「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」
平成27年度採択研究代表者

H28 年度
実績報告書

山名　早人

早稲田大学理工学術院基幹理工学部
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数理科学部門、教授）

② 研究項目

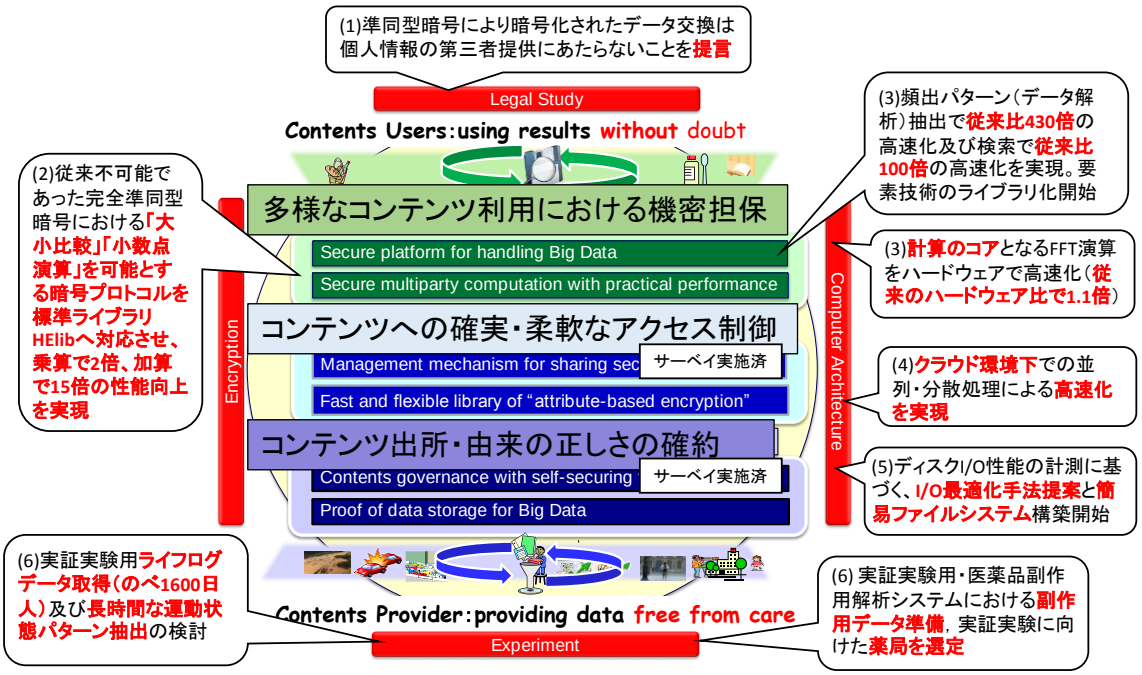
・実証実験（医薬品副作用解析システム構築）

§2. 研究実施の概要

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今まさに求められている。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。しかし、暗号化した状態で計算を実現するには膨大な時間が必要となるため実用化が困難である。これに対して本研究開発では、暗号理論とコンピュータアーキテクチャの両面で最適化を行うことにより、1,000 倍以上の高速化を行うことを目指している。

本年度は、当初計画として設定した「3 年度目までの 400 倍の高速化」を特定のアプリケーションに対して達成することに成功し、当初の予定通り多種多様なアプリケーションの高速化に寄与するようモジュール化を開始したところである。特に顕著な成果は、(a)新しい暗号プロトコル提案による高速化(乗算で 2 倍、加算で 15 倍)[1]、(b)完全準同型暗号処理でのベクトル化(パッキング)[2]、(c)暗号化されたデータの効率的な再利用手法(キャッシング)[2]、(d)クライアント・サーバ間のストリーム処理[2]の提案とそれらによる高速化の実現である。

全体の成果は図に示す通り、(1)暗号化データの扱いに関する提言、(2)完全準同型暗号をビッグデータ処理に活用する上での障壁であった大小比較、浮動小数点演算を実現する暗号プロトコルの標準ライブラリへの適用と高速化評価[1]、(3)解析アプリケーションでの従来比 430 倍の高速化[2]、検索アプリケーションでの従来比 100 倍の高速化の実現、(4)さらなる高速化のためのクラウド側での並列・分散処理の実現、(5)膨大なデータを高速処理する上で欠かせないディスク I/O 最適化手法提案[3]と簡易ファイルシステム構築開始、(6)実証実験アプリケーションの準備である。



[1] Seiko Arita and Shota Nakasato, Fully Homomorphic Encryption For Point Numbers, In Proc. of

INSCRYPT 2016, Beijing, Chaina, 2016.
[2] 今林広樹, 石巻 優, 馬屋原 昂, 佐藤 宏樹, 山名 早人, 完全準同型暗号による 安全頻出パターンマイニング計算量効率化, 情報処理学会論文誌 TOD, Vol.10, No.1, pp.1-12, 2017.
[3] Eita Fujishima, Kenji Nakashima, Saneyasu Yamaguchi, Performance improvement of I/O intensive OLAP with dynamic control of file storing location, In Proc. of the 11th International Conference on Ubiquitous Information Management and Communication, 2017