

⑦秘密計算技術に関する国内法制度



板倉陽一郎 | ひかり総合法律事務所／理化学研究所革新知能統合研究センター／国立情報学研究所

秘密計算技術の国内法制度における位置づけ

本稿は秘密計算技術に関する国内法制度を概観するものであるが、秘密計算技術は現時点で法令用語ではなく（平成30年7月23日現在の「秘密計算」のe-gov法令検索結果による）、裁判例においても用語として現れていない^{☆1}。つまり、秘密計算技術の国内法制度上の位置づけは、まだ確固たるものではない。

そこで、秘密計算技術の国内法制度における位置づけを、①推奨されるべき技術としての位置づけ、②安全管理措置（セキュリティ）の一環としての位置づけ、③個人情報や営業秘密の取扱いに関する規制における位置づけ、という3つの観点から見ていくことにする。

なお、秘密計算技術ないし秘密計算の具体的内容については本特集のほかの論考に譲る。概説書レベルでの定義としては、中川裕志名誉教授が、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として秘密計算を挙げ、「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」と説明する¹⁾。その分類についても諸説あるようであるが、佐久間淳教授は、著書において、①準同型暗号による秘密計算、②秘匿回路（本特集では Garbled cir-

cuit と表記）による秘密計算、③秘密分散による秘密計算の章を設けてそれぞれ解説している²⁾。ここでは、仮に、秘密計算については中川名誉教授の定義を参照することとし、佐久間教授の挙げる類型について、特記しない限りはまとめて秘密計算ないし秘密計算技術として扱う。

研究開発が推奨されるべき技術としての位置づけ

データの取扱いに関する基本法の類では、ある技術の研究開発を推奨する根拠となる規定が存在する場合がある。たとえば、官民データ活用推進基本法（平成28年法律第103号）16条は「国は、我が国において官民データ活用に関する技術力を自立的に保持することの重要性に鑑み、人工知能関連技術、インターネット・オブ・シングス活用関連技術、クラウド・コンピューティング・サービス関連技術その他の先端的な技術に関する研究開発及び実証の推進並びにその成果の普及を図るために必要な措置を講ずるものとする。」とし、サイバーセキュリティ基本法（平成26年法律第104号）は、「国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研

^{☆1} 特許庁審決では1件が確認される（「秘密計算システムおよび方法並びに管理サーバおよびプログラム」平成30年2月28日（不服2016-19034、拒絶査定不服審決））。これはまさに秘密計算にかかる特許が問題となったものであって、秘密計算の法的位置づけを与えるものではない。

究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。」とする。官民データ活用推進基本法に基づく「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」（平成30年6月15日、高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議）においては、秘密計算技術についての直接的な記載は見られない。他方、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：情報通信研究機構）、「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：産業技術総合研究所）との記載が見られる。秘密計算ないし秘密計算技術との名称こそ見られないが、明らかにこれらを指すものであり、「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：Target4』＝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、ついに研究開発が推奨されるべき技術として「秘密計算技術」が名指しで現れるに至っている。今後は、世界最先端デジタル国家創造宣言・官民データ活用推進基本計画等の政府の基本計画等にも盛り込まれることが期待される。

安全管理措置の一環としての位置づけ

安全管理措置についての法制度

前章では秘密計算技術が、国内法制度における研究開発が推奨されるべき技術に該当するか、という点を整理したが、実際の法的効果に結び付く技術としての位置づけは与えられているであろうか。ここでは、安全管理措置についての個別の法制度を見ていく必要がある。安全管理措置に関する個別の法制度は、1つには、安全管理措置を履行せよという義務規定として現れ、もう1つ、一定の安全管理措置が取られていた場合には、情報漏えい等の事案が生じて、監督官庁への通知義務が免除される、という規定として現れる。具体的に見ていこう。

安全管理措置に関する義務規定

安全管理措置に関する義務規定としては、個人情報保護に関する法律（平成15年法律第57号、個人情報保護法）20条が、民間事業者であるところの個人情報取扱事業者の義務の1つとして、「**個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。**」と定めている。包括的な規定であるが、違反した場合には個人情報保護委員会からの指導や勧告などがあり得る。また、公的機関に関しても、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号、行政機関個人情報保護法）および独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号、独立行政法人等個人情報保護法）において、行政機関の長および独立行政法人等に対して、「**保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならない。**」との義務が課せられている（行政機関個人情報保護法6条1項、独立行政法人等個人情報保護法7条1項）。個人番号（マイナンバー）に関しては、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（平成 25 年法律第 27 号、マイナンバー法）12 条が、個人番号利用事務実施者および個人番号関係事務実施者に対し、「**個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。**」との義務を課している。個人番号利用事務実施者および個人番号関係事務実施者には、民間事業者も、公的機関（地方自治体を含む）も該当し得る。

安全管理措置の具体例はガイドラインで例示されているが、個人情報保護法に関しては「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）」（平成 28 年 11 月（平成 29 年 3 月一部改正）、個人情報保護委員会）「8（別添）講ずべき安全管理措置の内容」のうち、「8-6 技術的安全管理措置」において、「(4) 情報システムの使用に伴う漏えい等の防止」の項目が存し、「個人データを含む通信の経路又は内容を暗号化する」との手法が例示されている。また、マイナンバー法に関しては、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（平成 26 年 12 月 11 日（平成 29 年 5 月 30 日最終改正）、個人情報保護委員会）の「(別添) 特定個人情報に関する安全管理措置（事業者編）」において、「F 技術的安全管理措置」「d 情報漏えい等の防止」の中で「特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。」とされ、「* 通信経路における情報漏えい等の防止策としては、通信経路の暗号化等が考えられる。」「* 情報システム内に保存されている特定個人情報等の情報漏えい等の防止策としては、データの暗号化又はパスワードによる保護等が考えられる。」との手法の例示がなされている。

秘密計算技術の中には、いわゆる暗号化とはいえないものも含まれるが、漏えい等を防止することに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、技術的安全管理措置の一部を構

成するといえよう。

監督官庁への通知義務の免除との関係

監督官庁への通知義務の免除との関係は、以下のとおりである。

個人情報保護法における個人データの漏えい等に関しては、「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）が定められており、「個人情報取扱事業者が保有する個人データ（特定個人情報にかかわるものを除く）の漏えい、滅失又は毀損」等の場合には「漏えい等事案」として監督官庁（主として個人情報保護委員会）への通知が告示レベルで義務付けられている。もっとも、「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合」には通知が不要であるとされ、その例として「漏えい等事案にかかわ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」が挙げられている。

個人情報保護委員会は「高度な暗号化等の秘匿化」について見解を示しており、「当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等事案に係る情報について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます。また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じ

ていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。」とする（『個人情報保護に関する法律についてのガイドライン』および『個人情報の漏えい等の事案が発生した場合等の対応について』に関するQ & A」（平成29年2月16日（平成30年7月20日更新）、個人情報保護委員会）、以下、「Q&A」. Q12-10 および A12-10）。

秘密計算技術が「高度な暗号化等の秘匿化」に該当するかについては、個人情報保護委員会のQ&Aにおいても特段の記述がない。もっとも、秘密分散技術についてはISO/IEC 19592-2:2017が平成29年10月に技術標準として発行しており、秘密分散による秘密計算については、少なくともISOに認められた方式が存在することを理由に、「第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置」に該当すると考えてよいであろう。準同型暗号や秘匿回路については「適切な評価機関等により安全性が確認されている」といえるまでの一般的な評価はないものと考えられる。「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」に該当するといえるためには、標準化等、安全性を社会的に確認させるための活動も重要であるということになる。また、「暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されている」といえるために、準同型暗号についてはQ&Aで定められている方式と同様の鍵管理が求められるであろう。他方、秘密分散や秘匿回路を用いる場合に、同等の「手段」として認められるためには、社会的受容を喚起する活動も必要になってこよう。たとえば、秘密分散でいえば、シェア共有者間に求められる関係性や（同一法人であってはならない、親子会社であってはならない、などが考えられる。

あくまで例である）、シェア共有者間での適切な契約の締結等が求められることになる。このように、秘密計算技術を利用することが「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」に該当しているといえるかについては、より一層の社会的受容のための活動が重要になってくる。技術的な改善にかかる研究は当然重要であるが、社会実装に関する活動も並行して行われる必要がある（本特集がその一環となることも期待される）。

個人情報や営業秘密の取扱いに関する規制における位置づけ

個人情報の取扱いとの関係

秘密計算技術に関連する個人情報保護法上の規制

ここまで、秘密計算技術は、研究開発が推奨されるべき技術になりつつあり、安全管理措置の一部を構成し、今後の社会的受容の努力いかんでは、個人データの漏えい等事案において、高度な暗号化等として通知を必要としない例外にも該当し得ることを検討してきた。しかしながら、「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」としての秘密計算の真髄は、複数の組織（法人等）のデータが、お互いに開示されることなく、計算結果だけが導き出されるというところにあるのであるから、これを、個人データに関して、本人の同意なしにできないか、と考えるのは一般的な期待であろう。秘密計算技術によって、本人の同意なしに計算結果を導出できるかについては、まず、個人情報保護法上の制度を確認する必要がある。

個人情報保護法上、個人情報取扱事業者は、個人情報を取り扱うにあたって、利用目的をできる限り特定し（15条1項）、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、または

公表しなければならない(18条1項)。ここではまず、「計算結果」を導出することが利用目的に該当するかが問われる。ここで、Q&Aでは、「個人情報を統計処理して特定の個人を識別することができない態様で利用する場合についても、利用目的として特定する必要がありますか」との問い(Q2-5)に対し、「利用目的の特定は「個人情報」が対象であるため、個人情報に該当しない統計データは対象となりません。また、統計データへの加工を行うこと自体を利用目的とする必要はありません」(A2-5)との個人情報保護委員会の見解が示されており、個人情報に該当しない統計や数値のような「計算結果」を得ること自体は利用目的規制の対象となるものではないと考えられよう。

他方、秘密計算の過程で「各組織の持つデータ」が「結合」される点については、個人データの第三者提供に該当し、本人の同意なしには許されないのではないかという問題がある(個人情報保護法23条1項柱書)。この点については、すでに個人情報保護委員会の見解が示されているほか、立法的な手段が模索されている痕跡がある。順に見ていこう。

秘密計算技術と第三者提供規制についての個人情報保護委員会の解釈

筆者が参与をつとめる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は、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、一定の条件を満たす秘密計算技術と第三者提供規制の関係について意見を述べたことがある。すなわち、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」とした上で、「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、さまざまな論点に関連し、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得ることなく、集計などの統計情報を得ることができると期待されている。」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)。

すなわち、個人情報保護委員会は、少なくとも準同型暗号を用いた秘密計算技術については、前節で論じたような、安全管理措置の一環であることは認めるものの、「個人情報該当性に影響するものではない」として、第三者提供規制の解釈上の例外であることは認めなかった。もとより、上記タスクフォースは、個人情報に該当しないので第三者提供規制の例外に該当するとの意見を述べたものではないので、意見と回答には齟齬があるが、いずれにせよ、秘密計算技術における、計算結果を得るための個人データの結合は、第三者提供に該当しないとはいえないとの見解が示されたものである。

秘密計算技術と第三者提供規制についての立法論

他方、経済産業省の産業構造審議会商務流通情報分科会情報経済小委員会分散戦略WG中間とりまとめ（平成28年11月）では、「秘密分散・計算技術の活用によるデータ協調環境整備の検討」との項目で、「企業が漏洩を気にすることなく、ビッグデータ分析のためにデータを容易に提供できるよう、秘密計算技術等を活用した、第三者に提供する場合の運用の在り方について検討する。」としている。「第三者に提供する場合の運用の在り方」とは、立法的措置を回避するための文言であると思われるが、産業構造審議会情報経済小委員会分散戦略WG（第7回）事務局資料（平成28年8月29日、経済産業省商務情報政策局）では、「秘密計算について、現行制度では解析のための第三者提供にあたっては同意が必要であるが、技術的に暗号がかかっている場合には、本人の同意を不要とするなどの検討が必要。」（54頁）として、明らかに立法による解決を意識した表記となっており、議事録においても、「新しい技術への対応でございますけれども、技術的に暗号がかかっている、秘密計算が可能な場合には、たとえば本人の同意を不要とするといった検討も必要ではないかということでございます。」と説明されていた（産業構造審議会商務流通情報分科会情報経済小委員会分散戦略ワーキンググループ（第7回）議事録8頁）。第8回（平成28年10月13日）では秘密分散技術と第三者提供について明確な発言はなく、第9回（平成28年11月7日）の配布資料である中間とりまとめ（案）では成案と同じ表現になっているため、この間、何らかの調整がなされたと思われる。いずれにせよ、秘密計算技術と第三者提供規制についての立法論が日の目を見ることはなく、現時点に至るまで「運用の在り方」についての検討も行われていない状況にあるといえよう。

秘密計算技術と第三者提供規制についての欧州の実例

以上の通り、個人情報保護法との関係では、秘密計算技術と第三者提供規制についての個人情報保護

委員会の解釈は特例措置とすることに否定的であり、立法論も「運用の在り方」も展開されていない状況にある。他方で、欧州では、秘密計算技術の利用が個人データの取扱い（処理）に当たらないとした例が見られる。

具体的には、平成26（2014）年1月27日付のエストニアデータ保護機関の見解であり、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、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したものである^{☆2}。具体的には、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³。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（Privacy Impact Assessment、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。

日本と欧州は相互の認定（欧州から日本への十分性認定、日本から欧州31カ国への同等性認定）についてほぼ合意に達している（「Joint Statement by Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan and Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission（熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント）」（平成30（2018）年7月17日）。一般データ保護規則（General Data Protection Regulation：GDPR）の

☆2 エストニアデータ保護機関の回答（nr 2.2.-7/13/557r）。

解釈については日本法の解釈にも有用であるということであり、GDPR 以前の EU データ保護指令およびエストニアデータ保護法に基づくデータ保護機関の判断であっても、現在も有効なものとして維持されている以上は、その趣旨は十分に尊重される必要がある。エストニアデータ保護機関が認めた要件、すなわち、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 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、との要件が満たされるとしても、解釈によって個人情報保護法上の個人データの第三者提供には該当しない、とするのは、条文の文言上は相当の無理があることは否めない。しかしながら、欧州のデータ保護機関の公的な解釈として、秘密計算技術と第三者提供規制についての立法論が展開される場合には、十分に参照される必要があると思われる。

営業秘密の取扱いとの関係

以上ほとんどの検討は、個人情報保護法に関して行ってきたが、産業データの活用の観点からは、不正競争防止法（平成 5 年法律第 47 号）における営業秘密について、秘密計算技術を用いて互いに提供し、計算結果を得た場合であっても営業秘密の秘密管理性が失われないかという論点が存する（平成 30 年改正によって導入された限定提供データの技術的管理性についても同様に問題になり得る）。

秘密管理性は規範的な要件であり、秘密計算技術を用いて互いに提供する両当事者間において秘密保持契約等の契約上の措置が取られていたことで肯定されることがある。秘密計算技術による相互の提供について、契約上の措置も加味すれば、秘密管理性が失われないという解釈は十分に可能であろう。

秘密計算技術の国内法上の位置づけに関する展望

これまで見てきた通り、秘密計算技術は、研究開発が推奨されるべき技術となりつつあり、安全管理措置の一部を構成するほか、今後の社会的受容性にも左右されるが、個人データの漏えい等事案において、高度な暗号化等として通知を必要としない例外にも該当し得る。また、欧州を参照しつつ、個人データの第三者提供の新たな例外としての立法論も考え得るところである。秘密計算技術は適切に用いることによって、個人データの本人にプライバシー侵害が生じる可能性を最小限にしつつ、必要な計算結果を導出できるものである。その社会的受容や立法上の導入については、社会への丁寧な説明や、開発や議論における透明性をもって進めていくことが寛容であろう。

参考文献

- 1) 中川裕志: プライバシー保護入門, 勁草書房, pp.217-218 (2016).
- 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).
- 3) Bogdanov, D., Kamm, L., Kubo, B., Rebane, R., Sokk, V. and Talviste, R.: Students and Taxes: A Privacy-preserving Study Using Secure Computation, Proceedings on Privacy Enhancing Technologies, 2016(3), pp.117-135 (2016).
(2018 年 8 月 11 日受付)

板倉陽一郎（正会員） itakura@hikari-law.com

2002 年慶應義塾大学総合政策学部卒業, 2004 年京都大学大学院情報学研究科社会情報学専攻修士課程修了, 2007 年慶應義塾大学法務研究科（法科大学院）修了, 弁護士（ひかり総合法律事務所パートナー）。2017 年より理化学研究所革新知能統合研究センター客員主管研究員, 2018 年より国立情報学研究所客員教授, 本会電子化知的財産・社会基盤研究会運営委員。