報道発表資料

2020 年 10 月 19 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
株式会社 QunaSys
ISARA Corporation

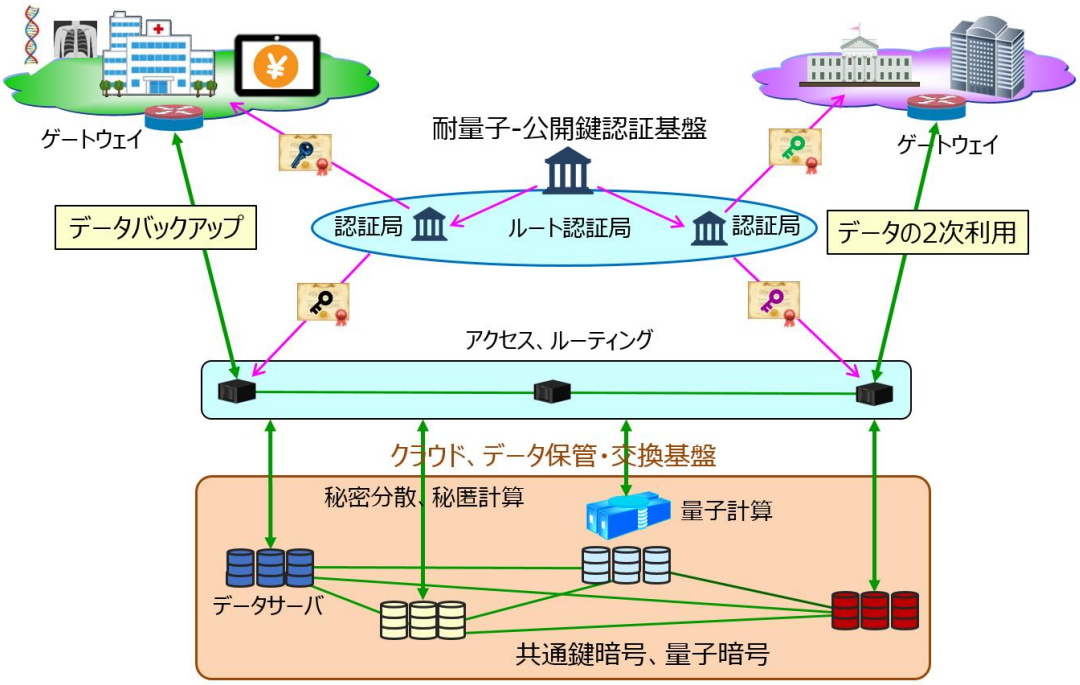
凸版印刷、NICT、QunaSys、ISARA の 4 者が連携 量子セキュアクラウド技術の確立に向けて始動

量子コンピューティング技術と量子暗号技術で安全なデータ流通/保管/利活用を実現

凸版印刷株式会社（本社：東京都千代田区、代表取締役社長：鷹 秀晴、以下 凸版印刷）、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）、株式会社 QunaSys（本社：東京都文京区、代表：楊 天任、以下 QunaSys）及び ISARA Corporation（本社：オンタリオ州・カナダ、CEO：Scott Totzke、以下 ISARA）は、高度な情報処理と安全なデータ流通/保管/利活用を可能とする量子セキュアクラウド技術の確立に向け 4 者連携を開始します。

量子コンピューティング技術とは、量子力学的な現象を持つ量子ビットを用いた計算処理技術であり、高い計算処理能力を有する次世代のコンピューティング技術として期待されています。

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。



量子セキュアクラウド技術の実装イメージ

■ 本連携の背景

近年、企業にとって、自然災害、大火災、テロ攻撃などの緊急事態時に、オフィスや工場、データセンターなどの経営資源の損害を最小限にとどめ、中核となる事業の継続あるいは早期復旧を可能とすることは、重要課題になっています。また、昨今のデジタルシフトを受け、企業の重要な経営資源の一つである大容量の情報を安全に保管し、必要に応じて完全に復元することは欠くことのできない課題です。しかし、予測不可能な自然・人為災害に対して、将来にわたって高いレジリエンス(※1)を保つことは技術的に限界があるため、情報を分散して安全に保管し、完全に復元できる超長期のセキュリティ性の高いクラウド技術が求められています。

一方、現在普及している暗号技術によって、現状の通信は安全に行うことができています。しかし、2030 年に実用化が期待されている量子コンピューティング技術により、電子決済や各種個人情報の電子申請など高秘匿情報通信に用いられる暗号が解読される恐れがあり、セキュリティの強化が社会課題となっていくことから、今後は決して破られない暗号技術が求められます。

■ 4 者の役割

- 凸版印刷

IC カードの開発や製造事業を通し、暗号技術、認証技術及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(※2)の適用及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。

- 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 Society5.0 実現化技術」の一環として、東京 QKD ネットワーク(※3)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、秘密分散及び次世代の耐量子-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(Healthcare long-term integrity and confidentiality protection system、以下 H-LINCOS)(※4)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とその国際標準化を目指して取り組んでいきます。

- QunaSys

量子コンピューター向けアルゴリズム及び量子コンピューターを活用した量子化学計算ソフトウェア「QunaSys Qamuy™」の開発を通し、量子コンピューティング技術を培ってきました。このような知見と経験を活かし、QunaSys は量子セキュアクラウド技術を活用した材料開発のサービス提供を推進していきます。また、ユーザ視点で量子セキュアクラウド技術の構築に貢献していきます。

- ISARA

ISARA は、長年にわたるサイバーセキュリティ技術の蓄積をもとに、現在のコンピューティングエコシステムを量子の時代まで守り続ける、アジャイルな暗号技術と耐量子セキュリティソリューション事業の世界的リーダーです。また、NICT と構築した「H-LINCOS」では、保健医療分野のための耐量子-公開鍵認証方式の開発を行いました。これらの暗号実装技術と公開鍵認証技術をアジャイル方式で開発してきたノウハウを活かし、量子セキュアクラウド技術の国際標準化に準拠する耐量子セキュリティソリューション開発を目指します。

凸版印刷、NICT、QunaSys 及び ISARA 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。

■ 具体的な連携内容

(1)量子セキュアクラウド技術の確立

システム設計や仕様検討、最新の量子暗号技術の実装、秘密分散技術を利用したバックアップやデータ保管の実装、耐量子-公開鍵暗号によるデジタル署名の開発などにより、データ保管/交換基盤及び耐量子-公開鍵認証基盤となる量子セキュアクラウド技術を確立します。

(2)量子セキュアクラウド技術の国際標準化の推進

NICT は戦略的イノベーション創造プログラム(SIP)において、量子 ICT フォーラム/量子鍵配送技術推進委員会や ITU-T(国際電気通信連合/電気通信標準化部門)、ISO/IEC(国際標準化機構/国際電気標準会議)や ETSI(欧州電気通信標準化機関)等の国際標準化組織へ、2022 年度までにネットワーク要件、ネットワークアーキテクチャ、ネットワークセキュリティ要件、及び鍵管理、量子暗号モジュールの評価・検定に関する提案を行い、国際標準化を推進していきます。凸版印刷は IC カードに関する知見を活かし、NICT をサポートしていきます。

■ 今後の目標

凸版印刷、NICT、QunaSys 及び ISARA の 4 者は連携して、量子セキュアクラウド技術の開発を推進し、2022 年度中に社会実装に向けたアプリケーションソフトウェアの実証実験を開始します。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。

■ 連携に関して

凸版印刷株式会社 DX デザイン事業部長　執行役員　柴谷浩毅のコメント

世界に先駆けた取り組みを行う各者と、Society5.0 の実現に向けた量子コンピューティングに関する研究開発ができることを誇りに思います。当社は長年、個人情報や機密性の高い情報を取り扱う事業、また認証・決済などのセキュリティ事業に携わってきました。近い将来、現在の暗号技術やセキュリティの危殆化が懸念されるなか、新しいセキュリティ技術を社会に実装していくことは、当社にとって大きな責務と捉えています。量子セキュアクラウド技術は、次世代量子暗号技術と秘密分散などセキュリティ技術を組み合わせた実用システムとして構想するものです。各者の知見を合わせて構想の実現を図り、量子コンピューティング時代の「安全・安心」に貢献していきたいと考えています。

国立研究開発法人情報通信研究機構　未来 ICT 研究所主管研究員
NICT フェロー　佐々木雅英のコメント

NICT は 20 年以上「量子暗号」の開発に取り組んでまいりました。国家レベルの機密通信や金融・医療機関などで使われつつありますが、まだ研究途上の技術であります。量子暗号の分野では中国が行う実験規模は他国を圧倒しており、日本はその点では遅れている状態です。そのため、この 4 者連携においても標準化へ向けて“メイド・イン・ジャパン”の品質保証基盤を構築し、日本が主導していきたいと考えます。また、Society5.0 においては、秘匿性の高い個人情報やビジネス価値の高い企業情報等が産み出され、企業やユーザがそれらを安心して保管、共有、利活用できるようになることは極めて重要です。この連携を通して量子セキュアクラウド技術を実現し、Society5.0 を支える基盤を構築することは、我が国の競争力強化に貢献できると確信しています。

株式会社 QunaSys　代表取締役　楊天任のコメント

Google による量子超越の実現をはじめ、近年量子コンピューターの実現に向けて多くのブレイクスルーが起き、実用が近づいております。しかし、新しい技術の発展・普及においては期待される点のみならず、懸念点も存在します。量子コンピューティングは、材料などの科学計算の高速化が期待される一方、現在使われている RSA 暗号は破られる可能性があります。QunaSys では、新材料という機密性の高いデータを扱っているため、秘匿性の高い情報を守れる量子暗号技術の必要性を感じており、今回構築を目

指す量子セキュアクラウド技術は、量子コンピューティング時代において、非常に重要なものになると考えております。量子セキュアクラウド技術を活用し、量子コンピューターの活用領域として期待される材料開発に関連するサービスの実現を目指していきます。

ISARA Corporation　Vice President, Research & Development　山田淳のコメント

量子コンピューティング時代が7～15年以内に到来し、既存暗号技術の危殆化が示唆されるため、量子コンピューティングでも解読できない耐量子暗号の標準化が進んでいます。大切なことは、耐量子暗号への移行には時間がかかることです。例えば、米軍での暗号近代化、中でも RSA から ECC への移行の取り組みは、20 年を経て未だ完了していません。脅威が顕在化してからでは遅く、今すぐにでも計画を策定し、取り組みを始めることが必要です。量子セキュアクラウド技術はそれら脅威に対抗できる技術であり、これを社会インフラとできるならば広い市場があると確信しています。ISARA の持つ耐量子暗号とアジャイル暗号技術による暗号移行に関する知見を活かして、量子コンピューティング時代のあるべき姿を模索し、社会変革に貢献していきます。

※1 レジリエンス

BCP では一般的に使用し、事業を継続・復旧する強靭性を意味する

※2　耐量子-公開鍵暗号

量子コンピューティング技術を利用しても解読できない公開鍵暗号技術

※3 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-NICT、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

※4 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

＊ 本ニュースリリースに記載された商品・サービス名は各者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