「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

H27 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 （工学院大学工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システム学研究科、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)

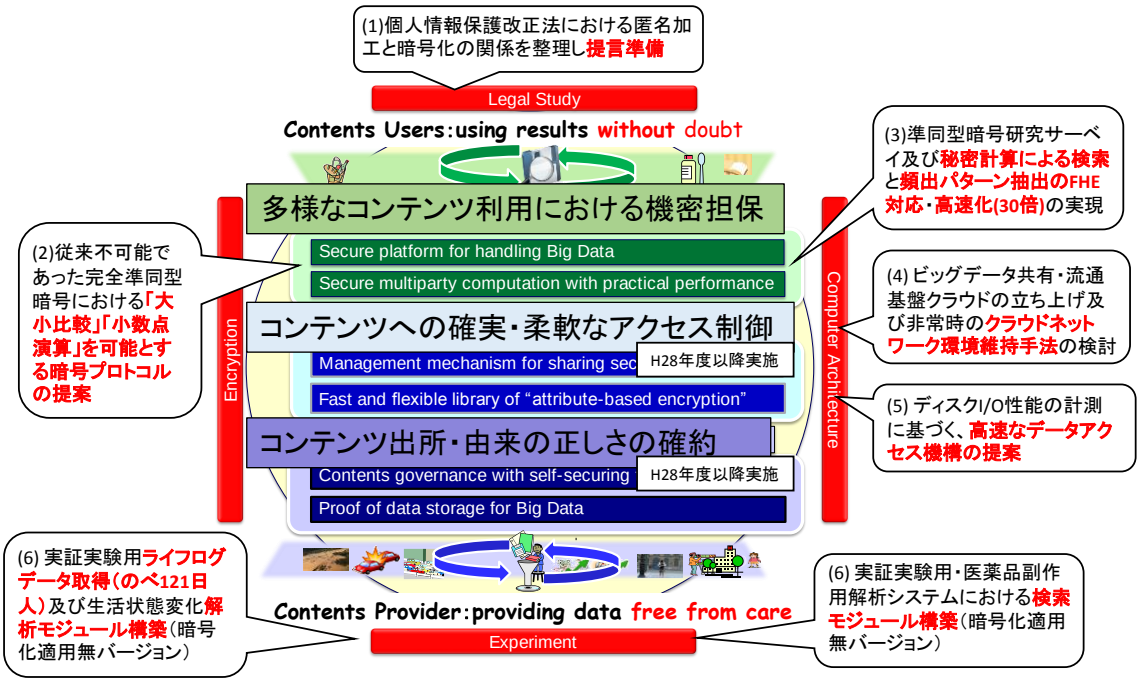
② 研究項目

・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、図に示す通り、 (1)暗号化の法律上の位置づけの整理、(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システムの提案[1]、(3) 検索及びデータマイニングにおける完全準同型暗号の実装とベクトル化による高速化[2]、(4) 実証実験用クラウド環境の立ち上げと災害時のクラウドネットワーク維持手法の検討[3]、(5) ディスク I/O 高速化にあたっての基礎データ取得、(6) 実証実験アプリケーションの準備を行った。特に、暗号化したままの状態では実現ができなかった(a)数値間の大小比較及び(b)浮動小数点演算の実現、さらに(c)検索及び頻出パターン抽出(データマイニング)を題材とした完全準同型暗号のベクトル化(パッキング)による約 30 倍の高速化は今年度の顕著な成果である。



[1] 有田正剛, 中里 翔太: Fully Homomorphic Encryption For Point Numbers, 2016 Symposium on Cryptography and Information Security (SCIS2016), 1E1-5, Jan.2016.
[2] 石巻 優, 清水佳奈, 縫田光司, 山名早人:完全準同型暗号を用いた高速なゲノム秘匿検索, 2016 Symposium on Cryptography and Information Security (SCIS2016) , 2A2-2, Jan.2016.

[3] Chihiro Maru, Miki Enoki, Akihiro Nakao, Shu Yamamoto, Saneyasu Yamaguchi, and Masato Oguchi: "Network Failure Detection System for Traffic Control using Social Information in Large-Scale Disasters," Proc. of ITU Kaleidoscope Conference 2015: Trust in the Information Society, pp.1-7, Dec.2015.