研究課題別事後評価結果

１．研究課題名：　ビッグデータ統合利用のためのセキュアなコンテンツ共有・流通基盤の構築

２．研究代表者名及び主たる研究参加者名（研究機関名・職名は研究参加期間終了時点）

研究代表者

山名早人　（早稲田大学理工学術院基幹理工学部　教授）

主たる共同研究者

後藤厚宏　（岩崎学園情報セキュリティ大学院情報セキュリティ研究科　教授）

小口正人　（お茶の水女子大学基幹研究院　教授）

山口実靖　（工学院大学情報学部　准教授）

新谷隆彦　（電気通信大学大学院情報理工学研究科　准教授）

野口　保　（明治薬科大学薬学部　教授）

事後評価結果

○評点：

A　優れている

○総合評価コメント：

（以下、2020 年度課題事後評価時のコメント）

ビッグデータの中には、個人や組織の秘密を含むものが少なくない。しかも、ビッグデータの解析を行う際には、データの管理者と解析サービスの提供者が同一でないことも多い。このような状況で、ビッグデータからの情報漏洩を非常に高いレベルで防ぐために、データを暗号化したまま解析する技術が存在する。代表例である完全準同型暗号方式は、従来、処理速度が非常に遅いという問題を抱えていた。本課題では、この方式の高速化を図るため、SIMD 計算向け方式設計などの理論的検討、メモリ管理の効率化などのシステムのチューニング、表検索による計算の置き換えなどのアルゴリズム面での工夫を総合的に駆使した研究を行なった。そして、この分野の標準的なライブラリである HElib より桁違いに高速（具体的な倍率はアプリケーションに大きく依存）なライブラリを開発した。成果は、情報セキュリティや情報システムの分野の国際会議などで多数発表されており、さらに、ライブラリはオープンソースで公開されている。また、サイバーフィジカルシステムへの応用などの取り組みが行われた。今後、処理スピードを犠牲にしてでも高いセキュリティレベルを求める分野の開拓をさらに進め、アプリケーションに特化した手法も組み合わせることで、実用化が進むことを期待したい。

（2021 年 12 月追記）

本課題は、新型コロナウイルスの影響を受け、6 ヶ月間期間を延長し、当初の研究期間中に実施が困難となった実証実験を行なった。また、公開ライブラリの拡充等も行なった。

その結果、リストバンド型センサデバイスを用いて、実験参加者から 1 万人日分を超えるライフログデータの収集を行い、データを暗号化したまま生活比較分析を行うことができた。また、実験参加者の許諾を得た 4,200 人日分のデータを公開することもできた。さらに、薬局をフィールドとした実証実験では、顧客のパーソナルデータを秘匿した医薬品副作用解析をテーマに 4 店舗での実験を行い、サービス提供の可能性を示すことができた。

延長により、現実の問題への適用可能性の検討・検証が進み、今後のイノベーションに向けた展開をより一層後押しする成果が得られた。