# 仕　様　書

1. 件名
超伝導量子コンピュータを用いた組合せ最適化ミドルウェアの開発

2. 研究の概要
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。）量子・AI融合技術ビジネス開発グローバル研究センターは、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の受託研究「量子・古典ハイブリッド技術のサイバー・フィジカル開発事業」の一環として、量子・AIハイブリッド技術の活用を加速する共通ライブラリ基盤の研究開発を実施している。
本基盤においては、量子・古典ハイブリッド技術の効果を実証し、それらを活用したユースケースを創出するため、量子ジョブと古典ジョブが密接に連携するアルゴリズムを効率的に実行する仕組みが必要である。そこで、量子コンピュータと古典コンピュータの両者を協調的に扱うことのできる量子・AIソフトウェアスタックの研究を行っている。

3. 本開発作業の背景
産総研が整備を進めている量子・AI 融合計算基盤（以下、「ABCI-Q」という。）は、大規模 HPC システム（以下、「システム H」という。）と、超伝導量子コンピュータ（以下、「システム F」という。）等の複数種類の量子コンピュータから構成される。量子・古典ハイブリッド技術の有効なユースケースの一つとして組合せ最適化問題がある。Fixstars Amplify は、組合せ最適化問題をイジングマシン、数理最適化ソルバ、ゲート型量子コンピュータ等を利用して解くことができるミドルウェアである。ABCI-Q では Fixstars Amplify を導入しているが、現時点でシステム F には対応していない。本件は、Fixstars Amplify SDK からシステム H を用いて組合せ最適化問題を求解する仕組みを開発するものである。
「ABCI-Q 利用者による組合せ最適化プログラム実行時のシステム全体の処理フロー」の流れを図１に示す。ABCI-Q の利用者は、システム H で Amplify SDK 及び Python を用いて記述された組合せ最適化プログラムを実行する。Amplify SDK は、そのロジックを OpenQASM 形式の QAOA プログラム（以下、「量子プログラム」という。）に変換し、REST サーバ経由でシステム F に実行要求する。システム F は量子プロセッシングユニット（QPU）と制御サーバから構成される。制御サーバは REST サーバをポーリングし、実行依頼された量子プログラムをトランスパイル後、QPU 上で実行する。その結果を REST サーバに送信し、データベースに格納する。なお、REST サーバは OQTOPUS Cloud[1]をベースとして実装している。

[1] https://oqtopus-cloud.readthedocs.io/latest/

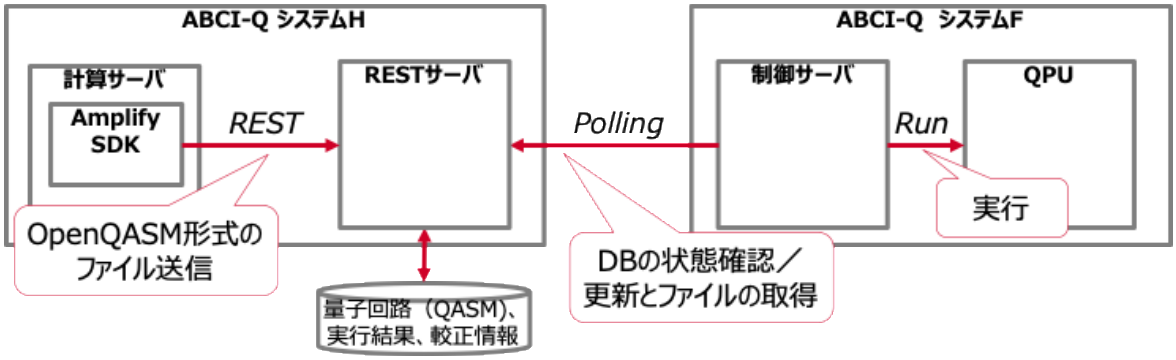


図１

4. 作業項目

Amplify SDK に以下の機能を追加すること。

（１）Amplifyのサブモジュールであるamplify qaoaからシステムFを呼び出すことを可能にすること。具体的には、OpenQASM形式のQAOAプログラムの実行をREST API経由でシステムFに要求し、結果を取得できること。

（２）追加機能はAmplify QAOAパッケージの拡張、もしくはAmplify SDK本体とは独立したパッケージ等の形態とすること。

（３）動作を確認するためのサンプルプログラムを2件以上納入すること。Fixstars Amplifyホームページのデモ＆チュートリアル[2]等、既存のソースコードを用いても良い。

（４）ABCI-Q利用者向け手順書の作成。なお、ABCI-Qのホームページに掲載することを想定し、日本語と英語版をMarkdown形式で作成すること。

5. 特記事項

（１） 業務の実施環境

① Linux 系 OS、および量子計算フレームワークが標準で対応するプログラミング言語（Python、C/C++等）を用いること。

② ABCI-Q のアカウントを貸与する。また、利用料は産総研が負担する。

③ 調達請求者と作業実施要員とで、定期的にコードレビューを含む打ち合わせを行う。頻度は 2 週に 1 回程度を予定している。開催頻度は調達請求者と協議の上で決定すること。

④ 開発や試験の必要性に応じて商用クラウドを利用する場合は、調達請求者と協議の上実施すること。ただし、商用クラウドの利用料は受注者が負担すること。

⑤ 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。

[2] https://amplify.fixstars.com/ja/demo

（２） 要員等の能力、要件

① Fixstars Amplifyもしくは同等の量子コンピューティングミドルウェアのシステム開発や運用に関する業務実績があること。
② 高性能計算システムを用いたアプリケーションやミドルウェアを開発した業務実績があること。
③ REST APIを用いたウェブサービスを開発した業務実績があること。
④ 情報セキュリティに関して十分な知識を有し、開発作業の機密性を十分に担保し情報提供を行えること。
⑤ 受注者は品質マネジメントシステムISO9001の認証を有すること。
⑥ 英語および日本語いずれのマニュアルも判読して作業を行えること。

6. 貸与品

（１）ABCI-Q アカウント（システムH、およびシステムF） 要員分

7. 完成品の試験・確認

納入前に、動作確認試験に係る試験仕様書を調達請求者に提出し、承認を得ること。その後、動作確認試験を実施し、その結果を動作確認試験報告書として提出すること。なお動作確認試験報告書には、試験仕様書を含めること。

8. 納入物品

ソースコード、ドキュメント類は電子データとして作成し、調達請求者が指定するファイル転送サービス等を用いて納入すること。

| | |
|---|---|
| （１）開発物のソースコード | 一式 |
| （２）ABCI-Q利用者向け手順書 | 日本語版、英語版1部ずつ |
| （３）動作確認用サンプルプログラム | 2件以上 |
| （４）動作確認試験報告書 | 1部 |

9. 納入の完了

作業完了後、「8.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。

10. 納入期限及び納入場所

納入期限：2026年2月27日（金）
納入場所：〒135-0064 東京都江東区青海2-4-7
国立研究開発法人産業技術総合研究所
量子・AI融合技術ビジネス開発グローバル研究センター
臨海副都心センター 別館（バイオ・IT棟）5階5203室

11. セキュリティ要件

・情報セキュリティポリシーに関する要件

（１）本業務の履行に当たっては、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。なお、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。

・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、速やかに返却または廃棄し、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）本業務の履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、定期的に情報セキュリティ対策の履

行状況を報告すること。

（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）本業務の履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。

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。

（２） 受注者は、成果に係る著作権（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。

（３） 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. 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こと。

（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）納入されたプログラム等における発注者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

## 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。