秘密計算で進むデータ利活用ビジネス

「データを暗号化したまま計算する」暗号技術により、従来では不可能であった、プライバシーを守ったままの委託計算やニーズマッチングが可能となった。この秘密計算技術が金融機関内の個人情報を含む膨大なデータの利活用の一助になると考えられる。

秘密計算とは「データを暗号化したまま計算する」技術である。暗号技術はデータを保護しつつ伝達するニーズから発展したが、秘密計算はさらに進んで、データ保有者が、データ分析・計算を委託する際に、計算受託者にもデータの中身を知られたくないニーズに応えるものだ。仕組みは、データ保有者は、データを暗号化した上で計算受託者へ渡す。受託者は、データを復号せずに計算を実行し、結果のみがデータ保有者に返される。これにより、計算委託側と受託側双方のプライバシーセキュリティが向上する。

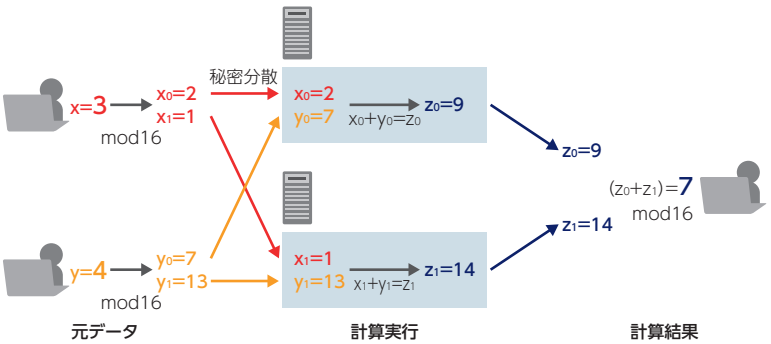
すでに海外では、コモディティの取引オークションや、個人の収入と教育履歴の分析、秘密鍵の管理などへの適用事例がある。はじめに秘密計算の実現方式を簡単に紹介する。

秘密計算の方式

秘密計算の代表的な実現方式に準同型暗号とMPC（Multi-Party Computation）ベースがある。準同型暗号は、足し算か掛け算どちらか一方が計算でき、かつ“完全”がつく完全準同型暗号では、両方できるのが特徴だ。足し算・掛け算が同時にできることは計算機のすべての演算ができることを意味する。ただし、この方式は複雑な処理に対して計算量が膨大になる難点がある。

次に、MPCベースは、秘密分散を利用するものでデータを断片化して複数の場所に分散保有することによって安全性を高める暗号技術である。分散されたデータの一つ一つには意味がないため、一つの片が盗まれても、元のデータが何であったか分からない。データ復元には、分散したデータ片を集める必要がある。計算実行には、秘密分散によって複数のサーバーに配置されたデータ片に対して、サーバー間で通信しながら計算を行う。そして各サーバーの結果を集めることで、意図する計算結果が復元できる仕組みだ。MPCベースの秘密計算は、ネットワーク環境含むサーバー構成が難しい反面、計算速度は速い。

図表　秘密分散を使った3＋4＝7の計算例



金融機関など企業のもつ個人情報の利活用

秘密計算は金融機関や一般企業の保有データの利活用に応用できる。すでに大手運輸会社では、乗車記録や購買データを秘密計算により、人の流れ分析やマーケティングに活かすプロジェクトを進めている。

また、金融機関内には預金額や預かり資産などを含む個人情報があり、これらをマーケティングや広告に結び付けるビジネスにチャンスがあると期待されている。その際、個人情報を目的外利用や分析するときに、秘密計算を応用するのである。ただし「暗号化された個人情報」が個人情報であるかなど、その扱いに関

しては、個人情報保護委員会で議論がされており、今後の方向性を見定める必要がある。

この問題を解決する方法として匿名加工情報に直すことが考えられる。匿名加工情報とは、個人名・IDの削除やデータのレンジ化などにより、個人が特定されず、元の個人情報への復元も不可とするものだ。これにより目的外利用や第三者利用へのハードルを下げつつ、統計・傾向分析も可能となる。

企業単体で活用するケースだけでなく、業界横断する共同利用型ケースも考えられる。共同利用型は、企業同士はデータを共有することなく、統計情報やAIモデルのみ共有する。この例として、金融機関の口座引き落としや・送金などのアクションについて、不正取引を検知するAIモデルの共同構築が社会実験として行われている。1つの金融機関が保有する不正取引データは少ないが、複数機関が集まることで、学習データは多くなり、AIの精度は向上する。各金融機関同士はお互いのデータは共有しないため、セキュリティは高い。

相対取引マーケットにおける活用

次に不動産などの相対取引マーケットでの応用がある。不動産仲介では匿名で物件情報や購入希望金額などを隠したまま、取引相手を探すニーズは高い。売却側は、物件を暗号化する一方で、購入側は価格・地域などの購入希望条件を暗号化する。これらを集めたプラットフォーム上で秘密計算を行い、ニーズをマッチングする。このようにすれば管理者やプラットフォーム運営側も、物件や購入希望条件をみることはできない。不動産仲介では一部社会実装が進んでいるが、多くの課題があるものの有力な応用分野である。

さらに応用が期待できる分野として、デジタルアセットや事業承継、M&A、オークションなどが挙げられる。とくにブロックチェーンと組み合わせると、不正・改ざんなどの防止手段となり、取引プラットフォームとしての価値は高まる。

秘密計算によるプライバシー保護

社会全体でデータは増え、その流通コストも下がる中で、データの共有・利活用は社会に多くのメリットを提供している。それは、すでにプラットフォーマーやポータルサイトが、クッキーデータやサイトへのアクセス分析により、広告ビジネスを展開し、大きな利益を上げていることから明らかだ。

一方で、このようなインターネット上のクラウドサービス内では、個人による自身のデータのコントロールは難しくなり、プライバシーが完全な意味で守られているかは確証できない。その欠点・不安を補いつつ、データを共有・利活用するための社会インフラとして、秘密計算の活用が期待される。

とりわけ多くの個人情報を保有している金融機関や一部企業にとって、これらの利活用や分析、業界を超えた共有は急務であり、その際にプライバシーを守りながらビジネス展開するために、暗号技術の駆使が必須である。

Writer's Profile

外園 康智 Yasunori Hokazono
ホールセールプラットフォーム企画部
上級研究員
専門は人工知能・暗号技術
focus@nri.co.jp