

(d) 量子暗号技術

研究責任者：藤原 幹生（国立研究開発法人情報通信研究機構 量子 ICT 協創センター 研究センター長）

参画機関：国立研究開発法人情報通信研究機構、日本電気株式会社、株式会社東芝、学習院大学、北海道大学、東京大学、株式会社 ZenmuTech

1) 研究内容

研究開発の全体像：

量子暗号は、どんな計算機でも解読できないことを証明できる現在唯一の暗号通信技術であり、重要デジタル情報の通信を保護する手段として期待される。しかし、既存の暗号技術に比べて割高であり暗号装置市場での競争力が低く、推奨標準の整備が遅れているなどの課題がある。また、量子暗号自体は通信の安全性を保証するものでデータ保存の安全性までは保証できない。そこで、市場競争力のある装置開発や標準化の取り組みを進めるとともに、量子暗号技術と従来から利用されている重要デジタル情報を安全に保管する手段としての秘密分散手法を組み合わせることで、理論上、将来にわたり機密漏洩を完全に防ぐデータ保管を初めて実現する。実施体制を図 2-4-1 に示す。

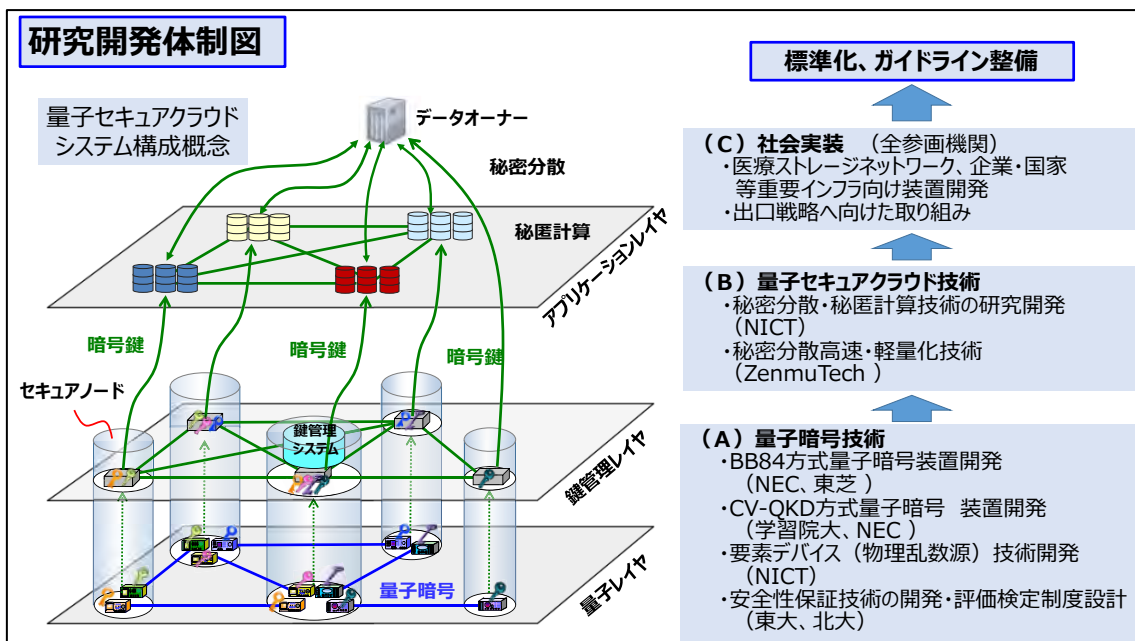


図 2-4-1. 研究開発の概要と実施体制

具体的な実施計画 (内容)：

A) 量子暗号技術

量子暗号には、使う検出器のタイプに応じて、BB84 方式^{*1} と CV-QKD 方式^{*2} という 2 つ

の方式があり、本研究開発では、両方式を使用して研究開発を行う。

BB84 方式は、現在、一部の部品を海外から調達して製造しているため、部品から装置製造までの国産化を目的として、高い鍵配送性能を維持した上で、部品の集約、モジュール化、ソフト化及び市販品の活用等により、市場競争力のある量子暗号装置を開発する。BB84 方式については 2020 年度までに事業化の目途を得たことで、ガバニングボードより SIP の最終年度を待たずに目標を達成したと判断されたため、2021 年度以降、小型化・低コスト化に関する項目については本プロジェクトの所掌範囲外となった。

CV-QKD 方式を使用しての研究開発では、大学－企業間連携により、企業へ CV-QKD 技術の移転を図るとともに、雑音耐性と光多重度を向上させ、さらにユーザー環境で安定かつ高信頼動作させるための技術開発を行い、研究試作品を完成させる。

また、両方式に共通の課題となっている下記の事項についても、研究開発を進める。

i) 安全性保証技術の標準化

量子暗号の情報理論的安全性を実環境で保証するために、基礎理論、実験、対策実装、検証のサイクルを継続的に実施し、耐タンパー対策やサイドチャネル攻撃対策を実装する。これらの取組みを着実に実施し、安全性保証技術の継続的な高度化を行い、順次標準化する。

ii) 物理乱数源の小型化

量子暗号の鍵生成の根幹となる物理乱数源について、高速化するとともに、量子暗号装置内での占有体積を従来比 2 分の 1 まで小型化する。

iii) 検定基準・推奨方式リストの整備

メーカーが適正な物理乱数源、量子暗号装置を製造・販売し、ユーザーがそれらを安心して利用するためには、検定基準や推奨方式リストの整備が必要となる。我が国には、まだその体制が無いため、将来の運用に向けた予備調査と運用に必要な基礎データの蓄積、エコシステムとして機能する制度設計提案を取りまとめる。

※1 BB84 方式

光の粒である光子を検出するための単一光子検出器を用いる量子暗号の代表的なプロトコル。物理法則が許すあらゆる盗聴攻撃、あらゆる計算能力を持つ計算機でも解読不可能なことが証明されている。以前より最も研究開発されてきており、現在、企業が試験稼働させている方式である。あらゆる盗聴の可能性を完全に排除する必要がある安全保障分野等のハイエンド用途が想定される。

※2 CV-QKD 方式

光の位相・振幅を検出するホモダイン検出器を用いる量子暗号のプロトコル。通信路への攻撃手法があるクラスの物理操作に限定されるが、その攻撃も当面の技術では実装が極めて困難であり、かつあらゆる計算能力を持つ計算機でも解読できないことが証明されている。光通信用の光ファイバー内でも、共存して動作可能であるため、既存光通信インフラへの適用が期待できるというメリットがある。BB84 方式よりも低コストでの開発が可能であるため、主に民生のハイエンド用途が想定される。

B) 量子セキュアクラウド技術

量子セキュアクラウド機能を実現するため、秘密分散技術、物理乱数源・量子暗号技術、電子署名・認証技術、秘匿計算技術を統合する。その際、量子セキュアクラウド機能を実現するためには、処理量の爆発的増加への対処と暗号鍵の非可逆性の担保が不可欠である。これらの解決に向けて、高速かつ軽量の秘密分散・秘匿計算技術と暗号鍵管理を統合運用するための最適なミドルウェアアプリケーションインタフェースを開発する。

C) 社会実装

代表的なアプリケーションとして、医療情報ストレージネットワークや企業・国家等重要インフラ網などを想定し、これらの分野の潜在ユーザーと連携しながら、社会実装を進める。

特に、それぞれの用途で扱うべき情報資産を、機密性の度合い、データサイズ、利活用の頻度等の観点から分類・優先付けし、ユーザーが必要とするデータに適時にアクセスし必要な処理やデータ復元が可能なアプリケーションを開発する。また、データ保管の際には、異なる組織間でもデータを相互参照できるよう、共通のデータフォーマットに変換するゲートウェイ機能も開発する。

国家等重要インフラ網を扱う潜在ユーザーとの連携を強化し、量子暗号装置の安全性・信頼性を向上させて国際市場競争力・ブランド力を高める。

民生分野でのビジネス拡大に向け、国民一人一人に係る医療情報分野や生体認証分野において、潜在ユーザーとの連携による量子セキュアクラウド技術の実証試験を加速する。特に、医療情報分野での POC では、量子暗号の要素技術と組み合わせた共通鍵暗号と、量子暗号をニーズ/導入コスト要件に応じて選択できるシステム設計や医療従事者のアクセス制御・管理機能の実装などを進め、現場ニーズへの適応性を高めつつ高秘匿通信サービスの導入モデルを確立する。「国家レジリエンスの強化」など SIP の他課題とも連携し、社会実装の多様化を図る。

これらの成果をもとに、プログラム内のレーザー加工および光電子情報処理のチームと連携しながらスマート製造分野への適用試験を進めビジネスモデルを構築する。特に、既存のアクセス系の光ファイバーを利用した実装が可能で、光ファイバー利用料や装置コストの低減を可能とする CV-QKD 装置を用いて POC に取り組む。

さらに、金融分野の潜在ユーザーと共同で調査研究を進めユースケースを設定し、ユーザーと共同で実証環境を構築して金融アプリケーションによる POC を実施し、量子暗号の導入による金融セキュリティの強化モデルの導出と有効性確認を実施する。

上記の社会実装の取り組みをさらに広範な用途へ普及させるために、本格的なインフラ化に向けて通信事業者とも連携を強化し、コンソーシアム活動なども活用しながらビジネスエコシステムのモデルを提案する。

2) 技術的目標 (計画)

事業終了時点アウトプット目標 (2022 年度の目標)

A) 量子暗号技術

- ・ CV-QKD 方式装置に関して、企業による準製品化 (ユーザー環境で稼動可能な研究試作品) を完了し、100 波の古典光が多重化された同一ファイバー内での鍵生成を実証する。
- ・ 安全性保証技術に関し、実装安全性評価や鍵管理など主要な作業項目について、量子 ICT フォーラム/量子鍵配送技術推進委員会や ITU-T、ISO/IEC や ETSI 等の国際標準化組織から勧告を発行する。
- ・ 物理乱数源に関して、現状比 10 倍の高速化 (生成速度～数 Gbps) かつ従来比 2 分の 1 の小型化 (量子暗号装置内での占有体積を半減化) を実現し、企業へ技術移転を達成する。
- ・ 量子暗号の運用ガイドライン及びセキュリティ設計仕様案を完成する。
- ・ 物理乱数源、量子暗号技術の安全性保証、検定基準、推奨方式リストの策定と更新を継続的に行うための制度設計提案書を取りまとめ、標準化関係省庁へ提案を実施する。

B) 量子セキュアクラウド技術

- ・ 秘密分散・秘匿計算の軽量化技術、鍵管理・運用技術、ユーザー権限に基づくアクセス権管理技術を統合するアプリケーションをフィールドテストベッド上にプログラム実装するとともに、データの属性 (種類・意味、機密性の度合い、データサイズ、利活用頻度等) に応じた安全なデータ二次利用技術を開発し、80GB 程度のゲノムデータ解析に適用して有効性を検証する。
- ・ 電子カルテの日々のトランザクションストレージ、長期間の標準化ストレージ、異なる病院間での安全なデータ相互参照を可能とするシステムを開発する。災害時等、ネットワーク品質の劣化を想定し、1Mbps 程度の比較的低容量の回線が含まれるネットワーク環境でも迅速なデータ復元・相互参照機能を支障なく実行するアプリケーションを開発し、H-LINCOS 上で動作を検証。開発したアプリケーションをフィールドテストベッド上でオープンソース化する。

C) 社会実装

医療情報ストレージネットワーク分野と企業・国家等重要インフラ分野において、都市圏スケールの分散ストレージネットワークにおいて、想定ユーザーと共に実施した POC の成果を反映し、運用ユーザー拡大のためのビジネスエコシステムのモデル構築を完了する。

以下に 5 年間の工程表を示す。

研究開発項目	2018年度計画	2019年度計画	2020年度計画	2021年度計画	2022年度計画	出口戦略	製品化
(研究開発項目2)光・量子通信							
①量子暗号技術							
1) 量子暗号技術	TRL2		TRL4		TRL7		
BB84方式 (超高速専用線向け)	●耐タンパー・低コスト化のための試作課題対策/仕様策定の完了	●耐タンパー性を保証しつつ部品調達コストを従来比で半減化	●自社内サービスプラットフォームへの適用と1か月連続稼働試験の完了	●量子暗号装置の保守運用技術の確立とガイドライン作成	●運用ガイドライン及びセキュリティ設計仕様書を作成	政府機関・医療等の重要通信インフラへの導入へ向け、事前営業活動により開発完了から普及へシームレスに移行 ・マーケティング (~2019) ・ビジネス可能性検証 (~2020) ・運用ノウハウ蓄積、啓蒙 (~2022) ・QKD普及開始 (2023頃~)	BB84方式によるQKD装置の実用化 (2021~) 達成 CV-QKD方式によるQKD装置の実用化 (2025~)
CV-QKD方式 (既存光回線秘匿化向け)	●準製品化のための要件定義と主要部品の選定完了	●光学系及び制御装置の試作と動作検証 ●基本設計の完了	●プロトタイプ試作 ●商用回線環境での動作実証	●部品手配、製造 ●試作評価/検証 ●準製品化装置の試運転、安定性と耐障害性テストの完了	●準製品化完了 ●通信キャリア商用回線での稼働試験 ●200kbps@10kmを実現		
要素デバイス技術	●物理乱数源の高速度化検討 ●光子検出器等のサブライチエーン検討	●物理乱数源の高速度化実装 ●部品ベンダーの調査	●物理乱数源の現状比10倍高速化 ●部品ベンダーとの交渉	●物理乱数源の小型化 ●部品サプライチェーン構築	●小型高速の物理乱数源の企業への技術移転 (サイズ:従来比2分の1、速度:現状比10倍) ●部品サプライチェーンの確立		
安全性保証技術、評価検定制度	●安全性評価項目の網羅的リスト作成 ●評価手法の開発 ●EITSにてAPI標準化方針の含意形成 ●量子鍵配送技術推進委員会の活動開始	●評価手法の実機検証 ●評価基準の更新手法確立 ●EITSにてAPIの標準化達成	●安全性保証基準書を作成し(社)量子ICTフォーラム等に技術文書として提案 ●EITSとの連携調整 ●ISO/IEC、ITU-Tへの寄書提出	●社会実装の結果を踏まえ、評価検定制度、推奨方式リストのドラフト作成、(社)量子ICTフォーラム等との調整を継続 ●評価、検定制度のモデル提案	●実機の安全性保証評価の達成 ●国内外の標準化組織より勧告の発行 ●制度設計提案書の作成、及び関係省庁・機関への提案		

BB84方式についてGBの判断では令和2年度まで達成とし、以降小型化・低コスト化に関する項目については本プロジェクトの所掌範囲外とする。

研究開発項目	2018年度計画	2019年度計画	2020年度計画	2021年度計画	2022年度計画	出口戦略	製品化
2) 量子セキュアクラウド技術							
	TRL3		TRL5		TRL7		
量子暗号鍵管理と高効率秘分散の統合設計	●量子暗号鍵管理と高効率秘分散の統合設計指針の確立 (使い捨て鍵管理、データ機密性、利用頻度に応じた高効率アクセス法) ●秘分散の軽量化手法の検討 (安全性・速度パラメータに関する複数候補の比較評価)	●100km圏量子暗号ネットワーク上での高効率秘分散の実装、基本機能検証 ●秘分散の軽量化方式の試作と様々なデータによる性能比較評価、最適方式の選定完了	●10Mbps以上の速度での秘分散機能検証を完了 ●電子カルテ等模擬テキスト情報の高速秘分散の実証 (320MBのデータを標準ストレージに3時間以内に格納)	●ゲノムデータTB級のデータに対し50Mbps以上の速度での分散ストレージの実証 ●秘分散ネットワーク上に秘分散機能およびデータフィルタリング機能を実装	●秘分散・秘分散計算、鍵管理技術、アクセス権管理技術のフィールドテストに実装ゲノムデータ解析(80GB)に対しての有効性を検証 ●災害時等1Mbps程度の低容量回線を用いても支障なく電子カルテデータの相互参照を実証	1) 量子暗号技術、2) 量子セキュアクラウド、に同じ出口戦略 政府機関・医療等の重要通信インフラへの導入へ向け、事前営業活動により開発完了から普及へシームレスに移行 ・マーケティング (~2019) ・ビジネス可能性検証 (~2020) ・運用ノウハウ蓄積、啓蒙 (~2022) ・QKD普及開始 (2023頃~)	量子セキュアクラウド技術のアプリケーションを製品化 (2025~) QKD装置量産化 (2025~)
3) 社会実装	●秘分散情報の分類と要件定義の完了 (種類、サイズ、優先度、利用頻度等) ●ゲノム解析データリアルタイム伝送の実証 (10km圏)	●SS-MIX等の標準化医療データ向けのアプリケーションの設計、試作 ●ゲノム情報の秘分散システムの構築 (3拠点、10km圏)	●10km圏3拠点ネットワーク上でのゲノム解析データの50Mbpsでの秘分散の実装 ●800km圏の電子カルテ秘分散保管システム(H-LINCOS)のD24Hと接続 ●100km圏ネットワークでのカルテデータ、生体認証用データの分散保管の長期安定性実証	●数10GBのSS-MIX準拠電子カルテ検索データの2Mbpsでの高速秘分散 ●HPKI準拠のアクセス制御の構築、顔認証と連動した多要素認証の実証 ●レーザー加工関連の重要データの秘分散の実現と連続稼働 ●金融業界での取引で使用されているプロトコルの実装と暗号化伝送	●ゲノム/医療分野や製造分野等での試験運用を継続 ●ビジネスモデルの構築、用途拡大、ユーザーに向けた営業活動		
医療ストレージネットワーク、企業・国家等重要インフラ		●レーザー加工プラットフォームとの連携					
レーザー加工ソリューションとの連携		●レーザー加工プラットフォームへの導入に向けた基礎検討と要件定義					
出口戦略へ向けた取り組み	●潜在顧客向けマーケティング活動、デモ ●製造、評価、検定のエコシステム化検討						
民間からの出資 (人材、物資、資金等)	(30%程度)	(35%程度)	(50%程度)	(50%以上)	(50%以上)		

3) 課題目標の達成度 (成果)

① 国際競争力

図 2-4-2 に欧米中とベンチマーク実施した結果を示す。参画機関の(株)東芝、日本電気(株)が開発している量子暗号装置は、海外製品と比較して同じ距離での鍵生成レートが 10 倍、配送可能距離も 2 倍程度の性能を実現している。性能が桁違いで高いことは EU における Open testbed Graz においても検証されている。そこで、装置単体の価格ではなく、価値・課金の源泉である鍵ビット単価を海外製品と比較すれば、1/10 を達成することが期待できる。言い換えれば鍵ビット単価に換算したサービス価格競争力は海外勢の 5~10 倍を持つとみなすことができる。

現在は、市場展開とその規模でスイスの ID Quantique が先行している。また運用ネッ

トワークの規模では中国が 4,600 km 網（日本の 40 倍）の規模で展開しており、我が国より進んでいる。しかしながら日本は 2022 年度に装置製造コストを従来比 1/4 まで低減し、サービス価格競争力をさらに向上させることで、市場シェアの挽回が可能と考える。また米中摩擦の影響で中国製品は西側市場への参入障壁があるため、今後の新たな市場展開において我が国の量子暗号製品には十分な商機がある。

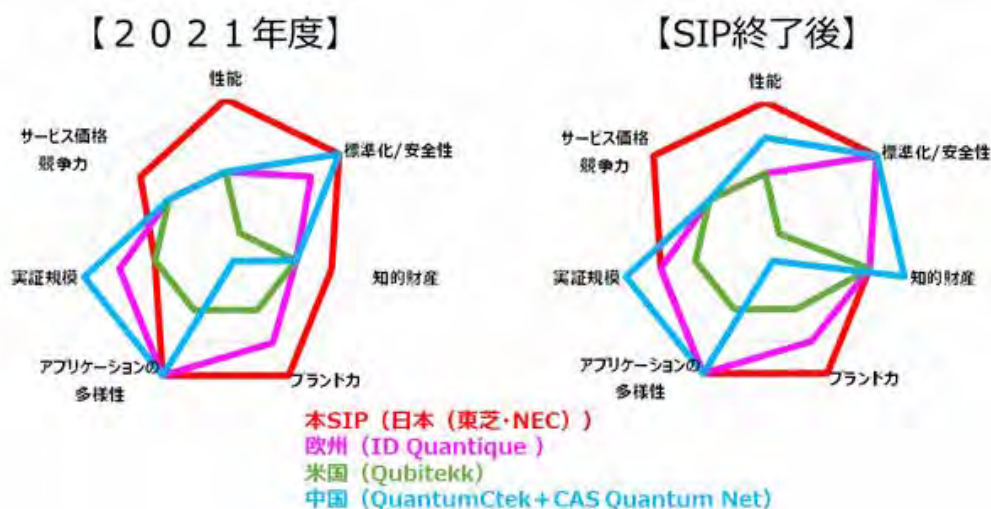


図 2-4-2. 欧米中との量子暗号装置のベンチマーク

② 研究成果で期待される波及効果

光・量子通信における研究開発の成果は、特に情報を秘匿し、安全に通信することが求められる医療分野、生体認証分野、製造分野、金融分野、安全保障分野など様々な分野に恩恵をもたらすと期待される。医療分野では電子カルテの管理・運用を、生体認証分野ではアクセス管理上の重要な個人情報、製造分野では企業秘密を、金融分野では顧客取引データを、安全保障分野では外交・防衛などの情報を取り扱う際に、光・量子通信の成果を活用することが想定される。現在、量子暗号技術のみならず、その要素技術を用いてセキュアな VPN を構築し、現行システムのセキュリティを強化するという極めて実用に近い実証から、遠隔手術等の安全かつ低遅延通信の実現などの中長期にわたる応用まで、様々なフェーズでの共同実証が進捗している。また上記分野でインフラ構築に必須となる通信キャリアとの連携にも着手し、量子暗号に関するビジネスモデルの構築に向け議論も進めている。また、強力な計算エンジンを量子セキュアクラウド内に取り込み、データの安全な二次利用を可能とすること、さらには昨今の個人情報を域内でのみ利用する方向での各国での法整備を利用し、安全なデータベースとしてのプラットフォームとして期待される。その有効性は、ゲノム解析での実証やレーザー加工チームと次世代アクセラレータとの組み合わせた POC で実証した。さらに量子暗号の POC に関する共同実証の申し出などを多数頂いており、光・量子通信の成果活用への期待が高いと考えている。

③ 達成度（１）※5年間の設定目標に対する達成度

量子暗号・量子セキュアクラウド・社会実装について、その達成度について以下に記述する。過去4年間及び最終年度の達成目標に対する達成度は以下の通りである。

(A) 量子暗号技術

- ・BB84装置の製品化が完了したため、SIPを円満卒業した。低コスト化実装が可能なセルフホモダイン方式であるCV-QKD装置はA方式、B方式とも、古典通信との共存動作が可能であることも確認した。また、A方式では短時間の受信信号から安全鍵生成速度を見積もり、207kbps@10kmであることを確認し、B方式では装置の光学系を簡略化した評価系において短時間の受信信号から安全鍵生成速度を見積もり、2.84Mbps@10km、600kbps@20kmを確認した。いずれも目標とする鍵生成速度（A方式：200kbps@10km、B方式：2Mbps@10km、200kbps@20km）を達成した。さらに、ユーザー環境で稼働可能な研究試作品を製作し、準製品化が実現できる事を確認した。
- ・物理乱数源の高速化（生成速度4Gbps）と従来比1/2の小型化を2021年度に実現し、企業への技術移転も完了し、目標を達成した。
- ・ITU-Tにおいて、日本の技術を骨格とする11編の標準勧告体系の整備を完了し、ETSI、ISO/IECでは、装置の評価・検定・認証に向けた規格作りに主導権を取りながら推進し、2022年度内に日本版Protection Profileの事前評価を完了した。
- ・別の国家プロジェクトにおいても本SIP光・量子課題で培われた技術を用いて、量子暗号技術の実証環境による評価が進んでいる。その活動を通じ、想定ユーザーの協力を得て量子暗号の運用ガイドライン及びセキュリティ設計仕様を完成させ、目標を達成した。
- ・物理乱数源の乱数性はあらゆる暗号技術のトラストアンカーといえる。それに対し、すでにNISTが先行してクライテリアを設定しているSP800-90Bの妥当性を検証するとともに、本SIP光・量子課題で開発した高速量子物理乱数源がSP800-90Bで求める性能を満たしていることを確認した。また本SIP光・量子課題で開発した高速量子物理乱数源を民間企業に技術移転し、製品化に向けた活動が開始されており、目標を達成している。

(B) 量子セキュアクラウド技術

- ・秘密分散技術、鍵管理・運用技術、アクセス管理技術が完成し、(株)東芝による80GBゲノムデータの高速分散バックアップのデモに成功しており、目標を達成した。
- ・秘匿計算技術とデータ2次利用技術の開発、及びゲノム解析での検証を京都大学の協力の下で進め、Tokyo QKD Network上に実装したシステムにおいて、ゲノム解析結果に対し、研究に不必要な個人情報をフィルタリングできる機能も実装した上で400Mbps以上のスループットを実現し目標を達成した。いわゆる信頼できるサーバーを想定した秘匿計算の実現であり、全ゲノムデータのような大容量かつ非構造化データを高効率に実施できるコンセプトとなっており、量子セキュアクラウドの高機能化に成功した。(図2-4-3)本成果は2022.11 Scientific Reports誌にて発表し、2022.11.17にプレスリリースも実施した。

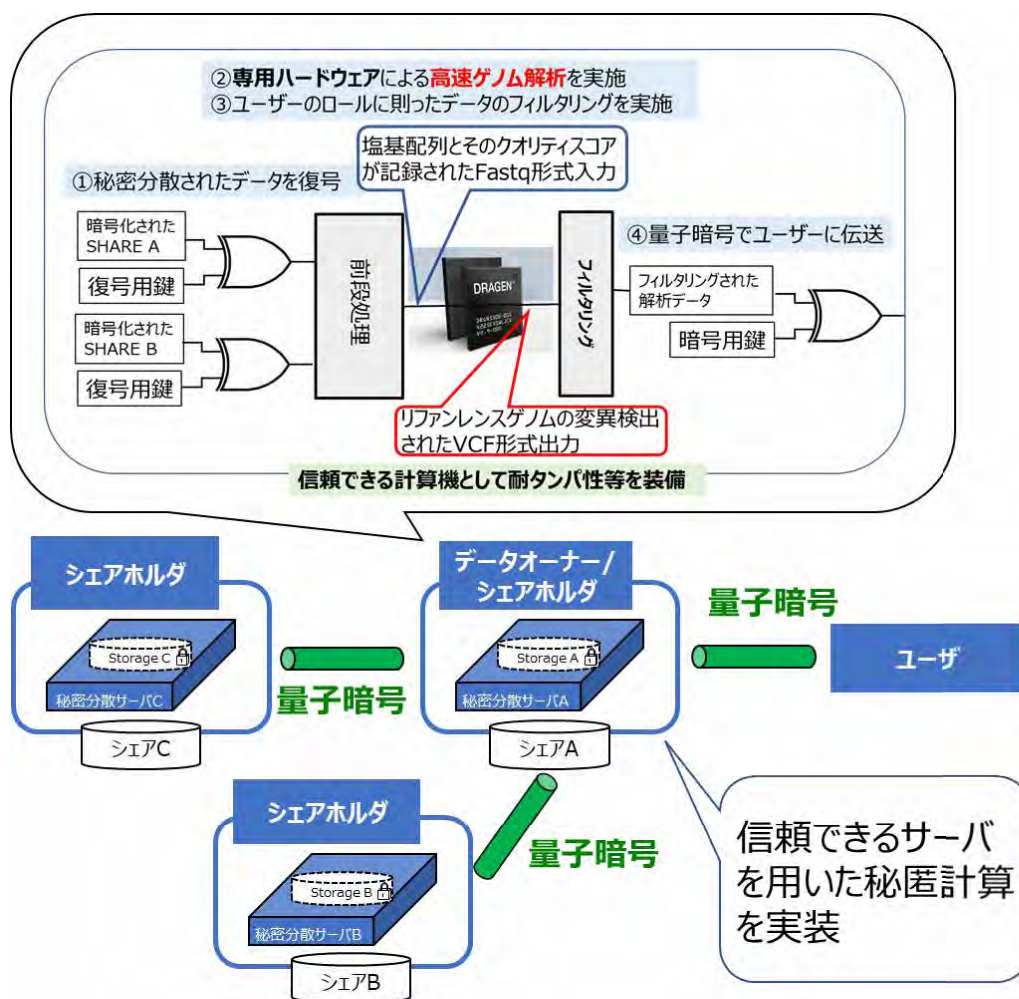


図 2-4-3. 信頼できるサーバを用いたゲノム解析用秘匿計算実装

・東京都内公的医療機関（系列 6 病院）のトランザクションデータ 320MB を 15 分以内で更新を実証した（2020. 10 プレスリリース）。また、世界初となる米国政府機関選定の耐量子計算機暗号を IC カードシステムに実装する技術を確認し、H-PKI 準拠のカードシステムにおいてデモに成功した（凸版印刷と共同 2022. 10. 24 プレスリリース）。さらに、本 SIP 光・量子課題間連携において、秘密分散のファイルシステム（ソフトウェア）を SIP AI ホスピタルチームが取り組む医療 AI プラットフォームの“AI 開発基盤”における安全なデータ伝送に応用することができた。

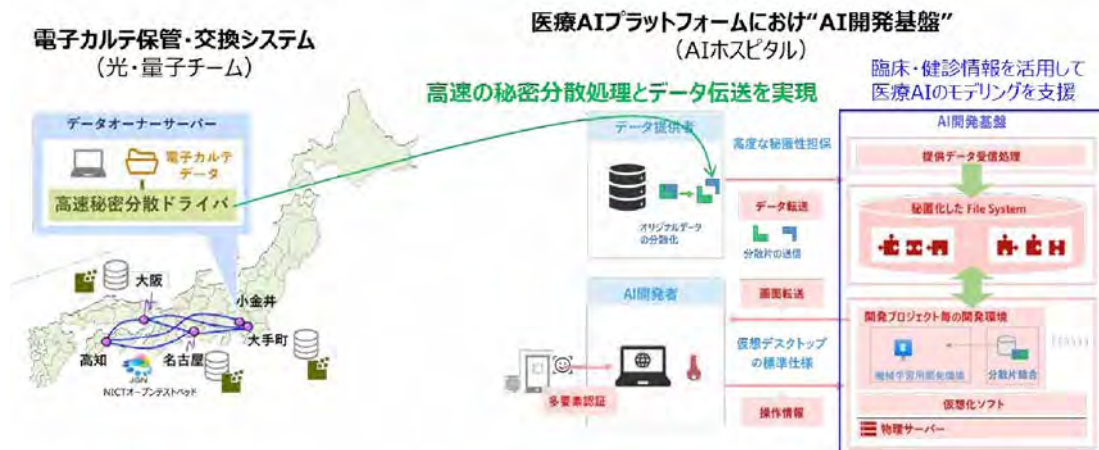


図 2-4-4. SIP 課題間連携 “AI ホスピタル” における高速の秘密分散処理とデータ伝送に応用

(C) 社会実装

電子カルテデータやゲノム解析データを扱う医療情報分野、および生体認証分野、スマート製造分野、金融分野等の重要インフラ分野において都市圏ネットワーク上での社会実装を着実に進めている。生体認証に関しては日本代表選手を有するスポーツ団体のカルテ情報の保護に活用し現在も稼働中である。また、金融分では野村証券・野村 HD とともにパフォーマンステストを継続実施中であり、様々な機関から注目を集めている。

さらに量子 ICT フォーラム等の産学官連携体制を積極活用し、ビジネスモデルの構築も進捗している。本 SIP 光・量子課題の技術を用いた別プロジェクトで公官庁での評価も実施中であり、目標を達成した。

④ 達成度（2）※社会実装の実現可能性

【計画及びその進捗状況】

目指す社会実装のロードマップを図 2-4-5 に示している。以下そのロードマップに従って進めている各分野での POC の結果をまとめる。

- ・HPKI と親和性のある SS-MIX データの分散バックアップシステム構築と医療関係者と共同による有用性を確認した。
- ・量子セキュアクラウド上でのゲノムデータの保管および安全な二次利用の実施と、想定ユーザーとの有用性を確認した。
- ・金融分野での量子セキュアクラウド技術の有用性を想定ユーザーと共に検証した。
- ・スマート製造現場での量子暗号技術の有用性を想定ユーザーと共に確認した。

【体制整備状況】

- ・量子暗号チーム全体で POC 及び標準化活動を一体的に実施した。また SIP の課題間連携は国家レジリエンスの強化グループに加え、AI (人工知能) ホスピタルによる高度診断・治

療システムチームへの技術移転を実施した（図 2-4-4 参照）。また、他の国家プロジェクトも活用した国内でのサプライチェーンとテストベッドの充実が進行中である。

【社会実装と認められる成果】

- ・ 参画機関が BB84 方式の量子暗号装置を 2020 年度から事業化した。
- ・ 小型高速の物理乱数源の企業 (YDK) への技術移転が完了（サイズ：従来比 2 分の一、速度：現状比 10 倍）した。
- ・ 量子暗号通信の普及に不可欠な国際標準化活動において、本 SIP 光・量子課題活動期間（5 年間）を通じて 11 件の勧告を成立させた。
- ・ AI ホスピタルチームが取り組む医療 AI プラットフォームの“AI 開発基盤”に、光・量子通信チームから高速秘密分散ドライバ技術を提供し、高速の秘密分散処理とデータ伝送を実現した。
- ・ 電子カルテで HPKI への親和性のある SS-MIX データの分散バックアップシステム構築と医療関係者と共同での有用性確認を完了し、HPKI 準拠のカードに耐量子公開鍵暗号を世界で初めて実装し、その成果を 2022. 10. 24 にプレスリリースを実施した。
- ・ ゲノム解析データの社会実装に関し、量子セキュアクラウド上でのゲノムデータの保管および安全な二次利用の実現と想定ユーザーと共同で有用性を確認し、個人情報保護しつつ全ゲノム解析を可能とするシステムを完成させた。その成果を論文発表 (Scientific Reports 誌 図 2-4-3 参照) するとともに 2022. 11. 17 プレスリリースを実施した。
- ・ 金融分野での量子セキュアクラウド技術の有用性を想定ユーザーと共に検証し、Q-STAR に QKD の普及に向けた提言書を提出し、2 度の講演依頼を頂いた。

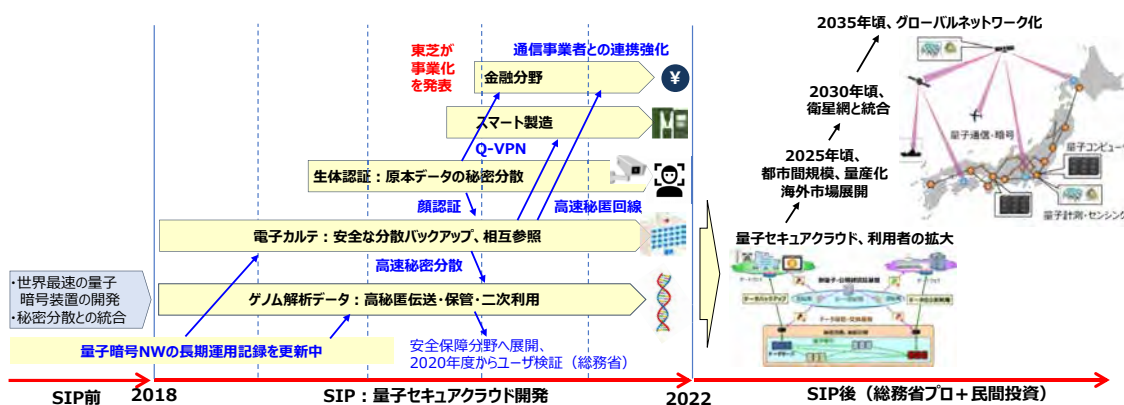


図 2-4-5. 社会実装のロードマップ

⑤ 知財戦略、国際標準化戦略、規制改革等の制度面の出口戦略

2017 年付近から中国等の出願が急増しており、出願件数での日本の優位性は担保されなくなっている。しかし、そのための挽回戦略として、国際標準化戦略に基づく知財戦

略、open/close 戦略を確実に推進し、国際市場での競争優位性を早期に確保する。具体的には、侵害検知可能な項目を特許化する一方、QKD モジュールの評価項目の国際標準化を進めつつ、評価法のノウハウは非公開とする。一方、事業化に係る知財戦略については、個社別に強化する。現在、各参画機関では多様な POC を通じて偏りの無い実装技術の充実を図っており、周辺分野の応用技術を生かした市場拡大を目指している。

国際標準化戦略の活動成果として、2022 年度は、11 月現在、標準化会合参加回数 14 回（ITU-T: 7 回、ESTI: 7 回）、のほか、22 編の寄書を提出した。図 2-4-6 に示すように、5 年間の活動では 178 編の寄書を提出し、11 件の標準化発刊、アクセプトに結実させ、量子暗号ネットワークの国際標準化を推進し、日本の技術を骨子とする基本勧告体系の整備と、量子セキュアクラウドの標準化に貢献した。

一般的に暗号技術の普及のためには認定制度やガイドラインの整備と、導入による利用者のメリットを設定し、導入インセンティブを向上させる必要がある。それを実現するためには公平性・公共性のある機関による検定制度と、量子暗号・量子セキュアクラウド利用についてのブランドイメージを醸成し、利用者メリットとして成長させることが重要である。現在、(一社)量子 ICT フォーラムや TTC(情報通信技術委員会)とも連携し、セミナー開催、省庁関係者を招いたブレインストーミングなどを実施し、国際標準化活動とも同期した運用ガイドラインの策定を進めている。また 2022.1 に(一社)量子 ICT フォーラム内に評価・検定・認証の準備組織を立ち上げた。

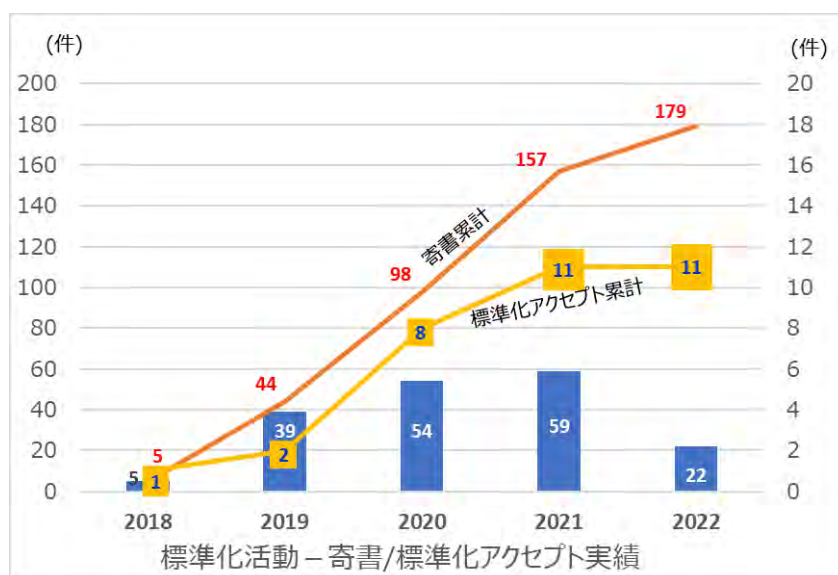


図 2-4-6. 5 年間の標準化活動状況(棒グラフは各年度の寄書数)

⑥ 成果の対外的発信

2022 年度はこれまでに、論文等 6 本、学会等 10 件の成果発表を行った。また、量子セ

キュアクラウドシステムを使った次世代レーザー設計の最適化の処理・高秘匿伝送・分散保管の実現（京都大学、慶應義塾大学と課題内連携）（2022. 10. 4）、HPKI 準拠のカードに耐量子公開鍵暗号を世界で初めて実装に成功（2022. 10. 24）、量子セキュアクラウドにゲノム解析専用装置を装備し、全ゲノムデータの安全な伝送・保管・解析をリアルタイムで実施できるシステムの開発（2022. 11. 17）、量子セキュリティ技術と個人認証を連携させたセキュアな個別化ヘルスケアユースケースの実証に成功（2022. 12. 8）についてのプレスリリースを行った。これら成果は新聞、電子メディア等でも報道された。

さらに、アウトリーチ活動の一環として春・秋の量子コンピューティング EXPO 展示会（2022. 5, 2022. 10）及び CEATEC 展示会（2022. 10）で成果展示を行った。

⑦ 国際的な取組・情報発信

先にも述べた通り、国際標準化活動においては、これまでに日本の技術を骨子とする基本勧告体系整備を完了した。また ISO/IEC や ETSI における装置安全性に関する会合において、2021 年度に世界トップとなる 40 編の寄書を出し、安全性保証技術の標準化においてもイニシアティブを取ると共に活動に貢献している。

国際的な取組みとしては、2021. 7 に US-Japan Quantum cooperation Workshop や EC-Japan Meeting on Quantum でパネリストとして発表や議論に参加するなどして、日本の取組を国際的にも紹介したほか、今後の国際連携推進などに関する議論に加わった。また 2021. 8 の Qcrypt2021 Industry Session 参加も踏まえ、2021. 12. 7~9 にオンラインで開催された国際シンポジウム QUANTUM INNOVATION 2021 を SIP 光・量子課題として共催し、SIP での活動成果を世界に発信した。2022 年度も同様に 2022. 11. 28~30 の QUANTUM INNOVATION 2022 を共催した。

このように国際的な取組や情報発信を積極的に実施している。さらに(株)東芝は、個社として本 SIP 光・量子課題で取り組んだ BB84 方式の量子暗号装置技術等を活かして、欧州、米州、韓国などで POC を展開するなど、実績作りを進めている。

(e) 次世代アクセラレータ基盤に係る研究開発

研究責任者： 戸川 望（早稲田大学 理工学術院 教授）

参画機関： 早稲田大学、株式会社フィックスターズ、株式会社 QunaSys 、慶應義塾大学

1) 研究内容

研究開発の全体像：

Society 5.0 の実現にはサイバー空間とフィジカル空間の高度な融合が不可欠であり、これを達成するには大規模かつ困難なデータ処理等、多くの計算ボトルネックが存在する。例えば、天文学的な多数の選択肢の中から「最適な答え」あるいは「準最適な答え」を瞬時に見つけ出すことが必要となる（組合せ最適化問題）。組合せ最適化問題は、ネットワーク型製造システムをはじめ自動運転、MaaS（Mobility as a Service：サービスとしての移動分野）等、Society 5.0 の実現に必要な多くの社会課題の解決にとって重要である。また、Society 5.0 の実現には、膨大なデータを高速・高精度に学習し、なおかつ学習結果に基づき、膨大なデータから実時間で推論する必要がある、機械学習の高速化・高度化も Society 5.0 の実現のために不可欠な構成要素となる。さらに、材料やエネルギーの領域においても、単純な性能追求だけでなく、環境負荷や資源枯渇などの社会課題への対応も求められており、トレードオフの関係にある場合には、これらの要求を高度に両立させることが必要となる。この実現のためには、これまでのような実験偏重・職人芸に頼った開発から脱却し、対象となるミクロな物理系をサイバー空間上でモデル化し、シミュレーションを通じて最適な解（分子構造や反応条件など）を導き出す必要性が高まっている。

こうした数多くの Society 5.0 実現に不可欠な計算ボトルネックの解決に期待されるのが、(1) イジング型コンピュータ（量子アニーリングマシンや古典技術を用いたアニーリングマシン）、(2) NISQ コンピュータ、(3) 誤り耐性ゲート型量子コンピュータと呼ばれる「次世代アクセラレータ」である。(1)～(3)の次世代アクセラレータは、既存の古典計算機と組み合わせることで、上述のような組合せ最適化問題の解法や機械学習、量子化学計算など古典計算機の計算ボトルネックを解消し、極めて高速・高精度にアプリケーションプログラムの実行が可能になると期待される。次世代アクセラレータを効果的に利活用することで、Society 5.0 の実現が加速する。

一方、Society 5.0 を実現するアプリケーションプログラムの特定部分に次世代アクセラレータを適用するには、(ア)アプリケーションプログラムから次世代アクセラレーションを呼び出すための入力データの準備、(イ)次世代アクセラレーションの実行、(ウ)次世代アクセラレーションからアプリケーションプログラムへの結果の受取り、の3段階より構成される。つまり、次世代アクセラレータの適用が優位となるのは、(イ)に要する時間に比較して、(ア)・(ウ)の時間が相対的に短く、また(イ)による効果（高速化や解の高精度化等）が期待される場合である。しかも、アプリケーションプログラムの特定部分の「動作」と、適用される次世代アクセラレータの組合せによって、(ア)・(イ)・(ウ)の時間ならびに動作

全体の精度は動的に変化する。

入力データの準備や出力データの取出しがいかに最適かつ効率的にできるかによって、次世代アクセラレータの適用の可否が変化することになる（次世代アクセラレータインタフェース技術）。Society 5.0の実現には、アプリケーションプログラムと次世代アクセラレータの集合が与えられたとき、古典計算機による解法ならびに各種次世代アクセラレータの解法を同時に考慮した上で、アプリケーションプログラムを最適に実行するしくみの構築が不可欠である（次世代アクセラレータ・コデザイン技術）。実施体制を図 2-5-1 に示す。

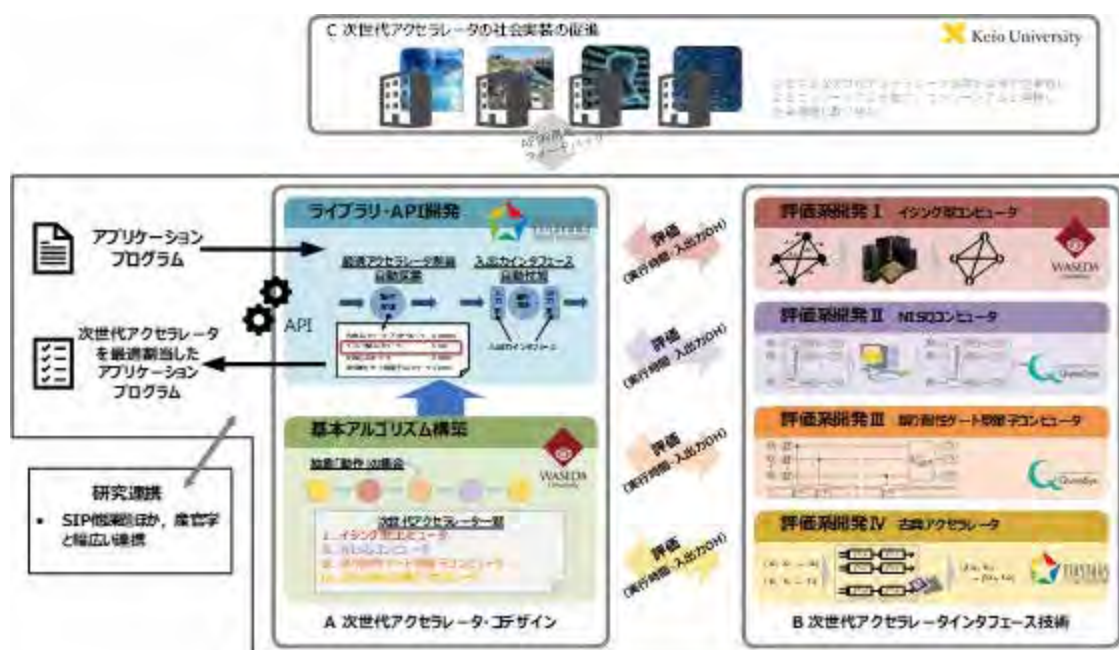


図 2-5-1. 研究開発の概要と実施体制

以上の背景のもと、本研究開発では(1)イジング型コンピュータ、(2)NISQ コンピュータ、(3)誤り耐性ゲート型量子コンピュータを次世代アクセラレータとし、これらを適材適所で利活用することで、Society 5.0に資するアプリケーションプログラム全体を高速化・高度化し、従来の計算方法と比較し格段に処理や解析を高速化・高度化する次世代アクセラレータ基盤の研究開発を目的とする（図 2-5-1）。すなわち、アプリケーションプログラムと次世代アクセラレータの集合が与えられたとき、適材適所に次世代アクセラレータを利活用し、アプリケーションプログラム全体を高速・高精度処理するソフトウェア群（最適化ライブラリ・API (Application Programming Interface)、次世代アクセラレータ評価系等）を構築する。研究開発全体を、(A) 次世代アクセラレータ・コデザイン技術、(B) 次世代アクセラレータインタフェース技術、(C) 次世代アクセラレータの社会実装の促進、に分け、これらを同時並行して進めることで効率的・効果的に研究開発を進める。

具体的な実施計画（内容）：

（A） 次世代アクセラレータ・コデザイン技術

Society 5.0 では、膨大なデータを高速かつ高精度に計算する必要があり、これを実現するための次世代アクセラレータとして、イジング型コンピュータ、NISQ コンピュータ、誤り耐性量子コンピュータ等が研究開発されている。これらは、それぞれ得意・不得意な分野を持ち、またアクセラレータを活用するためには、アプリケーションプログラムによって、アクセラレータに投入するデータを準備し、これをアクセラレータに投入、アクセラレータによる処理の後、計算結果を取り出し、これをもとに、元のアプリケーションプログラムの実行を継続する必要がある。アクセラレータの成否は、アクセラレータの処理時間だけでなく、アクセラレータへの入力データ準備・入力データ投入、さらには出力データ取り出し・出力データの解釈等、一連の処理全体で決まると言っている。さらに、最適な出力結果を得るために、パラメータや条件を適宜変化させながら、入力データの準備・投入や出力データの取り出し・解釈が複数回必要になる場合も考えられる。

アプリケーションプログラム全体を高速化・高度化するためには、イジング型コンピュータ、NISQ コンピュータ、誤り耐性量子コンピュータ、これらに加え GPU などの古典アクセラレータを前提に、プログラム中のどの部分に対して、どのようなアクセラレーションが適切か、また実際にアクセラレータとして何を使うべきかを考え、アプリケーションプログラムの最適化と、アクセラレータの最適化を同時に実行することが不可欠になる（次世代アクセラレータ・コデザイン）。上記を踏まえ、本研究開発では、次世代アクセラレータ基盤技術として次世代アクセラレータ・コデザイン問題を定式化し、これを最適解法するしくみを研究開発する。

具体的な研究開発事項として以下のものを取り上げる：

実施内容 A1： 次世代アクセラレータ・コデザインの基本アルゴリズムの研究開発

アプリケーションプログラムの動作を抽象化し「動作」の集合とする。そして、イジング型コンピュータ、NISQ コンピュータ、誤り耐性ゲート型量子コンピュータ、GPU 等の古典アクセラレータのうち、動作集合を構成するどの動作に対して、どのようなアクセラレーションが適切か、また実際に次世代アクセラレータとして何を使うべきかを考え、アプリケーションプログラムの最適化と、次世代ならびに古典アクセラレータの最適化を同時に実行する基本アルゴリズムを研究開発する。

実施内容 A2： 次世代アクセラレータ・コデザインのライブラリ・API の研究開発

次世代アクセラレータと既存コンピュータとを相互にやり取りするための共通インタフェースを設計・開発し、次世代アクセラレータ・コデザインのライブラリ・API を研究開発する。特に、共通インタフェースを抽象化し、アクセラレータ間の差異を意識させない相互利用を可能とすることにより、次世代アクセラレータ・コデザイン基盤を用いたアプリケーション開発エコシステムの構築を実現する。

(B) 次世代アクセラレータインタフェース技術

イジング型コンピュータ、NISQ コンピュータ、誤り耐性ゲート型量子コンピュータ、GPU を使った古典アクセラレータなど、各種アクセラレータについて、アプリケーションプログラムに対するインタフェース技術を研究開発する。

まず入出力データに関して調査し、これを最適化する技術を開発する。さまざまなアプリケーションプログラムにおいて、アプリケーションプログラムに必要なデータの実量を評価し、データ準備・データ入力・データ出力・原問題の解取出しのすべての工程において、これらの最適化を図る。その上で入出力オーバーヘッドを評価する。

また各種アクセラレータと、これを利用して解く問題の関係性を評価し、実施内容 (A) による次世代アクセラレータ・コデザインに適用する。アクセラレータと諸問題との性質を調査した上で、問題を次世代アクセラレータで解く際の実行時間を評価する実行時間評価系を構築し、実施内容 (A) による次世代アクセラレータ・コデザインに適用する。

最終的に入出力オーバーヘッド、実行時間評価を次世代アクセラレータ・コデザイン技術にフィードバックすることで次世代アクセラレータ・コデザイン基盤を実現する。

また上記と合わせて、各種次世代アクセラレータについて、実施内容 (A) と連携しながら、対象とする問題やこれらに対する入出力形式等を定義するものとする。

具体的な研究開発事項として以下の4つを取り上げる：

実施内容 B1： イジング型コンピュータのインタフェース技術の研究開発

イジング型コンピュータと諸問題との性質を調査した上で、イジング型コンピュータを対象に、入出力オーバーヘッド、実行時間の評価系を研究開発する。

実施内容 B2： NISQ コンピュータのインタフェース技術の研究開発

NISQ コンピュータと諸問題との性質を調査した上で、NISQ コンピュータを対象に、入出力オーバーヘッド、実行時間の評価系を研究開発する。

実施内容 B3： 誤り耐性ゲート型量子コンピュータのインタフェース技術の研究開発

誤り耐性ゲート型量子コンピュータと諸問題との性質を調査した上で、誤り耐性ゲート型量子コンピュータを対象に、高速シミュレータ等を利用して入出力オーバーヘッド、実行時間の評価系を研究開発する。

実施内容 B4： GPU 等古典アクセラレータのインタフェース技術の研究開発

GPU 等古典アクセラレータと諸問題との性質を調査した上で、GPU 等古典アクセラレータを対象に、入出力オーバーヘッド、実行時間の評価系を研究開発する。

(C) 次世代アクセラレータの社会実装の促進

次世代アクセラレータの社会実装の促進の研究開発では、以下の二点を実施する。

第一に、GPS スマート製造領域における次世代アクセラレータ活用の加速を行う。GPS スマート製造領域におけるボトルネック要因を定式化し、これを次世代アクセラレータで解法可能な形式に変換した上で、プロトタイププログラムを開発する。これをもとに GPS ス

マート製造領域のステークホルダーからフィードバックを得て、産業側ニーズを反映する。

第二に、さまざまな次世代アクセラレータの活用を検討する企業群からなる社会実装コンソーシアムを拡大する。昨今、さまざまな次世代アクセラレータを利用できるようになりつつあるため、イジング型コンピュータ、NISQ コンピュータ、誤り耐性ゲート型量子コンピュータ、GPU 等古典アクセラレータのどれか一種類のみに注目している企業は少なく、いずれの次世代アクセラレータについても注目している企業が多い。そのため、複数種の次世代アクセラレータの組合せ活用のプロトタイププログラムを開発し、それをもとに企業からフィードバックを得て、産業側ニーズを反映する。複数種の次世代アクセラレータの組合せ活用のプロトタイププログラムを基に産業界ニーズを汲み上げることで、イジング型コンピュータ並びにNISQ コンピュータの社会課題活用を目指す企業群からなる社会実装コンソーシアムを拡大する。

上記を受け、実施内容 C は以下の通りである：

実施内容 C： 次世代アクセラレータの社会実装の促進の研究開発

GPS スマート製造領域における次世代アクセラレータ活用を加速し、さまざまな次世代アクセラレータの活用を検討する企業群からなる社会実装コンソーシアムを拡大する。

社会実装（計画）：

本研究開発の社会実装に向けた戦略と取組みとして、以下のような段階的な戦略を想定する。まずオープン戦略として、研究開発の最終段階あるいは研究開発終了後まもなくの時期に、本研究開発によって得られた成果を部分的にもいち早く公開することにより、世界でデファクトスタンダードを目指す。システムインテグレータがより迅速に社会実装を展開し、事業化のために本研究開発技術を利活用することが期待される。そしてその後、順次クローズ戦略として、本研究開発を主体的に進める産業界を中心に、研究開発されたソフトウェア群を用いたアプリケーションプログラムの高速化・高度化サービス、研究開発されたソフトウェア群のライセンスなど競争領域にて事業展開を図る。

本研究開発では、社会実装の姿として、NEDO 事業や Q-LEAP 事業等と連携し、ネットワーク型製造システムや物流、材料、エネルギー・環境産業等からいくつかを想定し、これらの潜在ユーザーと、社会問題の抽出ならびに定式化／最適解法について連携しながら社会実装を進めるものとする。一部の次世代アクセラレータを用いた研究開発を既に行っているアーリーアダプタ層の企業群との強力な連携だけでなく、アーリーマジョリティ層となり得る企業群に対し、次世代アクセラレータの価値を明確化することにより、アーリーマジョリティ層の早期取り込みを行い、次世代アクセラレータ活用の早期拡大を目指す。レーザー加工分野においても、ネットワーク型製造システムに関するアプリケーションプログラムを想定し、研究開発技術を社会実装することを目指す。これらの研究開発成果のもと、企業による準製品化を完了し、社会実装コンソーシアムで活用する。

2) 技術的目標 (計画)

事業終了時点アウトプット目標 (2022 年度の目標)

- ・次世代アクセラレータ・コデザイン基盤を実現するソフトウェアを実装完了し、オープンテストベッド化を完了する (TRL7)。
- ・代表的なアプリケーションについて、次世代アクセラレータ基盤により、古典アクセラレータのみを活用した従来技術に比較して 10 倍~100 倍高速化を達成し、企業による準製品化を完了し、社会実装コンソーシアムで活用する (TRL7)。

以下に 5 年間の工程表を示す。なお 2018 年度は研究計画策定期間である。

研究開発項目	2018年度計画	2019年度計画	2020年度計画	2021年度計画	2022年度計画	出口戦略	製品化
(研究開発項目3)光電子情報処理 ①次世代アクセラレータ基盤に係る研究開発	<ul style="list-style-type: none"> ・内閣府「ImPACT」、文部科学省「Q-LEAP」、経済産業省・NEDO「高効率・高速処理を可能とするAIチップ・次世代コンピュータの技術開発事業」の状況を踏まえ、今後詳細を決定する。 ・上記検討にあたって、必要な調査を実施する。 	<p>1) 次世代アクセラレータ・コデザイン</p> <ul style="list-style-type: none"> ・各種アプリケーションプログラムのボトルネック調査 ・ボトルネックと次世代アクセラレータとの相関性調査 ・調査結果を踏まえた設計指針の確定 <p>TRL2</p>	<ul style="list-style-type: none"> ・次世代アクセラレータ・コデザイン関連の解法を確定 ・各種アプリケーションプログラムとアクセラレータを用いたプロトタイププログラム開発完了 (第1段階) 	<ul style="list-style-type: none"> ・次世代アクセラレータ・コデザイン関連の解法を確定 ・各種アプリケーションプログラムとアクセラレータを用いたプロトタイププログラム開発完了 (第2段階) <p>TRL5</p>	<ul style="list-style-type: none"> ・次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装完了とオープンテストベッド化の完了 ・代表的なアプリケーションへ適用評価し、古典アクセラレータのみの技術と比べ10~100倍の高速化し、企業による準製品化を完了し、社会実装コンソーシアムで活用 <p>TRL7</p>	<ul style="list-style-type: none"> ・次世代アクセラレータ・コデザインソフトウェアのオープン化による試用拡大 ・アプリケーション最適化サービスの事業化への貢献 	<p>アプリケーション最適化サービス (ユーザ試用: 2023~ 商用利用: 2025~)</p>
		<p>2) 次世代アクセラレータインタフェース技術</p> <ul style="list-style-type: none"> ・各種アクセラレータの入出力調査 ・各種アクセラレータの入出力計測・データ集調査 ・調査結果を踏まえた設計指針の確定 <p>TRL2</p>	<ul style="list-style-type: none"> ・各種アクセラレータと関連との性能調査 ・各種アクセラレータインタフェースのプロトタイプ設計完了 	<ul style="list-style-type: none"> ・各種アクセラレータ・コデザイン設計とコデザイン関連の解法への適用完了 <p>TRL5</p>	<ul style="list-style-type: none"> ・CPSスマート製造領域への次世代アクセラレータ活用の加速 ・さまざまな次世代アクセラレータの活用を検討する企業群からなる社会実装コンソーシアムの拡大 <p>TRL5</p>	<p>民間からの出資 (人材、物資、資金等)</p> <p>(25%)</p>	<p>(50%)</p>

3) 課題目標の達成度 (成果)

① 国際競争力

本研究開発は(1)イジング型コンピュータ、(2)NISQ コンピュータ、(3)誤り耐性ゲート型量子コンピュータを次世代アクセラレータとし、これらを適材適所で活用することで、Society 5.0 に資するアプリケーションプログラム全体を高速化・高度化し、従来の計算方法と比較し格段に処理や解析を高速化・高度化する次世代アクセラレータ基盤の研究開発するものであり、競合技術に比較して高い優位性を持つ。ここでは、本研究開発と競合技術とをグローバルベンチマークし、現時点での本研究開発を位置づけ、さらに研究開発が完了し後の本研究開発を位置づけることで、本研究開発の国際競争力を評価した。

グローバルベンチマーキングにあたり次世代アクセラレータとして、イジング型コンピュータ、NISQ コンピュータ、誤り耐性ゲート型量子コンピュータを対象とし、さらに、GPU を利用した古典アクセラレータを含め、次世代アクセラレータを活用し、(2)インタフェース開発要素を含むもの (図 2-5-2 参照) を焦点とした。

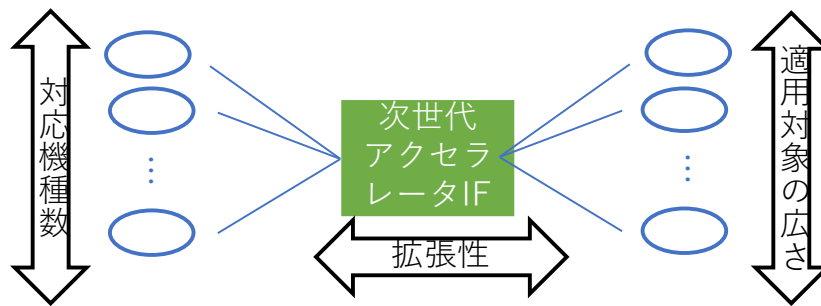


図 2-5-2. 次世代アクセラレータインタフェースの果たすべき役割

SIP 終了時のベンチマーク結果を表 2-5-1 に、これをレーダーチャートにしたものを図 2-5-3 に示した。

まず、次世代アクセラレータとして、イジング型コンピュータ、NISQ コンピュータ、誤り耐性ゲート型量子コンピュータ、加えて GPU による古典アクセラレータを開発対象に含み、企業が提供するサービスを評価対象とした。具体的には、欧米ならびに日本から幅広く、CUDA (米・NVIDIA)¹、次世代アクセラレータ導入コンサルティングサービス (米・QCWare)²、AWS braket (米・Amazon)³、tket (英・Cambridge Quantum Computing)⁴、次世代アクセラレータ導入コンサルティングサービス (加・1QBit)⁵、次世代アクセラレータ導入コンサルティングサービス (加・SoftwareQ)⁶、次世代アクセラレータ導入コンサルティングサービス (日本・NTT データ)⁷、PyQUBO (日本・リクルート)⁸、Microsoft Azure Quantum (米・Microsoft)⁹、Jij-Zept (日本・Jij)¹⁰ とした。それぞれ以下の情報をもとに評価した。

評価軸として、「次世代アクセラレータ向けのインタフェース」が幅広い市場に普及してこそ価値が出るものであるため、研究開発の価値を大きく、

- 市場性
- 社会貢献性

1 <https://developer.nvidia.com/cuda-toolkit>

2 <https://www.qcware.com/research>

3 <https://aws.amazon.com/jp/braket/>

4 <https://cambridgequantum.com/our-publications/>

5 <https://1qbit.com/products/>

6 <https://www.softwareq.ca/products>

7 <https://www.nttdata.com/jp/ja/services/quantum/>

8 <https://pyqubo.readthedocs.io/en/latest/>

9 <https://azure.microsoft.com/ja-jp/products/quantum/>

10 <https://www.jijzept.com/>

- コスト

の3つの観点とした。さらに市場性はより細分化して評価項目を設定した。

- 適用対象の広さ
- 対応可能なアクセラレータの機種数
- インタフェース自体の拡張性

以上の評価軸によって、現状のベンチマーク結果を見ると、本研究課題は、組合せ最適化問題、機械学習、量子化学計算をはじめ古典アクセラレータの全対象領域に適用可能であり、適用範囲の広さで大きな優位性を持つ。さらに、現状、実利用可能な次世代アクセラレータのすべてを対応可能とし、対応可能なアクセラレータの数においても優位性を持つ。一方、拡張性や社会貢献度、コストについては、ソフトウェア、API (Application Program Interface)、ライブラリの充実ならびに社会実装コンソーシアムの充実が求められる。

2021年度に比較して、2022年度においても本研究開発に継続した進捗があった。その部分については、表2-5-1において赤枠で示し、また図2-5-3では矢印で示した。

2019年度～2021年度の本研究開発の研究期間を通して、特筆すべき成果として例えば、以下のようなものがあり、最終的にこれらの成果を反映したものとなっている。

【拡張性】 京都大学・フォトリック結晶レーザーチームとの連携によるフォトリック結晶レーザーの性能指数 Q を向上させる結晶構造探索高速化がある。フォトリック結晶レーザーシミュレータ、古典計算機による機械学習、加えて次世代アクセラレータによる推論の3段階による量子・古典ハイブリッド手法を構築し、実際にフォトリック結晶レーザーの性能指数 Q を大幅に向上させることに成功している。さらに、NICTの研究開発成果を活用し、京都大学・NICT・慶応義塾大学を秘匿通信によって接続し「秘伝の書」を仲介したフォトリック結晶レーザーの構造最適化に成功している。製造分野に量子計算技術を適用可能とする好例となっている。

【拡張性】 加えて、2021年度に引き続き、物流倉庫における作業員最適配置では、これまでの成果を活用し、2022.10より実サービスが開始された。物流倉庫の実際のオペレーションに必要な制約事項を種々取り入れ、実仕様に対応するための作業員配置最適化エンジンが利用されている。また、作業員配置最適化エンジンの結果検証に向けた、現場における生産性のデータ化及び分析を行うことにより、物流倉庫のDX化が達成された。

【社会貢献度】 さらに、研究開発したソフトウェア(ライブラリやAPI)の普及のためには、実際にユーザー企業が使用し、ユーザーニーズに則した機能実装を進めることが肝要と考えており、本研究開発では、各種ユーザーコンソーシアムと連携した社会実装を志向している。(株)フィックスターズはAmplify SDKにより、多くのユーザー企業に量子計算のためのソフトウェアツールキットを提供している。一方、QPARCは(株)QunaSysが2020.4に立ち上げたコンソーシアムであり、国内の主要材料メーカー、及び、自動車・エレクトロニクス関連企業50社超から計算技術者が集まっている。最終的にSIPで開発するソフトウェアの社会実装の一環として、QPARCはAmazon AWSとの連携を通じ、QPARC参加企業が量子コンピュー

々実機を活用できる場を提供した。

表 2-5-1. 次世代アクセラレータ基盤のグローバルベンチマーク

評価軸	研究開発										
	SIP量子 (日本)	CUDA (米・ NVIDIA)	次世代アクセラレータ導入 コンサルテイング (米・ QCWare)	AWS braket (米・ Amazon)	Azure Quantum (米・ Microsoft)	tket (英・ Cambridge Quantum Computing)	次世代アクセラレータ導入 コンサルテイング (加・ 1QBit)	次世代アクセラレータ導入 コンサルテイング (加・ SoftwareQ)	次世代アクセラレータ導入 コンサルテイング (日本・NTT データ)	PyQUBO (日本・リ クルート)	JijZept (日本・ Jij)
適用対象の 広さ	◎ 組合せ最適化 機械学習 量子化学計算 古典アクセラレータの 対象領域	○ 古典アクセラ レータの対象 領域	△ 機械学習 量子化学計 算	○ 最適化計算 機械学習 量子化学計 算	◎ 組合せ最適化 数理最適化 機械学習 量子化学計 算	△ 量子化学計 算	△ 組合せ最適化	△ 量子化学計 算	△ 組合せ最適化	△ 組合せ最適化	△ 組合せ最適化
市場規模 対応可能な アクセラレー タ機種数	◎ 現状のイジング型コ ンピュータ・NISQ 型コンピュータ。将 来開発される誤り耐 性型量子コンピュ ータ	× 古典アクセラ レータ	△ 古典アクセラ レータ、一部 のNISQコ ンピュータ	○ 一部のイジ ング型コ ンピュータ、一部の NISQコ ンピュータ	◎ 複数のイジ ング型コ ンピュータ、複数の NISQコ ンピュータ	△ 複数のNISQ コンピュータ	△ 一部のイジ ング型コ ンピュータ	△ 複数のNISQ コンピュータ	△ 一部のイジ ング型コ ンピュータ	△ 複数のイジ ング型コ ンピュータ	△ 一部のイジ ング型コ ンピュータ
拡張性(自 動化、コデ ザイン性)	◎ 自動化、コデ ザイン	× 手動、コデ ザイン非 対応	△ 特定の量子 ・古典ハイブリ ッドアルゴリズム のみ対応	△ 特定の量子 ・古典ハイブリ ッドアルゴリズム のみ対応	△ 特定の量子 ・古典ハイブリ ッドアルゴリズム のみ対応	× 手動、コデ ザイン非 対応	× 手動、コデ ザイン非 対応	× 手動、コデ ザイン非 対応	× 手動、コデ ザイン非 対応	× 手動、コデ ザイン非 対応	× 手動、コデ ザイン非 対応
社会貢献度 (オープン開 発、コミュニ ティ育成)	◎ オープン開発要素を 含む開発、コンソー シアム活動によるコ ミュニティ育成	○ 古典アクセラ レータのみに 絞ったコミュニ ティ育成	× 個社対応	△ 研究用途、市 場拡大のため のコミュニ ティ育成	○ コンソーシアム 活動によるコ ミュニティ育成	× 個社対応	× 個社対応	× 個社対応	△ 個社対応 (複数の大 企業への対 応)	△ 研究用途、市 場拡大のため のコミュニ ティ育成	× 個社対応
コスト (導入、運 用)	◎ 膨大な業種からなる コンソーシアム参 画企業との対話から 得られたユーズ ケース、PoC 取り組みを通じた導 入コスト低減	○ 古典アクセラ レータ市場展 開実績有	△ ごく小数の ユーザ企業 のみため新規 顧客参入に 対する障壁大	○ 古典アクセラ レータ市場展 開実績有	○ 古典アクセラ レータ市場展 開実績有	△ ごく小数の ユーザ企業 のみため新規 顧客参入に 対する障壁大	△ ごく小数の ユーザ企業 のみため新規 顧客参入に 対する障壁大	△ ごく小数の ユーザ企業 のみため新規 顧客参入に 対する障壁大	○ 古典アクセラ レータ市場展 開実績有	— 研究用途の OSSであり当 該項目に該当 しない	△ ごく小数の ユーザ企業 のみため新規 顧客参入に 対する障壁大

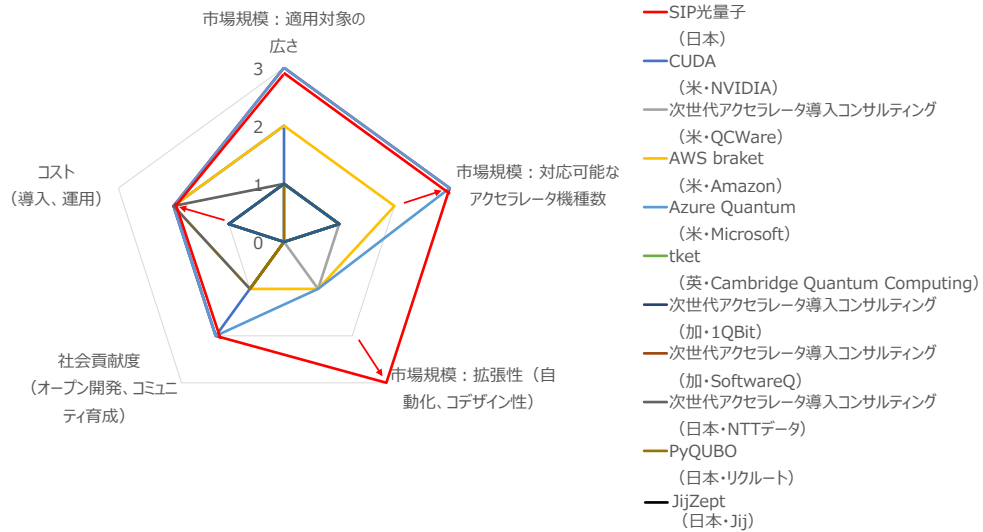


図 2-5-3. 次世代アクセラレータ基盤の他機関との比較。矢印は 2021 年度から 2022 年度にかけて、本 SIP 光・量子課題事業の進捗部分。

評価対象となる企業ならびにサービスについて、ソフトウェアやサービスの充実が予想されるが、利用する次世代アクセラレータの種類が限られ、またその活用技術が、手動や特定の量子・古典ハイブリッドアルゴリズムに限られるなど、拡張性(自動化、コデザイン性)の範囲が極めて限られる。社会貢献度やコストについても、本研究課題に比較すると、

進歩は限定的になると予想する。

これに対して、本研究課題における開発技術は、適用範囲の広さ、対応可能なアクセラレータ機種数について大きな優位性を持つと同時に、理論的な定式化やそれに基づくプロトタイプ設計、実ソフトウェア設計を通じて拡張性（自動化、コデザイン性）にも優れることになる。加えて、研究開発の初期の段階からオープン/クローズ戦略に基づき研究開発を実施し、社会貢献度（オープン開発、コミュニティ育成）にも優位性を持つ。さらに、50社超の様々な業種からなる QPARC 参画企業との対話から得られたユーザーフィードバック、POCによる取り組みを通じた導入コスト低減を図り、コスト面でも同等かそれ以上のものとなっている。

結果的に、すべての評価項目において、競争力を持った研究開発を実施することが可能となっている。ここまで 2019 年度から 2022 年度までの研究開発を通して、SIP 終了時のグローバルベンチマークをほぼ達成したと考えている。

② 研究成果で期待される波及効果

本研究開発の成果は、Society 5.0 を構成するさまざまな分野に波及可能である。具体的に、本 SIP 光・量子課題では以下の 4 項目を社会課題の例として社会実装を試みる。さらに、2019 年度～2022 年度までにこれらの各分野において、具体的な社会実装が達成されつつあり、研究成果の波及効果は大きいことが分かる。本研究開発によって、当該分野の科学技術が大きく進展するばかりでなく、社会実装を通じて新技術が確立され、量子計算技術を活用した新製品・新機能への展開、新たな海外市場を含む新たな市場創出が期待される。

GPS 型スマート製造：

従来の製造業は、少品種大量生産を前提とした一連のワークフローによって成立し、いくつかの工程では人の経験と勘に頼ってきた側面がある。一方で現在の製造業では、多品種少量生産に対するニーズに応えるためのさらなる高効率化が課題である。これに対応する鍵が次世代アクセラレータを駆使した GPS 型スマート製造である。スマート製造における重要な技術であるレーザー加工に対しては、対象スケール（マイクロ、マクロ）や対象材料に対して、レーザーと材料の相互作用によって駆動される光物理化学現象の力学・熱シミュレーション、適切な加工パラメータの算出の一部分を機械学習により実行すること等が次世代アクセラレータの対象となる。また、製造全体では、複雑化された各種工程を効率よく実行するスケジューリング最適化や、労働負担軽減を行うためのロボットにおいて必須の技術であるセンシングのための機械学習やロボットによる部品ピッキング・運搬の計画最適化等が次世代アクセラレータの対象となる。

物流・配送：

e コマースの飛躍的な進展を受け、B2C 物流の絶対量が年々増加している。また、物流業界における労働人口の不足や高齢化問題も指摘されている。さらに、省エネルギー等環境に配慮した持続可能な社会に向けた取り組みも求められている。これらに対応するには、フ

デジタル空間で集められたデータを積極的に活用した物流のさらなる効率化、配送の共同化等を推進する必要があると指摘されている。これらの課題に対し、想定される次世代アクセラレータの対象としては、モーダルシフトや人員配置等の各種リアルタイム最適化（考慮すべき制約として、倉庫数、顧客拠点数、配送指定時間・場所等がある）、貨物を運ぶトラックの配車スケジューリング等が挙げられる。

材料：

材料やエネルギーの領域では、従来の単純な性能追求（耐熱性、強度、変換効率、等）だけでなく、環境問題や資源枯渇などの社会課題への対応が求められており、通常トレードオフの関係にある要求を高度に両立させることが必要となる。このため、これまでのような実験偏重・職人芸に頼った開発から脱却し、対象となるミクロな物理系をサイバー空間上でモデル化し、シミュレーションとハイスループット実験を通じて膨大な可能性空間の中から最適解（分子構造や反応条件など）を導き出す必要性が高まっている。想定される次世代アクセラレータの対象としては、例えば、革新材料の発見や量子化学計算などがある。

センシング・データ解析：

IoTに代表されるビッグデータ分析、衛星データの視覚化、医療画像など、大規模データにおけるデータマイニングや統計解析では、特徴量の抽出やデータ分類、推定などが行われる。大量のデータを社会課題に役立てるには、実世界のリアルデータを高精度かつ膨大に取得することが求められる。特にデータ取得の際にノイズや誤りを含む可能性が有る場合の解析には、必要なデータと不要なデータの識別といった取捨選択、すなわち組合せ最適化が行われる。このようなデータの最適化に対し、高速かつ高精度に処理することが可能になれば、実社会において効率的かつ持続可能な社会システムの構築や、高度な医療技術の提供、新たなサービスやソリューションの創出と提供が可能になる。想定される次世代アクセラレータの対象としては、位置データの解析や画像データの解析等があげられる。

2019年度～2022年度の研究開発を通じて、以下の項目について、社会実装が成果を上げている（詳細は、③達成度(1)ならびに④達成度(2)を参照）：

(A) 次世代アクセラレータ・コデザイン技術

上述のセンシング・データ解析について、最適周波数割当ならびに位置情報解析を実現している。最適周波数割当では通信事業者と連携し、次世代アクセラレータの適用により次世代通信を対象とした周波数割当問題を解法し、最適な周波数割当を実現した。位置情報解析では、大規模位置情報解析業者と連携し、点群データを扱うアプリケーションソフトウェアを創出した。点群を自動で切り出すことで、これまでデータを個別に見ては出来なかった人的行動を抽出し、新たに多くの人間のデータを抽象化された行動傾向として地理情報と紐ついた解析への展開が期待される。

上述の物流・配送では、物流倉庫での実作業に対応するため、作業配置最適化エンジンを開発し、さらに合わせて作業配置最適化エンジンのサービスインが 2022.10 に実現

し、実用されている。結果検証に向けた現場における生産性のデータ化およびその分析を行うことで、さらに作業配置最適化エンジンを改良すると同時に、エンジンのプラットフォーム化を行った。これにより、当該現場に限らず福祉、研究開発への展開などへの波及を目指す。

(B) 次世代アクセラレータインタフェース技術

上述の材料について、NISQ コンピュータ実機をアクセラレータとして用い、量子化学向け計算時間推論のエンジンなどのインタフェース技術の開発を進め、革新的材料開発への応用を行っている。量子コンピュータ上で量子化学計算を実行できるソフトウェアへ研究開発成果を実装し、開発中のアルゴリズムエンジン、及び計算時間推論エンジンの有効性検証のため、Microsoft の Azure Quantum の量子コンピュータ実行プラットフォームを経由し、Honeywell System Model H1（イオントラップ型）という現時点で利用できる世界最高性能（Quantum Volume512）の量子コンピュータを利用して検証を実施した（分子の振動数解析を行った本計算は世界初の試み）。量子化学計算は、太陽電池・CO₂吸着・人工光合成触媒等への貢献余地が大きく、量子コンピュータによる開発加速が期待できる。

さらに CPS 型スマート製造と材料を融合した実応用例として、レーザー光源開発・レーザー加工時の状態解析への応用を実施し、レーザー照射時の電子状態の時間依存ダイナミクスを、古典コンピュータと量子コンピュータを組み合わせる手法など、量子ダイナミクス計算のための理論構築を推進した。量子コンピュータは励起状態計算や量子ダイナミクス計算を得意とし、従来行なえなかった現象の解析が可能となることで、新たな光源開発や加工条件の精密制御が可能となる。

(C) 次世代アクセラレータの社会実装の促進

特に、CPS 型スマート製造に注目し、フォトニック結晶レーザーの性能を向上させる結晶構造探索に成功した。人工知能と次世代アクセラレータ（イジング型コンピュータ）のハイブリッドアルゴリズムを活用し、性能指数 Q を高める非自明なフォトニック結晶構造を高速に発見することに成功した。この成果により、今後さらに先端半導体の最適設計に広く活用が期待される。

また、複合材料の安定構造探索シミュレーションの高速化にも取り組み、材料組織の安定構造探索計算を次世代アクセラレータ（イジング型計算機の実機）を用いて網羅的に実施し、高速計算にも成功しており、（例）脱炭素化に貢献する材料探索を早め、地球温暖化防止に役立つことが期待される。さらに、NICT の研究開発成果を活用し、京都大学・NICT・慶應義塾大学を秘匿通信によって接続し「秘伝の書」を仲介したフォトニック結晶レーザーの構造最適化に成功している。製造分野に量子計算技術を適用可能とする好例となっている。

③ 達成度（1）※5年間の設定目標に対する達成度

(A) 次世代アクセラレータ・コデザイン技術

実施内容 A1: 次世代アクセラレータ・コデザインの基本アルゴリズムの研究開発

実施内容 A1 では、複数の次世代アクセラレータを協調的に動作させる基本アルゴリズムを構築することを目的とする。構築する基本アルゴリズムは、対象とするアプリケーションプログラムの計算ボトルネックとなり得る各動作に対し、次世代アクセラレータならば古典アクセラレータから動作に最適なものを選択するものであり、アプリケーションプログラム全体を協調動作させる一連の仕組みを与える。2019 年度から 2022 年度にかけて次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装を完了し、オープンテストベッド化を完了した。代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ 10-100 倍の高速化を実現し、企業による準製品化を完了し、社会実装コンソーシアムで活用した。2019 年度から 2022 年度にかけての取り組みにより以下の成果を得た。

1) アプリケーションプログラムのボトルネック調査

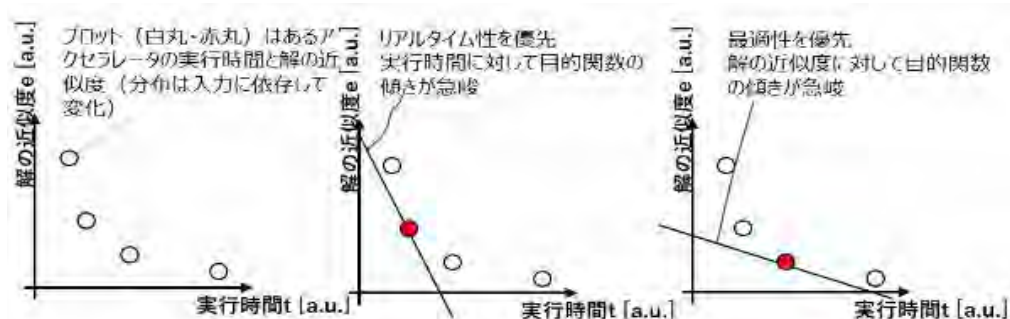
対象となるアプリケーションプログラムを想定し、ボトルネックとなる計算に時間がかかる処理を部分プログラムとして抽出した。いま Society 5.0 に資する典型的なアプリケーションプログラムの事例として、宅配業者が複数のトラックを使用して効率的に倉庫内の荷物を各家庭に配送するアプリケーションプログラムを考える。この場合に、倉庫内の荷物をデータとして入力する部分プログラムは次世代アクセラレータを使う必要がなく、通常の古典のコンピュータで実行することが望ましい。一方で荷物をトラックに割り当て、各家庭に配送する順序を決める部分プログラムは計算量が大きく、次世代アクセラレータを使うことが望ましい。

2) 次世代アクセラレータ・コデザイン問題を定式化し、各アクセラレータを協調的に動作させる最適化アルゴリズムを実現

対象となる部分プログラムを次世代アクセラレータで実行する「向き／不向き」を調査した。先の宅配アプリケーションプログラムの例では、次世代アクセラレータの適用の対象となる部分プログラムは容量制約付き配送問題(Capacitated Vehicle Routing Problem; CVRP)と呼ばれる最適化問題となる。この最適化問題に向く次世代・古典アクセラレータとしてはイジング型コンピュータ、NISQ、古典アクセラレータが考えられる。一方で誤り耐性量子コンピュータは、この最適化問題に不向きであり協調動作する場合は使用しないことが望ましい。さらに検討を重ねると次世代アクセラレータの対象となる部分プログラムは、さらに細かい部分プログラムに分解可能であることが判明した。この CVRP の場合はクラスタリング問題と巡回セールス問題に分解可能である。分解された部分プログラムにも次世代アクセラレータ適用の向き不向きがある。

次世代アクセラレータを使用するにあたり実行時に最適化したい項目は異なる。部分プログラムの出力を解の品質と定義し、この解の品質と実行時間を多目的に最適化することを考えた。多目的関数を 1 次元の評価指標に落とし込む優先度というハイパラメータを定義し、その 1 次元の評価指標の最適化が多目的関数の最適化に結びつく変換方法を構築した。次世代アクセラレータ・コデザイン問題を入力プログラムに対し、実行時間と解の

品質（近似度）を多目的に最適化する部分プログラムとアクセラレータの割当問題として定式化を完了した（図 2-5-4）。



入力	目的関数 F [s]	選択アクセラレータ
chr12a	7.242	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数1,000,000回）
chr12b	6.724	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数1,000,000回）
chr12c	7.196	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数1,000,000回）

リアルタイム性を優先する（実行時間が小さい方がよい）問題の場合

入力	目的関数 F [s]	選択アクセラレータ
chr12a	10006.242	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数1,000,000回）
chr12b	10022.262	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数100,000,000回）
chr12c	10021.561	次世代アクセラレータ（イジング型コンピュータ，イテレーション回数100,000,000回）

最適性を優先する（解の近似度が小さい方がよい）問題の場合

図 2-5-4. 実行時間と解の品質（近似度）を多目的に最適化するアルゴリズム（上）とベンチマークに対する最適化結果（下）

3) 複数の次世代アクセラレータを協調して動作させるコデザイン基盤となるソフトウェアの実装と、次世代アクセラレータ・コデザインソフトウェアを公開し、オープンテストベッド化を達成

次世代アクセラレータ・コデザインの最適化アルゴリズムを実現するソフトウェア（図 2-5-5）を実装した。プログラムは API を通じてクラウドサーバーと通信するが Wrapper API を用意することで複数の部分プログラムをまとめ、効率的な処理を可能とする。Wrapper API が実際に、部分プログラムごとにプリミティブな API で計算するか、あるいは部分プログラムをまとめた状態で計算するか、はシステム内で決定される。推定モジュールとして部分プログラムのパラメータに対する実行時間をプロファイルしておき、ソフトウェアは各種アプリケーションの API として与えられ、基本構造となるプリミティブな API とそれらを複合して動作する API として与えられる。

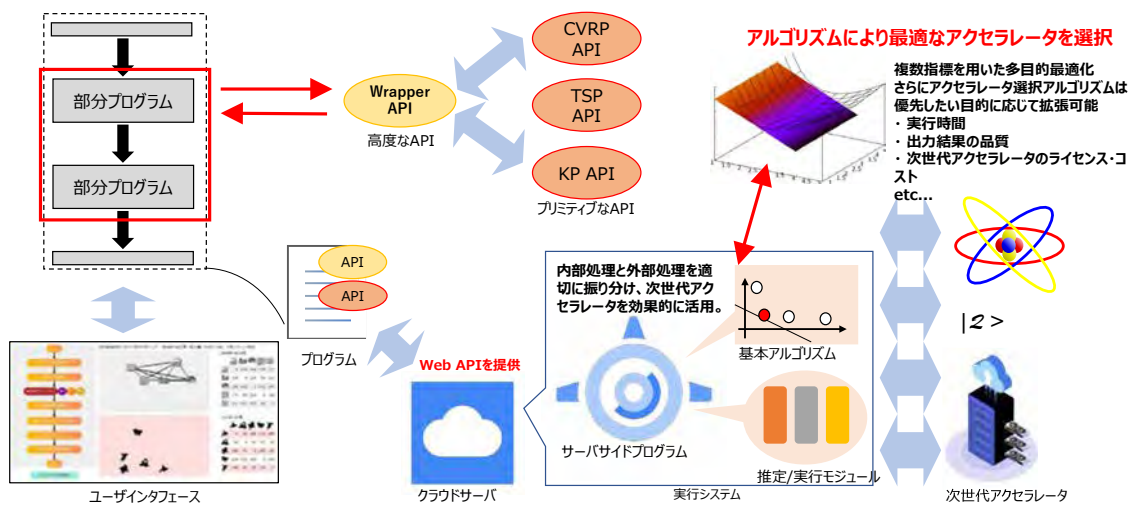


図 2-5-5. 次世代アクセラレータ・コードデザインソフトウェア

4) 位置情報アプリケーションと周波数割当最適化アプリケーションに対して、古典計算機や古典アクセラレータのみの技術との比較で次世代アクセラレータ・コードデザインソフトウェアが1桁以上の高速化を達成

位置情報アプリケーションは入力された複数の位置情報からノイズを除去し意味あるまとまりを出力するアプリケーションである（図 2-5-6）。人間の行動を解析するにあたりモバイル端末から GPS データを取得するとそれは時間と位置座標のペアとして得ることができる。大量の時間と位置座標のペアはそれだけでは意味をなさないため、注目すべき位置座標群を時空間上のまとまりを検出して解析結果として出力する。

周波数割当最適化アプリケーションは周波数干渉を起こさないように複数の時間枠における基地局と周波数との割当を最適化するアプリケーション（図 2-5-7）である。近い位置にある基地局が同時刻に干渉する周波数を用いることは避けなければならないハードな制約となる。基地局には通常複数の周波数を割当てることが可能であるが、なるべく連続した周波数領域を割当てることが望まれており、これがソフトな制約となる。ハードな制約を満たしつつ複数のソフトな制約に相当するコスト関数を最小化する問題を、次世代アクセラレータを用いて解法する。

位置情報アプリケーション（2パタン）の高速化スキームを構築

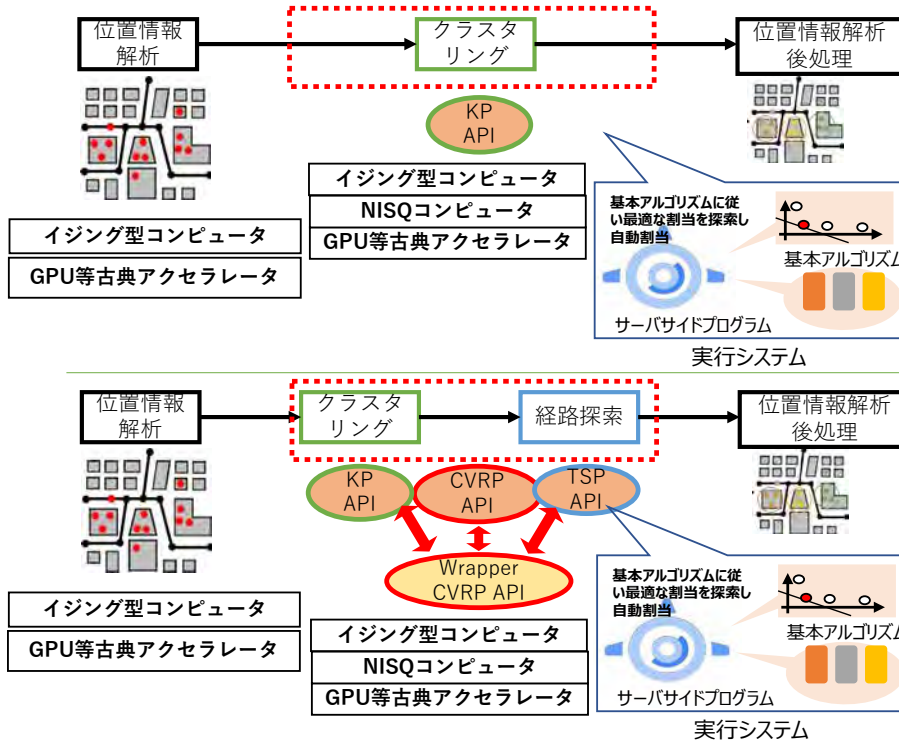


図 2-5-6. 位置情報アプリケーション

周波数割当最適化アプリケーションの高速化スキームを構築

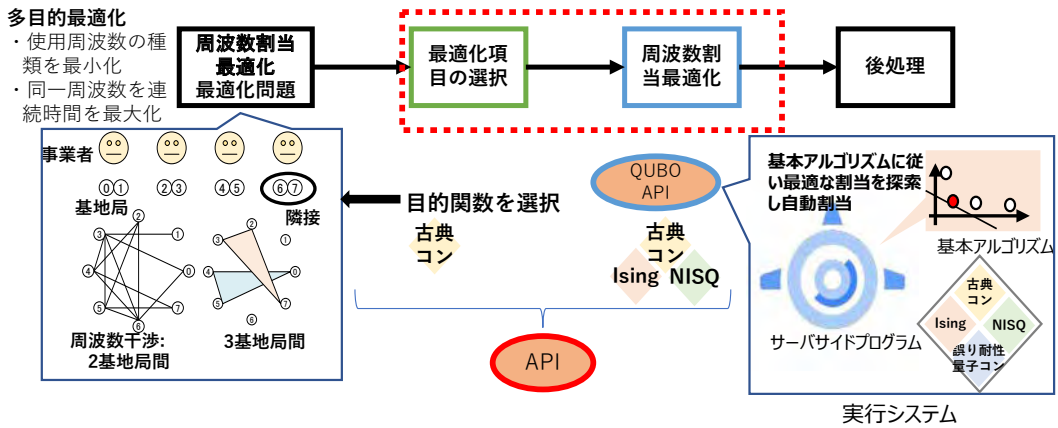


図 2-5-7. 周波数割当最適化アプリケーション

これらのアプリケーション古典計算機や古典アクセラレータのみの技術との比較で次世代アクセラレータ・コードデザインソフトウェアが1桁以上の高速化を達成した(表 2-5-2)。

表 2-5-2. 周波数割当最適化アプリケーションで1桁以上の高速化

5.7x~32x

(m,n,f,t) m:事業者数、 n:基地局数、 f:チャネル数、t: タイムスロット	古典ヒューリスティック		次世代アクセラレータ Fujitsu DA PT mode		次世代アクセラレータ・コデザイン		
	時間 [s]	品質 [a.u.]	時間 [s]	品質 [a.u.]	時間 [s]	品質 [a.u.]	選択された アクセラレータ
(4,8,4,2)	0.54	-14.38	5.81	-14.38	0.23	-14.38	Amplify AE
(4,12,5,2)	1.04	-15.52	3.87	-16.24	0.18	-16.24	Amplify AE
(4,16,15,2)	6.49	-116.50	11.87	-118.59	0.20	-112.93	Amplify AE
(4,20,15,2)	9.37	-99.22	29.20	-103.11	4.12	-102.36	Fujitsu DA EX mode
(4,24,15,2)	15.33	-80.15	40.43	-53.47	3.34	-74.12	Fujitsu DA EX mode

5) ポストコロナ時代の働き方に対応する次世代アクセラレータ活用の人員計画最適化基盤ソフトウェアの有効性を確認。一部の企業とのサービスイン合意をとり企業による準製品化を完了し、社会実装コンソーシアムにおける活用を達成

次世代アクセラレータ（量子計算技術）を活用することで、新型コロナウイルスの影響を加味した柔軟な人員計画最適化ソフトウェアを作成した。新型コロナウイルスの影響による職場環境における新たな制約を遵守し、生産現場や介護現場等の人員計画最適化の有効性を確認した。これまで人手により朝・昼・夕の合計で数時間を越える多大な時間が割かれた人員計画最適化が、配置調整を行いたいタイミング（予定外の欠勤、急な帰宅者発生、生産進捗の状況等）に随時・何度でも行うことができ、人員計画最適化の処理時間も数十分程度と大幅に短縮できるようになった。さらに、100名あまりの人員配置に際しての公平性（作業場所、チームの組合せ、担当外の業務割り当て等）を最適化要素に組み込むことで職場の満足度向上も期待される。新型コロナウイルスの影響が緩和される新時代においても、世界規模での生産性向上を実現し、SDGsの「8.働きがいも経済成長も」に対応する多様な働き方を達成かつ生産性を高めることが見込まれる。

[SIP 第2期の研究開発実績（まとめ）]

- ・アプリケーションプログラムを構成する部分プログラムの一部を次世代アクセラレータ・古典コンピュータ上で部分的に実行し、各種アプリケーションプログラムのボトルネックを調査した。ボトルネックと次世代アクセラレータとの相関性を調査した。
- ・次世代アクセラレータ・コデザイン問題を定式化し、各アクセラレータを協調的に動作させる最適化アルゴリズムを実現した。
- ・複数の次世代アクセラレータを協調して動作させるコデザイン基盤となるソフトウェアの実装を達成した。次世代アクセラレータ・コデザインソフトウェアを部分公開し、オープンテストベッド化を達成した。
- ・代表的なアプリケーションとして位置情報アプリケーションと周波数割当最適化アプリケーションに対して、古典計算機や古典アクセラレータのみの技術との比較で次世代ク

- セラレータ・コデザインソフトウェアが1桁以上の高速化を達成した。
- ・ポストコロナ時代の働き方に対応する次世代アクセラレータ活用の人員計画最適化基盤ソフトウェアの有効性を確認できた。一部の企業とはサービスインの合意をとり、企業による準製品化を完了し、社会実装コンソーシアムにおける活用を達成した。

実施内容 A2：次世代アクセラレータ・コデザインのライブラリ・API の研究開発

本実施内容 A2 における具体的な研究開発事項は、次世代アクセラレータと既存コンピュータとを相互にやり取りするための共通インタフェースを設計・開発し、次世代アクセラレータ・コデザインのライブラリ・API を研究開発することを目的とする。特に、共通インタフェースを抽象化し、アクセラレータ間の差異を意識させない相互利用を可能とすることにより、次世代アクセラレータ・コデザイン基盤を用いたアプリケーション開発エコシステムを構築することを目指す。

2019 年度～2020 年度の研究活動においては、次世代アクセラレータの比較検討を行うための統合計算機環境の設計を実施した。具体的には、以下の研究・開発を行うことにより、次世代アクセラレータ研究開発プラットフォームを構築した。

- ・イジング型コンピュータ/NISQ コンピュータへのアクセス手段の確立、および GPU/HPC 上で動作する誤り耐性ゲート型量子コンピュータ環境の構築を行った。
- ・次世代アクセラレータの比較検討を行う統合計算機環境の設計を行った。
- ・イジング型コンピュータ共通プラットフォーム向けインタフェースの開発を行った (NEDO との連携)。
- ・種々のアクセラレータで実行可能なライブラリ・API のプロトタイプの開発を行った。

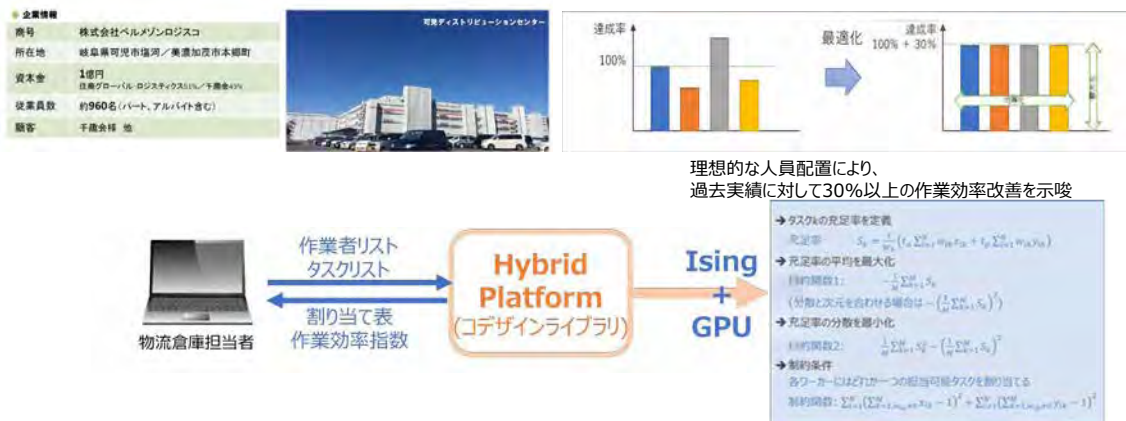


図 2-5-8. 物流倉庫における作業員最適配置の実証実験

また、構築した次世代アクセラレータ研究開発プラットフォームを用い、住友商事グループの物流倉庫における作業員最適配置の実証実験を実施した。この実証実験に際しては、実施内容 B4 と連携して実証実験のためのプロトタイプ API を開発した。この実証実験の目

的は最適化問題をコーデザイン・ライブラリで実行することであった。本実験では、作業員 100 名の 4 種類のタスクについて、イジング型コンピュータ及び GPU を実行環境として実行したところ、70 ミリ秒の計算時間で、理想的な人員配置により、過去実績に対して 30% 以上の作業効率改善を示唆する結果が得られた（図 2-5-8）。

2021 年度～2022 年度の研究活動においては、次世代アクセラレータの比較検討を行う統合計算機環境の設計を継続し、以下 2 項目を実行できる環境を完成させた。図 2-5-9 に次世代アクセラレータ研究開発プラットフォームを示す。

- ・イジング型コンピュータを選択的に実行可能とするインターフェースを構築した。
- ・NISQ コンピュータと誤り耐性ゲート型量子コンピュータのシミュレータと接続して、需要の高い組合せ最適化問題対応ができる環境を実現できた。

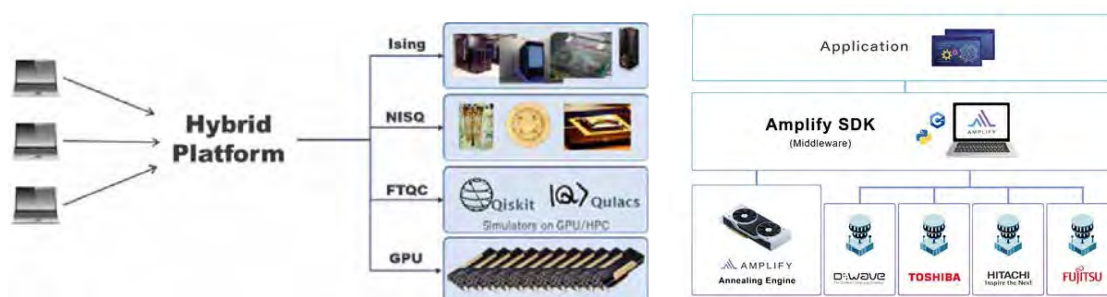


図 2-5-9. 次世代アクセラレータ研究開発プラットフォームと Amplify SDK の開発

更に 2022 年度の研究活動においては、2021 年度の次世代アクセラレータ研究開発プラットフォームを発展させ、次世代アクセラレータ・コーデザイン基盤を実現するソフトウェアの実装完了とオープンテストベッド化を完了し、代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術との比較評価を実施した。

- ・イジングマシン（商用マシン全て）、量子アニーリングマシン（D-Wave）、量子ゲートマシン（IBM-Q）、量子コンピュータシミュレータ、および数理最適化ソルバ（Gurobi/CBC）を利用可能な開発環境（図 2-5-10）を完成し、無償で一般に提供した。

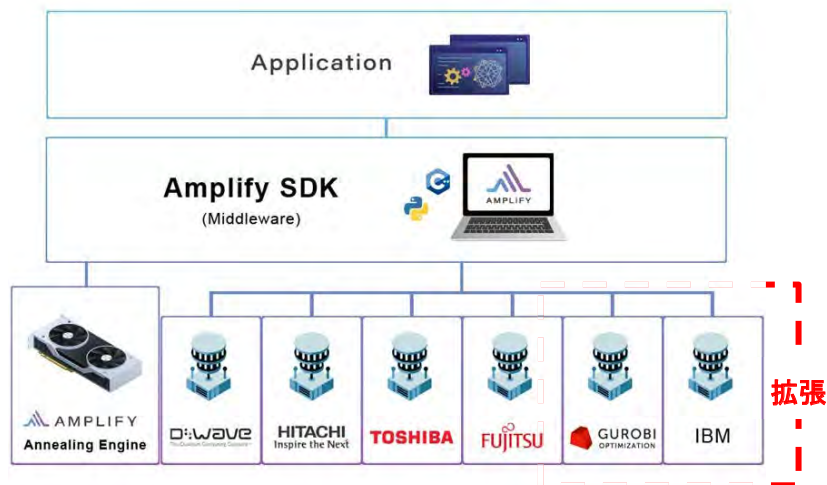


図 2-5-10. 次世代アクセラレータ統合実行環境で最適マシンを選択できる開発環境の拡張

- ・(株)フィックスターズで無償提供しているイジングマシン（Amplify Annealing Engine）の大幅な性能向上も実施した（2021年度の最大64倍：(株)フィックスターズ比）。
- ・また住友商事(株)と進めてきた物流倉庫における作業配置最適化問題に対して、上記の研究成果を活用し、計算速度は10倍以上を実現し、計算精度に関しても人による最適化と比べて大幅な生産性と満足度の向上を実現した。

[SIP 第2期の研究開発実績（まとめ）]

2022年度の設定目標である、次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装を完了し、オープンテストベッド化を完了する目標、および代表的なアプリケーションについて、次世代アクセラレータ基盤により、古典アクセラレータのみを活用した従来技術に比較して10-100倍の高速化を達成し、企業による準製品化を完了し社会実装コンソーシアムで活用する目標に対して、以下を実施し目標を達成できた。

- ・A1 のコデザインアルゴリズムとの連携により、次世代アクセラレータ統合実行環境で最適なマシンを選択できる開発環境（図 2-5-11）を実現できた。

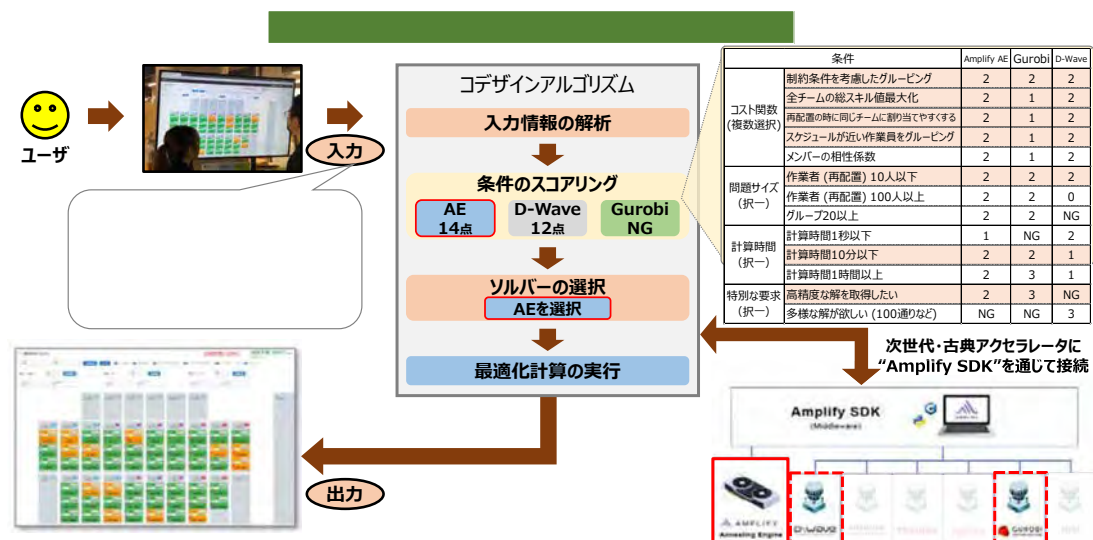


図 2-5-11. 最適な次世代アクセラレータを選択

- ・ イジングマシン（商用マシン全て）、量子アニーリングマシン（D-Wave）、量子ゲートマシン（IBM-Q）、量子コンピュータシミュレータ、および数理最適化ソルバ（Gurobi/CBC）を利用可能な開発環境を完成した。
- ・ Amplify SDKにより、多くのユーザー企業に量子計算を容易に実現できるためのソフトウェア開発ツールの提供を実現した。2022.9時点で、ユーザーの累計実行回数は、1,300万回を突破した。
- ・ 住友商事(株)と進めているスマート物流の社会実装において、問題に応じた適切な実行マシンの調査・検討が可能になり、計算速度・計算精度の向上を実現するための開発が完了した。
- ・ さらに、住友商事(株)と進めているスマート物流の社会実装において、物流倉庫における作業員最適配置でのこれまでの成果を活用し、(株)ベルメゾンロジスコにおいて2022.10より実サービスが開始された。本研究成果の活用により計算速度は10倍以上を実現し、計算精度も人による最適化とくらべて大幅な生産性と満足度の向上を実現した。

(B) 次世代アクセラレータインタフェース技術

実施内容 B1: イジング型コンピュータのインタフェース技術の研究開発

イジング型コンピュータのインタフェース技術の研究開発では、次世代アクセラレータの一つとして期待されているイジング型コンピュータを効率よく利用するためのインタフェース技術の研究開発を行った（図 2-5-12）。イジング型コンピュータでは、相互に関係を有する-1または1の値をとるスピンの集合（イジングモデル）が2つのスピン間の相互係数と自分のエネルギーの二次式で表された総エネルギーを最小化するようにスピンの向きを決めるという物理現象に基づいている。このため、本インタフェースでは解きたい問題

を制約条件やイジングモデルに変換する機能も含めて基本ソフトウェアを構築している。なお、問題によっては、イジングモデルと等価である 0 または 1 の値をとる変数の二次式を最小化する QUBO (Quadratic Unconstrained Binary Optimization) モデルが用いられる。

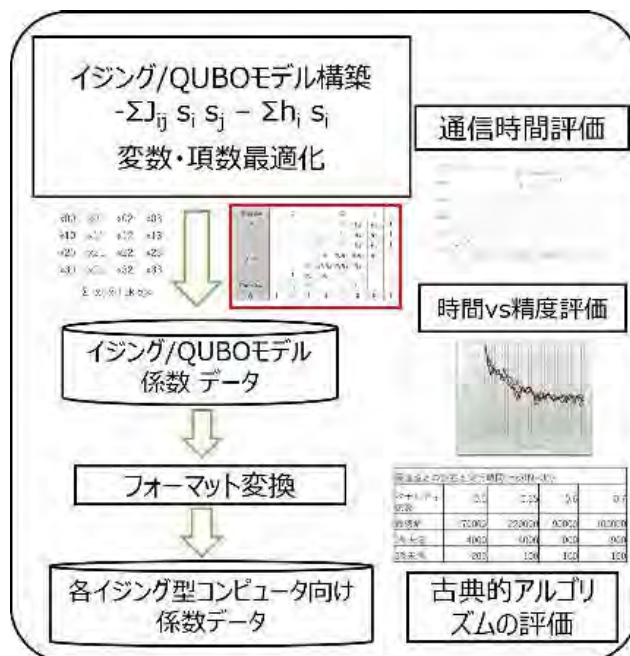


図 2-5-12. イジング型コンピュータのインターフェース

1) 組合せ最適化問題に対するインターフェースの整備を行い、問題をイジング/QUBO モデルへ変換するとともに、個別のイジング型コンピュータのフォーマットへ変換する環境の構築を行った。

代表的な組合せ最適化問題であるグラフのマックスカット問題、巡回セールスマン問題、二次割り当て問題について、イジング/QUBO モデルに変換する環境を構築した。また、イジング型コンピュータ毎で入力のフォーマットが少しずつ異なるので、いくつかのイジング型コンピュータに対してフォーマット変換を行うと同時に、イジング型コンピュータに独自のパラメータを問題ごとで決める方式を示した。

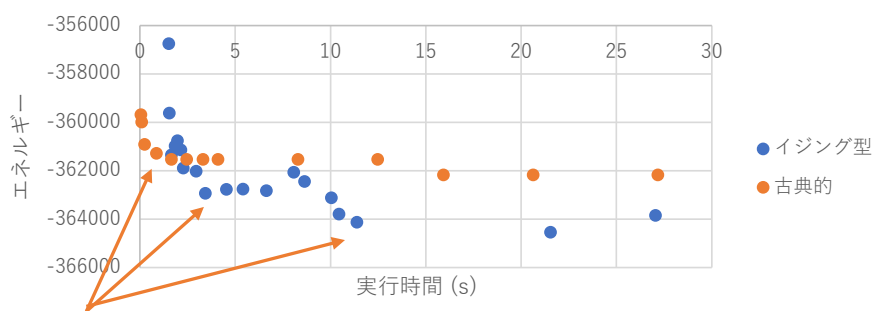
2) 組合せ最適化問題以外に対するインターフェースとして、因数分解に対するイジング/QUBO モデルの構築環境および古典的アルゴリズムと組み合わせる解く手法の提案を行い、60 ビットまでの二進数の因数分解を可能とするインターフェースを構築した。

因数分解は公開鍵暗号の基礎となるなど、計算量的に困難な問題として知られている。二進数の因数分解は二つの二進数の乗算の結果が因数分解したい二進数になるとして定式化でき、二進数の乗算を部分積の加算として表すことでイジング/QUBO モデルに変換できることが知られていた。しかし、既存手法では 30 ビット程度の二進数しか因数分解できなかった。それに対し、部分積の加算部の制約を一部しか使わないことと、古典的なアルゴリズム

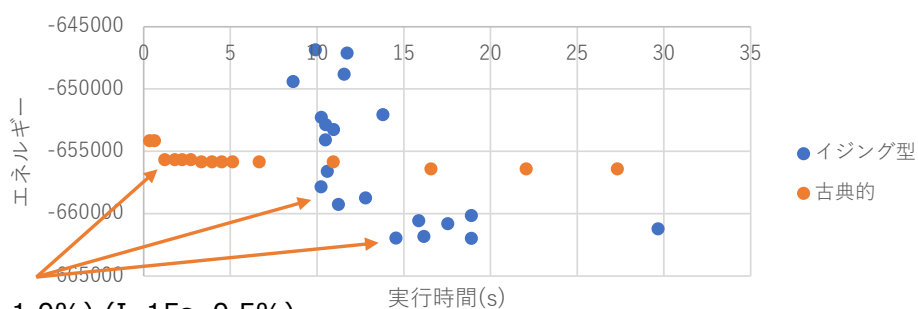
ムの組み合わせで、60 ビットの二進数の因数分解ができる手法の提案を行い、提案手法を用いるためのインタフェースを構築した。

3) イジング型コンピュータの実行時間、ペナルティ定数と解品質の評価をランダムに生成した巡回セールスマン問題および二次割り当て問題について行い、問題サイズと解品質に対して必要な実行時間の関係を明確化した。

いくつかのイジング型コンピュータに対して、ランダムに生成した巡回セールスマン問題や二次割り当て問題などについて実行時間と解の品質の調査を行った。また、同時にこれらの組合せ問題をイジング/QUBO モデルに変換するときに導入するペナルティ定数についても調査を行い、問題ごとに最適なペナルティ定数の決定方法を求めた。ローカルの計算機で実行することができるイジング/QUBO モデルのエネルギーを小さくする古典的なグリーディアルゴリズムを実現し、それを用いて問題を解く場合との比較を行った(図 2-5-13)。イジング型コンピュータを用いることで、古典的アルゴリズムに比べ、1/10 の実行時間でより品質の良い解が得られることが分かった。



(C, 1s, 1.5%), (I, 5s, 0.5%) (I, 15s, 0.2%)



(C, 1s, 2%), (I, 10s, 1.0%) (I, 15s, 0.5%)

50工場の二次割当問題 (サイズ 104MB)

図 2-5-13. 実行時間と得られたエネルギーの関係

4) イジング型コンピュータの実行時間について、入力データの転送時間を含めた総実行時間の推定手法を確立した。

イジング/QUBO モデルの構築においては、多項式変換などにより、入力である係数データのサイズが大きくなることがある。サーバーとして運用されているイジング型コンピュータを利用するには、入力データをサーバーまで送る必要があり、それがオーバーヘッドとなる。サーバーまでの通信環境はユーザーごとで異なるので、サーバーまでの通信時間をサンプルデータの転送で評価し（評価結果の一部を図 2-5-14 に示す）、それをういてイジング型コンピュータを用いて問題を解くのに必要な総実行時間の事前推定を行う手法を確立した。イジング型コンピュータは短時間の実行で比較的良好な解を得られるため、データの転送時間が総実行時間に占める割合は小さくない。ローカルの計算機で実行できる古典的なグリーディアルゴリズムでの実行時間を考慮し、ユーザーがイジング型コンピュータの利用の最適化を行えるようにした。

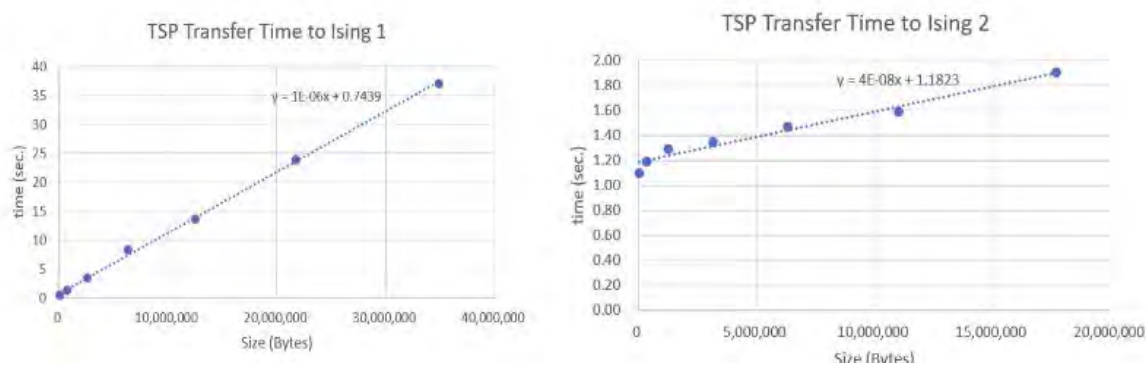


図 2-5-14. イジング型コンピュータサーバーに対する通信時間評価

5) イジング型コンピュータに関するインタフェースをいずれも API としてローカルコンピュータあるいはサーバーで動作するように実現し、配布できる形で整備を行った。

イジング型コンピュータ向けのイジング/QUBO モデルの作成とパラメータ値の推定、各種イジング型コンピュータフォーマットへの変換、データ通信時間を含む総実行時間の推定、イジング/QUBO モデル上の古典的アルゴリズムはいずれも API として実現し、古典的なローカルコンピュータあるいはサーバー上で動作する形で整備した。なお、サンプルデータを用いたイジング型コンピュータサーバーへのデータ通信時間は、データの存在するローカルコンピュータで行う必要があり、その結果を API で登録し、総実行時間の推定に用いる形で実現した。

[SIP 第 2 期の研究開発実績（まとめ）]

- ・ 組合せ最適化問題に対するインタフェースの整備を行い、問題をイジング/QUBO モデルへ変換するとともに、個別のイジング型コンピュータのフォーマットへ変換する環境を構築した。
- ・ 組合せ最適化問題以外に対するインタフェースとして、因数分解に対するイジング/QUBO モデルの構築環境および古典的アルゴリズムと組み合わせる解く手法の提案を行い、60 ビ

- ットまでの二進数の因数分解を可能とするインタフェースを構築した。
- ・イジング型コンピュータの実行時間、ペナルティ定数と解品質の評価をランダムに生成した巡回セールスマン問題および二次割り当て問題について行い、問題サイズと解品質に対して必要な実行時間の関係を明確化した。
- ・イジング型コンピュータの実行時間について、入力データの転送時間を含めた総実行時間の推定手法を確立した。
- ・イジング型コンピュータに関するインタフェースをいずれもAPIとしてローカルコンピュータあるいはサーバーで動作するように実現し、配布できる形で整備した。

実施内容 B2: NISQ コンピュータのインタフェース技術の研究開発

実施内容 B2 では、量子化学計算を対象とし、NISQ 上で量子化学計算を行うためのライブラリの実装、及び、(左記ライブラリを利用した) 実行時間見積インタフェースの実装を目的とする。NISQ コンピュータのインタフェース(実行時間の評価系)を考える上では、NISQ コンピュータがヒューリスティックであり、計算精度とアルゴリズム実行時間の関係は理論的には求まらない点を認識する必要がある。これに対して、本研究開発では、「経験的に」計算実行時間を求めるというアプローチを採っている。つまり、実際に様々な問題で計算した結果(実行時間)をデータとして蓄積し、既存のデータ点の内外挿により対象問題の実行時間を推計するという機械学習的なアプローチで実行時間見積機能を実装している。このアプローチを採るためには、実際に計算を実行してその結果を蓄積するための計算手法(ライブラリ)の充実が不可欠である。

2019 年度から 2022 年度にかけて次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装を完了し、オープンテストベッド化を完了した。代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ 10-100 倍の高速化を達成し、企業による準製品化を完了し、社会実装コンソーシアムで活用した。具体的な取組は以下の通り。

1) 次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装完了とオープンテストベッド化の完了

(1-1)実問題適用に向けた量子化学向けアルゴリズムエンジンの拡充

本研究開発では、多くの量子化学計算技術者が実際に研究開発の現場で使用する物性値を計算できるライブラリの実現を目指し、革新的なアルゴリズム開発を行うプレイヤーとの連携体制を構築し研究を進めた。2019 年度から 2022 年度にかけて以下の機能の実装を完了した。

- ・分子動力学: 第一原理電子状態計算で得られたポテンシャルエネルギーと原子核にかかる力を用いて古典軌道を追跡する手法で、化学反応や電子励起状態など多様な化学現象を高精度に記述できる。量子コンピュータ上で動作するエネルギーの核座標微分アルゴリズム

を用いて、第一原理分子動力学計算やその発展である Surface hopping 計算などを実施する機能を実装した。

- ・ 振動数解析：化学物質解析における重要な手法の一つ。振動数解析で得られる分子振動スペクトルは、分子の「指紋」のようなものであり、石油精製や水素製造プロセスにおける触媒反応解析等で重要な解析となっており、量子コンピュータ上で動作するアルゴリズムを実装し、潜在顧客への試験的公開を行った。
- ・ 光吸収スペクトラム：電子状態遷移に伴う可視光吸収スペクトルの計算が可能なアルゴリズムを実装し、潜在顧客への試験的公開を行った。
- ・ 構造最適化：よりエネルギーの小さい構造を算出し分子の安定構造を求める手法で、平衡状態の分子特性予測に有用とされている。量子コンピュータ上で動作するエネルギーの核座標微分アルゴリズムを実装し、潜在顧客への試験的公開を行った。
- ・ 周期系バンド構造計算：半導体やエネルギー変換材料等、あらゆる無機機能材料の機能設計に活用可能であり、高精度計算ニーズが高い。系の基底状態のエネルギーだけでなく、多体効果を取り入れたバンド構造の計算ができるアルゴリズムを実装し、潜在顧客への試験的公開を行った。
- ・ 相対論量子化学計算：相対論効果を含む 相対論的量子化学は重元素を含む分子の正確な物性予測に欠かせない。量子計算アルゴリズムでは相対論効果を（古典計算機とは異なり）ほぼ追加コスト無しで取り入れることができ、量子コンピュータ上で動作する相対論的効果を取り入れたアルゴリズムを実装し、潜在顧客への試験的公開を行った。

(1-2) NISQ コンピュータの計算時間推論エンジンの API 公開と古典アクセラレータとの比較インタフェース開発及びオープンテストベッド化の完了

計算時間推論エンジンの API 公開と古典アクセラレータとの比較インタフェース開発として、様々なサイズの分子の基底状態計算でアクセラレータ別（NISQ：計算エラーの由来としてショットノイズのみを仮定した VQE、古典コンピュータ：FCI 計算）の計算時間を見積もり、比較できるインタフェースを開発した（図 2-5-15）。

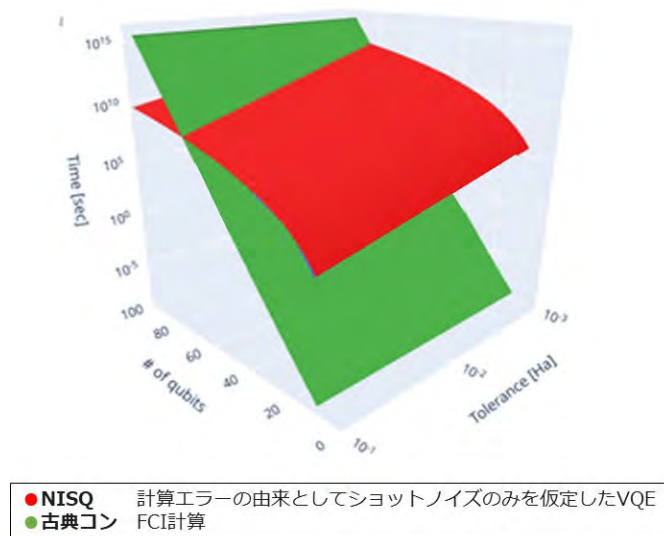


図 2-5-15. NISQ-古典アクセラレータの比較インターフェース

開発したライブラリ及び実行時間見積インターフェースは、(株)QunaSys が運営する社会実装コンソーシアム QPARC との連携の中で参加企業に実際に活用頂くことで、オープンテストベッド化を完了した。またオープンテストベッド的に活用して頂く中で、学術的・産業的な成果も得ることができた。具体的には以下の通りである。

- ・ 構造最適化：(株)豊田中央研究所との論文を出版した。原子核と電子の波動関数の虚時間ダイナミクスに基づいた分子の構造最適化手法を提案した (Hirotooshi Hirai, et al. Molecular Structure Optimization Based on Electrons-Nuclei Quantum Dynamics Computation, ACS Omega 2022, 7, 23, 19784-19793.)。
- ・ 光吸収スペクトラム：三菱ケミカル(株)・IBM と論文を出版した。量子コンピュータを用いて光化学で重要な量である「遷移振幅」を精度良く計算する手法を提案した (Yohei Ibe, et al. Calculating transition amplitudes by variational quantum deflation, Phys. Rev. Research 4, 013173 - Published 3 March 2022.)。
- ・ 振動数解析：ENEOS との取組が Microsoft の事例として公開された。上記に加え、分子軌道が縮退した際の数値不安定性を回避するような改良も実施した (アセチレン分子で安定して振動解析が可能に)。

<https://customers.microsoft.com/ja-jp/story/1536149625843093498-eneos-energy-azure-quantum-japanese>

また本取組は、Honeywell System Model H1 という取組時点で利用できる世界最高性能 (Quantum Volume512) の量子コンピュータを利用し、実機上でも、実際に要求精度を満たした計算が可能であることを確認した。計算時間見積誤差は±20%に収まり、計算時間のばらつき等のデータも収集ができた。

2) 代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ 10-100 倍高速化し、企業による準製品化を完了し、社会実装コンソーシアムで活用。
 (2-1) 特定の計算課題（分子など）において NISQ コンピュータが古典アクセラレータに比べて 10-100 倍高速化するユースケースの明確化

(1)にて開発を行った計算時間推論エンジンの API 公開と古典アクセラレータとの比較インターフェースを用いて、NISQ コンピュータが古典アクセラレータに比べて 10-100 倍高速化するユースケースを探索した。具体的には、分子の基底エネルギー計算の手法・マシン毎に実行コストを比較するための算出フローを整理するとともに、ベンゼンを対象にした計算を実行した。以下の通り、古典コンピュータよりも NISQ 計算が高速化するという見積結果が得られた（図 2-5-16）。

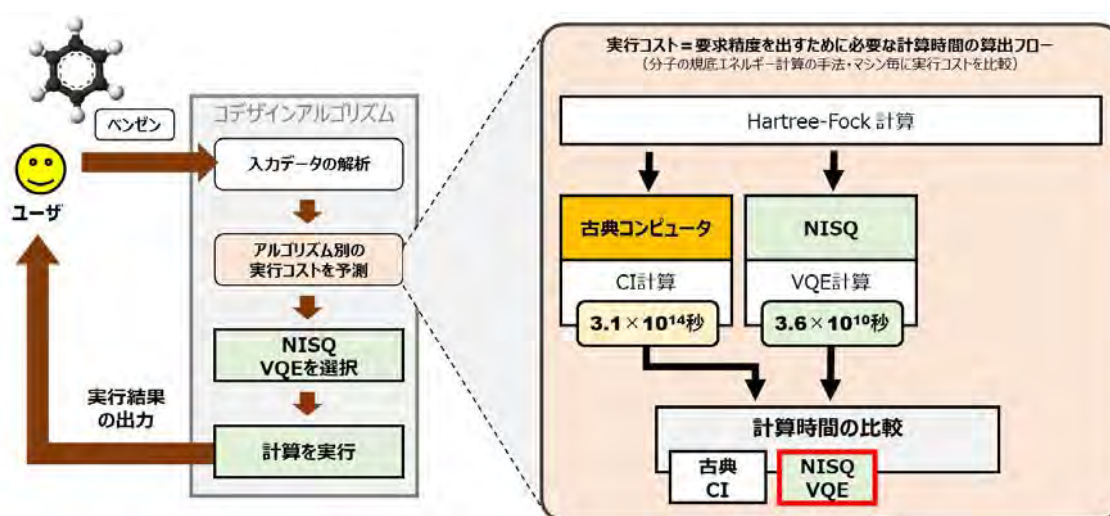


図 2-5-16. NISQ-古典コデザインのデモ計算（ベンゼン）。古典コンピュータ： 3.1×10^{14} 秒、NISQ： 3.6×10^{10} 秒。

(2-2) 社会実装したソフトウェアをコンソーシアムを通じて提供

コデザインのデモ計算は、(株)QunaSys が運営する社会実装コンソーシアム QPARC にて、民間企業に公表するとともにソフトウェアの利用意向及びフィードバックを獲得した。また、アルゴリズムライブラリを活用したハッカソンを開催し、世界中からオンラインで集まった参加者へチュートリアルを実施することでアウトリーチを推進した。

【SIP 第 2 期の研究開発実績（まとめ）】

- ・実問題適用に向けた量子化学向けアルゴリズムエンジンを拡充した（分子動力学・振動数解析・光吸収スペクトラム・構造最適化・周期系バンド構造計算・相対論量子化学計算）。
- ・NISQ コンピュータの計算時間推論エンジンの API 公開と古典アクセラレータとの比較インターフェース開発し、オープンテストベッド化を完了した（構造最適化：豊田中央研究所との論文を出版・光吸収スペクトラム：三菱ケミカル(株)・IBM との論文を出版・振動数解析：ENEOS との取組が Microsoft の事例として公開）。

- ・特定の計算課題（分子など）において NISQ コンピュータが古典アクセラレータに比べて 10-100 倍高速化するユースケースを明確化した（ベンゼンを対象にしたコデザインのデモ計算実施）。
- ・実装したソフトウェアをコンソーシアムを通じて活用を推進した（QPARC を通じたフィードバックの獲得やグローバルなハッカソンの実施）。

実施内容 B3: 誤り耐性ゲート型量子コンピュータのインタフェース技術の研究開発

実施内容 B2 の NISQ コンピュータとは異なり、誤り耐性ゲート型量子コンピュータは理論的な背景が強固であり、計算精度とアルゴリズム実行時間の関係を理論的に導出可能である。実問題という観点では、B2 で対象としている量子化学計算向けに、分子のエネルギーを求める「位相推定アルゴリズム」が提案されており、このアルゴリズムに基づいて実行時間を求めることが可能である。誤り耐性ゲート型量子コンピュータについては、現在世界的に開発が加速化しているものの、その実現は 10 年以上先となることを見込まれている。従って、本研究開発においては、古典計算機上のシミュレータを活用し、当該インタフェースの検証を進めた。

2019 年度から 2022 年度にかけて次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装を完了し、オープンテストベッド化を完了した。代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ 10-100 倍高速化し、企業による準製品化を完了し、社会実装コンソーシアムで活用した。具体的な取組は以下の通りである。

1) 次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装完了とオープンテストベッド化の完了

(1-1) 位相推定アルゴリズムを分子のエネルギー計算に応用した際の計算コストを推定するためのプログラムの実装

本研究開発では、実行時間見積インタフェースとして、位相推定アルゴリズムを分子のエネルギー計算に応用した際の計算コストを推定するためのプログラムの実装を完了した。誤り耐性ゲート型量子コンピュータで分子のエネルギーを求めるのに用いられる「位相推定アルゴリズム」について、いくつかの実装方法が提案されている。

- ・ Trotter 分解に基づく手法 : M. Reiher et. al., Proceedings of the National Academy of Sciences, Vol. 114, No. 29, pp. 7555-7560 (2017).
- ・ Qubitization に基づく手法 : D. W. Berry et. al., Quantum 3, 208 (2019).

2019 年度から 2022 年度にかけて先行研究を基にした実装及び最終年度は実際のハードウェアを開発しているベンダーと連携し、より精緻な時間見積を実現する実装を行った。

2020 年度は Trotter 分解に基づく手法での実装を完了した。先行研究の Trotter 分解による手法を基にプログラムを実装し、下記を行うことで実行時間推論エンジンのプロトタイプを開発した。

- ・ 計算コスト=必要な T ゲートの数
- ・ 種々のエラー量に対する最適化(最小化)

2021 年度は前年度に開発したプロトタイプの開発をさらに進めるため、前年度に実施した Trotter 分解よりも低コストで FTQC 実装が可能とされ、有力視されている手法である Qubitization を基にしたコスト推定の実装を行った。分子のエネルギーを求めた場合の計算時間見積を定式化し、API 向けに実装を完了した。

さらに 2022 年度は、光量子コンピュータのハードウェアベンダーである PsiQuantum と連携し、ハードウェアに即した、より精緻な実行時間予測を検討した。PsiQuantum のハードウェアを前提とした場合の計算リソース見積もり（特に、必要な計算時間と物理量子ビット数）について、プログラミングコード作成を実施した（PsiQuantum による論文 <https://arxiv.org/abs/2104.10653> と同等の手法を使用）。

PsiQuantum の提唱する Fusion based quantum computing に基づく光量子コンピュータハードウェアを用いた場合の予想計算時間および必要な論理量子ビット数・物理量子ビット数を算出するプログラムを作成し、実際の分子に対する検討も実行した（表 2-5-3）。

表 2-5-3. 水分子 H₂O に対する見積もり基底関数・論理量子ビット数・物理量子ビット数・推定実行時間

basis	logical qubits	physical qubits	time
STO-3G	1.0×10^3	2.0×10^6	4 m
DZ	2.1×10^3	4.5×10^6	30 m
6-311G	5.3×10^3	1.3×10^7	1 h 30 m
cc-pVDZ	6.9×10^3	1.8×10^7	5 h
cc-pVTZ	7.3×10^4	2.6×10^8	17 d

(1-2) 計算時間推論エンジンの API 公開と古典アクセラレータとの比較インタフェース開発
 実施内容 B2 における取組内容（図 2-5-16. NISQ-古典アクセラレータの比較インタフェース）に対して、本実施内容の成果を実装する開発を行った（図 2-5-17）。

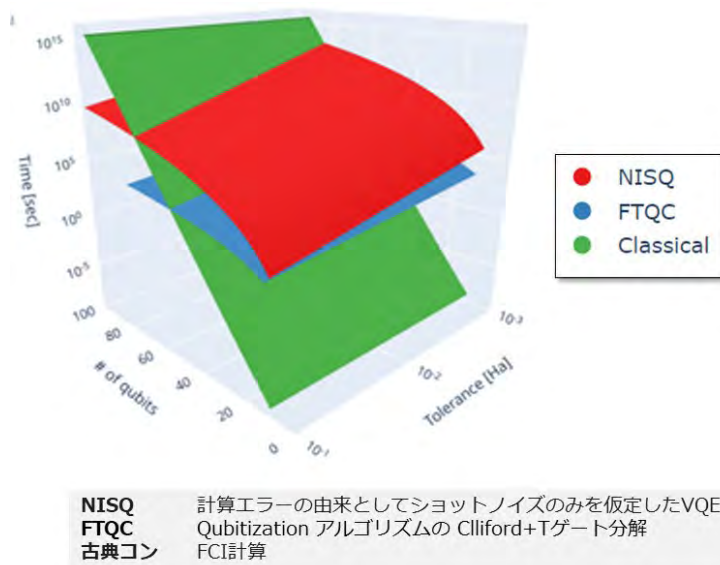


図 2-5-17. FTQC-NISQ-古典アクセラレータの比較インタフェース

2) 代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ 10-100 倍高速化し、企業による準製品化を完了し、社会実装コンソーシアムで活用 (2-1) 特定の計算課題において誤り耐性ゲート型量子コンピュータが古典アクセラレータに比べて 10-100 倍高速化するアプリケーション要件の定義

実施内容 B2 における取組内容 (図 2-5-16. NISQ-古典コデザインのデモ計算 (ベンゼン)) に対して、本実施内容の成果を実装する開発を行った。ベンゼンを対象にした計算を実行した。以下の通りで、FTQC 計算が古典コンピュータ及び NISQ よりも高速化する見積結果が得られた (図 2-5-18)。

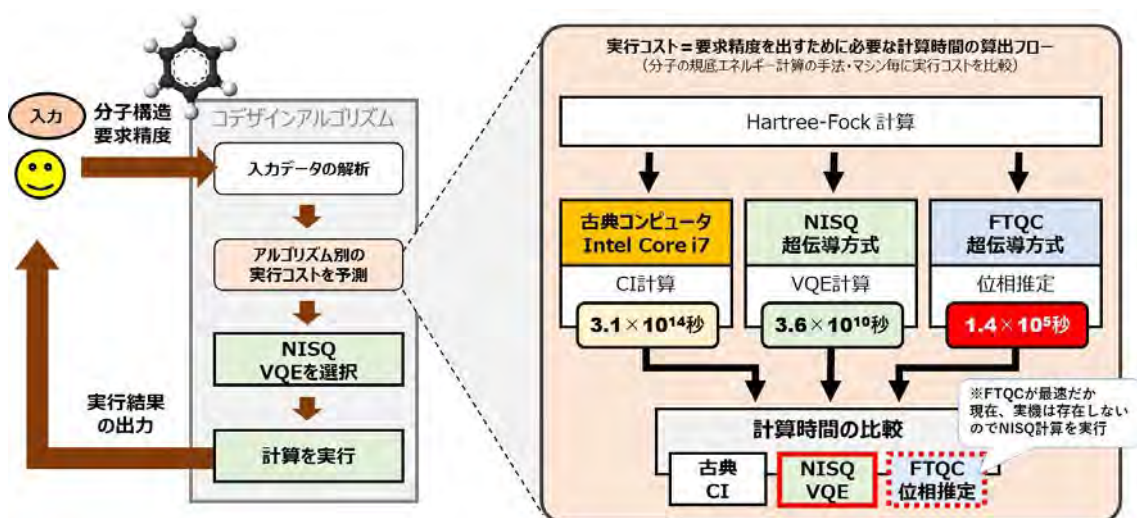


図 2-5-18. コデザインの計算過程 (ベンゼン)。古典コンピュータ : 3.1×10^{14} 乗秒、NISQ : 3.6×10^{10} 乗秒、FTQC : 1.4×10^5 乗秒。

(2-2) 実装したソフトウェアをコンソーシアムを通じて提供

本実施内容の成果は、上述の(株)QunaSys が運営する社会実装コンソーシアム QPARC にて、民間企業に公表するとともにソフトウェアの利用意向及びフィードバックを獲得した。それらの結果を踏まえ、SIP 開発期間終了翌年（2023 年度）より、本実施内容の成果を活用し 民間企業と共同事業開発を実施する。

[SIP 第 2 期の研究開発実績（まとめ）]

- ・位相推定アルゴリズムを分子のエネルギー計算に応用した際の計算コストを推定するためのプログラムの実装を完了した（ Trotter 分解に基づく手法・Qubitization に基づく手法・ Fusion based quantum computing に基づく手法）。
- ・計算時間推論エンジンの API 公開と古典アクセラレータとの比較インターフェースを開発した（実施内容 B2 の成果と連携し、NISQ・古典アクセラレータと本実施内容で実装した手法で計算時間を比較できる API を開発した）。
- ・特定の計算課題において誤り耐性ゲート型量子コンピュータが古典アクセラレータに比べて 10-100 倍高速化するアプリケーション要件を定義した（実施内容 B2 の成果と連携しベンゼンを対象にしたコデザインのデモ計算を実施した）。
- ・実装したソフトウェアをコンソーシアムを通じて提供した（民間企業における活用意向を踏まえ、SIP 終了後にプログラムとして活用する準備を行った）。

実施内容 B4: GPU 等古典アクセラレータのインターフェース技術の研究開発

本実施内容 B4 における具体的な研究開発事項は、GPU 等古典アクセラレータと諸問題との性質を調査した上で、GPU 等の古典アクセラレータを対象に、入出力オーバーヘッド、実行時間の評価系を研究開発することである。

2019 年度～2020 年度の研究活動においては、特に GPU 等古典アクセラレータのインターフェース技術の構築のために以下の研究開発を行った。

- ・イジング型コンピュータと GPU アクセラレータによる統合計算機環境の実現、およびその接続インターフェースの設計を実施した。
- ・古典アクセラレータによる古典対抗アルゴリズムの検討、および一部の実現を完了した。

これらの成果により、古典アクセラレータの性能を最大限に引き出す最適化コアアルゴリズムに適用でき、かつ統合計算機環境を実現できた(図 2-5-19)。



図 2-5-19. 統合計算機環境

2021 年度～2022 年度の研究活動においては、特に GPU 等古典アクセラレータのインタフェース技術の構築のために以下の研究開発を行った。またスマート物流の社会実装の実運用、GPS 型スマート製造の社会実装において、先進的成果の実現を行った。

- ・古典アクセラレータの性能を最大限に引き出す最適化技術をコアアルゴリズムに適用する研究の開発、および古典アクセラレータによる連携・補完・対抗アルゴリズムの開発を完了した。
- ・GPU 等古典アクセラレータのインタフェース設計とコデザイン問題の解法への適用を完了した。
- ・また、次世代アクセラレータ研究開発プラットフォームの社会実装に向けた取組みにおいては、2020 年度より住友商事(株)および住友商事グループの(株)ベルメゾンロジスコとのスマート物流プロジェクトでの協業を継続してきた。実際のオペレーションに必要な制約事項を反映した作業員配置最適化エンジンの開発を完了するとともに、現場における生産性のデータ化・分析を進めた。図 2-5-20 に物流倉庫における作業員最適化配置の社会実装開発の状況を示す。



図 2-5-20. 物流倉庫における作業員最適化配置の社会実装開発

- ・住友商事(株)と進めてきたスマート物流の社会実装の実運用に向けて開発した作業員配置

最適化エンジンをクラウドシステムと連携させ、2022.10より物流倉庫（㈱ベルメゾンロジスコ）においてサービスを開始した（図2-5-21）。



図2-5-21. 物流倉庫（ベルメゾンロジスコ）にて作業配置最適化サービスの運用開始

- ・GPS型スマート製造の社会実装の取組として、慶應義塾大学の田中先生・関先生とのレーザー設計条件最適化、慶應義塾大学の村松先生との材料安定構造シミュレーション計算開発に協力し、先進的成果を実現することができた。

[SIP第2期の研究開発実績（まとめ）]

2022年度の設定目標である、次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装を完了し、オープンテストベッド化を完了する目標、および代表的なアプリケーションについて、次世代アクセラレータ基盤により、古典アクセラレータのみを活用した従来技術に比較して10-100倍の高速化を達成し、企業による準製品化を完了し、社会実装コンソーシアムで活用する目標に対して、以下を実施し目標を達成した。

- ・QUBOで表される組合せ最適化問題が、GPU等古典アクセラレータおよび商用イジングマシンで統合的に実行可能なインタフェースの設計と実装を完了した（NEDO連携）。
- ・住友商事㈱と進めているスマート物流の社会実装において問題に応じた適切な実行マシンの調査・検討が可能になり、10倍以上の計算速度・計算精度の向上を実現できた。
- ・住友商事㈱と進めているスマート物流の社会実装の実運用に向けた取り組みをクラウドシステム連携により加速させ、2022.10より㈱ベルメゾンロジスコにて実サービスを開始できた。
- ・GPS型スマート製造に関しても社会実装に向けた取り組みを加速し、慶應義塾大学の田中先生・関先生とのレーザー設計条件最適化、慶應義塾大学の村松先生との材料安定構造シミュレーション計算開発研究において先進的成果を実現できた。

(C) 次世代アクセラレータの社会実装の促進

本実施項目では次世代アクセラレータの社会実装の促進を行うため、産業界から課題として認知されている、あるいは、産業界における幅広い課題につながる具体的な問題を設定し、それを次世代アクセラレータで処理するための定式化を行い、次世代アクセラレータを活用して解法した。

第一に、本 SIP における京都大学・フォトニック結晶レーザーチームとの連携による、フォトニック結晶レーザーの性能を向上させる結晶構造探索の定式化を行った（図 2-5-22（左））。この手法は、既利用のソフトウェア（フォトニック結晶レーザーシミュレータ、京都大学提供）、AI による学習、次世代アクセラレータ（イジングマシン）による推論の 3 段階から構成される。この手法について、次世代アクセラレータ・コデザインによる有効性評価を行った。推論部分について、従来計算機を用いた最急降下法、従来計算機を用いたメタヒューリスティクス、イジングマシンの三種類をもとに有効性評価を行ったところ、探索範囲が狭い場合には、従来計算機を用いたメタヒューリスティクスが有効、探索範囲が広い場合には、イジングマシンが有効であることを発見した。この結果をもとに、フォトニック結晶レーザーの性能を向上させるための最適化計算を行った。その結果、フォトニック結晶レーザーが有する多様な設計自由度を活用することにより、レーザーの性能を表す重要な指標である「光出力」「ビーム拡がり角」「直線偏光比」の 3 つ全てを向上することが可能な新たな構造を見出すことに成功した（図 2-5-22（右））。比較対象として用いた、従来コンピュータを用いたメタヒューリスティクスに比べ、少ない計算回数で高い性能が得られることが確認された。本成果は、製造分野への量子計算技術の適用可能性を示唆する重要な一歩である。また、この最適化計算を横展開した方法に基づく共同開発を社会実装コンソーシアムの企業とともに進めた。

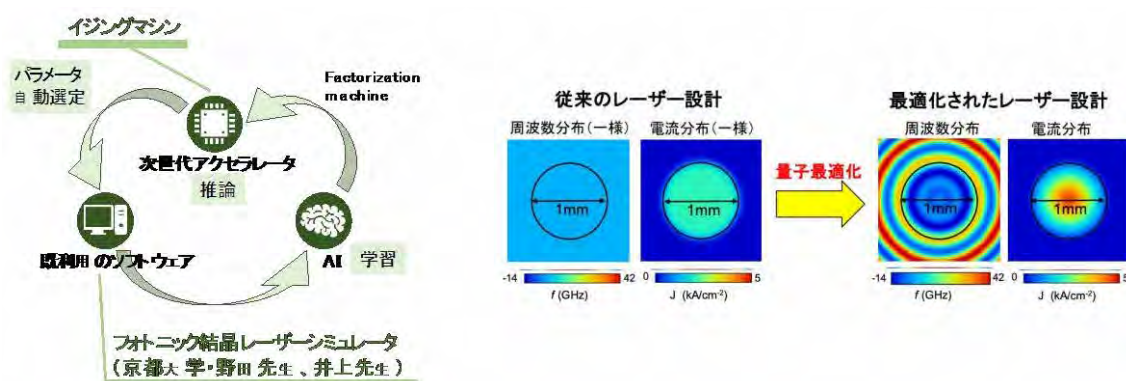


図 2-5-22. 左図はフォトニック結晶レーザーの性能を向上させる結晶構造探索高速化の定式化の概念図で、右図は提案手法によって得たレーザーの性能を表す重要な指標である「光出力」「ビーム拡がり角」「直線偏光比」の 3 つ全てを向上できるフォトニック結晶構造。

第二に、次世代アクセラレータの有用な用途として知られており、化学産業からも注目を集めている分子の基底状態計算について、次世代アクセラレータの一種であるイジング

マシンによる解法での解精度と近似度の関係について調査した。特に、分子の基底状態計算をイジングマシンで行う際に必須の近似度パラメータと解精度の関係を解析的に導出し、その結果をイジングマシン実機 (Fixstars Amplify) で検証した。

第三に、各種産業界からのニーズの高いブラックボックス連続最適化について、イジングマシンを用いて解法する方法の定式化を、SIP 第 2 期「統合型材料開発システムによるマテリアル革命」と連携して実施した。イジングマシン実機 (D-Wave Advantage) を利用して定式化の実証を行った。その結果、従来手法に比べて解精度の面で優位であることを見出した。

第四に、化学メーカーや素材メーカーからのニーズが高い複合材料の安定構造探索計算の定式化を、SIP 第 2 期「統合型材料開発システムによるマテリアル革命」と連携して実施した。またその定式化をイジングマシン実機 (Fixstars Amplify) で実証した。図 2-5-23 にあるように、網羅的なパラメータ依存性を調査することに成功した。また、提案手法は従来手法に比べ、3 桁程度の高速化が確認できた。また、この最適化計算を横展開した方法に基づく共同開発を社会実装コンソーシアム (QPARC) の参画企業とともに進めている。

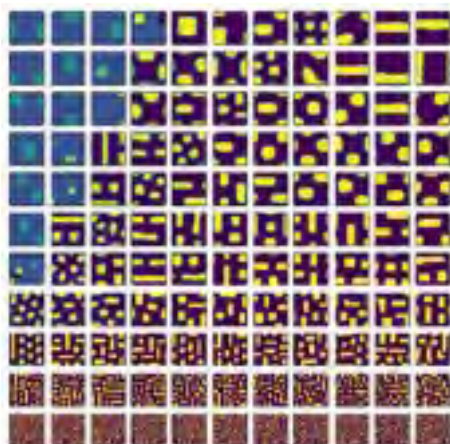


図 2-5-23. 複合材料の安定構造探索計算をイジングマシン実機 (Fixstars Amplify) で実行し、様々な物理パラメータ領域において安定構造を得ることに成功した。

第五に、第一で述べたフォトニック結晶レーザーの最適化計算について、量子セキュアクラウドシステムを用いた実証実験を実施した (図 2-5-24)。本実証実験では、量子計算技術を利用した次世代アクセラレータによって最適化された次世代レーザー (フォトニック結晶レーザー) の高度な設計情報を、今回初めてインターネット回線を用いて離れた拠点間で安全に送受信できることを確認した。

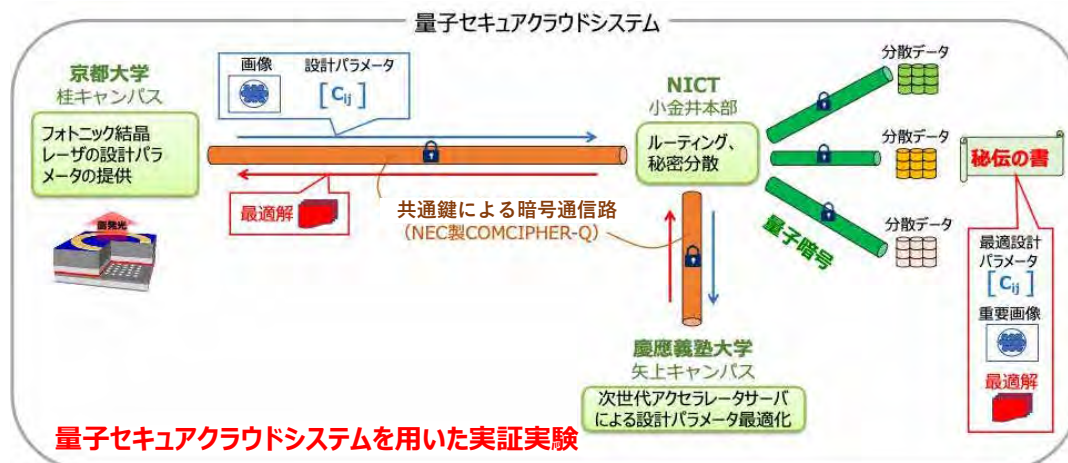


図 2-5-24. 量子暗号技術と秘密分散技術を融合した量子セキュアクラウドシステムを適用した検証試験の概念図

[SIP 第 2 期の研究開発実績 (まとめ)]

- ・ フォトニック結晶レーザーの高性能化を目的とした最適化計算を、次世代アクセラレータ・コデザインによる有効性評価に基づき実行し、従来コンピュータによるメタヒューリスティクスに比べ、少ない計算回数で高い性能が得られることが確認された。さらに、この最適化計算を横展開した方法に基づく共同開発を社会実装コンソーシアムの企業とともに進めた。
- ・ 分子の基底状態計算について、次世代アクセラレータの一種であるイジングマシンによる解法での解精度と近似度の関係について調査した。
- ・ ブラックボックス連続最適化について、イジングマシンを用いて解法する方法の定式化を実施した。この定式化を元にイジングマシン実機を用いたところ、従来手法に比べて解精度の面で優位であることを見出した。
- ・ 複合材料の安定構造探索計算の定式化を実施し、これをイジングマシン実機で実行したところ、従来手法に比べ 3 桁程度の高速化が確認できた。この最適化計算を横展開した方法に基づく共同開発を社会実装コンソーシアム (QPARC) の参画企業とともに進めている。
- ・ 量子セキュアクラウドシステムを用いた実証実験を実施した。

[達成度 (1) のまとめ]

SIP 第 2 期 5 年間の設定目標に対する達成度 (進捗状況) について得られた成果の新規の学術的・技術的価値、国際的な優位性を以下にまとめる。

実施項目	SIP第2期の目標	現状の達成度
A. 次世代アクセラレータ・コデザイン B. 次世代アクセラレータインタフェース技術 C. 次世代アクセラレータ活用の社会実装発	<ul style="list-style-type: none"> 次世代アクセラレータ・コデザイン基盤を実現するソフトウェアの実装完了とオープンテストベッド化の完了 (→ 達成) 	<ul style="list-style-type: none"> 複数の次世代アクセラレータを協調して動作させるコデザイン基盤となるソフトウェアの実装を達成 次世代アクセラレータ・コデザインソフトウェアを公開し、オープンテストベッド化を達成 スマート物流の作業配置最適化の社会実装において、コデザインアルゴリズムを適用した最適化計算の実行を実施。コスト削減、問題サイズ、計算時間、特別な制約条件を加味した計算において最適ソルバーを選択できることを実証 イジングマシン（商用マシン全て）、量子アニーリングマシン（D-Wave）、量子ゲートマシン（IBM-Q）、量子コンピュータシミュレータ、および数値最適化ソルバ（Gurobi/CBC）を利用可能な開発環境を完成し、無償での一般提供を実施済
	<ul style="list-style-type: none"> 代表的なアプリケーションへ適用評価し、古典計算機や古典アクセラレータのみの技術と比べ10-100倍の高速化し、企業による準製品化を完了し、社会実装コンソーシアムで活用 (→ 達成) 	<ul style="list-style-type: none"> 代表的なアプリケーションとして位置情報アプリケーションと基地局配置アプリケーションに対して、古典計算機や古典アクセラレータのみの技術との比較で次世代アクセラレータ・コデザインソフトウェアが1桁以上の高速化を達成 住友商事と進めてきた物流倉庫における作業配置最適化の問題に対して、上記の研究成果を活用し計算にかかる時間は10倍以上、計算精度に関しては人による最適化とくらべて大幅な生産性と満足度向上を実現

④ 達成度（2）※社会実装の実現可能性

1. 社会実装に向けた計画と進捗状況

本研究開発では、社会実装の考え方として適用領域（アプリケーション）と事業フェーズを2軸に、コアとなる基盤技術を確立しつつ、適用領域と事業フェーズを拡大することを狙う（図2-5-25）。また、CPS型スマート製造をはじめ、物流・配送、材料、センシング・データ解析など、さまざまな分野に適用領域を拡大しながら、Society 5.0社会の実現を図る。SIP第2期終了後にも継続的な社会実装創出を行うべく、早稲田大学に量子計算アプリケーション拠点を構築する。これにより、SIP事業期間内に加入の社会実装コンソーシアム企業（アーリーアダプタ層）との社会実装実例をもとに次世代アクセラレータに興味を抱くアーリーマジョリティ層の呼び込みやレイトマジョリティ層の取り込みを積極的に進めていく。いま着手できる社会実装対象から順次、社会実装対象を拡大していくという計画を進めている。

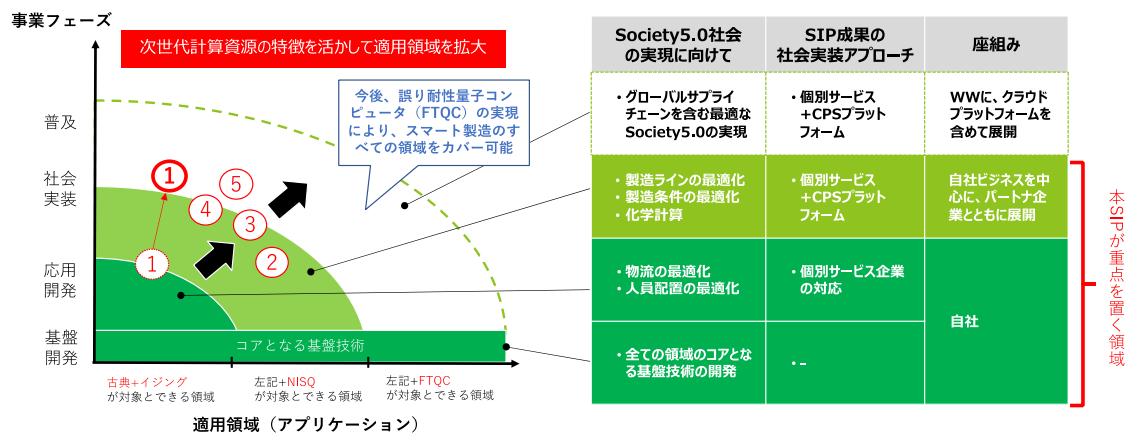


図 2-5-25. 本事業の社会実装の考え方

上記の計画をもとに、2022年度までに、すでに

- ① 物流倉庫における作業員最適配置の実証実験と基盤化
- ② レーザー加工への応用を見据えた実証実験
- ③ 化学計算領域におけるコンソーシアム立ち上げ
- ④ APIを通じた開発ライブラリの試験的な公開
- ⑤ 様々なユーザー企業との協業

を実施しており、後述する社会実装の体制等も活用し、順調に進展している。特に、①物流倉庫における作業員最適配置の実証実験と基盤化においては、2021年度の成果を活かし、更にユーザー企業との緊密な議論により、ユーザー企業のニーズを取り込んだ研究開発を実施し、2022.10には商用化が実現し、実工場現場で利用が開始された。以下、各項目について述べる。

① 物流倉庫における作業員最適配置の社会実装開発

2020年度からPOCが行われてきた、物流倉庫における作業員最適配置の社会実装開発（スマート物流プロジェクト）でのこれまでの成果を活用し、(株)ベルメゾンロジスコ（住友商事グループ）において2022.10より実サービスが開始された（図2-5-26）。物流倉庫の実際のオペレーションに必要な制約事項を種々取り入れ、実仕様に対応するための作業員配置最適化エンジンが利用されている。また、作業員配置最適化エンジンの結果検証に向けた、現場における生産性のデータ化及び分析を行うことにより、物流倉庫のDX化が達成された。

■ 実仕様に対応するための作業員配置最適化エンジンの開発



- ※『実際のオペレーションに必要な制約事項』を反映
- ・ 1人1タスク
 - ・ 3人で1チーム
 - ・ 手動で固定配置
 - ・ 相性ボーナス・ペナルティ
 - ・ 出荷予測値最大化
 - ・ 期ごとにグルーピング
 - ・ 出勤時間でグルーピング
 - ・ 一括配置・部分配置

本年10月より住友商事グループのベルメゾンロジスコでの、作業員配置最適化サービスを開始



解を瞬時に出力してくれるので、状況の変化にすぐに対応できる!

3人組のスキルまで考慮してくれるから、生産性が上がった!

人の配置を決めるのは負担が大きかったが、今は気持ち良くなった。

■ スキルデータを元に、工程進捗状況の可視化による当日の物流生産量に対する予実管理をリアルタイムに行えるSaaSとの連携

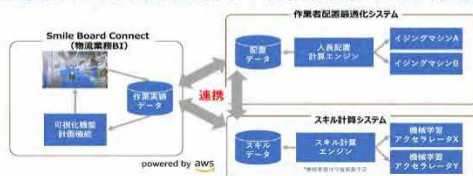


図 2-5-26. 物流センター現場での利用風景

② フォトニック結晶レーザーの構造最適化

フォトニック結晶レーザーの性能を向上させる結晶構造探索の定式化を行った。この手法は、既利用のソフトウェア（フォトニック結晶レーザーシミュレータ、京都大学提供）、AIによる学習、次世代アクセラレータ（イジングマシン）による推論の3段階から構成さ

れる。この手法について、次世代アクセラレータ・コデザインによる有効性評価を行った。推論部分について、従来計算機を用いた最急降下法、従来計算機を用いたメタヒューリスティクス、イジングマシンの三種類をもとに有効性評価を行ったところ、探索範囲が狭い場合には、従来計算機を用いたメタヒューリスティクスが有効、探索範囲が広い場合には、イジングマシンが有効であることを発見した。この結果をもとに、フォトニック結晶レーザーの性能を向上させるための最適化計算を行った。

その結果、フォトニック結晶レーザーが有する多様な設計自由度を活用することにより、レーザーの性能を表す重要な指標である「光出力」「ビーム拡がり角」「直線偏光比」の3つ全てを向上することが可能な新たな構造を見出すことに成功した。比較対象として用いた、従来コンピュータを用いたメタヒューリスティクスに比べ、少ない計算回数で高い性能が得られることが確認された。本成果は、製造分野への量子計算技術の適用可能性を示唆する重要な一歩である。また、この計算スキームを用いた量子セキュアクラウドシステムを用いた実証実験を実施した（図 2-5-27）。本検証試験では、量子計算技術を利用した次世代アクセラレータによって最適化された次世代レーザー（フォトニック結晶レーザー）の高度設計情報を、今回初めてインターネット回線を用いて離れた拠点間で安全に送受信できることを確認した。

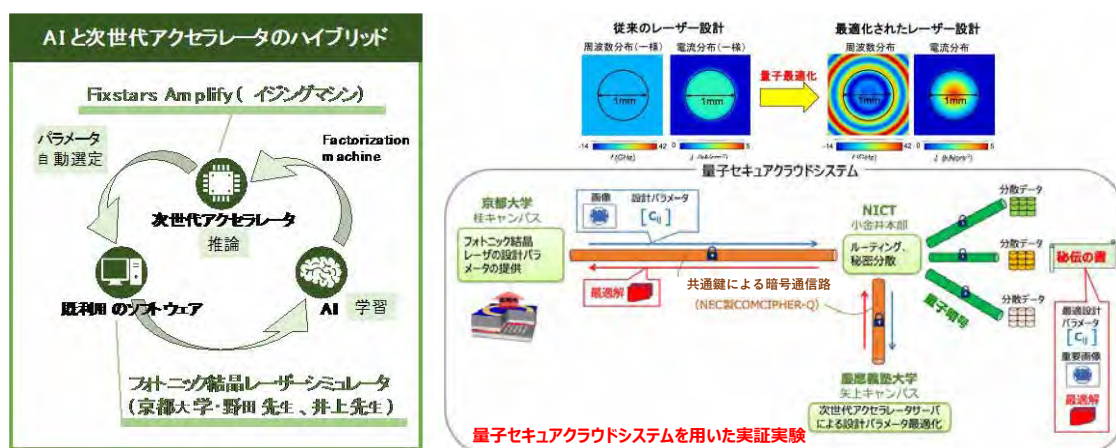


図 2-5-27. フォトニック結晶レーザーの最適化計算を題材とした量子暗号技術と秘密分散技術を融合した量子セキュアクラウドシステムを適用した検証試験の概念図

③ 化学計算領域における社会実装コンソーシアム QPARC

インタフェースの普及のためには、実際にユーザー企業が使用し、ユーザーニーズに則した機能実装を進めることが肝要と考えており、本研究開発では、各種ユーザーコンソーシアムと連携した社会実装を志向している。QPARC は株式会社QunaSys が 2020.4 に立ち上げたコンソーシアムであり、国内の主要材料メーカー、及び、自動車・エレクトロニクス関連企業 50 社超から計算技術者が集まっている。

QPARC を通じて、SIP の研究開発成果について、将来ユーザーとなる民間企業の研究者からフィードバックを得つつ、研究開発を推進した。

2022 年度においては、次世代アクセラレータ基盤の研究開発と社会実装をアウトリーチするため、早稲田大学・(株)フィクスターズ・慶應義塾大学・(株)QunaSys の 4 社で QPARC を活用したセミナーを実施した。

量子技術の社会実装における産学連携の課題と重要性をユーザー企業にも強く理解して頂くことを狙いとし、約 40 社から約 100 名が参加した。(図 2-5-28)



図 2-5-28. QPARC を通じた社会実装イベントの実施

量子コンピュータの産業化という観点から社会実装の課題を討議し、参加企業への社会実装に関するアンケートも実施し、次世代アクセラレータの取組に対して関心があるというフィードバックを得られた。(図 2-5-29)

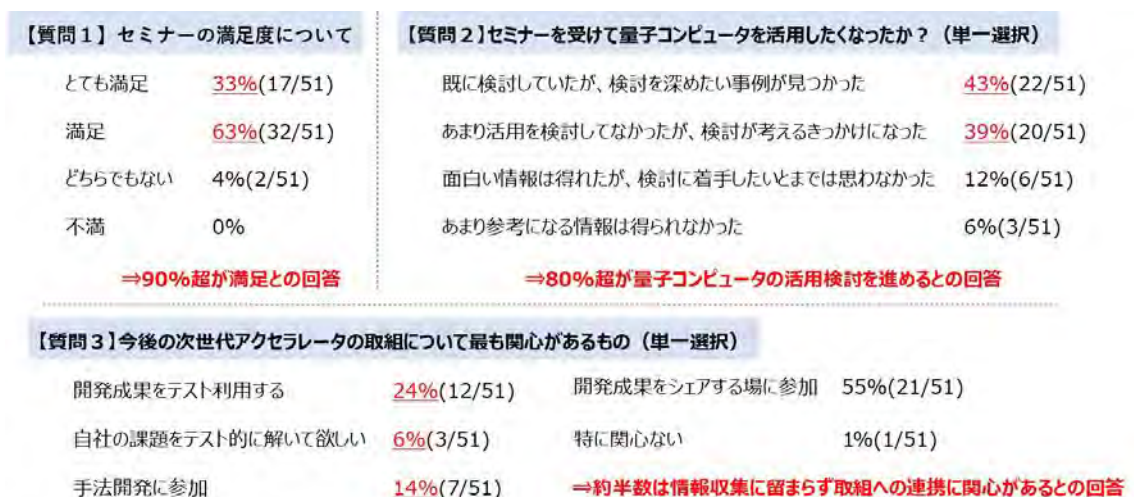


図 2-5-29. 参加企業へのアンケート結果