

(報道発表資料)

2023.1.23

情報・システム研究機構 国立情報学研究所

日本電信電話株式会社

NII と NTT、秘密計算システムの大学向けトライアルを開始

～世界初の「AI 4 大カテゴリの主要なアルゴリズムによる学習・推論が可能な秘密計算 AI ソフトウェア」を提供～

情報・システム研究機構 国立情報学研究所(東京都千代田区、所長:喜連川優、以下 NII)は、オープンサイエンスの実現に向け、大学の研究データを適切に管理しつつ利活用を加速するため、秘密計算を用いた安全なデータ分析基盤に関する研究を進めています。

今回、日本電信電話株式会社(東京都千代田区、代表取締役社長:島田明、以下 NTT)と共同で、データを暗号化したまま一度も元に戻さずに、世界初の AI 4 大カテゴリの主要なアルゴリズムによる学習・推論が可能な秘密計算 AI ソフトウェアを利用できるトライアルを提供することになりました。

本トライアルは、NII と NTT の共同研究の一環として、NII の計算機上で秘密計算 AI ソフトウェアを実験的に利用する大学等のパートナーを募集するものです。

NII と NTT は、本取り組みを通じて安全にデータを共有できる基盤技術を確立し、誰もが安心してデータを利活用できる社会の実現を目指します。

1. 背景・経緯

昨今、第四のパラダイムとも呼ばれるデータ駆動型科学の普及にともない、研究データを原則公開し多分野での利活用を図るオープンサイエンスの機運が高まっています。しかし、個人のプライバシーに関わるデータや営業秘密に関わるデータなどは、情報漏洩や不正利用の懸念もあり利活用が進んでいない現状があります。その解決策として注目されているのが、データを暗号化したまま一度も元に戻さず処理ができる秘密計算技術です。

国内唯一の情報学の総合研究所である NII は、大学や研究機関における研究活動を支える次世代学術研究プラットフォーム「NII Research Data Cloud」(NII RDC)の構築に 2017 年から取り組み、2021 年から本格的なサービスの運用を開始しました。この基盤上で研究データ利活用の可能性をさらに広げるため、秘匿解析機能を含む 7 つの高度化機能を開発中であり、その要素技術として秘密計算技術の研究を進めています。

NTT は世界に先駆けて秘密計算技術の研究開発に取り組んでおり、秘密計算による統計処理に加え、秘密計算で深層学習を行う技術の世界で初めて実現しています(2019 年 9 月 2 日報道発表)。ここから更に研究開発を進め、機械学習の基本である回帰・分類・クラスタリング・データ次元圧縮の代表的なアルゴリズムを秘密計算で実現し、世界初の秘密計算 AI ソフトウェアを開発しました。

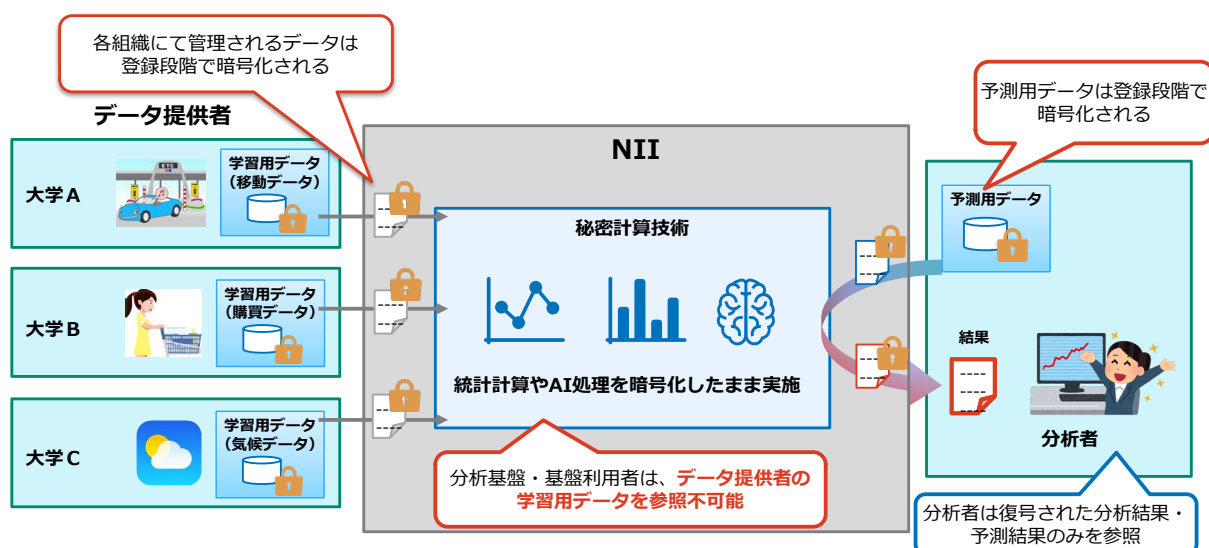
今回、NII と NTT は秘密計算を用いた安全なデータ分析基盤に関する共同研究の中で、NII が所

有する計算機上に NTT の秘密計算 AI ソフトウェア環境を構築し、研究者に試用していただく機会を設けることとしました。第一線で活躍する研究者からのフィードバックを得て、実際の研究における秘密計算技術の有用性を評価するとともに、次世代 NII RDC の秘匿解析機能の開発を見据えた技術検証を行い、世界最先端の学術基盤の構築をめざしていきます。

2. トライアルの概要

- ・利用対象者: 国内の大学・研究機関に所属する教職員・研究者の方
- ・提供期間: 2023 年 1 月末から 2024 年 3 月末までを予定
- ・利用料金: 無料
- ・利用目的: 実験目的(非商用目的)に限る
- ・受付方法: こちらの URL でご案内します。 <https://rcos.nii.ac.jp/news/2023/01/20230123-0/>

<トライアルのイメージ>



<トライアルの役割分担>

参加者	役割
NII	・次世代 NII RDC に搭載される秘匿解析機能の設計・開発・運用を見据えた技術検証を行う。 ・研究者との対話を通じて秘密計算 AI ソフトウェア技術の評価し、研究者にとって有用な秘匿解析機能の設計につなげる。
NTT	・NII 所有計算機へ秘密計算 AI ソフトウェア環境を構築する。 ・クラウド基盤における秘密計算技術のフィージビリティを検証する。

3. 秘密計算 AI ソフトウェアの技術ポイント

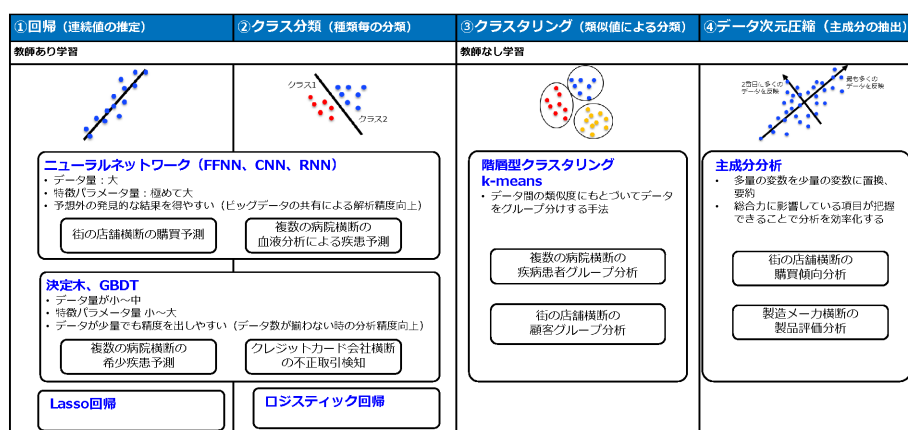
NTT では独自の工夫により、データを暗号化したまま整列や分割操作を高速に行う技術や、浮

動小数点演算を扱った実数演算及び初等関数を効率よく実行する技術を開発しており、これらの技術を AI アルゴリズムにも応用することで、秘密計算による AI 処理のためのプロトコルを効率よく実現しました。

これにより、世界で初めて AI の 4 大カテゴリ(回帰・クラス分類・クラスタリング・データ次元圧縮)の主要なアルゴリズムによる学習・推論が可能な秘密計算 AI ソフトウェアを実現しました。具体的には、勾配ブースティング木・ニューラルネットワーク・階層型クラスタリング・主成分分析などを秘密計算で実行できます(図 1)。

秘密計算 AI ソフトウェアは、データサイエンティストが AI 処理を実施する際に一般的に用いられている、Python を利用して容易にプログラミングすることが可能です。

秘密計算AIで実現したAI 4大カテゴリの 主要なアルゴリズム



Copyright 2022 NTT CORPORATION

2

図 1 秘密計算 AI で実現した 4 大カテゴリの主要なアルゴリズム

4. NII RDC の構想、技術ポイント

NII RDC は研究データの管理基盤 (GakuNin RDM)、公開基盤 (WEKO3)、検索基盤 (CiNii Research) から構成されています(図 2)。

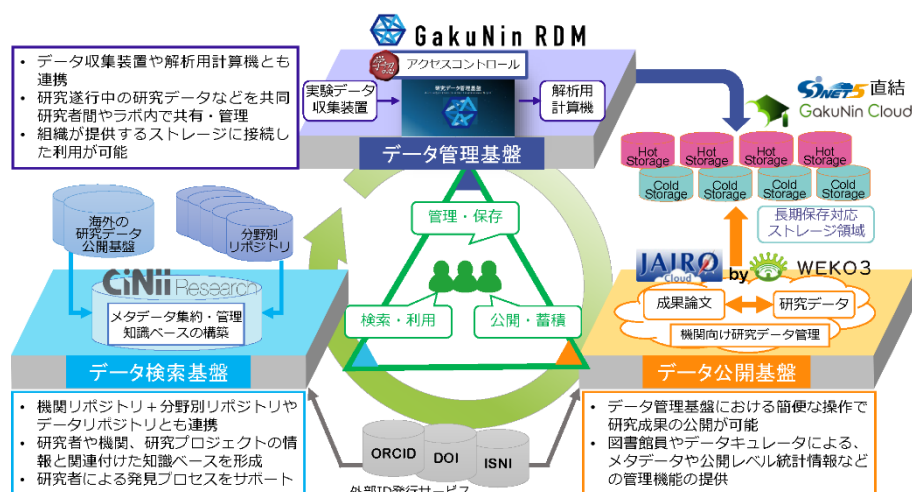


図 2 NII RDC の概要

このうち GakuNin RDM は、研究プロジェクト実施中に、個人の研究者あるいは研究グループが研究データや関連の資料を管理するための研究データ管理基盤です。既存のストレージや研究ソフトウェアと連携し、クローズドな空間で、研究プロジェクトに関わるファイルのバージョン管理や、メンバー内でのアクセスコントロールを実現しており、全国の 52 機関(2022 年 11 月時点)で利用が進んでいます。

今回の取り組みは、次世代 NII RDC における高度化機能(図 3)のひとつである「秘匿解析機能」の実現に向けて、その要素技術として秘密計算技術の有用性を検証することを目的としています。

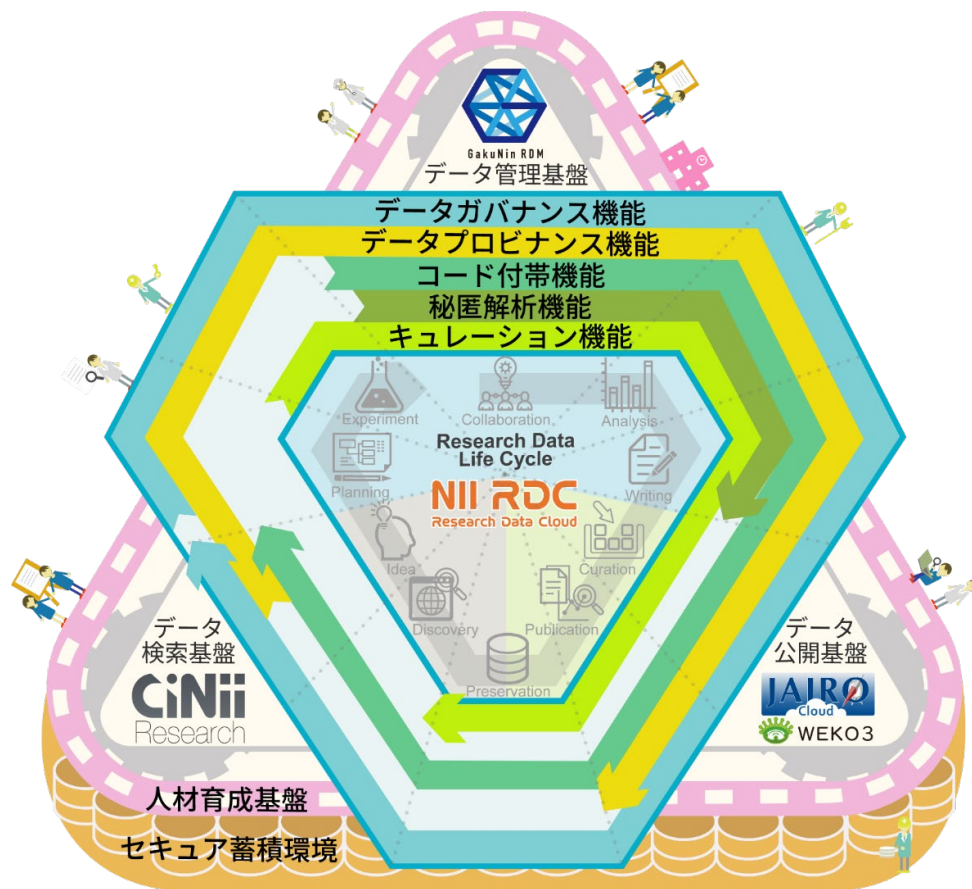


図 3 秘匿解析機能を含む次世代 NII RDC の全体像

5. 今後の取り組み

NII は、本トライアルで得られた研究者からのフィードバックを活かして、研究現場で役立つ秘匿解析機能の開発を目指します。NTT は、本取り組みを通じて安全にデータを共有できる基盤技術を確立し、誰もが安心してデータを利活用できる社会の実現を目指します。これらの取り組みがデータ利活用のハードルを下げ、オープンサイエンスの促進につながることを期待しています。

■ 本件に関する報道機関からのお問い合わせ先
情報・システム研究機構 国立情報学研究所 総務部企画課 広報チーム
media@nii.ac.jp

日本電信電話株式会社
サービスイノベーション総合研究所
企画部広報担当
nttrd-pr@ml.ntt.com