Vol.2019-EIP-83 No.1
2019/2/15

諸外国における秘密計算技術の法的位置付け

板倉陽一郎[12] 藤村明子[23] 亀石久美子[3] 間形文彦[3]

秘密分散を中心とした秘密計算技術について，我が国では法的位置付けを含む議論が始まりつつあるが，解釈論を展開するにせよ，立法論に進むにせよ，諸外国の動向を踏まえることは重要である．本発表では，諸外国における秘密計算技術の法的位置付けにつき検討し，我が国における検討に資することとする．

Legal position of SECURE MULTI-PARTY COMPUTATION in foreign countries

YOICHIRO ITAKURA[12] AKIKO FUJIMURA[23]
KUMIKO KAMEISHI[3] FUMIHIKO MAGATA[3]

Discussions including SECURE MULTI-PARTY COMPUTATION, which focuses on secret sharing, including the legal position are beginning to take place in Japan. Whether developing an interpretive theory or advancing legislation theory, it is important to consider the trends of foreign countries. In this presentation, we will consider the legal status of SECURE MULTI-PARTY COMPUTATION in other countries and contribute to the study in Japan.

1. 問題意識

秘密計算とは，中川裕志名誉教授の概説書によれば，プライバシーを技術的に保護するための匿名化以外の方法であり，「複数の組織が，各組織の持つデータを他組織に知られることなく，全組織のデータを結合した計算結果を得る手続き」と説明されている[1]．その分類については諸説あるが，佐久間淳教授の概説書では，①準同型暗号による秘密計算，②秘匿回路による秘密計算，③秘密分散による秘密計算が章を設けてそれぞれ解説されている[2]（なお，秘密分散による秘密計算については図 1 参照）．複数の組織が，他の組織に対して，いわゆる生データを開示することなく，全組織のデータを結合して計算した結果だけが得られるということで，個人情報保護法上の個人データや，不正競争防止法上の営業秘密・限定提供データへの応用がすぐに思いつくところである．

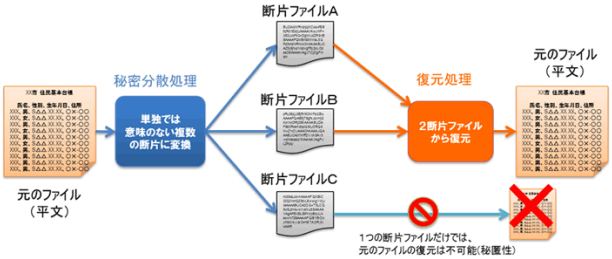

図 1 秘密分散処理の利用例（NTT 持株会社ニュースリリース「秘密分散技術の初の国際標準に NTT の秘密分散技術が採択」より

我が国からは，日本電信電話株式会社の秘密分散技術が、国際標準化機構（International Organization for Standardization、以下 ISO）が発行した秘密分散技術の国際標準”ISO/IEC 19592-2 Information technology -- Security techniques -- Secret sharing -- Part 2: Fundamental mechanisms”において、標準技術として採択され，日本電気株式会社においても，いわゆるトップカンファレンスにおける研究成果を複数公表するなど[3]，特に秘密分散を中心とした秘密計算技術について強みを持つところから，各国に先駆けて，秘密計算技術に関し，法的位置付けを含む議論を始めつつある．他方，秘密計算技術についての諸外国における法的位置付けに関する議論としては，エストニアデータ保護機関が，秘密計算を用いた研究プロジェクトについて，EU データ保護指令上の「処理」に該当しないという公式見解を表明している点が目立つが，この公式見解は関係者においても必ずしも強調されていないように思われる．

本発表においては，日本における秘密計算技術の法的位置付けに関する従来の議論を概観した上で，諸外国，特に欧州圏における秘密計算の法的位置付けの議論を検討し，日本において法的に位置付ける際の示唆を得ることとする．

2. 日本における秘密計算技術の法的位置付け

日本における秘密計算技術の法的位置付けについては，筆者（板倉）による整理がなされており[4]，ここではその内容を概観する．

2.1 研究開発が推奨されるべき技術としての位置付け

サイバーセキュリティ基本法に基づく「サイバーセキュリティ研究開発戦略」（平成 29 年 7 月 13 日，サイバー

1 弁護士・ひかり総合法律事務所
Attorney at Law, Hikari Sogoh Law Offices
2 理化学研究所革新知能統合研究センター（AIP）
RIKEN AIP
3 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories

セキュリティ戦略本部）においては，「（参考）各府省の研究開発の例」において，「パーソナルデータの利活用に向け、暗号化したままビッグデータ解析や機械学習を行う技術を開発」（総務省・NICT），「暗号技術において、暗号化したままデータ処理や認証・認可を実現する高機能暗号技術について、高速処理を可能とする新方式や暗号文サイズが世界最小値となる技術を開発（経済産業省，AIST）」との記載が見られ，「サイバーセキュリティに関する研究開発」の例として位置づけられているといえる．さらに，与党・自民党の政策提言文書である「「経済構造改革戦略：Target 4」＝経済構造改革に関する特命委員会 最終報告＝」（平成 30 年 4 月 27 日，自由民主党）においては，「研究開発等の推進」として，「個人情報保護の観点から開発を進めている秘密計算技術をはじめ、最新のセキュリティ技術の研究開発を推進する．…」とされ，研究開発が推奨されるべき技術として「秘密計算技術」が現れている．

2.2 安全管理措置の一環としての位置付け

秘密計算技術は，必ずしも暗号を用いるものに限られないが，漏えい等を防止するための技術としても有用であることは明らかであり，適切に用いられていることを前提に，個人情報保護法制上の技術的安全管理措置の一部を構成するといえる．また，漏えい等の事案が発生したとしても，個人情報保護委員会等への通知義務が免除されるための「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」という要件において，秘密計算技術の利用が「高度な暗号化等」に該当する可能性も示唆される．

2.3 個人情報保護法上の第三者提供規制との関係

筆者（板倉）も加わった一般財団法人情報法制研究所（JILIS）の個人情報保護法タスクフォースが，平成 27 年改正個人情報保護法のガイドライン策定時のパブリックコメントにおいて，提出した意見が参考となる．すなわち，同 TF は，表題を「暗号化によって秘匿されていても個人情報であるとされるが、準同型暗号を用いたプライバシー保護データマイニングによるデータ交換は、個人情報の提供に当たらないとみなすべき」としたうえで，「法 2 条 1 項のガイドラインで、「個人に関する情報とは……であり、……暗号化等によって秘匿化されているかどうかを問わない．」とされている．確かに、個人情報を暗号化したデータが個人情報に該当するかというとき、復号鍵を誰が利用できる状態にあるかといった条件にかかわらず、暗号化された個人情報も個人情報であるとする法解釈が多数説となっていた．これにはクラウドと委託の関係等、様々な論点が関連し、議論の残るところと考えるが、少なくとも、準同型暗号を用いたプライバシー保護データマイニング（Privacy-Preserving Data Mining、PPDM）におけるデータ交換は個人情報（個人データ）の提供に当たらないと解釈されるべく、法律上の位置づけの再整理をお願いしたい．この技術を用いれば、暗号化する事業者と復号する事業者のどちらも、どの情報がどの元情報に対応しているか知り期待されている．」との意見を述べたところ，個人情報保護委員会の回答は，「暗号化については、安全管理措置の一つとして考慮されるべき要素であり、個人情報該当性に影響するものではないと考え、本ガイドライン（通則編）案 2-1 において、「暗号化等によって秘匿化されているかどうかを問わない」と記載しております．なお、本ガイドライン（通則編）案 4 にあるとおり、漏えい等の事案が発生した場合の対応については、別に定めることとしております．」というものであった（「個人情報の保護に関する法律についてのガイドライン（通則編）（案）」に関する意見募集結果 27 番）．このように，現時点での個人情報保護委員会の見解においては，秘密計算技術を用いたとしても，個人情報保護法上の第三者提供規定等について適用外とはされていない．

2.4 小括

このように，我が国における秘密計算技術は，研究開発が推奨される技術や，安全管理措置の一環としての位置付けが認められるが，個人情報保護法上の第三者提供規制等との関係で，適用外であるという整理はなされておらず，現時点では，事業者としては，個人情報保護法を遵守した利用が求められるということになる．

3. 欧州一般データ保護規則（GDPR）における秘密計算技術の法的位置付け

欧州のデータ保護制度における秘密計算技術の法的位置付けとしては，筆者（板倉）による論稿でも紹介されているエストニアデータ保護機関の見解が，データ保護機関によるものとしては唯一であると思われる．ここではエストニアデータ保護機関の見解をやや詳細に紹介するとともに，GDPR 上の別の法的位置付けに関する見解を整理する．

3.1 エストニアデータ保護機関の見解（「処理」非該当）

エストニアのデータ保護機関である Estonian Data Protection Inspectorate は，平成 26（2014）年 1 月 27 日付で，秘密計算技術に関する法的見解を示している．その内容と背景は以下のとおりである．

秘密計算技術が用いられたのは，2013 年から 2015 年に掛けて行われた PRIST というプロジェクトである．これは，政府関係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）の相関関係たる計算結果を導出する処理に秘密計算を用いたものであった[5]（図 2）．秘密計算におけるシェアは，エストニア金融庁の IT センター，エストニア情報システム庁，エストニア

Cybernetica 社がそれぞれ保有者となっている．Cybernetica 社は，秘密計算技術を有するエストニアの IT 企業であり，PRIST における秘密計算も，同社の Sharemind というサービスを用いて実行された．そして，EU データ保護指令下でのエストニア個人データ保護法においては，センシティブデータの処理に関して，事前にデータ保護機関の許諾が必要であったところ，教育情報には，センシティブデータが含まれていたため，PRIST における秘密計算技術の利用には，エストニアデータ保護機関の事前の許諾が必要なのではないかが問題となった．

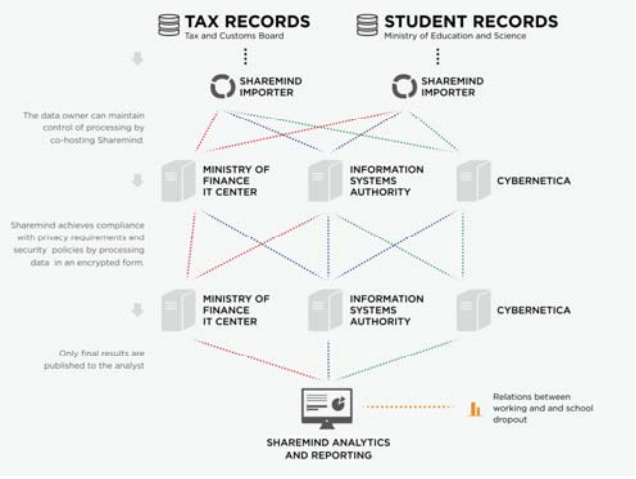

図 2 PRIST project における各主体

結論としては，本件における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，データ保護機関の事前許諾は不要とされた[6]．ただし，個人データの処理に該当しない前提として，①研究目的であり，②導出されるのが統計データであり，③秘密計算のソースコードについて事前のレビューがなされ，PIA（プライバシー影響評価）が実施され，④秘密分散による秘密計算を行う組織間での結託を防止する契約が締結されていたことが挙げられている．

このようなエストニアデータ保護機関の見解が欧州一般データ保護規則（GDPR）においても妥当し，秘密計算技術による個人データの処理が GDPR 上の「処理」に該当しないということであれば，欧州全域において秘密計算技術による計算結果の導出は GDPR の適用を免れることになるが，その後，エストニア以外のデータ保護機関から追随する見解は示されていないようである．Cybernetica 社のゼネラル・カウンセルである Triin Siil は欧州データ保護監察官（EDPS）も共催する会議である IPEN Workshop 2017（2017 年 6 月 9 日）においてこの見解を公表しているが，同時に，秘密計算技術の法的位置付けとして管理者にとっては GDPR25 条 1 項及び 2 項の技術的措置であるとか，処理者にとってはリサイタル（前文）26 項の匿名化データの分析に有益であるという見解を示しており，エストニアデータ保護機関の見解に拘泥する様子は見られない[7][8].

3.2 「個人データ」非該当

3.2.1 特定識別性の欠如

秘密計算技術におけるシェアは GDPR 上の「個人データ」に該当しないので，GDPR の適用はないという見解も存在する[9]（独ゲッティンゲン大学 Gerald Spindler 教授らによる）．この見解は，そもそも，GDPR 上の「個人データ」について，「絶対的アプローチ（Absolute Approach）」を採用すべきか，「相対的アプローチ（Relative Approach）」を採用すべきか，という整理を行う．ここで，絶対的アプローチとは，暗号化されたデータとの関係では，世界の誰もが復号できない状態になければ，個人データのままであるとする見解であり，相対的アプローチとは，管理者がデータ主体を特定識別するためには，必要な努力のみが求められるとする見解である．Spindler らは，相対的アプローチを是とした上で，秘密計算上のシェアは個人データには該当せず，結合されるまでのシェアの取扱いには GDPR の適用はないとする．また，そうであるとしても，シェアの保有者には安全性と秘密保持について強いインセンティブがあり，法的にも契約で拘束されるであろうから問題ないとする．「個人データ」に該当しないということは GDPR の適用が全面的になくなるということであり，その意図するところは JILIS 個人情報保護法タスクフォースのパブリックコメント提出意見に近いと思われる．エストニアデータ保護機関の見解が条件付きであったのと比しても，個人データ該当性の解釈によって，シェアは個人データではないとするものであるから，無条件での，GDPR 非適用という結論を導き出す．

3.2.2 「匿名化データ」該当による「個人データ」非該当

他方，同じく独ゲッティンゲン大学 Gerald Spindler 教授らによる論稿（但し第一著者は同教授ではない）において，個人データのセットが完全に匿名化され，合理的には，本人を特定する方法が存在しなくなることから，「匿名化データ」に該当するので個人データではないという理由付けで，GDPR 自体の適用がないという見解も存在する[10]．しかしながら，「匿名化データ」は，リサイタル 26 項によって「識別された自然人又は識別可能な自然人との関係をもたない情報、又は、データ主体を識別できないように匿名化された個人データ」と定義づけられており，秘密計算技術において処理される情報が常に匿名化データに該当するといえるかについては，必ずしも丁寧な論証があるわけではない．また，同論稿においては，データ保護・バイ・デザイン（GDPR25 条）としての位置付けにも触れられており，「匿名化データ」該当による「個人データ」非該当という結論を強く主張するものとは見られない．

3.3 小括

GDPR 上，秘密計算技術におけるシェアは個人データに該当しないであるとか，秘密計算技術を用いた処理におけるデータは匿名化データに該当するということを理由に GDPR の適用を排する見解が見られるが，提唱にとどまっている．勿論，これらの見解が認められるということになれば，GDPR 自体の適用がないのであるから，秘密計算技術は大いに用いられることとなろうが，個人データ該当性における「相対的アプローチ」は必ずしも一般的に受け入れられているものではないこと，「匿名化データ」についての GDPR 上の定義は極めて厳しいことからすると，直ちに採用される見解であるかどうかについてはなおも議論があろう．他方，データ保護・バイ・デザイン（GDPR25 条）における技術的措置としての位置付けについては特段の争いはないと思われる．

4. 米国における秘密計算技術の位置付け

米国においては，連邦レベルで包括的なデータ保護法が存在するものではないこともあり，秘密計算技術の利用を，データ保護法制において何らかの効果に結びつけようという試みは見いだせない．他方で，秘密計算技術は，証拠に基づく政策（Evidence-Based Policymaking）の分野で注目されており，いくつかの法案の提出例を見ることができる．第 115 回連邦議会において上院に提出された Student Right to Know Before You Go Act of 2017 法案（S.2169）[11]は，高等教育機関の透明性を高めることを義務付けようとするものであるが，2 条 12 項において” SECURE MULTI-PARTY COMPUTATION” を ”a computerized system that enables different participating entities in possession of private sets of data to link and aggregate their data sets for the exclusive purpose of performing a finite number of pre-approved computations without transferring or otherwise revealing any private data to each other or anyone else.”として定義しようとする．また，下院に提出された FORWARD Act of 2018 法案（H.R.6562）[12]は，米国の風土病であるコクシジオイデス症の研究を支援し、ワクチン開発を奨励し、新しい抗真菌療法と診断法を発見することを目的とした法案であるが，”secure multiparty encrypted computing”について”a form of cryptography in which parties can jointly compute a function of inputs while keeping those inputs private from each other, and from all other parties, such as multiparty homomorphic encryption, threshold encryption, and secure multiparty computation.”と定義し，これを組み込んだソフトウェアを「特定病院」における研究で用いさせることを想定している．

いずれの法案も成立の見込みは不明であるが，秘密計算技術の証拠に基づく政策における利用が，法案における概念の導入レベルで検討されているという点で注目されるべきであろう．

5. 終わりに

本稿では，欧州一般データ保護規則（GDPR）における秘密計算技術の法的位置付け，特に GDPR の適用範囲外としようとする試みを概観した．また，米国においては，証拠に基づく政策における利用が，法案における秘密計算技術の定義として現れてきている点を指摘した．秘密計算技術自体は，我が国における発展及び実用化を見せようとしているものであるが，その法的位置付けについては欧州の試み，米国における概念の導入ともに，参考となるものであろう．我が国における法的位置付けの議論に対しても，一資料を提供するものである．

[1] 中川裕志『プライバシー保護入門』(勁草書房, 2016 年) 217-218 頁.
[2] 佐久間淳『データ解析におけるプライバシー保護』(講談社, 2016 年).
[3] プレスリリースで挙げているものとして T. Araki, A. Barak, J. Furukawa, M. Keller, Y. Lindell, K. Ohara and H. Tsuchida. "Generalizing the SPDZ Compiler For Other Protocols". *ACM CCS 2018.*等.
[4] 板倉陽一郎「安全なデータ活用を実現する秘密計算技術：7. 秘密計算技術に関する国内法制度」情報処理 59 巻 10 号 909-915 頁（2018 年）.
[5] Bogdanov, D., Kamm, L., Kubo, B., Rebane, R., Sokk, V., & Talviste, R. (2016). Students and taxes: a privacy-preserving study using secure computation. *Proceedings on Privacy Enhancing Technologies*, *2016*(3), 117-135.
[6] エストニアデータ保護機関の回答（nr 2.2.-7/13/557r）.
[7] Triin S,'Sharemind: A Secure Multi- Party Computation (MPC) Platform Implementing Privacy by Design and Privacy by Default', *IPEN Workshop 2017.*
[8] David W. Archer and Dan Bogdanov and Y. Lindell and Liina Kamm and Kurt Nielsen and Jakob Illeborg Pagter and Nigel P. Smart and Rebecca N. Wright. From Keys to Databases -- Real-World Applications of Secure Multi-Party Computation. The Computer Journal, Volume 61, Issue 12, 1 December 2018, Pages 1749–1771.
[9] Spindler, G., & Schmechel, P. . Personal Data and Encryption in the European General Data Protection Regulation. *J. Intell. Prop. Info. Tech. & Elec. Com. L., 2017(7),* 163-177.
[10] Veeningen, M., Chatterjea, S., Horváth, A. Z., Spindler, G., Boersma, E., Gutteling, J., ... & Veugen, T. Enabling Analytics on Sensitive Medical Data with Secure Multi-Party Computation. *Studies in health technology and informatics, 247, (2018)* 76-80.
[11] https://www.congress.gov/bill/115th-congress/senate-bill/2169
[12] https://www.congress.gov/bill/115th-congress/house-bill/6562