

日本安全保障貿易学会 第38回研究大会

量子情報科学技術をめぐる 国際的な競争と協調

京都先端科学大学
准教授 土屋貴裕

はじめに

- 量子情報科学技術(Quantum Information Science and Technology, QIST)は、近年急速に発展している科学技術分野
- 「量子覇権」をめぐって国家間が競争と協調を生み出している
- 量子情報科学技術には、量子コンピューティング、量子通信(量子鍵配送、量子インターネット)、量子センシングなど、多岐にわたる技術が含まれている
- 量子情報科学技術の獲得は、国家の安全保障や経済的競争力に直結する可能性がある

量子技術をめぐる国際的な競争

➤ 量子コンピュータの開発競争が顕著

- ・従来のコンピュータでは解決困難な問題を高速に解く能力を持つ
- ・実用化により経済、軍事、サイバーセキュリティをはじめとする多くの分野での優位性をもたらすことが期待

➤ 米国、中国、欧州をはじめ諸外国が量子技術の研究開発に巨額の投資

- ・米国は、量子技術において長年リーダーシップを維持
→国防総省や国立科学財団を通じて研究を進めている
- ・中国は、量子通信技術において大きな進展
→世界初の量子通信衛星「墨子号」を打ち上げ、QKDネットワークを敷設・延伸
- ・2019年4月、中国RMY社が米国企業Princeton Lightwave社からキーデバイスである光子検出用APD技術とデバイスビジネスを買収

For Internal Use Only Until: Permanent

量子技術をめぐる国際的な協調

➤ 量子情報科学技術は、その複雑さと多様性から、国際的な協調が不可欠

- ・量子技術の研究には膨大なリソースと専門知識が必要に
- ・量子コンピューティングの進展により、量子通信が必要に
- 一か国のみでの進展には限界

➤ 各国は共同研究プロジェクトや国際会議を通じて知識とリソースを共有し、技術の進展を図っている

Ex) 欧州連合の「量子フラッグシッププログラム」

- ・欧州全域の研究者を集め、量子技術の発展を加速させるために設立
- 米国・欧州間で量子通信や量子コンピューティングに関する共同研究が活発化



ORGANISATION



eqtc.qt.eu

CONFERENCE MANAGEMENT
Mandiconventus
eqtc@mandiconventus.pt



For Internal Use Only Until: Permanent

競争と協調のバランス

➤ 量子情報科学技術における国際的な競争と協調のバランス

- ・競争は技術革新を促し、各国が技術的優位を追求する動機となるが、過度な競争は国家間の緊張を高め、技術の進展を妨げる可能性
- ・協調は技術の発展を加速させるが、知的財産権や技術ノウハウの流出等、経済安全保障上のリスクのみならず、国家安全保障上のリスクを招く可能性

→各国は競争と協調のバランスを慎重に保ちながら、量子情報科学技術の発展を進めている

⇒国際的なルールや標準を策定し、技術の開発と使用において公正な競争と協力を促進する必要

For Internal Use Only Until: Permanent

プロトコルと標準化の重要性

➤ 量子鍵配送(Quantum Key Distribution, QKD)

- ・現在、量子通信のためのプロトコルとして最も広く研究
- ・“量子状態に書き込まれたデジタル情報”を伝送する
トラステッド・ノード(Trusted Node)ネットワーク
※QKDによって転送される情報は量子ビットに書き込まれた古典ビット
→現行の量子暗号ネットワークはQKDの運用に特化
- ・量子鍵を利用して通信を行うことで、理論的に盗聴不可能な通信を実現
※量子情報を用いた量子インターネット・アプリケーションは実装できない
- ・中国では、2017年に北京と上海、浙江を繋ぐ「京滬幹線」
(National quantum secure communication backbone network)が完成
→QKDに関する層の厚い産業チェーンを構築、アプリケーションも続々登場

For Internal Use Only Until: Permanent

プロトコルと標準化の重要性

➤ 量子インターネット

- ・量子情報科学技術の中でも極めて重要な分野であり、量子状態を直接伝送する通信ネットワークを構築する技術

→量子コンピュータ間の通信をはじめ、秘匿型量子計算など現行のインターネットや量子暗号ネットワークでは実装できないアプリケーションの提供が可能

⇒情報の安全性とプライバシーの新たな基準をもたらす可能性

➤ 量子インターネットの実用化に向けたプロトコルとその標準化

- ・異なる国や組織が開発したシステムや技術が相互運用可能となるよう、共通のルールや基準が設定(標準化)されたプロトコルが必要

→量子通信プロトコルが標準化されることで、異なる量子ネットワーク間でのシームレスな通信が可能となる

⇒相互接続されていくことで量子インターネットとしてのグローバルな展開が促進

For Internal Use Only Until: Permanent

標準化に向けた国際的なルール形成

➤ 量子インターネットにおける標準化

- ・国際的な協力とルール形成が必要

→国際機関が関与し、量子通信に関する標準を策定するために、多国間の協議を行い、技術仕様を決定

Ex)

・国際電気通信連合(ITU)

- ・量子情報技術に関する研究グループを設置
- ・QKDの国際標準化に向けた議論を開始

・欧州電気通信標準化機構(ETSI)

- ・量子暗号に関する標準を策定するためのタスクフォースを設置
- ・欧州内外の関係者と協力してプロトコルを開発



Implementation Security of Quantum Cryptography
Introduction, challenges, solutions
First edition - July 2018
ISBN No. 978-2-9505202-2-4

For Internal Use Only Until: Permanent

課題と展望

- 量子インターネットの標準化に向けた国際的なルール形成
 - ・いくつかの課題が存在
 - ・量子技術はまだ発展途上
 - 各国が異なるアプローチや技術を採用しているため、共通のプロトコルを合意することが難しい
 - ・標準化プロセスは時間がかかる
 - 技術の進展が早い量子情報科学技術分野においては、標準が時代遅れになるリスク
 - ・標準化には国家間の競争も絡んでおり、特定の国が主導権を握ろうとすることで、協議が難航
 - ・グローバルな技術インフラとしての量子インターネット
 - ・長期的な視点からの国際的な協力・協調が不可欠
 - 国内技術が国際的に劣後することを防ぎ、標準化における存在感を示すためにもハードウェア・ソフトウェアの継続的な開発が重要

For Internal Use Only Until: Permanent

おわりに

- 量子情報科学技術をめぐる国際的な競争と協調は今後も続く
 - ・同分野での成功は、国家の未来にとって極めて重要
 - 競争と協調のバランスを保つことが、技術の進展を最大限に引き出し、国際社会全体に利益をもたらす鍵となる
- 量子インターネットで相互接続された量子コンピュータが目指される
 - ・サイバー・フィジカルシステムへ接続されることで、現在は実装できない、より高度なアプリケーションが提供可能に
 - ⇒ハイブリッド型サイバー・フィジカルシステム
- 量子インターネットのプロトコルや標準化をめぐる国際的なルール形成が量子情報科学技術の発展において重要な要素に
 - ・量子技術の普及と相互運用性の確保のために、国際的な協力・協調と標準化が必要不可欠
 - ※技術力の不足や独占はグローバルな量子インターネットの構築を妨げる
 - 国際社会は、競争と協調のバランスを保ちつつ、量子インターネットの未来を築くために取り組む必要がある

For Internal Use Only Until: Permanent

