News Release

TOPPAN

2026 年 8 月 3 日
TOPPAN 株式会社

TOPPAN、デュアルインターフェイス IC カードで世界初 耐量子計算機暗号を搭載した「PQC CARD® Dual」を開発

省メモリ技術により接触・非接触の両通信が可能な IC カードで PQC 対応を実現
行政・医療分野などに向けた次世代の安全・安心な認証インフラ構築に貢献

TOPPAN ホールディングスのグループ会社である TOPPAN 株式会社（本社：東京都文京区、代表取締役社長：野口 晴彦、以下 TOPPAN）は、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）を搭載した、接触・非接触のどちらの通信方式でも利用可能なデュアルインターフェイス IC カード「PQC CARD® Dual」を世界で初めて（※1）開発しました。高いセキュリティ性が要求される国民 ID カードや医療向け認証カードなどへの実装に向けて行政・医療分野へ 2027 年度からの提供を目指します。

「PQC CARD® Dual」は、独自の省メモリ技術により、PQC の膨大な暗号演算処理で使用するメモリ容量を最適化しました。これにより、従来の暗号方式よりも大きなデータサイズを必要とする PQC において、メモリ容量が限定されているデュアルインターフェイス IC チップ上での実装を可能にしました。また、搭載しているアルゴリズムは、米国政府機関の国立標準技術研究所（以下 NIST）により選定され長期的な安全性が確保された暗号技術に準拠しています。さらに、PQC と現行暗号の双方をサポートすることで、現行暗号から PQC へのスムーズな移行にも対応します。

TOPPAN は、今後も、量子コンピュータ時代を見据えた認証技術の実用化・高度化に向けた取り組みを推進し、安全・安心な次世代認証インフラの構築に貢献していきます。

デュアルインターフェイス IC カード「PQC CARD® Dual」と使用イメージ ©TOPPAN Inc.

■ 背景

インターネットを通じたサービスにおける暗号技術は、今後膨大な計算能力を持つ量子コンピュータの実用化によって解読されるリスクが指摘されており、PQC への移行が世界的に急務となっています。IC カードにおいても安全な認証技術の導入が検討されていますが、PQC は暗号鍵や電子署名のデータサイズが極めて大きく、演算処理も複雑なため、メモリや処理能力が限られた IC カードへの実装が困難であるという課

TOPPAN ホールディングス株式会社 広報本部
E-mail:kouhou@toppan.co.jp

題がありました。

特に、デュアルインターフェイス IC カードへの PQC 実装は、限られたメモリリソースの中で、接触・非接触の通信制御機能と、PQC が要求する膨大な演算処理を並行して実行させる必要があるため、高い技術的障壁がありました。タッチ式の利便性と、差し込み式の信頼性を両立するデュアルインターフェイス IC カードは、銀行・金融サービスや ID カードの普及などで急速な拡大を続けており、そのグローバル市場規模は、2032 年度に 2025 年度比で約 2.6 倍の 107 億ドルと推定されており(※2)、PQC 対応への潜在的なニーズが高まっています。

これらの背景のもと、TOPPAN は、IC カードの開発で培ってきた省メモリ技術とこれまで取り組んできた量子および耐量子計算機暗号における研究開発の知見を基に「PQC CARD® Dual」を開発。世界で初めて PQC 対応のデュアルインターフェイス IC カードを実現しました。

■ 本製品の特長

・世界初、接触・非接触の両通信に対応した PQC 実装 IC カード

PQC を接触・非接触のどちらの通信方式にも対応するデュアルインターフェイス IC カードに実装しました。NIST にて標準化された PQC アルゴリズム(ML-KEM、ML-DSA (※3))と、従来の暗号技術(RSA、ECC(※4)など)を搭載しており、1 枚のカードで両方の暗号方式に対応が可能です。そのため、現行暗号から PQC への移行期においても、既存のインフラ環境を活かしながら、スムーズに PQC 環境への移行を実現します。なお、接触・非接触単体での PQC 対応も可能です。

・独自の省メモリ技術により PQC の高速処理を実現

PQC の実装には膨大な作業用メモリが必要であり、また IC カードのプラットフォームとして主流となっている汎用 OS は占有するメモリ容量が大きい、という課題がありました。TOPPAN は、長年 IC カードの開発で培ってきた省メモリ技術により、限られたメモリ領域を圧迫することなく、PQC が要求する膨大な演算処理をスムーズに実行させることに成功しました。

・世界標準の汎用 OS への実装による柔軟な運用支援

世界標準の IC カードプラットフォームであり、既存の IC カードに多く導入されている汎用 OS「Java Card」上で PQC 機能を実現しました。そのため既存の IC カードに実装されている決済や社員証、アクセス管理などのアプリケーションはそのままに、暗号機能だけを PQC へアップデートするなどの運用も可能です。

■ 今後の目標

TOPPAN は、「PQC CARD® Dual」と関連システムに関して、2026 年度中に高いセキュリティ性が要求される行政・医療分野などを対象とした実証実験の実施を目指します。有用性の検証を経て、米国や欧州などの各国がターゲットとする 2030 年代の本格的な PQC 移行ロードマップを見据え、 2027 年度からの「PQC CARD® Dual」の提供開始を目指します。今後も、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、認証技術の実用化・高度化に向けた取り組みを推進していきます。

※1 接触・非接触通信の両方のインターフェイスに PQC 対応した IC カードとして(2026 年 7 月時点、TOPPAN 調べ)

※2 出典:Global Dual Interface Smart Card Market 2026(H&I グローバルリサーチ)を参考
https://www.globalresearch.co.jp/industry-data1/global-dual-interface-smart-card-market-report-gr-c029568

※3
ML-KEM:FIPS203 として、NIST によって標準化された PQC 標準の鍵カプセル化(鍵交換)アルゴリズム
ML-DSA:FIPS204 として、NIST によって標準化された PQC 標準の電子署名アルゴリズム

TOPPANホールディングス株式会社 広報本部
E-mail:kouhou@toppan.co.jp

※4

RSA：1977 年に開発された、巨大な素因数分解の困難性を安全性の根拠とした、世界初の本格的な公開鍵暗号および電子署名アルゴリズム

ECC(Elliptic Curve Cryptography)：「楕円曲線上の離散対数問題」の数学的困難性を安全性の根拠とする公開鍵暗号方式

＊ Java は、Oracle、その子会社及び関連会社の米国及びその他の国における登録商標です。

＊ 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

TOPPANホールディングス株式会社　広報本部
E-mail:kouhou@toppan.co.jp