SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

秘匿 SQL Window 関数プロトコルの提案
Secure SQL Window Functions

須藤 弘貴 *　　菊池 亮 *
Hiroki Sudo　　Ryo Kikuchi

キーワード 秘密計算, 秘密分散, データベース

あらまし

近年，様々なデータを収集できるようになり，機械学習技術等の分析技術の発展もあり，データ利活用に対する期待が高まっている．その一方で，機密情報保護リスクから，安易に情報を扱うことはできず，利活用とセキュリティの両立をどのように実現するかが問題となっている．

この問題の解決に向けて期待されているのが，秘密計算技術である．秘密計算技術は暗号化したまま計算を行う技術の総称である．秘密計算技術によりデータを暗号化してクラウドに預け，暗号化を解くことなく秘匿したまま計算を行うことができる．

秘密計算は通常の計算と比べオーバーヘッドが大きいことが課題であったが，近年では高速化なフレームワーク [1] が提案されている他，秘密計算上で JOIN[2, 3] や GROUP BY[4] などのデータベース操作を効率的に行う手法も提案されている．

本稿ではデータベース操作の中でも，SQL Window 関数の代表的な集約関数 (max/min, sum) を秘密計算上で実現する手法を提案する．Window 関数は「窓枠」を指定して所定の集約関数等により集計を行うことができる SQL SELECT 機能の一つである．

参考文献

[1] 桐淵直人, 五十嵐大, 濱田浩気, 菊池亮. プログラマブルな秘密計算ライブラリ MEVAL3. In *SCIS2018*, pp. 1–8, 2018.

[2] 桐淵直人, 五十嵐大, 諸橋玄武, 濱田浩気. 属性情報と履歴情報の秘匿統合分析に向けた秘密計算による高速な等結合アルゴリズムとその実装. In *CSS2016*, pp. 1–8, 2016.

[3] 五十嵐大, 濱田浩気, 菊池亮. 僕たちは一番大切なものに気づいていなかった-秘密外部結合プロトコルの設計と実装-. In *CSS2018*, pp. 1–8, 2017.

[4] 菊池亮, 濱田浩気, 五十嵐大, 高橋元. 横断的動線分析を秘密計算でやってみよう. In *SCIS2020*, pp. 1–8, 2020.

* NTT 社会情報研究所 〒 180–8585 東京都武蔵野市緑町 3–9–11. NTT Social Informatics Laboratories, 3–9–11, Midoricho, Musashino, Tokyo, Japan.