ビッグデータ統合利活用のための次世代基盤技術の創出・体系化
2015 年度採択研究代表者

2019 年度
実績報告書

山名　早人

早稲田大学理工学術院
教授

# 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

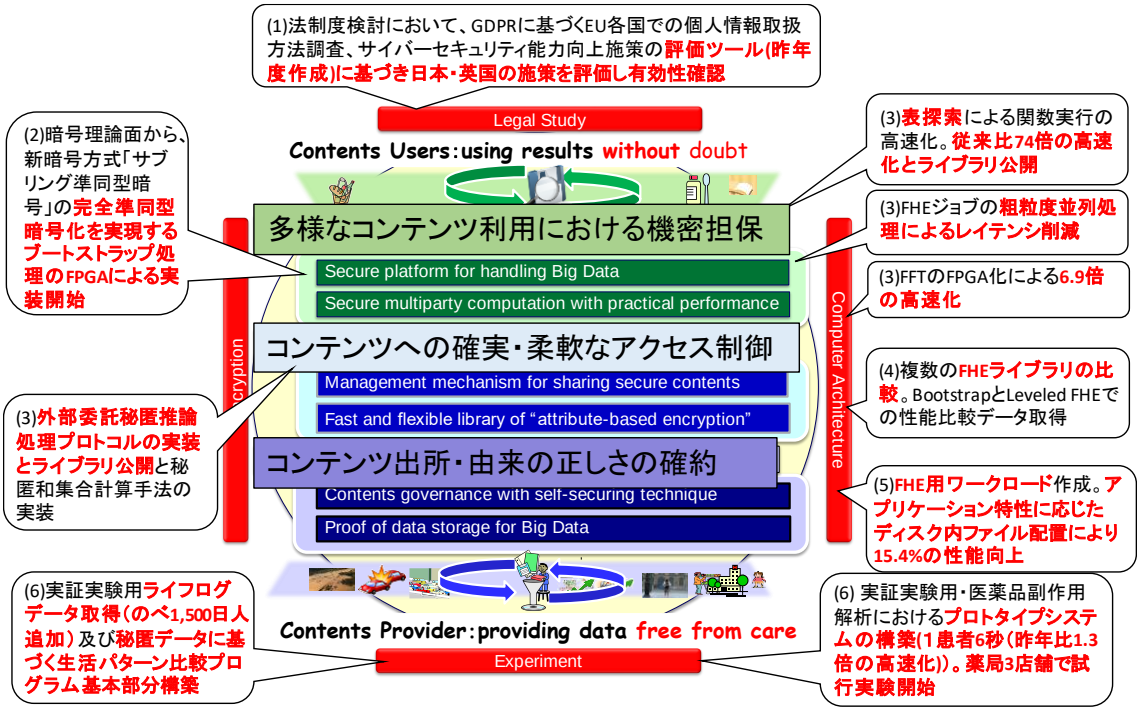
## §1. 研究成果の概要

ビッグデータの利活用推進のためには、コンテンツ提供者が安心してデータを提供でき、コンテンツ利用者が信頼して結果を利用できる基盤が求められる。これに応えるため本研究では、「匿名化」や「通信時の暗号化」から脱却し、コンテンツを常に暗号化した状態で扱うことのできる基盤の構築を目指している。

令和元年は、以下で述べる要素技術の高度化だけでなく、完全準同型暗号の応用として推論処理が重要な分野であることに鑑み、学習済モデル、クライアントからのクエリ、推論結果をサーバ（クラウド）から隠した状態で推論処理を行うプロトコルを考案、実装し[1]、ライブラリとして公開した。また、主な要素技術としては、ディスクアクセスにおいてディスク外周部のアクセス速度が内周部の約 2 倍となることに着目し、アプリケーションの特性に応じてディスク内ファイル配置を行う最適化手法を提案、評価し[2]、完全準同型暗号に限らず様々なアプリケーションに適用可能であることを示した。一昨年度提案した独自の準同型暗号方式「サブリング準同型暗号方式」[3]については、さらなる高速化を目指し、Bootstrap 処理の FPGA 実装を開始した。

最終年度に向けての実証実験の準備を進めており、医薬品副作用解析システムにおいては、薬局との連携のもと試行実験を開始した。ライフログデータ解析システムにおいては、必要となるライフログの収集を継続すると共にプログラム構築を行った。

本年度の顕著な成果は、図に示す通り、(1)法的検討面から各国の施策評価、(2)「サブリング準同型暗号方式」の FPGA 実装、(3)完全準同型暗号で様々な計算を実現するための関数実行方式の提案、(4)完全準同型ライブラリ比較、(5)ディスク内データ配置最適化、(6)実証実験アプリケーションの準備である。なお、今年度、新たに公開を開始したライブラリは3件であり、合計 7 件のライブラリをこれまでに公開した。https://www.yama.info.waseda.ac.jp/crest/ から入手できる。




[1] Yoshiko Yasumura, Yu Ishimaki, Hayato Yamana, "Secure NaIve Bayes Classification Protocol over Encrypted Data Using Fully Homomorphic Encryption," Proc. of the 21st International Conference on Information Integration and Web-based Applications & Services (iiWAS2019), pp.45-54 (2019.12) DOI: 10.1145/3366030.3366056

[1] M. Nakagami, J. A. B. Fortes and S. Yamaguchi, "Job-Aware Optimization of File Placement in Hadoop," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, pp. 664-669 (2019.7) DOI:10.1109/COMPSAC.2019.10284

[3] Seiko Arita, Sari Handa, "Fully Homomorphic Encryption Scheme Based on Decomposition Ring," IEICE TRANS., vol. E103-A, no. 1, pp.195-211 (2020.1) DOI:10.1587/transfun.2019CIP0027

## §2. 研究実施体制

(1)「山名」グループ

① 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情報理工学科　教授）

② 研究項目

・暗号ライブラリ構築(コンピュータアーキテクチャ面からの高速化)

・クラウドプラットフォーム構築

(2)「後藤」グループ

① 主たる共同研究者:後藤　厚宏 （情報セキュリティ大学院大学情報セキュリティ研究科　教授）

② 研究項目

・法的検討・ガイドライン策定

・暗号ライブラリ構築（暗号理論面からの高速化）

(3)「小口」グループ

① 主たる共同研究者:小口　正人 （お茶の水女子大学基幹研究院　教授）

② 研究項目

・クラウドプラットフォーム構築

(4)「山口」グループ

① 主たる共同研究者:山口　実靖 （工学院大学情報学部情報通信工学科　准教授）

② 研究項目

・暗号ライブラリ構築（I/O 面からの高速化）

(5)「新谷」グループ

① 主たる共同研究者:新谷　隆彦 （電気通信大学大学院情報理工学研究科　准教授）

② 研究項目

・実証実験(ライフログデータ取得・解析システム構築)

(6)「野口」グループ

① 主たる共同研究者:野口　保 （明治薬科大学薬学部薬学教育研究センター　教授）

② 研究項目

・実証実験（医薬品副作用解析システム構築）