報道発表資料

2023 年 3 月 14 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、耐量子計算機暗号に対応した プライベート認証局を構築

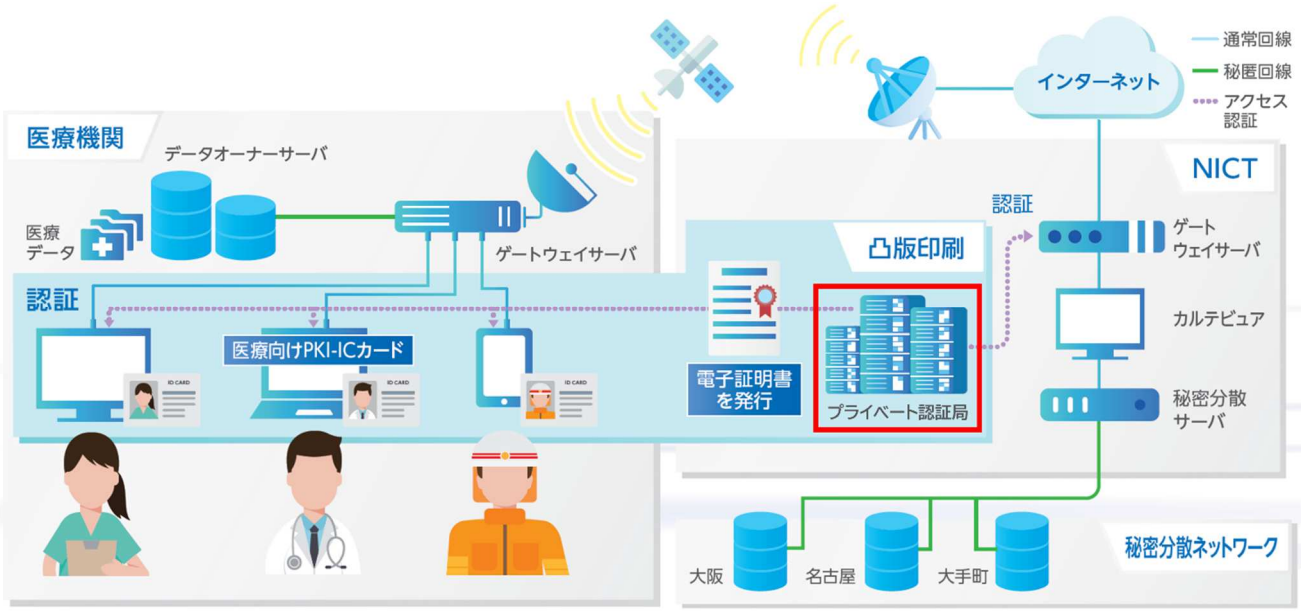
保健医療用の長期セキュアデータ保管・交換システムで有効性を確認 インターネットのセキュリティを担保し、安全・安心な社会インフラ実現を目指す

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とされる耐量子計算機暗号（Post-Quantum Cryptography　以下 PQC）（※1）に関し、連携して研究を進めています。

このたび、凸版印刷と NICT は、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 H-LINCOS（Healthcare Long-Term Integrity and Confidentiality Protection System）」（※2）において、PQC 対応のプライベート認証局（※3）を構築し、電子署名・電子証明書発行機能の追加と凸版印刷と NICT が開発した「PQC　CARD®」との連携を通した改ざん検知機能を実装し、その有効性の検証に成功しました。

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）の社会実装を推進していきます。また、量子コンピューティング時代において、インターネット上で日常的に行われる電子メールや　SNS、オンラインショッピング、IoT　関連システム、コネクテッドカー（※5）などのサイバー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 プログラム「光・量子を活用した Society　5.0　実現化技術」（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）によって実施されました。



H-LINCOS でのアクセス制御の構成図（赤枠が今回、構築したプライベート認証局）

■ 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、インターネットを介したサービスでは、信頼された第三者機関である認証局によって、安全にデータ通信を行うことができています。認証局とは、電子証明書を発行したり、電子証明書の有効期限を確認・検証したりする安全性が担保された独立機関です。また認証局は、電子署名の正当性を公に対して示すパブリック認証局と、社内などの閉じられた領域内に示すプライベート認証局の二つに分類でき、どちらもインターネット上で通信相手を信頼するために利用者から求められる機能は同じです。

現在、認証局は公開鍵暗号方式(※6)に基づいて電子署名や認証をすることで、通信相手のなりすましやデータの改ざんなどのリスクを防ぎ安全なデータ通信を可能としています。しかし、2030 年頃に実用化が期待されている量子コンピュータにより、現在の公開鍵暗号は破られる恐れがあり、量子コンピュータを用いても破ることが困難とされる PQC を用いたセキュリティの強化が課題となっています。また、PQC を用いてデータ通信を行ったとしても、通信相手が正しく保証されていなければ、安全なデータ通信は行えません。そのため、今後は PQC の実用化に向けて、認証局の早期実現が求められています。

凸版印刷と NICT はこれらの課題に対し、ISARA Corporation(本社:カナダ・オンタリオ州、CEO:アツシ・ヤマダ、以下 ISARA)がもつ PQC に関する先端技術を活用することで、PQC に対応したプライベート認証局を構築し、H-LINCOS でのより実際の運用場面に即した安全な IC カード認証と電子カルテデータへのアクセス制御が可能となりました。

■ 2 者の役割

・凸版印刷

ISARA との連携を通じた PQC 対応プライベート認証局の H-LINCOS への実装、「PQC CARD®」と PQC 対応プライベート認証局のシステム間連携・開発

・NICT

本開発の全体構成、詳細仕様の策定、テストベッドである「H-LINCOS」環境の提供

■ PQC 対応プライベート認証局の特長

(1)H-LINCOS において、「CRYSTALS-Dilithium」に対応した PQC 電子証明書の発行を実現

H-LINCOS において、「PQC CARD®」を用いた電子カルテデータへのアクセス制御をする際、「PQC CARD®」に格納された電子証明書を検証することで、正しい権限を持った本人であるかを確認しています。今回、その電子証明書を PQC 対応のプライベート認証局が CRYSTALS-Dilithium(クリスタルダイリチアム)(※7)と呼ばれる PQC の電子署名アルゴリズムを用いて発行するという機能を構築しました。

(2)H-LINCOS を実運用に即した環境にアップデート

PQC 対応のプライベート認証局で電子証明書を発行し、その電子証明書を「PQC CARD®」に格納するという一連の機能を構築することで、H-LINCOS をより実際の運用場面に即したテストベッドへとアップデートしました。また、この「PQC CARD®」を用いて、H-LINCOS における IC カード認証と電子カルテデータへのアクセス制御を検証し、問題なく動作することを確認しました。

■ 今後の目標

凸版印刷と NICT は、プライベート認証局をはじめ関連する技術を活用し、2025 年に「量子セキュアクラウド技術」の限定的な実用化を、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、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、ヘルスケア・金融・行政などにおける個人情報管理をはじめ、電子メールや SNS、オンラインショッピング、IoT 関連システム、コネクテッドカーなど広範囲なサービスへの PQC の適用・拡大を目指します。

※1 耐量子計算機暗号
米国政府機関の国立標準技術研究所(以下 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 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

※3 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、サーバー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。

※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 コネクテッドカー
コネクテッドカーとは、ICT 端末としての機能を有する自動車のことであり、車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することで、新たな価値を生み出すことが期待されている。

※6 公開鍵暗号方式
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。

※7 CRYSTALS-Dilithium(クリスタルダイリチアム)
米国政府機関の国立標準技術研究所によって 2022 年 7 月に選定された次世代暗号アルゴリズム。電子署名の一つで、格子ベースの公開鍵暗号方式。

＜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 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