資料２

日本成長戦略会議　第3回量子ワーキンググループ
ヒアリング資料

量子通信への東芝の取り組み

TOSHIBA

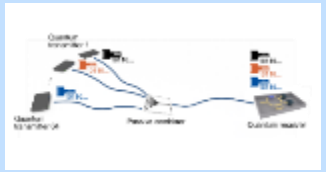
株式会社東芝　代表取締役　社長執行役員CEO
一般社団法人 量子技術による新産業創出協議会（Q-STAR）　代表理事
島田 太郎
2026年3月26日

東芝における量子暗号通信の技術開発と実証試験

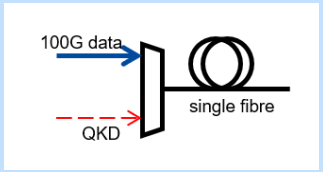
技 術 開 発

QKD>100km

QKD>1Mb/s

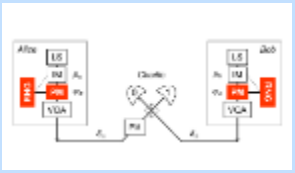


量子アクセス
ネットワーク



QKD 多重化

QKD>10Mb/s



Twin-field QKD

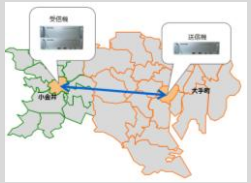
QKDチップ

QKD装置

2004 2010 2013 2016 2018 2019 **事業開始** 2020 2022 2024 2026

最初のQKD
ネットワーク実
証SECOQC[*1]
ウィーン,
2004-08

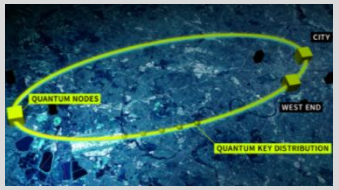
GHz QKDネット
ワーク実証
東京(NICT)
Tokyo QKD
2010-15



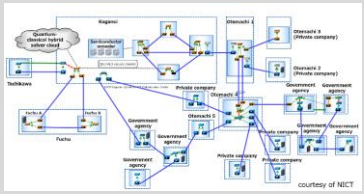
多重化QKD実証
Cambridge
Quantum
Network, 2015+

ユースケース実証
6テストベッド
OpenQKD[*2],
2019+

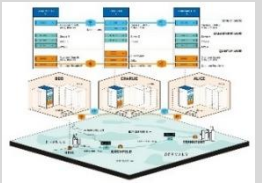
メトロネットワークの
商用トライアル
BT, 2022



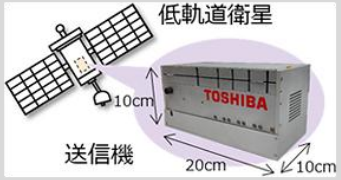
量子セキュア
クラウド
東京(NICT)
Tokyo QKD
2023+



Twin-field QKD
実証254 kmの敷
設済みファイバー
ドイツ, 2024



衛星搭載用
QKD送受信
システム実証,
英国,2026



実 証 試 験

*1 https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001/pdf

*2 https://openqkd.eu/

量子セキュア通信プラットフォーム

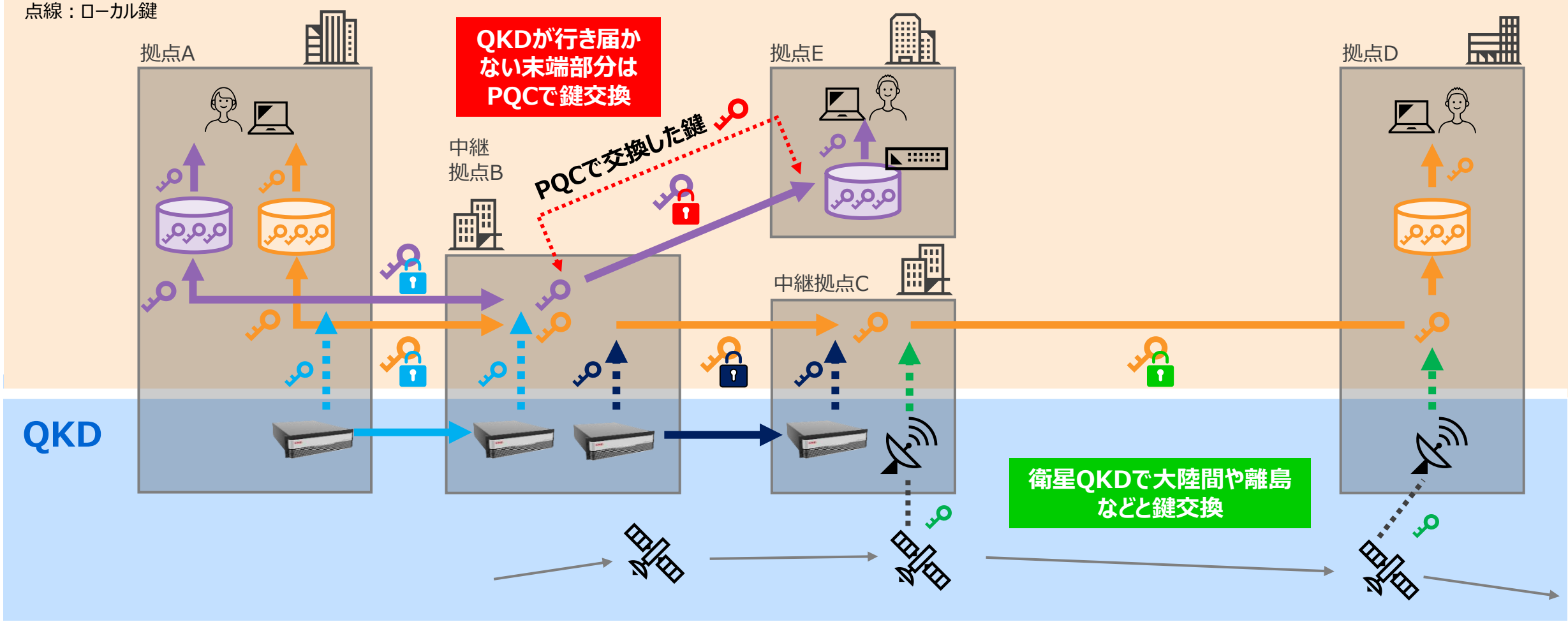
地上QKD+衛星QKD+PQC

鍵管理システム(KMS)

鍵管理システム(KMS)が属性の異なる鍵交換リンクを統合。任意の拠点に安全な暗号鍵を配送・蓄積し、暗号通信の可用性を担保

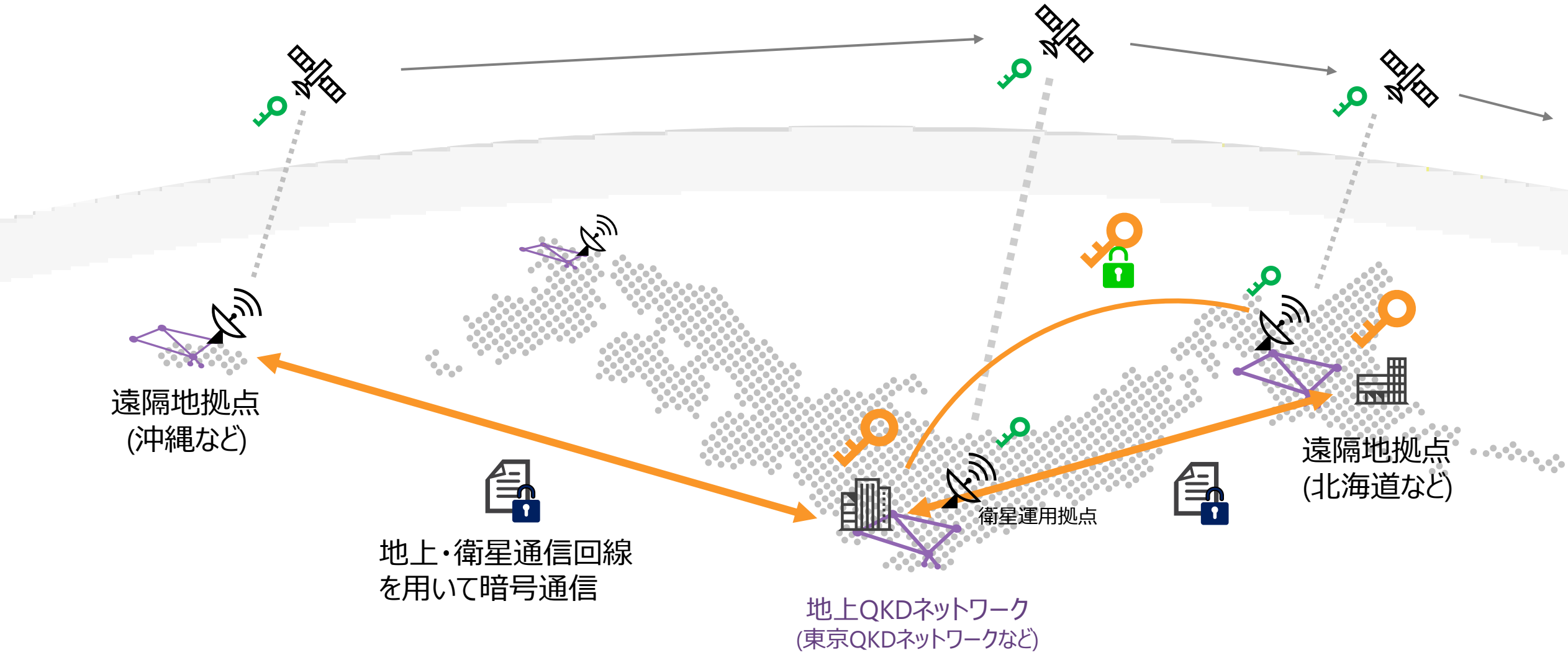
衛星・地上QKDが連携し、広域に安全な暗号鍵を供給、地上・衛星通信回線を用いて暗号通信。拠点間通信はQKDで強固に防御、拠点内の端末など末端部分はPQCで防御

実線：グローバル鍵
点線：ローカル鍵



量子セキュア広域通信ネットワーク

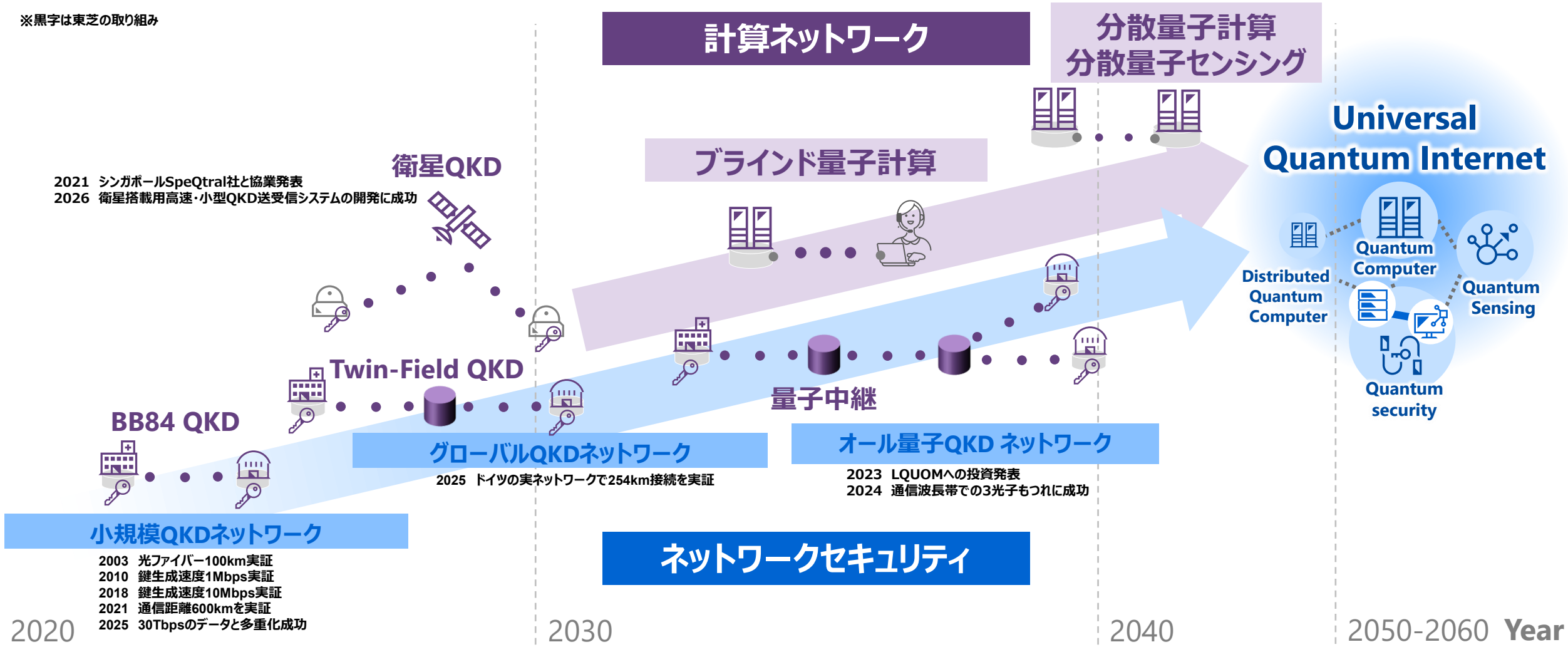
衛星・地上QKDが連携し、広域に安全な暗号鍵を供給、地上・衛星通信回線を用いて暗号通信



量子鍵配送から量子インターネットへ

QKD技術が 汎用量子インターネットUniversal Quantum Internet に進化していく

※黒字は東芝の取り組み



スタートアップ連携による技術強化

自社技術×エコシステムで量子インターネットの実現を加速

量子インターネット社会実装を目指すLQUOMが、東芝を引受先とするSeries Aエクステンションラウンド資金調達を実施

LQUOM株式会社　2023年5月9日 10時00分

2

LQUOM株式会社は株式会社東芝を引受先とする第三者割当増資により、Series Aエクステンションラウンドで資金調達を実施したことを発表いたします。本資金調達は、株式会社東芝のNextビジネス開発部 新規事業推進室が行うCVC機能により実施されました。これによって量子通信におけるエコシステム形成を始めとした事業化を加速して参ります。

LQUOM Quantum Communication　TOSHIBA

2023.5.9　報道発表

TOSHIBA　Japan　検索　English　Global　サイトマップ　お問い合わせ

製品・サービス　企業情報　ニュース

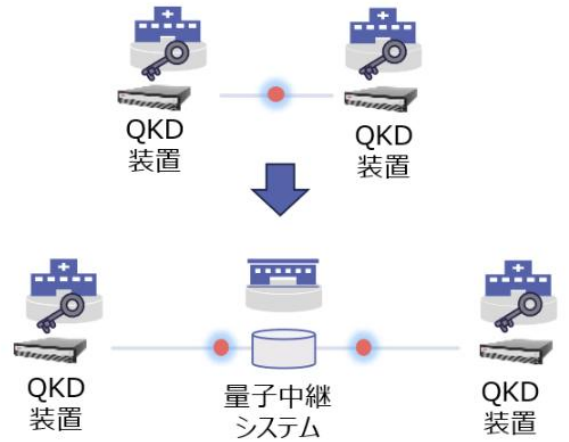
ニュース > 量子中継技術を用いた長距離量子鍵配送システムに関する共同研究契約を締結

量子中継技術を用いた長距離量子鍵配送システムに関する共同研究契約を締結

～量子インターネット実現を見据えた長距離量子鍵配送の技術検討を加速～

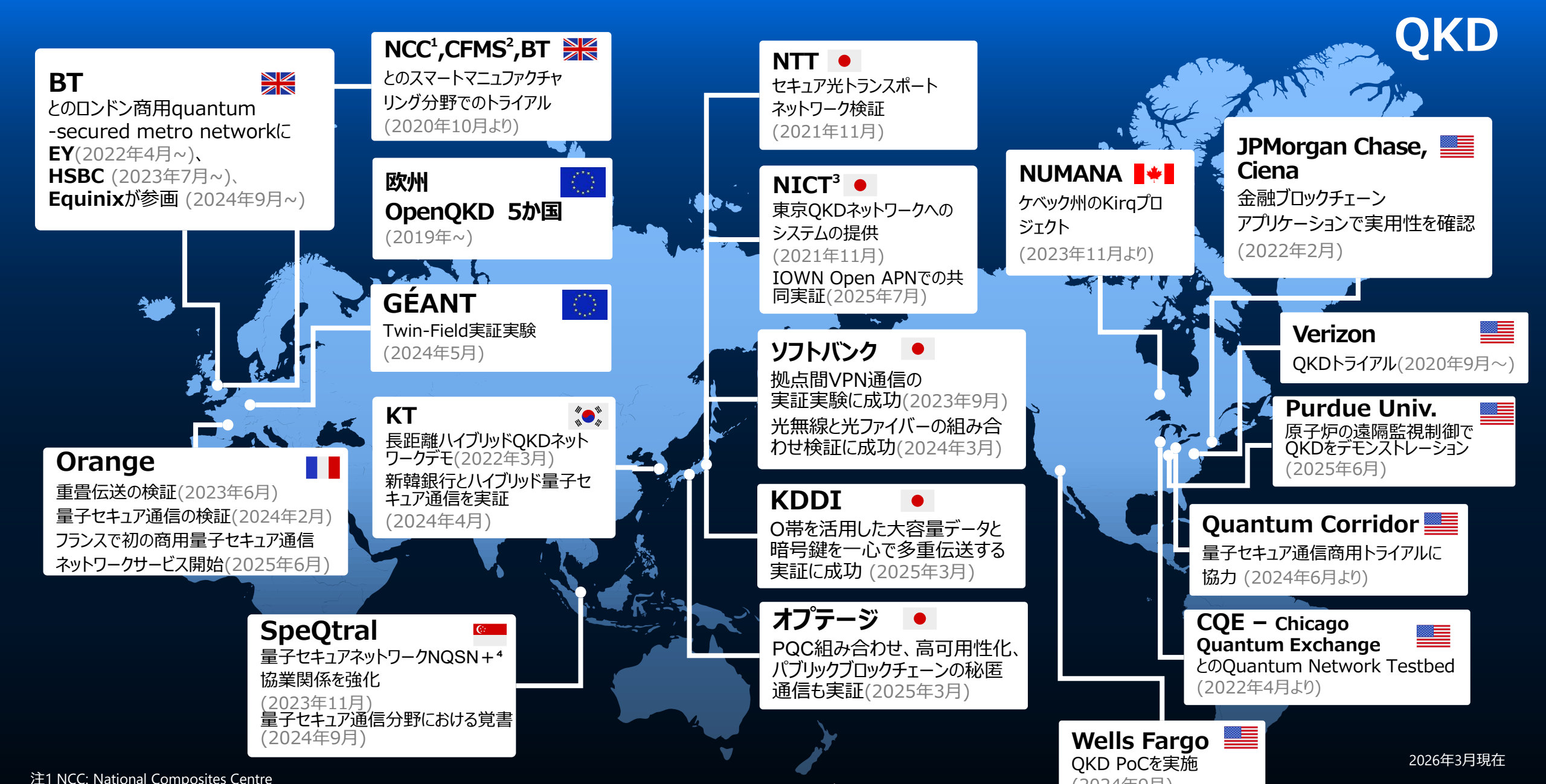
2026年03月19日

株式会社 東芝
LQUOM株式会社



2026.3.19　報道発表

量子中継技術で量子鍵配送のさらなる長距離化を図る



BT
とのロンドン商用quantum -secured metro networkに**EY**(2022年4月～)、**HSBC** (2023年7月～)、**Equinix**が参画 (2024年9月～)

NCC[1],CFMS[2],BT
とのスマートマニュファクチャリング分野でのトライアル
(2020年10月より)

欧州 OpenQKD 5か国
(2019年～)

GÉANT
Twin-Field実証実験
(2024年5月)

KT
長距離ハイブリッドQKDネットワークデモ(2022年3月)
新韓銀行とハイブリッド量子セキュア通信を実証
(2024年4月)

Orange
重畳伝送の検証(2023年6月)
量子セキュア通信の検証(2024年2月)
フランスで初の商用量子セキュア通信ネットワークサービス開始(2025年6月)

SpeQtral
量子セキュアネットワークNQSN＋[4]協業関係を強化
(2023年11月)
量子セキュア通信分野における覚書
(2024年9月)

NTT
セキュア光トランスポートネットワーク検証
(2021年11月)

NICT[3]
東京QKDネットワークへのシステムの提供
(2021年11月)
IOWN Open APNでの共同実証(2025年7月)

ソフトバンク
拠点間VPN通信の実証実験に成功(2023年9月)
光無線と光ファイバーの組み合わせ検証に成功(2024年3月)

KDDI
O帯を活用した大容量データと暗号鍵を一心で多重伝送する実証に成功 (2025年3月)

オプテージ
PQC組み合わせ、高可用性化、パブリックブロックチェーンの秘匿通信も実証(2025年3月)

NUMANA
ケベック州のKirqプロジェクト
(2023年11月より)

Wells Fargo
QKD PoCを実施
(2024年9月)

JPMorgan Chase, Ciena
金融ブロックチェーンアプリケーションで実用性を確認
(2022年2月)

Verizon
QKDトライアル(2020年9月～)

Purdue Univ.
原子炉の遠隔監視制御でQKDをデモンストレーション
(2025年6月)

Quantum Corridor
量子セキュア通信商用トライアルに協力 (2024年6月より)

CQE – Chicago Quantum Exchange
とのQuantum Network Testbed
(2022年4月より)

協業実績

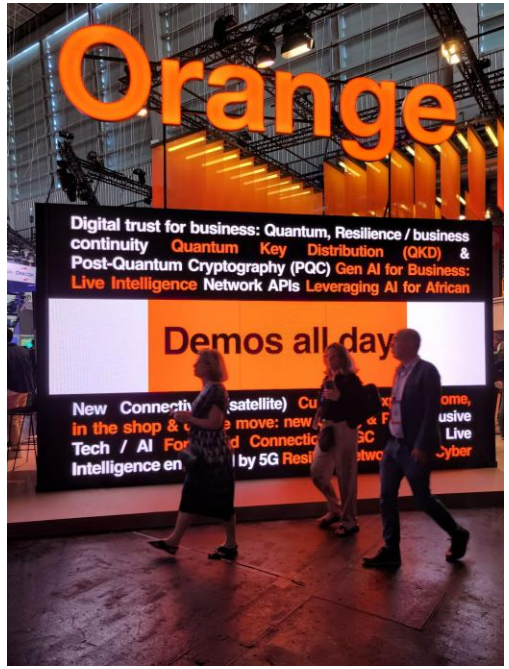
2026年3月現在

注1 NCC: National Composites Centre
注2 CFMS: Centre for Modelling and Simulation
注3 NICT: 国立研究開発法人情報通信研究機構
注4 NQSN+: National Quantum-Safe Network Plus(国家耐量子ネットワーク・プラス)

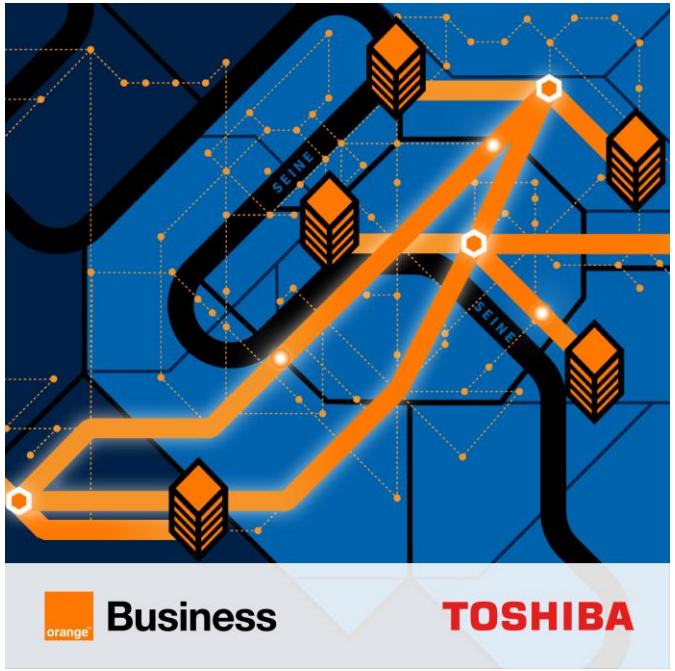
商用化 商用量子セキュア通信ネットワークサービスを提供開始

- 2025年6月11日、Orange Business 社※は量子セキュア通信ネットワークサービス「Orange Quantum Defender」をパリで商用提供開始
- 商用環境はロンドン・メトロネットワークに続く2例目であり、現在**世界で唯一の商用量子セキュア通信サービス**
- 東芝の量子鍵配送と耐量子計算機暗号を組み合わせた多層防御技術を利用
- パリ市とその周辺を含むパリ大都市圏で提供を開始し、フランスの大手金融企業が最初のユーザーとして、秘匿性の高い金融データのセキュリティを保ちながら通信を開始

※Orange Business社：Orangeグループ（旧France Telecom）のエンタープライズ部門で、ネットワークとデジタルのインテグレーションを提供。65カ国に3万人の従業員を擁し、世界中で3万社を超えるB2B顧客を抱える。



2025年6月にパリで開催されたVIVA Tech（欧州最大級のテックイベント）にてOQDサービスを発表、展示・デモを実施



パリ量子セキュア通信ネットワークのイメージ図： QKD 3ノードで、リング状にコアネットワークを構成。各ノードよりユーザーアクセスリンクを張る。

量子暗号通信テストベッドの拡張に向けて

世界的に競争力のある長距離テストベッド環境の構築
機密情報（政府・国防・医療・金融など）での実証

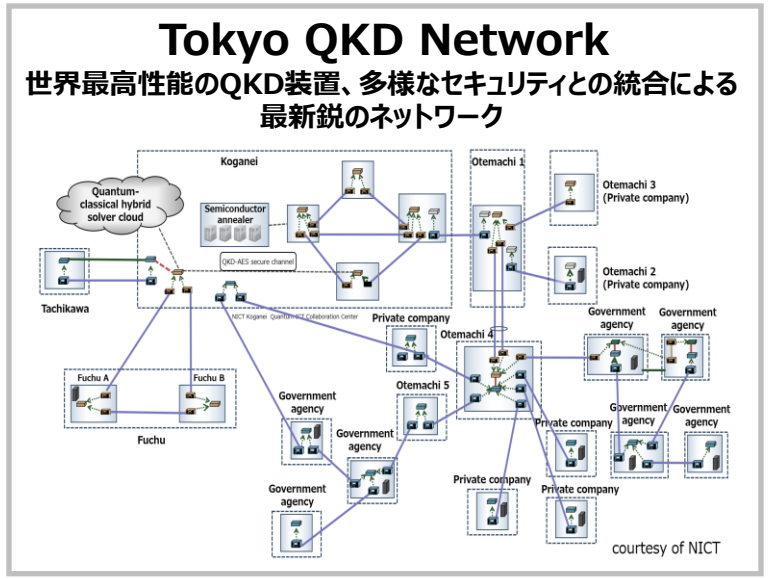
最新鋭の量子暗号通信テストベッドが
東京にて稼働
（産官学がオープンに利用可能な仕組み）

<u>主要都市間への拡大</u>
東京QKDネットワークを拡張し
東名阪で利用可能に

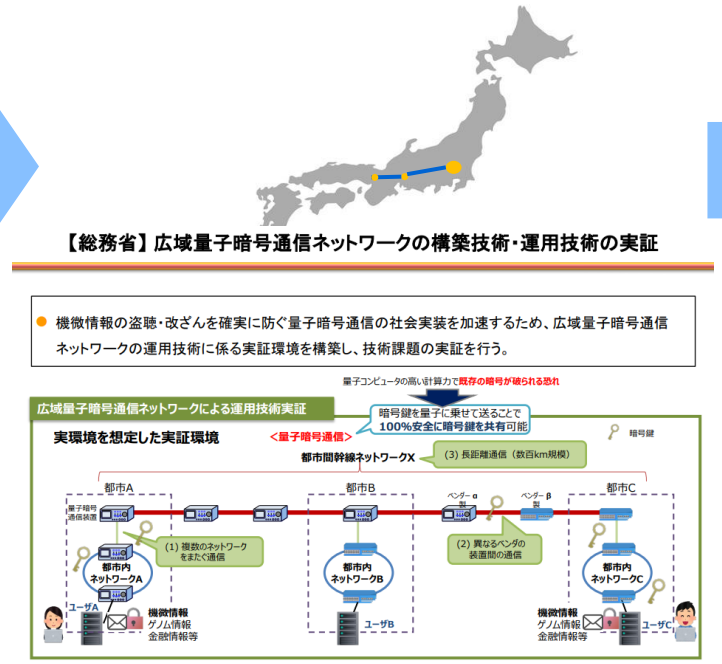
政府機関(防衛・医療など)が主導する実利用と
国際標準の実装で競争力を磨く

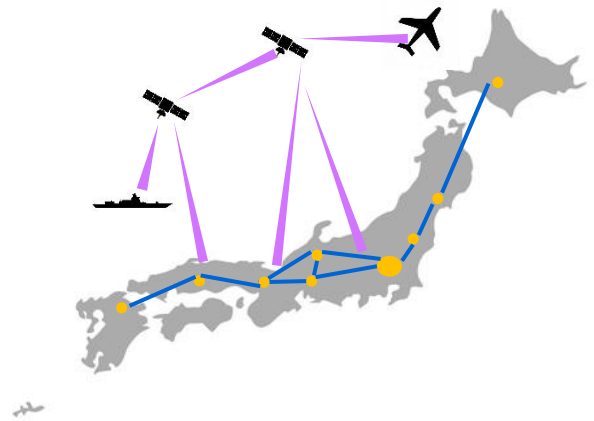
<u>全国ネットワークの実現</u>
日本全国に拡張
ユースケースのさらなる拡大

研究開発が進む衛星QKDと地上網の実装
民間での本格導入を進める



QKD: Quantum Key Distribution
NICT: National Institute of Information and Communications Technology



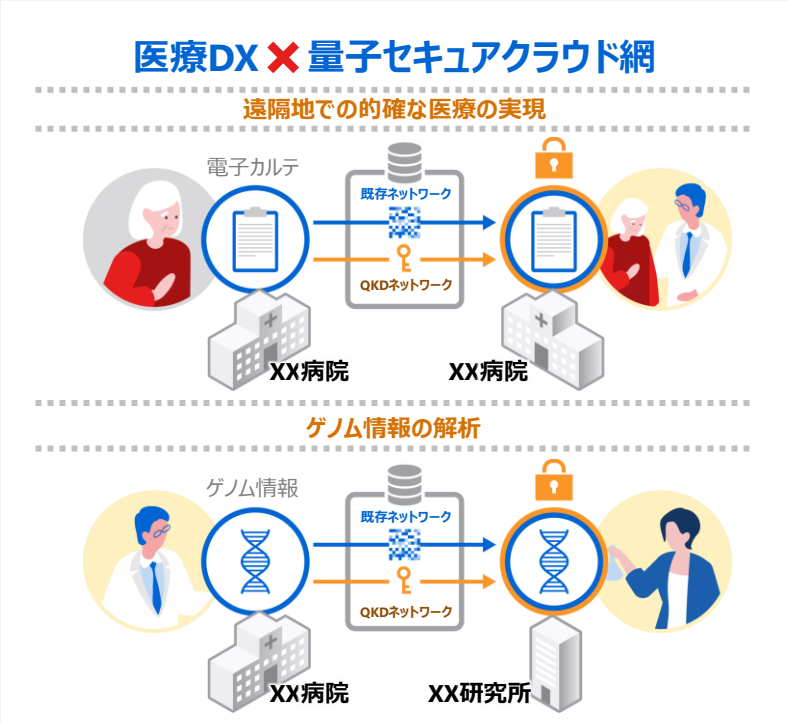


量子技術イノベーション戦略の戦略見直し検討ワーキンググループ（第４回）
資料2　佐々木構成員資料『量子セキュリティ分野の動向と展望』
（令和３年12月6日）
https://www8.cao.go.jp/cstp/ryoshigijutsu/kento_wg/4kai/siryo2.pdf
を参考に作成

ユースケース例① 医療分野（Healthcare / Medical Data）

安心・安全・快適な国民生活

地域医療情報連携ネットワーク（電子カルテ等）、医療画像など、国民の生活に密着し、その質向上に資するためのICTの活用・DX化の推進を、安全確実な通信インフラで支える。



主な狙い

- **患者データ・医療画像・ゲノム情報**の長期秘匿性
- 医療機関間データ連携（院内・院外・クラウド）の安全性
- 「Harvest now, decrypt later」対策
  （将来の量子計算機耐性）

代表的ユースケース

1.病院間データ連携（EHR / PACS）

- 大学病院 ↔ 地域医療機関間の電子カルテ共有
- 医療画像（CT/MRI）の転送鍵をQKDで生成
- 特に**都市部の光ファイバ網**と親和性が高い

2.遠隔医療・手術支援

- 遠隔手術・診断における制御信号・映像ストリームの鍵管理
- 「通信が改ざんされない」ことの**物理的保証**が重要

3.医療クラウド接続

- 病院 ↔ 医療データセンター間のVPN鍵をQKDで供給
- QKD + AES / PQC の**ハイブリッド構成**で堅牢性と
- フレキシビリティを両立

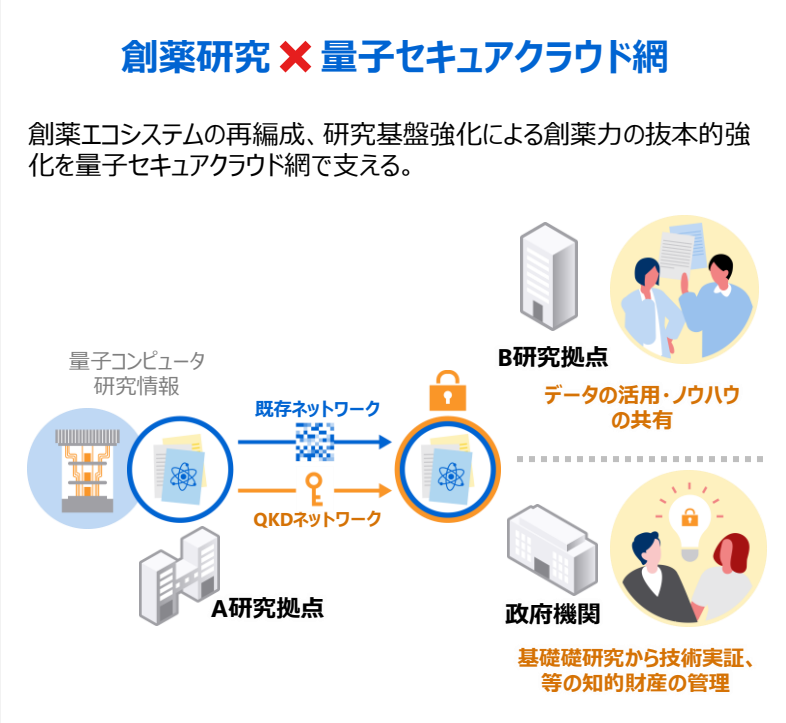
ポイント

- 医療は**規制産業（GDPR, HIPAA 等）のため**
  → **QKDの「理論安全性」が説明責任**に使いやすい

ユースケース例② 創薬・ライフサイエンス（Drug Discovery / Pharma）

最先端技術の育成・イノベーション促進

創薬・ライフサイエンス研究など、日本の国際競争力に直結する戦略産業・戦略技術の発展・成長を安全確実な通信インフラで支える。



主な狙い

- **知的財産（IP）・未公開研究**データの保護
- 企業間・国際共同研究の安全なデータ共有
- 将来の量子計算による解読リスク回避

代表的ユースケース

1.製薬企業 × 研究機関の共同研究

- 分子構造データ
- シミュレーション結果
- AI創薬モデルのパラメータ

2.臨床試験データ（Phase I–III）

- 症例データ・統計解析結果
- 国際治験におけるデータ越境転送

3.HPC / 量子計算リソース接続

- 創薬用HPCセンター ↔ 製薬企業
- 将来的には量子計算クラウド＋QKD鍵配送という構図も想定

ポイント

・創薬は「**国家安全保障レベルの産業競争力**」と考えられ、防衛と同等のセキュリティが要求される

・**NDA・特許戦略**と相性がよく、ステークホルダの理解が得やすい

ユースケース例③ 防衛・安全保障（Defense / National Security）

国民の生命・身体・財産の安全確保

防衛関連情報（装備品・兵站等）、犯罪捜査関連情報（カジノ含む金融犯罪に係る情報含む）公安関連情報など、日本国民の生命・財産を脅かす脅威から守るための活動を安全確実な通信インフラで支える。

防衛 ✕ 量子セキュアクラウド網

例）監視・偵察用ドローンの画像データ・制御データをQKDで保護し、量子セキュアクラウドに安全に保管

犯罪捜査 ✕ 量子セキュアクラウド網

金融犯罪等、民間事業者と警察組織との間の緊密な協力関係による犯罪捜査の高度化をQKD網で支える。

公安情報 ✕ 量子セキュアクラウド網

国の安全保障に係る情報を関係機関にて安全・確実・迅速に共有し、網羅的な対策の実現をQKD網で支える。

主な狙い

- **指揮・統制（C2）通信の絶対的秘匿**
- 衛星・基地・艦艇間の安全通信
- 量子計算時代を見据えた長期安全性

代表的ユースケース

1.軍・政府専用ネットワーク
- 拠点間光ファイバでのQKD
- 国家機密レベルの鍵生成

2.衛星QKD
- 地上局 ↔ 衛星 ↔ 地上局
- 国境を越えた安全鍵配送
- 中国・欧州を中心に実証・運用が進行

3.重要インフラ防護
- 電力・通信・交通の制御ネットワーク
- サイバー攻撃＋量子計算の複合脅威対策

ポイント

・防衛用途ではPQC単独ではなく**「QKD＋PQC」ハイブリッド**が必須（長期機密データはPQCでは秘匿性を保証できない）

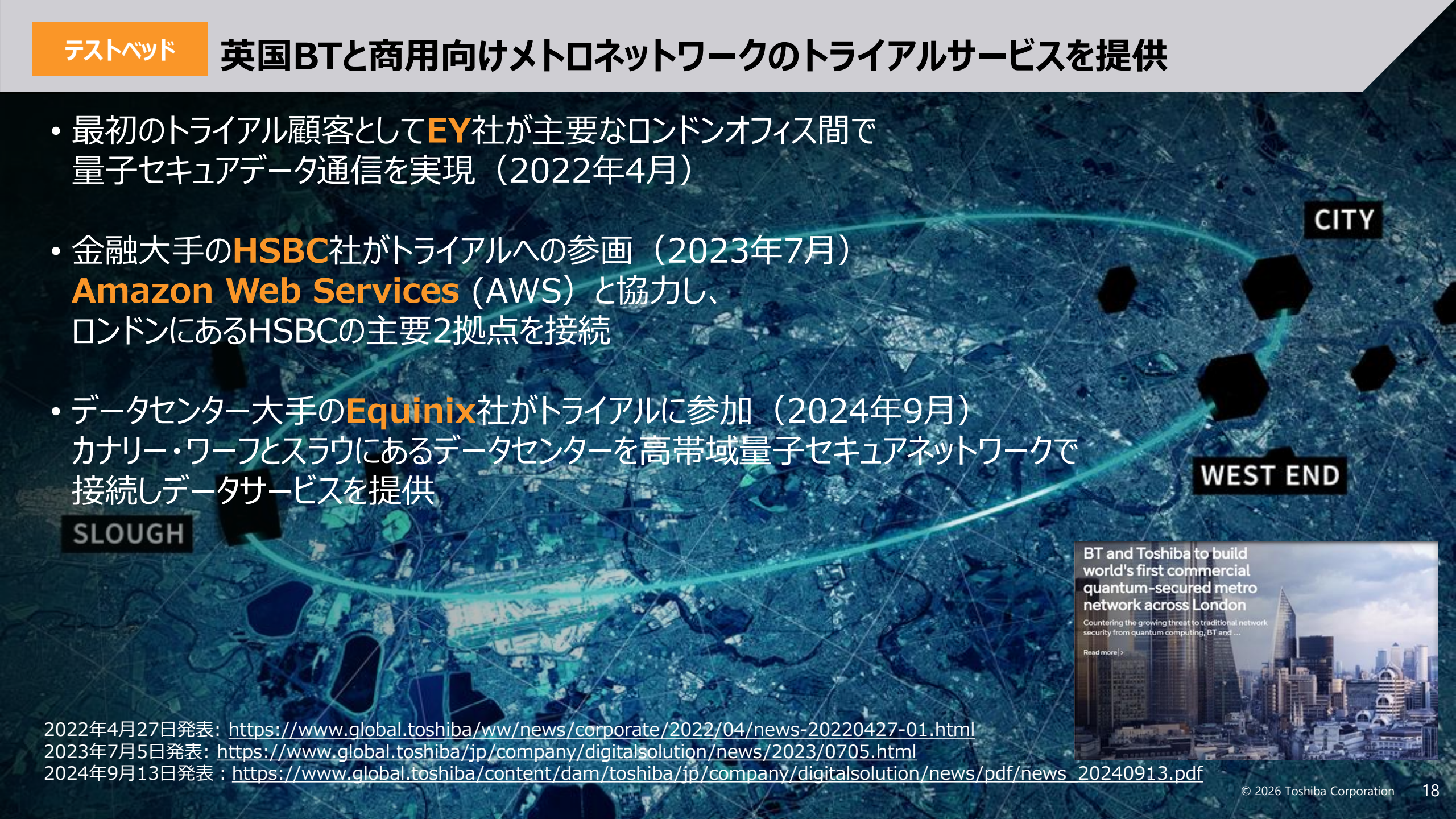
TOSHIBA

Appendix

テストベッド

英国BTと商用向けメトロネットワークのトライアルサービスを提供

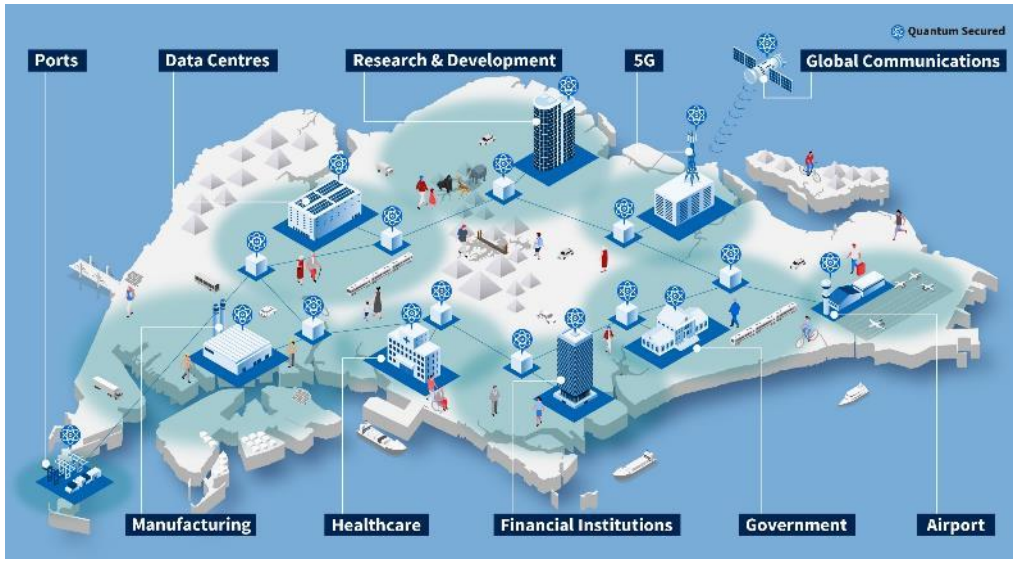
- 最初のトライアル顧客として**EY**社が主要なロンドンオフィス間で量子セキュアデータ通信を実現（2022年4月）
- 金融大手の**HSBC**社がトライアルへの参画（2023年7月）
  Amazon Web Services（AWS）と協力し、ロンドンにあるHSBCの主要2拠点を接続
- データセンター大手の**Equinix**社がトライアルに参加（2024年9月）
  カナリー・ワーフとスラウにあるデータセンターを高帯域量子セキュアネットワークで接続しデータサービスを提供



2022年4月27日発表: https://www.global.toshiba/ww/news/corporate/2022/04/news-20220427-01.html
2023年7月5日発表: https://www.global.toshiba/jp/company/digitalsolution/news/2023/0705.html
2024年9月13日発表：https://www.global.toshiba/content/dam/toshiba/jp/company/digitalsolution/news/pdf/news_20240913.pdf

テストベッド

シンガポールのNQSN+商用トライアルに協力

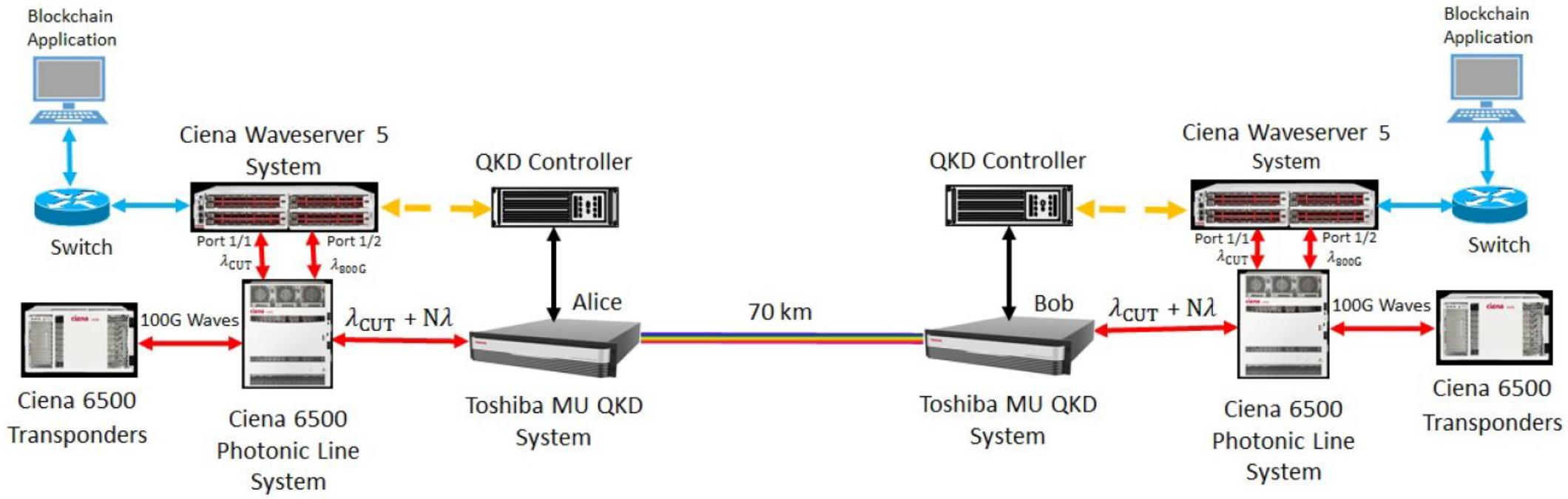


- NQSN+: National Quantum Safe Network plus = シンガポール政府機関が推進する量子セキュアネットワーク商用実証プロジェクト（2024年~2027年）
- 現地パートナーのSpeQtral社、通信サービスプロバイダーのSPTel社に量子セキュアネットワークプラットフォームを提供

- 金融監督庁や大手金融機関が量子セキュア通信の実証実験を実施
- 他業界からも実証実験参加予定

事例　金融アプリケーションで量子暗号通信の実用性を確認

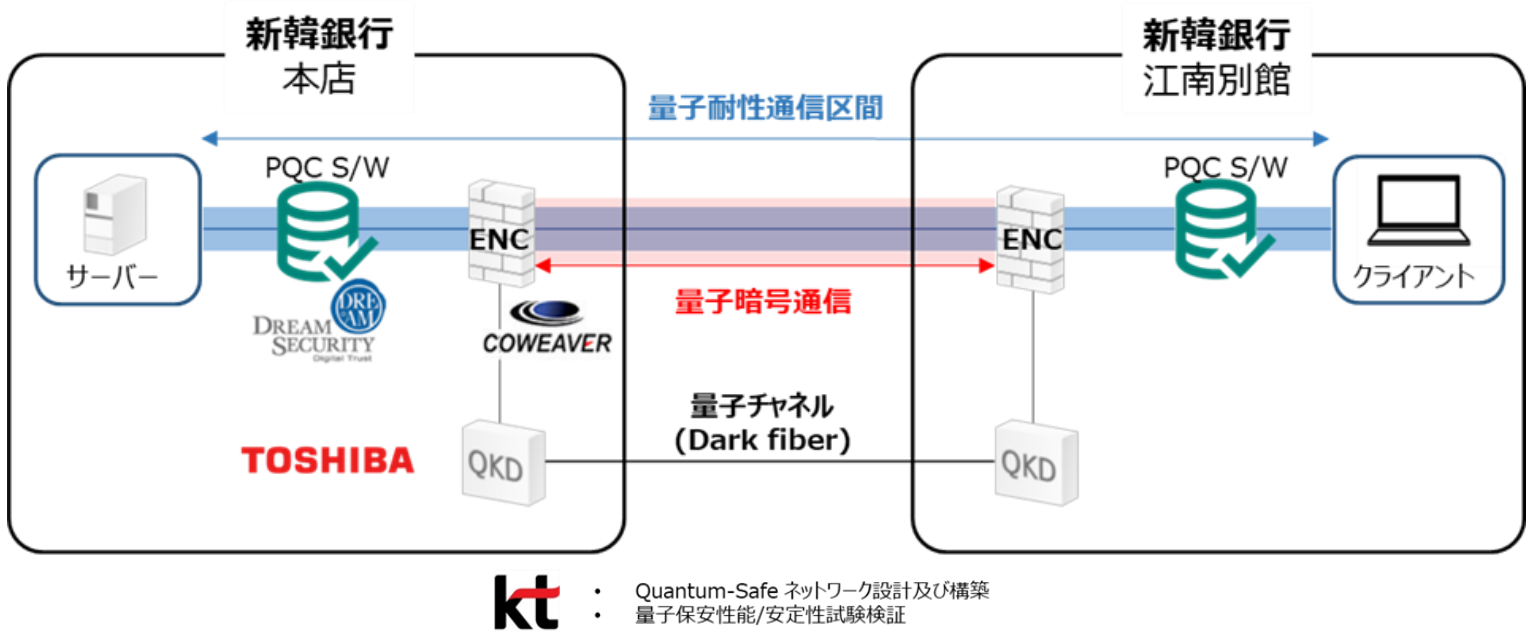
- 東芝アメリカ、JPモルガン・チェース、シエナの3社によるPoC
- 金融分野におけるブロックチェーンアプリケーションで送受される情報を保護するためにQKDネットワークを使用し、大都市において、最大100㎞の距離で、実用レベルの800Gbpsの伝送速度で暗号通信が可能であることを確認
- 高速大容量かつ低遅延なデータ伝送が厳格に求められるミッションクリティカルな金融分野において、盗聴者を即座に検出・防御し、来る量子コンピューター時代において、より安全で効率的なネットワークの構築が可能であることを実証



- **2022年2月18日発表**：https://www.global.toshiba/jp/company/digitalsolution/news/2022/0218.html
- 本実証実験の技術成果（英文）：https://arxiv.org/abs/2202.07764

事例　金融ネットワークのサイバーセキュリティ強化に向けハイブリッド量子セキュア通信を実証

- 韓国の大手通信事業者**KT Corporation（KT）**、および大手銀行の**新韓銀行**とのコラボ
- 量子計算機を用いたサイバー攻撃の脅威から金融ネットワークを保護するため、量子暗号通信（Quantum Key Distribution：QKD）と耐量子計算機暗号（Post Quantum Cryptography：PQC）を結合したハイブリッド量子セキュア通信を実証
- 3社が連携し、ソウルにある新韓銀行本店と江南別館の約22km区間を結ぶ実証網を構築し、盗聴をブロックし光回線の物理層を保護するQKDと、インターネットセキュリティプロトコルに適用してホームページログインなどのアプリケーションサービスを保護するPQC公開鍵アルゴリズムによるハイブリッド量子セキュア通信の評価を行った
- また、本実証には韓国企業のCoweaverとDream Securityが技術協力を行った。Coweaverは、KTから技術移転を受けた量子通信対応回線暗号装置（Encryptor: ENC）を本実証網に適用し、当社のQKDシステムで生成された秘密鍵を受けてデータを暗号化し、物理層のデータ伝送を保護した。Dream SecurityはKTと連携し、アプリケーション層保護のためのPQCサービスを提供した。



2024年4月19日発表：https://www.global.toshiba/jp/news/digitalsolution/2024/04/news-20240419-01.html

事例 QKDを用いた原子炉遠隔制御の量子セキュア通信実証

- 米パデュー大学原子核工学部(Purdue University School of Nuclear Engineering)は、米エネルギー省のオークリッジ国立研究所(Oak Ridge National Laboratory) および東芝と共同で、東芝のQKD技術を活用し、パデュー大学原子炉1号機(PUR-1) における量子セキュア通信の実証を行った。
  https://arxiv.org/abs/2505.17502

- 実証では最大135kmの距離まで安全かつ遅延のない監視を実現。
  また、障害による鍵配送不能時においても、鍵プールによりOTPベースの暗号化で最大82km、AESベースの暗号化で最大140kmで
  リアルタイム暗号化データ交換が継続可能であることを実証

OTP：One Time Pad　AES：Advanced Encryption Standard

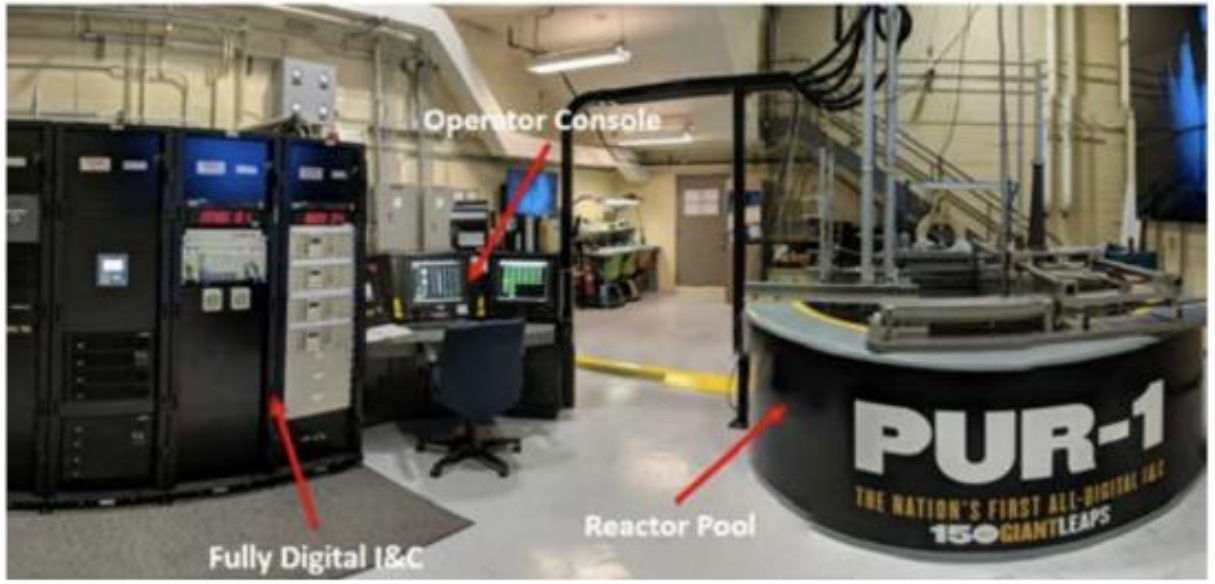
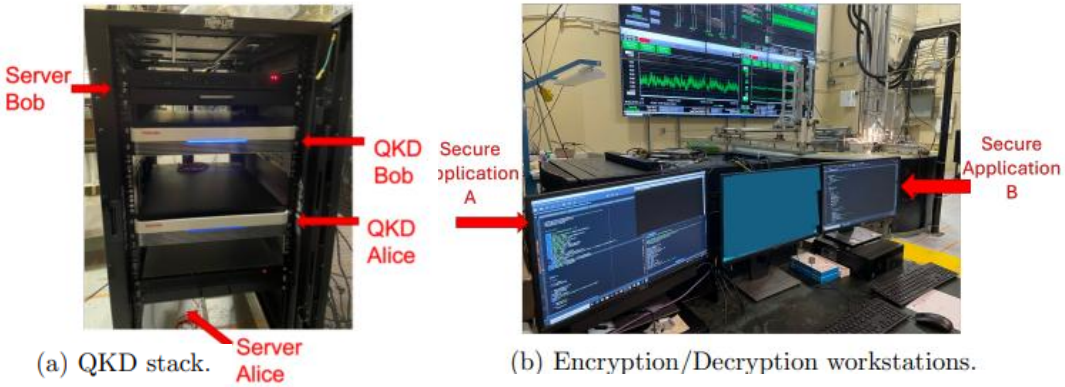
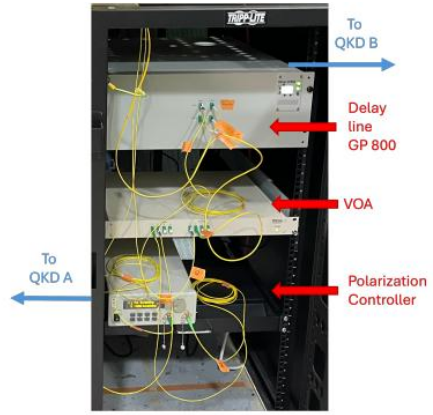


Figure 4: PUR-1 reactor room.



(a) QKD stack.　(b) Encryption/Decryption workstations.



(c) Equipment intercepting quantum and classical channel. Red arrows identify the devices, while blue arrows indicate integration with the QKD system.

Figure 5: QKD installation in PUR-1 control room.