報道発表資料

2026 年 4 月 9 日
TOPPAN ホールディングス株式会社
国立研究開発法人情報通信研究機構
ISARA Corporation

TOPPAN ホールディングス・NICT・ISARA、認証局における耐量子計算機暗号へのシームレスな移行技術を実証

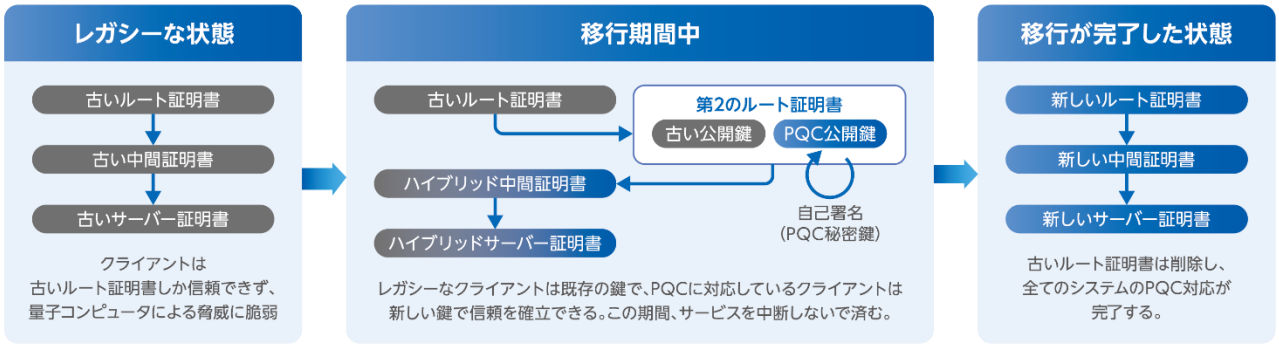
第 2 ルート証明書により、サーバーとクライアント間における通信の安全性を維持
現行暗号から耐量子計算機暗号へ段階的な移行が可能に

TOPPAN ホールディングス株式会社（本社：東京都文京区、代表取締役社長 COO：大矢 諭、以下 TOPPAN ホールディングス）、国立研究開発法人情報通信研究機構（本部：東京都小金井市、理事長：大野 英男、以下 NICT（エヌアイシーティー））、ISARA Corporation（本社：カナダ・オンタリオ州、CEO：アツシ・ヤマダ、以下 ISARA）の 3 者は、インターネット通信のセキュリティ基盤となる認証局の仕組みにおいて、現行暗号から量子コンピュータでも解読が困難とされる耐量子計算機暗号（Post-Quantum Cryptography 以下 PQC）へのシームレスな移行技術の実証実験に成功し、有用性を確認しました。

インターネット通信では、通信相手が本物であることを証明する電子証明書と、それを発行・署名する認証局による公開鍵認証基盤（※1）がセキュリティを支えています。しかし、公開鍵暗号は将来的に量子コンピュータに対し脆弱になると考えられており、PQC への移行が急務となっています。その移行の際、認証局の最上位であるルート認証局の暗号アルゴリズムを耐量子化するにあたっては、サービスの分断や停止を招く恐れがあり課題となっています。

本実証では、ISARA が開発した、ECDSA（※2）等の現行暗号から ML-DSA（※3）等の PQC への移行を簡便にする「第 2 の暗号アジャイルルート認証局が発行する電子証明書（※4）（以下 第 2 ルート証明書）」を、NICT が構築した量子暗号ネットワークテストベッド上で、TOPPAN ホールディングスが開発した IC カードシステムに適用しました。IC カードによる本人認証とWebアクセスを対象に、PQC 移行過渡期の現行暗号と PQC が混在した環境をシミュレーションした結果、既存の認証基盤を停止させることなく、スムーズな PQC 環境への移行を確認できました。これにより、医療・金融・行政など長期的な機密性が必要な分野において、サービスを停止することなく量子コンピュータの脅威に対抗可能なセキュリティレベルへの段階的な移行に貢献します。

なお、本実証の一部は、内閣府 SIP プログラム『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：国立研究開発法人量子科学技術研究開発機構）の支援を受けて実施されました。また、本実証の取り組みは、2026 年 4 月 15 日（水）から 17 日（金）に開催される「第 6 回量子コンピューティング EXPO【春】」（会場：東京ビッグサイト）にて展示します。



「第 2 ルート証明書」を活用した PQC 移行の概要 ©TOPPAN Holdings Inc.

■ 背景

インターネットのセキュリティは、公開鍵暗号を使って通信相手が本物であることを証明するデジタル証明書と、それを発行・保証する信頼された第三者機関である認証局、そして認証局から発行される証明書の連鎖（以下 証明書チェーン）とそれらの検証によって成り立っています。しかし、この基盤技術である公開鍵暗号は、将来的に量子コンピュータによって解読される可能性が指摘されています。このため、米国政府機関の国立標準技術研究所（以下 NIST）が PQC の標準化を進めており、そのアルゴリズムとして ML-DSA や ML-KEM（※5）などが選定され、世界的に PQC への移行準備が進められています。特に金融・医療・行政など、長期にわたり機密情報を保護する分野では、早期の対応が必要です。

しかし、証明書チェーンの最上位であるルート認証局が発行するルート証明書の暗号アルゴリズム変更は、社会インフラ全体に重大な影響を及ぼすため、慎重な移行が求められています。特に、現行暗号のアルゴリズムのみ対応するいわゆるレガシー端末では、新たな PQC 証明書を検証できず、通信が成立しない可能性があります。一方で、すべての利用環境を同時に PQC 対応へ更新することは現実的ではなく、移行期間中にサービスを停止することも許されません。そのため、レガシー環境と PQC 環境を、コストを抑えつつ共存させ、サービスの継続性と互換性を確保しながら、安全かつ円滑に PQC へ移行することが喫緊の課題となっていました。

これらの課題に対し、TOPPAN ホールディングス・NICT・ISARA の 3 者は、既存のルート証明書と互換性を持ちつつ、ML-DSA 等の PQC にも対応したハイブリッド証明書を証明書チェーンに介在させることができる「第 2 ルート証明書」を、IC カードシステムに適用することで、その有用性を検証しました。

■ 実証実験の概要

・実施期間：2025 年 10 月～2026 年 3 月（システム開発期間を含む）
・実施場所：TOPPAN 内の量子暗号ネットワークテストベッド接続拠点
・検証項目：ISARA の「第 2 ルート証明書」を用いて IC カード認証基盤を構築し、以下の 3 つの移行フェーズにおいて、暗号化通信プロトコル接続および相互認証（クライアント/サーバー）の動作を検証しました。本実証では、テストベッド上に閉じられたネットワークで認証を可能とするプライベート認証サーバーを設置し、本サーバーと接続することで、PQC CARD®（※6）による認証を行い、認証成功後、量子暗号による秘匿通信が可能なアプリケーションへ接続する構成としています。この時使用した PQC は、NIST が策定・公表した ML-DSA 等の標準化アルゴリズムに準拠しています。

＜フェーズ 1＞レガシー環境（現行暗号のみ）
＜フェーズ 2＞ハイブリッド移行環境（現行暗号と PQC のハイブリッド）
＜フェーズ 3＞完全 PQC 環境

・検証結果：移行段階においても安全性が維持され、既存の IC カードシステムから、システム停止を伴わずにスムーズに PQC 環境へ移行可能であることを確認しました。また、量子暗号ネットワークと連携することで、データ送受信者間での盗聴を不可能にする量子鍵配送と、利用者の真正性を保証する PQC 認証を組み合わせた多層防御を実現しました。

■ 3 者の役割

TOPPAN ホールディングス：IC カードシステムの開発・提供、量子暗号ネットワークテストベッドへの参画
NICT：本実証の全体構成、量子暗号ネットワークテストベッドの構築・提供
ISARA：第 2 ルート証明書の開発、技術提供

■ 今後の目標

3 者は今回の実証で得られた知見を基に、まずは高い安全性が要求される医療・金融業界などで実用化を行い、2030 年頃の本格的な社会実装を目指します。

また、TOPPAN ホールディングスは本実証で確立したスムーズな移行プロセスを踏まえて、IC カードシステムに限らず、Web サービスや IoT 機器など多様な既存システムの PQC 移行をサポートしていくことを

目指します。また、今後も、NICTなどと量子暗号ネットワークテストベッドのPQCを用いた高度化に取り組み、量子セキュアクラウド技術の基盤強化と社会実装を推進していきます。これらを通じて、高秘匿情報を将来にわたって安全に流通・保管・利活用できるデータ流通基盤の構築を目指します。

※1 公開鍵認証基盤

インターネット上で安全な通信を行うために「公開鍵暗号技術」と「電子証明書」を用いて、情報の暗号化、電子署名、本人認証を一元的に管理する仕組みです。

※2 ECDSA

公開鍵暗号方式ECCベースの電子署名アルゴリズム。同じく公開鍵暗号方式RSAと比較して約10分の1の鍵サイズでありながら同等の安全性を持つという特長があります。

※3 ML-DSA

量子コンピュータでも解くことが難しいとされる格子問題を応用した電子署名アルゴリズム「CRYSTALS-Dilithium」を基に、NISTがFIPS 204として標準化したPQCの電子署名アルゴリズムです。

※4 第2の暗号アジャイルルート認証局が発行する電子証明書

現行暗号とPQCの両方で署名されたハイブリッドルート証明書です。現行の暗号検証プロセスとの完全な後方互換性を保ちながら、並行してPQCによる証明書チェーンを構築することで、既存システムを止めないシームレスな移行を実現します。

※5 ML-KEM

量子コンピュータでも解くことが難しいとされる格子問題を応用した鍵交換アルゴリズム「CRYSTALS-Kyber」を基に、NISTがFIPS 203として標準化したPQCの鍵交換アルゴリズムです。

※6「PQC CARD®」

PQCを搭載したICカード。

https://www.holdings.toppan.com/ja/news/2022/10/newsrelease221024_1.html

＊ 本ニュースリリースに記載された商品・サービス名は各社の商標または登録商標です。

＊ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。

以　上

＜報道に関するお問い合わせ先＞
・TOPPANホールディングス株式会社　広報部
TEL: 03-3835-5636 / MAIL: kouhou@toppan.co.jp
・国立研究開発法人情報通信研究機構　広報部　報道室
MAIL：publicity@nict.go.jp
・ISARA Corporation
TEL: +1-877-319-8576 / MAIL: media@isara.com