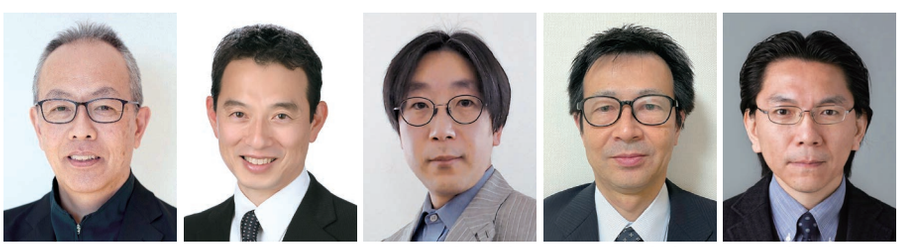
4 秘密計算 AI ソフトウェア

世界初の「AI4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」を試験提供

NTT 社会情報研究所（以下、社会研）は AI4 大カテゴリーの主要なアルゴリズムによる学習・推論を、データが暗号化されたままの状態で実行可能な「秘密計算 AI ソフトウェア」を世界で初めて開発した。国立情報学研究所（以下、NII）と社会研はこのソフトウェア環境を NII の計算機上に構築し、大学や研究機関の研究者に試用してもらうトライアルを 2023 年 1 月末から実施している。



NTT 社会情報研究所　社会情報流通研究プロジェクト
（左から）チーフ・セキュリティ・サイエンティスト／セキュリティマスター　**高橋 克巳**氏
秘密計算技術グループ グループリーダ　**森田 哲之**氏
主任研究員　**諸橋 玄武**氏、研究主任　**太田 賢治**氏
国立情報学研究所 オープンサイエンス基盤研究センター 特任准教授　**下山 武司**氏

長年にわたる秘密計算技術の研究開発実績

さまざまなデータの利活用により成立する「データ駆動型」のビジネスや、大量の学習データによる AI を活用したサービスの普及が進んでいる。学術分野においても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る。しかしプライバシーや機密情報の漏洩、または不正利用の懸念から、組織を横断したデータの利活用はあまり進んでいない。

この問題を解決するものと期待されている技術の 1 つが、データを暗号化したまま一度も元に戻さず演算を行う秘密計算技術だ。社会研には NTT が長年にわたって研究に取り組んできた知見やノウハウがあり、この分野で日本トップの特許出願件数を誇る。秘密計算方式の構成要素の 1 つである秘密分散では NTT の技術が ISO 標準技術に採択されるなど、国際的にも評価されている。

2021 年 8 月には NTT コミュニケーションズ株式会社がその研究成果を活用し、秘密計算技術を利用したデータ集計や回帰分析などさまざまな統計分析が可能なクラウドサービス“析秘（せきひ）”の提供を開始した。

世界で初めて AI4 大カテゴリーの主要アルゴリズムに対応

AI 処理への対応も進めており、2019 年 9 月にはディープラーニングの標準的な学習処理が可能な秘密計算技術を世界で初めて実現したことを発表した。さらに 2023 年 1 月には、AI の 4 大カテゴリーにおける代表的なアルゴリズム（図 1）に対応した秘密計算 AI ソフトウェアを開発したと発表した。こちらも世

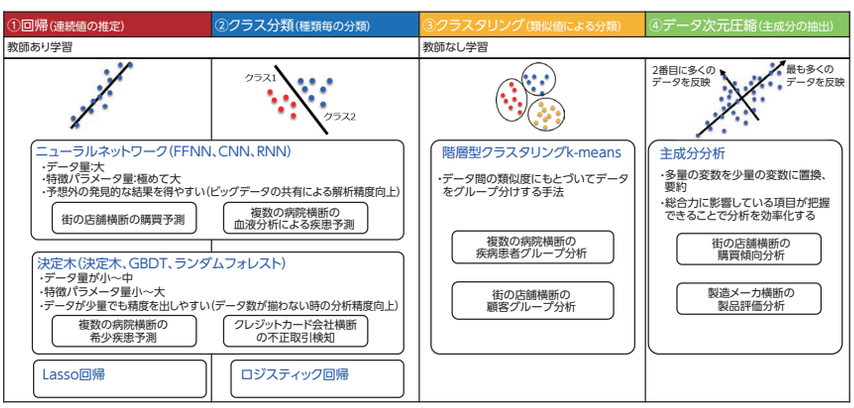


図 1　AI4 大カテゴリーの代表的アルゴリズムに対応

界初となる成果であった。

「幅広い機械学習アルゴリズムに対応しつつ、一度もデータを復号することなく学習と予測が可能です。暗号状態での演算でありながら大規模データによる学習を実用的な時間で処理できるよう工夫した点も大きな特長の 1 つです。」（太田氏）

NII と共同で秘密計算 AI ソフトウェアのトライアルを実施

秘密計算 AI ソフトウェアの発表と合わせ、NII の計算機上に同ソフトウェア環境を構築し、国内の大学・研究機関に所属する教職員・研究者に無償で試用してもらうトライアルの実施を発表した（図 2）。期間は 2024 年 3 月 31 日までを予定している。

「NII の基盤上で多くの研究者に利用してもらうことにより、機能の充足性や演算性能などのフィージビリティを検証することが目的です。我々の思い込みだけで開発することになってしまわないよう、研究者のニーズや反応を確かめたいと考えています。」（森田氏）

オープンサイエンスを促進する NII RDC の機能強化

NII は学術情報ネットワーク“SINET”や学術認証フェデレーションをはじめ、学術研究・教育活動の連携・推進を目的とするシステムを多数構築・運営している。2021 年には研究データ基盤システム“NII Research Data Cloud（以下、NII RDC）”（図 3）の本格稼働を開始した。今回のトライアルは、研究者との対話を通じ次世代の NII RDC 向けに有用な秘匿解析機能を設計すること、また設計・開発・運用を見据えた技術検証を行うことを目的としている。NII の下山氏は次のように述べている。

「2021 年 6 月に政府が発表した“統合イノベーション戦略 2021”においてオープンサイエンス時代の研究データ基盤構築に言及されるなど、オープンサイエンスへの関心が高まっています。その推進には研究において使用・生成された情報の適切な管理が不可欠です。研究者の負担を軽減するため、余計な作業をなくす DX が重要だと考えています。こうした背景も踏まえ、構築・運用しているのが NII RDC です。次期開発では 7 つの機能追加を予定しており、秘匿解析機能もその 1 つです。機微な情報も含む研究データを安全に管理することは容易ではありません。そのための業務に煩わされることなく、研究者が本来の研究活動に安心して集中できる環境作りに貢献したいと考えています。」

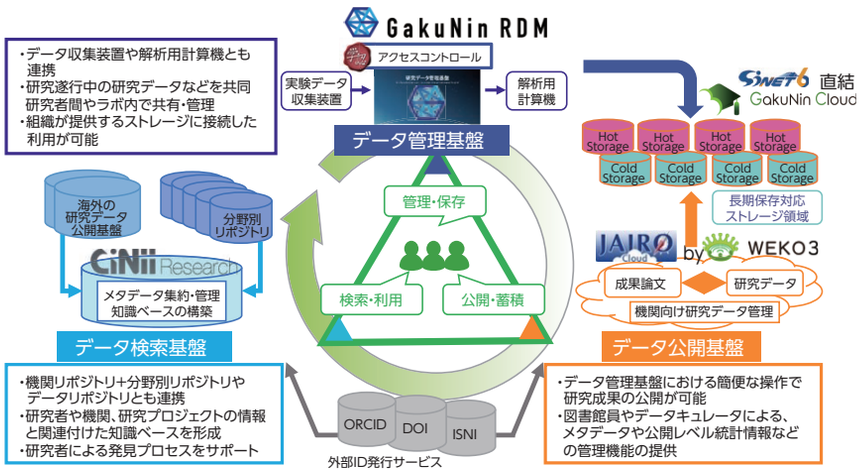


図 3　NII RDC 概要

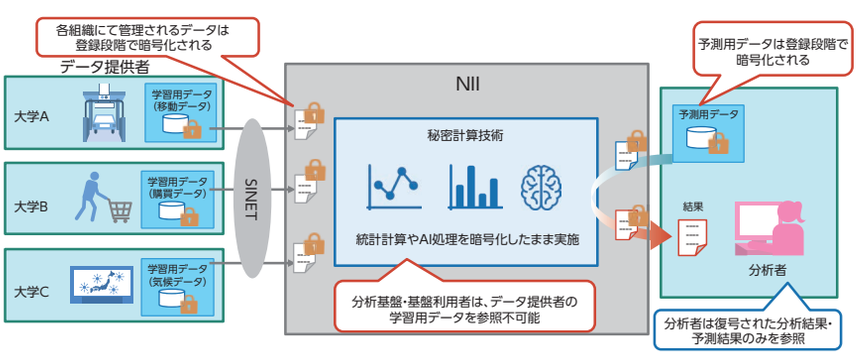


図 2　トライアル概要

さまざまなデータ活用基盤への秘密計算技術の活用を期待

本トライアルへの期待を、森田氏は次のように述べている。

「最新の秘密計算技術の候補の 1 つということで NTT の技術を活用していただいていると認識しています。今回のような実証を経て、秘密計算技術がさまざまなデータ活用基盤の実現につながっていくことを期待しています。」