

盗聴・解読が不可能な安心・安全な通信ネットワークの実用化に向けて大きく前進  
**国内初 量子暗号システムの相互接続実験に成功**

三菱電機株式会社(執行役社長:下村節宏、以下三菱電機)、日本電気株式会社(代表取締役執行役員社長:矢野薫、以下 NEC)、東京大学生産技術研究所(所長:前田正史、以下東大生研)は、絶対的な安全性を物理法則で保証する量子暗号システムの相互接続実験に、国内で初めて成功しました。この実験では、三菱電機とNECの量子暗号システムを相互に接続し、東大生研がその安全性の評価を行いました。

このたびの成果は、情報通信研究機構(理事長:長尾真、以下 NICT)の委託研究「量子暗号技術の研究開発」(平成13年度~17年度)プロジェクトにおいて三菱電機とNECがそれぞれ開発した量子暗号システムをベースに、新たに改良を加えたシステムによって実現したものです。

今回の成功は、安全な中継点を置けば、複数人利用や量子暗号の通信距離の問題を解決でき、また中継点を網の目のように結んだ量子暗号ネットワークへの展開を意味しており、次世代の絶対的安全性を有する高秘匿通信ネットワークの実現に大きく貢献するものと期待されます。

#### 開発の背景と概要

「現代暗号」と呼ばれる現在の暗号技術(暗号アルゴリズム)は、解読するために膨大な計算時間が必要であることを安全性の根拠にしています。このため将来超高速な計算機が出現した場合には、安全性が脅かされることが指摘されています。

これに対し「量子暗号」は光子の量子状態を利用してデータを運ぶもので、盗聴されたことを必ず検出できるという特長があることから、絶対に解読されない究極の暗号として実用化が期待されています。

しかし「量子暗号」では、暗号アルゴリズムの詳細や通信に必要な光学機器の構成が標準化されていないために、異なるシステム間を相互接続した例は国内になく、多者間通信ネットワークの構築が課題でした。

今回の研究では、三菱電機とNECのシステムの相互接続を実現する技術を開発し、NICTが有する研究開発テストベッドネットワーク JGN2 秋葉原アクセスポイントにおける実験により、その有効性を実証しました。

#### 主な開発成果

##### 1. 異なる方式の量子暗号システムの相互接続方式を確立し、実証実験で確認

三菱電機とNECはそれぞれ独自に量子暗号システムの開発をしていますが、そのままでは相互のシステムを接続することができません。両社は今回、量子暗号システムを相互に接続するインターフェース機能と暗号鍵を共有する機能を新たに開発し、その方式を用いて両社の端末間で相互通信する実証実験を行い、複数の量子暗号システム間で利用可能なことを確認しました。

量子暗号システムの標準化を進める基礎技術を確立できたことで、今後の高秘匿通信ネットワークの実現が期待できます。

##### 2. 相互接続システムの安全性の検証

従来、三菱電機とNECは個別にそれぞれのシステムの安全性評価を行ってきましたが、第三者が、より客観的に安全性を評価する必要がありました。

今回の研究では、東京大学・生産技術研究所の今井秀樹前教授(現 中央大学教授 兼 産業技術総合研究所 研究センター長)のグループが、最新の量子暗号理論とセキュリティ技術の視点から実装により発生する脆弱性、更に盗聴により漏洩する情報を解析し、開発した方式が安全であることを検証・確認しました。

#### 今後の展開

関係機関の連携で、今後も相互接続可能な量子暗号システムの研究に取り組み、5年後を目標に量子暗号ネットワークの実用化を目指します。

## 開発内容の補足

図1に、三菱電機製量子暗号システムとNEC製量子暗号システムを相互接続した量子暗号ネットワークの構成を示します。従来、三菱電機製の量子信号システム(機器A・機器B)とNEC製の量子暗号システム(機器C・機器D間)は、それぞれ独立に構成され、各々のシステム内に閉じた通信が行われていました。異なる量子暗号システムをネットワーク化するためには、それらの中継する手順と方式が必要です。今回、それぞれのシステムに影響を与えることなく、相互接続可能な中継方式を新たに開発し、量子暗号ネットワークの構築に成功しました。ネットワークとしての安全性は東大生研で理論的に解析しました。

構築した量子暗号ネットワークで、鍵を共有する手順は次のとおりです。

まず、機器A・機器B間と機器C・機器D間、それぞれの通信に適用する鍵を、量子暗号を用いて設定します。機器Aと機器Bの間では鍵K1を共有、機器Cと機器Dの間では鍵K2を共有します。

次に、機器Aと機器Dが最終的に共有すべき鍵K3をセンターで生成し、機器Bと機器Cを通じて機器Aと機器Dに送ります。機器Bから機器Aには鍵K1を用いて暗号化したK3を送り、機器Cから機器Dには鍵K2を用いて暗号化したK3を送ります。機器Aと機器Dは各々復号して鍵K3を得ます。

以上の手順により機器Aと機器Dは量子暗号の理論に基づく安全な方法で鍵K3を共有できます。このK3を暗号鍵として機器Aと機器Dはデータのやりとりを安全に行うことが可能となります。

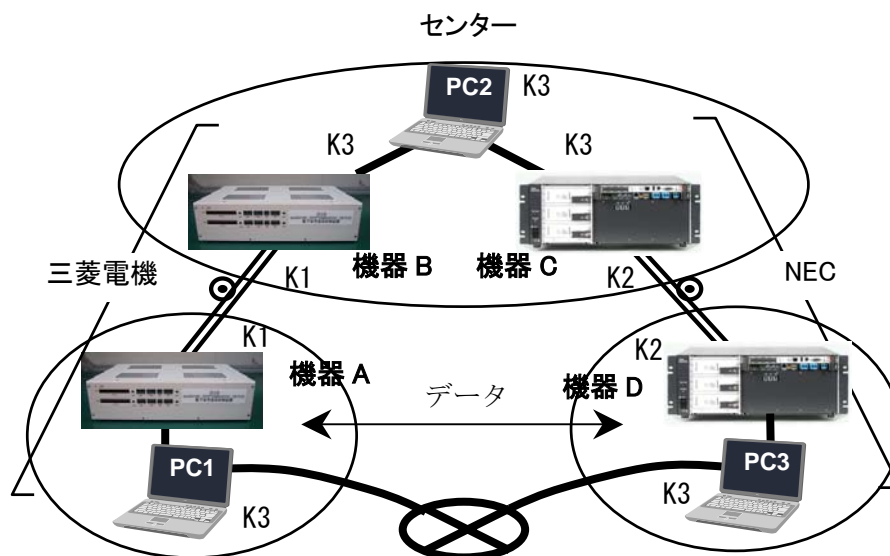


図1 量子暗号ネットワークの構成

## JGN2秋葉原アクセスポイントについて

JGN2とは、NICTが有する研究開発テストベッドネットワークで、各都道府県ならびに米国、タイ、シンガポールにアクセスポイントがあり、地方自治体や、国内外の大学、研究機関、民間企業などがネットワーク関連技術やアプリケーション技術の研究開発に利用しています。特に、秋葉原アクセスポイントでは、総延長600kmを超える実フィールドでの光伝送実験環境のほか、10G(ギガ)bpsのIPネットワークなどが利用可能です。

URL <http://www.jgn.nict.go.jp/>

## お問い合わせ先

三菱電機株式会社

<報道関係からのお問い合わせ先>

広報部

〒100-8310 東京都千代田区丸の内二丁目7番3号

電話 03-3218-2333 FAX 03-3218-2431

<開発内容に関するお問い合わせ先>

情報技術総合研究所 計画部 業務グループ

〒247-8501 神奈川県鎌倉市大船5-1-1

FAX 0467-41-2142

[http://www.mitsubishielectric.co.jp/corporate/randd/inquiry/index\\_it.html](http://www.mitsubishielectric.co.jp/corporate/randd/inquiry/index_it.html)

日本電気株式会社

<開発内容に関するお問い合わせ先>

NEC 中央研究所研究企画部 企画戦略グループ

[https://www.nec.co.jp/r\\_and\\_d/ja/cl/contact.html](https://www.nec.co.jp/r_and_d/ja/cl/contact.html)

東京大学生産技術研究所

<報道関係からのお問い合わせ先>

[koho@iis.u-tokyo.ac.jp](mailto:koho@iis.u-tokyo.ac.jp)