

日本電気株式会社
国立研究開発法人情報通信研究機構
国立大学法人京都大学
慶應義塾大学

**量子セキュアクラウドシステムを使って次世代レーザー設計の
最適化の処理・高秘匿伝送・分散保管を実現**
**～次世代アクセラレータと連携した量子セキュアクラウドにより
スマート製造分野における適用可能性を確認～**

日本電気株式会社(注 1、以下 NEC)、国立研究開発法人情報通信研究機構(注 2、以下 NICT)、国立大学法人京都大学(注 3、以下 京都大学)、慶應義塾大学(注 4)は、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(注 5)を適用した検証試験で、スマート製造分野での設計情報の最適化の処理・高秘匿伝送・分散保管に成功しました。

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(注 6)によって最適化された次世代レーザー(フォトリック結晶レーザー、注 7)の高度設計情報(注 8)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伝送できることを確認しました。

本検証試験の成功により、将来のスマート製造の核となると期待されるフォトリック結晶レーザーの重要な設計情報である最適設計パラメータを量子計算によって導く際に、量子セキュアクラウドシステムの適用可能性が実証できたと言え、今後、半導体産業や自動車産業など様々な製造分野への適用が期待されます。

なお、本検証試験は、内閣府が主導する戦略的イノベーション創造プログラム(SIP、注 9)「光・量子を活用した Society 5.0 実現化技術」(管理人:国立研究開発法人量子科学技術研究開発機構)の一環として実施しました。

【背景】

先端技術を用いて設計・製造工程などをデジタル化するスマート製造を実現するためには、サイバー空間(仮想空間)とフィジカル空間(現実空間)を高度に融合させたシステムが必要とされています。人材不足や技術伝承などの課題を抱える半導体産業や自動車産業などの製造分野でもこうしたシステムが生産性向上の鍵となりますが、日々巧妙化する組織化されたサイバー攻撃への懸念がこうしたシステムの実現を阻んでいます。さらに、最近では現在の暗号を高速に解読できることが知られている量子コンピュータ技術の研究開発が急速に進展するなど、潜在的な脅威もますます高まっています。

こうした中、経済安全保障の観点からも、日本の製造業の持続的な競争力の強化に寄与する技術情報や設計情報など価値の高い機密情報を安心して流通・保管・利活用できるオンプレミスのシステムの整備が求められています。

【検証試験の概要】

今回 NEC と NICT は、機密情報を安心して流通・保管・利活用できるサイバー空間を整備するため、製造分野への量子計算技術の適用可能性の検証を進めている京都大学および慶應義塾大学の間、インターネット回線も用いて構成した量子セキュアクラウドシステムを構築しました。

現在、京都大学および慶應義塾大学では、製造分野の最適化問題の具体的な例題として、将来のスマート加工用レーザー光源としての普及が期待されるフォトリック結晶レーザーの量子最適化問題に連携して取り組んでいます。本連携では、京都大学で導出したフォトリック結晶レーザーの設計パラメータおよび性能評価プログラム(機密情報に相当)を、慶應義塾大学の次世代アクセラレータに伝送して解析を行いますが、今回、両大学の研究者が安全にデータの伝送および秘密分散保管が行えるネットワークを構築しました。

現在、製造現場で使用されているレーザー加工機に革新を起こす可能性があるフォトリック結晶レーザーは、日本発の独創的な技術であり、その設計パラメータや解析プログラムは確実に守る必要がある重要な技術情報です。そこで、本検証試験では、NEC の回線暗号装置 COMCIPHER-Q(注 10)を NICT、京都大学、慶應義塾大学の計 3 拠点に設置しました。専用回線を新たに敷設するこ

となくインターネット回線上に、量子鍵配送装置で生成した暗号鍵を用いて仮想的な暗号回線を構築し、異なる組織の3拠点間で安全にデータを伝送できることを確認しました。さらに、本検証試験では拠点間の伝送と同時に NICT から Tokyo QKD Network(注 11)上に形成した秘密分散システムへ接続し、秘密分散保管を行いました。

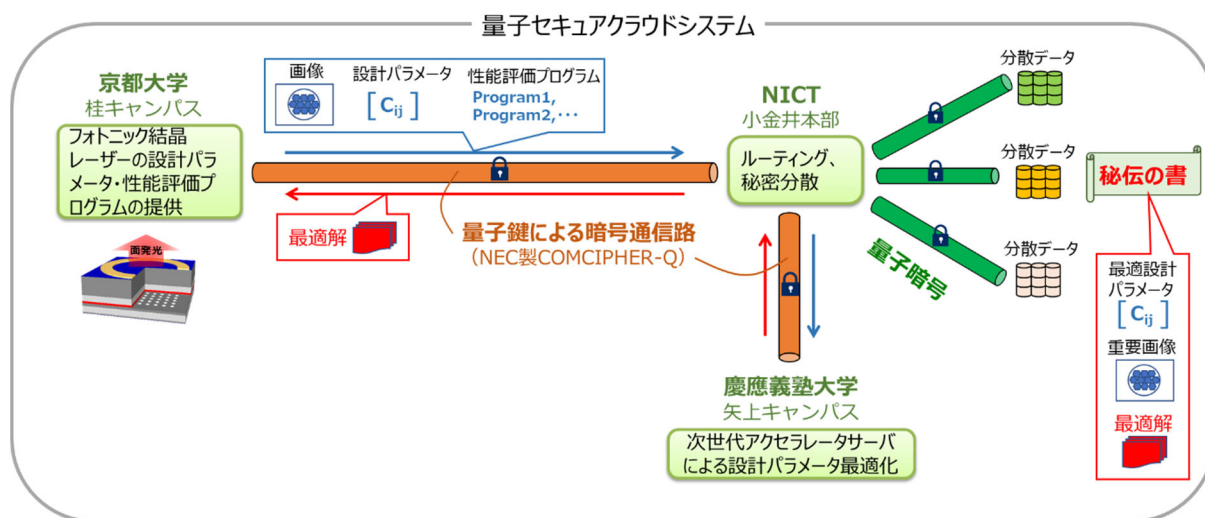


図 本検証試験のシステム構成図

今回の検証試験では、次世代アクセラレータなど優れた計算エンジンを包含した量子セキュアクラウドシステムをユーザ環境でも動作させることができました。本検証試験は、今後、様々な製造分野で適用可能であると言え、日本の製造業の国際競争力の向上に貢献できることを示しました。

【実施体制】

- ・ NEC :
 - 量子セキュアクラウドシステムと連携するネットワークの構築・運用
- ・ NICT :
 - 秘密分散システムの提供
- ・ 京都大学 :
 - ユーザ環境の提供、フォトニック結晶レーザーの設計パラメータおよび性能評価プログラムの提供
- ・ 慶應義塾大学 :

ユーザ環境の提供、次世代アクセラレータによる構造最適化の実施、最適化した設計パラメータの提供

【今後の展望】

NEC は、本検証試験や SIP の成果を踏まえて、量子暗号技術の社会実装に向けた開発を加速するとともに、量子技術を融合した先進的なネットワークの研究に取り組んでいきます。

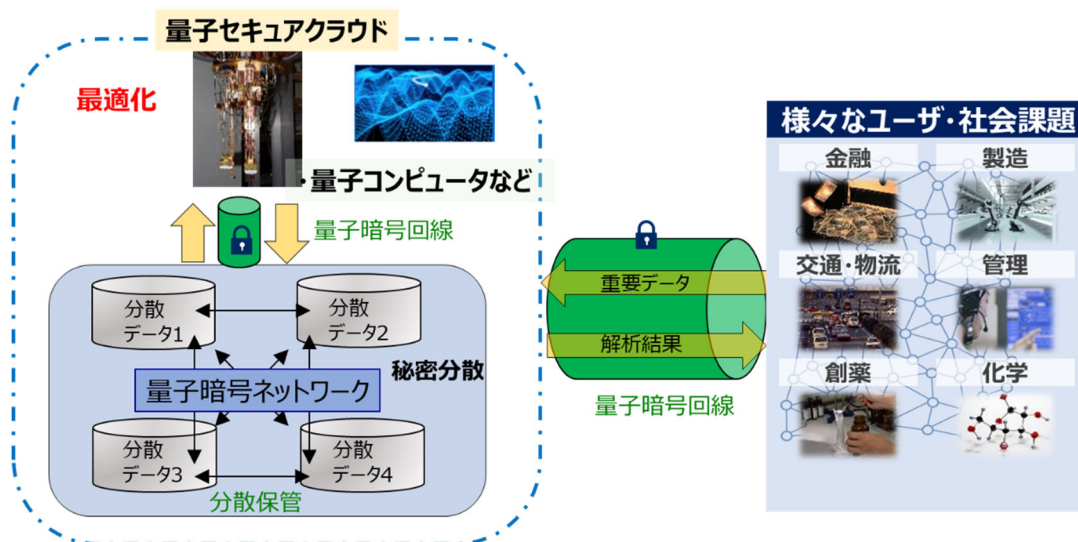
NICT は、超長期に秘匿する必要があるデータを安心して預けることができる量子セキュアクラウド技術を確立し、価値の源泉と成り得るデータを安心して利用可能な技術の研究開発を続けていきます。

京都大学は、スマート製造分野およびスマートモビリティ分野へのフォトニック結晶レーザーの適用を目指して、量子技術を活用しながらフォトニック結晶レーザーのさらなる性能向上および社会実装に取り組んでいきます。

慶應義塾大学は、本検証試験や SIP の成果を踏まえて、今後の次世代アクセラレータの社会実装に向けた研究開発を進めていきます。

以上

- (注 1) 本社：東京都港区、代表取締役執行役員社長 兼 CEO：森田 隆之
 (注 2) 所在地：東京都小金井市、理事長：徳田 英幸
 (注 3) 本部：京都府京都市、総長：湊 長博
 (注 4) 本部：東京都港区、塾長：伊藤 公平
 (注 5) 量子セキュアクラウドシステム：
 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。



量子セキュアクラウドシステムの展望イメージ

- (注 6) 次世代アクセラレータ：
 一部の計算処理に対して高効率に実行することが期待されているコンピュータ。イジングマシン、ゲート式量子コンピュータ等を指す。
- (注 7) フォトニック結晶レーザー：
 2次元フォトニック結晶(2次元状に波長程度の周期的屈折率分布をもつ光ナノ構造)を内蔵した面発光型の半導体レーザー。従来の半導体レーザーと比較して10000倍以上大きな発光面積でも単一モードで動作可能であり、高出力かつ高ビーム品質なビームを実現可能。
- (注 8) プレス発表「量子アニーリングを活用したフォトニック結晶レーザーの構造最適化に成功ー量子計算技術を活用したスマート製造分野の発展に向けてー」を参照。
<https://www.t.kyoto-u.ac.jp/ja/news/topics/research/20220908>
- (注 9) 戦略的イノベーション創造プログラム(SIP)：
 内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。
<https://www8.cao.go.jp/cstp/gaiyo/sip/>
- (注 10) 回線暗号装置(COMCIPHER-Q)：
 安全保障などの高セキュリティ要求分野で使用されている回線暗号装置(COMCIPHER(AES)シリーズ)に、量子鍵配送のための機能を追加したカスタム品(研究試作品)。FPGA(Field Programmable Gate Array)による高速なハードウェア処理を実現した暗号化・復号機能により低遅延・安定した暗号通信を実現。更にソフトウェアで機能追加することにより量子鍵配送向け機能の追加を実現。
- (注 11) Tokyo QKD Network：
 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(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。
<https://www.nict.go.jp/press/2010/10/14-1.html>