

仕 様 書

1. 件名

クラウドデータ解析基盤構築作業

2. 研究の概要

国立研究開発法人産業技術総合研究所ゼロエミッション国際共同研究センター（以下、「産総研」という。）では、電力データ活用支援等事業「電力個データを活用した次世代家庭エネルギーマネジメントシステム開発に向けた基盤構築」事業のもと、エネルギーの安定供給と脱炭素社会の両立に向けて、家庭の電力個データを活用した研究開発に取り組んでいる。本研究開発では、一般社団法人電力データ管理協会（以下、「電管協」という。）から提供される電力個データを解析するため、大規模なデータ解析に耐え得るクラウド型高速分散データベース（Snowflake ベース）の解析基盤開発を行い、将来に向けた高度データ解析活用基盤を構築する。

3. 作業の概要

解析対象となる電力個データは、30分ごとの消費電力データの記録及び逆潮流のデータとその世帯の属性情報から構成された時系列データとなっている。本事業では新たに約 3500 世帯の電力個データを収集すると同時に既に産総研が保有する 15 万世帯電力個データを一括して解析可能とするシステムを構築する。データ量は数百億レコードに達する。こうした大規模時系列データを解析するためには専用の解析基盤が必要となる。本件は、Amazon Web Services（以下、「AWS」という。）と Snowflake を連携させデータ基盤の構築を行う。

4. 作業項目

以下に記載する作業を行い、その結果を業務報告書として提出する。

- 4.1. セキュリティ対応
- 4.2. インフラ構築
- 4.3. データ移行
- 4.4. システム連携・データ投入
- 4.5. 運用支援

5. 作業項目別仕様詳細

- 5.1. セキュリティ対応
 - 5.1.1. 認証・アクセス制御

- ・ AWS Identity and Access Management (以下、「IAM」という。)のポリシーに基づき設計し、適用すること。
- ・ Snowflake のロールベースのアクセス制御 (以下、「RBAC」という。)による権限管理体系を構築すること。
- ・ IAM と Snowflake のユーザについて多要素認証を設定すること。
- ・ IP ホワイトリスト、接続元制限、AWS Private Link (以下、「Private Link」という。)等によって、ネットワークポリシーを設計・設定すること。

5.1.2. 監査・コンプライアンス対応

- ・ AWS CloudTrail や Snowflake アクセス履歴等を設定して監査ログを保持すること。

5.1.3. データ管理

- ・ 研究プロジェクト毎にスキーマを分離し、アクセスを制御するよう設計すること。

5.2. インフラ構築

5.2.1. AWS 構築

- ・ AWS アカウントは産総研が提供する。また、産総研が提供する AWS アカウントを利用する場合、AWS 利用料は本契約に含める必要はない。
- ・ AWS の管理者・運用者・利用者の権限を適切に設計・設定すること。
- ・ Amazon VPC (以下、「VPC」という。)、サブネット、セキュリティグループ、ルーティング等を適切に設計し、セキュアなネットワークを構築すること。
- ・ 産総研オンプレ環境から Private Link を介し、セキュアに AWS に接続できるよう設計・設定すること。
- ・ データロード用の AWS S3 バケット (以下、「S3」という。)を作成し、適切なアクセス制御を設計・設定すること。
- ・ IAM ロールにより、S3 から Snowflake にアクセスできるように設計・設定すること。

5.2.2. Snowflake 構築

- ・ 産総研が契約者として Snowflake アカウントを新規に取得すること。取得したアカウントで、日本国内をリージョンとする AWS 上で、ウェアハウスサイズ XL を Business Critical エディション環境にて、120 時間以上動作させる環境とすること。
また、10TB の計算用データを 4 ヶ月保存可能である能力を提供可能であること。
- ・ AWS から Private Link を介し、セキュアに Snowflake に接続できるよう設計・設定すること。
- ・ 既存データに基づいて、データベースのスキーマ・テーブルを設計・設定

すること。

- ・サイズ、自動停止、自動再開、クラスタリングを考慮して、Snowflake 仮想ウェアハウスを設計・設定すること。
- ・クレジット使用料を監視し、閾値を超過した場合アラートが通知されるよう設計・設定すること。
- ・オンラインにて使用方法について研修を実施すること。
- ・契約終了後は、請負者の Snowflake の権限を無効化または制限すること。

5.3. データ移行

産総研担当者が指定する大規模研究業務ネットワーク内のデータを Snowflake データ基盤に移行すること。

5.3.1. 準備

- ・フェーズ分け、優先順位、スケジュール等を考慮したデータ移行の計画を策定し、産総研担当者の了承を得ること。

5.3.2. 実行

- ・産総研の指定する 10TB 程度のデータを移行すること。
- ・件数、合計値、サンプリングによって移行したデータの整合性を検証すること。

5.4. システム連携・データ投入

5.4.1. データ投入機能

- ・Web UI や Snow SQL を使用した手動アップロード機能を有すること。
- ・S3 経由で大容量のデータを投入できること。
- ・CSV、JSON、Parquet 等のファイル形式に対応し、テンプレートを作成すること。
- ・データ投入時のエラー処理とログ出力ができるよう設計・設定すること。

5.4.2. 既存ツール連携

- ・IBM SPSS Modeler と連携できること。
- ・Python からの接続手順を記載したドキュメントを作成すること。

5.5. 運用支援

5.5.1. 運用ドキュメント整備

- ・詳細なデータ投入手順を記載したユーザ向けの手順書を作成すること。
- ・ユーザ管理、権限管理、リソース管理等について記載した管理者向けの手順書を作成すること。

5.5.2. スキルトランスファー

- ・実際の研究データを使用した投入訓練を行うこと。

- ・よくあるエラーと対処法について、説明すること。

5.5.3. 移行期サポート

- ・データ移行期の問い合わせに対応すること。

6. 納入期限および納入場所

納入期限：2025年12月26日

納入場所：茨城県つくば市小野川16-1 国立研究開発法人産業技術総合研究所
つくばセンター西事業所 西-4A棟 2115室

7. 納入物品

- 7.1. 業務報告書 1部(紙媒体または電子媒体)
- 7.2. Python 接続手順書 1部(紙媒体または電子媒体)
- 7.3. ユーザ向け手順書 1部(紙媒体または電子媒体)
- 7.4. 管理者向け手順書 1部(紙媒体または電子媒体)

※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。

8. 納入の完了

「7. 納入物品」に記載の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の確認を行い、納入の完了とする。

9. 特記事項

- 9.1. 産総研は、請負者が本作業を遂行するうえで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。
- 9.2. 請負者は、本作業において作成した著作物についての著作権を産総研に無償で譲渡するものとし、著作者人格権を行使しないものとする。
- 9.3. 請負者は、産総研に対し、納品した成果物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、納品した成果物について、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、請負者は、その責任と負担においてこれを処理するものとする。

10. セキュリティ要件

10-1: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(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。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。

10-2: 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貸与品は産総研担当者の了解なしに所外に持ち出しまたは複製してはならない。
- ④産総研の所外へ持ち出しまたは複製した貸与品については一覧表を作成し、産総研担当者に提出すること。なお、契約終了後、速やかに返却又は廃棄し、産総研担当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、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。
- ⑥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。
- ⑦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。
- ⑧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。
- ⑨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、

産総研が提示するチェックリストの内容に基づき、適宜情報セキュリティ対策の履行状況を報告すること。

- ⑩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。
- ⑪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。
- ⑫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。
- ⑬本業務の履行においては、十分な秘密保持を行うこと。
- ⑭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、当該成果物を産総研担当者の許可を得て、抹消すること。また、受注者は、産総研担当者の指示に従い、当該成果物の抹消の確認を受けること。

1.1. 付帯事項

- (1) 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。
- (2) 受注者は、業務上知り得た一切を産総研の許可なく他に漏らしてはならない。また、他の目的に利用してはならない。
- (3) その他、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者との協議の上決定するものとする。

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。）の埋込み又は組み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み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。