報道発表資料

2024 年 10 月 7 日
TOPPAN デジタル株式会社
国立研究開発法人情報通信研究機構
ISARA Corporation

TOPPAN デジタル・NICT・ISARA、耐量子計算機暗号と現行暗号のハイブリッド対応が可能な IC カードシステムを開発

安全・安心な社会インフラ実現に向けて、耐量子計算機暗号への円滑な移行を可能に

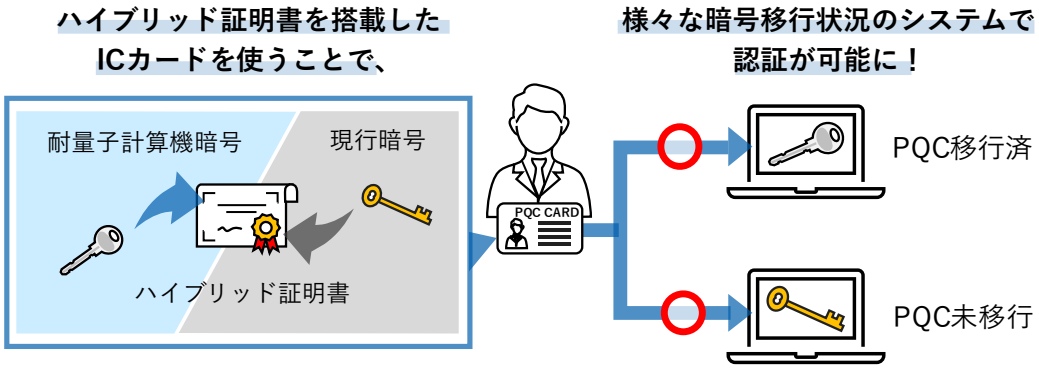
TOPPAN ホールディングスのグループ会社である TOPPAN デジタル株式会社（本社：東京都文京区、代表取締役社長：坂井 和則、以下 TOPPAN デジタル）、国立研究開発法人情報通信研究機構（理事長：徳田 英幸、以下 NICT（エヌアイシーティー））、ISARA Corporation（本社：カナダ・オンタリオ州、CEO：アツシ・ヤマダ、以下 ISARA）は、量子コンピュータでも解読が困難とされる耐量子計算機暗号（Post-Quantum Cryptography 以下 PQC）と現行の暗号の双方に対応可能な IC カードシステム「SecureBridge™（セキュアブリッジ）」を開発しました。

3 者は PQC の IC カードへの実装に関し 2021 年 4 月から連携して研究を進めており、今回、2022 年 10 月に開発した「PQC CARD®」（※1）およびプライベート認証局（※2）を、PQC と現行暗号による認証を両方可能とする電子証明書（以下 ハイブリッド証明書）に対応するようアップデートしました。

また、本システムを NICT が運用する量子暗号ネットワークテストベッド上に実装された「保健医療用の長期セキュアデータ保管・交換システム（Healthcare Long-term Integrity and Confidentiality Protection System、以下 H-LINCOS）」（※3）のユーザ認証に適用し、その有効性を確認しました。

今後 3 者はこの技術も活用し、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、量子セキュアクラウド技術の実用化・高度化に向けた取り組みを推進していきます。

なお、本検証の一部は、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。



ハイブリッド対応可能な PQC CARD®の利用イメージ図

©TOPPAN Digital Inc.

■ 背景

オンライン診療や電子商取引などのインターネットを通じたサービスは、暗号技術によって安全に守られています。しかし、将来的に量子コンピュータによって、現在普及している暗号技術が破られる恐れがあります。そのため、特に医療・金融・行政など重要な情報を扱うシステムにおいて、量子コンピュータで

も解読が困難とされる PQC への早急な移行が求められています。2024 年 8 月には米国政府機関の国立標準技術研究所(以下 NIST)によって、事実上の世界標準である PQC アルゴリズムが発表され、今後さらに移行の流れは加速していくと考えられます。

しかし、近年の情報システムは肥大化・複雑化が進んでおり、完全な PQC への移行期間は長期に渡ると想定されています。移行できたシステムと移行できていないシステムが混在した場合、アクセスする側とされた側で同じ暗号技術を使えないため、認証や暗号通信が困難になります。

そこでこの度、TOPPAN デジタル、NICT、ISARA は PQC と現行暗号の双方にハイブリッド対応した IC カードシステム「SecureBridge™」を開発しました。また、それらシステムを H-LINCOS と組み合わせ、動作検証を実施しました。今後は安全・安心な社会インフラの実現に向けて、PQC への円滑な移行を可能にします。

■ ハイブリッド対応可能な IC カードシステム「SecureBridge™」の特長

・PQC および現行暗号の両方に対応

NIST が 2024 年 8 月に発表した、事実上の世界標準である PQC 署名アルゴリズム「ML-DSA」(※4)、および現行の暗号標準で使用されている署名アルゴリズムである「ECDSA」(※5)の両方に対応可能。これにより、様々な移行状況のシステムに対して認証を行うことができます。

・長期の移行期間を支え、安全かつ円滑な移行を実現可能

重要な情報を扱うシステムは、複雑で大規模な場合が多いため、PQC への移行期間は長期に渡ると想定されます。ハイブリッド証明書は移行期間における様々なシステムの状況に対応可能なため、長期の移行期間を安全に保つことができ、円滑な移行をサポートできます。

■ 実証実験の概要

実施目的:ハイブリッド対応可能な IC カードシステム「SecureBridge™」を用いて、ユーザ認証などの基本動作確認と技術的課題の抽出

実施期間:2024 年 4 月から 9 月まで

実施内容:NICT が運用する H-LINCOS において、医療従事者が持つ資格証明書である HPKI カード(保健医療用公開鍵認証カード)にみたてた、現行暗号のみに対応した IC カードと、ハイブリッド対応可能な IC カードを用いて、いずれの場合も正しく本人認証が行われ、電子カルテシステムを閲覧できることを確認しました。

成果:ハイブリッド対応しているサーバに対して、IC カードが現行暗号のみに対応している場合、あるいはハイブリッド対応している場合、いずれにおいても正しくユーザ認証できることが確認できました。これにより、ハイブリッド証明書を用いれば、様々な移行状況のシステムにおいても認証ができることが検証できました。これは長期に渡るPQCへの移行期間を安全かつスムーズにすることに貢献可能であると言える結果です。

■ 3 者の役割

TOPPAN デジタル:ISARA との連携を通じた「PQC CARD®」含めた IC カードシステムのハイブリッド証明書対応開発、およびそれらの H-LINCOS との連携

NICT:本開発の全体構成、保健医療応用を目指した長期セキュアデータ保管・交換システム「H-LINCOS」の提供

ISARA:TOPPAN デジタルとの連携を通じたプライベート認証局のハイブリッド証明書発行機能の開発、IC カード用「ML-DSA」ファームウェア(※6)の開発

■ 今後の目標

TOPPAN デジタルは、ハイブリッド証明書に対応した IC カードシステム「SecureBridge™」に関し、2025 年に高いセキュリティ性が要求される医療・金融業界などで限定的な実用化を行い、2030 年の本格的な提供開始を目指します。

また、TOPPAN デジタル、NICT、ISARA は、この技術を活用し、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、量子セキュアクラウド技術の実用化・高度化に向けた取り組みを推進していきます。医療・金融・行政などにおける個人情報の保護や管理をはじめ、IC カードのセキュリティにとどまらず広範囲なインターネットを通じたサービスへの PQC の適用・拡大を目指し、活用事例の開拓や実証を推進していきます。

※1「PQC CARD®」

PQC を搭載した IC カード。

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

※2 プライベート認証局

プライベート認証局とは、社内ネットワークなど限られた範囲で運用され、サーバの正当性を保証する電子証明書を発行する機能を持つシステム。

※3 H-LINCOS

保健医療用の長期セキュアデータ保管・交換システム H-LINCOS（Healthcare long-term integrity and confidentiality protection system）は、秘密分散と量子暗号など秘匿通信、および公開鍵認証基盤の技術により、電子カルテデータのセキュアかつ可用性の高いバックアップや、医療機関間での相互利用などを行う保健医療用の長期セキュアデータ保管・交換システムです。

参考：2019 年 12 月 12 日 NICT プレスリリース https://www.nict.go.jp/press/2019/12/12-1.html

※4 ML-DSA

NIST によって 2024 年 8 月に連邦情報処理標準（Federal Information Processing Standards：FIPS）として決定された次世代暗号アルゴリズム。格子暗号を使う電子署名アルゴリズム「CRYSTALS-Dilithium」から派生しました。

※5 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。

※6 ファームウェア

ハードウェアの制御のため、機器に組み込まれたソフトウェアのこと。

＊ 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