「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 26 年度採択研究代表者

H27 年度
実績報告書

宮地　充子

大阪大学大学院工学研究科
教授

ビッグデータ統合利活用促進のためのセキュリティ基盤技術の体系化

§1. 研究実施体制

(1)セキュリティコア技術グループ

① 研究代表者:宮地　充子 （大阪大学　大学院工学研究科　教授）

② 研究項目

- セキュアデータ管理
- 耐サイバー攻撃
- セキュアデータマイニング
- セキュアデータ運用

(2)セキュアデータ流通管理グループ

① 主たる共同研究者:清本　晋作(KDDI研究所　グループリーダ)

② 研究項目

- 耐サイバー攻撃
- プライバシ設定支援
- 匿名化技術のリスク評価手法
- データ漏洩抑止技術

(3)予防安全テストベッド実証グループ

① 主たる共同研究者:西田　佳史(産業技術総合研究所　首席研究員)

② 研究項目

- 予防安全テストベッド

(4)医療テストベッド実証グループ

① 主たる共同研究者:山本　隆一(東京大学大学院医学系研究科　特任准教授)

② 研究項目

- 医療テストベッド

§2. 研究実施の概要

グループ全体の成果統合図を図 1 に示す。各チームの研究実施概要は下記のとおりである。

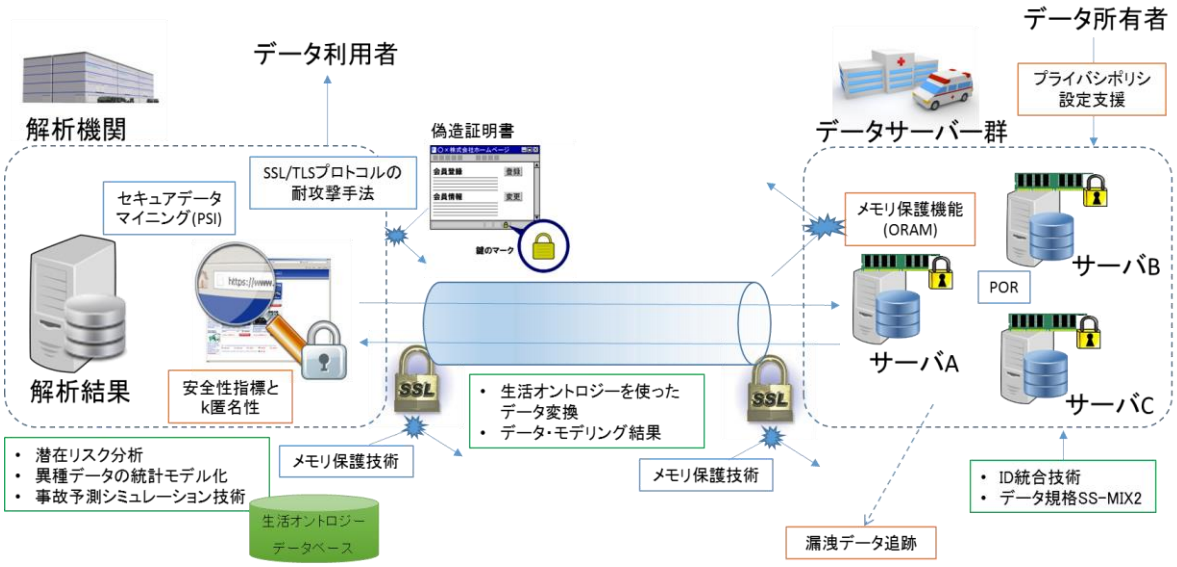

図 1 成果統合図

「セキュリティコア技術グループ」

セキュアデータ管理では、元のデータの機密性を保ちつつ新たなクラウドサーバの符号化データを生成できる **POR**（Proofs of Retrievability）方式（H26 年度提案）のソフトウェアを作成し、実装評価を実施した。また、対話型プロトコルを通して、クライアントのアクセスパターンを秘匿する **ORAM**（Oblivious RAM）技術では、クライアント・サーバ間に安全かつ効率な ORAM 方式を H27 年度に提案した[1]。さらに、提案方式の実装・評価を行った。耐サイバー攻撃システムでは、偽造証明書を排除する証明書検証システム（H26 年度提案）に関して、実用性を検証するために Web ブラウザにプロトタイププログラムを組み込んだツールを作成し、課題を抽出した。セキュアデータマイニングでは、プライバシを保護しながら、多機関が独立に収集したデータの統計処理を実現できる **PSI**(Private Set Intersection)方式に着目し、アウトソーシングが可能でかつ機関数に計算量が依存しない多機関 PSI 方式を H27 年度に提案した[2]。さらに、提案方式の実装・評価を行った。

「セキュアデータ流通管理グループ」

実装上の脆弱性をつく SSL 等へのセキュリティ機能への攻撃を防ぐ**メモリ保護技術**を研究開発し、OpenSSL に実装して効果を検証した。プライバシ設定を推測する手法について評価を行い、80 項目に対して、提供に対する抵抗意識を 3 段階（提供してもよい、どちらともいえない、提供したくない）で回答するアンケートを 10,000 人の被験者に回答いただいたデータを用いて評価を行い、約 86%の精度で推測できることを明らかにした。追跡可能な匿名化データ生成手法について、安全性指標を定義し、利便性とセキュリティの関係について明らかにした。匿名化データの**リスク評価**手法について、事前に木構造を構築することにより高速化を実現した。

「予防安全テストベッド実証グループ」

平成 26 年度に構築した外傷データベースを用いて、多機関分散データを統合的に活用するアルゴリズムと、初期のアプリケーション開発を行った。具体的には、複数の学校に分散している外傷データに適用することで、類似事故状況下での重症事例の予測機能を開発した[3](図 2)。これにより、個々の学校のデータだけでは、レアケースか、重症に至るリスクが存在するのかの判断が難しいという問題を、個別の学校の守秘は保ちつつ、解決可能となる。また、乳幼児が事故を起こしにくい家庭環境の整備のために各家庭環境に合わせて事故把握から**事故予測**への応用を目指したアプリケーションを開発した。医療機関、研究機関、メーカなど複数の機関が保有する、事故データ、乳幼児の発達データ、製品・環境データ、製品との相互作用に関するデータといった項目が異なるデータを、**統計モデル化**したり、構造化されたデータにすることで統合可能にし、環境や乳幼児の年齢などの情報を入力することで、個別環境内に存在する物体から起こりうる事故状況を予測する新たなシミュレーション技術の開発を行った(図 3)。

図 2 類似事故状況下重症事例提示の例

図 3 事故状況の4次元再現の例
(誤飲・熱傷事故の状況可視化)

「医療テストベッド実証グループ」

分散した診療情報にかかわるデータベース統合に向けて、**ID 統合技術**としての IHE-ITI の XDS、ATN、PIQ、PDQ、XCA の日本語化を行い、また我が国に固有の事情を付加し(例えば住基4情報)た。また、医療情報を横断的にビッグデータとして分析するために、一定の共通情報モデル化(common data model)のためのデータ規格を検討し、**SS-MIX2** を採用した。これらは、山本が代表を務める医療情報標準化推進協議会(HELICS)の推奨標準として制定した。また、SS-MIX2 からテストベッド実証システム向けにデータ抽出を行うためのソフトウェアを開発した。また、セキュリティコア技術グループで開発した ORAM ソフトウェア、証明書検証システムのプロトタイプについて、実際の運用シーンを想定した動作検証、評価を行った。ORAM ソフトウェアについては大規模ストレージへの適用を考慮した検証を引き続き行う。

[1] Steven Gordon, Atsuko Miyaji, Chunhua Su, Karin Sumongkayothin, "A Matrix based ORAM: Design, Implementation and Experimental Analysis", IEICE Transactions, Vol.E99-D, No.8, Aug.2016.
[2] Atsuko Miyaji and Syouhei Nishida, "A Scalable and Efficient Multiparty Private Set Intersection", The 9th International Conference on Network and System Security (NSS

2015), Lecture Notes in Computer Science, 9408, 376-385, 2015.
[3] Koji Kitamura, Kenta Imai, Yoshifumi Nishida, Hiroshi Takemura, Tatsuhiro Yamanaka, "Potential Risk Assessment System by Integrating Injury Data at Multiple Schools", The 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015), pp. 1991-1998, July 2015.