特集
Special Feature

安全なデータ活用を実現する秘密計算技術

編集にあたって

竹之内隆夫 | NEC セキュリティ研究所
高橋克巳 | NTT セキュアプラットフォーム研究所
菊池浩明 | 明治大学

AI や IoT 等の技術の進展に伴い，多くの企業・組織にとって，データの重要性はますます高まってきている．特に一部の企業では，戦略的にデータを収集・分析・活用し，企業価値を高めている．

従来のデータ活用は組織内におけるデータの活用にとどまっていたが，今後は組織を跨いだ，さらには社会的な問題解決への活用が期待されている．しかし，複数組織でのデータ共有は，プライバシ侵害の恐れや，データの囲い込み思考があり，実際には十分には進んでいないのが現状と考える．

この課題を解決する 1 つの技術として，秘密計算技術が注目されつつある．秘密計算とは，データを秘匿したまま処理できる技術である．この技術によって，複数の組織間でデータを秘匿しながら結合し，分析し，その結果だけを出力できる．これにより，安全な組織間でのデータ活用が促進され，さまざまな価値を生むことが期待されている．

秘密計算は 1986 年に Yao によって，基礎的な技術が提案された．当時は，処理速度がきわめて遅く，実用化には程遠いと考えられていた．しかし，その後さまざまな方式やアルゴリズムが提案され，近年では桁違いに性能が向上し，実用化への期待が高まりつつある．

しかし，秘密計算にはさまざまな方式が存在することや，さまざまな利用形態が存在することから，一般の技術者からの理解が十分とは言いがたいのが現状である．さらに秘密計算を社会実装していくことを考えると，制度等の整備も必要となる可能性がある．そのため，法律家や一般利用者へ，技術を分かりやすく説明することも必要と考えている．

本特集では，秘密計算の基本的な解説を行いつつ，さまざまな秘密計算の方式や利用形態を紹介する．また，技術の説明だけでなく，実用化を見据えた研究開発や実証などについても説明する．さらに，関連する制度の動向についても説明する．

まず，**「1. 秘密計算による安全なデータ共有」**では，NEC の竹之内隆夫より，秘密計算技術の概要と典型的な利用例やさまざまな方式について簡単に解説する．特に秘密計算には，代表的な方式として

- 秘密分散を用いた秘密計算
- Garbled circuit を用いた秘密計算
- 準同型暗号を用いた秘密計算

などが存在することを説明する．

次に「**2. 秘密計算の実用化に向けた研究の歴史と現在**」では，NTT セキュアプラットフォーム研究所の五十嵐大氏より，実用に進んでいる研究の歴史を振り返りながら，秘密計算の実装ライブラリの実例を説明する．

続いて「**3. 秘密分散法を用いた 3 者秘密計算の有用性**」では，NEC の荒木俊則氏と産業技術総合研究所の森田啓氏と花岡悟一郎氏から，秘密分散型の秘密計算について説明する．特に，3 者が協力して秘密計算を行う方式について，基本的なアルゴリズムについて説明する．

続いて「**4. Garbled circuit を用いた秘密計算と混合的構成**」では，NTT セキュアプラットフォーム研究所の菊池亮氏と産業技術総合研究所の Nuttapong Attrapadung 氏より，Garbled circuit 型の秘密計算について説明する．この方式は，1986 年に Yao によって提案された方式であり，その後の研究で改良が進められていることを説明する．

そして，「**5. 準同型暗号を用いた秘密計算技術と実用化に向けた活動**」では，筑波大学／理化学研究所の佐久間淳教授と筑波大学の陸文傑氏から，準同型暗号を用いた秘密計算について説明する．特にゲノム分析に適用した実用化を目指した研究についても紹介いただく．

続いて，本特集では，秘密計算の技術面の紹介だけでなく，関連する法制度についても説明する．特に，秘密計算が目指している組織間での安全なデータ結合分析に関連して，まず，「**6. 組織間データ結合における海外制度の動向**」では，日立コンサルティングの美馬正司氏より，海外の組織間でのデータ結合に関する制度について説明する．組織間でのデータ結合は，秘密計算技術を用いずに信頼のおける第三者を設置するのも 1 つの方法である．この記事を通じて，信頼のおける第三者を設置するのがよいか，それとも秘密計算を用いて信頼のおける第三者の設置を不要とするのがよいかの検討の参考になればと考えている．

そして最後に，「**7. 秘密計算技術に関する国内法制度**」にて，ひかり総合法律事務所の板倉陽一郎弁護士から，秘密計算に関連する法制度について説明していただく．現状の法制度では，組織間でのデータ結合が容易でないことを説明いただく．

上記のように本特集では，秘密計算の概要とさまざまな方式の説明だけでなく，関連する法制度についても説明する．この特集全体を通じて，一般の技術者だけでなく法学者や政府関係者などにも技術の理解を深め，秘密計算技術の社会実装に向けた議論を活発化していければ幸いである．

なお，秘密計算は，秘匿計算やセキュア関数計算とも呼ばれる．また，複数の参加者が通信し合って処理する場合もあるため，マルチパーティ計算やマルチパーティプロトコルとも呼ばれる[☆1]．より上位概念で，データマイニングの際のプライバシの観点で，プライバシ保護データマイニングとも呼ばれることもある．本特集ではこれらのさまざまな技術や呼び方の総称として秘密計算と表記する[☆2]．

（2018 年 8 月 3 日）

☆1 準同型暗号を用いる場合など，マルチパーティでない場合もある．

☆2 英語でも Secure function evaluation，Secure computation，Secure multi-party computation，Multi-party protocol などの表記がある．Secure とは安全という意味になるが，本特集ではよく使われる表記である秘密計算に統一する．