仕　様　書

1. 件名

秘密計算システムの入出力フォーマット変換 API の設計およびプログラム作成作業

2. 研究の概要

国立研究開発法人産業技術総合研究所サイバーフィジカルセキュリティ研究センター(以下、「産総研」という)では、戦略的イノベーション創造プログラム（SIP)「先進的量子技術基盤の社会課題への応用促進」のサブ課題「量子セキュリティ・ネットワーク」の中で、「省リソース化された実用的秘密計算システムの実現に関する研究開発」を実施している。その課題の１つに、異なる秘密計算システム間のインターオペラビリティ機能の実現があり、他のサブ課題実施機関と連携しながら実現方法の検討を行っている。

3. プログラムの概要

本件は、産総研の研究開発成果が実用化された秘密計算システムの計算結果を他の秘密計算システムで活用できるようにする、またその逆（他の秘密計算システムの計算結果を使った産総研の秘密計算システムでの活用）をできるようにするために必要となる機能、すなわち、入出力フォーマットを統一的なものへと変換する処理への API（統合分析 API）の設計およびプログラム開発である。

4. プログラムの構成

4-1:統合分析 API 用インターフェイス機能

5. 構成別仕様詳細

5-1:統合分析 API 用インターフェイス機能

サブ課題「量子セキュリティ・ネットワーク」の参加機関の間で議論し決定された統合分析 API と産総研の研究成果である秘密計算システムとの間で秘密計算の入出力情報のやり取りを可能とする機能を実現すること。詳細には、以下の規定 A,B,C に基づいて実装を行い、そのプログラム設計書、プログラムソースコード、プログラムバイナリーを作成すること。

A. インターフェース仕様規定

(1) 統合分析 API 実行リクエストの受付

統合分析 API は、curl コマンドを用いて HTTP リクエストにより呼び出すものとする。

統合分析 API は以下の情報が含まれたリクエストを受け付ける機能を備えるものとする。詳細な形式については、調達請求者の指示に従うこと。

- 分析対象のテーブル識別子
- 分析に用いるカラムの識別子
- 実行する分析処理の種類
- 必要に応じた追加のパラメータ

(2) 分析処理の振り分け

受け付けたリクエストを、各秘密計算システムに適した形式に変換する機能を実現すること。それぞれの形式については、調達請求者の指示に従うこと。

(3) 分析結果の統合

各システムから返却された分析結果を共通の形式に変換する機能を実現すること。API は以下の情報を含む形で結果を返却するものとする。詳細な形式については、調達請求者の指示に従うこと。

- リクエストで指定された識別子情報
- 実行された分析処理の種類
- 統合された分析結果

B. データ形式に関する規定

(1) データの識別子

テーブルやカラムの識別子は、連携する秘密計算システム間で共通の値を使用する。

(2) 結果の形式と精度

- 変換 API により、各システムの結果形式を共通の形式に変換する。具体的な変換形式は、調達請求者と協議の上決定するものとする。
- 数値データの精度はそれぞれの秘密計算システムに応じたパラメータに基づいて適切に調整するものとする。

C. 実行処理に関する規定

- すべての処理は同期的に実行されるものとする。
- 処理のタイムアウトが発生しないよう適切な設定を行う。

6.特記事項

6-1:作業者は上記作業の実施にあたり、以下の要件を満たしていること。

- 二者間及び三者間計算などの複数の異なる秘密計算システムへの深い知見を有すること。
- 情報セキュリティ関連システム開発業務に関する実務経験を 1 年以上有すること。
- 日本語を用いたシステム開発および邦文書類作成等の実務経験を 1 年以上有すること。
- プライバシーデータ保護技術に関するシステムの構築を 1 年以上継続して実施していること。
- クライアント補助型二者間秘密計算の安全な構成方法に関する深い理解を有し、本役務を実施する者の内少なくとも１名は、当該技術に関して情報セキュリティ関連の学会で実施した経験を有すること。

6-2: フォーマットの変換機能の作成に当たっては、産総研と他の連携機関で決定した、統合分析 API 及びそれに接続される複数の秘密計算システム方式間の違いによって生じる秘密データの表現形式や内部的な代数構造の違いを考慮しつつ、適切にデータ型やパラメータを変換できるよう設計・実装すること。

7.貸与品

7-1: 産総研の究成果である秘密計算システム試用環境一式を貸与する。また、試作システム構成図、統合分析 API のリクエストと分析結果フォーマットの情報を貸与する。

8.確認試験

8-1:調達請求者の立ち合いのもと、受注者は 9 項で示されたプログラム設計書およびプログラムの使用方法に関する取扱説明書に記載されている操作手順を実際に実行し、仕様書に記載されている機能・性能が実現されていることおよびドキュメント類の内容・品質を確認すること。
プログラムの完成度および品質は, API の形式やパラメータが 6 項に記載されている規定に従っていること、取扱説明書に従ってプログラムを

操作し、仕様書に規定されている個別変換機能の動作を検証することで確認する。

9.納入物品

9-1　プログラム設計書 一式

9-2　プログラムソースコード 一式

9-3　プログラムバイナリー 一式

9-4　プログラムの使用方法に関する取扱説明書　1部

上記の納入物品は全て、原則として安全なファイル共有サービスを用いて電子データで納入すること。

10.納入場所

10-1:〒135-0064 東京都江東区青海 2-3-26
国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究センター
臨海副都心センター　本館 1104 室

11.納入の完了

11-1:本件は「9. 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。

12.納入期限

12-1:2025 年 3 月 26 日（水）

13.成果の取扱い

13-1:産総研は、受注者がプログラム作成等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。

13-2:受注者は、成果物の著作権（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。

13-3:受注者は、契約条項に定める検査に合格後、直ちに別紙様式による著作者財産権譲渡証書及び著作者人格権不行使証書を産総研に提出しなければならない。

13-4: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。）※1 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。

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、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。※2
⑫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。
⑬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。
⑭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。※3
⑮本業務の履行においては、十分な秘密保持を行うこと。
⑯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。
⑰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。

15.付帯事項

15-1:受注者は、調達請求者の求めにより、作業の進捗状況及び作業内容について報告しなければならない。

15-2:納入時には、本プログラムの操作について講習を行うこと。

15-3:納入されたプログラム等における発注側の責めによらない納入の完了後1 年以内の動作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。

15-4:本仕様書の技術的内容及び知り得た情報に関しては、守秘義務を負うものとする。

15-5: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。

15-6:サプライチェーン・リスクに対応するため、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続きに関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ）に基づき対応を求めることがあるので応じること。

別紙様式

〇〇〇〇年〇〇月〇〇日

著作者財産権譲渡証書

国立研究開発法人産業技術総合研究所　殿

受注者
住所
会社名
代表者氏名　　印

ソフトウェア作成請負契約　　（〇〇〇〇年〇〇月〇〇日　契約）
件　名

上記契約により作成した成果物の所有権及び著作権（著作権法第 27 条及び第 28 条に規定する権利を含む）は、国立研究開発法人産業技術総合研究所に譲渡したことに相違ありません。ただし、上記契約締結前に自己所有していた権利は除くものとします。

別紙様式

〇〇〇〇年〇〇月〇〇日

著作者人格権不行使証書

国立研究開発法人産業技術総合研究所　殿

受注者
住所
会社名
代表者氏名
印

ソフトウェア作成請負契約　　（〇〇〇〇年〇〇月〇〇日　契約）
件　名

上記契約により作成した成果物の著作権（著作権法第 27 条及び第 28 条に規定する権利を含む）に係わる著作者人格権を行使しないことを約束します。
なお、著作者人格権を行使しようとする場合は、国立研究開発法人産業技術総合研究所の承認を得るものとします。