仕　様　書

1. 件名

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（以下、「産総研」という。）サイバーフィジカルセキュリティ研究センターでは、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。

本件は、この分散型基盤の実現に向けて必要となるネットワークの推奨設計を行うとともに、ブロックチェーン接続を含めた基本プロトコルのプロトタイプ実装を行うものである。

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	産総研担当者	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。（調達請求者）
	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。

カテゴリ	用語	説明
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。
	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。
	ブロックチェーンオラクル	ブロックチェーンと外部の現実世界のデータ（例: 市場価格、天気情報）をつなぐ役割を持つシステム。スマートコントラクトに外部データを供給する。
	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。

3. 役務の概要

本件は、分散型秘密計算基盤の実現を目指し、モバイル、デスクトップ、ウェブ、サーバーなどの多様なプラットフォームで、本研究が進める秘密計算の基本プロトコルを利用できるネットワークの推奨設計を行うものである。次に、想定したネットワーク設計に基づき、ユーザインセンティブの仕組みを実現するため、ブロックチェーンへの接続を含む基本プロトコルのプロトタイプ実装を行う。

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. 役務作業構成

(1) 分散型秘密計算基盤のネットワークの推奨設計

(2) 想定した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基本プロトコルのプロトタイプ実装

(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ネットワークの推奨設計

下記の仕様を満足する設計を行い、産総研担当者に仕様実装方法を確認のうえ「分散型秘密計算基盤のネットワークの推奨設計」を作成し、納入すること。

(1) 秘密計算基盤のネットワーク、ならびに、当該ネットワークで実施される秘密計算に係る役務の対価分配基盤として必要な、ブロックチェーンおよびスマートコントラクトに関する推奨構成を作成し、設計書にまとめること。

(2) 秘密計算基盤のネットワークに用いる秘密分散方式、および、その基本原理を適切な参照文献を明示した上で納入する設計書にまとめること。なお、適切な方式の選定については、必要に応じて産総研担当者と協議のうえ決定すること。

(3) 本件における「秘密計算基盤のネットワーク」は、少なくとも1名以上、通常複数が想定される入力者(Input Party)と、必ず複数の計算者(Computing Party)と、1名以上の出力者(Output Party)によって構成されるシステムで、以下の要件を満たすものであること。

(a) 入力者(Input Party)は、計算者(Computing Party)に対し、必要な入力値のシェアを提供する立場であり、秘密計算のプロトコルに従い、入力値を秘密計算可能なシェアに分割し、計算者ら宛に引き渡す役割を果たす。
計算者(Computing Party)は、秘密計算を実行する立場であり、入力者から与えられた入力値のシェアと、出力者から与えられた集計式を基に、複数の計算者らと協力の下、秘密計算を実行し、出力者(Output Party)宛に、秘密計算結果のシェアを引き渡す役割を果たす。

(b) 計算者(Computing Party)は、自身が担当した秘密計算結果のシェアに対応するコミットメントを生成し、この値をブロックチェーンオラクルに書き込む役割を果たす。

(c) 出力者(Output Party)は、秘密計算を企図する立場であり、入力者(Input Party)らに対して、入力値の提供を求め、計算者(Computing Party)らに対して、秘密計算のために式を与え、秘密計算の実行を要求する役割を果たす。

(d) 出力者(Output Party)は、各々の計算者(Computing Party)から秘密計算結果のシェアを受け取り、集計結果を復元し、その値をブロックチェーンオラクルに書き込む役割を果たす。

(e) 入力者(Input Party)、計算者(Computing Party)、出力者(Output Party)は、いずれも、どの役割も兼務できる。

(4) 分散型秘密計算基盤のネットワークにおいて、情報通信の効率化、情報共有の効率化等を補助するパーティを追加配置しても良く、その場合はその目的も設計書内に記載すること。

(5) 分散型秘密計算基盤のネットワークにおいて、ある目的の秘密計算ラウンドへの参加を希望する各パーティは、予め定めた参加費を、所定のスマートコントラクト宛にデポジットした上で参加するものとすること。

(6) 計算者（Computing Party）が、ブロックチェーンオラクルに登録した、各々の秘密計算結果のシェアに対応するコミットメントついて、スマートコントラクトを用いて、欺瞞されていないことを検証可能な機構を設けること。また、欺瞞が発覚した場合、当該計算者（Computing Party）がデポジットした参加費を没収し、その他パーティ宛に均等に分配すること。

(7) 分散型秘密計算基盤のネットワークにおいて、秘密計算に係る各パーティの役務の対価に関する評価式を定義すること。

(8) 分散型秘密計算基盤のネットワークにおいて、秘密計算に係る各パーティの役務の対価の評価式に基づき、各パーティの役務の対価を算定し、自動分配するスマートコントラクトを構成すること。

(9) 各参加者向けに実施状態を確認できる適切なユーザーインターフェースを用意すること。

(10) 上記の機能を実装し動作させるために必要な、入力者・計算者・出力者の各 Party の動作環境（OS、ソフトウェア、ハードウェアその他実行環境に関する要件）に関して推奨される仕様の提案を、設計書にまとめること。

6-2. 想定した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基本プロトコルのプロトタイプ実装

下記の仕様を満たす、秘密計算ネットワークおよびブロックチェーンへの接続の概念実証を行うためのプロトタイプ実装を作成し、このプロトタイプのソースコードを収めた電子媒体およびその操作方法を記載したマニュアルを納入すること。

(1) 6-1. で検討した方針に基づいて、実際に動作するプロトタイプとしてスマートコントラクトを開発し、ブロックチェーン上（パブリックブロックチェーンのテストネット）に配置すること。

⑵ 当該スマートコントラクトの実行を指図するトランザクションを送信する仕組みを用意すること。

⑶ 当該スマートコントラクトにおける、実行前後のステート変化を確認できる簡易のユーティリティを用意すること。

⑷ 当該スマートコントラクトの操作方法を記したマニュアルを用意すること。

6-3. 定例報告

⑴受注者は、6-1. 6-2. に関する定例報告を 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. 作業者の能力、要件

作業者は上記業務の実施にあたり、以下の要件を満たすこととする。

⑴ 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。

⑵ 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。

⑶ 秘密分散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. 完成品の確認

⑴調達請求者は、納入物品に含まれる「仕様書の記載内容と納入物品の記載内容を比較したドキュメント（10. 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。

9. 納入の完了

本件は、「10.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。

10. 納入物品

⑴ 6-1. 項各号をまとめ、1綴りにした報告書（紙媒体） 1 部
「分散型秘密計算基盤のネットワークの設計書」

⑵ 6-2. 項に掲げたプロトタイプのソースコードを収めた電子媒体（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。） 1 個

⑶ 6-2. 項に掲げたプロトタイプの操作方法を記したマニュアル（紙媒体） 1 部

⑷ 仕様書の記載内容と納入物品の記載内容を比較したドキュメント（紙媒体） 1 部
（上記「8. 完成品の確認」を参照）

11. 納入期限および納入場所

納入期限： 2025 年 3 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センター
臨海副都心センター本館 1104 室

12. 成果の取り扱い

⑴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。

⑵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。

⑶ 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。

⑷ 受注者は、産総研に対し、納入した納入物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、納入物品について、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。

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。

14. 付帯事項

(1) 受注者は、請求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。

(2) 本仕様書の技術的内容する質問等については、調達請求者の指示に従うこと。

(3) 本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議すること。

(4) 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)に基づき対応を求めることがあるので応じること 。

(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。

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。