秘密計算及び統計的開示制御を組み合わせた セキュアな統計処理システムの提案

NTT セキュアプラットフォーム研究所　高橋 慧，千田 浩司
一橋大学経済研究所　白川 清美

1. はじめに

現在，公的統計の個票データの活用においては，プライバシー保護のため厳格な管理体制や，集計結果の秘匿性検査の実施など様々な課題がある．そこで我々は，これらの課題解決のため秘密計算の活用を検討する． 秘密計算はデータを暗号化したまま統計処理を可能とする技術であり，機微なデータの利活用と保護を両立させる技術として注目されている．しかし，秘密計算は分析結果から漏れ得る元データの情報 (出力プライバシー) については一般に考慮していない．そのため，出力プライバシーを保護する統計的開示制御と秘密計算を組み合わせた手法の確立が求められる．

本研究では秘密計算で既に実現されているフィルタリング演算およびシャッフル演算を用いて必要最小限のミクロデータを秘密計算により求め，当該ミクロデータから出力プライバシーが保証された統計結果を求める手法を提案する．また，既存の秘密計算システムおよび統計的開示制御を備えた統計処理ソフトウェアを用いて実際に提案手法を実装し，正しく結果が得られることを確認する．

2. 秘密計算

秘密計算は，暗号化などの方法でデータを秘匿したまま，元のデータに復元することなく計算ができる技術である．本論文では秘密分散法をベースとしたマルチパーティプロトコルによる秘密計算法[1]に着目し，検討を行う．秘密計算技術はデータを暗号化して保管することで，元データの情報が外部に漏えいすることを防ぐことができるが，演算結果から元データについて推計することを防ぐ出力プライバシーへの対応については現状では保証外としている．

3. τ-ARGUS

τ-ARGUSは，データ保護責任者が安全な表を作成することを支援するために設計されたソフトウェアツールである．本ソフトウェアを用いることにより，ユーザはGUI操作によって集計表に対する秘匿処理を行う事が可能となる．

4. 秘密計算システムとτ-ARGUSの連携

本論文では公的統計の個票データ活用に向けて、データの漏えいを防ぐ技術として秘密計算を適用し，秘密計算の課題であった出力プライバシーに対応する目的でτ-ARGUSを適用する．これにより，秘密計算を用いてデータ保管時の安全性を確保し，τ-ARGUSを用いて出力データからの情報漏えいを防ぐ．

本検討において想定する連携システム構成を図1及び図2に示す．

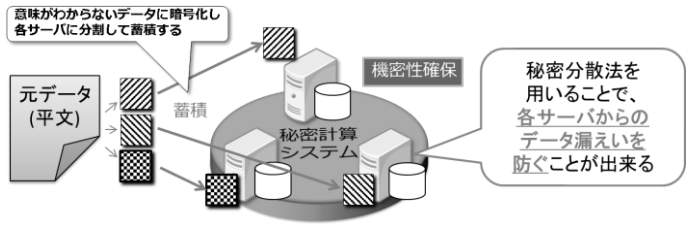

図 1 秘密計算システムへのデータ登録

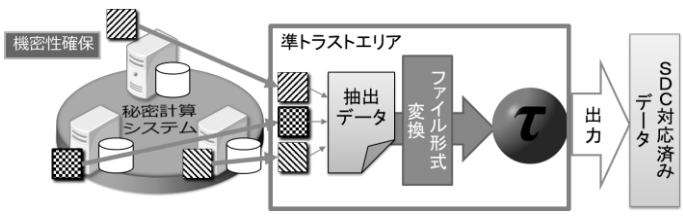

図 2 秘密計算システムからの出力と SDC の適用

[1] 菊池 亮,五十嵐 大,濱田 浩気,千田 浩司."改ざん検知機能付きの実用的な秘密計算システム MEVAL2"SCIS 2015