２０２１－８－２６
株式会社東芝
東北大学東北メディカル・メガバンク機構
東北大学病院
国立研究開発法人情報通信研究機構

量子暗号通信技術と秘密分散技術を活用しゲノム解析データの分散保管の実証に成功
～ゲノム研究・ゲノム医療分野における安全なデータ管理に貢献～

株式会社東芝（以下、東芝）、東北大学東北メディカル・メガバンク機構（以下、ToMMo）、東北大学病院、国立研究開発法人情報通信研究機構（以下、NICT）は、量子暗号通信技術と秘密分散技術を組み合わせたデータ分散保管技術を開発し、大規模ゲノム解析データ(*1)を複数拠点に分散して安全にバックアップ保管する実証実験に世界で初めて(*2)成功しました。本技術により、長期にわたり機密漏洩やデータ改ざんを防ぐバックアップデータ保管が可能となり、ゲノム研究・ゲノム医療分野における安全なデータ管理への貢献が期待できます。

本研究は、内閣府総合科学技術・イノベーション会議の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」（管理法人：量子科学技術研究開発機構）により実施されました。東芝、ToMMo・東北大学病院、および NICT は、本成果の技術と実証内容の詳細を、8 月 23 日～27 日に開催される国際会議 QCrypt 2021（11th International Conference on Quantum Cryptography）で発表します。

秘密情報や個人情報に対するセキュリティ保護の重要性が高まる中、医療分野でもサイバーセキュリティ対策の強化が進んでいます。中でも、ゲノム解析データは法律上個人を識別する個人情報として取り扱われることから、保管および伝送を行う際、厳重なセキュリティ保護により情報漏洩に備える必要があります。同時に、さらなる普及が見込まれるゲノム医療における活用のため、システムの障害、あるいは自然災害等によるデータの消失・棄損等に備えた、ゲノム解析データのバックアップも必要になります。これまで、大容量で機密性の高いゲノム解析データのバックアップは、情報漏洩リスクを考慮しネットワークを介したバックアップではなく、ディスク・テープ等のメディアに保存し、場合によっては遠隔拠点に保管することが行われていました。しかし、メディアの安全な輸送や保管には、コストや時間がかかるため、大容量で機密性の高いデータのバックアップ手法の確立、バックアップのコスト削減・利便性/可用性の確保が課題でした。

今回、量子力学の原理に基づきあらゆる盗聴や解読に対して安全な暗号通信を実現する「量子暗号通信技術」と、原本データを無意味化された複数のデータ片（シェア）に変換す

ることで安全なデータ保管を実現する「秘密分散技術」を組み合わせた「分散保管技術」を開発し、大容量ゲノム解析データのバックアップへの適用を実証しました。開発したデータ分散保管技術は、データの通信および保管の双方にて、情報理論的安全性(*3)を担保することができます。量子暗号通信技術により、あらゆる盗聴・解読に対して安全な通信を実現すると同時に、秘密分散技術により、システム障害や自然災害等で保管データの一部が棄損あるいは漏洩しても、元データの機密性は確保され、かつ、棄損せずに残った保管データから元のデータを復元することが可能です。

ゲノム解析データの保管の際は、(1)「XOR 閾値秘密分散法」と呼ぶ高速秘密分散を可能とするアルゴリズムにより、元のゲノム解析データに対応した複数のシェア（無意味化されたデータ）に分散し、(2)量子鍵配送によって生成・蓄積した暗号鍵を用いたワンタイムパッド暗号通信(*4)によって、各シェアを異なる拠点に分散保管します。また、ゲノム解析データを復元する際は、(1) 同様のワンタイムパッド暗号通信によって各シェアを異なる拠点から 1 つの拠点に集め、(2)「XOR 閾値秘密分散法」アルゴリズムによって複数のシェアから元のゲノム解析データを復元します。

本開発において、(A)シェアデータの保存先を、各拠点におけるディスクのセクタ単位で指定することで高速にシェアデータの読み書きを行う「ダイレクトアクセス技術」、(B)量子鍵配送によって生成した暗号鍵を大量に蓄積し、ソフトウェアの並列実行によって、情報理論的安全が保証されるワンタイムパッド暗号を高速に実行する「並列ソフトウェア技術」等を用いて秘密分散およびワンタイムパッド暗号通信の高速化を実現しました。これらの高速化技術を活用することで、情報理論的安全性を確保しつつ、大容量のゲノム解析データを実用的な時間で分散保管する技術を確立しました。

東芝、ToMMo・東北大学病院、および NICT は、開発した分散保管技術を利用し、東芝ライフサイエンス解析センター（LSA、仙台市青葉区南吉成）、ToMMo（仙台市青葉区星陵町）、東北大学病院（仙台市青葉区星陵町）の 3 拠点でゲノム解析データを分散保管する実証実験を行いました。まず、ToMMo においてゲノム解析データに対して NICT が開発した秘密分散技術を用い、3 つのシェア(シェア A、シェア B、シェア C)を計算します。その後、シェア A は ToMMo にて保管、シェア B は東芝の量子暗号技術による暗号化伝送で東北大学病院に伝送・保管され、シェア C は同様に量子暗号技術による暗号化伝送で LSA に伝送・保管されます。オリジナルの解析データを復元する場合、3 つのシェアのうち 2 つのシェアを ToMMo の拠点に集め、秘密分散技術を利用して復元します（図 1)。

1 検体のゲノム解析データ（約 80GB）を対象に、分散保管および復元に要する時間とスループットを測定した結果、分散保管処理時は約 30 分(356Mbps)、復元処理時は約 21 分(502Mbps)となりました(*5)。ToMMo における最小バックアップ単位(100 検体)に換算した場合、およそ 50 時間となります。これは、現状のテープ等のメディアを用いたゲノム解析

データの遠隔保管地から物理的に運搬するユースケースと比べて実用的な速度に相当します。

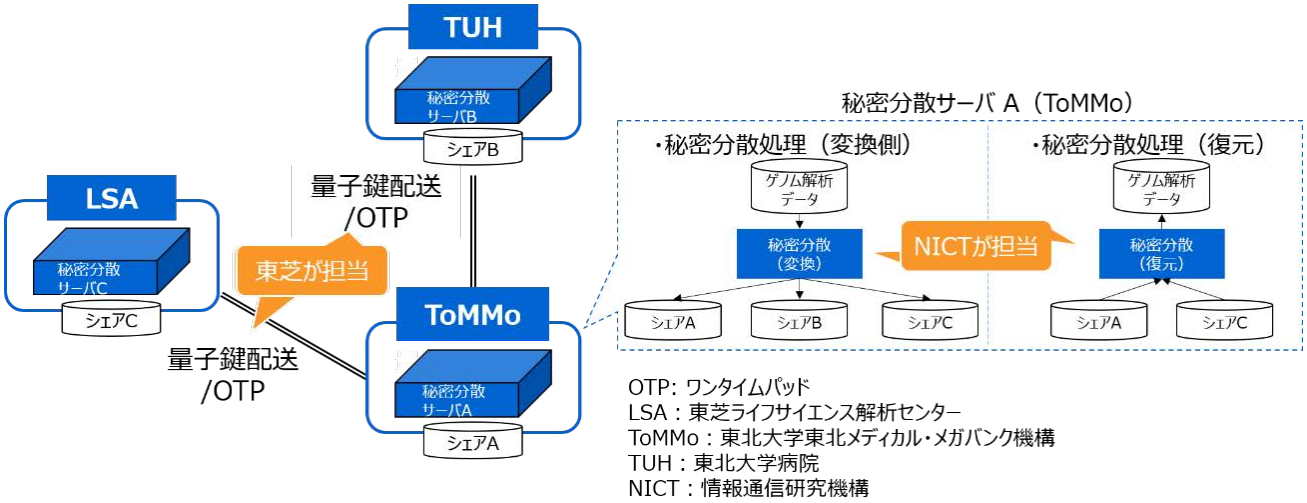

図 1 ゲノム解析データ分散保管実証実験の概要

東芝は今後も、秘密分散技術と組み合わせたシステム実証を含む様々な量子暗号通信技術の研究開発に取り組み、医療・金融・政府機関・通信インフラ等の多様なアプリケーションでの量子暗号通信技術の実用化を推進していきます。

ToMMo と東北大学病院は引き続き、ゲノム情報に基づいた未来型医療の実現に向け、安全・安心な ICT 技術の活用を推進していきます。

NICT は引き続き、量子通信分野における先端的・基礎的研究開発と産業への貢献に向け、量子暗号・光量子制御等の技術の研究開発に取り組みます。

実施体制

今回の実証は以下の体制・分担で実施しました。

東芝： 量子暗号通信システムと高速ワンタイムパッド暗号通信の開発。全体システム構築および運用。

ToMMo ・東北大学病院：検証拠点・検証ユースケースの提供、ゲノム医療分野での適用可能性確認。

NICT： 高速秘密分散システムとデータバックアップシステムの開発。

(*1)約 80GB（ギガバイト）

(*2)2021 年 8 月 26 日。東芝調べ。ゲノム解析データを量子暗号通信技術と秘密分散技術を

組み合わせたデータ分散保管技術で保管する実証の成功が世界初。

(*3) 一般的な暗号技術に用いられる、「特定の数学的な問題を解くことが難しい」という仮定に依存した安全性(計算量的安全性)とは異なり、攻撃者・盗聴者が得られる情報と、秘密情報との確率論的な独立性をもって安全性が保証される性質。理論上、如何なる盗聴攻撃によっても、情報が漏洩することは無い。

(*4) 送信する情報（平文）のデジタルデータと同じ長さの乱数を暗号鍵として用意し、1 回ごとに使い捨てる暗号通信方式。異なる平文ごとに、異なる暗号鍵を使う。平文と暗号鍵データの排他的論理和によって暗号文を生成して伝送し、受信側で再び暗号文と暗号鍵データの排他的論理和によって平文を復号する。情報理論的安全性を満たす方式であり、どんなに高い計算能力を持つ攻撃者・盗聴者であっても、暗号文から平文を永遠に解読できないことが証明されている最も安全で強固な暗号化方式である。

(*5) 各シェアデータのサイズは、元データであるゲノム解析データと同じ約 80GB となる。

以上

【報道機関からのお問い合わせ先】
株式会社　東芝
メディアコミュニケーション室
大石、本行
03-3457-2100
media.relations@toshiba.co.jp

東北大学東北メディカル・メガバンク機構
広報戦略室
教授　長神風二
022-717-7908
pr@megabank.tohoku.ac.jp

東北大学病院広報室
022-717-8032
press@pr.med.tohoku.ac.jp

国立研究開発法人情報通信研究機構
広報部 報道室
publicity@nict.go.jp

【技術に関するお問い合わせ先】
株式会社　東芝
研究開発センター
inquiry@rdc.toshiba.co.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
042-327-7552
fujiwara@nict.go.jp