

革新的研究開発推進プログラム（ImPACT）

終了時評価報告書（平成30年度）

「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」

平成31年3月13日

P M 名：山本 喜久

P M補佐名：加古 敏

佐藤 由希子

研究開発プログラムの全体計画

(1) 研究開発プログラムの構想

① 解決すべき社会的課題

現代社会の様々な分野（創薬・生体触媒、無線通信、圧縮センシング、機械学習、電力・物流・交通ネットワーク、宇宙開発、金融工学など）に現われる組合せ最適化問題・連続量最適化問題は計算量理論でいうところの NP 完全・NP 困難クラスに属しており、現代の高性能コンピュータを以ってしても、これを効率よく解くことは容易ではない（図 1）。変数が離散値を取る組合せ最適化問題・変数が連続値を取る連続量最適化問題に特化した量子コンピュータや量子アニーリングマシンが欧米を中心に研究開発されているが、実問題を解くことができる大規模なシステムを実現する目処は立っていない。

現代コンピュータの性能限界に安全基準をおく現代暗号（公開鍵暗号）は、コンピュータ技術の進展に伴って将来盗聴される、あるいは既に盗聴されている危険性を内包しており、常に改訂や変更を繰り返す必要があるシステムである。また、クラウドサービスの普及が進み、クラウド上に保存した個人情報・機密情報や計算データのセキュリティをどう担保するか、が重要な社会的課題となっている。これらの問題を解決すべく量子鍵配送の研究開発が過去 30 年にわたって世界各国で行なわれてきたが、この技術は通信路のセキュリティの確保にのみ有効であり、クラウドも含めた情報通信システム全体のセキュリティ解決策にはまだなっていない。

新物質（例えば、室温超伝導材料、トポロジカル物質）探索はこれまで材料・物性研究者の直感に頼る形で発展を遂げてきた。その理由の一つは、物質内の電子の振る舞いを記述する量子力学的モデルを、現代コンピュータで効率よくシミュレーションできなかったからである。代わって、制御性のよい別の量子系を用いた模擬実験、いわゆる量子シミュレーションの研究が世界的に行なわれているが、簡単・自明な小規模問題での原理実証段階に留まっている。

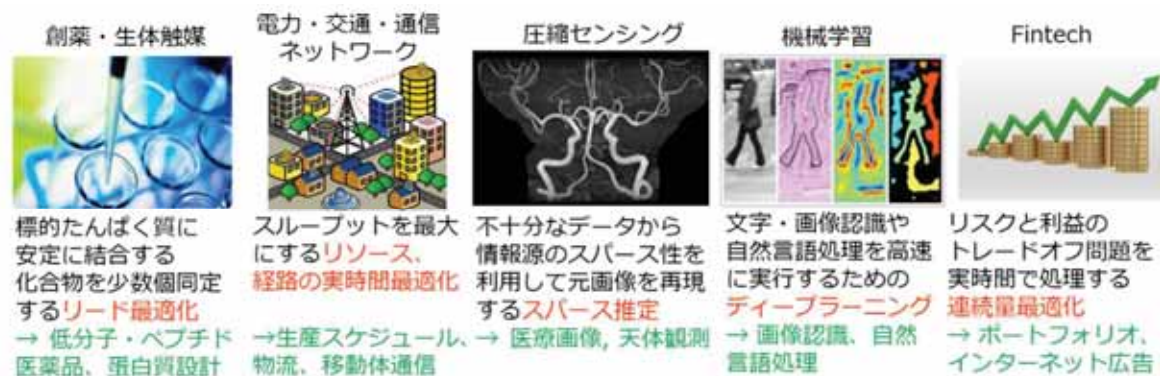


図 1. 代表的な組合せ・連続量最適化問題.

② 上記の社会的課題を解決し、産業や社会のあり方に大きな変革をもたらす PM の構想

安い労働力と長時間労働により、既知の原理、知識、技術を組み合わせて商品化し、価格競争を以って市場を獲得し国を支えるという産業構造だけでは 21 世紀の日本を支えられない。新しい原理・知識を世界に先駆けて獲得し、その知識に基づく新技術や新サービスを資源として国を支える高度知識社会へ変貌を遂げていく必要がある。量子コンピュータ技術とそれが創造するであろう新たな知識・技術・サービスは、そうした社会変革の中核をなす原動力のひとつとなりうる。実際世界各国の主要研究機関では、量子コンピュータの開発に多額の研究費が投下されている。表 1 に代表的なものをまとめる。

表 1. 3 つの量子コンピュータの原理、主要研究機関、性能の比較。

	ゲート型	アニール型	ネットワーク型
原理	線形干渉計	量子トンネリング	非線形発振器
主要開発機関	IBM/Google/Intel	D-WAVE/MIT	NTT/Stanford
ビット数 *	20 (50~100) ビット	2,000 (8,000) ビット	2,000 (100,000) ビット
有効ビットの割合	—	98%	100%
結線数	—	6,000 (スパース結合)	4,000,000 (全結合)
デコヒーレンス時間	1~10 μ sec	$\lesssim$ 100 nsec	$\gg$ 10 msec
解ける問題サイズ	—	$N \lesssim 60\sim70$	$N \lesssim 2,000$
動作温度	極低温 (10mK)	極低温 (10mK)	室温 (300K)
条件	超高真空	超高真空	常圧
物理系	超伝導量子回路	超伝導量子回路	光パラメトリック発振器 ネットワーク
量子性 $k_B T / \hbar \omega$	0.06	0.06	0.02
消費電力	—	25 kW	1 kW

* カッコ内の数字は次期マシンのビット数

このうち、ゲート型あるいはアニール型の量子コンピュータを実用的なマシンにするためには、量子ビット数が $10^8\sim10^{11}$ にも達する大規模なシステムとならざるをえない。これは、次のような理由による。ゲート型では、量子誤り訂正とユニバーサル量子計算を可能にするために、計算に直接使う量子ビットに加え膨大な補助量子ビットを必要とする。一方、アニール型では、量子情報が局所スピンに格納されているため、その相互接続に限界があり（通常は隣接量子ビット間でのみ結合）、解くべき問題の埋め込み（マイナー・インベディングという手法が用いられる）に膨大なグラフサイズが必要になるためである。この点、ゲート型、アニール型量子コンピュータは、メモリとプロセッサが空間的に分離されている現代コンピュータやニューロン間の密シナプス結合が実装上のボトルネックとなる古典ニューラルネットワーク電気回路と同じ弱点を持っているといえる。我々は、全ての量子情報

をネットワーク（計算機）全体に広がった1つの巨大な波動関数に載せることにより、この相互接続（通信ボトルネック）の問題は解決できるはずであると考えた。

もうひとつの視点として、ゲート型あるいはアニール型の量子コンピュータは、組合せ最適化、連続量最適化という視点から見ると、このタスクからかけ離れた非常に論理回路的な動作原理に基いている。ゲート型では、状態ベクトルのユニタリ回転のみを道具立てとし、アニール型では、ハミルトニアン of 断熱変化のみを道具立てとし、最適化というタスクを実現させようとしている。我々はここに（達成したいタスクとマシンの動作原理の間に）重大なミスマッチがあると考えている。一方、自然界における相転移現象、例えば、水が 0°C 以下で氷になる液相一固相転移では、膨大な数にのぼる状態の中からエネルギーが最小となる秩序相を系が自発的に捜し実現している。このような相転移臨界現象をそのままハードウェアに埋め込んだコンピュータこそが、我々が必要としているものではないか、というのが基本的な考え方である。

このような思想に基いて設計されたネットワーク型の量子コンピュータがコヒーレント・イジングマシン、コヒーレント SAT ソルバー、コヒーレント XY マシン、コヒーレント暗号マシンである。現代コンピュータのアクセラレータとしてこれらのマシンをメインフレームに接続したものが、本プロジェクトで開発しようとする量子人工脳である（図2）。

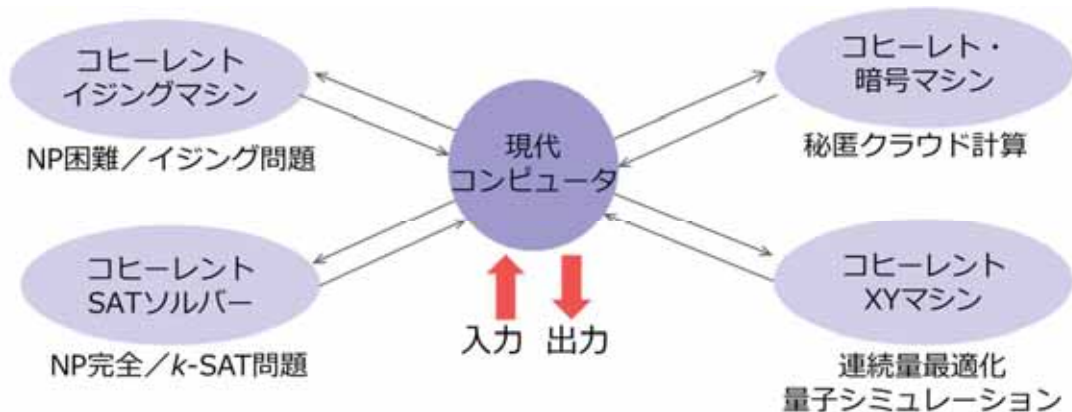


図2. 量子人工脳：現代コンピュータのアクセラレータとしての4種類の量子ニューラルネットワークから成る。

現代コンピュータが不得意な4つのタスクである、NP 困難組合せ最適化問題はコヒーレント・イジングマシンに、NP 完全組合せ最適化問題はコヒーレント SAT ソルバーに、NP 困難連続量最適化問題・量子シミュレーションはコヒーレント XY マシンに、これらの計算を秘匿クラウド計算として実行するタスクはコヒーレント暗号マシンに、それぞれ分担させる。現代社会の様々な分野に現われるこれら最適化問題を高速に解く複数の量子ニューラルネットワークを、現代コンピュータのアクセラレータとして使うというのが、我々の量子コンピュータ技術の将来像である。

③ 出口目標及び出口に至るシナリオ

量子人工脳

開発するコヒーレント・イジングマシン、SAT ソルバー、XY マシンの正答率／近似精度、サンプリング性能、計算時間、消費電力を現代コンピュータに搭載した最先端アルゴリズムと定量的に比較し、その優位性を実証すると共に欠点を明らかにする。長所・短所を明らかにすることにより、適用分野を絞り込む。開発したマシンをクラウドサービスに供し（平成 29 年度から実施）、世界の量子コンピュータ研究の主流（メインストリーム）であるゲート型、アニーリング型に加え、ネットワーク型の特徴を世界へ向けてアピールする。プロジェクト外のソフト開発者も巻き込んで、新たなアプリケーション・アルゴリズムの開発を行い、社会実装につなげる。コヒーレント暗号マシンに関しては、基礎研究段階にあるものと捉え、ユニタリ暗号化の手法を発見し知財の獲得を目指す。

量子セキュアネットワーク

物理層／鍵管理層／アプリケーション層の 3 階層構造でシステムを開発する。物理層は 10km 圏、50 km 圏、90 km 圏の量子鍵配送（QKD）リンクから構成し、盗聴検知機能、及びサイドチャネル攻撃対策を実装する。鍵管理層には、異なるベンダーから供給される鍵を統一的かつ効率的に運用する機能を実装し、かつ盗聴攻撃への自動経路切り替え機能などスマート化を進める。アプリケーション層には、しきい値秘密分散プロトコルを実装して、サーバ上の保存情報の秘匿化を実現する。防衛・金融・医療・スマートインフラ分野のユーザと密接な情報交換を行いながら開発し、専用暗号システム、汎用的なルータ、サーバ、スマート機器への自在な鍵供給を実現する（図 3）。3 階層の開発は並行して進め、プロジェクト終了時までの完成を目指す。その後、順次社会実装を目指す。

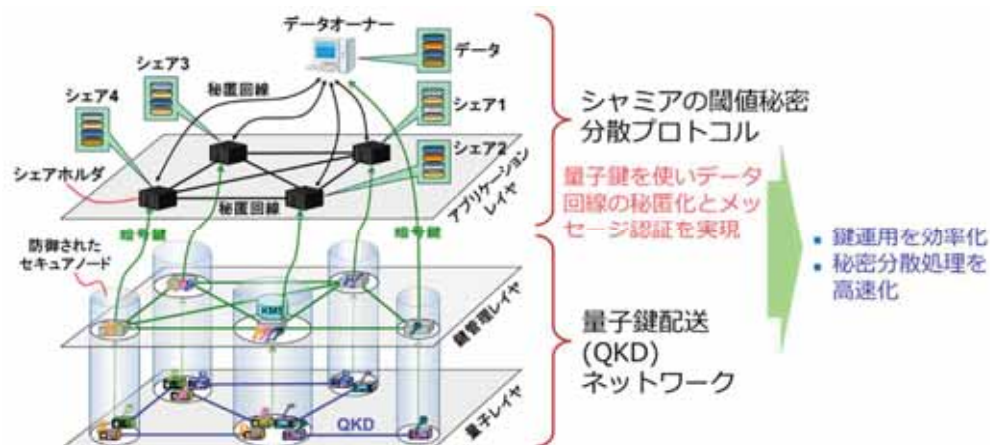


図 3. 3 階層構造からなる量子セキュアネットワークシステム。

量子シミュレーション

超伝導転移温度 T_c が、銅酸化物超伝導体の T_c ($\approx 120\text{K}$) の3倍（すなわち室温）に至る結晶構造を理論的に探索し、光格子中の冷却原子を用いた大規模模擬実験により、予言の正当性の検証を行う。具体的には、2次元2層正方格子構造における電子相関系にターゲットをおく。また、様々な量子系のダイナミクスを記述する理論モデルを用いた数値シミュレーション・プログラムを開発し（図4）、これをオープンソースとして公開し、世界の研究者への普及に努める（平成29年度中に開始）。さらに、ボゾンでもフェルミオンでもない第3の量子粒子と言われるエニオンの実現とその量子情報処理への適用可能性を探索する。



図4. 量子シミュレーションモデルの階層構造。

④ 解決のための発想・アイデア及びブレークスルーのポイント

量子人工脳

ブレークスルーのポイントは、1つの新概念と2つのデバイス技術からなる。

➤ 量子臨界計算（新概念）

以下に述べる量子ニューロン（光パラメトリック発振器）が生成する真空スクイーズ状態が有する（正の振幅 $|X\rangle$ と負の振幅 $|-X\rangle$ の）線形重ね合わせ状態を用いた量子並列探索により与えられた問題の最適解（global minimum）を絞り込み、その後パラメトリック発振（自発的対称性の破れ）現象を用いて一つの最適解を選択し、更に光子の誘導放出現象（bosonic final state stimulation）を利用して選択した解を量子レベルから古典レベルへ一気に増幅し、出力する（量子 - 古典クロスオーバー）。この3ステップからなる量子臨界計算という新原理が最も重要な基本発想である（図5）。

➤ 量子ニューロン（デバイス #1）

光ファイバーリング共振器を周回する多数（ $10^2 \sim 10^6$ ）の光パラメトリック発振光パルス一つ一つを量子ニューロンとして用いる（図6）。この量子ニューロンは、発振しきい値以下のポンプレートではアナログ素子として振舞い、量子並列探索を可能とする。一方、発振しきい値以上のポンプレートでは、この量子ニューロンはデジタル素子として振舞い、量子 - 古典クロスオーバーにより確定した

古典情報（0 または 1）を出力する。このアナログ／デジタルの両側面をあわせ持つ量子ニューロンを情報キャリアとする。

➤ 量子シナプス（デバイス #2）

光パラメトリック発振光パルスの一部を時分割で光ファイバーリング共振器外に取り出して、ホモダイン検波することにより、内部の光パルスの量子状態を保護しつつ、光パルスの振幅と位相を読み出し、デジタル電子回路と光変調器を用いてフィードバック光パルスを生成し、ターゲット光パルスに注入する。こうして、量子ニューロン（光パルス）間の任意の結合を一つの量子測定フィードバック回路だけで実現できる（図 6）。これまで困難であった全てのニューロン間の任意の重みによる全結合を実装できる。

➤ 他方式との比較

表 1 に、ゲート型、アニール型、ネットワーク型の量子コンピュータの現時点での実機性能を比較した。ネットワーク型の優位性はこの表から明らかであるが、その主な長所（室温動作、2000 ビット全結合、無欠陥量子ビット）は、光パラメトリック発振器を量子ニューロンとして採用したこと、測定フィードバック回路を量子シナプスとして採用したことに起因している。

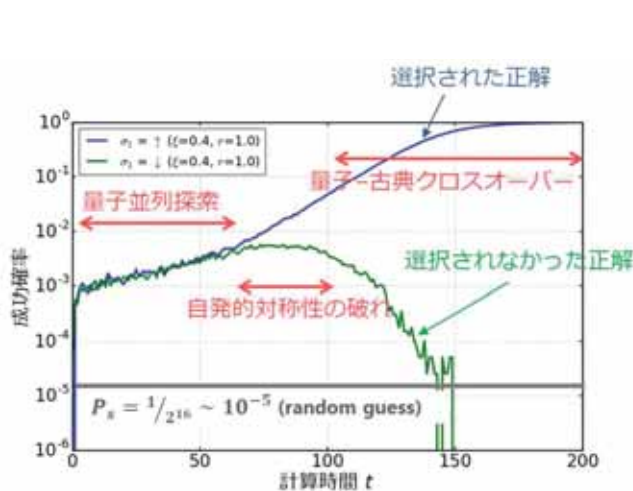


図 5. 量子臨界計算における 3 ステップを示した数値シミュレーション例。
 $N = 16$ 次元イジングリングの正答率対計算時間。

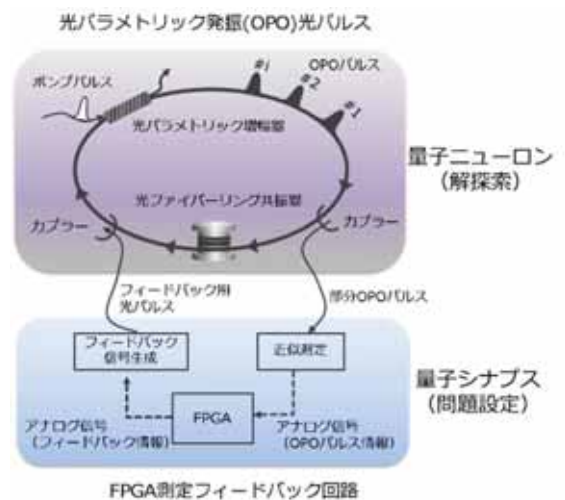


図 6. 量子ニューロンと量子シナプスの構成。

量子セキュアネットワーク

ブレークスルーのポイントは、量子鍵配送と one time pad 暗号通信による通信路セキュリティの確保としきい値秘密分散によるクラウドセキュリティの確保を組み合わせた点にある。

➤ クラウド上の超長期間安全性保証

原理的に盗聴を許さない量子鍵配送による秘密鍵生成技術と one time pad 暗号通信に、情報理論的安全性が保証されているしきい値秘密分散による秘密情報の

保存技術を組み合わせて、クラウド上の情報の超長期間安全性（＞100 年）を実現する。

量子シミュレーション

大規模・均一・無欠陥の量子多体系を実装できる、それぞれ固有の特徴を有する光格子中の冷却原子や超伝導回路、半導体素子を量子シミュレータのハードウェアとして採用した。また、効率的な数値シミュレーションを可能にする理論モデルとして、平均場理論、量子モンテカルロ法、などを取り上げ、それぞれの改良に取り組んだ。室温超伝導を目指す取り組みとして、電子間斥力（電子相関）と電子格子相互作用の両者がどのように絡み合っているかを、ダイアグラム量子モンテカルロ法を用いて調べる。また、超伝導体を非平衡にドライブしたときのダイナミクスや、ヒッグス・モードのような集団励起との関わりを、非平衡動的平均場理論等を用いて調べる。

➤ 2次元2層正方格子

斥力相互作用を持つスピンを有する電子を図7に示すような2次元2層正方格子上に配すると、銅酸化物超伝導体（2次元単層正方格子）と同様、電子相関による超伝導が発現し、同時に2次元単層正方格子ではd波超伝導体になってしまったものが、2層にすることにより、これとは異なるs波超伝導体を実現する。その臨界温度 T_c は銅酸化物超伝導体のその3倍以上になると予測される。

➤ Yb 冷却原子量子シミュレータ

上記仮説を実証するため、レーザ光の干渉縞により2次元2層正方格子を作り、ここにレーザ冷却されたYbフェルミ原子を電子の代わりにトラップして、その超流動転移温度の評価から、上記理論予測を定量的に評価する。

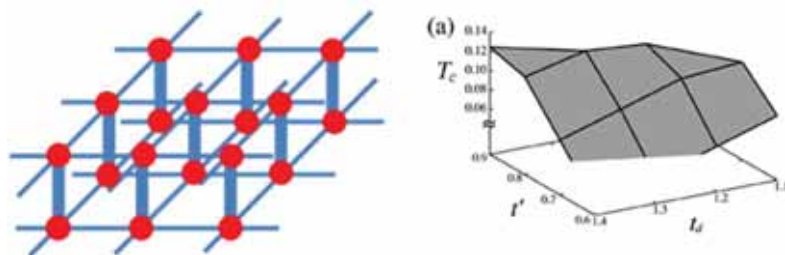


図7. 2次元2層正方格子中の斥力相互作用を持つスピンを有する電子が示す超伝導臨界温度 T_c 対トンネル係数 t' , t_d .

(2) 研究開発プログラムの達成目標

- ニューロン数 100、シナプス結合数 10,000（全結合）の小規模量子ニューラルネットワーク、ニューロン数 2048、シナプス結合数 4,194,604（全結合）の中規模量子ニューラルネットワークを開発し、量子臨界計算のコンセプトを原理実証する。開発したマシンをインターネットを介して外部ユーザに供し、世界中の研究者が自由に使えるクラウドサービス環境を実現する。

- ニューロン数が $\sim 100,000$ 、ニューロン間シナプス結合数が $\sim 10^{10}$ （全結合）の大規模量子ニューラルネットワークを光パラメトリック発振器-FPGA フィードバック回路で実現し、現代アルゴリズムによる最適化計算に対する優位性を確実なものにする。
- 開発した量子ニューラルネットワークに搭載する実問題アルゴリズム（アプリケーション）を、創薬、無線通信、圧縮センシング、金融工学、機械学習、などの組合せ最適化・連続量最適化の分野で開発する。これにより、量子コンピュータハード・ソフト開発のメインストリームとして量子ニューラルネットワークの地位を不動のものにする。
- 商用ファイバー環境での量子鍵配送の長期安定化、様々なアプリケーションを支える鍵供給インターフェースと秘密分散法による大規模鍵管理システムの実現、システム全体の安全性評価技術の確立を行なう。広い動作領域をカバーする変復調回路、誤り訂正符号、及び秘匿ランダム化関数を収納し高速駆動する専用基板の開発を行なう。
- 2次元2層正方格子を冷却フェルミ原子と光格子で構成し、s波超流動の臨界温度を実験的に検証して、室温超伝導体開発への道を切り開く。また、様々な量子モデルを数値シミュレーションするプログラムをオープンソースとして公開し、世界の研究者に供する。

(3) 研究開発プログラムの全体構成図

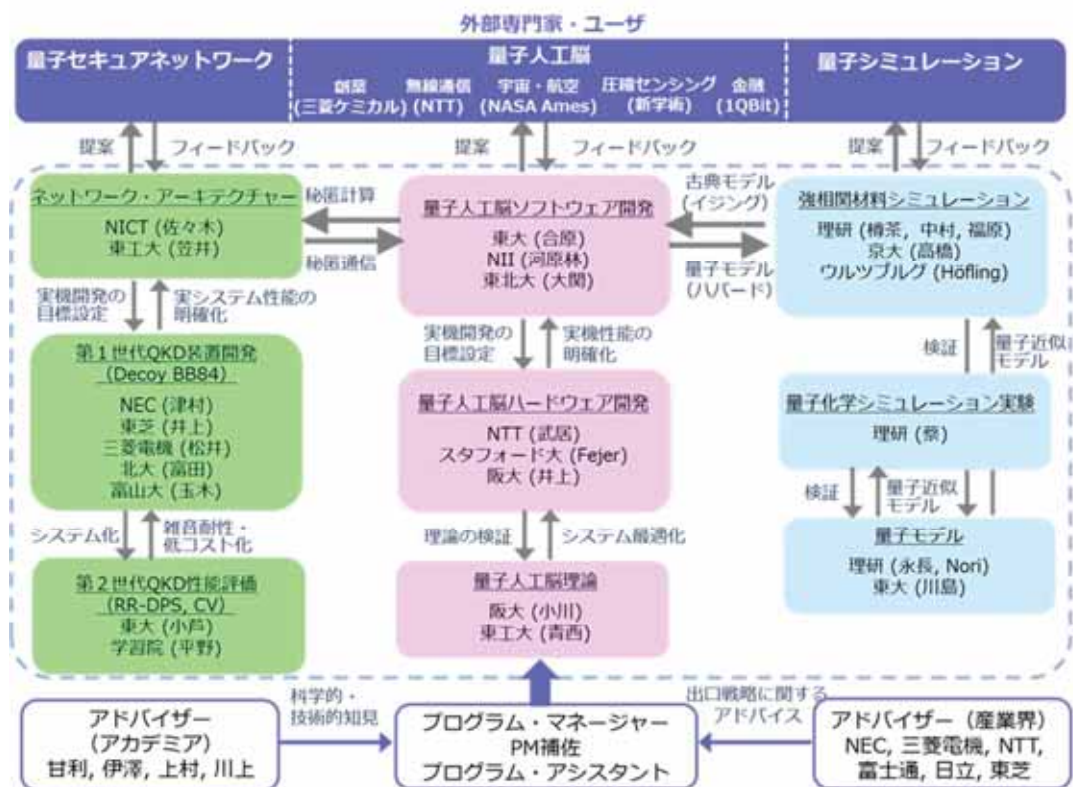


図8. 現在のプロジェクト構成（平成28年度以降）。

(4) 具体的な取組

① 量子人工脳プロジェクト

i) 研究開発の概要

1. $N = 100$ ニューロン (OP0 パルス数に対応) を $N^2 = 10^4$ シナプスで全結合した小規模量子ニューラルネットワークを開発し、NP 困難クラスの代表的問題である MAX-CUT 問題を用いてベンチマークを行なう。具体的には、厳密解を求める正答率を評価し量子アニーラ (D-WAVE マシン) の性能と定量的に比較する。
2. $N = 2000$ ニューロンを $N^2 = 4 \times 10^6$ シナプスで全結合した中規模量子ニューラルネットワークを開発し、MAX-CUT 問題の近似解 (87.8%精度) を求める計算時間を評価し、現代アルゴリズムの性能と定量的に比較する。
3. $N = 10^5$ ニューロンを $N^2 = 10^{10}$ シナプスで全結合する大規模量子ニューラルネットワークを開発し、上記現代アルゴリズムに対する圧倒的な優位性を実証する。
4. 量子ニューラルネットワークの適用先として、創薬におけるリード最適化、無線通信における実時間周波数割当て、圧縮センシングにおけるスパース推定、の3つにターゲットを絞って、最適化アルゴリズムを開発し、数値シミュレーションと実機への実装により、その効率を検証する。表2に、代表的な適用先をまとめる。

表2. 量子ニューラルネットワークの適用先.

問題	適用先	機能・タスク	スピン数	厳密解	近似解	ボルツマン・サンプリング
リード最適化	化合物探索(創薬) 生体媒質設計 (化学工業)	病原となる蛋白質の活性を抑制する化合物探索、 化学反応を促進する生体媒質探索のための初期フィルタリング	サイト数 ($n = 50$) x 原子種 ($k = 20$) 1,000	制約項 (1原子種/サイト、化学結合条件、毒性除去)		コスト関数 (蛋白質-化合物相互作用エネルギー)
2次割り当て問題	無線通信・物流・電力ネットワーク	最適なリソース割当てを実時間でできない、端末間の通信容量の最大化を実現	周波数バンド数 ($n = 20$) x 端末数 ($k = 500$) 10,000	制約項 (1周波数バンド/基地局)	コスト関数 (端末間の干渉電力)	
スパース推定	圧縮センシング (MRI, 天体観測)	不完全なセンシングデータから、元データのスパース性を推定しながら、復元を図る	画素数 (n) 60,000~100,000		スパース性を最適化しながら、エラーを最小化する	
MAX-CUT問題	最大クリーク問題 (化合物/蛋白質構造比較) コミュニティ検出	全ての頂点間に枝がある頂点の部分集合で最も大きなものは何か?	問題サイズ (n) 2,000~20,000	制約項 (枝で結ばれていない頂点ペアを選んではいけない) コスト関数 (なるべく多くの頂点を選ぶ)		
	彩色問題 (スケジューリング、使って、枝を共有するレジスタ割り付け/飛行高度割り付け)	n 個の頂点を k 色だけを (スケジューリング、使って、枝を共有するレジスタ割り付け/飛行高度割り付け) 塗り分けることは可能か?	頂点数 (n) x 色数 (k) 2,000~40,000	制約項1 (頂点に1つだけ色を割り当てる) 制約項2 (2つの頂点が枝で結ばれている時、同じ色を割り当ててはいけない)		
k-SAT問題	ハード・ソフト検証 知識証明	n 個の変数の中から選ばれた k 個の変数からなる論理式の積が成立するか、どうか?	ハードウェア検証 ($40,000 \sim 800,000$ bit) ソフトウェア検証 ($\leq 3,200,000$ bit)	ソフトウェア/ ハードウェア検証	計画、知識証明	

5. これらのハード・ソフト開発の成果を、順次論文発表し、クラウドサービスに導入し、広く世界の量子ハード・ソフト技術の開発に携わる研究者にアピールする。

ii) 成果目標

1. $N = 100$ ニューロンに対して $N^2 = 10^4$ シナプス全結合を有する小規模量子ニューラルネットワークが、スパースな結合しか持たない量子アニーラ（D-WAVE マシン）に比べて、正答率の問題サイズ依存性において圧倒的に優れた性能を持つことを定量的に示す。
2. $N = 2000$ ニューロンを $N^2 = 4 \times 10^6$ シナプス全結合した中規模量子ニューラルネットワークが、現代コンピュータに載せたアルゴリズムに比べて（30 倍～1000 倍）高速に 87.8%の近似解を求めることができることを示す。
3. $N = 10^5$ ニューロンを $N^2 = 10^{10}$ ニューロンで全結合する大規模量子ニューラルネットワークにより、図 9 に示す数値シミュレーション結果の予測通り、上記現代アルゴリズムによる計算速度に比べて、 $10^5 \sim 10^6$ 倍の高速化が実現されることを示す。

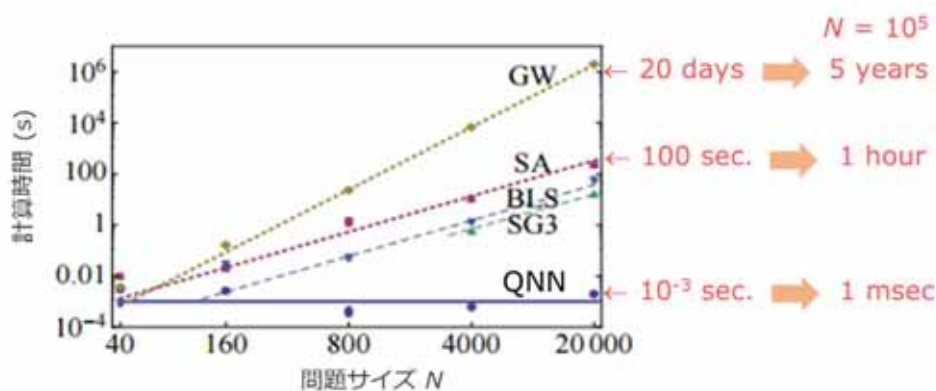


図 9. 完全グラフに対する MAX-CUT 問題で 87.8%近似解を求める計算時間の比較。
GW: SDP 近似アルゴリズム、SA: 焼きなましアルゴリズム、BLS, SG3: ヒューリスティック、QNN: 量子ニューラルネットワーク（コヒーレント・イジングマシン）。

4. コヒーレント・イジングマシンを記述する様々な量子モデルを相互比較し、その性能を理論的に評価する。それぞれの最適化問題に対して最も強力な現代アルゴリズムと比較し、本方式にメリットがあるかどうかを定量的に明らかにする。
5. $N = 2000$ ニューロンを搭載した中規模量子ニューラルネットワークと GPU 上に構築した「仮想量子ニューラルネットワーク」をバック・エンドとするクラウドシステムを構築し、2017 年 11 月を目処に世界に向けてクラウドサービスを開始する。

② 量子セキュアネットワークプロジェクト

i) 研究開発の概要

1. 量子セキュアネットワークを物理層/鍵管理層/アプリケーション層の3階層構造で開発する(図3)。物理層には量子鍵配送(QKD)機能、盗聴検知機能、及びサイドチャネル攻撃対策を実装する。鍵管理層には、異なるベンダーから供給される鍵を統一かつ効率的に運用する機能を実装し、かつ盗聴攻撃への自動経路切り替え機能などスマート化を進める。アプリケーション層はしきい値秘密分散により実現し、防衛・金融・医療・スマートインフラ分野のユーザと密接な情報交換を行いながら開発し、専用暗号システム、汎用的なルータ、サーバ、スマート機器への自在な鍵供給を実現する。
2. アプリケーション層には、標準的なセキュリティ技術(IPsec, TLS)とのインターフェースを実装し、共通鍵暗号装置、モバイル端末(スマートフォンやドローンなど)との統合化を実現する。さらに、情報理論的安全性を持つ秘密分散プロトコルをアプリケーション層に実装し、将来の安全性脅威に怯えることなく重要情報を超長期間にわたって伝送・保存・処理できるストレージネットワークの試験システムを開発し、医療分野の潜在ユーザと共同で機能検証を行う。
3. 量子セキュアネットワークの都市圏実装を着実に進めつつ、そこから派生した要素技術、すなわち物理乱数発生器と誤り訂正技術及び認証技術を組合せ、秘匿性と伝送効率を両立させる物理層暗号化システムの開発にも取り組み、小型衛星やドローンを用いた無線通信に適用する。

ii) 成果目標

1. 量子鍵配送技術の第1世代であるDecoy-BB84方式を用いて上記物理層を構築し、鍵管理層、アプリケーション層へ接続する。同時に、量子鍵配送技術の第2世代であるRR-DPS-QKD方式、CV-QKD方式の基礎検討を進める。特に、光ホモダイン検波によるフィルタリング機能を利用して、波長多重デジタルコヒーレント光通信チャネルと同一光ファイバー内で共存できる量子鍵配送を実現し、システムの低コスト化を図る。
2. 超長期間の保存を必要とする個人の医療情報のストレージネットワークを量子鍵配送/one time padと秘密分散を組み合わせた形で実現する。
3. 本研究開発から派生した要素技術(物理乱数発生器、認証技術、誤り訂正技術など)を、個別に実装できる通信システムへの応用を開始する。

③ 量子シミュレーションプロジェクト

i) 研究開発の概要

制御性の良い別の量子多体系に目標となる量子多体系モデルをマッピングし、模擬実験を通して必要な知見を得る量子シミュレーションの手法を確立する。産業や社会に変革をもたらす物質として、「室温超伝導体」と「新量子粒子（エニオン）」を取り上げる。それぞれ、超伝導転移温度向上のアイデアを冷却原子を用いた模擬実験により検証し、耐性の高い新量子粒子を励起子ポラリトンを用いて生成することを目指す。また、様々な量子多体系モデルに対する大規模科学計算を実行する数値シミュレーション・プログラムを開発し、オープンソースとして公開する。

ii) 成果目標

1. 超伝導転移温度向上の指導原理を発見する手段として、4つの数値シミュレーションモデル（量子モンテカルロ法、量子マスター方程式、動的平均場法、テンソルネットワーク法）を確立する。これらのモデルを冷却原子、超伝導回路を用いた模擬実験と比較し、その有効性を確認する。さらに、第一原理計算を得意とする外部研究グループと協力して室温超伝導に適した結晶構造を预言する。
2. 銅酸化物高温超伝導体より3倍程度高い転移温度が期待できる結晶構造（2次元2層正方格子）を冷却原子-光格子系で実装する。模擬実験によりその超流動現象を誘起するメカニズムを定量的に明らかにし、当該理論モデルに基づく物質探索の有効性を実証する。
3. 超伝導量子回路を用いて、強相関多体系・非平衡開放量子系の平衡状態・非平衡状態にアプローチする実験手法、ボソンサンプリング回路を開発し、高温での量子秩序発現、分子の振動スペクトルシミュレータの可能性を明らかにする。
4. 励起子-ポラリトン凝縮系、及びトポロジカル超伝導系（HgTe ナノ細線と超伝導の接合）を用いて世界初となる非可換エニオンの検出法、制御法を開発する。
5. 量子多体系、量子開放系の数値シミュレーションを実行するソルバーを、オープンソースソフトウェア(Quantum Toolbox in Python: QuTip)として提供する。

(5) 研究開発プログラムの全体ロードマップ

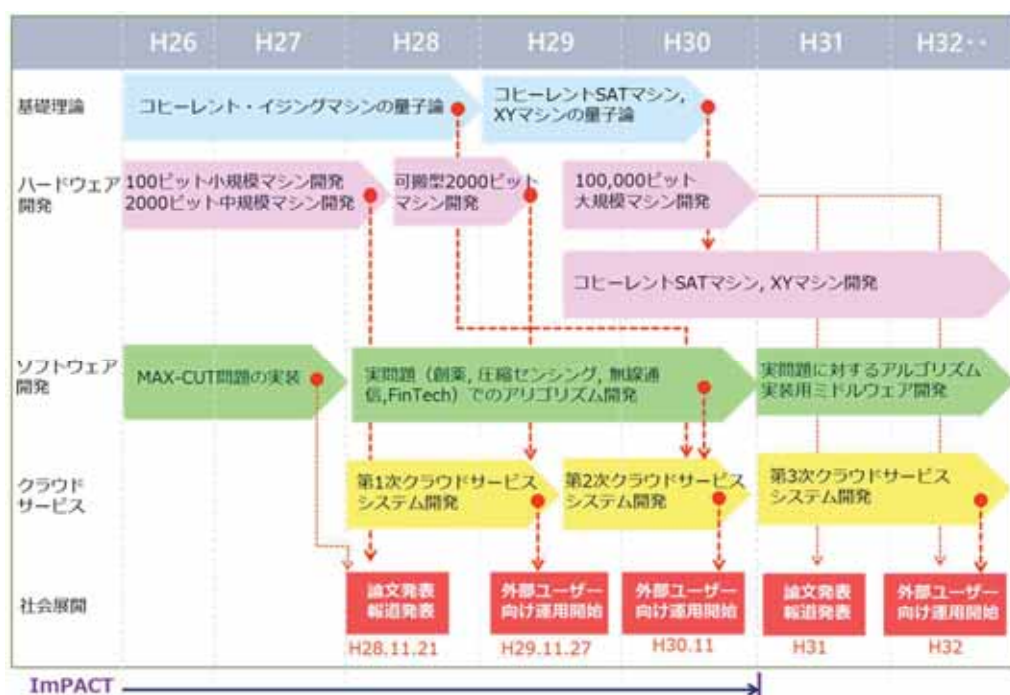


図 10. 量子ニューラルネットワーク開発ロードマップ。



図 11. 量子セキュアネットワークワーク開発ロードマップ。



図 12. 量子シミュレーション開発ロードマップ。

(6) 研究開発プログラムのマイルストーン

- 平成 28 年度末までに、100 ビット小規模量子ニューラルネットワーク、2000 ビット中規模量子ニューラルネットワークの開発を完了し、その有効性を確認して論文化し、報道発表を行う。
- 平成 29 年度半ばまでに、2000 ビット量子ニューラルネットワーク（可搬型）を開発し、これを用いた外部ユーザ向けクラウドサービスを開始し、合わせて報道発表を行なう。
- 平成 30 年度半ばまでに、様々な実問題に対するアルゴリズムを開発し、これを GPU 上に実装したバーチャル量子ニューラルネットワークを開発し、その実用性を定量的に明らかにする。
- 平成 30 年度末までに、～100,000 ビット（全結合）大規模量子ニューラルネットワークを開発し、その有効性を確認して論文化し、その後報道発表を行う。
- 平成 30 年度末までに、量子鍵配送／one time pad、しきい値秘密分散ストレージ、ネットワーク技術を融合して、超長期デジタル・アーカイブシステムを構築する。合わせて、医療情報の秘密分散バックアップの実証試験を成功させる。
- 平成 30 年度末までに、2 次元 2 層正方格子中の斥力相互作用するスピンを持った冷却フェルミ原子の超流動転移を実現し、室温超伝導物質開発への指針を得る。
- 平成 30 年度末までに、強相関電子系・光学系の（数値）量子シミュレーション手法を開拓し、これを QuTip のオープンソースプログラムとして公開する。

(7) 研究開発プログラム実施期間

平成 26 年 10 月 2 日から平成 31 年 3 月 31 日まで（4.5 年間）

2. 研究開発プロジェクトの計画及び実施状況

(1) 量子人工脳プロジェクト

① プロジェクトの計画

研究開発課題	平成 26年度 (6ヶ月)	平成 27年度	平成 28年度	平成 29年度	平成 30年度 (9ヶ月)
1. ハードウェア開発					
・ 2×10^3 スピン3値全結合マシン開発	←→		←→		
・ 10^2 スピン3値全結合マシン開発	←→		←→		
・ 10^5 スピン3値全結合マシン開発				←→	←→
・500スピン連続値全結合マシン開発				←→	←→
2. ソフトウェア開発					
・連想記憶メモリ(ホップフィールドモデル)			←→	←→	←→
・創薬のためのリード最適化	←→	←→	←→	←→	←→
・CDMA復号器・スパースコーディング			←→	←→	←→
・2次割当て問題／無線通信のリソース割当て			←→	←→	←→
3. 基礎理論					
・量子ニューラルネットワークの量子論	←→	←→			
・量子ニューラルネットワークの数値シミュレーション		←→	←→	←→	←→
・量子ダーウィニズム、量子カオス、量子分岐理論				←→	←→
4. クラウドシステム					
・システム開発				←→	←→
・サービス運用				←→	←→

② プロジェクトの体制

研究開発課題	内容、研究開発プロジェクトにおける役割等	研究開発機関
全体統括	プロジェクト全体の統括	日本電信電話株式会社
ハードウェア開発	スピン数100～100,000の小・中・大規模量子ニューラルネットワークを開発し、システム実験を通して、その性能を評価 光遅延線を用いた光フィードバック技術開発、FPGA回路による量子測定フィードバック技術開発	日本電信電話株式会社 大阪大学 スタンフォード大学

ソフトウェア開発	適用領域・問題と量子ニューラルネットワークハードウェアを結ぶアルゴリズム開発、数値シミュレーション、ベンチマークによる性能評価	国立情報学研究所 東京大学生産技術研究所 東北大学 東京工業大学 広島市立大学
基礎理論	光パラメトリック発振器、光遅延線結合、測定フィードバック結合の量子論	国立情報学研究所 東京大学生産技術研究所 大阪大学
クラウドサービス	量子ニューラルネットワークハードウェア実機と現代コンピュータ上に構築した数値シミュレータを同時に、インターネットを通して世界中の研究者が利用できるクラウドシステムとして公開する	国立情報学研究所 日本電信電話株式会社

③ プロジェクトの進捗状況、獲得成果及び目標達成への貢献度

- 1) ニューロン数 2000、シナプス結合数 4×10^6 （全結合）の中規模量子ニューラルネットワークを用いて、NP 困難 MAX-CUT 問題の正答率を評価し、競合技術である量子アニーラに対する優位性を明らかにした。図 13 に示すように、MAX-CUT 問題に対して、量子アニーラの正答率は問題サイズ $N = 40$ 程度まで N^2 の指数関数で減少するのに対して、量子ニューラルネットワークでは問題サイズ $N = 100$ 程度でも 20% という高い正答率を確保していることを実証した。

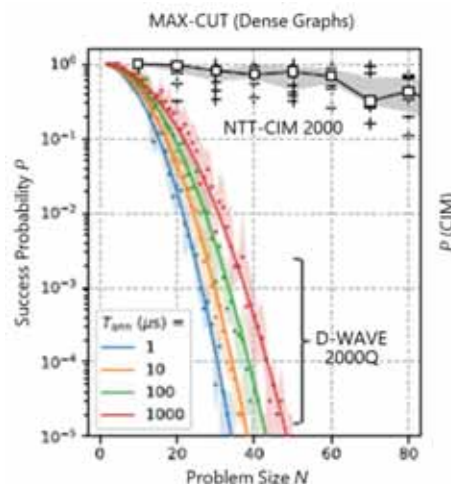


図 13. 量子ニューラルネットワークと量子アニーラの完全グラフ MAX-CUT 問題に対する正答率対問題サイズ. 計算時間 1 msec.

- 2) ニューロン数 2048、シナプス結合数 4, 194, 604（全結合）の中規模量子ニューラルネットワークを用いて、完全グラフ MAX-CUT 問題の近似解（87.8%）を得る計算時間を評価し、現代アルゴリズムに対する優位性を明らかにした。図 14 および表 3 に示すように、完全グラフの MAX-CUT 問題に対して、4 種類の古典ニューラルネットワークが 87.8% 近似解を得るために、1~100 msec かかったのに対し、量子ニューラルネットワークは 0.07 msec で同じ近似解を得ることができた。

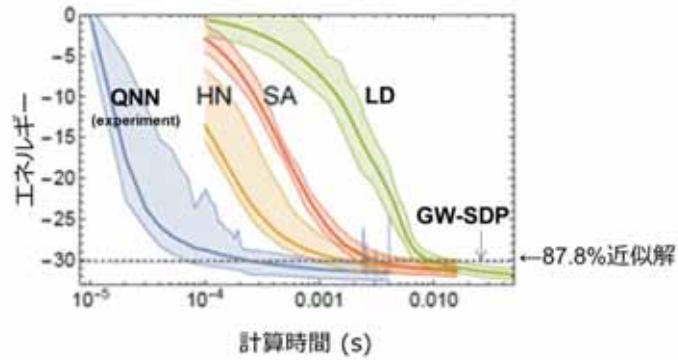


図 14. 量子ニューラルネットワーク (QNN)、ホップフィールドネットワーク (HN)、焼きなまし法 (SA)、ホップフィールド・タンクニューラルネットワーク (HTNN) のエネルギー対計算時間.

表 3. 量子ニューラルネットワークと 4 つ現代アルゴリズムの比較. 問題サイズ $N = 2000$.

マシン	最短時間 (msec)	平均時間	ハードウェア
量子ニューラルネットワーク	0.071	0.264	OPO/FPGA
現代アルゴリズム			
Hopfield Network	0.924	1.84	CPU (Intel Xeon, E3-1225, 3.2 GHz)
Simulated annealing	2.10	3.20	CPU (Intel Xeon, E3-1225, 3.2 GHz)
Hopfield-Tank Network	7.04	9.67	SC (PEZY, 1024 Core, 8192 Threads, 733 MHz)
Langevin Dynamics	100	120	SC (PEZY, 1024 Core, 8192 Threads, 733 MHz)

- 3) これらの成果を基に世界中の研究者がインターネットを介して使えるクラウドシステムを開発し、平成 29 年度 11 月よりサービスを開始した。
- 4) また、ニューロン数が 100,000、ニューロン間シナプス結合数が 10^{10} (全結合) の大規模量子ニューラルネットワークの実現に向けて、 10^5 のパルスを同時発生できる光パラメトリック発振器の実証実験に成功した (図 15)。さらに FPGA 設計・構築を進め、平成 30 年 12 月までに完成した。

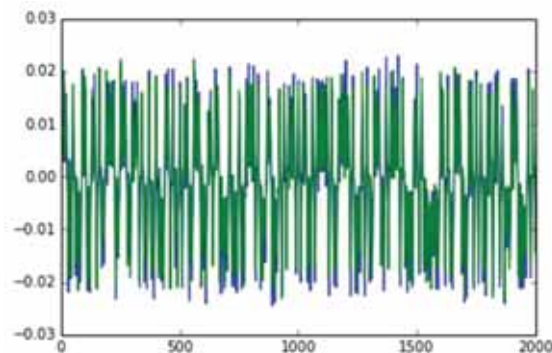


図 15. $N = 10^5$ の OP0 発生実験結果 (位相測定結果). 横軸は時間で 1 pt = 10 ps. 緑線は、青線部分から 123548 パルス分シフトした部分の位相測定結果を表す. 全く同じ位相パターンが再現していることから、123548 個の独立した OP0 パルスが発生したことを確認できた。

さらに、量子ニューラルネットワークに搭載するアルゴリズムを、創薬、無線通信、圧縮センシング、金融、機械学習、などの組合せ最適化の分野で開発を進めた。

④ 競合する技術・アプローチに対するベンチマーク

グラフに対する NP 困難 MAX-CUT 問題において、量子ニューラルネットワークが最適解を出力する成功確率が、量子アニーリングを実行する商用機である D-Wave 2000Q と比較して優れた性能（問題サイズ $N = 55$ において、量子ニューラルネットワークの正答率は量子アニーラのそれに比べて、7 桁高い）を示すことを実証した（図 13）。ゲート型、アニーラ型、ネットワーク型の 3 つの量子マシンの原理・性能の比較は表 1 にまとめてある。ネットワーク型の有利な点は、光を用いているため室温・常気圧動作すること、測定フィードバック方式の採用により大規模な問題サイズに対応できること、一つのリング共振器中に同時に生成された多重光パルスニューロン素子としているため欠陥素子がないこと、消費電力が低いこと、低価格であること、などである。

ベンチマーク問題として、Sherrington-Kirkpatrick (SK) スピングラス問題（全結合グラフ）、エッジ密度 50%の MAX-CUT 問題（密結合グラフ）、エッジ数 3 の MAX-CUT 問題（疎結合グラフ）の 3 つを取り上げ、正解を得るのに要する計算時間を、ゲート型量子コンピュータ (QC)、量子アニーラ (QA)、量子ニューラルネットワーク (QNN) について比較した。QC ではグローバールアルゴリズムを用いたユニバーサル量子計算を行うため、上記 3 つの問題に対して、同一の計算時間（理論値）が予測される。これを表 4 にまとめた。ここで、（ゲート型）量子コンピュータには、デコヒーレンスはなく、ゲートエラーもなく、従って量子誤り耐性も必要なく、また全ての量子ビット間に全結合が張られている、という仮定をおいた。従って、表 4 の数値は理論限界値である。一方、QA と QNN に対する数値は、D-WAVE 社の 2000 ビットマシン、NTT の 2000 ビットマシンでの実験値である。問題サイズの小さい疎結合グラフでは QA は QNN よりも優れた特性を示すが、問題サイズが大きくなると、このアドバンテージは消失する。また、密結合、全結合グラフでは、QNN は QA に比べて圧倒的に優れた性能を示している。

表 4. 量子コンピュータ (QC)、量子アニーラ (QA)、量子ニューラルネットワーク (QNN) の計算時間の比較.

QC		SK				MAX-CUT (dense)				MAX-CUT ($d = 3$)				
N		N	DW2Q	CIM	Factor	N	DW2Q	CIM	Factor	N	DW2Q	CIM	Factor	
20	4.0 ms	10	6.0 μ s	25 μ s	0.2	10	6.0 μ s	25 μ s	0.2	10	1.0 μ s	50 μ s	0.02	
		20	35 μ s	100 μ s	0.3	20	0.4 ms	100 μ s	4	20	3.0 μ s	100 μ s	0.03	
		40	6.1 ms	0.4 ms	15	40	6.1 s	0.4 ms	10^4	50	12 μ s	0.4 ms	0.03	
50	600 s	60	1.4 s	0.6 ms	2000	55	10^4 s	1.2 ms	10^7					
						80	(10^{11} s)	1.8 ms	(10^{13})					
						100	(10^{19} s)	2.3 ms	(10^{21})					
100	2×10^{10} s	100	(10^5 s)	3.0 ms	(10^7)	100	(10^{19} s)	2.3 ms	(10^{21})	100	100 μ s	3.3 ms	0.03	
150	6×10^{17} s										150	2.8 ms	22 ms	0.1
											200	11 ms	51 ms	0.2

図 16 には、SK スピングラス問題に対して、正解が得られなかった問題の割合 P_0 が計算時間 t^{CPU} を増加させた時にどう減少するか、を CPU を用いたシミュレーションで評価した結果を示す。青色の破線は現在最も強力だと思われるヒューリスティック（Breakout Local Search: BLS）を用いた結果である。赤色の実線は、振幅不均一エラーを訂正する機能を実装した QNN を記述する理論モデルを一種のヒューリスティックと見立てて、このアルゴリズムを CPU で評価した結果を示す。やさしい問題に対しては、BLS は QNN アルゴリズムよりも優れた特性を示すが、難しい問題に対しては QNN の方が BLS よりも優れていることがわかる。もし、振幅不均一エラーを訂正する機能を持つ QNN が実現されたならば、計算時間は図 16 に示した CPU 時間（赤線）に比べて、1/1000 程度に短縮されることが予想される。

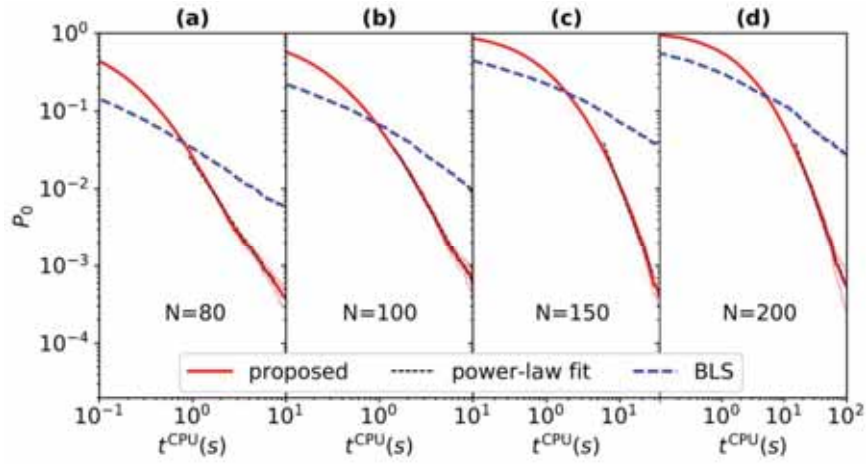


図 16. BLS と QNN アルゴリズムによる正解が得られなかった問題の割合 P_0 対 計算時間 t^{CPU} . SK スピングラス問題をベンチマーク問題とした。

表 4 と図 16 の結果は、以下の論文として発表された。

- “Experimental investigation of performance differences between coherent Ising machines and a quantum annealer,” Sci. Adv. (to be published).
- “Destabilization of local minima in analog spin systems by correction of amplitude heterogeneity,” Phys. Rev. Lett. (to be published).

(2) 量子セキュアネットワークプロジェクト

① プロジェクトの計画

研究開発課題	平成 26年度 (6ヶ月)	平成 27年度	平成 28年度	平成 29年度	平成 30年度 (9ヶ月)
A. 量子セキュアネットワーク・アーキテクチャ					
・プロジェクト全体の統括	←				→
・鍵管理システムの開発	←				→
・アプリケーションの開発・実装		←			→
・潜在ユーザとの共同フィールド実験(医療データの秘密分散バックアップ、秘匿ドローン通信)				←	→
B. 第1世代量子鍵配送技術(Decoy-BB84方式)					
・QKD装置(Decoy-BB84)設計・試作	←			→	
・信頼性・安全性評価、改修、ネットワーク化			←		→
・回線暗号化システム、秘匿スマートフォン開発		←			→
C. 第2世代量子鍵配送技術(RR-DPS/CV方式)					
・RR-DPS:実用的装置モデルによる理論構築	←		→		
・RR-DPS:新原理量子鍵配送の性能評価			←		→
・CV:要素技術開発と装置設計・実装		←		→	
・CV:高機能化とシステム実証試験			←		→

② プロジェクトの体制

研究開発課題	内容、研究開発プロジェクトにおける役割等	研究開発機関
全体総括、量子セキュアネットワーク・アーキテクチャ技術	プロジェクトの全体総括統括、鍵管理アーキテクチャの研究開発、QKD装置の評価・校正技術の研究開発、QKDプラットフォームのアプリケーションの研究開発、秘密分散とQKDによる重要情報の長期間秘匿保存技術の開発	情報通信研究機構
第1世代量子鍵配送技術 (Decoy-BB84 方式)	秘匿量子光送受信技術、現代暗号と量子暗号の融合技術、QKDデバイス及びネットワークの安全性評価技術、物理レイヤセキュリティ技術の開発。	日本電気株式会社、株式会社東芝、三菱電機株式会社、北海道大学、富山大学、東京工業大学
第2世代量子鍵配送技術 (RR-DPS/CV 方式)	雑音耐性、小型化・低コスト化に優れたRR-DPS-QKD技術、CV-QKD技術の開発	東京大学 学習院大学

③ プロジェクトの進捗状況、獲得成果及び目標達成への貢献度

- 量子鍵配送の Decoy-BB84 方式に関しては、日本電気（株）と（株）東芝が開発、製造した装置を物理層へ設置し、それぞれの装置で生成された暗号鍵を鍵管理層へ供給し相互接続動作を確認するとともに、アプリケーション層への鍵供給と運用機能も実証した。また、盗聴検知機能、及び当初想定されたサイドチャンネル攻撃の対策を実装し、3階層からなる量子セキュアネットワークシステムの基本機能確認を計画通りに完了した。現在、フィールド環境上での長期信頼性試験を継続中であり、その結果についてはプロジェクト終了後も標準化活動へ活用してゆく。更に、QKD 送信機のクロック速度を 1GHz 程度まで高速化した際にパターン効果と呼ばれるサイドチャンネル（実装上の脆弱性）が存在することを発見し、簡易実装可能な対策を提案し、特許申請と論文発表を完了した。今後、盗聴攻撃に対する自動経路切替え機能とともに装置への実装を進める。また、第 2 世代である CV-QKD 方式の装置開発においては、100 波多重かつ光増幅した 18.3Tbps のコヒーレント光通信と CV-QKD をファイバ 1 芯の中で共存伝送できることを実証した。この多重化実験は図 17 に示すように従来発表された実験結果に対して劇的な性能改善になっており、中継器のある商用回線での CV-QKD の利用へ向けた突破口となる成果である。プロジェクト終了後も実用化に向けた取り組みを加速させる。

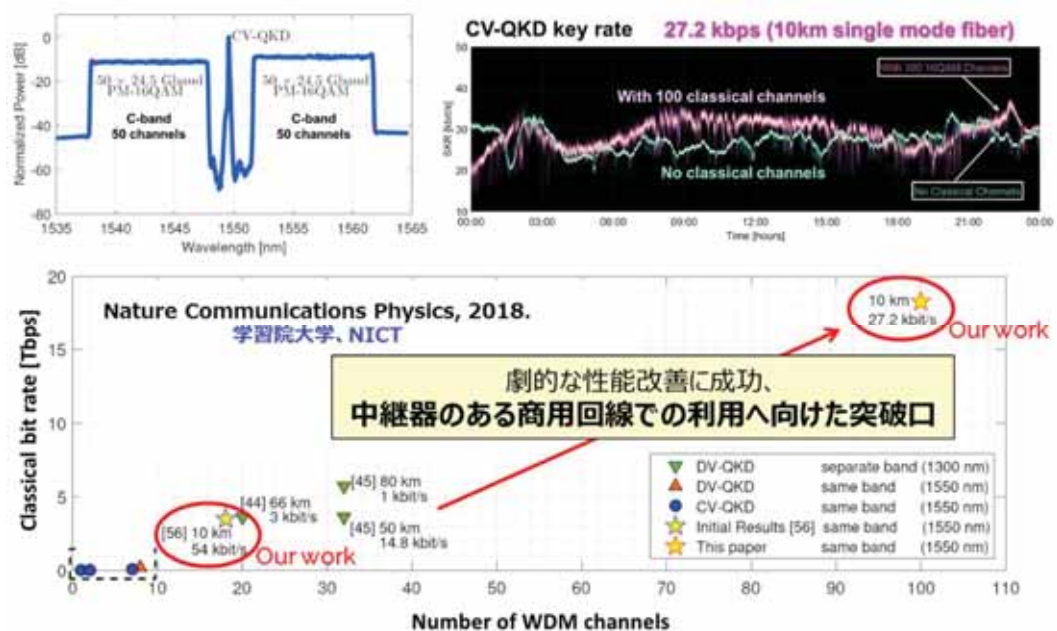
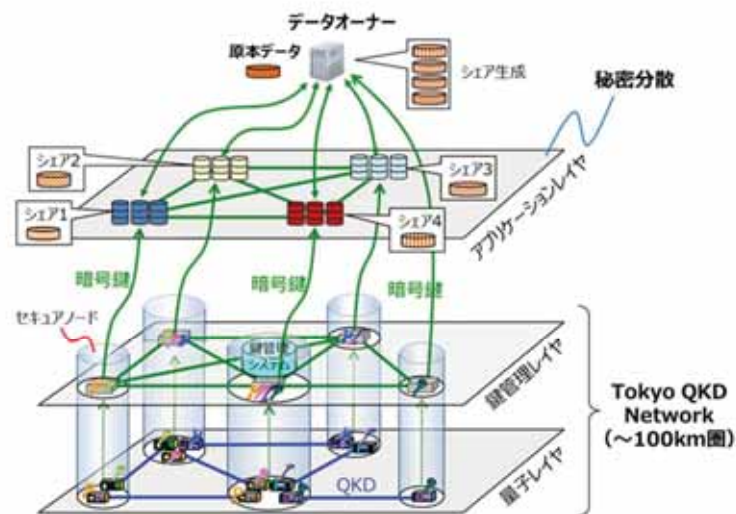


図 17. 100 波多重・光増幅した 18.3Tbps のコヒーレント光通信と CV-QKD の共存伝送の実験結果. 左上：CV-QKD と 100 波多重コヒーレント光通信のスペクトル. 右上：CV-QKD の鍵生成速度の時間変化. 下段：光通信伝送速度-多重化した波長数で比較したベンチマーク.

アプリケーション層では標準的なセキュリティ技術 (IPsec, TLS) とのインターフェースを実装し、共通鍵暗号、スマートフォン、ドローン通信の高秘匿化シ

システムを開発し実証実験を完了し目標を達成した。秘匿ドローン通信は国家戦略特別区域等のフィールド実証を終え、製品化の最終仕上げの段階に入っている。また、情報理論的安全性を持つ秘密分散プロトコルを QKD ネットワークのアプリケーション層に実装し、重要情報を超長期間にわたって伝送・保存・処理できるストレージネットワークの実証実験を完了した（図 18a）。ここで開発した物理乱数源と鍵管理技術を共通鍵暗号による秘匿ネットワーク及び耐量子-公開鍵暗号に基づくユーザ認証技術と統合し 800km の秘密分散ストレージシステムを構築した、さらに、高知医療センターの協力を得て、電子カルテ模擬データの分散バックアップの実証実験を完了し目標を達成した（図 18b）。

a. Tokyo QKD Network上に実装した秘密分散ストレージシステム



b. 800kmの秘匿ネットワーク上に実装した秘密分散ストレージシステム

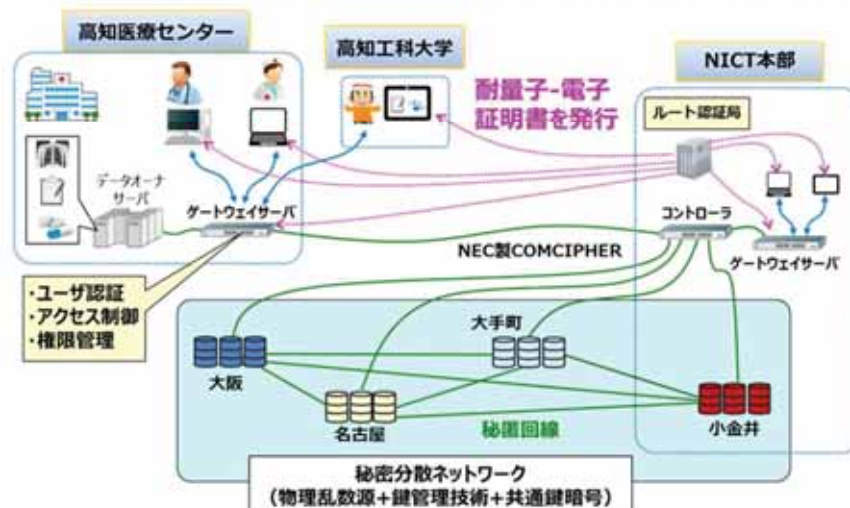


図 18. 秘密分散バックアップシステムの概要図. a. Tokyo QKD Network 上に実装した秘密分散ストレージシステム. b. 800km の秘匿ネットワーク上に実装した秘密分散ストレージシステム.

- 2) 本研究開発から派生した物理乱数発生器、誤り訂正技術、認証技術などの要素技術を組合せ、秘匿性と伝送効率を両立させる物理層暗号化システムを開発し、地上 8km の光空間リンク上で光学ロスが-55dB のという劣悪な条件下においても約 7Mbps の高速な鍵生成が可能であることを実証し、論文発表を完了して目標を達成した。本成果は今後、総務省のプロジェクト等で実用化に取り組む。

④ 競合する技術・アプローチに対するベンチマーク

本研究開発における Decoy-BB84 方式の量子鍵配送装置は中国、欧州の機関が開発した装置と比較して、鍵生成速度、安全性対策において世界最高性能を誇るに至っている。しかしながら世界最高レベルの装置をもってしてもファイバー長 50 km において鍵生成速度が数 100kbps～1Mbps 程度であり、利便性の向上・サービスエリアの拡張には“信頼できるノード”を用いた量子鍵配送ネットワークの構築が不可欠である。本プロジェクトにおいて、異なるベンダー間による鍵リレーはもとより、鍵管理サーバを中心においた集中管理型のネットワークアーキテクチャの提案・実装とその長期信頼性試験を進めている。さらに様々なアプリケーションに安全な鍵を供給するインターフェースを開発、ネットワークスイッチへ供給し、伝送するデータの one time pad 暗号化の実施やスマートフォンへの鍵供給を行い安全な通話を可能としている。これによりユーザが意識することなく安全な通信を実現することが可能となっている。このようなネットワーク管理技術まで一貫した開発、実証が出来ている組織は世界を見ても他になく、もっとも洗練された量子鍵配送ネットワークを実現するに至っている。またネットワークアプリケーションの中で分散ストレージ・クラウドサービスは生活に欠かせないものとなりつつあるが、その一方でその安全性は多くの専門家が不安視しており、現代暗号研究やネットワークセキュリティの研究分野で現在研究が精力的に進められている。本プロジェクトでは量子鍵配送の情報理論的安全な伝送能力と既存の秘密分散との組合せを世界に先駆け開発し、情報理論的安全な分散ストレージの実現に成功した。本プロジェクトで開発した情報理論的安全な伝送・保存・認証・復元ができる分散ストレージシステムは現代暗号だけでは決して解決できない課題を克服しており、市場に受け入れられる QKD 技術を用いたキラーアプリとなる可能性を大いに秘めている。表 5 に分散ストレージシステムの評価指標とベンチマークを示す。本研究開発は従来技術に比べて明らかな優位性を持っている。

表 5. 分散ストレージシステムの比較.

分散ストレージシステム	本研究開発 “QKD+秘密分散”	現代暗号 “格子暗号”
秘匿性	◎ 危殆化しない安全性が証明済み	× ~ △ 安全性評価途中
可用性	○	○
機能性	○ 秘密計算機能	○ 秘密検索及び計算機能
データ長期保存機能	◎ 閾値仮定劣化防止対策済	△ 解読攻撃手法が多数提案されており厳密な証明はない
現在の通信インフラとの親和性	○ Tokyo QKD Network で検証済	△ 暗号用鍵長が大きく変わるため未装備

表 6 に QKD 技術を用いた他のアプリケーション提案との比較を示す。本研究開発では H29 年度中にユーザとの共同実証実験を予定しており、理論提案にとどまっている他の提案と比較して大きく進んでいる。

表 6. 量子鍵配送 (QKD) 技術を適用したクラウドサービス技術に関する取組の比較.

クラウドサービス	本研究開発	Russian Quantum Center 他 https://arxiv.org/pdf/1705.09258.pdf
方式	量子鍵配送+ 秘密分散	量子鍵配送+ ブロックチェーン
機能	機密データの保存	ビットコイン
用途に対する実現性	○ 秘密計算機能など機密データの第三者利用も可能な情報データバンクを形成	△ 安全な商取引の実装であるためユーザ数の数だけQKDリンクが必要
ネットワークセキュリティの実装	◎ 暗号 ネットワークセキュリティを含めた安全性検証を日々実施	× 未検討
現状	○ Tokyo QKD Networkで検証済	× 未実装

(3) 量子シミュレーションプロジェクト

① プロジェクトの計画

研究開発課題	平成 26年度 (6ヶ月)	平成 27年度	平成 28年度	平成 29年度	平成 30年度 (9ヶ月)
1. 理論量子シミュレーションモデル					
・量子モンテカルロ法によるボゾン系のシミュレーション	←				→
・厳密対角化法によるボゾン系のシミュレーション	←				→
・動的平均場法によるフェルミオン系のシミュレーション			←		→
・テルソンネットワーク法によるボゾン系のシミュレーション			←		→
2. 実験					
<u>冷却原子</u>					
・様々な光格子構造の実装	←	→			
・フェルミハバードモデルの実装	←			→	
・非平衡ダイナミクスの単一原子レベルでの測定		←			→
<u>超伝導回路</u>					
・様々な格子構造の実装	←	→			
・ボゾン強相関多体系モデルの実装と量子多体系の相転移の観測		←			→
・ボゾンサンプリングの実装と分子振動スペクトル観測	←				→
<u>量子ドット／量子井戸</u>					
・非平衡結合系のダイナミクス、フィードバック制御	←				→
・新規量子相(エニオン)の探索と実証		←			→

② プロジェクトの体制

研究開発課題	内容、研究開発プロジェクトにおける役割等	研究開発機関
理論 量子シミュレーションモデル	量子モンテカルロ法によるボゾン系のシミュレーション手法の確立	理化学研究所 東京大学
	動的平均場法によるフェルミオン系のシミュレーション手法の確立	東京大学
	テルソンネットワーク法によるボゾン系のシミュレーション手法の確立	東京大学
実験 冷却原子	フェルミハバードモデルの実装、様々な結晶格子構造の実現、単一原子レベルの測定	京都大学 理化学研究所
実験 超伝導回路	ボゾン強相関多体系モデルの実装、様々な結晶格子構造の実現、ボゾンサンプリング法による分子振動スペクトルのシミュレーション	理化学研究所
実験 量子ドット／ 量子井戸	新規量子相の探索、実証、新量子材料の発見	理化学研究所 ウルブルグ大学

③ プロジェクトの進捗状況、獲得成果及び目標達成への貢献度

理論グループ（量子シミュレーションモデル）、実験グループ（冷却原子、超伝導回路、量子ドット／量子井戸）が、本研究開発プロジェクト内でのそれぞれの役割・研究分担内容について、適宜連携しながら研究を進め、着実に成果を上げることができた。それらは多くの論文および国際会議での招待講演として積極的に発表している。量子シミュレーションモデルをオープンプログラムとして公開した

“Quantum Toolbox in Python: QuTIP” は 15 万回のアクセス数、10 万回のダウンロード数を記録した。QuTIP を用いて数値シミュレーションを行ったことを明らかにした学術論文数は 1000 件にのぼった。これらの数字は、このサービスが世界の研究者の間で広く使われ始めたことを示すものである。

特に、本量子シミュレーションプロジェクトにおいて量子多体問題の最高峰と位置付ける、フェルミハバードモデルによって記述される高温超伝導について（図 4 参照）、冷却原子を用いた実験グループと理論グループとの連携により、室温超伝導への示唆を与えうる特定の格子モデルとして、銅酸化物系高温超伝導体よりも 3 倍ほど高い転移温度を预言している 2 次元 2 層正方格子モデルを選定し、このモデル格子上に、斥力相互作用する 2 成分フェルミ原子系を導入し、期待される超流動発現に向けた実験研究を進めた。また、理論グループは、やはり超伝導を有利化する可能性として、平坦バンド起源の超伝導を詳しく調べた。これを受け、冷却原子系では、平坦バンド起源の超流動発現に向けたリープ格子を用いた実験も進めた。さらに、光誘起高温超伝導などの可能性に繋がりうる、量子多体系の非平衡ダイナミクスの研究も進めた。

具体的には、まず、2 層構造正方格子の系について光超格子による実装を実現し

た。特に、ブラッグ散乱分光法を用いたエネルギーバンド測定により、設計通りに2層構造正方格子が実現できていることを確認した(図19)。さらに、低温フェルミ原子気体を2層構造正方格子に導入することにも成功し、その基本的な振る舞いとして、i) この系のバンド構造の特徴である非連結フェルミ面の存在について、各バンド占有の運動量分布の観測により明らかにした。

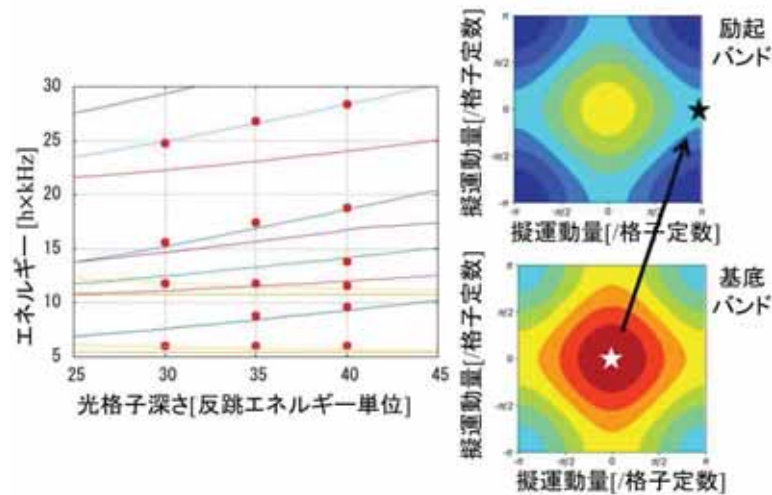


図 19. ブラッグ分光を用いた2層正方光格子のエネルギーバンドの測定. 右図における星印間に選択的に励起する外部光を入射し、その振動周波数を変化させて励起バンドと基底バンドのエネルギー差を測定した結果を左図に示す.

さらに、ii) 超流動転移よりも高い温度での発現が期待される、層間での短距離の量子磁性の存在について、スピン1重項—3重項振動の検出により確認することに成功した(図20)。また、その振舞いから理論の予言する超伝導転移温度の約10倍程度の超低温にまで現在迫ることができていることが判明した。

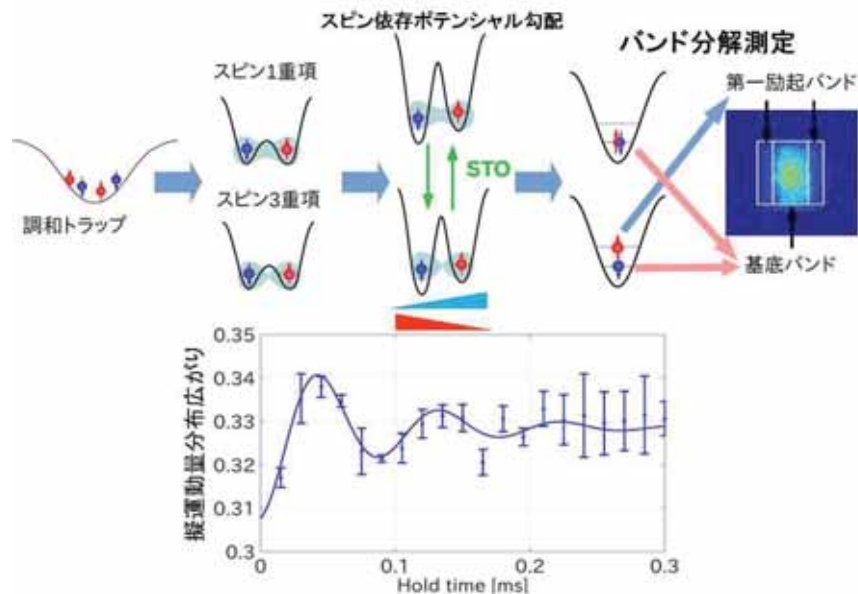


図 20. スピン1重項-3重項振動を通じた隣接スピン相関観測. 超低温の2成分フェルミ原子を2層正方格子に導入した後、スピン依存ポテンシャル勾配を印加して、STO ((スピン1重項-3重項振動)を誘起し(図上)、その結果励起バンドに原子が分布することによる擬運動量分布の変化を測定した(図下)。

さらに低温を実現するために、我々が実験で用いている Yb 原子で最大のポメラランチュク冷却効果が期待できるスピン 6 成分系を 2 層正方格子に導入し、その系での隣接サイト間の短距離量子磁性を観測することに成功した。図 21 にその結果を示す。

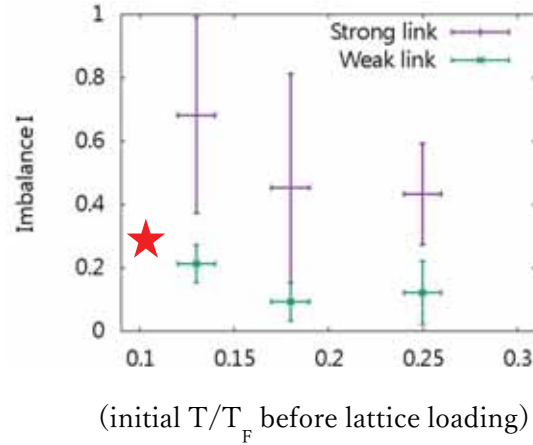


図 21. SU(6) スピン系での隣接スピン相関観測. 大きなトンネリング結合で繋がれた 2 つの層間の原子間 (strong link、紫) と、層内での小さなトンネリング結合で繋がれた原子間 (weak link、緑) での反強磁性スピン相関を、2 層型正方格子に原子を導入する前の調和型トラップ中での原子温度を変えて測定した結果. このスピン 6 成分の結果とともに、スピン 2 成分の strong link の結果も同時に示している (赤星印)。

この測定から、まず、1) トンネル結合がより大きな、2 層間の原子同士に、より大きなスピン相関が発達している、2) 6 成分スピン系においてより大きなスピン相関が発達している、という重要な知見を得ることができた。前者は、2 層型正方格子での超伝導発現の前駆的振る舞いと期待される量子スピン相関の発達の仕方にかかわるものであり、また後者は、大きなスピン自由度が大きなエントロピーを担うことによる系の冷却効果である、ポメラランチュク効果が、2 層型正方格子での量子磁性に対して有効に機能した証拠である。この実験結果を、孤立したダイマーの近似に基づく理論計算と比較することにより、系の温度を推定すると、約 8 nK と見積もることができ、SU(2) 系でのフレックス近似による超流動転移温度の 2 nK の 4 倍に迫ることができていることが分かった。この実験結果を精密な理論計算と比較することにより系の温度を正確に決定することができ、また、実験で得られた strong link と weak link の振る舞いを説明することができるかにより理論モデルのベンチマークとして利用できる、重要な結果である。

また、リープ型格子の光格子による実装にも成功し、ボース粒子およびフェルミ粒子をリープ格子、特にその平坦バンドに導入し、平坦バンド上の粒子の局在性に起因する特異な振る舞い (原子の局在現象および空間的断熱通過現象) を観測することに成功した。また、引力および斥力相互作用するフェルミ粒子の系の平坦バンドにおいて超伝導が発現するとの理論研究に対応して、引力および斥力相互作用するフェルミ粒子系を、空間断熱通過法により、平坦バンドのみに導入し、その 2 重

占有などの振る舞いを観測することに成功した。さらに、新たに、リープ格子の副格子サイトについて選択的に2重占有を測定する手法を開発し、これをスピン6成分の斥力相互作用する超低温イッテルビウム原子系をリープ格子に導入した実験により実証することに成功した。平坦バンド上の超伝導に関しては、理論面でも、大きな量子もつれ（エンタングルメント）に起因した特異なものである兆しを、密度行列繰り込み群（テンソルネットワーク法の一つ）等を用いて示した（図22）。

非平衡ダイナミクスについても、制御された散逸を導入した量子多体系や、強相関モット絶縁体領域から超流動状態へのクエンチ後の運動エネルギーおよび相互作用エネルギーの時間発展に関する新たな知見を得ることに成功した。それぞれのエネルギーがクエンチ後にホッピングの時間スケールで変化するとともに、孤立系であることの直接的証拠である全エネルギーが保存することを実験的に初めて明らかにした。また、クエンチ後に位相コヒーレンスが光円錐状に時空間的に発展していく様子を実験で見出し、最新の理論計算に対するベンチマークとすることができた。このほかにも、空間時間反転対称な散逸を導入した強相関量子系を実現し、その原子ロスの振る舞いを実験的に明らかにし、また、フェルミ粒子系に散逸を導入することにより、多粒子エンタングル状態であるDicke状態を生成することに成功した。

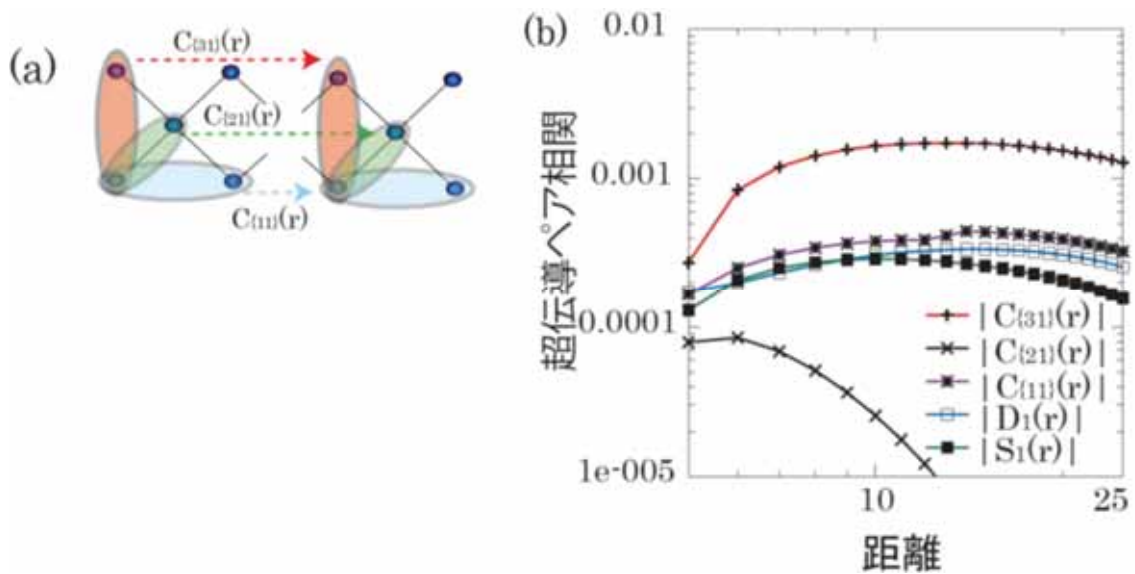


図22. (a) 平坦バンドの最も簡単な模型の一つである、ダイヤモンド鎖の構造と、その上での様々な超伝導クーパー対（楕円で囲まれたもの）。(b) 密度行列繰り込み群（テンソルネットワーク法の一つ）を用いて得られたクーパー対の相関関数。(a)において赤で示したペアが、長距離相関をもつことが分かる。

④ 競合する技術・アプローチに対するベンチマーク

光格子中の冷却原子を用いた量子シミュレーション：

ごく最近、米国で斥力相互作用する2成分フェルミ原子気体の反強磁性相が観測された。この反強磁性は、銅酸化物高温超伝導の引力起源となり、*d*波超流動実現にむけた非常に重要な成果であり、異常金属相などの理解も深まることが期待される。また、同じ米国で、引力相互作用する2成分フェルミ原子気体について、*s*波

超流動の前駆現象として密度揺らぎの増大が観測されている。さらに、ドイツにおいて、強い量子揺らぎのある 1 次元系での反強磁性相関が観測されている。以上の結果は、2 次元正方格子および 1 次元格子での結果であり、本研究のような、高い超伝導転移温度が期待される、2 層 2 次元平方格子での量子磁性相の観測は例がなく、ImPACT の成果は独自の成果である。

また、最近ドイツおよびスイスにおいて、ハニカム型光格子を用いた研究がすすみ、トポロジカル相転移などの研究が行われているが、平坦バンドを有する光格子に関する実験は、世界的にも、本研究のリープ型光格子および米国のグループによるカゴメ型光格子のみで、特に、平坦バンドまで超低温の原子を導入できているのは当研究のみであり、これも独自の成果である。

3. 研究開発プログラムの全体成果

(1) 目標達成の状況（目標達成できた場合の要因分析、目標達成が困難となった場合の原因分析も記載）

- ニューロン数 100、シナプス結合数 10,000（全結合）の小規模量子ニューラルネットワーク、およびニューロン数 2048、シナプス結合数 4,194,604（全結合）の中規模量子ニューラルネットワークの原理実証を完了し、高インパクト学術雑誌（Science）への掲載および記者発表を行った。またこの成果をもとにクラウドサービス環境（QNNcloud）を実現した。公開から1年間実機は中断なく稼働し、この間アクセス総数は520万件を超えた。この数字は、QNNの存在が世界の研究者の間で広く認知されたことを示すものである。
- ニューロン数が100,000、ニューロン間シナプス結合数が 10^{10} （全結合）の大規模量子ニューラルネットワークは実機が完了し、現在その性能を評価している。
- 量子ニューラルネットワークに搭載するアルゴリズム（応用例）を、創薬、無線通信、圧縮センシング、などの組合せ最適化の分野で開発が進められている。
- 商用ファイバー環境での量子鍵配送の長期安定化、様々なアプリケーションを支える鍵供給インターフェースと大規模鍵管理システムの実現、システム全体の安全性評価技術の確立を行った。超長期間安全性を持つデジタルアーカイブ技術を実現できる見通しが立った。
- 室温超伝導体の実現につながる2次元2層正方格子上の斥力を有する冷却原子による超流動現象の実証とその定量的評価を実現する見通しが立った。

(2) 参考指標

① 民間企業等とのマッチング及び橋渡しの状況

	目標値	26年度	27年度	28年度	29年度	30年度
企業の研究者数	80	20	39	40	34	31
協力企業数 ※	9	2	5	5	6	4

注：平成30年度分は平成31年3月11日時点

※ 研究開発に参画する企業だけでなく、研究成果の展開に意欲を示し、ImPACTで得た機密情報を開示する秘密保持契約等を具体的に結んだ企業の数

② 論文

	目標値	26年度	27年度	28年度	29年度	30年度
全 体 数	約660報	13	68	138	126	102
うち IP ファクター 10 以上	50 以上	0	8	13	12	15

注：平成30年度分は平成31年1月末時点

③ 学会発表

	目標値	26年度	27年度	28年度	29年度	30年度
全 体 数	約 1300	46	248	299	306	233
学会賞等の受賞数		2	2	15	13	7

注：平成30年度分は平成31年1月末時点

④ 国際学会における招待講演

	目標値	26年度	27年度	28年度	29年度	30年度
全 体 数	270	11	61	61	67	53

注：平成30年度分は平成31年1月末時点

⑤ 特許出願件数

	目標値	26年度	27年度	28年度	29年度	30年度
国内	35	0	2	15	11	2
海外	15	0	0	1	10	1
合 計	50	0	2	16	21	3

注：平成30年度分は平成31年1月末時点

⑥ 知財・標準化等の取組状況

1) QKD ネットワーク関連

- ・ NICT と NEC が中心になってアプリケーション・インターフェース(API)、鍵フォーマット、ライフサイクルを管理できるネットワークアーキテクチャを開発し、現在運用を進めている。それらの実績を基に NEC より ETSI : European Telecommunications Standards Institute (欧州電気通信標準化機関) の下で開催された ETSI ISG-QKD にて標準化の提案を行なった (平成29年6月)。
- ・ 東芝からは、アプリケーションへの鍵供給インターフェースの標準化提案がなされ、2019年2月に標準化を完了した(ETSI GS QKD 014 V1.1.1 (2019-02), Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API)。
- ・ 安全性評価・校正技術に関して NICT、NEC、北大、東大において新たな QKD のサイドチャネルの発見と対処方法の提案がなされ、特許申請 (特願2016-176364) と論文発表を行った。今後、安全性評価・校正技術の標準化提案を行う予定である。
- ・ 本プロジェクトで開発した量子セキュアネットワークのレイヤ構造と鍵管理技術は、国際電気通信連合-電気通信標準化部門 (ITU-T) の Study Group 13 及び Study Group 17 に提案し勧告草案化した。2020年の勧告発行に向けて今後とも標準化活動を推進して行く予定である。

- ・ 秘密分散ストレージネットワークの今後のサービス実現に向けて、基本特許「クラウドサービスを用いた安全な秘密分散保管システム」を申請した。

2) ドローン通信関連

- ・ ドローン通信セキュリティ技術に関しては、物理乱数列による鍵生成、鍵共有の前提となる相互機器認証、鍵を配送する際の秘密鍵交換などのドローン通信システムの標準化を担う団体が国内にないのが現状である。今後、NICTでは他機関と協力し既存関連団体や協議会（例えば内閣府所掌の「小型無人機に係る環境整備に向けた官民協議会」等）にセキュリティ標準化を議論する場の設置を目指してプロジェクト終了後も取り組んでゆく予定である。
- ・ 秘匿ドローン通信に関する基本特許「移動体制御システム」（特願 2015-17948）、ドローンを活用した柔軟かつダイナミカルな鍵配送ネットワークに関する基本特許「無人航空機を介した暗号鍵共有システム、無人航空機による信号伝送システム、無人航空機」（特願 2016-20885）を出願した。今後、標準化や実用化の足がかりとして活用してゆく予定である。

⑦ アウトリーチ等の状況

	目標値	26年度	27年度	28年度	29年度	30年度
アウトリーチ回数	70	9	22	15	66	13
新聞、TV等の報道数		3	14	26	20	40

注：平成30年度分は平成31年1月末時点

⑧ その他特筆すべき取り組み

ImPACT プログラムの最大の目標は、新技術の創出、その社会実装、産業界へのインパクトであるが、将来の人材、ブレークスルーの種を育てておくことも重要なミッションである。そのような観点から、プロジェクト発表論文を目的別に3つのカテゴリーに分け、バランス良くプロジェクト運営が取れているかどうかをチェックしている。2018年9月現在の発表状況は表7に示すようになっており、パイプラインングへの手当てもできていると判断している。

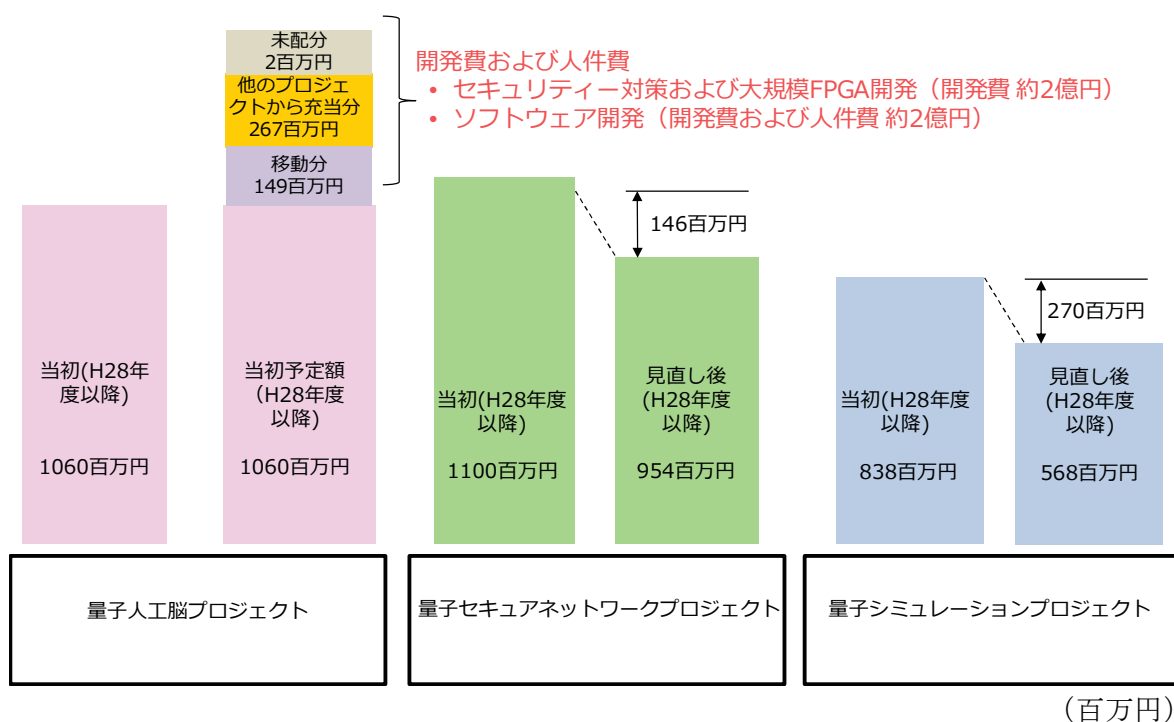
（2019年3月までの発表論文数は年度内に更新予定）

表 7. ImPACT プロジェクトからの発表論文数.

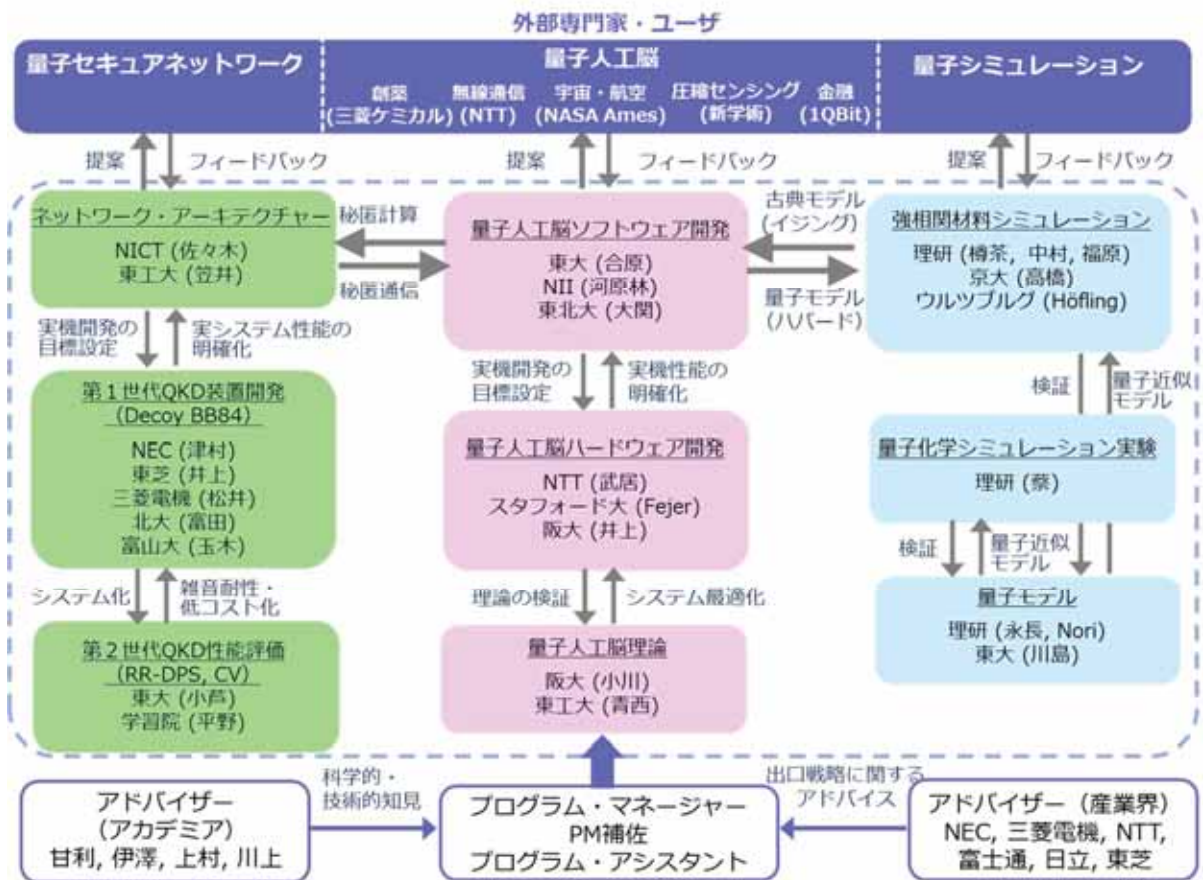
指標	雑誌名	Im pact factor	論文数	合 計
最先端の研究分野で世界をリードする競争力を保持しているか	Nature	41.577	2	49
	Science	41.058	3	
	Nature Materials	39.235	1	
	Nature Nanotechnology	37.490	2	
	Nature Photonics	32.521	6	
	Nature Physics	22.727	3	
	Advanced Materials	21.950	1	
	Physics Report	20.099	3	
	Phys. Rev. X	14.385	3	
	Reports on Progress in Physics	14.257	1	
	Nature Communications	12.353	17	
	Nano Letters	12.080	2	
	Science Advances	11.511	5	
学問を深化させ、将来の研究者・教育者の育成に貢献しているか	Small	9.598	2	241
	npj Quantum Information	9.206	7	
	Phys. Rev. Lett.	8.839	37	
	Optica	7.536	1	
	ACS Photonics	6.880	1	
	IEEE Trans. Inf. Foren. Sec.	5.824	1	
	Journal of High Energy Physics	5.541	2	
	Phys. Rev. Applied	4.782	2	
	Scientific Reports	4.122	20	
	Phys. Rev. B	3.813	54	
	Optics Letters	3.589	3	
	New J. Phys	3.579	17	
	Applied Physics Lett.	3.495	4	
	Optics Express	3.356	5	
	Phys. Rev. A	2.909	65	
	J. Chem. Phys.	2.843	1	
	Phil. Trans. R. Soc. A.	2.746	1	
	IEEE Photonics Journal	2.627	1	
	J. Phys. Condens. Matter	2.617	1	
	Applied Physics Express	2.555	1	
	Chaos	2.415	1	
	Entropy	2.305	2	
	Phys. Rev. E	2.284	9	
	Semicond. Sci. Tech.	2.280	2	
	IEEE T. Inform. Theory	2.187	1	
将来のブレークスルーの種となるアイデアを創出しているか	J. Phys. A. Math. Theor.	1.963	2	33
	Physica D	1.960	1	
	Physica Scripta	1.902	1	
	Neural Comput.	1.651	1	
	European Physical Journal B	1.536	1	
	Int. J. Bifurcat. Chaos	1.501	4	
	J. Phys. Soc. Jpn	1.485	10	
	Jpn. J. Appl. Phys.	1.452	1	
	IEEE Security & Privacy	1.239	1	
	Int. J. Mod. Phys. B	0.769	1	
	Quantum Science and Technology	---	9	
	Journal of Physics Communications	---	1	
		合計		323

4. 研究開発プログラム予算の推移

当初計画よりも早期に小規模・中規模量子ニューラルネットワークの開発が終了し、中規模量子ニューラルネットワークを世界中の研究者が自由に使えるクラウドサービス環境を開発し、合わせてニューロン数が 100,000、ニューロン間シナプス結合数が 10^{10} （全結合）の大規模量子ニューラルネットワークの開発を新たに行うために当初計画を変更し、この開発に向けて約 4 億円の予算をプロジェクト内の配分変更により確保した。



5. 研究開発プログラムの推進体制



6. 研究開発プログラムの実施管理状況

(1) 研究開発プログラムのガバナンス

① 進捗状況の把握及び指導・管理状況

- 研究開発プログラムの基本思想・戦略を大所高所の立場からアドバイスしていただくプログラム・アドバイザー（アカデミア）として、甘利俊一（脳科学）、伊澤達夫（フォトニクス）、上村洸（計算物理）、川上則雄（物性理論）の4名をプログラム内に配した。また、研究開発プログラムの出口探索という観点から、江村克己（NEC）、山田真治（日立）、中川路哲男（三菱電機）、寒川哲臣（NTT）、斉藤史郎（東芝）、佐相秀幸（富士通研究所）の6名をプログラム・アドバイザー（インダストリー）として配した。
- アドバイザー会議を年2回ほど開催し、プロジェクト側から研究開発の進捗状況を報告し、コメントをいただいた。
- プログラム全体会議を年1回（3日間、最終年度は1日、一般公開）の日程で開催している。全ての研究代表者が発表し、参加研究者がポスター発表を行う。
- 量子人工脳プロジェクトでは、クラウドシステム開発チーム、クラウドサービス開発チーム、アルゴリズム開発チームの3ワーキングチームを立ち上げ、2週に1回のペースで作業部会を開催し、研究開発の促進を図った。また、3ヶ月毎に1回のペースで量子人工脳ミーティングを開催し、研究開発の方向性を議論した。
- 量子セキュアネットワークプロジェクトでは、3ヶ月毎に1回のペースで勉強会を開催し、研究開発の方向性を議論した。
- 量子シミュレーションプロジェクトでは、研究進捗報告会を月1回のペースで（サイトビジットと組み合わせて）開催した。
- PMはこれらの機会に必ず出席し進捗状況の把握と共に、研究開発の方向性を現場と共有した。

	26年度	27年度	28年度	29年度	30年度
運営会議等の開催数	9	19	19	14	11
研究開発機関等の訪問回数	25	55	65	27	28

② 新たな発想・アイデアの採用（若手・女性人材の育成を含む）に関する取り組み

プロジェクト参加研究者（特に、大学院生、ポスドク）と、1対1のミーティングを日常的に行ない（通常は1時間ほど）、研究上の発見やチャンスを見逃さないように努めている。

③ 研究開発機関等の評価及び追加変更の状況

	26年度	27年度	28年度	29年度	30年度
参画研究機関数	13	26	29	29	26
参画研究者数	92	220	254	239	204
うち中止（解任）	2	29	62	58	6
追加（新任）	92	130	63	48	27

* 平成31年度は平成30年3月11日時点

④ 「選択と集中」に向けた取り組み

- 量子人工脳のソフト開発に関しては、量子論に基く数値シミュレーション手法を具体的な問題に応用して性能を評価し、アルゴリズム開発チーム全体で情報を共有し、チームワークで目標達成を目指した。量子人工脳のハード開発に関しては、NTT-阪大グループがクラウドサービス用中規模機開発と大規模機の技術開発を、NII-スタンフォード大グループが小規模機による原理実証を進めつつ、開発が加速するようオープンな情報交換を行なう体制を構築した。コヒーレント・イジングマシンとコヒーレント SAT マシンに集中して開発に取り組んできた。
- 量子セキュアネットワークの物理層装置開発に関しては、日本電気、東芝、三菱電機が技術の優劣を相互に評価できるような競争的環境で進めつつ、一方では、それぞれの強みを生かしたアプリケーションを開発させ win-win の関係で国際競争力を高められるように進めてきた。鍵管理層の開発に関しては、3社が協働していく形で進めてきた。アプリケーション層の開発に関しては、NICTが中心になり潜在ユーザとの対話を重視し、マーケティング開拓に努めた。
- 量子シミュレーションのハード開発に関しては、京大（冷却原子）と理研（超伝導量子回路と半導体量子ドット）、ウルツブルグ大（量子井戸ポラリトン）の量子シミュレータの性能が相互にチェックできる形で進めてきた。有効性の検証に関しては、3機関で協働して進めてきた。

（２）研究成果の展開に向けた今後の方針及び取り組み

① これまでの取り組み

- プロジェクトの成果物の一つとなる知財に関しては、知財戦略と知財出願は、NTT（量子人工脳担当）、NICT（量子セキュアネットワーク担当）、理研（量子シミュレーション担当）の知財部門と運営会議メンバーが中心となって、これに当たった。
- 国際技術動向調査を目的として、欧州における量子セキュアネットワーク開発の中心である EU Flagship プロジェクトおよびイギリス国家プロジェクト（Quantum Technology Hub）との情報交換（ワークショップ形式）を年1回の

ペースで行った。米国における量子アニーリング開発の中心プロジェクト（IARPA）との情報交換を年1回のペースで行った。

- 平成29年11月に量子ニューラルネットワーク・クラウドサービスを開始後は、米国、欧州、中国の主要研究機関への宣伝を積極的に行ない、量子コンピュータ開発のメインストリームとしての地位の確立を目指した。
- 量子コンピュータの様々な方式の特徴を理解し、応用分野の開拓に資する機会を作るために、量子コンピュータのベンチマークを目的とした第一回目の研究会「量子コンピュータ研究会」を平成31年1月に開催した。

② 今後の方針と具体的な取り組み計画

- 「量子コンピュータ研究会」を「量子に発想を持つアクセラレータ研究会」と名称を変えて、今後、年1回の割合で開催する。今後は海外の専門家も交えた国際フォーラムにしていく予定である。
- 量子ニューラルネットワークの研究機関を集めて、最新のアイデアや結果を情報交換する共通の場を提供するため、国際フォーラム“Coherent Network Computing”を立ち上げた。第一回目は平成31年3月に東京で開催し、その後は、ヨーロッパ、アメリカと順に開催していく予定である。

7. PMの自己評価

(1) PMが実施管理を行った研究開発プログラム（研究成果）に関する評価

① 産業や社会のあり方の変革（漸進的でなく、非連続的なイノベーション）をもたらす見通しは得られたか。

量子コンピュータの将来の産業や社会へ及ぼすインパクトを測る上で、以下の特性が評価基準になると考えられる。

- ・ 性能（計算速度、計算精度）
- ・ 適用領域の広さ
- ・ 価格
- ・ 保守の容易さ
- ・ 大規模化（スケーラビリティ）

表8に従来型（ゲート型）の量子コンピュータとImPACTで開発を進めた量子ニューラルネットワークをこれらの特性毎に比較した。表から明らかなように、漸進的ではなく、非連続的なイノベーションが達成された。

表8. 量子コンピュータと量子ニューラルネットワークの比較。

	量子コンピュータ	量子ニューラルネットワーク
計算速度 ¹⁾		
$N = 50$	600 (秒)	0.37 (ミリ秒)
$N = 100$	~700年	2.5 (ミリ秒)
$N = 150$	~200億年	54.0 (ミリ秒)
適用領域	狭い（因数分解など問題に周期性がある場合に有効）	広い（組合せ最適化など問題に周期性がない場合でも有効）
価格	≥10億円	≤1億円
保守の容易さ	困難 （量子ビットの個別制御必要） （極低温、超高真空が必要）	容易 （量子ビットの個別制御不要） （室温・常圧動作可）
大規模化 （開発期間）	50ビット（30年）	10 ⁵ ビット（6年）

1) NP困難クラスの N ビットMAX-CUT問題の正解を得るのに必要な計算時間で評価

- 現代社会で重要な組合せ最適化問題を、現代コンピュータ（アルゴリズム）に比べて、高速・高精度で解けることを実証した。
- 従来の量子コンピュータ研究では常識であった低損失な系を実現しなければ量子加速は期待できない、という基本的な考えをくつがえした。
- 複数の基本特許が権利化され、実用化技術はNTTへ移転された。

- ② 上記①以外の派生的な効果（派生的に生み出された成果、新たな学術的知見の創出、失敗から得られた知見等）として、どのようなものが得られたか。

量子情報科学分野では、長らくエンタングルメントの存在する（分離できない部分系からなる）量子系とエンタングルメントが存在しない（分離できる部分系からなる）古典系という切り分けが一般的な考え方であった。しかし、今世紀に入ってから、エンタングルメントは存在しないが、非古典的相関（量子ディスコードという量で評価される）は部分系に存在する量子系というものがあることが、一部の数学者の間で発見されていた。量子ニューラルネットワークは、この新しい量子系の実現そのものになっていることが明らかになった。

（２）PM自身の活動（プログラム・マネージメント）に関する評価

- ① <目標設定>産業や社会のあり方変革を目指した研究開発プログラムとして、目標設定の水準は妥当であったか。

平成 23 年～24 年頃まで、我々は最も高速なクロック周波数(40GHz)で動作するゲート型量子コンピュータ（光パルス制御量子ドットスピンを用いた方式）の開発を行っていた。超伝導量子ビットを用いたゲート型量子コンピュータの開発をしていた IBM、Google と激しい開発競争を行っていた。平成 23 年～24 年になると、開発すべきゲート型量子コンピュータの全体像（全量子ビット数 $10^8 \sim 10^9$ 、全計算時間 2～14 日が必要という事実）が理論的に明らかになり、我々は 15 年に及んだこの研究開発路線を中止することを決め、より実用性が高い光発振器ネットワーク型に舵を切った。世界中の研究者が目指している方向と全く逆の路線（量子ビットではなく光発振器、閉鎖系ではなく開放系）を採用することに不安を持つ研究者もいたが、幸い小数の研究者がリスクを取ることに賛成してくれ、ImPACT プロジェクトの立ち上げが可能となった。それから 4.5 年、リスクを取り世界と戦う意志を持った仲間は着実に増え、従来路線を継続している IBM や Google との開発競争を再び行なえるところまで到達した。

- ② <作り込み>トップ研究者の採用や異分野研究者との融合、外部専門家からの助言聴取など、国内外から斬新なアイデアや最先端の知見等を結集して研究開発を推進できたか。また、研究開発の実施体制は適切であったか。

困難な目標に挑戦するという ImPACT の主旨、PM の抱いている現状に対する危機感がプロジェクト全体に伝わるよう、全体会議、アドバイザー会議、各種研究会、プロジェクト・メンバーへのメールなどを通して PM の意見を率直に述べてきた。また、プロジェクトを牽引するキープレーヤー（助教、ポスドク、大学院生を問わず）を定期的に JST へ呼び、1 対 1 で直接進捗報告を聞き取り、研究指導・アドバイスを与えることで研究開発の加速に務めた。

③ <進捗管理> 研究開発の進捗状況や国内外における研究開発動向（ベンチマーク）等に応じ、各プロジェクトの加速、減速、中止、方向転換等を果敢に行うことができたか。

ImPACT プロジェクトの開始後は、量子ニューラルネットワークを中心に据えた研究開発方針は変更していない。それは以下のような情勢判断に基いている。

- 1) 情勢 IBM と Google の超伝導量子コンピュータ開発チームが着実に技術力を磨き、近い将来に 50～100 量子ビットマシンを開発し、量子コンピュータの古典コンピュータに対する優位性（量子サブリマシーと彼らは呼んでいる）の実証に結びつけようとしている。

PM の判断 50～100 量子ビットマシンで解ける実問題はなく、応用先は恐らく見つかるまい。量子サブリマシーの中味は、これまで数多くの量子光学、冷却原子実験で繰り返し実証されてきたものと同じであり、学問的にも新規性はない。よって、IBM や Google のエフォートが ImPACT にとって直接の脅威になることは当分の間ないと判断している。真の脅威は、新しい量子誤り訂正符号が発見されて、必要な量子ビット数が大幅に改善された場合に起きる。この時には、ゲート型はネットワーク型にとって強力な競合技術の一つになり得る。

- 2) 情勢 Microsoft がトポロジカル量子コンピュータ開発チームを、米国と欧州の有力グループを統合して立ち上げ、世界の量子コンピュータ開発のメインストリームに立とうとしている。

PM の判断 ボソンでもフェルミオンでもない第 3 の量子粒子（エニオン）を用いることで、デコヒーレンスの問題をクリアするというのが中心的アイデアであるが、現実の材料に必ず存在する素励起 (quasi-particle) により必ず有限のデコヒーレンス時間が現われ、量子誤り訂正技術は使わざるをえなくなる。また量子計算のユニバーサル性を担保するための非クリフォードゲート実装のためのマジック状態の生成と純粋化をオフラインで実行しなければならず、Microsoft の数学グループが考えているほど容易な道筋ではない。よって、現時点では純粋基礎研究と位置付けるべきものとする。真の脅威は、マジック状態の生成を必要としないフィボナッチ型エニオン粒子が見つかった場合に起きる。この時には、トポロジカル量子計算はネットワーク型にとって強力な競合技術のひとつになり得る。量子シミュレーション（理研）グループの一部が、この場合の手当てとして配された。

- 3) 情勢 D-WAVE が 500 ビット、1000 ビットマシンに続き、2000 ビット量子アニーラマシンを開発し、クラウドサービスに供した。このクラウドサービスを利用するユーザ集団が、無視できない大きさに成長しつつある。

PM の判断： D-WAVE マシンは、量子ビットをキメラグラフというスパースな配線をつないだシステムであり、与えられた実問題（任意のグラフ）を解くためには、これをキメラグラフに埋め込まなければならない。このため、1000 ビットマシンでは問題サイズ $N \leq 40$ 、2000 ビットマシンでも問題サイズ $N \leq 70$

の実問題へしか対応できない。よって、今のところ ImPACT にとって強力なライバルであるとは考えていない。

④ <関係者の巻き込み> 研究開発に関連する産業界を巻き込み、それら関係者の自発的な研究開発投資を誘導することはできたか。

⑤ <成果の展開> 得られた研究成果の産業界への橋渡しや将来的な実用化・事業化に向けた戦略（知財及び標準化を含む。）及び体制が構築できたか。

（＊④⑤の項について以下あわせて記載）

ハード（コヒーレント・イジングマシン）とソフト（各種応用アルゴリズム）の開発体制に関しては、ImPACT プロジェクト内に必要最低限のリソースが配されており、世界と十分に戦える戦力は保持してきた。しかし、AIP やコンパイラの開発を含むミドルウェア全体の開発には、リソースが回っていないのが現状である。現在、量子コンピュータのミドルウェア開発で最も高い技術レベルを保持しているのは、カナダのスタートアップ（1QBit 社）であると判断している。量子ニューラルネットワークのハード開発の中心にある NTT と優れたミドルウェア技術を有する 1QBit 社をはじめとする北米の研究開発会社の協力体制を確立すべく、NTT の新研究所を主戦場と目されるシリコンバレーに開設することとなった。

⑥ <PM 支援機能の活用> PM 補佐や JST、外部支援の活用など PM 支援機能を有効に活用できたか。

できた。

⑦ <アウトリーチ> アウトリーチ活動等が積極的に行われ、研究開発の意義・重要性等に関し、関連する産業界や一般の理解が深まったか。

PM エフォートのおおよそ 50% はこれに当てられた、と言っても過言ではない。ImPACT プログラム開始後、現在までに PM が世界各地で行った基調講演、招待講演を表 9 にまとめる。4.5 年間に行った基調講演、招待講演、コロキウムの総数は 89 件におよぶ。

表 9. 基調講演、招待講演リスト.

日にち	会議名	場所
2014/12/9	Nonequilibrium phase transitions in diverse physical systems	東京大学 本郷キャンパス（東京）
2014/12/20	応用物理学会・量子エレクトロニクス研究会	上智大学軽井沢セミナーハウス（長野）
2015/1/10	情報処理学会・第56回プログラミング・シンポジウム	ラフォーレ伊東（静岡）
2015/2/4	NZIAS-MPIPKS Tandern Workshop	Novotel Rotorua Lakeside, Rotorua, New Zealand
2015/2/7	武田シンポジウム	東京大学 武田ホール（東京）
2015/3/23	UK-Japan Quantum Technology Workshop	英国大使館（東京）
2015/4/17	Symposium on Advances in "Quantum Materials, Quantum Physics and Nanophotonics"	Universität Würzburg, Germany
2015/5/30	Hybrid Photonics and Materials (HPM2015)	Petros M. Nomikos Conference Centre, Santorini, Greece
2015/7/13	東京大学-NTT 技術交流会	ホテルニューオータニ 東京（東京）
2015/7/15	ISC High Performance (ISC 2015)	Messe Frankfurt, Germany
2015/7/22	International Conference on the Strong coupling between Light and Matter	National Chiao Tung University, Taiwan

日にち	会議名	場所
2015/8/3	第28回 回路とシステムワークショップ	淡路夢舞台国際会議場（兵庫）
2015/8/7	International Nano-Optoelectronics Workshop (iNOW 2015)	東京大学生産技術研究所（東京）
2015/8/25	量子現象利用デバイス技術分科会	(社)電子情報技術産業協会（東京）
2015/8/27	The 11th Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR 2015)	BEXCO, Busan , Korea
2015/9/17	日本物理学会2015年秋季大会シンポジウム	関西大学 千里山キャンパス（大阪）
2015/9/22	12th US-Japan Seminar	Monona Terrace Convention Center, Madison, WI, USA
2015/10/1	5th International Conference on Quantum Cryptography (QCrypt 2015)	如水会館（東京）
2015/11/11	Japan-Netherlands Forum	ANAインターコンチネンタルホテル東京（東京）
2015/11/16	防衛省情報本部研究会	防衛省（東京）
2015/12/10	US-Japan Workshop on Quantum Annealing and Coherent Computing	Stanford University, CA, USA
2016/1/26	第3回SNT研究会	産総研臨界副都心センター（東京）
2016/1/27	Nanotech Robotics 2016	東京ビックサイト（東京）
2016/3/4	光材料・応用技術研究会 第4回研究会	東京大学山上会館（東京）
2016/3/11	IBM Research Almaden's Science Colloquium Series	IBM Research - Almaden, San Jose, CA, USA
2016/3/31	17th International Conference on Physics of Light-Matter Coupling in Nanostructures (PLMCN17)	東大寺総合文化センター（奈良）
2016/5/24	9th International Conference on Quantum Dots (QD 2016)	Ramada Plaza Jeju Hotel, Korea
2016/5/31	2016 Canadian-Japanese Scientific & Cultural Exchange Meeting on Quantum Computing via Quantum Annealing	カナダ大使館（東京）
2016/6/27	23rd Central European Workshop on Quantum Optics (CEWQO 2016)	Orthodox Academy of Crete, Greece
2016/7/16	Ultrafast Dynamics at the Nanoscale 2016 (UDN 2016)	沖縄科学技術大学院大学（沖縄）
2016/12/1	EMN Meeting on Quantum Matter 2016	Labourdonnais Waterfront Hotel, Port-Louis, Mauritius
2016/12/14	Initiative Seminar on Quantum Technology	Chalmers Conference Centre, Gothenburg, Sweden
2017/2/3	第3回 浜松ICTシンポジウム	ホテルクラウンパレス浜松（静岡）
2017/2/6	International Solid-State Circuits Conference (ISSCC 2017)	The San Francisco Marriott, CA, USA
2017/3/23	2017 Sweden-Japan International workshop on quantum nanophysics and nanoelectronics	パシフィコ横浜（神奈川）
2017/5/9	Systems X Focus Group Meeting	Stanford University, CA, USA
2017/5/25	CREST「量子技術」公開シンポジウム	東京大学生産技術研究所 ENEOSホール（東京）
2017/6/15	大阪大学基礎工学部シグマ講演会	大阪大学豊中キャンパス（大阪）
2017/7/10	18th International Conference on Physics of Light-Matter Coupling in Nanostructures (PLMCN18)	Neubaukirche, Universität Würzburg, Germany
2017/7/17	Principles and Applications of Control in Quantum Systems (PRACSYS 2017)	Hotel Deca, Seattle, WA, USA
2017/8/24	24th General Congress of Int'l Commission for Optics (ICO-24)	新宿京王プラザホテル（東京）
2017/8/29	15th International Conference on Advanced Materials (ICAM 2017)	京都大学（京都）
2017/9/1	ロードバンド・ユビキタス調査会	明治記念館（東京）
2017/9/12	Network-based Biocomputation (Bio4Comp)	Vienna House QF Dresden, Dresden, Germany
2017/9/18	QSIT Colloquium	ETH, Zurich, Switzerland
2017/9/20	International Symposium "20 Years Nano-Optics"	Max Planck Institute, Erlangen, Germany
2017/10/2	Okinawa School in Physics: Coherent Quantum Dynamics (CQD 2017)	沖縄科学技術大学院大学（沖縄）
2017/10/3	Okinawa School in Physics: Coherent Quantum Dynamics (CQD 2017)	沖縄科学技術大学院大学（沖縄）
2017/10/4	Okinawa School in Physics: Coherent Quantum Dynamics (CQD 2017)	沖縄科学技術大学院大学（沖縄）
2017/11/15	System X Fall Conference	Stanford University, CA, USA

日にち	会議名	場所
2017/12/1	応用物理学会 超伝導分科会 第56回研究会	アットビジネスセター東京駅（東京）
2017/12/6	三菱ケミカルリサーチワークショップ	三菱ケミカルリサーチ（東京）
2017/12/20	原財団 特別セミナー「量子コンピュータ関連政策とブレークスルー」	ホテルニューオータニ東京（東京）
2017/12/27	理学部情報科学科 講義	お茶の水大学（東京）
2017/1/29	System X Seminar	Stanford University, CA, USA
2018/4/5	NTT CIM チームキックオフミーティング	箱根湯本開雲（神奈川）
2018/5/8	2nd Annual Symposium on Quantum Science and Quantum Engineering	Technion, Haifa, Israel
2018/5/9	Special Physics Colloquium	Weizmann Institute of Science, Rehovot, Israel
2018/5/16	東京大学講義	東京大学（東京）
2018/6/4	第38回量子情報技術研究会（QIT38）	広島国際会議場（広島）
2018/6/25	東京理科大学講義	東京理科大学（東京）
2018/6/29	第321回科学技術展望懇談会	帝国ホテルタワー（東京）
2018/7/3	11th International Conference on Nanophotonics (ICNP2018)	WUST, Wroclaw, Poland
2018/7/10	IEEE Photonics Society Summer Topical Meeting	Hilton Waikoloa Village, Hawaii Island, USA
2018/7/13	IQC Quantum Frontiers Distinguished Lecture	Waterloo University, Waterloo, Canada
2018/7/18	9th International Conference on Spontaneous Coherence in Excitonic Systems (ICSCE9)	ITHQ, Montreal, Canada
2018/7/31	Japan-Canada Conference	カナダ大使館（東京）
2018/8/1	CLEO Pacific Rim 2018 (CLEO-PR 2018)	Hong Kong Convention & Exhibition Centre, Hong Kong
2018/8/11	物理と量子情報（蔡先生シンポジウム）	東京理科大学（東京）
2018/8/24	ImPACTシンポジウム（光化学）	JST（東京）
2018/8/27	Quantum Computing Materials Challenges	UCLA IPAM, LA, CA, USA
2018/9/4	CREST-EU QT Flagship Joint Workshop	UPMC, Paris, France
2018/9/7	東大セミナー	東京大学 本郷キャンパス（東京）
2018/9/11	日本物理学会2018年秋季大会	同志社大学（京都）
2018/9/20	Photonics in Switching and Computing - PSC-18	St. Raphael Resort, Limassol, Cyprus
2018/9/27	13th Japan-US Joint Seminar on Quantum Electronics and Laser Spectroscopy	金沢APAホテル（石川）
2018/10/7	サイエンス・テクノロジーフォーラム第15回記念会合	京都国際会館（京都）
2018/10/22	19th Chitose International Forum of Photonics Science and Technology (CIF19)	千歳タウンプラザ（北海道）
2018/11/15	三菱商事調査部	三菱商事本社（東京）
2018/12/10	日本学術振興会協力会 理事会・評議員会 特別講演	東京グリーンパレス（東京）
2018/12/14	応用物理学会 量子エレクトロニクス研究会	上智大学軽井沢セミナーハウス（長野）
2019/1/7	49th Winter Colloquium on the Physics of Quantum Electronics (PQE-2019)	Snowbird, Utah, UT, USA
2019/1/13	Heraeus Seminar on "Scalable Hardware Platforms for Quantum Computing"	Physikzentrum Bad Honnef, Bonn, Germany
2019/1/18	Institut für Physik Seminar	Humboldt-Universität zu Berlin, Germany
2019/1/30	量子コンピュータ研究会	国立情報学研究所（東京）
2019/2/7	Weekly Quantum Lunch Seminar	Los Alamos National Laboratory (LANL), NM, USA
2019/3/6	ISDCS Workshoo on Optoelectronics	広島大学（広島）
2019/3/8	学振130委員会	東京理科大学（東京）
2019/3/18	Coherent Network Computing (CNC 2019)	NTT厚木研究所（神奈川）

- ⑧ <人材育成>若手や女性を含め研究人材の育成にどの程度貢献できたか。また、基礎研究からイノベーションを生み出す取り組みに関する参画研究者の意識改革がどのように進んだか。

ImPACTに参加した博士研究員（ポスドク）で、大学等の教員となったリストを以下に示す。

表 10. ImPACT 出身の大学教員

	ImPACT 研究機関	大学におけるポスト
Alireza Marandi	NII	Assistant Professor @ Caltech
Peter McMahon	NII	Assistant Professor @ Cornell Univ.
宮崎 涼二	NII	特任助教 @ 東北大学
香取 勇一	東京大学	准教授 @ 公立はこだて未来大学
Timothee Leleu	東京大学	特任助教 @ 東京大学
神山 恭平	東京大学	特任助教 @ 東京大学
佐々木 寿彦	東京大学	助教 @ 東京大学
村上 雄太	東京大学	助教 @ 東工大
北村 想太	東京大学	助教 @ 東京大学
大塚 朋廣	理研	准教授 @ 東北大学
Zhihui Peng	理研	Professor @ Hunan Normal Univ.
Simon John Devitt	理研	Lecturer @ Univ. of Technology Sydney
Lin Zhirong	理研	Chief Professor @ Shanghai Institute of Microsystem and Information Technology (SIMIT)
山口 真	理研	特任講師 @ 東海大学
蔡 恩美	京都大学	助教 @ 東京大学
加藤 宏平	京都大学	特任助教 @ 大阪市立大学

- ⑨ <全体>更なる研究開発の発展や、我が国の産業競争力の強化、困難な社会課題の解決に向け、どれほどの貢献ができたか。

特になし。

- ⑩ <全体>目標通りの成果が得られなかった事例等の原因分析や解析が適切に行われ、そこから得られた知見や教訓を次の挑戦に活かすことができるか。失敗を通して次の挑戦につながる道筋は描けたか。

特になし。

(3) その他、ImPACT プログラム全体に対する所感・提言（自由記載）

特になし。