

# ERATO 今井量子計算機構プロジェクト 追跡評価報告書

## 総合所見

量子情報科学は、数学、情報学、物理学、化学、工学など、様々な分野の研究者が参画し、急速に成長している新しい学問分野である。ERATO「今井量子計算機構」プロジェクトはこの分野の中心的テーマである量子情報、量子計算において、理論、実験の双方で世界をリードする研究を行ってきた。本プロジェクトは、SORST「量子情報アーキテクチャー」などに引き継がれ、さらなる発展を見た。SORSTでは、量子情報基礎理論、量子アルゴリズムや、量子通信の原理実証実験などの基礎研究を発展させるとともに、量子暗号通信の実用化に向けた研究が精力的に進められ、安全性保証理論とセットになった量子鍵配送システムの開発が成された。その後、NICT 委託研究を中心とした実用的な量子暗号の試験ネットワークへと進められた。

具体的な研究テーマとしては、有限長コードに対するデコイ法の安全性評価の理論研究と量子鍵配送装置への適用や、多者間プロトコルである匿名ネットワークにおけるリーダー選挙問題を解く量子アルゴリズムの発明と線形光学素子による実装など、理論家と実験家の有機的な協働による独創的な取り組みが展開された。

本プロジェクトでは、ERATO Conference on Quantum Information Science (EQIS) という、関連分野を広く包括する高いレベルの国際会議を開催してきた、ERATO 終了後は Asian Conference on Quantum Science (AQIS) に発展的に改組され、アジア地域における量子情報分野の最重要国際会議としての地位を得ている。

人材育成に関しては、メンバーが IBM 科学賞を受賞するなど、数学及び情報科学分野において、実験科学者との共同研究能力に優れた、日本を代表する若手研究者を多数育成した。また、日本における量子情報の研究分野の過去十年の進展を考えると、直接の研究成果や人材輩出にとどまらない貢献が認められる。分野の黎明期において、質の高い国際会議を毎年開催することで、研究者の裾野を拡げ、交流を活発にし、若い学生が世界の最先端の研究に触れる機会を提供し続けたことは、量子情報分野における日本のプレゼンスを確立する上で、有形無形の影響を与えてきたといえる。

## 1. 研究成果の発展状況や活用状況

ERATO「今井量子計算機構」プロジェクトの研究テーマは、SORST「量子情報アーキテクチャー」プロジェクト、NICT 委託研究「量子暗号の実用化のための研究開発」、科学研究費などによる研究に引き継がれ、それぞれ順調に発展、進化をとげてきた。多数の影響のある論文、総説、出版物、特許、招待講演などの成果を生み出すとともに、量子情報技術を実用に供するための、重要課題の解決に大きく貢献してきた。

量子鍵配布に関しては、有限長コードに対するデコイ法の安全性評価の理論研究、さらに、その量子鍵配送装置への適用は、世界先駆けて、実用上避けられない有限長コードでのシステムの安全性評価を行ったものとして、高く評価される。実用化に向けた舵取りのもと、トータルとして安全性保証理論に裏打ちされた量子鍵配送システムの開発が **SORST** で行われ、その後 **NICT** 委託研究に引き継がれている。これらの研究は、2010 年行われた量子暗号ネットワークの実証実験（東京 **QKD**）の基盤となっており、実用化に向けて大きく貢献した。

現在では量子鍵配送システムは、ほぼ実用段階に入っており、**ERATO** で培われた安全性評価に裏付けされたシステムが我が国の強みとなっており、今後の国際的な規格化、標準化において重要な役割を果たすことが期待されている。

量子暗号を超える、多者間の量子プロトコルとして、**ERATO** 期間内に発明された、匿名ネットワークにおけるリーダー選挙問題を解く量子アルゴリズムについても、その後、線形光学素子によって実装することに成功している。

本プロジェクトで行われてきた量子情報に関する質の高い研究は、プロジェクトの研究者達の以降の研究にも大きく影響を与えている。たとえば、メンバーの一人は古典情報理論ではあるが、**information spectral method** において画期的な成果を挙げ、2011 年の **IEEE IT** における年間論文賞を受賞した。量子リスト符号、あるいは量子公開鍵暗号に関して、プロジェクト中に得た成果をさらに発展させたものが、影響力のある論文誌に掲載されてるなど、研究の発展が続いている。

量子計算の分野での新たな展開としては、量子対話型証明に関して大きな進展を得ている。このテーマは解析が非常に難しく、世界の一線の研究者の多くが手を焼いたもので、プロジェクト中にも未解決として残された問題が多かった。そのうちいくつかの重要な問題が解決された。理論計算機科学の国際会議の最高峰といわれている **IEEE Ann. Sympos. Foundations Theoretical Computer Science** で発表している（2009 年）。

全般的に見て、**ERATO** プロジェクトの期間中に培った理論家と実験家の有機的な協働体制は我が国の量子情報分野の進展に非常によい影響を与えており、今後の同様のプロジェクトの運営における重要な指針をあたえらる。

## 2. 研究成果から生み出された科学技術的、社会的及び経済的な効果・効用及び波及効果

### 2.1 科学技術の進歩への貢献

本プロジェクトで特筆すべきこととして、国際シンポジウム **ERATO Conference on Quantum Information Science (EQIS)** の創設が挙げられる。**EQIS** は、理論研究者、実験研究者やその分野が広く包括され、かつ、適切な査読制度により高いレベルの研究成果が発表される場として、海外からも高く評価される国際会議となった。**ERATO** 終了後は **Asian Quantum Information Science (AQIS)** に発展的に改組され、さらにアジア地域における量子情報分野における重要な国際会議として、重要な役割を果たしている。最近になって北

米の著名な会議の日本への誘致が決まるなど、日本がこの分野における国際的な地位を確立する上で大きく貢献してきた。

また、研究においても、コンピュータサイエンスの視点からの量子情報処理へのアプローチは、国内においてユニークなものであり、重要な貢献が引き続き行われている。特に、「量子リーダー選挙アルゴリズムの提案と実証」は、量子情報処理が、量子暗号や量子コンピュータ以外にも適用可能であることを、理論的に提案、さらに実験により実証したもののとして、高く評価できる。

さらに、量子暗号について、鍵が有限長である場合の厳密な解析は、量子鍵配布装置の具体的な安全性を議論する上で必要不可欠だけでなく、国際的に見ても非常にユニークなものであり、国際的な研究の潮流をかえるほどの貢献を行っている。世界で初めて提唱された量子版ユニバーサル符号は、量子情報理論の基礎を成す研究であり、最新の量子情報理論の研究にも大きな影響を与えている。また、メンバーによって著された **Quantum Information: Introduction (Springer, 2006)** は、世界の量子情報の研究者のための基本的テキストの一つとなっている。この中にはプロジェクトで得られたと思われる未出版の研究内容も多く盛り込まれており、ERATO から量子情報理論の一つの流れを作った本ということができる。

また、量子計算の能力の本質的起源と限界の解明という、非常に重要かつ困難な課題についても、量子アルゴリズムと古典アルゴリズムによる通信量比較などを着実に進めていることも評価できる。量子情報理論における重要な未解決問題のひとつが最近解決されたが、そこに至る研究の流れの中には、ERATO プロジェクトの成果が大きな位置を占めている。実際的な量子計算の実現にはまだまだ時間がかかると思われるが、本プロジェクトやその後継で得られた成果や人材、あるいは研究運営の手法が、次の課題解決に大いに役立つと期待される。

## 2.2 応用に向けての発展

本プロジェクトならびにその後継プロジェクトでの最も大きな成果は、量子暗号鍵配送 (QKD) システムの実装とその展開研究である。その実装にはノイズがあるような伝送路でも安全性を保証できるような技法が必要だったが、前項でもふれたように、デコイ法を適用するための基礎理論を構築し、それに基づいてシステムの開発が行われた。2010年には、本プロジェクトで培われた知見、技術を生かし、実用的な量子暗号の試験ネットワークが東京で稼働し成功を収めるなど、量子暗号通信の技術は、実用段階に近づいている。また、ニーズとコストの問題が真剣に議論され、国際標準化に向けた活動が活発化するレベルに至っている。

その他、もつれ合い光子対光源の開発、高速量子鍵配布装置の開発など、社会・経済的にインパクトをもたらす技術への取り組みも十分行われている。量子計算に関しては、実際的なシステムの構築やその上での展開には時間を要すると考えられるが、本プロジェク

トで得られた成果はその実現に向けての重要な基盤となると期待される。

本プロジェクトのように、広範かつ深遠なテーマに挑戦する場合、プロジェクト内での集中的な研究に加えて、それを支える広がりをもったコミュニティを創成することが不可欠である。国際会議の立ち上げやテキストの作成などが有効に機能したと考えられる。

### 2.3 参加研究者の活動状況

本プロジェクトのユニークな点として、技術参事として2名の若手研究者を雇用、育成した点が挙げられる。技術参事として、さまざまなプロジェクト会合に具体的に参画し、またマネジメントに携わることが、貴重な経験となったであろうことは想像に難くない。

その他の、プロジェクト当時の若手研究者も、大学で教授、准教授のポストに就いて、研究および教育において活躍している。多くの研究者が量子情報関連分野で指導的役割を果たしている。また、ERATO プロジェクトの成果が、後に IBM 科学賞などの重要な受賞や注目すべき論文などの成果にもつながっている。プロジェクト当時参加していた学生も、世界に通用する研究者として育てている。海外からの参加した研究者も国内外の研究機関で活躍している。

また、プロジェクトの研究者の有志で、「量子冬の学校」を毎年開催をしており、同分野における後進の学生、若手研究者の育成を行なっている点も高く評価したい。

### 3. その他特筆すべき事項

量子情報科学は、数学、情報科学、物理学、化学、工学など様々な分野の研究者が参画する新しい学問領域である。その中で本プロジェクトでは、数学及び情報科学分野において、実験科学者との共同研究能力に優れた、日本を代表する若手研究者を著しく多数育成したことは特筆すべきと考える。

現在においても、量子情報科学は、量子シミュレーションや量子計測など、多様な展開を見せている。したがって、本プロジェクトで創成、展開された、数学及び情報科学分野の優秀な研究者と実験科学者の共同研究に対する支援が今後も期待される。

プロジェクト開始時より、毎年、国際会議 **EQIS** を開催し、終了後もアジアに拠点を拡大した **AQIS** として継続されている。量子情報分野の成長期に、我国でレベルの高い国際会議が毎年開催されたことは、日本のこの分野における地位向上に大いに貢献した。

本プロジェクトの成功要因として、研究員に学生の教育の負担を負わせることなく研究に専念させることができた点が挙げられている。さらに、個々の研究者の顔が見えるような配慮がなされていた。その結果、研究者は研究に集中することができ、学界において良い成果をあげて、キャリアアップにつなげるという好循環が生まれたと考えられる。しかし、一般論として、教育経験がキャリアアップや研究者の質的深化に重要な要素であることも確かであり、また、「研究員の顔が見えるような配慮」を制度的に促すのは簡単ではない。研究員の研究・教育のエフォート配分の設計については画一的な解というものはなく、今

後の ERATO 研究制度においては、様々なフィードバックを得て少しでも良い制度設計を目指してもらいたい。