2023年11月22日掲載

経済透視図 (97)

データ漏えい・不正利用減

秘密計算技術の社会実装

SMBC日興証券
プライベート・キャピタル・ソリューション室
片山 大樹

ビジネスにおけるデータ利活用が活発化する中、高機密性データの企業間連携やプライバシー保護の世界的な潮流への対応などが課題となっている。経団連の「データ連携の進展状況に関するアンケート」によると、個人データの取り扱いやデータの標準化、個人や他社の理解を得ることなどを課題と捉える企業が多い。これらの課題を解決する技術として「秘密計算」の社会実装が期待される。

秘密計算とは、データを秘匿したまま処理・計算を行うことが可能となる技術の総称である。従来、暗号化されたデータを分析する際にはいったん復号する必要があり、分析時にデータ漏えいや不正利用のリスクがあった。秘密計算の活用により、こうしたリスクの最小化が可能となる。

代表的な手法には秘密分散型マルチパーティー計算（MPC）や準同型暗号がある。

秘密分散型MPCとは、秘密分散（データを複数の断片に分割、無意味化する仕組み）と、複数サーバーであらかじめ指定された手順で計算を行うマルチパーティー計算の技術をいう。その他、GCやTEE方式などが存在し、それぞれ異なる特性を有する。

準同型暗号とは、準同型性という数学的な性質を用いて暗号化したまま計算を行う方式をいう。

ここで、秘密計算の活用事例として、金融領域におけるAI（人工知能）を活用した不正送金検知自動化への取り組みを取り上げる。

一般的に、単独の金融機関が持つ不正送金に関するデータ量は機械学習では不十分な上、個人情報を含むデータは外部に持ち出せないため、複数の金融機関が協力して機械学習を行うことが困難であった。これらの課題に対し情報通信研究機構（NICT）や銀行などが連携し実証実験が行われ、目標である「不正送金検出精度80%以上」を達成、現在も実験が継続中である。

金融領域以外にも、製造サプライチェーン（部品供給網）の高度化、AI創薬および化合物探索など適用範囲は広い。今後はさまざまな領域で事例が積み上がるだろう。

特に、個社では十分な学習データ量が確保できない、企業秘密や個人情報を含む外部持出しが難しいなどの問題を抱える領域で実装が進むと期待する。

一方、社会実装には課題も残される。秘密分散型MPCでは連携システム設計の必要があること、準同型暗号では暗号文のデータ量が膨大になり計算時間を要することなどが挙げられる。

こうした課題に対し、システム構成等があらかじめ設定されたクラウドサービスの提供、特化型の半導体の開発やソフトウエア・アルゴリズムの最適化、などの取り組みがみられる。今後ますますデータ利活用の重要性が高まると考えられ、引き続きこれらの取り組みに注目したい。

（隔週水曜日に掲載）