2025 年 1 月 15 日

NTT コミュニケーションズ株式会社

世界初、NTT Com 特許技術を活用した
量子コンピューターでも解読出来ない暗号通信を実現

ドコモグループの法人事業ブランド「ドコモビジネス」を展開する NTT コミュニケーションズ株式会社(以下 NTT Com)は、プライバシーを保護したままデータを処理する IOWN PETs※1 の技術要素である耐量子セキュアトランスポート※2 と NTT Com 特許技術を活用し、鍵供給まで含めたシステム全体において量子コンピューターでも解読出来ない暗号通信に関する実証実験(以下 本実証)に成功しました。

1.背景

2030 年頃に実用的な量子コンピューターが登場すると予想されており、それに伴い既存の暗号技術による通信が解読される可能性が懸念となっています。アメリカの NIST※3 を中心に、世界各地で量子コンピューターでも解読不可能な次世代暗号への移行が課題となっており、日本では 2024 年 7 月から金融庁でも次世代暗号への移行に関する検討会が開始されました。

本実証により、IOWN PETs の技術要素の 1 つである耐量子セキュアトランスポートと NTT Com の特許技術を組み合わせることで、量子コンピューターでも解読不可能な通信をシステム全体で実現し、量子コンピューターを使った新たなサイバー攻撃から通信上の機密データを保護することに貢献します。

2.本実証の概要

本実証では、量子コンピューターでも解読不可能な複数の次世代暗号技術を NTT Com のサービスを活用して構築し、スマホやタブレットなどの端末で安全な Web 会議が実現できることを確認しました。

IOWN PETs の技術要素である耐量子セキュアトランスポートの鍵交換※4 機能を NTT Com のクラウドシステム上に設置し、クラウドシステム上からアプリケーションに対して暗号化用の鍵データを供給しました。さらに、NTT Com 特許技術を活用し、鍵供給の際にも解読されないよう安全な供給を実現しました。アプリケーションには、NTT Com が提供するビデオ・音声通話などの開発ツール「SkyWay」※5 を活用し、これらの暗号技術を組み込んだ Web 会議システムを構築することで、量子コンピューターにも解読出来ない安全な通信を実証しました。なお、本実証は日本電信電話株式会社から技術協力を受けるとともに、国立研究開発法人情報通信研究機構「NICT（エヌアイシーティー）」量子 ICT 協創センターより情報理論的に安全な鍵を供給していただきました。

本実証で用いた技術の主な特長は以下の通りです。

(1) 複数の次世代暗号技術を利用した鍵交換機能

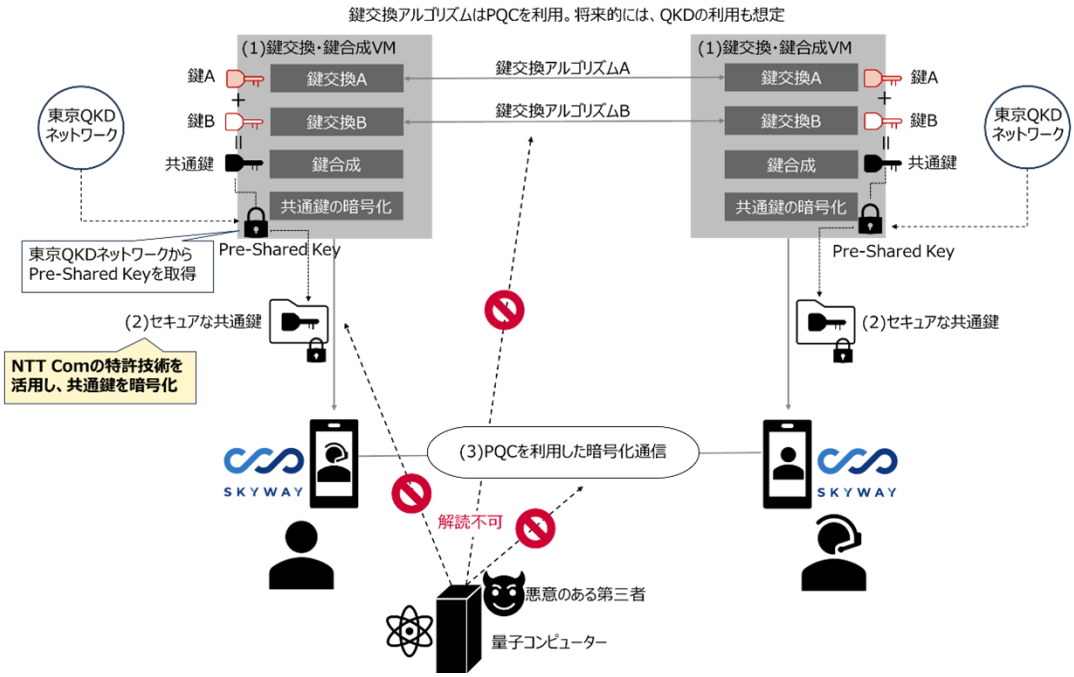
次世代暗号技術には、耐量子計算機暗号※6(PQC：Post-Quantum Cryptography、以下 PQC)を利用しました。複数の PQC を利用することで、将来的にいずれかの PQC の解読方法が発見された場合も、暗号方式を入れ替えることでセキュリティの安全性を担保します。さらに、複数の PQC で生成された共通鍵を合成することも可能です。将来的には、量子鍵配送※7（QKD：Quantum Key Distribution、以下 QKD）の利用も想定しています。

(2)NTT Com 特許技術を用いたセキュアな共通鍵の供給

(1)の機能で生成した共通鍵のデータを Pre-Shared Key※8(以下 PSK)によって、セキュアな状態にすることで、安全にアプリケーションに共通鍵を供給しています。共通鍵を PSK によって暗号化する部分に NTT Com の特許技術※9 を活用しています。なお、PSK は東京 QKD ネットワーク※10 から取得しました。

(3)PQC を利用した暗号化通信を組み込んだ Web 会議システム

1 対 1 の Web 会議間の通信を(2)で受け取った共通鍵を用いて PQC で暗号化する安全な Web 会議を「SkyWay」を用いて実現しました。スマートフォンを使った Web 会議においても、ユーザー側での追加設定など不要で簡単に動作させることが可能です。



<本実証のイメージ>

3.本実証の成果

本実証は世界で初めて、IOWN PETs の技術要素の 1 つである耐量子セキュアトランスポートと NTT Com 特許技術を組み合わせることで、システム全体の通信において量子コンピューターでも解読出来ない暗号通信を実現することに成功しました。

さらに、ユーザーが簡単に利用できるスマートフォン対応の Web 会議アプリと組み合わせることで、次世代暗号通信を手軽に導入できることを確認しました。

4.今後の展開

本実証の成果をもとに、PQC や QKD といった量子コンピューターにも解読出来ない暗号技術、IOWN 技術、析秘などの NTT Com のサービスを組み合わせた、次世代暗号通信技術の商用化をめざします。そして、機密なデータを取り扱う業界のパートナーとともに、量子コンピューター時代に向けたユースケースを創出していきます。

※1：IOWN PETs とは、NTT が提唱するデータの生成から消滅に渡る一貫したデータ主権の実現をめざすことをコンセプトとする技術です。

※2：耐量子セキュアトランスポートとは、量子コンピューター時代でも安全な通信を実現する暗号通信技術です。

※3：NIST とは、National Institute of Standards and Technology（アメリカ国立標準技術研究所）の略称で、アメリカ商務省配下の研究機関です。

※4：鍵交換とは、複数の暗号アルゴリズムを用いて複数の鍵を装置間で共有する技術です。

※5：SkyWay とは、NTT Com が提供するリアルタイムコミュニケーションを実現するマルチプラットフォーム SDK です。https://skyway.ntt.com/ja/

※6：耐量子計算機暗号(PQC)とは、量子コンピューターが苦手とすると考えられている問題を基に設計された暗号アルゴリズムです。https://journal.ntt.co.jp/article/4738

※7：量子鍵配送(QKD)とは、量子力学の原理を利用して、信頼された 2 者に対して暗号鍵を供給する方式の 1 つです。

※8：Pre-Shared Key とは、暗号化通信を行う際に、事前に送信者/受信者間で鍵を共有する方式です。

※9：特許第 4789536 号「データ分割装置、データ分割方法およびコンピュータプログラム」に関する発明

※10：東京 QKD ネットワークとは、NICT が 2010 年から東京圏に構築・運用している量子鍵配送（QKD）ネットワークのテストベッドです。