライバシーなど理論成果の実サービスへの導入が進んでいる。 ・産学の人材交流も活発である。
欧州	基礎研究	○	→	・GDPR施行もあって、データ利活用とプライバシーを見据えた基礎的な研究が活発である。
	応用研究・開発	◎	↗	・エストニアにおける秘密計算の実用化など、実用を見据えた動きは活発である。
中国	基礎研究	○	↗	・中国本土の大学・企業でも、分野問わずトップ国際会議における論文数は年々増加している。
	応用研究・開発	○	↗	・民間企業において、秘密計算などの実用例が出始めている。
韓国	基礎研究	○	→	・各種の暗号アルゴリズムの基礎的な研究を行い、国際標準に提案活動を行っている。
	応用研究・開発	△	→	・特に目立った活動は見られない。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDSの調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1）独立行政法人情報処理推進機構（IPA）『情報セキュリティ白書2020』, https://www.ipa.go.jp/files/000087025.pdf

2）Latanya Sweeney, “k-Anonymity：A Model for Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, no. 5（2002）：557-570. doi：10.1142/S0218488502001648

3）M. Hastings et al., “Sok：General purpose compilers for secure multi-party computation”, 2019 IEEE Symposium on Security and Privacy（SP）（2019）：1220-1237. doi：10.1109/SP.2019.00028

4）Unbound, “Secure Cryptographic Keys Across Any Environmrnt”, UNBOUND, https://www.unboundtech.com/
5）SEPIOR, “The New Standard for Key Management & Protection：Preventing Key Theft and Misuse for Data Privacy and Digital Asset Security, SEPIOR, https://sepior.com/
6）CURV, “The Institutional Standard for Digital Asset Security”, CURV, https://www.curv.co/
7）Yehuda Lindell and Benny Pinkas, "Privacy Preserving Data Mining", CRYPTO 2000, Lecture Notes in Computer Science 1880（2000）：36–54. doi：10.1007/3-540-44598-6_3
8）Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-preserving data mining", Proc. of the ACM SIGMOD 2000 29, no. 2（2000）：439–450. doi：10.1145/342009.335438
9）Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes", EUROCRYPT’99, Lecture Notes in Computer Science 1592（1999）：223–238. doi：10.1007/3-540-48910-X1_6
10）Ronald L. Rivest, Adi Shamir and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystems”, CACM 21, no. 2（1978）：120-126. doi：10.1145/359340.359342
11）Cynthia Dwork et al., “Calibrating noise to sensitivity in private data analysis”, Journal of Privacy and Confidentiality 7, no. 3（2006）：17-51. doi：10.29012/jpc.v7i3.405
12）S. P. Kasiviswanathan et al., “What can we learn privately?”, SIAM Journal on Computing 40, no. 3（2011）：793-826.
13）国立研究開発法人科学技術振興機構　研究開発戦略センター　システム・情報科学技術ユニット『科学技術未来戦略ワークショップ報告書 Society 5.0 システムソフトウエア』（CRDS-FY2020-WR-04）（2020年6月）.
14）T. B. BROWN et al., “Language models are few-shot learners”, 34th Conference on Neural Information Processing Systems（2020）：1-25.
15）デジタル・ガバメント閣僚会議　データ戦略タスクフォース『データ戦略タスクフォース　第一次とりまとめ（案）』（2020年11月）, https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai3/siryou2-1.pdf
16）統合イノベーション戦略推進会議『AI戦略 2019　～人・産業・地域・政府全てにAI～』, https://www.kantei.go.jp/jp/singi/tougou-innovation/pdf/aisenryaku2019.pdf