プレスリリース

2026 年 11 月 25 日

報道関係者各位

国立大学法人　奈良先端科学技術大学院大学
株式会社 ZenmuTech

「話しかけるだけ」で専門知識がなくても秘密計算を使える研究データ基盤を開発

～奈良先端大 ARWIT のセキュアデータ流通プラットフォームに生成 AI を連携、機密データを守ったままベイズ最適化～

【概要】

奈良先端科学技術大学院大学（奈良県生駒市、学長：塩﨑 一裕、以下「奈良先端大」）先端科学技術研究科 情報科学領域の林 優一 教授、藤本 大介 准教授らの研究グループと株式会社 ZenmuTech（東京都中央区、代表取締役社長 CEO：阿部 泰久、以下「ZenmuTech」）は、データを秘匿したまま検索・計算できる秘密計算（注 1）の基盤に生成 AI（注 2）を連携させ、暗号やプログラミングの専門知識がない研究者でも、日常の言葉で指示するだけで機密データの登録から解析・ベイズ最適化までを行える仕組みを開発しました。

本技術は、奈良先端大が文部科学省「地域中核・特色ある研究大学強化促進事業（J-PEAKS）」のもとで構築を進める自律的研究強化・社会実装システム「ARWIT（アーウィット）」（注 3）のうち、ARWIT 推進センター セキュアデータ流通部門が整備する「セキュアデータ流通プラットフォーム」の中核機能として導入するものです。同プラットフォームは、ZenmuTech の秘密計算ソリューション「QueryAhead®」を基盤として採用し、データを意味のない断片に分割する秘密分散（注 4）によって複数のサーバーに分散保管したまま、検索やベイズ最適化（注 5）などの計算を実行できます。

今回、AI エージェント（注 6）がデータ登録、解析モデルの作成、ベイズ最適化の実行といった一連の操作を対話形式で案内・代行する機能を新たに開発しました。これまで Python によるプログラムの作成と、秘密分散やベイズ最適化についての専門的な理解が必要だった処理を、プログラムを書くことなく実行できます。暗号技術の安全性を保ったまま使いやすさを大きく高めることで、高度な暗号技術を社会に広く普及させるうえで欠けていた「誰でも使える入口」を実現する成果です。

【背景】

材料・化学やバイオの研究開発では、AI による予測やベイズ最適化の精度を高めるために、組織の

枠を越えてデータを持ち寄ることが期待されています。一方で、実験データや配合条件は各組織の競争力の源泉であり、秘密保持契約を結んでも開示できない情報が残ります。さらに近年は、サイバー攻撃などによる情報漏えい事案が相次いでおり、データを預ける側にとって、預け先のサーバーや管理者を信頼しなければならない仕組みそのものがリスクとなっています。

秘密計算は、データを秘匿したまま計算できるため、こうした課題を解決する技術として注目されています。しかし、秘密計算を実際の研究に使うには、暗号技術の仕組みを理解したうえで、専用のプログラムを書いて操作する必要がありました。このため、利用できるのは暗号や情報処理に詳しい一部の専門家に限られ、本来最もデータ活用の恩恵を受けるはずの分野外の研究者が使いにくいことが、社会実装の大きな壁となっていました（図 1）。

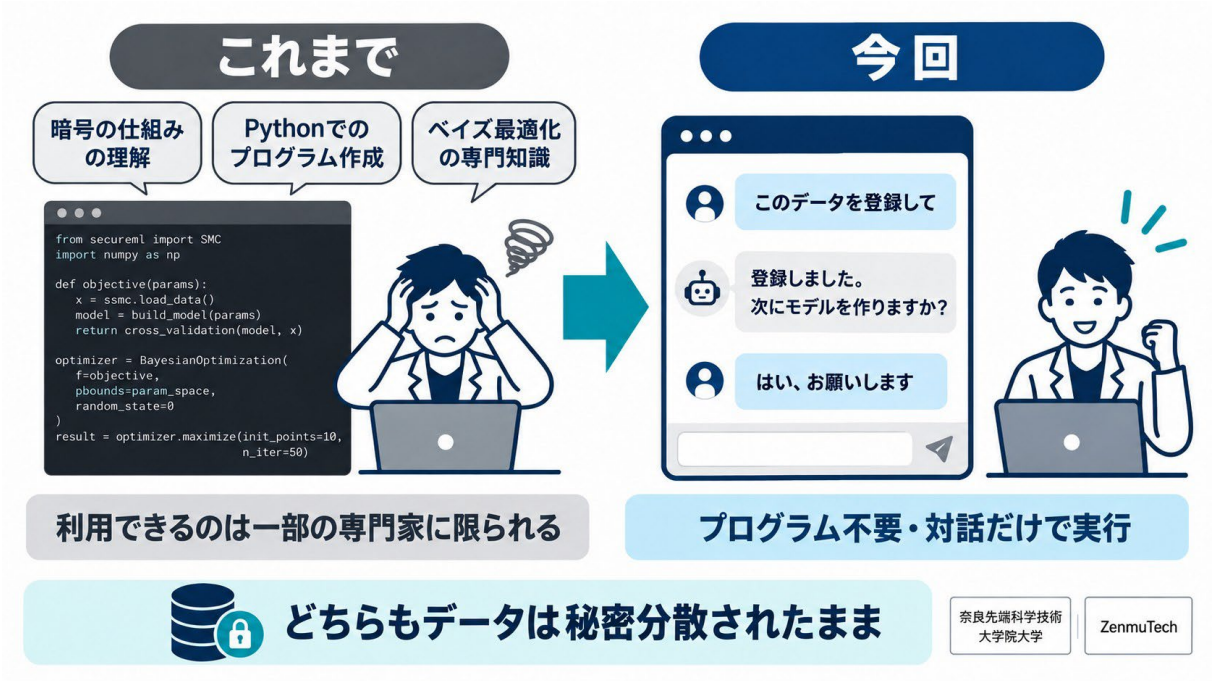


図 1　専門的なプログラム操作から、対話による操作へ

【これまでの取り組み】

奈良先端大は、ARWIT のもとで、自動実験装置により実験とデータ取得を行う「ファウンドリ」と、データを安全に集約・活用する「セキュアデータ流通プラットフォーム」を両輪とする研究基盤の整備を進めています。セキュアデータ流通プラットフォームでは、ZenmuTech の QueryAhead®を採用し、さらに、データの内容だけでなく、利用者が何を調べようとしているのかという検索条件（クエリ）そのものも秘匿する機能や、機密データを開示することなく次に試すべき実験条件を探索するベイズ最適化機能を共同で開発してきました。これらは、機密性の高い研究データの安全な活用と、データに基づく効率的な実験探索を両立するものであり、研究開発の高度化に向けた重要な成果です（図 2）。

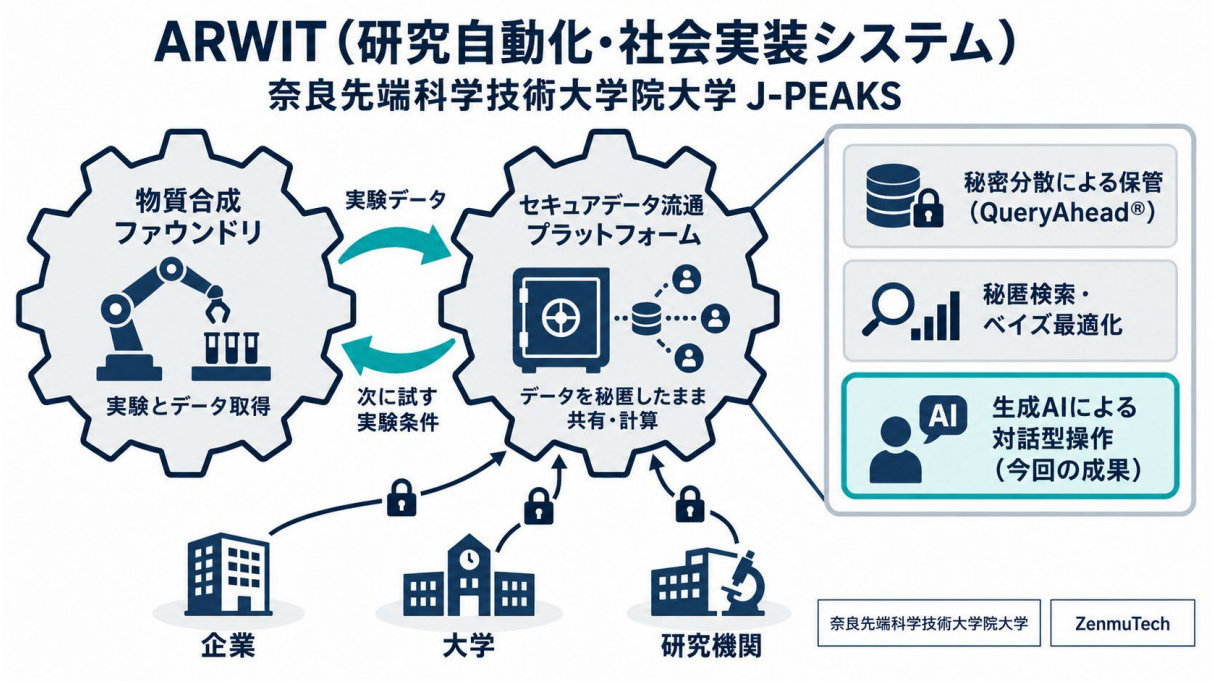


図 2　ARWIT におけるセキュアデータ流通プラットフォームの位置づけ

【今回の成果】

今回開発した機能では、利用者が AI エージェントに日常の言葉で話しかけると、AI エージェントが必要な手順を案内し、利用者の確認を得ながら秘密計算基盤への操作を実行します。例えば、手元の実験データ（CSV ファイル）を示して「このデータを登録したい」と伝えると、AI エージェントが登録名を提案し、了承を得たうえでデータを秘密分散して登録します。続いて、モデルの作成、説明変数と目的変数の選択、モデルの更新、次の実験候補の探索までを、対話を通じて進めることができます。処理の状況はウェブ上の管理画面（ダッシュボード）にも反映され、実行中の計算や作成したモデルを一覧で確認できます（図 3）。

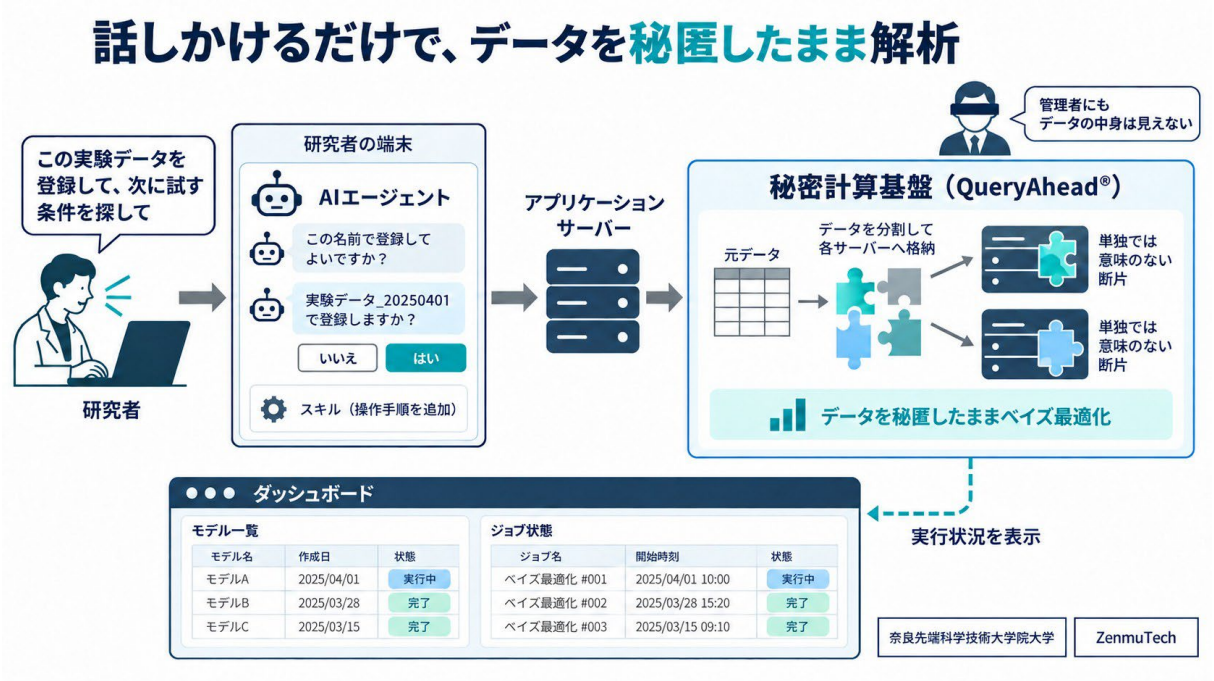


図３　話しかけるだけで、データを秘匿したまま解析

主な特長は次のとおりです。

- **専門知識・プログラミングが不要**：従来は Python のプログラムで行っていたデータ登録からベイズ最適化までを、対話だけで実行できます。
- **データは秘匿されたまま**：AI エージェントは利用者の操作を代行するだけで、データは秘密分散された状態でサーバーに保管・計算されます。個々の分散片だけでは、元データの内容を読み取れない仕組みです。
- **確認しながら進む安全な操作**：データの登録や計算の実行など重要な操作の前には、AI エージェントが内容を提示して利用者の確認を求めます。
- **導入が容易**：AI エージェントに機能を追加する「スキル」と呼ばれる仕組みで実装しているため、利用者の端末にファイルを配置するだけで導入できます。

【今後の展開】

奈良先端大は今後、ARWIT 推進センターにおいて本機能を紹介するとともに、学内外の研究者による試行利用を進めます。今後は、入力内容の妥当性を自動で確認する機能の強化や、物質合成ファウンドリとの連携を進め、企業や研究機関が機密データを開示することなく持ち寄り、AI を活用して研究開発を加速できる環境の実現を目指します。

ZenmuTech は、本取り組みで得られた知見を QueryAhead®の機能拡充に生かし、秘密計算の幅広い分野での社会実装を推進します。

【コメント】

奈良先端科学技術大学院大学 先端科学技術研究科 教授／ARWIT 推進センター セキュアデータ流通部門長　林 優一

「秘密分散のような高度な暗号技術は強力ですが、その仕組みを理解して使いこなせる人はごく一部です。今回、生成 AI を入口に据えることで、暗号の専門家でなくても安全にデータを活用できる

ようになりました。最先端の暗号技術を社会に広く届けるために必要なピースの一つを埋められたと考えています。ARWIT を通じて、データを守りながら分野や組織を越えて共創できる研究環境を広げていきます。」

株式会社 ZenmuTech　代表取締役社長 CEO　阿部 泰久

「AI の急速な進展により、機密性の高いデータを安全に保護しながら、その価値を最大限に活用できる秘密計算技術の重要性は、今後ますます高まっていくと考えています。

今回奈良先端大との協働によって、これまで専門知識が必要だった秘密計算を生成 AI との連携により、誰もが利用しやすい技術へと進化させることができたことを、大変嬉しく思います。

この取り組みが秘密計算の普及に向けた大きな一歩となることを期待するとともに、今後も産学連携による技術革新と社会実装を推進し、『データはもっと自由になれる』社会の実現に貢献してまいります。」

【謝辞】

本研究は、JSPS 地域中核・特色ある研究大学強化促進事業 JPJS00420240021 の支援を受けたものです。

【J-PEAKS 事業】

本研究成果は、文部科学省「地域中核・特色ある研究大学強化促進事業（J-PEAKS）」の一環として創出されました。J-PEAKS は、日本全体の研究力の発展を牽引する研究大学群の形成を目的とした事業です。令和 6 年度に採択された本学の J-PEAKS 事業では、「研究シーズの社会実装をデジタル技術で推進し、国際連携の下で人口減少社会の持続的発展に貢献する大学」をビジョンとして掲げています。本研究成果は、J-PEAKS のもとで構築を進める ARWIT の中核機能として、機密性の高い研究データを守ったまま、専門知識のない研究者でも組織や分野を越えて活用できるようにするものです。データ駆動型の研究開発と研究シーズの社会実装をデジタル技術で加速するものであり、本学のビジョンの実現に直結する成果です。

【用語解説】

注 1 秘密計算：データを秘匿したまま検索や計算を行い、結果だけを得る技術。計算を行うサーバー側でもデータの中身を知ることができない。

注 2 生成 AI：大量のデータから学習し、文章などを生成する AI。本機能では利用者の指示を理解し、操作を代行するために用いる。

注 3 ARWIT（アーウィット）：奈良先端大が J-PEAKS のもとで構築を進める「自律的研究強化・社会実装システム」。研究開発の自動化を表す Automated Research Workflow と、社会実装を表す Industrial Translation を組み合わせた名称。研究の自動化・自律化と、データの安全な共有・利活用を組み合わせ、研究成果の社会実装を推進する。

注 4 秘密分散：データを複数の分散片に分け、別々に保管する技術。所定の条件を満たす分散片を組み合わせることで元データを復元できる一方、個々の分散片だけでは元データの内容を読み取れない。

注 5 ベイズ最適化：これまでの実験結果から、次に試すべき条件を効率よく選ぶ手法。少ない実験回

数で良い条件を見つけられるため、材料開発などで用いられる。

注 6 AI エージェント：利用者の指示に基づき、必要な手順を判断してソフトウェアの操作などを自律的に実行する AI。

【ZenmuTech について】

株式会社 ZenmuTech は、秘密分散技術を用いたデータ保護ソリューションを開発・提供しています。主な製品に、秘密分散技術のソフトウェア開発キット「ZENMU Engine」、PC からの情報漏えい対策製品「ZENMU Virtual Drive」があります。また、産業技術総合研究所との協働による研究を基礎として、データを秘匿したまま計算できる秘密計算データベースプラットフォーム「QueryAhead®」を提供し、秘密計算技術の社会実装に取り組んでいます。

URL：https://zenmutech.com/

【お問い合わせ先】

＜研究に関すること＞
奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域
教授　林 優一／准教授　藤本 大介
E-mail：yu-ichi@is.naist.jp／fujimoto@is.naist.jp

＜報道に関すること＞
奈良先端科学技術大学院大学 企画総務課 渉外企画係
TEL：0743-72-5063/5112　FAX：0743-72-5011　E-mail：s-kikaku@ad.naist.jp

株式会社 ZenmuTech
広報担当： 松倉
E-mail：press@zenmutech.com