通信・
情報処理

プライバシー保護とデータ連携が両立可能な秘密計算基盤の構築

A secret calculation achieving both privacy protection and data linkage

東京理科大学
工学部 電気工学科　教授
岩村　恵市
Keiichi Iwamura

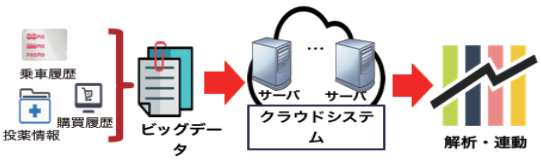
研究概要

内閣府の科学技術政策第５期科学技術基本計画に示されるサイバー空間とフィジカル空間を高度に融合させたSociety5.0（超スマート社会）において、サイバー空間におけるデータ連携を、データを秘匿したまま実行し、プライバシー保護との両立を可能にします。特に、既存技術に必要な大型計算機などの計算環境に依存することなく、軽量な計算によって計算環境を選ばず、データ連携をどこでも誰でも容易に実行可能にします。

研究成果

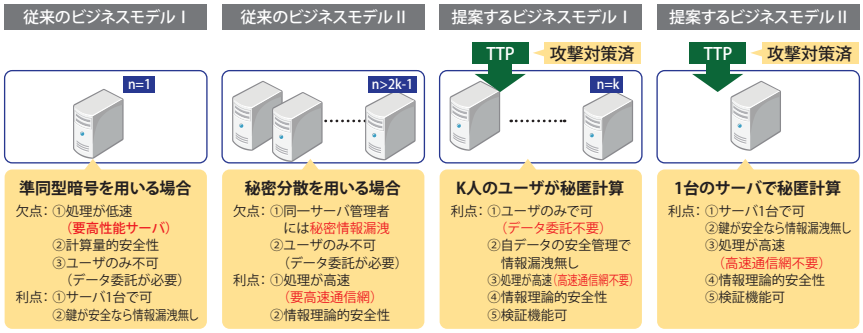
（Ⅰ）秘密情報を預からないユーザによる秘密計算：既存のビジネスモデルと異なり、下記ポイントの③から、ユーザは大型計算機などをもち秘密計算をビジネスとする企業に自分の秘密情報を委託することなく、自らのPC等で秘密計算を実行できます。
（Ⅱ）計算環境に依存しない1 台のサーバによる秘密計算：既存の秘密計算と異なり、秘密分散法を用いても下記ポイントの①,②から、最小1台のサーバ数で計算環境に依存せず秘密計算を行えます。

図１．研究背景



Society5.0（超スマート社会）を実現するためには、IoTなどから得られる膨大なビッグデータを解析・連動させ、かつ、個人のプライバシーを守りながら利活用できる技術が重要となる。

図2. 提案するビジネスモデルとその比較



POINT

①秘密分散を用いて2k-1台未満（最小1 台）のサーバで秘密計算を実行できる。
②暗号との組みわせにより、全てのサーバが攻撃されても秘密情報が漏洩しない。
③大型計算機やサーバ間の高速な通信網を必要とせず高速処理が可能。

従来・競合との比較

- 大型計算機などが無くても1台のサーバで高速に秘密計算可能。
- 単一の組織がサーバを管理しても秘密情報や秘密計算結果は漏洩しない。
- 計算環境に依存せず情報を秘匿したままでデータ連携が可能。

想定される用途

- 膨大なデータを秘匿したまま高速な検索機能を持つクラウドサービス。
- 秘匿された膨大なデータをそのまま用いる情報の分類・解析サービス。
- 異なる組織や業種間のデータの相互運用サービス。

実用化に向けた課題／企業など研究パートナーに期待すること

①秘密計算を用いた具体的応用の実用化。
前記想定される用途などを含む新たな課題をお持ちの企業と共同して課題解決。
②Society5.0（超スマート社会）を見据えたベンチャー企業の立ち上げ。
本技術はSociety5.0に必須の技術であり、それを見据えたベンチャーの起業。

今後の展開

2021.11 ～ 2022.03：以下の２つを行い、秘密計算基盤の土台を構築する。
①物理乱数生成法を取り込んだ TTP を実装する。
②秘匿計算ライブラリの構築・最適化
2022.04 ～ 2022.08：本事業の技術内容の完成と周知を行う。
①前記より秘密計算基盤の土台ができれば、マスコミ発表や研究会・展示会などで本事業の周知を行う。
②本事業で用いる TTP を用いた秘匿計算法を論文発表し、技術を完成させる。
2022.09 ～：AI 技術との融合を行い、完成後起業する。

■知的財産権：
特願2018- 28308：入力者装置、演算支援装置、装置、秘匿演算装置、及びプログラム
特願2018-185931：分散装置、秘匿演算装置、検証復元装置、分散システム、秘匿演算検証復元システム、及びプログラム
特願2021-108577：第三者装置、秘匿計算システム、及びプログラム
■活用した公的資金事業等の名称：
平成26 年度科研費 基盤（C）課題番号26420373
（個人制御可能な秘匿計算手法に関する研究）

東京理科大学　産学連携機構
〒162-8601 東京都新宿区神楽坂一丁目３番地　TEL：03-5228-7440　E-MAIL：ura@admin.tus.ac.jp

検索キーワード
Society5,0（超スマート社会）　データ連携　プライバシー保護
機密データ保護　秘密分散

2022.04