仕　様　書

１．件名

事前知識を活用した科学情報のための AI モデルのセーフティ管理技術の研究開発支援

２．研究の概要・目的

2-1.概要・目的

国立研究開発法人産業技術総合研究所人工知能研究センター（以下「産総研」という）では、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）「ＡＩの安全性確保に関する研究開発・検証等の推進事業／ＡＩセーフティ強化に関する研究開発」を行う。

本作業では、事前知識の活用によるAIモデルのセーフティ管理技術を開発する目的で、科学における法則や知識などを組み入れたAI基盤モデルの開発に向け、「有害」データの収集、整備を行う。これにより、AIモデルによって予測された結果や生成されたデータが、法則や知識と整合性がないリスクや、有害物を生成するリスクの低減を目指す。

2-2.用語の定義

本仕様書で使用される用語とその意味について、以下に記す。

用語	説明
産総研担当者	本作業の企画及び運用等を担当する者及び所管部署の業務運用担当者。
受注者	本調達の対象となる業務に従事する事業者。

３．作業の概要

本件は、NEDO プロジェクト「ＡＩの安全性確保に関する研究開発・検証等の推進事業／ＡＩセーフティ強化に関する研究開発」において、産総研が担う研究課題「事前知識を活用した科学情報のための AI モデルのセーフティ管理技術の研究開発」に基づき、科学データに関する「有害」データの収集、整備を行うものである。

４．研究開発の背景

AI 製品・サービスのリスクを評価・管理するための基盤技術は、世界的にも研究開発途上にある。また、大規模言語モデル（Large Language Model: LLM）やマルチモーダル AI を含む生成 AI のセーフティ基準は策定されておら

ず、各国ではAIセーフティ・ インスティテュート(Artificial Intelligence Safety Institute: AISI)を立ち上げ、AIセーフティの確保に関する制度設計を急速に推進している。

こうした背景を踏まえ、基盤モデルに対するセーフティ管理技術の確立を目指し、研究開発を実施する。具体的には、科学的な法則や事前知識を取り込んだAI基盤モデルを構築し、それによりAIモデルが生成・予測した結果が、科学的知見と整合性を持たない場合のリスクや、有害物を生成するリスクの低減を図るため、有害物についての事前知識データを収集、整理する。

５．作業項目

5-1.既存データベース・論文からの有害データの収集
5-2.収集データからの学習用データベース構築
5-3.有害データを利用した生成抑制のプロトタイプモデルの構築

６．作業項目別仕様

6-1. 既存データベース・論文からの有害データの収集

事前知識を活用したAI モデルのセーフティ管理技術の開発に向け、広義の有機化学分野における分子に特化したデータを、公開されている化学分子データベースや、ウイルスに関するデータベース、文献データベースなどから幅広く収集すること。具体的には、分子の構造、物性、科学文献、大規模言語モデルによる情報などを対象とする。以下の方法により、有害性に関するラベル付きデータの収集を行うこと。

【6-1-1】既存データベースからの収集

・収集対象とする既存データベースの仕様調査
・収集対象とする既存データベースからの有害ラベル付きデータの収集

【6-1-2】論文からの収集

・有害ラベルのデータを含む論文の収集
・収集した論文からRetrieval-Augmented Generation（RAG）を利用した有害ラベル付きのデータの収集

6-2. 収集データからの学習用データベース構築

6-1で収集したデータを用いて、科学的な法則や事前知識を取り込んだAI基盤モデルの開発に向けた学習用データベース（以下、「データベース本体」という）を構築すること。

【6-2-1】6-1 で収集したデータの分類、正規化

6-3. 有害データを利用した生成抑制のプロトタイプモデルの構築

6-2 で構築した学習用データベースをもとに、AI による有害物の生成抑制機能を備えたプロトタイプモデルを構築すること。毒物や病原性の高いウイルス由来タンパク質などの生成リスクを評価し、安全性を検証する。

【6-3-1】 6-2 によって構築した学習用データベースを利用し、有害物の生成を抑制するモデルの構築

【6-3-2】構築したプロトタイプモデルの評価

７．受注者の条件等

7-1. 受注者の能力、要件等

① バイオインフォマティクス、機械学習、タンパク質言語モデルの知識を有し、プログラム開発とデータベース構築の実績が５件以上あること。

② ウェブで公開されている機械学習のソースコードをダウンロードし、GPU などのハードウェア環境も適切に組み合わせた上で、動作可能にできること。

③ 英語の論文を読解でき、かつ日本語での円滑なコミュニケーションができること。

④ データベース作成の進捗について、作成したプログラムと共に詳細を報告すること。

８．貸与するデータ及び容量等

特になし

９．完成品の試験・確認

データベース本体とプロトタイプモデルの完成度と品質は、進捗報告を通して産総研側が試験および確認する。受注者は、その確認作業において産総研担当者を支援し、その結果を報告書として提出すること。

１０．納入の完了

本件は、「１１．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。

１１．納入物品

産総研担当者の指示する方法にて以下を納入すること。

(1)データベース本体（ファイルを産総研が提供する box 環境に保存）

(2)報告書及び環境構築手順書（電子媒体）

各課題項目に該当する報告書・手順書を作成し、納入すること。

・開発「既存データベース・論文からの有害データの収集」
検証のための環境構築手順書、動作確認手順書

・開発「収集データからの学習データベース構築」
検証のための環境構築手順書、動作確認手順書、及び構築したデータベースの仕様書

・開発「有害データを利用した生成抑制のプロトタイプモデルの構築」
検証のための環境構築手順書、動作確認手順書、及び検証結果の報告書

※電子媒体の場合、原則として USB メモリ等の外部電磁的記録媒体は用いないこと。

１２．納入期限及び納入場所

納入期限： 2026 年 1 月 30 日

納入場所：東京都江東区青海 2-4-7
国立研究開発法人産業技術総合研究所人工知能研究センター
臨海副都心研究センター別館 8 階 08202 室

１３．成果の取扱い

(1)産総研は、受注者がプログラム作成により得られた技術上の成果のうち産総研が指示するもの（以下「成果」という。）についての利用及び処分に関する権利を専有するものとする。

(2)受注者は、成果に係るソフトウェアの著作権（著作権法第 27 条及び第 28 条に規定する権利を含む。）及び意匠登録を受ける権利を産総研に譲渡するものとし、著作者人格権を行使しないものとする。ただし、パッケージ製品に係るものは除く。

(3)受注者は、産総研に対し、納品した成果品が第三者の知的財産権を侵害しないことを保証するものとする。なお、納品した成果品について、第三者の権利侵害の問題が生じ、その結果、産総研又は第三者に費用や損害が生じた場合は、受注者は、その責任と負担においてこれを処理する

ものとする。

１４．セキュリティ要件

14.1.情報セキュリティポリシーに関する要件

① 本業務の履行に当たっては、産総研の情報セキュリティポリシー(別途定める読み替え条項に従うものとする。以下同じ。)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。なお、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産総研担当者に事前に報告し承認を得ること。

14.2.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提供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 提供する資料は産総研担当者の了解なしに所外に持ち出してはならない。
④ 産総研の所外へ持ち出した資料については一覧を作成し、産総研担当者に提出すること。なお、契約終了後、速やかに返却または廃棄し、産総研担当者に報告すること。
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産総研担当者に提出すること。
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、産総研担当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、事前に産総研担当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 本業務の履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、産総研が提示するチェックリストの内容に基づき、定期的に情報セキュリティ対策の履行状況を報告すること。

⑪ 産総研担当者より、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 本業務の履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。

１５．付帯事項

・　受注者は、産総研担当者の求めにより、作業の進捗状況などの報告に応じること。

・　納入されたデータ等における発注側の責めによらない納入の完了後１年以内の不良等不具合については、その補修、調整等責任をもって無償で速やかに行うこと。

・　本仕様書の技術的内容に関する質問等については、産総研担当者と協議すること。

・　本仕様書に定めのないこと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。

・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。

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、又は知り得るべきソースコード、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産総研担当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、又は知り得るべきソースコード等の埋込み又は組込みその他産総研担当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、又は知り得るべきものに限り、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、本業務に産総研担当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産総研担当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産総研担当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、本情報システムに産総研担当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。