

仕 様 書

1. 件名

秘匿計算プラットフォームの構築

2. 研究の概要

国立研究開発法人産業技術総合研究所化学プロセス研究部門(以下、「産総研」という。)では、2025 年度国立研究開発法人 新エネルギー・産業技術総合開発機構 (NEDO) 先導研究プログラム「エネルギー・環境新技術先導研究プログラム／次世代高速通信を実現する革新材料開発」を受託し、研究を推進している。

特にテーマ A では、複数企業(以下、「各企業」という。)間でのデータ連結を可能とする秘匿計算プラットフォームを構築し、実験の加速を図っている。本先導研究では、将来の国家プロジェクト等における秘匿計算プラットフォームの本格構築に先立ち、各種課題を洗い出すとともに、その実行可能性を検証し、実証的に評価する。

3. 作業の概要

各企業から供与された解析用サンプルデータを用いて、デバイス向け材料開発における有望な実験候補点を導出する。導出に際しては、有機・無機を問わず各企業が取り扱う多様な材料を検討対象とするための方法論を構築し、統合データを基盤として、秘匿計算やアルゴリズムを含む機械学習モデルを活用した解析を行う。また、並行して秘匿 MI-PF の目的・用途を含む広範な枠組みについて協議・定義を進め、今後の実装に向けた準備を整える。

4. 作業の構成

4-1: 供与データの前処理

- ・各企業から供与されたデータ(以下、「供与データ」という。)を対象に前処理を実施する。

4-2: 異種材料を扱う方法論の検討

- ・有機・無機を含む多様な材料を扱うための方法論について検討・協議・決定する。

4-3: 共通尺度・パラメータ設定

- ・解析に用いる共通の尺度や取り扱うパラメータを定義する。

4-4: データ接続

- ・MI 技術を用いて潜在空間上でデータを接続する。

4-5: データ統合

- ・データ統合の方法を決定し、供与データに基づき秘匿計算を実施する。

4-6: 機械学習モデルの構築

- ・ 供与データを基に機械学習モデルを構築する。

4-7: 実験推奨点の導出

- ・ 各企業が設定した探索範囲に基づき、構築した機械学習モデルと材料開発特化アルゴリズムを用いて実験推奨点を導出する。特に、既存のベイズ最適化に加え、潜在空間構造を活用して材料群間の関係性を捉える独自手法を検討することで、標準的手法よりも少ない実験回数で高性能領域に到達することを目指す。

4-8: モデル更新

- ・ 追加の実験データが供与された場合、必要に応じてモデルを更新する。

4-9: 秘匿 MI-PF の要件定義

- ・ プラットフォームの目的・用途・形式・対象素材・使用者を定義するとともに、実行する解析やモデルの種類、入出力データの種類・形式を整理する。

5. 構成別仕様詳細

5-1: 供与データの前処理

- ・ 供与データを対象に前処理を実施すること。
- ・ 前処理に供するデータセット数は、最大 30 点とする。
- ・ データの入力は、クラウド形式で各自登録するか、産総研が共同研究先からデータを預かり入力するかいずれの方式を採用すること。

5-2: 異種材料を扱う方法論の検討

- ・ 有機・無機を含む多様な材料を扱うための方法論について検討・協議・決定すること。
- ・ 受注者は、最大 2 回、方法論についての議論に応じること。打ち合わせは最大 2 時間/1 回とする。

5-3: 共通尺度・パラメータ設定

- ・ 解析に用いる共通の尺度や取り扱うパラメータを定義すること。
- ・ パラメータの決定については、調達請求者と相談の上決定すること。

5-4: データ接続

- ・ MI 技術を用いて潜在空間上でデータを接続すること。
- ・ データの接続は受注者が実施すること。

5-5: データ統合

- ・ データ統合の方法を調達請求者と協議の上決定し、供与データに基づき秘匿計算を実施すること。

5-6: 機械学習モデルの構築

- ・ 供与データを基に機械学習モデルを構築すること。

- ・ ガウス過程回帰およびベイズ最適化に立脚して機械学習モデルを構築すること。

5-7: 実験推奨点の導出

- ・ 各企業が設定した探索範囲に基づき、構築した機械学習モデルと材料開発特化アルゴリズムを用いて実験推奨点を導出すること。特に、既存のベイズ最適化に加え、潜在空間構造を活用して材料群間の関係性を捉える独自手法を検討することで、標準的手法よりも少ない実験回数で高性能領域に到達することを目指すこと。
- ・ 実験推奨点の導出については、産総研および共同研究先企業それぞれに対して、実施すること。ただし、関係者を集めて同時に開催しても可とする。

5-8: モデル更新

- ・ 追加の実験データが供与された場合、必要に応じてモデルを更新すること。
- ・ モデルの更新は最小1回、最大2回実施する。

5-9: 秘匿 MI-PF の要件定義

- ・ プラットフォームの目的・用途・形式・対象素材・使用者を定義するとともに、実行する解析やモデルの種類、入出力データの種類・形式を整理すること。
- ・ 要件定義の議論について、受注者は、最大2回、方法論についての議論に応じること。打ち合わせは最大2時間/1回とする。ただし、5-2.に記載の会議と同時に実施することも可とする。

6. 受注者に求める要件等

- ・ 受注者は情報漏洩に細心の注意をはらいデータの管理を実施すること。
- ・ 本業務全般を管理する責任者を1名以上置くこと。
- ・ 外部事業者のデータに対する MI の解析について十分な実績がある担当者を1名以上選定し、調達請求者の了承を得たうえで手配すること。

7. 貸与品

- ・ 供与データおよびこれまでの研究データ 一式(電子媒体)

8. 納入物品

- ・ 解析プロセスなどを含む報告書 1部
- ・ 供与データを元に、機械学習モデルを用いて導出した実験候補点 一式
- ・ 秘匿 MI-PF の要件定義に必要な各種情報 一式

※いずれも紙媒体または電子媒体にて納入すること。

※電子媒体で納入する際は原則として外部電磁的記録媒体（USB メモリ、外付 HDD、DVD-R 等）を用いないこと。

9. 納入期限および納入場所

納入期限：2026 年 2 月 27 日(金)

納入場所：茨城県つくば市東 1-1-1

10. 納入の完了

本作業は、「8. 納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。受注者は確認にかかる作業を支援すること。

11. 付帯事項

- ・ 本仕様書の技術的内容及び知り得た情報については、守秘義務を負うものとする。
- ・ 本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。また、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。
- ・ 本業務に起因する不具合等に関しては、原因究明に関し、納入の完了後 1 年間は無償で対応を行うこと。
- ・ 請負者の責において及ぼした損害は、請負者が賠償すること。
- ・ サプライチェーン・リスクに対応するため、別紙に記載する事項に従って契約を履行しなければならない。

12. セキュリティ要件

12.1. 情報セキュリティポリシーに関する要件

- ① 本業務の遂行に当たっては、産総研の情報セキュリティポリシーを遵守するとともに、情報セキュリティポリシーにおいて産総研に求められる水準の情報セキュリティ対策を講じること。産総研の情報セキュリティ規程については、下記URLを参照のこと。その他の情報セキュリティポリシーの詳細については受注者決定後に提示する。

【国立研究開発法人産業技術総合研究所情報セキュリティ規程】

https://www.aist.go.jp/Portals/0/resource_images/aist_j/outline/comp-legal/pdf/securitykitei.pdf

- ② 産総研の情報セキュリティポリシーの見直しが行われた場合は、見直しの内容に応じた情報セキュリティ対策を講じること。なお、対応内容については調達請求者に事前に報告し承認を得ること。

12.2. その他セキュリティに関する要件

- ① 受注者は、本業務の履行に際して、秘密である旨を示されて貸与を受けた秘密情報を秘密として適切に保持することとし、第三者に開示又は漏洩してはならない。
- ② 受注者は、本業務の履行によって知った一切の情報を本業務の履行以外 の目的に利用してはならない。契約終了後も同様とする。

- ③ 貸与品は調達請求者の了解なしに所外に持ち出したりは複製してはならない。
- ④ 産総研の所外へ持ち出したりは複製した貸与品については一覧表を作成し、調達請求者に提出すること。なお、契約終了後、速やかに返却又は廃棄し、調達請求者の確認を得たうえで一覧表からの削除を行うこと。
- ⑤ 受注者は、契約締結後、情報セキュリティ管理体制を記載したドキュメントを調達請求者に提出すること。
- ⑥ 受注者は、本業務において、受注者の従業員若しくはその他の者によって、意図せざる変更が加えられない管理体制とすること。
- ⑦ 受注者は、産総研の求めに応じて、資本関係、役員等の情報、委託事業の実施場所並びに委託事業従事者の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍に関する情報提供を行うこと。
- ⑧ 本業務にかかる情報に関する情報セキュリティインシデントが生じた場合、速やかに報告の上、原因の分析を実施し、調達請求者と対処内容及び再発防止策を検討すること。当該インシデントへの対処を実施するにあたっては、事前に調達請求者の確認を得ること。
- ⑨ 情報セキュリティインシデントが生じたことで、受注者の作業環境等の確認が必要となった場合には、産総研の調査に協力を行うこと。
- ⑩ 産総研で情報セキュリティインシデントが発生した場合、速やかに調査及び復旧に協力を行うこと。
- ⑪ 調達請求者より、情報セキュリティ対策の履行が不十分であると指摘された場合は、速やかに是正処置を講ずること。
- ⑫ 本業務の遂行における情報セキュリティ対策の履行状況を確認するために、産総研が情報セキュリティ監査の実施を必要と判断した場合、受注者は、産総研が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報セキュリティ監査を受け入れること。
- ⑬ 受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、受注者に求めている情報セキュリティ対策を、再委託先が実施することを再委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を産総研に提供し、承認申請書を提出して、事前に産総研の書面による承認を受けた場合はこの限りではない。
- ⑭ 本業務の履行においては、十分な秘密保持を行うこと。
- ⑮ セキュリティに十分配慮した設計を行い、利用権限のない者が不正にアクセスし、データを閲覧・更新等できない設定、構築を行うこと。
- ⑯ 本業務の履行において、セキュリティの脆弱性が発見された場合には、対応内容について調達請求者と協議し、必要に応じて速やかに対応すること。
- ⑰ 本業務の履行において、該当する場合は、以下を含むアプリケーションの脆弱性

を回避すること。

- ・ SQL インジェクション
- ・ OS コマンドインジェクション
- ・ ディレクトリトラバーサル
- ・ セッション管理の脆弱性
- ・ アクセス制御欠如と認可処理欠如の脆弱性
- ・ クロスサイトスクリプティング
- ・ クロスサイトリクエストフォージェリ
- ・ クリックジャッキング
- ・ メールヘッダインジェクション
- ・ HTTP ヘッダインジェクション
- ・ eval インジェクション
- ・ レースコンディション
- ・ バッファオーバーフロー及び整数オーバーフロー

⑮ 本業務の履行において、管理する情報システムのログを点検又は分析を実施した結果、ログの異常を検知した場合には、調達請求者に報告すること。

⑯ 本業務の履行において、管理する情報システムの不正プログラム対策を実施した結果、定義ファイルの更新失敗、またはマルウェア等を検知した場合には、調達請求者に通知すること。

受注者は、本業務の履行において、第三者のクラウドサービスを利用する場合、原則として、政府情報システムのためのセキュリティ評価制度（ISMAP）クラウドサービスリストに登録されているクラウドサービスを利用すること。ただし、登録されているクラウドサービスに利用可能なものが無い場合には、以下いずれかのクラウドセキュリティ認証を取得、または監査フレームワークに対応していること。

【クラウドセキュリティ認証】

ISO/IEC27017（JIS Q 27017）

JASA クラウドセキュリティ推進協議会 CS ゴールド マーク

米国 FedRAMP Moderate または High

【監査フレームワーク】

AICPA SOC2またはSOC3

また、利用するクラウドサービスの選定にあたっては、国内にデータセンターを持ち、日本法に準拠しているクラウドサービスを選定すること

⑰ 受注者は、本業務の履行において、第三者のクラウドサービスを除く外部サービスを利用する場合、産総研が受注者に求めている情報セキュリティ対策と同等の対策の実施を、当該外部サービス事業者に課すこと。

⑱ サプライチェーン・リスクに係る情報セキュリティ上の事象が発生した場合、受注

者は原因調査などについて調達請求者と協議の上、主導的に解決を図ること。

- ②②受注者は、受注先及び再委託先において作成した委託事業に係る成果物（システム構成・設定情報、等を含む。産総研に帰属しない著作物を除く。）の納入の完了後速やかに、当該成果物を調達請求者の許可を得て、抹消すること。また、受注者は、調達請求者の指示に従い、当該成果物の抹消の確認を受けること。

サプライチェーン・リスク対応に係る特記事項

1. サプライチェーン・リスクへの対応

受注者は、機器等の意図的な不正改造及び情報システム又はソフトウェアに不正なプログラムを埋め込むなど、国立研究開発法人産業技術総合研究所（以下、「産総研」という。）の意図しない変更が加えられたときに生じ得る情報の漏えい若しくは破壊又は機能の不正な停止、暴走その他の障害等の情報セキュリティ上のリスク（以下「サプライチェーン・リスク」という。）に対応するため、受注者は「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30年12月10日関係省庁申合せ）に基づく対応を図らねばならない。

2. 意図しない変更に対する対策

①受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得べきソースコード、プログラム等（以下「ソースコード等」という。）の埋込み又は組込みその他調達請求者の意図しない変更を行ってはならない。

②受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得べきソースコード等の埋込み又は組込みその他調達請求者の意図しない変更が行われないように相応の注意をもって管理しなければならない。

③受注者は、本業務の履行に際して、情報の窃取等により研究所の業務を妨害しようとする第三者から不当な影響を受けるおそれのある者が開発、設計又は製作したソースコード等（受注者がその存在を認知し、かつ、サプライチェーン・リスクが潜在すると知り、又は知り得べきものに限り、主要国において広く普遍的に受け入れられているものを除く。）を直接又は間接に導入し、又は組み込む場合には、これによってサプライチェーン・リスクを有意に増大しないことを調査、試験その他の任意の方法により確認又は判定するものとする。

3. サプライチェーン・リスクにかかる調査の受入れ体制

①受注者は、本業務に調達請求者の意図しない変更が行われるなど不正が見つかったときは、追跡調査や立入検査等、産総研と連携して原因を調査し、サプライチェーン・リスクを排除するための手順及び体制を整備し、当該手順及び体制を示した書面を調達請求者に提出しなければならない。

4. サプライチェーン・リスクを低減するための対策

①受注者は、サプライチェーン・リスクを低減する対策として、本業務の設計、構築、運用・保守の各工程における不正行為の有無について定期的または必要に応じて監査を行う体制を整備するとともに、本業務により産総研に納入する納入物品に対して意図しない変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、受注者において適切に設定するものとする。

②機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、4.

①の対応は不要。

5. 受注者の業務責任者等

①受注者は、本業務の履行に従事する業務責任者及び業務従事者（契約社員、派遣社員等の雇用形態を問わず、本業務の履行に従事する全ての従業員をいう。以下同じ。）を必要最低限の範囲に限るものとする。

②機器納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、5. ①の対応は不要。

6. 再委託

6.1 本業務の第三者への委託の制限

受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、6.2に定める事項を遵守する場合はこの限りではない。

6.2 第三者への委託に係る要件

①受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について記載した承認申請書を、委託元である産総研に提出し、書面による事前承認を受けなければならない。

②受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託した業務に伴う再委託者の行為について、全ての責任を負わなければならない。

③受注者は、知的財産権、情報セキュリティ（機密保持を含む。）及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施し、その内容について委託元である産総研の承認を得なければならない。

④受注者は、受注者がこの仕様書の定めを遵守するために必要な事項について本仕様書を準用して、再委託者と約定しなければならない。

⑤受注者は、前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍についての情報を委託元である産総研へ提出すること。

⑥受注者は、再委託先において、産総研の意図しない変更が加えられないための管理体制について委託元である産総研に報告し、許可又は確認（立入調査）を得ること。

7. その他

①提出された資料等により調達請求者に報告された内容について、サプライチェーン・リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、調達担当者は受注者に是正を求めることがあり、受注者は相当の理由があると認められるときを除きこれに応じなければならない。

②産総研は、受注者の責めに帰すべき事由により、本情報システムに調達請求者の意図しない変更が行われるなど不正が見つかった場合は、契約条項に定める契約の解除及び違約金の規定を適用し、本業務契約の全部又は一部を解除することができる。