

量子鍵配送ネットワークのグローバルビジネス展開

Global Expansion of Quantum Key Distribution Network Businesses

リー ジョンソン Lee JOHNSON 川倉 康嗣 KAWAKURA Yasushi 佐藤 英昭 SATO Hideaki

東芝グループは、量子鍵配送（QKD）システムを活用したQKDネットワークを構築し、鍵提供サービスをグローバルに展開するために、様々な国や地域のパートナーと協業し、ユーザー企業とともにQKDネットワークを実証するテストベッドの構築を進めている。

英国ではBTと共同で、世界初^(注1)の商用向けメトロネットワークを構築し、トライアルサービスを開始した。米国ではJPモルガン・チェース及びCienaと共同で、金融分野のブロックチェーンにQKDを適用する実証実験を行った。韓国ではKTと共同で、韓国ソウル特別市と釜山市の間の約490 kmを、異機種のQKD装置でつないだ韓国最長^(注2)となる長距離QKDネットワークを構築し、サービス品質を検証した。

With the aim of supplying quantum key distribution (QKD) services to the global market by means of QKD networks using QKD systems, the Toshiba Group has been making efforts, in collaboration with partners in various countries and regions, to construct testbed environments in order to implement various demonstration experiments on QKD networks together with user companies.

In the United Kingdom, in cooperation with BT, we have constructed the world's first quantum-secured commercial metro network and commenced trial services. In the United States, in cooperation with JPMorgan Chase & Co. and Ciena Corporation, we have conducted demonstration experiments on the application of QKD technologies to blockchains in the financial field. In South Korea, in cooperation with KT Corporation, we have constructed South Korea's longest hybrid QKD network built with different QKD systems over a distance of approximately 490 km from Seoul to Busan, and evaluated its quality of service (QoS) through demonstration experiments.

1. まえがき

東芝グループは、QKDとQKDネットワークの技術をコンピタンスとした鍵提供ビジネスをグローバルに展開するため、様々な国や地域のパートナー企業と協業し、QKDネットワーク実証のためのテストベッド構築を進めている。テストベッドでは、パートナー企業とQKDサービスを運用するための課題を明らかにするとともに、ユーザー候補の企業が参画し、実用面の課題を明らかにしていく計画である。これまでに、欧州、北米、及びアジアにおいて複数の実証を進め、QKDネットワークの構築・運用ノウハウを獲得して、商用ネットワーク構築に向けた運用実績を積んできた。

ここでは、英国における都市規模のQKDネットワーク商用テストベッド、米国におけるブロックチェーン技術へのQKD適用実証、及び韓国における長距離QKDネットワークの実証について、各システムの概要・特徴、及び各国のQKDネットワークビジネスの方向性について述べる。

2. 欧州の事例

2.1 欧州の動向

世界中で、量子コンピューター技術の開発や量子技術企業への投資などを推進する発表が、日々行われている。また、量子コンピューターがセキュリティにもたらす脅威を認識して対応を計画している欧州の政府機関、事業者、更にはその顧客企業からも、QKDへの関心が寄せられている。

政府に関しては、大規模な投資を行うEuroQCI (European Quantum Communication Infrastructure)^(注3)などのイニシアティブが、そのほか各国の追加投資によるプログラムとともに進行中である。東芝グループは、これらに関係する複数のコンソーシアムに参加しており、その進捗に従って、QKDネットワークの興味深い展開とユースケースが見られると考えている。

2.2 英国におけるBTとの商用テストベッド

東芝グループは、複数の通信事業者との協力関係を構築している。特に、英国では過去数年間にわたって、BTと

(注1) 2022年4月時点、東芝及びBT調べ。

(注2) 2022年3月現在、東芝、東芝デジタルソリューションズ(株)、及びKT調べ。

(注3) 27のEU加盟国をまたがって欧州全域をカバーする量子通信基盤構築プログラム。

連携して東芝グループのQKDネットワーク技術を検証しており、この結果として、Quantum Secure Metro Network (QSMN) の世界初の商用トライアルを共同で展開するに至った。

QSMNは、ロンドン中心部、ウエストエンド、及びロンドン中心部から西へ約32 kmに位置するスラウに展開され、金融、メディア、政府機関など、BTが持つ価値の高い潜在顧客が存在する大都市圏をカバーしている。BTは、QSMNの最初の顧客となったErnst & Youngと接続を完了し、Ernst & Youngは、ロンドンにおける二つの主要拠点間で機密情報を安全に配信するために、このネットワークの利用を始めた。BTと東芝グループは、QSMNへの接続とサービスの利用を希望する可能性のある、ほかの大企業とも協議を進めている。

QSMNは、BTのネットワーク上で東芝グループのQKD装置を利用している。BTは東芝グループによる支援の下でQSMNを運用し、専用的高帯域エンドツーエンド暗号化リンクを含めた、多様な耐量子通信サービスを複数展開することを予定している。

QSMNは、BTの従来の回線を利用してBTの主要な拠点(量子ノード)を接続し、QKDのコアリングを構成している(図1)。そして、BTの完全子会社であるOpenreachのOptical Spectrum Access Filter Connect (OSA FC) のファイバーソリューションを使って、顧客をネットワークに接続する。QKDネットワークはメッシュ構成で、BTの既存のネットワーク管理基盤に組み込まれて、東芝グループの鍵管理システム(KMS)を使ってユーザーに暗号鍵を配送する予定である。

BTは、従来のセキュリティーポートフォリオ、ネットワーク、及びエンドツーエンドのサービスにQKDを付加するこ



図1. QSMNにおけるQKDコアリング

ロンドン中心部から郊外までをカバーする、都市規模のQKDネットワークを構築した。

QKD core ring in quantum-secured commercial metro network

とで、英国における信頼の提供者としての地位を確立することを計画している。BTは、ビジネスケースと大規模なQKDネットワークの展開・運用に必要な課題を理解するために、QSMNを活用している。この活動の一部として、BTは、QKD as a Service (QKDaaS) やQKDとPost Quantum Cryptography (PQC) の組み合わせなどを含む、様々なサービスの開発を行う。

英国でのQSMNの展開は、東芝グループのQKD事業にとって重要な価値を持っている。これは、主要通信事業者の運営するネットワーク及びその事業において、東芝グループのQKD製品が簡易に適用できることを実証し、QKDにおける東芝グループのグローバルテクノロジーリーダーとしての立場を証明した。また、東芝グループのQKD製品の開発が更に進むとともに、世界におけるQKDの商業展開を加速させ、新たな収益を生み出すことにつながる。

BTと東芝グループの両社にとって、QSMNはQKDを採用する上での大きなマイルストーンである。これは、量子セキュアな通信を実現するための英国内全域ネットワーク構築への重要なステップであり、世界的な量子経済の成長を促進するものである。

3. 米国の事例

3.1 米国の動向

米国では、2018年12月に制定された国家量子イニシアティブ法に基づき、量子経済開発コンソーシアムQED-Cや量子情報科学研究センターなどが設立され、国家を挙げて量子技術推進に取り組んでいる。通信分野では、米国立標準技術研究所(NIST)がPQCの標準化に取り組むとともに、エネルギー省及びその傘下の研究機関が量子インターネットブループリントを公表し、量子ネットワークの先端技術研究を行っている。民間では、通信キャリア・データセンター事業者・金融会社などが、量子コンピューターによるセキュリティー環境への影響に強い危機感を持ち、量子通信をいかに使いこなすかを研究している。

これらを背景に、東芝グループが米国で実施した二つの実証実験について述べる。

3.2 金融アプリケーションでのQKDの実用性実証

ブロックチェーンや暗号通貨などの技術のセキュリティー環境は近い将来に変化すると考えられ、JPモルガン・チェースは東芝グループ及びCienaと共同で、金融アプリケーションの実行基盤でQKDの実用性を実証した⁽¹⁾。

ミッションクリティカルな金融アプリケーションでは、高速大容量かつ低遅延なデータ伝送とともに、盗聴などのセキュリティー脅威に対して即座に検出・防御することで、安

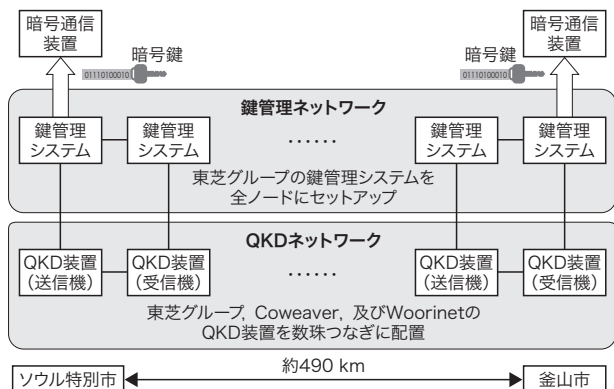


図3. 韓国におけるQKD実証システムの概要

QKD実証システムは、複数の異なるQKD装置と鍵管理システムから構成される。

Outline of hybrid QKD network demonstration system in South Korea

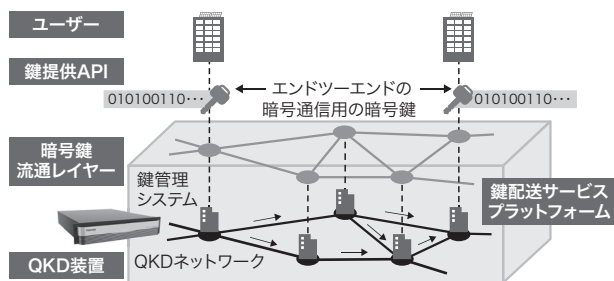


図4. QKDネットワークと鍵管理システム

QKDネットワークと鍵管理ネットワークにより、安全な暗号鍵をユーザーに提供する。

QKD network and key management system

暗号鍵を取得するために、ETSI (欧州電気通信標準化機構) GS QKD 014⁽⁴⁾で規定されるAPI (Application Programming Interface)を実装している。また、鍵を中継するための経路を動的に変更する機能もあり、経路の状況に応じた最適な経路を選択するだけでなく、途中の経路の障害を迂回(うかい)して可用性を確保することも可能である(図4)。

このような実証システムを構築し、1か月以上の安定稼働を確認するとともに、ITU-T (国際電気通信連合-電気通信標準化部門) Y.3807⁽⁵⁾に規定される鍵配送サービスの品質(QoS)測定を、KTが実施した。QoSパラメーターには、鍵取得時の応答遅延や鍵損失率などが含まれる。

この実証で得た成果を基に、今後も潜在ユーザーがQKDネットワークをトライアル利用できるテストベッドシステムを構築して技術評価を行い、QKDネットワークを活用したサービス開発支援を推進する計画である。量子産業のエコシステム拡大を目指して、QKDネットワークサービスのオープンなテストベッドを運用していく。

5. あとがき

QKDネットワーク事業のグローバル展開を視野に入れた、各国での取り組みについて述べた。これまでに東芝グループは、英国、米国、及び韓国におけるパートナー企業と連携し、QKD事業を各国の通信インフラサービスとして展開していくためのトライアルを実施してきた。技術的な検証及びシステム運用上の課題の確認を通して、ユーザー企業における要求仕様やシステムの使用感について知見を得ることができた。

今後は、テストベッドシステムを活用して、QKDネットワークによる持続可能なサービス事業の実現に向けたビジネスモデルの開発に取り組み、各国において、パートナー企業とともにQKDaaSの実現を目指す。

文 献

- (1) Toudeh-Fallah, F. et al. Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments. Quantum Physics. 2022, arXiv:2202.07764. <https://arxiv.org/abs/2202.07764>, (accessed 2022-07-21).
- (2) Chicago Quantum Exchange. "Chicago expands and activates quantum network, taking steps toward a secure quantum internet". News. <https://chicagoquantum.org/news/chicago-expands-and-activates-quantum-network-taking-steps-toward-secure-quantum-internet>, (accessed 2022-07-21).
- (3) National Security Agency/Central Security Service. "QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY (QC)". <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>, (accessed 2022-07-21).
- (4) ETSI GS QKD 014 V1.1.1:2019. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. <https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf>, (accessed 2022-07-21).
- (5) ITU-T Y.3807 : 2022. Quantum key distribution networks - Quality of service parameters. <https://www.itu.int/rec/T-REC-Y.3807>, (accessed 2022-07-21).



リー ジョンソン Lee JOHNSON
東芝欧州社 量子技術事業部
Toshiba Europe Ltd.



川倉 康嗣 KAWAKURA Yasushi
東芝デジタルソリューションズ(株)
ICTソリューション事業部
エネルギー・インフラデジタルトランスフォーメーション推進部
Toshiba Digital Solutions Corp.



佐藤 英昭 SATO Hideaki
東芝デジタルソリューションズ(株)
ICTソリューション事業部 QKD 事業推進室
情報処理学会会員
Toshiba Digital Solutions Corp.