（報道発表資料）

2024.10.30

日本電信電話株式会社

世界初、通信を止めずに暗号方式を切り替え可能な耐量子セキュアトランスポートシステムを開発

発表のポイント：

- ◆ **暗号を柔軟に切り替える新技術で通信の継続性と安全性を両立**：システム停止なしに暗号方式を更新できるため、サービス中断を防ぎつつ最新のセキュリティを維持します。
- ◆ **量子コンピュータ時代の脅威に先手を打つセキュリティ対応**： 耐量子計算機暗号への迅速な移行を可能にし、未来のセキュリティリスクを未然に防ぎます。
- ◆ **オープン光通信装置で社会全体のセキュリティを強化**： オープン光トランスポート装置による光ネットワークへの適用で、社会インフラ全体の安全性を高めます。

日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：島田明、以下「NTT」）は、通信を止めることなく暗号方式を切り替え可能な耐量子セキュアトランスポートシステムを開発しました。本システムは、NTT 独自の Elastic Key Control 技術（複数の暗号方式を柔軟に組み合わせる技術）を採用し、異なる暗号方式を迅速かつ安全に組み合わせられ、さらにスムーズに切り替えることができます。これにより、現在および将来のセキュリティ脅威からデータを効果的に保護できます。また、本システムは暗号方式として最先端の耐量子計算機暗号を組み込め、アメリカの標準化機関NIST（米国国立標準技術研究所）が求める新しいセキュリティ基準にも対応し、量子コンピュータによる解読を効果的に防げます。

本システムは日本と台湾を結ぶ IOWN 国際間オールフォトニクスネットワーク（APN）で使用され、2024 年 11 月 25 日～29 日に開催される NTT R&D FORUM 2024 ―IOWN INTEGRAL（※1）に展示予定です。

1. 背景

暗号は、高度に発展したデジタル社会の基盤となる重要な技術です。しかし、コンピュータ技術の急速な進化や新たな攻撃手法の出現により、使用中の暗号方式を定期的に更新する必要が生じています。特に量子コンピュータの技術進展は、現在広く使用されている多くの暗号方式を解読可能にするため、これに対処することは、デジタル社会の信頼性と安全性を維持するために不可欠です。

この問題に対して、アメリカの標準化機関である NIST は、量子コンピュータに耐えうる新しい暗号技術の開発とその標準化を進めています。これらの新しい耐量子計算機暗号は 2030 年までの普及をめざしており、特に長期保存するデータや重要な通信においてはできるだけ早急に耐量子計算機暗号への移行が推奨されています。しかし、新しい暗号方式への移行は技術的にも困難が多く、「暗号の 2030 年問題」として広く認識されています。

このような未知の脅威に対応するため、暗号方式を迅速に更新できる「クリプトアジリティ（暗号の柔軟性）」が重要な概念となっています。これは暗号方式を迅速に更新できる能力のことで、新たなセキュリティ脅威が発生した場合にも速やかな対応を可能にします。NIST を含む多くの専門機関が、この能力の重要性を強調し、将来のセキュリティ対策としてクリプトアジリティを推奨しています。

2. 成果および技術のポイント

量子コンピュータ時代に向けて、NTT は高度なクリプトアジリティ（暗号の柔軟な更新能力）をサポートする世界初となる耐量子セキュアトランスポートシステムを開発しました。これにより、サービスの中断やセキュリティリスクを最小限に抑えつつ、新しい暗号方式への迅速な移行が可能となりました。

本システムは、NTT 独自の Elastic Key Control 技術を使用し、複数の鍵交換アルゴリズムを組み合わせて用いることで高度なセキュリティを実現しました（図 1）。Elastic Key Control 技術は、 1）鍵交換の方式として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し、 2)複数の鍵からハイブリッド化により単一の共通鍵を生成する、という二段階構成で動作します。この構造により、使用中のすべての暗号方式が同時に破られない限り通信の安全を保持することができ、従来技術にはない高いセキュリティを提供できます。さらに、アーキテクチャとして複数鍵をサポートするように設計されているため、システムを停止することなく暗号方式をスムーズに更新できます。そのため、本システムは通信の信頼性を維持しながら継続的なサービス提供ができるとともに、将来的な脅威に対して迅速かつ柔軟に対応することができます。

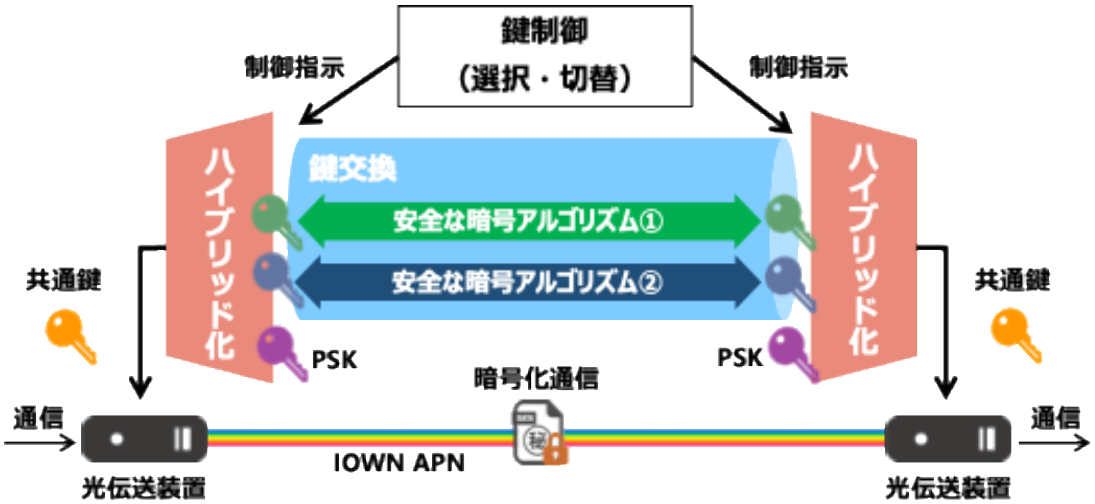

図 1：開発実装した Elastic Key Control 技術

また、従来の光トランスポート装置は一体型で提供されていましたが、近年の技術進化と要請により装置のオープン化が進んでいます。しかし、暗号処理モジュールは装置のネットワークオペレーティングシステム（NOS）に依存しており、暗号処理に関しては柔軟性が乏しい状況でした。そこで、本システムでは柔軟性を高めるために、暗号処理を NOS から切り離した「機能分離（ディスアグリゲーション）」構成を実装しました（図 2）。これにより、鍵管理や、セッション管理、暗号処理を外部から制御できるようになり、量子コンピュータに対応できる暗号機能をオープン光トランスポート装置に

統合・制御できるようになりました。開発したシステムが対応している暗号方式等の仕様は表 1 のとおりです。

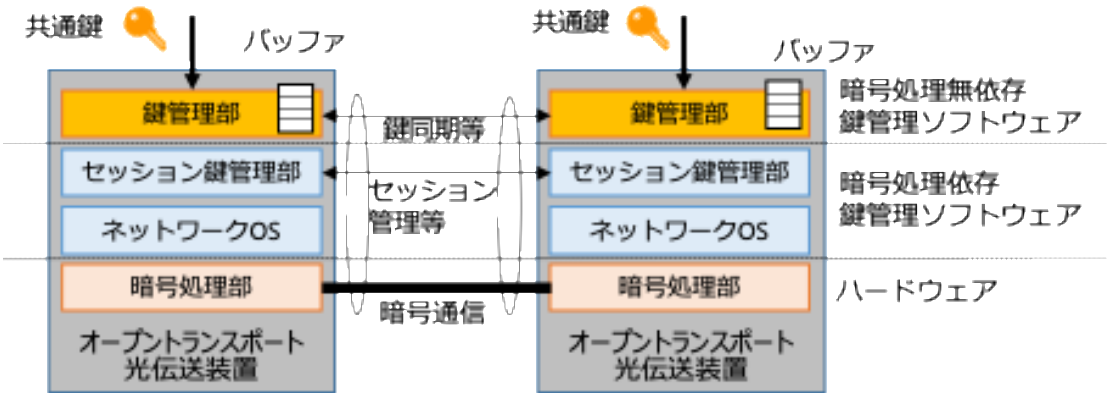

図 2：開発実装した暗号処理のディスアグリゲーション構成

表 1：耐量子セキュアトランスポートシステムの機能と仕様

機能	仕様
鍵交換機能	楕円曲線暗号（古典暗号） CRYSTALS-Kyber（耐量子計算機暗号） NTRU（耐量子計算機暗号）
鍵合成機能	複数の鍵交換方式の鍵を合成して一つの暗号鍵が生成可能
管理・制御基本機能	暗号化通信を止めずに、鍵の合成の組み合わせが変更可能
鍵管理機能	MACsec AES-GCM-256
耐障害機能	鍵更新継続時間：180s

3. 今後の展開

開発した耐量子セキュアトランスポートシステムの社会実装により、金融、医療、行政などの重要インフラのセキュリティを強化し、安心・安全な社会の実現に寄与します。また、国際間通信のセキュリティ向上にも寄与し、グローバルな信頼性確保に貢献します。本システムは、日本と台湾間を接続する世界初の IOWN 国際間オールフォトニクスネットワーク(APN)で利用される予定です。

【参考】

※1：「NTT R&D FORUM 2024 ―IOWN INTEGRAL」 公式サイト https://www.rd.ntt/forum/2024/

国際 APN を活用したデータレプリケーションや、GPU over APN といったユースケースへの適用に加え、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 IOWN PETs（IOWN Privacy Enhancing Technologies）の一部としても、デモ展示される予定です。

■本件に関する報道機関からのお問い合わせ先
日本電信電話株式会社
IOWN 総合イノベーションセンタ　広報担当
nttrd-pr@ml.ntt.com