仕　様　書

1. 件名

分散型秘密計算における拡張ネットワーク設計およびプロトコルの先進プロトタイプ実装作業

2. 作業の目的

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、科学技術振興機構受託研究事業「戦略的創造研究推進事業／サステナブルな分散型秘密計算基盤」（以下、「本研究」という。）を実施している。秘密計算は、データを秘匿したまま処理が可能な暗号技術であり、個人・企業の機密情報の利活用を促進すると期待されている。本研究では、従来の秘密計算技術における課題である「秘密計算プロバイダへの信頼の必要性」および「プロバイダが不在の状況の運用の困難性」を解決し、ユーザ同士で構成されるオープンな分散環境下の効率的な秘密計算の基礎理論確立、および、ユーザインセンティブ設計が組み込まれ持続可能な運用が可能となるスマートコントラクトの記述が可能なブロックチェーンに基づく分散型基盤の開発を行い、その両者を融合することでサステナブルな秘密計算基盤を目指す。

産総研では、「サステナブルな分散型秘密計算基盤」の構築に向けて、2024 年度に「分散型秘密計算におけるネットワーク設計およびプロトコルのプロトタイプ」（以下、「ベースシステム」という。）を開発し、データ投入から秘密計算の実行、出力、インセンティブ分配に至る一連の処理が有効に機能することを確認した。

一方で、ベースシステムは技術的な基本検証という観点では一定の成果を上げたものの、多人数・多拠点からの利用を想定した構成や、入力者・計算者・出力者といった各類ユーザが独立的に利用可能な環境の実現、計算内容を柔軟に指定可能とする機能、および、ウォレットアドレスを用いたインセンティブ分配状況の確認が可能となるユーザーインターフェース（以下、「UI」という。）の未整備など、実運用上求められる機能が不足している。また、システム構成が中央集権的なアーキテクチャに依存しているという構造的な課題も残されている。

本作業は、これらの機能的な不足および構造的な課題の解消を目的とし、ベースシステムと統合可能な形で、拡張されたネットワーク設計およびプロトコルの先進的なプロトタイプを開発するものである。

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。

カテゴリ	用語	説明
組織及び人物	調達請求者	本システム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。
	調達担当者	本調達の契約手続き等を担当するもの。
	受注者	本調達の対象となる業務に従事する事業者。
情報セキュリティー関連	情報セキュリティインシデント	産総研が望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
	情報セキュリティポリシー	産総研の情報セキュリティ基本方針、情報セキュリティ規程、情報セキュリティ実施要領及び情報セキュリティ実施ガイドの総称。
技術関連	秘密計算	暗号化もしくは秘密分散されたデータを復号化せずに直接

		演算処理を行う技術。機密性の高いデータの共有や分析に利用される。
	ベースシステム	2024 年度調達「分散型秘密計算におけるネットワーク設計およびプロトコルのプロトタイプ」において開発されたシステム。
	スマートコントラクト	ブロックチェーン上で動作するプログラムで、取引や契約を自動実行するためのコード。条件が満たされた場合に事前にプログラムされた処理を行う。
	ブロックチェーン	分散的な合意形成アルゴリズムに基づき、取引履歴などの情報を一貫性および耐改ざん性をもって管理する仕組み。本仕様では、報酬のトークン分配などに用いられる。
	シェア	秘密計算において、機密情報を分割して生成される断片。シェア単体では元の情報を復元できず、複数を組み合わせることで復元可能。
	デポジット	特定の目的のためにスマートコントラクトに預託する資産。
	コミットメント	データや計算結果を保証するための暗号学的手法で、結果を事前に隠しながらも後で検証可能にする仕組み。
	拡張ネットワーク	2024 年度に構築されたベースシステムを基盤とし、多人数・多拠点からの利用、自律的な各種ユーザの接続、UI による可視化など、分散型秘密計算の実運用を想定した構成を指す。具体的内容および構成要素については第 6 章にて詳細に示す。

3. 作業の概要

本作業では、「サステナブルな分散型秘密計算基盤」の実現に向け、2024 年度に構築したベースシステムを基礎として、拡張ネットワーク設計およびプロトコルに関する先進的なプロトタイプの開発を行う。具体的には、多人数・多拠点からの分散的な利用に対応可能なネットワーク構成の整備、計算内容を柔軟に指定可能とする機能の実装、インセンティブ分配状況を可視化・操作可能な UI の整備、ならびに中央集権的アーキテクチャからの脱却を図る分散通信機構の設計を含む。

4. システム開発の属性

本システム開発は、産総研の仕様指示で作成する形態である。

5. 開発作業構成

5-1. 分散型秘密計算基盤の拡張ネットワークの推奨設計

5-2. 想定した拡張ネットワーク設計に基づき、ブロックチェーンへの接続を含むプロトコルの先進プロトタイプ実装

5-3. 定例報告

6. 構成項目別作業内容

6-1. 分散型秘密計算基盤の拡張ネットワークの推奨設計

産総研から貸与予定の研究論文に含まれる、各種プロトコル等に用いられる数式や理論、ならびに、ベースシステムの資料（推薦設計書、ネットワークプロトタイプ設計書、システム操作マニュアル）および、ソースコード内で使用している各種技術の内容を理解した上で、次項に示すとおりの、ベースシステムに対する改良点の要求仕様を踏まえて、拡張ネットワークの推奨設計を行うこと。

6-2. 想定した拡張ネットワーク設計に基づき、ブロックチェーンへの接続を含むプロトコルの先進プロトタイプ実装

拡張ネットワークの設計は、ベースシステムに対する要改良点を記した、以下の要求仕様を踏まえて詳細設計を行い、当該設計に基づく先進プロトタイプ実装は、ソースコード一式、ならびに、その操作方法を記載したマニュアルも作成し、納入すること。

(1) 秘密計算の拡張ネットワークを構成する各参加者が、それぞれ独立して、自律的に動作できる環境下で動作するものとし、採用する通信アーキテクチャは、中央集権的方式を用いず、各参加者同士が直接通信するピアツーピア方式のものとすること。

(2) 秘密計算の拡張ネットワークへの参加者が、秘密計算の対象となる入力値を提供する「入力者」、入力値に関する秘密計算を実行する「計算者」、秘密計算の結果を受け取る「出力者」の 3 種類の役割に分類されるものとすること。

(3) 秘密計算に関する計画立案、秘密計算の目的となる計算式作成、ブロックチェーン上のスマートコントラクトの配置と進行等を実施する目的で、「入力者」「計算者」「出力者」以外の「特別な役割を果たす参加者」を配置してもよい。ただし、特別な役割を果たす参加者の責任範囲は、必要最低限にとどめ、システム全体における権限が集中しないものとすること。

(4) 計画立案で設定する必要がある「入力者」「計算者」「出力者」の各人数は任意に変更できるものとすること。ただし、入力者数に関しては、秘密計算の計画段階では数を確定できない状況下に対応可能なものとすること。

(5) 計画立案で設定する必要がある秘密計算の対象となる関数は、 DSL(ドメイン固有言語)を用いて、任意の計算式をプログラミング可能なものとすること。なお、DSL は、入力値に関する、最大値(max)、最小値(min)、平均値(average)、中央値(median)、最頻値(mode)等を用いたデモンストレーション可能なサンプルコードも添付すること。

(6) 計画立案の内容に合意し、秘密計算セッションに参加表明する者は「入力者」「計算者」「出力者」のいずれかの希望する役割を選択した上で、所定の参加費をデポジットすることにより、当該秘密計算セッションへの参加権を得るものとすること。また、先述の「特別な役割を果たす参加者」を、秘密計算の拡張ネットワークに参加させる場合は、当該参加者も参加費をデポジットすることで参加権を獲得し、エコシステムの一員として振る舞うものとすること。

(7) 秘密計算セッションに対する参加費のデポジット、および、役務の対価報酬の分配に使用されるトークンは、ブロックチェーン上に配置されるスマートコントラクトに定義される、本プロジェクトの為に発行されたトークンを用いること。そして、当該デポジットは、払込み用のスマートコントラクトアドレス宛に支払われるものとし、払込み方法は、ブロックチェーン用の汎用ウォレットアプリケーションを用いてトランザクションを発行することによって行うことができるものとすること。

(8) 当該デポジットにより、秘密計算セッションへ参加権を得た「入力者」「計算者」「出力者」および「特別な役割を果たす参加者」は、立案された計画どおりの時間内に集合して当該秘密計算セッションに参加し、相互協力の下それぞれの役務をこなすものとすること。

(9) 秘密計算セッションに係る役務の対価報酬の分配は、ブロックチェーン上に配置されるスマートコントラクトにより、各参加者が参加表明時に申告したウォレットアドレス宛に直接支払われるものとすること。

(10)秘密計算セッションにおいて不正検知が生じた場合、その是非をブロックチェーン上のスマートコントラクトに合意をはかり、問題を解消するプロセスにおいては、悪意ある参加者による虚偽申告に対する名誉回復が可能となる手段も講じること。

(11)(1)～(10)の動作プロセス、および、動作結果、ならびに、各参加者のウォレットアドレス内のトークン残高等を参照するために必要な UI を用意すること。

6-3. 定例報告

(1) 受注者は、6-1.および 6-2. に関する定例報告会を 2 週間に 1 度以上オンサイトまたはオンラインにて開催し、議事進行に係る資料を用意すること。

7. 受注者の能力、要件

受注者は作業の実施にあたり、以下の要件を満たすこととする。

1 ピアツーピア方式の自律分散型ネットワークに関する 1 年以上の設計および開発の経験を有すること。
2 ブロックチェーンに関する外部参照可能な論文または書籍等の執筆、発表経験を有すること。
3 ブロックチェーンを用いたスマートコントラクトに関する 1 年以上の設計および開発の経験を有すること。
4 秘密分散技術ならびに秘密計算ネットワークに関する 1 年以上の設計および開発の経験を有すること。

8. 発注側で貸与するデータ及び容量等

本仕様書に基づく作業を実施するにあたり、受注者には以下の資料を貸与する。

(1)2-2.項に記載したベースシステムの資料(推薦設計書、ネットワークプロトタイプ設計書、システム操作マニュアル) 一式

(2)2-2.項に記載したベースシステムのソースコード 一式

そのほか、必要に応じて本研究プロジェクトで使用するデータの必要情報を貸与する。貸与範囲および容量等については調達請求者と別途協議の上決めるものとする。

9. 完成品の確認

(1)調達請求者は、仕様書と「11. 納入物品」を比較したドキュメント(「11. 納入物品」(4))の内容に基づいて納入物品の内容・品質を確認する。

(2) 6 項の各仕様の実現精度・品質については、受注者と調達請求者で協議の上決めるものとし、受注者は善管注意義務を負った上で最善を尽くすものとする。

10. 納入の完了

本作業は、「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。受注者は確認にかかる作業を支援すること。

11. 納入物品

納入は中間納入と最終納入の二段階で実施すること。内容については定例会等で調整のう

え、その時点で提示可能な範囲の成果物を提出すること。納入物品は全て、原則として USB メモリ等の外部電磁的記録媒体以外で納入すること。

11-1.　中間納入物品
(1) 6-2. 項に掲げたプロトタイプ（暫定版）のソースコード（電子媒体）　一式
(2) 6-2. 項に掲げたプロトタイプ（暫定版）の操作方法を記したマニュアル（紙媒体）　1 部

11-2.　最終納入物品
(1) 6-1. 項各号をまとめ、1綴りにした報告書（紙媒体）　1 部
(2) 6-2. 項に掲げたプロトタイプ（完成版）のソースコード（電子媒体）　一式
(3) 6-2. 項に掲げたプロトタイプ（完成版）の操作方法を記したマニュアル（紙媒体）　1 部
(4) 仕様書と納入物品の内容を比較したドキュメント（紙媒体）　1 部（9.(1)を参照）

12. 納入期限および納入場所
納入期限：（中間納入期限）2025 年 10 月 22 日
（最終納入期限）2025 年 11 月 28 日
納入場所：　〒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部門
臨海副都心センター本館 1104 室

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調達請求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提供する資料は調達請求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、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。
（履行期間が半年以上の場合のみ）
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本業務の履行においては、十分な秘密保持を行うこと。
⑮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。

15. 付帯事項
(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。
(2) 本仕様書の技術的内容する質問等については、調達請求者と協議すること。
(3) 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。
(4) 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。
(5) 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。

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、又は知り得る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。