配信先: 総務省記者クラブ、テレコム記者会、
文部科学記者会、科学記者会、
大阪科学・大学記者クラブ

プレスリリース
2025 年 3 月 13 日

国立研究開発法人情報通信研究機構
国立研究開発法人理化学研究所
国立大学法人大阪大学
株式会社 QunaSys

量子セキュアクラウドと量子コンピュータの統合実証に成功

～量子コンピュータから生み出される付加価値の高い情報の安全な伝送・保管を実証～

【ポイント】

- 情報通信研究機構の量子セキュアクラウドに理化学研究所の量子コンピュータの利用環境を接続
- 量子セキュアクラウド技術で量子コンピュータの計算結果の情報理論的に安全な伝送・保管が可能に
- ノウハウやニーズの共有により、量子技術の社会実装の加速に貢献

国立研究開発法人情報通信研究機構（ＮＩＣＴ、理事長: 徳田 英幸）、国立研究開発法人理化学研究所（理研、理事長: 五神 真）、大阪大学量子情報・量子生命研究センター（QIQB、センター長: 北川 勝浩）及び株式会社 QunaSys（QunaSys、CEO: 楊 天任）は、NICT が整備して研究開発及び運用を進めている量子セキュアクラウド[*1]と理研が中心となって開発した国産ゲート型量子コンピュータ[*2]を接続し、国産ゲート型量子コンピュータを安全に利用するための相互接続環境を構築しました。量子セキュアクラウドのユーザーが国産量子コンピュータ機能を利活用でき、生み出されたデータを安全に伝送・保管できることを実証しました。

今後、NICT、理研の各拠点のトライアルユーザー双方に機能を提供し、ノウハウやニーズの共有を含めた交流を深め、量子技術の社会実装の加速に貢献していきます。

【背景】

現在、量子技術を様々な社会課題の解決に利活用することを目指して、国内外で活発な研究開発が進められています。その中でも、NICT が中心となって取り組んでいる量子セキュアクラウド技術と理研が中心となって取り組んでいる量子コンピュータの技術は、いずれも産学官の連携の下、社会実装に向けた研究開発が実を結びつつある研究開発として注目されています。そのような中、政府が 2020 年に策定した量子技術イノベーション戦略に基づいて発足した量子技術イノベーション拠点では、NICT は量子セキュリティ拠点として、理研は量子コンピューテーション開拓拠点として位置付けられ、量子技術の基礎研究から技術実証、オープンイノベーション、知的財産管理、人材育成等に至るまで産学官で一気通貫に取り組んでいます。

今回、両拠点の相互接続を実現したことで、産学官連携強化や国際協力強化に向けてより強固な体制の下、我が国の産業の強みを生かし、量子技術を軸とした新産業創出や社会課題解決に向けた環境を実現しました。

【今回の成果】

NICT と理研がそれぞれ主導する研究開発チームの協力により、量子セキュアクラウドが構築されている NICT の東京 QKD ネットワーク[*3]と理研の量子コンピュータを相互に接続する環境を構築しました（図 1 参照）。これにより、量子コンピュータを遠隔地から利用する際の通信に量子暗号[*4]技術を用いることが可能になりました。例えば、個人の遺伝子情報は極めて高い秘匿が要求される個人情報であるため、絶対に他人に盗み見られることがないようにすることが肝要です。このように秘匿性の高いデータを量子コンピュータで処理する際

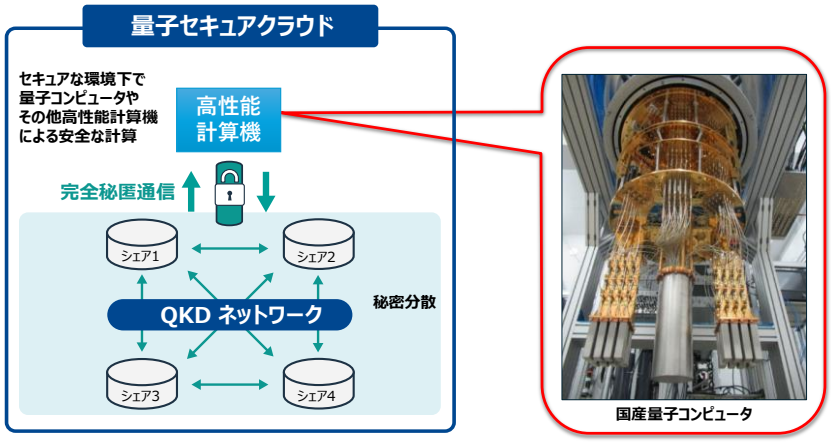

図 1 NICT の量子セキュアクラウド（左）と理研の量子コンピュータ（右）の統合

には、その入出力を傍受されないようにする必要があります。さらに、そのような付加価値の高い情報を超長期に安全に保管する必要があります。

今回の実証では、東京 QKD ネットワーク上の鍵管理システムから供給された鍵を利用し、ユーザーは完全秘匿通信路を介して理研の量子コンピュータを操作することが可能になりました。今後は、NICT と理研の間で QKD リンクを定常的に運用することにより、東京 QKD ネットワーク上に構築している量子セキュアクラウドに安全に保管したデータを量子コンピュータで処理し、その処理結果を量子セキュアクラウドに再び保管することで、通信内容の傍受を不可能とし、重要なデータを絶対に盗み見られることなく、かつ、従来の古典的なコンピュータでは実現できなかったような高速なデータ演算処理が可能になるための道筋が切り拓かれました。

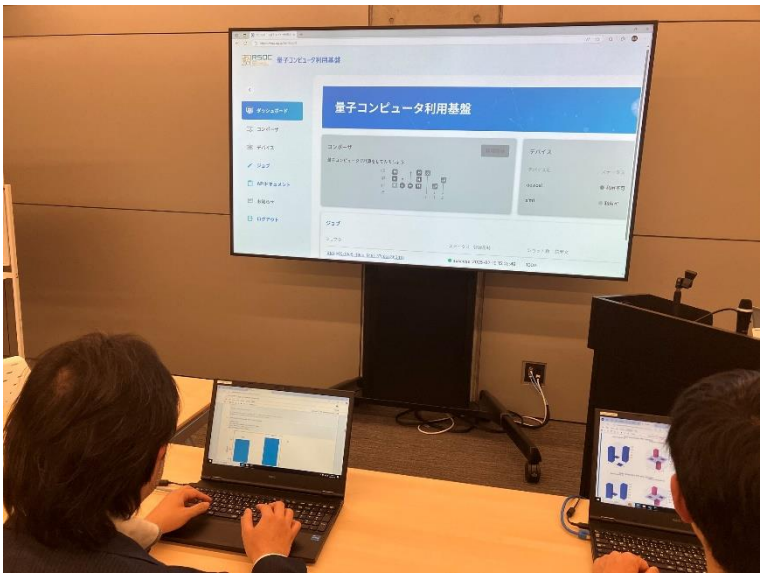

図 2 東京 QKD ネットワークから量子コンピュータを操作する様子

【今後の展望】

今後、NICT、理研の各拠点のトライアルユーザー双方に機能を提供し、ノウハウやニーズの共有を含めた交流を深め、量子技術の社会実装の加速に貢献していきます。

＜各機関の役割分担＞

・NICT: 量子暗号ネットワークテストベッドの運用、相互接続環境の構築、セキュアストレージの提供
・理研: 量子コンピュータの提供・運用
・QIQB: 量子コンピュータミドルウェア[*5]・コミュニケーションサイトの構築・運用
・QunaSys: 量子・古典ハイブリッドのユーザアプリケーション環境の整備

＜関連する過去の報道発表＞

・2023 年 12 月 18 日 複数の企業間を結ぶ量子暗号ネットワークテストベッドの運用試験を開始
https://www.nict.go.jp/press/2023/12/18-1.html
・2023 年 3 月 24 日 量子コンピュータを利用できる「量子計算クラウドサービス」開始
－国産超伝導量子コンピュータ初号機の公開－
https://www.riken.jp/pr/news/2023/20230324_1/index.html

なお、本研究の一部は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「先進的量子技術基盤の社会課題への応用促進」（研究推進法人: QST）の研究開発テーマの「量子セキュアクラウドを用いた高度情報処理基盤の構築」と「国産量子コンピュータによるテストベッドの利用環境整備と運用」によって実施されました。

＜ 本件に関する問合せ先 ＞
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
藤原 幹生
E-mail: qictcc-info@ml.nict.go.jp

国立研究開発法人理化学研究所
量子コンピュータ研究センター
萬 伸一
E-mail: shinichi.yorozu@riken.jp

大阪大学量子情報・量子生命研究センター
森 俊夫
E-mail: t.mori.qiqb@osaka-u.ac.jp

株式会社 QunaSys
広報担当
E-mail: pr@qunasys.com

＜ 広報（取材受付）＞
国立研究開発法人情報通信研究機構
広報部 報道室
E-mail: publicity@nict.go.jp

国立研究開発法人理化学研究所
広報室 報道担当
E-mail: ex-press@ml.riken.jp

大阪大学量子情報・量子生命研究センター
企画室 プレスリリース窓口
E-mail: press_qiqb@ml.office.osaka-u.ac.jp

株式会社 QunaSys
広報担当
E-mail: pr@qunasys.com

＜用語解説＞

***1 量子セキュアクラウド**

量子暗号技術と秘密分散技術を融合したクラウドシステムであり、データの安全な流通・保管・利活用を可能とする。量子コンピュータとの連携により、改ざん・解読が不可能な高いセキュリティ性を担保するだけでなく、例えば、金融、製造、交通・物流、管理、創薬、化学分野で蓄積された個人情報や企業情報など秘匿性の高いデータの分析・処理を含めた利活用が期待されている。

***2 量子コンピュータ**

量子力学の原理を利用した、現在の（古典）コンピュータとは異なる方式で動くコンピュータ。古典コンピュータとは動作原理が異なるため、特定の問題を超高速で解けることが知られている。例えば、量子系の効率的なシミュレーションや素因数分解などの問題が高速に解けると期待されている。

***3 東京 QKD ネットワーク**

NICT が 2010 年から東京圏に構築・運用を続けている量子鍵配送（Quantum Key Distribution: QKD）ネットワークのテストベッド。NEC、東芝、NTT-NICT、学習院大学などの様々な産学機関で開発された QKD 装置が導入され、装置改良の研究開発、長期運用試験、相互接続やネットワーク運用試験など、QKD ネットワーク技術の実用化に向けた研究開発のほか、QKD ネットワークを現代セキュリティ技術と融合した新しいセキュリティアプリケーションの研究開発などを進めている。

***4 量子暗号**

量子暗号は、「量子鍵配送」による暗号鍵の共有と、それを用いた「ワンタイムパッド暗号」から構成される。量子鍵配送では、送信者が光子を変調（情報を付加）して伝送し、受信者は届いた光子一個一個の状態を検出し、「鍵蒸留」と呼ばれる情報処理により、盗聴の可能性のあるビットを排除して、絶対安全な暗号鍵（暗号化のための乱数列）を送受信者間で共有する。変調を施された光子レベルの信号は、測定操作をすると必ずその痕跡が残る（ハイゼンベルクの不確定性原理）ため、この原理を利用して盗聴を見破る。ワンタイムパッド暗号では、送信情報のデジタルデータを、それと同じ長さの暗号鍵（0 と 1 のランダムなビット列）と足し算することで暗号化し、復号は更にもう一度足し算をすることで行う。パッドとは暗号鍵を意味する。一度使用した乱数列は二度と使わないというのがワンタイムパッド暗号の規則である。ワンタイムパッド暗号は、解読が絶対的に不可能であることがシャノンにより証明されている。

***5 ミドルウェア**

ミドルウェアでは、ユーザー認証、量子計算プログラムデータのスケジューリング管理、量子コンピュータ実機で利用できる形式への変換等を行う。