報道発表資料

2022 年 10 月 24 日
凸版印刷株式会社
国立研究開発法人情報通信研究機構

凸版印刷と NICT、世界初、米国政府機関選定の耐量子計算機暗号を IC カードシステムに実装する技術を確立

保健医療用の長期セキュアデータ保管・交換システムで有効性を確認

凸版印刷株式会社（本社：東京都文京区、代表取締役社長：麿　秀晴、以下　凸版印刷）と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））は、量子コンピュータでも解読が困難な耐量子計算機暗号（Post-quantum　cryptography　以下 PQC）（※1）を搭載した IC カード「PQC　CARD®」を世界で初めて開発し、NICT　が運用するテストベッド「保健医療用の長期セキュアデータ保管・交換システム」における医療従事者の IC カード認証と電子カルテデータへのアクセス制御に適用し、その有効性の検証に成功しました。

今回開発した「PQC　CARD®」には、米国政府機関の国立標準技術研究所（以下　NIST）（※2）が　2022 年 7 月に標準技術候補として選定した次世代の電子署名方式「CRYSTALS-Dilithium（クリスタル・ダイリチアム）」（※3）を採用しました。「PQC　CARD®」の開発では、PQC　に関する先端技術を有する　ISARA Corporation（本社：カナダ・オンタリオ州、CEO：アツシ・ヤマダ、以下　ISARA）とも連携しています。

凸版印刷と　NICT　は、今後この技術を活用し、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（※4）の開発を推進してまいります。また、量子コンピューティング時代において、IC　カードのセキュリティにとどまらず、インターネット上で日常的に行われる電子メールや、オンラインショッピング、キャッシュレス決済、ネットバンキングなどインターネットのセキュリティを担保する基盤技術を構築し、安全・安心な社会インフラの実現を目指します。

なお、本研究の一部は、内閣府 SIP『光・量子を活用した Society　5.0 実現化技術』及び総務省『グローバル量子暗号通信網構築のための研究開発(JPJ008957)　』の支援を受けて実施されました。

「PQC CARD®」

.

■ 開発の背景

電子メールや、オンラインショッピング、キャッシュレス決済、各種電子申請など、情報社会におけるインターネットサービスは、公開鍵暗号（※5）に基づく電子署名や認証と鍵交換、及び共通鍵暗号（※6）によるデータの暗号化などによって安全に守られています。

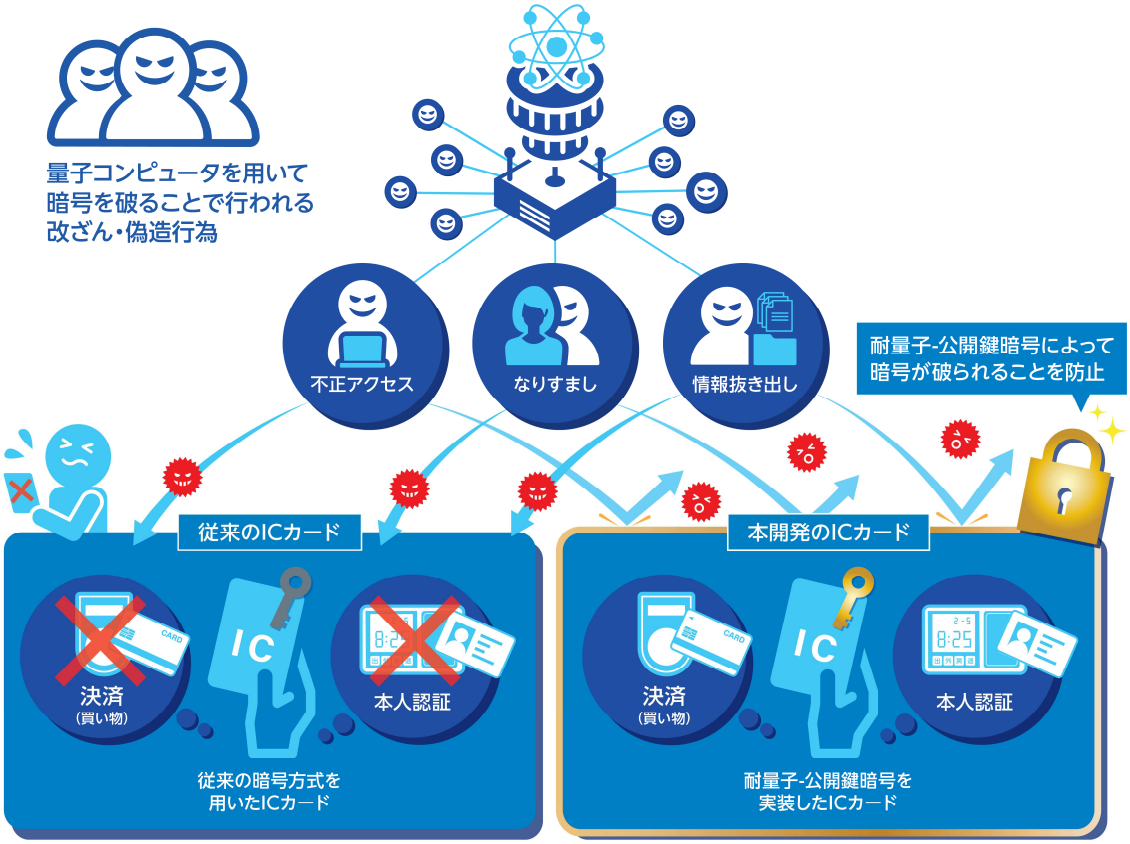
しかし、研究開発が急速に進展している量子コンピュータによって、現在普及している暗号技術が破られる恐れがあります。そこで、量子コンピュータが実用化されても解読が困難とされる耐量子計算機暗号への移行準備が始まっています。その移行は、かつてない規模で 2025 年頃から本格化すると予想されます。

NIST では耐量子計算機暗号の標準化を進めており、2022 年 7 月にその候補となる技術の選定結果を公表しました。選定された暗号方式は事実上の世界標準になり、今後世界中で置き換えが進められていくと考えられています。米国ではすでに 2022 年 5 月、大統領令（※7）が発布され、量子コンピュータがサイバーセキュリティにもたらすリスクに対処するため、強固な新暗号技術の確立と普及への動きが始まっています。

新しい暗号方式への移行は、完全に置き換わるまでに 10 年規模の時間を要すると予想されることから、量子コンピュータの実用化のスピードに間に合わせるべく、早急な取り組みが必要になります。

このような課題に対し、凸版印刷と NICT は、ISARA 社と連携し、NIST が選定した PQC の一つである「CRYSTALS-Dilithium」を搭載した IC カード「PQC CARD®」を世界に先駆けて開発し、NICT が運用するテストベッド「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）」（※8）における医療従事者の IC カード認証と電子カルテデータへのアクセス制御に適用し、その有効性の検証に成功しました。

本成果により、PQC を IC カードシステムに実装する技術が確立されるとともに、PQC の普及が進み、量子コンピューティング時代へ向けた暗号インフラのスムーズな移行に繋がると期待されます。凸版印刷と NICT は今後も連携しながら、PQC の早期の普及を図り、世界の安全・安心な情報流通基盤の構築及び維持に貢献します。



従来の IC カードと「PQC CARD®」の違い

■ 「PQC CARD®」の特長

(1) 世界で初めて、NIST 選定 PQC「CRYSTALS-Dilithium」を IC カードに実装

PQC は量子コンピュータを用いても極めて解読が困難であるとされる暗号技術であり、NIST は 2017 年より標準化選考を進めていましたが、2022 年 7 月に「CRYSTALS-Dilithium」を含む複数方式を選定。今後、規格化が進められていき、事実上の世界標準になると見られています。

(2) 利用者側での変更はなく、従来の利便性を保持

「PQC CARD®」のリーダライタや通信プロトコルなどは、現行暗号方式を実装した既存 IC カード利用時から変更することなく使用でき、ハードウェアを更新する必要はありません。また、認証スピードなどのパフォーマンスも良好で、従来同様に利用可能です。

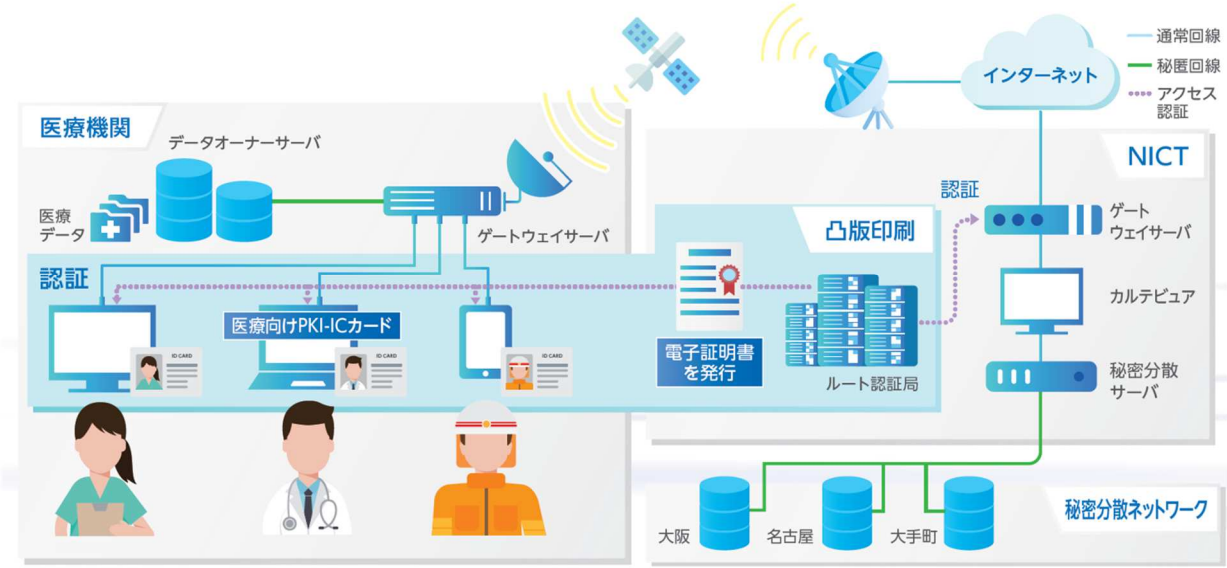
■ 実証実験の概要

実施目的:「PQC CARD®」を用いて、H-LINCOS における医療従事者の認証、アクセス制御などの基本動作確認と技術的課題の抽出

実施期間:2022 年 8 月から 10 月まで

実施内容:「PQC CARD®」を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、IC カード認証と顔による生体認証を組み合わせることで、電子カルテを閲覧する際の多要素認証を実施しました。また、電子カルテを閲覧するブラウザとサーバ間の通信に用いる PQC をアップデートし、動作検証を実施。H-LINCOS 全体の耐量子性の向上とその有効性の検証を行いました。

成果:正しい権限をもった者のみが、その権限に応じた電子カルテ情報にアクセスできることを確認。また、「PQC CARD®」を用いることで、H-LINCOS 全体の耐量子性の向上とその有効性、実導入に対する課題を確認することができました。



「PQC CARD®」を用いた H-LINCOS でのアクセス制御の構成図

■ 今後の目標

凸版印刷は、「PQC CARD®」と関連システムに関し、2025 年には医療や金融などの用途で限定的な実用化を行い、2030 年に本格的な提供開始を目指します。

また、凸版印刷と NICT 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に向けた取り組みを推進していきます。IC カードのセキュリティにとどまらず、インターネットのセキュリティを担保する基盤技術として、電子メールや、オンラインショッピング、キャッシュレス決済、ネットバンキング、また、現行暗号方式で技術確立が進む IoT 関連システムやコネクテッドカーなどへの PQC の適用・拡大を目指します。

※1 耐量子計算機暗号
NIST が選定した耐量子計算機暗号（Post-quantum cryptography）には、公開鍵暗号と電子署名の各々において、複数の暗号方式が含まれています。凸版印刷と NICT ではこれまで両者を含めて公開鍵暗号と表記してきましたが、NIST の表記にならい、耐量子計算機暗号と表記を改めます。

※2 国立標準技術研究所（National Institute of Standards and Technology）
米国国内の技術や工業などに関する規格標準化に当たる連邦政府機関

※3 CRYSTALS-Dilithium
耐量子計算機暗号で用いる NIST が選定した電子署名の一つで、格子ベースの公開鍵暗号方式。

※4 量子セキュアクラウド技術
量子暗号や秘密分散、耐量子計算機暗号を融合した次世代暗号基盤と、量子コンピュータや最新の半導体コンピュータを融合した次世代コンピューティングから構成され、重要情報の安全な流通/保管/利活用を可能とするクラウド技術
参考：NICT 量子ネットワークホワイトペーパー https://www.nict.go.jp/press/2021/04/01-3.html

※5 公開鍵暗号
情報の暗号化と復号において、異なる 2 つのペアとなる鍵を用いる暗号方式。

※6 共通鍵暗号
情報の暗号化と復号において、共通の鍵を用いる暗号方式。

※7 米国大統領令（2022 年 5 月 4 日）
「National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems」
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

※8 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、及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

＊「PQC CARD」は凸版印刷株式会社の登録商標です。
＊ 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。

＜問い合わせ先＞
凸版印刷株式会社 広報本部
E-Mail： kouhou@toppan.co.jp

国立研究開発法人情報通信研究機構
量子 ICT 協創センター 佐々木雅英
E-Mail： psasaki@nict.go.jp

国立研究開発法人情報通信研究機構
未来 ICT 研究所 小金井フロンティア研究センター 量子 ICT 研究室 藤原幹生
E-Mail: fujiwara@nict.go.jp

＜報道機関からの問い合わせ先＞
凸版印刷株式会社 広報本部
E-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
E-Mail: publicity@nict.go.jp