仕　様　書

1.件名:秘密計算システム間のインターオペラビリティシステムの拡張機能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部門(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インターオペラビリティシステムの拡張機能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:秘密計算システム間のインターオペラビリティシステムの拡張機能

5.構成別仕様

5-1:秘密計算システム間のインターオペラビリティシステムの拡張機能

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開発が進められている、秘密計算システム間で秘密計算の入出力情報のやり取りを可能とするインターオペラビリティシステムに求められている以下の拡張機能を実現すること。プログラム開発に加え、本インターオペラビリティシステムは、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て決定されるものであり、またその内容が作業内容と密接に関係していることから、それら議論に参加し、本件で開発する内容等の情報を提供すること。

＜拡張機能＞

A. 現開発途中のインターオペラビリティシステムにおける追加機能

A-1.連携先システムに存在するテーブルの一覧を取得する機能

本機能は、リクエスト内で指定したシステムで利用可能なテーブル（データ）の一覧を取得する機能である。具体的には、システム内における以下の動作を実装する。

- システム利用者のテーブル一覧取得リクエストを統合 API に送信
- 統合 API から秘密計算システムのクライアントにテーブル一覧取得リクエストの送信
- クライアントから秘密計算システムのサーバにテーブル一覧取得リクエストの送信
- 秘密計算システムのサーバからテーブル一覧取得結果をクライアントへの送信
- クライアントからテーブル一覧取得結果をシステム内の共有の形式に変換した後に統合 API に送信
- 統合 API からテーブル一覧取得結果をシステム利用者に送信

A-2.連携先システムにあるテーブルのテーブル構造を取得する機能

本機能は、指定したシステムおよびテーブル ID に基づき、各システム内に存在するテーブルのカラム ID・データ型を取得する機能である。具体的には、システム内における以下の動作を実装する。

- システム利用者のテーブル構造取得リクエストを統合 API に送信

- 統合 API から秘密計算システムのクライアントにテーブル構造取得リクエストの送信
- クライアントから秘密計算システムのサーバにテーブル構造取得リクエストの送信
- 秘密計算システムのサーバからテーブル構造取得結果をクライアントへの送信
- クライアントからテーブル構造取得結果をシステム内の共有の形式に変換した後に統合 API に送信
- 統合 API からテーブル構造取得結果をシステム利用者に送信

A-3. 実行可能な分析一覧取得機能

本機能は、指定したシステムにおいて実行可能な分析の一覧を取得する機能である。具体的には、システム内における以下の動作を実装する。

- システム利用者の実行可能な分析一覧取得リクエストを統合 API に送信
- 統合 API から秘密計算システムのクライアントに実行可能な分析一覧取得リクエストの送信
- クライアントから実行可能な分析一覧取得結果を統合 API に送信
- 統合 API から実行可能な分析一覧取得結果をシステム利用者に送信

B. 今後参加機関の間で議論して決定される、「改良型インターオペラビリティシステム」で必要となる産総研の秘密計算システムにおけるデータ復元機能

「改良型インターオペラビリティシステム」は、一方の秘密計算システムに存在するデータを一度復元して、もう一方の秘密計算システムに連携して分析を実行するシステムである。本システム内で必要となるセキュアな中間領域におけるデータ復元機能の実現を以下の通り実装する。

- 他の秘密計算システムのクライアントからのデータ復元・秘匿化連携 API への実行命令を受けて、産総研の秘密計算システムのサーバにデータの復元リクエストを行って、復元結果を受け取る。

6.特記事項

6-1:受注者は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、本作業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発表した経験を有すること。

6-2:拡張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、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.完成品の試験・確認

産総研担当者の立ち合いのもと、受注者は「9.納入物品」に記載の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「5. 構成別仕様」に従っていることならびに取扱説明書に従ってプログラムを操作し、仕様書に記載した個別変換機能の動作を検証することで確認する。

8.貸与品

8-1: 産総研研究成果である秘密計算システム試用環境　一式

8-2: 試作システム構成図、現開発段階のインターオペラビリティシステムの情報　一式

9. 納入物品（提出文書、電子ファイル、ソースコード等）

納入は、中間納入と最終納入の二段階で実施すること。納入物品は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。

9-1. 中間納入物品

9-1-1: 5-1.A.A-1～5-1.A.A-3 の機能の設計書、ソースコード、バイナリ　一式

9-1-2: 使用方法に関する取扱説明書　１部

9-2. 最終納入物品

9-2-1: 9-1-1 を含む全機能を統合したシステムの設計書、ソースコード、バイナリ　一式

9-2-2: 5-1.B の機能の設計書、ソースコード、バイナリ　一式

9-2-3: 全機能の使用方法に関する取扱説明書　１部

10. 納入場所

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部門

臨海副都心研究センター　本館 1104 室

11. 納入の完了

本作業は「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「7. 完成品の試験・確認」に従って確認して、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。

12. 納入期限

中間納入期限：2025 年 8 月 29 日（金）

最終納入期限：2025 年 12 月 26 日（金）

13. セキュリティ要件

13-1: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。

13-2: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、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。
⑫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。
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。

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産総研担当者と協議の上、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。

14.付帯事項

14-1:受注者は、産総研担当者の求めにより、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。

14-2: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。

14-3: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。

14-4: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。

14-5: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。

14-6: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。

別紙

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。