仕　様　書

１．件名

フルポテンシャル KKR コードによる電気伝導度計算のための拡張機能の整備

２．研究の概要・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マテリアル DX 研究センター(以下、「産総研」という)では、科学研究費助成事業（学術変革領域研究（B））の一環として、フルポテンシャル Korringa-Kohn-Rostoker 法(KKR 法)とコヒーレントポテンシャル近似(以下、「FPKKR-CPA」という)に立脚したプログラムを中核にする電子状態シミュレーション・システムを用いて、遷移金属酸化物をベースとした機能性材料の電子物性、電子輸送と磁性を理論的に研究している。

FPKKR-CPA プログラムは小倉昌子氏（ルートヴィヒ・マクシミリアン大学ミュンヘン）が開発したものであり、調達請求者は使用許諾の権利を受けている。

今年度、FPKKR-CPA プログラムにさらに不純物や不規則性に起因する電子散乱と有限温度におけるフォノンおよびマグノン励起による電子散乱の効果を取り入れた線形応答理論に基づいて電子輸送を計算するための拡張機能を追加する。本機能により規則系・不規則系の有限温度での電子輸送を含めた電子物性の計算が可能となり、電子状態シミュレーション・システムの充実と予測デザイン能力が大きく強化される。特に、強相関スピントロニクス材料の材料設計に対して有力な手法を提供することとなる。

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。
その他	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。

３．プログラム開発内容

現在のプログラムは、2024 年度までの研究開発によって、FPKKR-CPA プログラムにより合金系を含む磁性体の第一原理計算に基づく電子状態や磁気特性の精密計算が可能になっている。

本件は、既存の FPKKR-CPA コードに「任意の温度における不規則性」、「フォノンおよびマグノン励起による電子散乱の効果を取り入れた線形応答理論に基づき電子輸送を計算する機能」を既存の FPKKR-CPA プログラム（FORTRAN 言語により記述）にサブルーチンプログラムとして追加する。それに伴うプログラムの変更、削除にはパッチファイルを作成し適用すること。

４．開発内容構成

(1)CPA と不規則局所モーメント（LMD）を用いて有限温度の効果（フォノン及びマグノン）を記述する機能

(2)Current matrix の計算機能

(3)散乱積分演算子の 2 乗項の計算機能

(4)Vertex correction 計算機能

(5)直流電気伝導テンソルの計算機能

５．プログラム追加仕様

(1)CPA と不規則局所モーメント(LMD)を用いて有限温度の効果(フォノン及びマグノン)を記述する機能の追加

(2)Current matrix の計算機能の追加

・フルポテンシャルに対応していること

(3)散乱積分演算子の 2 乗項の計算機能の追加

・フルポテンシャル及び有限温度に対応していること

(4)Vertex correction の計算機能の追加

・補正の有無を選択できること

(5)直流電気伝導テンソルの計算機能の追加

・直流電気伝導テンソルのエネルギー依存性を出力できること

６．プログラム作成の条件等

(1)プログラム作成使用言語及び動作環境等

・プログラム作成に使用する言語は Fortran とする。

・プログラムの動作環境は UNIX もしくは Linux OS とする。

(2)プログラム作成者の能力、要件等

・受注者は FPKKR-CPA プログラムの開発に際しその許諾を得ていること。またその開発に関して十分な知識、経験、業績があること。

・受注者は Fortran 言語に関して、十分な知識があること。

７．特記事項

・受注者は「５．プログラム追加仕様」に基づき、要求仕様書、設計書の作成を行うこと。また必要であれば調達請求者と協議の上で作成を行うこと。

・上記をもとに調達請求者の同意のもと、サブルーチンプログラム作成作業を行うこと。

・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。

８．完成品の試験・確認

調達請求者は、ドキュメントに記載されている操作手順を実際に実行するなどして、ドキュメント類の内容、品質を確認する。

①システムの完成度は、システムの取り扱い説明書に記載されている手順に従ってシステムを操作し、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を確認する。

②システムの品質は、プログラム検査仕様書（プログラムテスト計画書）、プログラム検査成績書（プログラムテスト結果報告書）により確認する。

９．納入の完了

本システムは、「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

(1)プログラム設計書	一式
(2)サブルーチンプログラムとパッチファイル	一式
(3)パッチを適用後のプログラム	一式
(4)プログラムテスト計画書	１部
(5)プログラムテスト結果報告書	１部

※上記(1)から(5)を、クラウドストレージ「BOX」を利用して納入すること。

１１．納入期限及び納入場所

納入期限：2026 年 2 月 27 日

納入場所：〒305-8568　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　つくばセンター中央事業所 2 群 2-1D 棟 614-2 室　マテリアル DX 研究センター

１２．成果の取扱い

(1)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（譲渡対価は契約金額に含まれるものとする。）、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、産総研に対し、納品した成果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、納品した成果品について、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。

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本業務の履行においては、十分な秘密保持を行うこと。

⑭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。

１４．付帯事項

・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。
・本プログラムのインストール作業は受注者側で行うこと。（若しくは、調達請求者側で行う場合は、支援を行うこと。）
・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。
・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。
・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。

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。