【1 分解説】秘密計算とは？

総合調査部 政策調査グループ 研究理事　重原正明

秘密計算とは、個々のデータの内容がわからないまま、それらについて集計や分析などの計算を行うことです。

個人情報や取引情報などのデータには秘匿性が重視されるものがあります。一方、データ分析上は、個別データではなく平均値などの統計量のみが重要な場合もあります。このような際に、元のデータについて知ることなく、統計量のみを得る技術の一つが、秘密計算です。

秘密計算には現在大きく 2 つの手法があります。一つは秘密分散を利用する方法です。データを 2 つ以上の要素に分解し、各要素別々に計算した上で統合して、元データに対する計算結果を得る方法です。分割した要素は単独では元の要素を復元できないものでなければならないので、分割には乱数等が使われます。

もう一つは準同型暗号を用いる方法です。準同型暗号とは、例えば足し算で考えると、暗号化したデータを足したものが、元データを足した上で暗号化したものと等しくなる暗号のことです。暗号化されたデータを受け取り、それの合計や平均を出した後で、元データの保有機関に返して解読してもらえば、元データに触れられない者もその合計や平均を得ることができます。

秘密計算は医療情報の分析、購買データの共同分析などに使われています。今後このような技術により健全な情報の活用が進むことを期待します。