仕　様　書

1. 件名

令和 7 年度　材料・化学領域大規模研究業務ネットワーク運用監視支援業務

2. 研究概要

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。）材料・化学領域では、データ駆動型材料開発を実施するネットワーク基盤としてとして産総研情報セキュリティ規程第 16 条第 1 項に規定する大規模研究業務ネットワーク「材料・化学領域大規模研究業務ネットワーク」（以下、「材化ネットワーク」という。）を構築し運用を行っている。

3. 本業務の概要

本業務は、材化ネットワークの安定稼働、利用者の円滑なネットワークの利用、情報セキュリティリテラシーの向上を目的とした運用監視業務を支援するものである。また、その支援業務を効率的に行うための運用監視業務環境の整備を実施するものである。

4. 対象となるネットワークの概要

(1) ネットワーク全体の概要

材化ネットワークは大きく分けて 4 つのセグメントより成り立っており、Blue Zone、Green Zone、Orange Zone、Laboratory Zone が存在する。また SINET 網を経由し各地域センターと接続されているほか、民間企業のデータセンターとも試験的に接続されている。

(2) 利用者概要

想定する利用者は研究職員及びそれを支援する役職員や事業者等、全拠点含めて約 300 人であり、原則として 24 時間 365 日利用されている。

(3) 設置機器概要

設置機器（2025 年 6 月 1 日現在）については以下のセグメントから成り立つ。

① Blue Zone

ファイアウォール装置 2 台、物理スイッチ 8 台、物理サーバ 13 台、仮想サーバ 18 台

② Green Zone

ファイアウォール装置 2 台、物理スイッチ 9 台、物理サーバ 12 台、仮想サーバ 14 台

③ Orange Zone

ファイアウォール装置 3 台、物理スイッチ 2 台、物理サーバ 4 台

④ Laboratory Zone

ファイアウォール装置 10 台、物理スイッチ 80 台、物理サーバ 15 台※
（※つくばセンター、地域センターの合計）

(4) 設置場所

① 産総研　つくばセンター
〒305-8560 茨城県つくば市梅園 1-1-1

② 産総研　東北センター
〒983-8551　宮城県仙台市宮城野区苦竹 4-2-1

③ 産総研　中部センター
〒463-8560　愛知県名古屋市守山区桜坂四丁目 205 番地

④ 産総研　関西センター
〒563-8577　大阪府池田市緑丘 1-8-31

⑤ 産総研　中国センター
〒739-0046　広島県東広島市鏡山 3-11-32

⑥ さくらインターネット株式会社
石狩データセンター（住所非公開）

5. 対象業務別仕様

以下の支援業務を行うこと。
記載業務内容実施についてはオンサイトでの作業を基本とし、遠隔可能な範囲においては遠隔からのログ管理等を可能とする。

(1) つくばセンター材化ネットワーク運用監視支援業務

次の各システムの安定的な稼働状態の維持のために障害時対応・予防処置対応を行うこと。また必要に応じて他事業者の支援等を行うこと。

① 仮想化基盤システム
② 認証基盤システム
③ ログ収集管理システム
④ 総合エンドポイントセキュリティ管理システム
⑤ バックアップ管理システム
⑥ 大容量ファイルシステム（Lustre File System）

(2) 東北センター材化ネットワーク運用監視支援業務

次の各システムの安定的な稼働状態の維持のために障害時対応・予防処置対応を行うこと。また必要に応じて他事業者の支援等を行うこと。

① 認証基盤システム
② 大規模研究業務ネットワーク用機器
③ ログ収集管理システム

(3) 中部センター材化ネットワーク運用監視支援業務

次の各システムの安定的な稼働状態の維持のために障害時対応・予防処置対応を行うこと。また必要に応じて他事業者の支援等を行うこと。

① 認証基盤システム
② 大規模研究業務ネットワーク用機器
③ ログ収集管理システム

(4) 関西センター材化ネットワーク運用監視支援業務

次の各システムの安定的な稼働状態の維持のために障害時対応・予防処置対応を行うこと。また必要に応じて他事業者の支援等を行うこと。

① 認証基盤システム
② 大規模研究業務ネットワーク用機器
③ ログ収集管理システム

(5) 中国センター材化ネットワーク運用監視支援業務

次の各システムの安定的な稼働状態の維持のために障害時対応・予防処置対応を行うこと。また必要に応じて他事業者の支援等を行うこと。

① 認証基盤システム
② 大規模研究業務ネットワーク用機器
③ ログ収集管理システム

(6) 産総研運用担当者等支援業務

材化ネットワークの円滑な利用や運用促進をするため、産総研運用担当者等への支援を実施すること。

① テクニカルサポート
② ハードウェア管理支援
③ ソフトウェア管理支援
④ 情報セキュリティ業務支援
⑤ システム監視業務支援

(7) 情報セキュリティインシデント対応支援業務

以下の業務について、円滑な実施ができるよう支援を行うこと。

① 本業務管轄内での情報セキュリティインシデント発生における調査実施
② 外部機関もしくは産総研内部からの依頼に基づく調査実施

(8) 監視・障害予防措置対応・故障修理対応支援業務

材化ネットワークの安定的な稼働状況の維持のため、以下の対応及び必要に応じた他事業者の支援ができるよう支援を行うこと。

① ネットワーク機器及びサーバ機器の状態監視
② ネットワークトラフィック管理
③ ログ監視

④　故障修理対応に関する支援
⑤　テクニカルオンサイトサポート

(9) 緊急時対応支援業務
以下の緊急時において対応可能な緊急時体制を整備すること。
①　停電（法令停電を除く）
②　災害
③　情報セキュリティインシデント

6. 運用監視業務環境整備作業
既存の運用手順マニュアルについて、改修が必要な場合は修正した最終版を納入すること。記載内容については産総研担当者と協議のうえ決定することとし、産総研担当者の承認をもって納入すること。

7. 運用支援業務
運用サポート業務を行うこと。業務遂行における遵守事項については本項にまとめる。
(1) 運用体制
受注者は、13-2.⑤および⑥を満たす体制を構築し提示すること。
(2) 実施期間
契約日から 2026 年 3 月 31 日まで。
※ログ収集・解析など 2025 年 4 月 1 日まで遡り実施し報告すること。
(3) 業務報告
①　本業務の運用等に関する説明や報告、情報を共有するために、産総研の求めにより月 1 回程度の打ち合わせを行うこと。
②　本ネットワークで発生した障害または情報セキュリティインシデント対応等の発生や本業務に関わる緊急対応時、システム導入時、改善提案等を行う場合等、必要に応じ臨時の打ち合わせの実施すること。
③　受注者は業務報告書を月次ごとに作成・提出すること。業務報告内容については産総研担当者と協議の上決定し、これをもとに各種報告書を作成すること。必要に応じて産総研担当者に対して、本業務での運用状況や運用上の問題点について、報告、説明を行うこと。
(4) 改善提案
材化ネットワーク運用上必要な改善点がある場合は、以下の提案を行うものとする。
①　運用業務のフローに関する改善提案
②　運用業務の機器等に関する改善提案
③　その他、実際に起こったインシデントに関する具体的な改善提案
(5) 業務引継ぎ
産総研運用担当者のほか、産総研が指定する他事業者（サービス提供事業者、アプリ開発事業者、新規システム導入事業者、その他関連する役務事業者等）が、対象

システムの運用状況の把握、更新等の目的で行う調査や作業などが円滑に可能とするよう、業務内容を明らかにした書類整備等の準備を行い、次回実施者への円滑な引継ぎが実施されるよう必要な措置を講じること。

8. 貸与品

以下の資料について、調達担当者に貸与申請を行い、申請が認められた場合貸与するものとする。

(1) 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
(2) 情報セキュリティ実施要領
(3) セキュリティ実施ガイド
(4) 材料データプラットフォーム仮想化システム基盤　設定内容報告書
(5) 材料データプラットフォーム仮想化システム基盤拡張　設定内容報告書
(6) マテリアル・イノベーションプラットフォーム ネットワーク構築　設定内容報告書
(7) 材料・化学領域大規模実験業務ネットワーク運用ガイド

※その他本業務において必要なネットワークアカウント等も貸与するが、詳細については、契約相手先決定後に契約相手先にのみ開示する。

9. 受注者の要件

(1) 受注者は ISMS（ISO27001）情報セキュリティマネジメントシステムを取得していること。
(2) 民間企業または公的機関において複数台のネットワーク通信機器及びサーバ機器で構成されるシステムに関する運用保守契約実績が過去 3 年以内に 1 件以上あること。
(3) 民間企業または公的機関において次の製品について 3 年以内に 1 件以上の納入実績があること。
    ① VMware
    ② HPE ProLiant DL
    ③ ALOG
    ④ Acronis
    ⑤ Lustre File System
    ⑥ FortiGate

10. 納入の完了

作業完了の後、「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、納入の完了とする。

11. 納入物品

(1) 運用手順マニュアル（改訂版）　1 部（電子媒体）
(2) 運用監視支援業務月次報告書（契約開始月～2026 年 3 月分）※

各 1 部（電子媒体）

(3) 運用監視支援業務年次報告書　　1 部（電子媒体）

月次報告をまとめ、年間を通じた業務の振り返り等を含んだ報告書。
内容については、産総研担当者と協議の上決定する。

※月次報告書については各翌月 15 日までに提出すること。
但し、2026 年 3 月分の月次報告書については、2026 年 3 月 31 日までに提出すること。

12. 履行期間、納入期限および納入場所

履行期間：契約日～2026 年 3 月 31 日
納入期限：2026 年 3 月 31 日
納入場所：茨城県つくば市梅園 1-1-1
国立研究開発法人産業技術総合研究所
マテリアル DX 研究センター
つくば中央事業所　第 2 群　2-1D 棟 715 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事項

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 提供する資料は産総研担当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、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 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。
⑫ 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。
⑬ 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。
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 セキュリティに十分配慮した設計を行い、利用権限のない者が不正にアクセスし、データを閲覧・更新等できない設定、構築を行うこと。
⑯ 本業務の履行において、セキュリティの脆弱性が発見された場合には、対応内容について産総研担当者と協議し、必要に応じて速やかに対応すること。
⑱ ユーザの不注意、故意等によってデータが失われることのないように保護対策を設けるなど、可用性の確保に十分配慮した対応を行うこと。
⑲ 本業務の履行において、該当する場合は、以下を含むアプリケーションの脆弱性を回避すること。
・SQL インジェクション

・OS コマンドインジェクション
・ディレクトリトラバーサル
・セッション管理の脆弱性
・アクセス制御欠如と認可処理欠如の脆弱性
・クロスサイトスクリプティング
・クロスサイトリクエストフォージェリ
・クリックジャッキング
・メールヘッダインジェクション
・HTTP ヘッダインジェクション
・eval インジェクション
・レースコンディション
・バッファオーバーフロー及び整数オーバーフロー

㉑ 本業務の履行において、暗号化機能又は電子署名を導入する場合には「電子政府推奨暗号リスト」に記載されたアルゴリズム及びそれを利用した安全なプロトコルを採用すること。また、暗号アルゴリズムが危殆化した場合の対策が講じられていること。

㉒ 本業務の履行において、管理する情報システムのログを点検又は分析を実施した結果、ログの異常を検知した場合には、産総研担当者に報告すること。

㉓ 本業務の履行において、管理する情報システムの不正プログラム対策を実施した結果、定義ファイルの更新失敗、またはマルウェア等を検知した場合には、産総研担当者に通知すること。

㉔ 受注者は、本業務の履行において、第三者のクラウドサービスを除く外部サービスを利用する場合、産総研が受注者に求めている情報セキュリティ対策と同等の対策の実施を、当該外部サービス事業者に課すこと。

㉕ 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。

㉖ 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

(1) 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。

(2) 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。

(3) 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。