仕　様　書

１．件名

ハイブリッドクラウド環境における経路特性保証型ネットワーク技術の標準化にかかる研究支援および技術検証作業

２．作業の目的

２．１．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。）インテリジェントプラットフォーム研究部門では、新エネルギー・産業技術総合開発機構（NEDO）プロジェクト「経済安全保障重要技術育成プログラム／ハイブリッドクラウド利用基盤技術の開発／ハイブリッドクラウド利用基盤技術の開発／経路特性保証型のクラウドネットワーク技術」事業において、複数の特性の異なるクラウドプラットフォームやネットワークを相互に接続したハイブリッドクラウドシステムにおける、通信経路の特性が意図通りに維持され、万が一特性が想定から逸脱した際には警告や抑止を行うことができるような、経路特性保証型ネットワーク技術の設計・開発を行っている。

本作業では、IETF(Internet Engineering Task Force)において、経路特性保証型ネットワーク技術に関する標準化作業を推進することを目的としている。

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
情報セキュリティ	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。

２．３．概要

産総研インテリジェントプラットフォーム研究部門は、IETF において、経路特性保証型ネットワーク技術に関する標準化作業に従事している。

本作業では、この業務における標準化作業を支援するものである。

３．作業項目

３．１．IETF における標準化活動

IETF において、産総研インテリジェントプラットフォーム研究部門の技術的提案に対して、専門家としてのコメントや追加提案などを実施することにより、標準化活動を推進すること。

1) 調達請求者が現在 Internet Draft として提案している技術文書 (draft-oiwa-secure-hybrid-network-01、参考：https://datatracker.ietf.org/doc/draft-oiwa-secure-hybrid-network/) について、通信分野に関する専門家として、技術議論およびコメント提案、図版の作成など、改版文書作成を支援すること。文書の形式については、IETF の定める Internet Draft の様式を満たすテキストデータとすること。

2) 1)に付随する作業として、産総研が提案する経路特性保証技術の実現に向けて、以下の調査・検討・検証を行うこと。なお、実施に当たっては、作業内容を調達請求者と協議した上で、合意を取りながら進めること。

   ① 経路特性保証技術を実現するために参照する状態情報について、RFC9232 (Network Telemetry Framework、参考 https://datatracker.ietf.org/doc/rfc9232/)のフレームワークに基づいて、クラウドやネットワーク等の実システムから収集するために利用するインターネットプロトコルの選定及びその使用方法について調査・検討すること。

   ② 利用者が指定する経路検索条件に基づいて、①で収集した状態情報を効率的に検索するための、条件指定記法とその検索方法について、検討及び検証のための試作を実施すること。

3) IETF 124（モントリオール開催：2025 年 11 月 1 日～11 月 7 日）において、標準化作業を円滑に行うために現地参加し、IETF ハッカソンへの参加や 1)に関するプロジェクトの実施などを行い、標準化活動に関する議論に参加して、調達請求者による提案活動を支援すること。

4) 3）において、関係する技術分野に関する複数の WG（Working Groups）を抽出し、ミーティングに出席し、情報の収集を行い、その結果を調達請求者との打ち合わせで議論・共有すること。

5) 3）において、現地での IETF 関係者との打ち合わせなどの計画について、調達請求者による検討に有識者として助言し、事前調整等を行うこと。

6) 1）2）3）5）で必要となる資料を作成すること。

7) 1）2）3）4）5）における活動内容を要約した作業報告書を、作成・提出すること。

４．特記事項

・ 週１回の定例会(所要時間１時間)を開催し、作業内容の協議および作業実施状況の報告・

確認を行う。定例会は対面・またはオンラインで実施する。
・ 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．受注者の要件等
・ 受注者のメンバーには、Internet Draft の執筆・改訂の経験、または IETF の WG ミーティング・BoF（Birds of a Feather）ミーティング・メーリングリストにおける標準化活動の経験者が含まれていること。
・ 受注者は、直近 5 年程度の IETF 会議に（CoVID-19 の影響による遠隔を含め）最低年 2 回参加している有識者を中心とした体制であること。

６．納入物品
納入物品は電子データとして作成し、メールやファイル転送サービス等の磁気記録媒体を使用しない方法で納入すること。
① 作業報告書　　1 部（電子媒体）
② 執筆した Internet Draft のテキストデータ　一式（電子媒体）

７．納入の完了
作業完了の後、「６．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。

８．履行期間、納入期限及び納入場所
履行期間：契約締結日～２０２５年１１月２６日
納入期限：２０２５年１１月２６日
納入場所：国立研究開発法人産業技術総合研究所
インテリジェントプラットフォーム研究部門
臨海副都心センター別館 7 階 07207 室
東京都江東区青海２－４－７

９．セキュリティ要件
9.1.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。

9.2.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。

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。

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。

１０．成果の取扱い

(1)産総研は、受注者が Internet Draft の執筆・改訂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。

(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。

(3)受注者は、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、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。

１１．付帯事項

・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。
・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。

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

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。