報道発表資料

2021 年 4 月 5 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

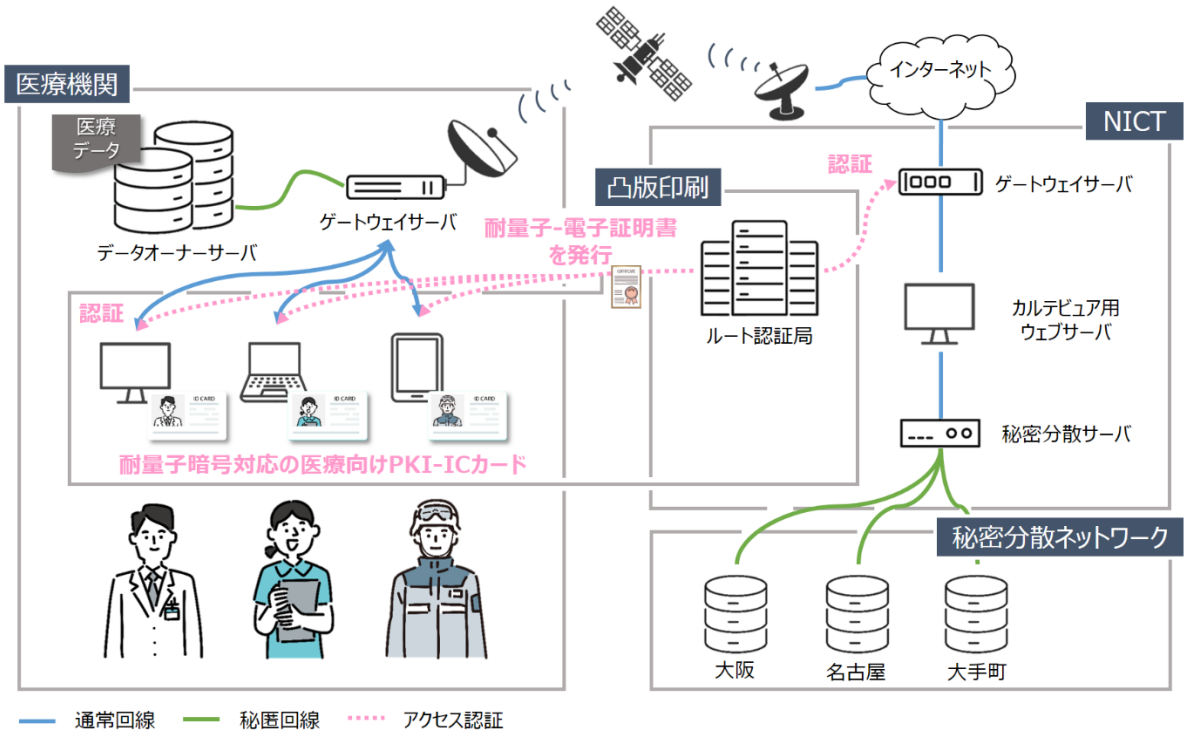
凸版印刷と NICT、耐量子−公開鍵暗号の技術確立に関する共同研究契約を締結

量子セキュアクラウド技術に耐量子−公開鍵暗号を組み込み
安全なデータ流通、保管、利活用を実現

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）は、量子セキュアクラウド技術への耐量子−公開鍵暗号の組み込みに関する共同研究契約を締結しました。

量子セキュアクラウド技術は量子暗号技術と秘密分散技術を融合し、データの安全な流通、保管、利活用を可能とするクラウド技術です。量子セキュアクラウド技術の確立により、改ざん・解読が不可能な高いセキュリティ性を担保するだけでなく、例えば、医療、新素材、製造、金融分野で蓄積された個人情報や企業情報など秘匿性の高いデータの収集、分析、処理、利用を可能とします。

本研究では、量子セキュアクラウド技術への、耐量子−公開鍵暗号を実装した IC カードを用いたアクセス制御・管理技術を開発することで、耐量子−公開鍵暗号の社会実装を推進し、量子セキュアクラウド技術の利用拡大を狙います。具体的には、耐量子−公開鍵暗号を実装した IC カードによるアクセス制御・管理技術を NICT 等が開発し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」（※1）へ適用し、保健医療分野における実用性を検証します。



本共同研究のイメージ図

■ 本研究の背景

量子コンピューティングが実現すると現在インターネットで使われている公開鍵暗号は解読されてしまいます。近年の量子コンピューティング技術の発展は目覚しく、量子コンピューティングが実現した時代においても、解読が難しいと期待される公開鍵暗号技術、いわゆる耐量子-公開鍵暗号の開発と標準化が世界各国で行われています。

NICT 等が開発した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」では、保健医療分野の 26 種の国家資格に基づく権限管理表と耐量子-公開鍵暗号に基づく高セキュアなユーザ認証の機能が実装されており、これらを用いてアクセス制御が行われます。しかし、現在の「H-LINCOS」の実装形態では、医療従事者が医療端末に ID 番号とパスワードを入力する必要があり、その情報をもとに医療端末が本人認証し、格納された耐量子-電子証明書を参照して、アクセス制御を行っています。今後は、医療従事者が端末に触ることなく簡便かつセキュアに必要な情報を閲覧できるようなアクセス制御・管理が求められています。例えば、非接触型の生体認証や自分の ID カードをリーダーにかざす操作等の組み合わせによる負担の少ないアクセス制御・管理が望まれます。

■ 本研究の概要

凸版印刷と NICT はこれらの課題に対し、これまで培ってきた IC カードのセキュリティ技術や認証技術を用いて、電子情報を安全・安心に運用するための耐量子-公開鍵暗号の実装および認証システムの開発を進めてまいります。

本共同研究では、量子鍵配送や耐量子-公開鍵暗号といった量子暗号技術を実装した量子セキュアクラウド技術を国際標準化していくことで、量子セキュアクラウド技術の開発を優位に進めることが可能となり、ビジネスの有利な展開が期待できます。

これにより、高秘匿情報を将来にわたって安全に流通、保管、利活用できる社会を実現できると期待されます。

■ 2 者の役割

・凸版印刷

凸版印刷は IC カードの開発や製造事業を通し、暗号技術、認証技術および不正アクセス防止技術など、IC カードのセキュリティ技術を培ってきました。このような知見を活かし、凸版印刷は IC カードへの耐量子-公開鍵暗号の適用および量子セキュアクラウド技術の利用拡大に向けた導入支援、秘匿性の高い情報の安全なバックアップやデータ流通サービス、ソリューションの提供など、量子コンピューティング時代における安全・安心な社会の実現に向けて取り組んでいきます。

具体的には、NICT らが開発した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」にて、耐量子-公開鍵暗号を実装した IC カードによる量子セキュアクラウド技術へのアクセス認証の技術検証を行います。

・NICT

内閣府が主導する戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society 5.0 実現化技術」の一環として、東京 QKD ネットワーク（※2）などを活用し、量子セキュアクラウド技術の研究を行っています。これまでに量子暗号、秘密分散および次世代の耐量子-公開鍵認証基盤を搭載した、保健医療用の長期セキュアデータ保管・交換システムを開発しています。このような知見と経験を活かし、「H-LINCOS」やさらに高度な計算エンジンを搭載した量子セキュアクラウド技術の確立に取り組んでいきます。また、これらの国際標準化を目指して取り組んでいきます。

凸版印刷と NICT は量子セキュアクラウド技術の確立に向けて、これまでに培った各々の技術・知見・経験を融合し、連携していきます。

■ 具体的な共同研究内容

(1)耐量子-公開鍵暗号の IC カードへの適用と認証システムの技術検証

「H-LINCOS」における耐量子-公開鍵暗号を実装した IC カードの適用と認証システムの技術検証を行います。

(2)耐量子-公開鍵暗号のアップグレード

量子セキュアクラウド技術に組み込まれている耐量子-公開鍵暗号を、米国にて標準化が進む最新のバージョンにアップグレードし、高秘匿情報の安全なデータの流通、保管、利活用の技術検証を行います。

■ 今後の目標

凸版印刷と NICT の 2 者は、量子セキュアクラウド技術の開発を推進し、2022 年に耐量子-公開鍵暗号の IC カードへの適用および認証システムの技術検証を開始します。2025 年に限定的な実用化を、2030 年にサービス化を目指します。

■ 第 1 回 量子コンピューティング EXPO【春】

凸版印刷は 2021 年 4 月 7 日(水)から 9 日(金)に開催される「第 1 回量子コンピューティング EXPO【春】」(会場:東京ビッグサイト)に出展します。凸版印刷ブース(6-12)では本共同研究に関する内容をはじめ、量子コンピューティングに対する凸版印刷の取り組みを紹介します。

※1 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)
秘密分散と秘匿通信の技術により、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、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
参考:NICT プレスリリース 2019 年 12 月 12 日 https://www.nict.go.jp/press/2019/12/12-1.html

※2 東京 QKD ネットワーク
NICT が 2010 年に東京圏に構築した量子鍵配送(QKD)ネットワークのテストベッド。NEC、東芝、NTT、学習院大学等の産学機関で開発された。QKD 装置が導入され、装置改良の研究開発、長期信頼性試験、相互接続やネットワーク運用試験、さらには QKD 技術と現代セキュリティ技術を融合した新しいセキュリティアプリケーションの研究開発などが行われている。

以　上

■ 本件に関する報道からのお問い合わせ先

凸版印刷株式会社　広報部
TEL:03-3835-5636　E-mail:kouhou@toppan.co.jp

国立研究開発法人情報通信研究機構(NICT)
広報部 報道室 E-mail: publicity@nict.go.jp