2022 年 12 月 8 日

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

量子セキュリティ技術と個人認証を連携させ、セキュアな個別化ヘルスケアユースケースの実証に成功
～多数の個人のゲノムデータを情報理論的に安全に保管・伝送し、個人の許諾に応じて活用できるシステムを構築～

概要

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(トモ))、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(エヌアイシーティー))は、量子暗号通信技術および秘密分散技術を活用した量子セキュリティ技術と個人認証技術を連携させて、多数の個人のゲノムデータを複数拠点に分散保管し、医療や健康管理に活用する個別化ヘルスケア(*1)システムを世界で初めて構築・実証しました(*2)。本技術により、情報理論的に安全で将来にわたり盗聴の脅威のない形でゲノムデータの漏洩・改ざん・喪失を防ぐことに加え、いつでも個人認証と連携して復号・復元(*3)して活用することが可能となり、個別化ヘルスケアの実現や普及への貢献が期待できます。

本研究の一部は、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。

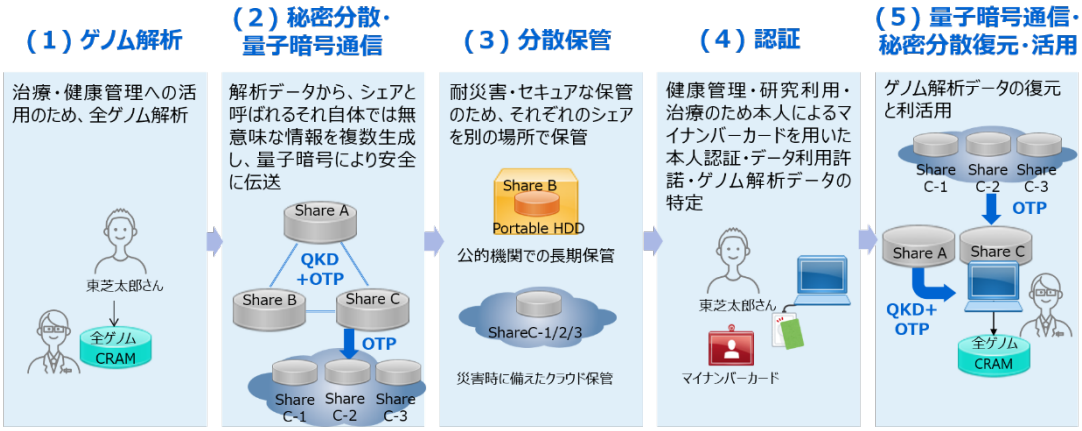

図 1　個別化ヘルスケアの全体シーケンス

開発の背景

近年のゲノムデータ解析技術の著しい進展に伴い、個別化ヘルスケアの実現への期待が加速度的に高まっています。個別化ヘルスケアでは、従来のように病気への罹患後にその種類や年齢・性別による一律的な治療を行うのではなく、個人のゲノムデータなどを生活習慣などの環境因子と共に解析し、病気の罹患へのリスク等を計算した上で個人に合った最適な予防法を提案します。個人の遺伝情報や生活習慣などに基づいて、最適な健康リスク管理を提案し、個人の多様性を考慮した個別化ヘルスケアが可能となります。

個別化ヘルスケアの実現のためには、ゲノムデータの解析技術に加え、ゲノムデータを含む個人の健康データを安全・安心に伝送・保管して利用する技術が必要です。ゲノムデータは、一定の条件を満たすと改正個人情報保護法において個人情報と同等とされる個人識別符号に位置付けられ、個々人の情報を守る必要があることはもちろんのこと、一度漏洩すると複数の世代・家系にわたってリスクに発展する可能性があります。ゲノムデータは“世紀単位”で保護する必要があり、個人の ID に関連付けて保管し、個人の利用許諾に合わせて復号・復元して利活用するためのセキュアなデータ伝送・保管基盤の構築が不可欠です。

東芝、ToMMo、東北大学病院、および NICT の 4 者は、2021 年 7 月に量子セキュリティ技術による「データ分散保管技術」を開発し、大規模ゲノム解析データを複数拠点に分散してバックアップ保管し、その後復元する実証実験に世界で初めて成功しました(2021 年 8 月公表(*4)。以下、従来の分散バックアップ手法)。従来の分散バックアップ手法は、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、原本データを一見乱数にしか見えない複数の分散片(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」の組み合わせにより実現しています。しかし、大容量データを一括伝送・保管することに主眼を置いた方式のため、多数の個人のゲノムデータを個別に扱うことが困難であり、また「量子暗号技術」と「秘密分散技術」の機能を独立して実装・運用するため、大規模システムとしての統一的な運用が難しいという課題があり、個別化ヘルスケアの実現に向けた次のステップとして効率的に大規模システムを運用する技術の開発が求められていました。

本技術の特長

そこで 4 者は、個別化ヘルスケアの実現に貢献するため、新たに「統合鍵管理システム」および「シェア制御システム」を開発し、ゲノムデータの安全な一括保管・復元に続き、随時、多数の個人データを分散保管し、個人認証と連携して必要時に復元するユースケースの実証に取り組みました。「統合鍵管理システム」は、量子暗号・秘密分散・個人認証を統一的に管理運用するためのプラットフォームであり、量子暗号や秘密分散の機能で大量に利用される暗号鍵および乱数の提供機能の統合と、データ伝送・保管の統一的な運用を実現しました。さらに、同じフォーマットで暗号鍵と乱数を提供するため、それぞれを切り替えて

利用可能で、より効率的に大規模システムを運用できます。

また、大量のゲノムデータの伝送には大量の量子暗号鍵が必要となりますが、暗号鍵の生成速度には限界があります。従来の分散バックアップ手法は、複数のシェアを異なる拠点に分散保管する際、データの保管先が固定的だったため、多数の個人データを随時分散保管する本ユースケースにおいて、量子暗号鍵を効率的に利用できないという課題がありました。今回開発した「シェア制御システム」は、各分散拠点の量子暗号鍵の残量情報からシェアを保管する最適な拠点を決定し、個人 ID と関連付けて保持することができます。これにより、大規模なシステムにおいて、多くの個人データを安全かつ効率的に分散保管し、また、個人認証をトリガーとして該当するシェアを特定し、安全に復元・利用することが可能になります。

4 者は、2021 年 7 月に開発・実証した「データ分散保管技術」に、今回開発した「統合鍵管理システム」および「シェア制御システム」と連携させることで個別化ヘルスケアシステムを構築し、ToMMo および東北大学病院のオペレーションにより実証を行い、情報理論的に安全で現実的な個別化ヘルスケアシステムの構築が可能であることを確認しました。今回モデルとして構築した、個別化ヘルスケアシステムでは、個人のゲノムデータのシェアの利用にマイナンバーカードによる認証を組み入れ、カードを保有する本人の利用許諾が無い限り、医療拠点においてもゲノム解析データの復元ができず、情報流出が起こらない仕組みを実現しました。さらに、このシステムでは拠点の一部が災害などでデータを喪失しても他拠点で格納しているシェアからデータを復元することが可能になります。

実施体制

東芝： 量子暗号通信システムと個別化ヘルスケアシステムの開発・構築・運用

ToMMo・東北大学病院: 検証拠点の提供・個別化ヘルスケアユースケースの具体化・オペレーション・適用可能性確認

NICT： 高速ワンタイムパッド(OTP) (*5)技術および高速秘密分散技術の開発・運用

今後の展望

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を加速し、医療・金融・政府機関・通信インフラなどの多様なアプリケーションでの量子暗号通信技術の早期実用化を推進していきます。

ToMMo および東北大学病院は引き続き、ゲノム情報に基づく未来型医療の実現に向け、安全・安心な ICT 技術の活用を進め、個別化ヘルスケアの実現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・光量子制御などの技術の研究開発に取り組んでいきます。

*1　個別化ヘルスケア：個人のゲノムデータなどを生活習慣などの環境因子と共に解析し、病気の罹患へのリスク等を個人ごとに計算した上で個人に合わせて最適化した健康リスク管理。

*2　2022 年 12 月 8 日、東芝調べ。個人のゲノムデータを、情報論理的に安全な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し、また個人認証と連携して復元し、医療や健康管理に活用できる個別化ヘルスケアシステムの構築・実証の成功が世界初。

*3　復号：量子暗号で暗号化されたデータの暗号化を解くこと。
復元：秘密分散されたシェアを 2 つ組み合わせて元の原本データに戻すこと。

*4　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(2021.8.26)
https://www.global.toshiba/jp/technology/corporate/rdc/rd/topics/21/2108-02.html

*5　ワンタイムパッド(OTP)：一度使用した暗号鍵を何度も使い回さずに、一度使用したら破棄する方式。

【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
高木、齊藤、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
022-717-7149
pr@hosp.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

別紙：参考資料

実証の概要

1. 実証内容

（1）量子暗号通信技術・秘密分散技術によってゲノム解析データを情報理論的に安全な形で伝送・保管できる。

（2）本人が所有するマイナンバーカードをアクセスキーとし、本人の利用許諾がある場合にのみゲノム解析データを復元して利活用できる。

2. 本実証において想定した個別化ヘルスケアのシーケンス

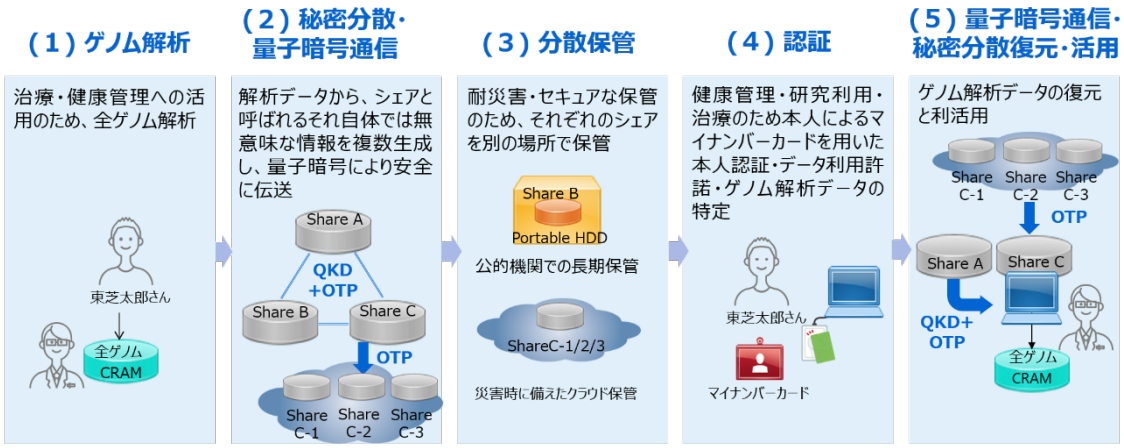

図 2　個別化ヘルスケアの全体シーケンス（再掲）

（1）ゲノム解析：生涯にわたる健康管理や医療への活用を想定し、個人の全ゲノム解析を行う。

（2）秘密分散・量子暗号通信：解析結果として得られたゲノム解析データは、秘密分散技術によって、シェアに分割し、シェアを保管する拠点を適切に選択した上で、該当拠点へと量子暗号通信により安全に伝送する。

（3）分散保管：セキュリティ確保や災害時のデータ保全を目的として、複数の拠点にシェアを保管する。シェアの一部は、大規模災害時にもデータ復元が可能なようにクラウドにも分散保管する。

（4）認証：健康管理・研究利用・医療での必要性に応じて、本人のマイナンバーカードを用いて、ゲノム解析データの利用許諾を行う。

（5）量子暗号通信・秘密分散復元・活用：本人がゲノム解析データの利用を許諾すると、本人のゲノム解析データに相当するシェアが量子暗号通信による暗号通信によって伝送され、分散保管されたシェアを一つの拠点へと集約させ、秘密分散によって元のゲノム解析データを復元し、利活用できる状態にする。

3. 実証システムの構成

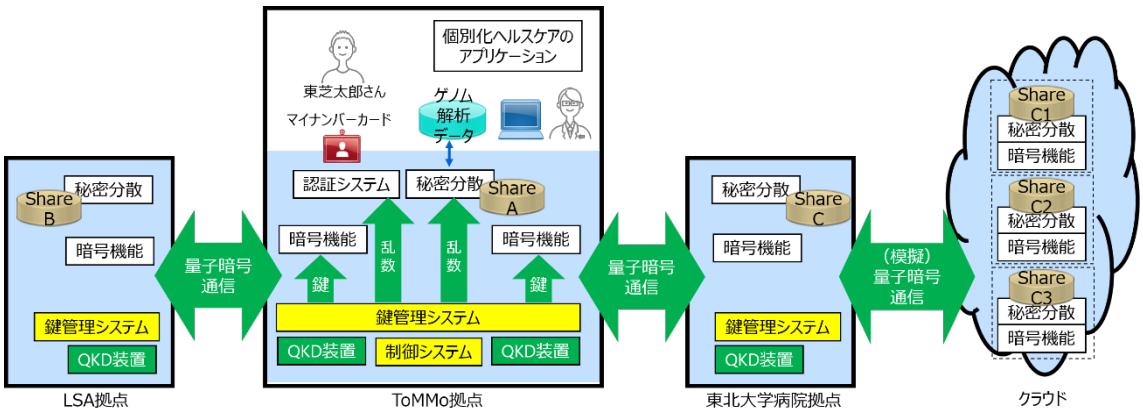

図 3　実証システム構成

実証環境として、ToMMo(仙台市青葉区星陵町)、東芝ライフサイエンス解析センター(以下、LSA、仙台市青葉区南吉成)、東北大学病院(仙台市青葉区星陵町)の 3 拠点と、3 拠点外に形成したクラウドに見立てた IP ネットワーク上のサーバ(3 式)を用いました。このうち、ToMMo -LSA 間リンク、ToMMo -東北大学病院間リンクでは、東芝が開発した量子暗号通信装置および OTP 暗号通信機能により暗号通信を行います。量子暗号通信装置によって、量子力学で安全性が保証される暗号鍵共有を行い、共有された暗号鍵を使った OTP 暗号通信機能によって、解読が不可能な情報理論的安全性を持つ暗号通信を実現します。

東北大学病院とクラウドとの間およびクラウド上に用意した 3 つのサーバ間には、実験の都合上、量子暗号通信装置を用いず、あらかじめ拠点間で共有・保管した乱数データを量子暗号鍵とみなし、NICT が開発した高速 OTP 暗号通信機能による暗号通信を行います。3 拠点およびクラウド上の 3 つのサーバはそれぞれ、新規に開発した「統合鍵管理システム」と、秘密分散機能を備えます。また、ToMMo の拠点には、「シェア制御システム」と、データの保管や参照をするための個別化ヘルスケアのアプリケーションが設置されます。「統合鍵管理システム」は、暗号通信機能への暗号鍵の提供と、秘密分散機能および認証システムへの乱数データの提供を統一的な手法で行います。「シェア制御システム」は、実証環境においてシェアを保管する場所を決定し、また各シェアの保管場所の情報を管理します。

4. 実証の手順

（1） ゲノム解析データとして、ToMMo がゲノム解析を実施した CRAM データフォーマット（ゲノムデータ向けのデータフォーマットのひとつ）のゲノム解析データ(16GB)を用います。また、該当ゲノム解析データの ID および認証データ(ハッシュデータ)を該当する個人が所有するマイナンバーカードに格納します。なお、本実証ではマイナンバーカードに見立

てた個人認証用非接触 IC カードとして、規格 ISO/IEC 14443 type A に準拠するカードを利用しました（以下、非接触 IC カード)。

（２） ToMMo の拠点にて、（１）の CRAM データフォーマットのゲノム解析データを、秘密分散機能により 3 つのシェア (Share A, Share B, Share C)に変換します。次に「シェア制御システム」により、該当のシェアを複数拠点へと分散保管します。シェア制御システムは、各拠点間リンクの量子暗号鍵の残量などを含むシステムの状況から、シェアを保管する拠点を決定します。ここでは、Share B が LSA へ、Share C が東北大学病院へ、それぞれ量子暗号通信によって暗号化されて伝送されます。なお、シェア制御システムは、個人の ID と、該当するゲノム解析データのシェアの ID およびその格納拠点の情報を関連付けて管理します。

（３） 東北大学病院に格納されたシェア (Share C)をさらに、秘密分散によって 3 つのシェア(Share C1, Share C2, Share C3)へ分割し、これらをクラウド上の 3 サーバに分散保管します。東北大学病院 -クラウド間、クラウド上のサーバ間のシェア伝送は、高速 OTP 暗号によって暗号化されます。なお、クラウド上の 3 サーバにシェアを格納した後、東北大学病院におけるシェア(Share C)を削除します。このときシェア制御システムは、各シェアの格納場所情報を、クラウド上のサーバへと変更します。

（４）本人が ToMMo で非接触 IC カードを提示し、ゲノム解析データの利用を許諾すると、非接触 IC カードに格納されている ID および認証情報に基づいて、認証システムにおいて認証され本人が特定されます。次に、シェア制御システムが参照され本人に対応する復元すべきシェアが特定されます。

（５） クラウド上で、2 つのシェア(例えば Share C1 と Share C2)が選択され Share C を復元し、OTP 暗号によって東北大学病院へ伝送されます。次に Share C は、量子暗号通信によって東北大学病院から ToMMo へ伝送されます。ToMMo では、Share C と Share A とから、原本データにあたるゲノム解析データが復元されます。非接触 IC カードに格納されたハッシュデータを確認することで、本人のデータであることが確認された後、ゲノム解析データが利活用可能な状態になります。なお、LSA に格納されたシェア(Share B)はバックアップデータに相当し、例えば、遠隔の公的医療機関において保管されます。