

量子暗号通信の現状と課題

総務省 情報通信審議会 技術戦略委員会 ヒアリング資料

株式会社東芝
2024年11月

TOSHIBA

© 2024 Toshiba Digital Solutions Corporation

01

量子暗号通信とは

進化するサイバー攻撃の脅威

将来への備え

量子コンピュータによる暗号解読

量子コンピュータが、現在広く利用されている暗号アルゴリズムを短時間で破る可能性
大規模な量子コンピュータが**完成する前に対策が必要**

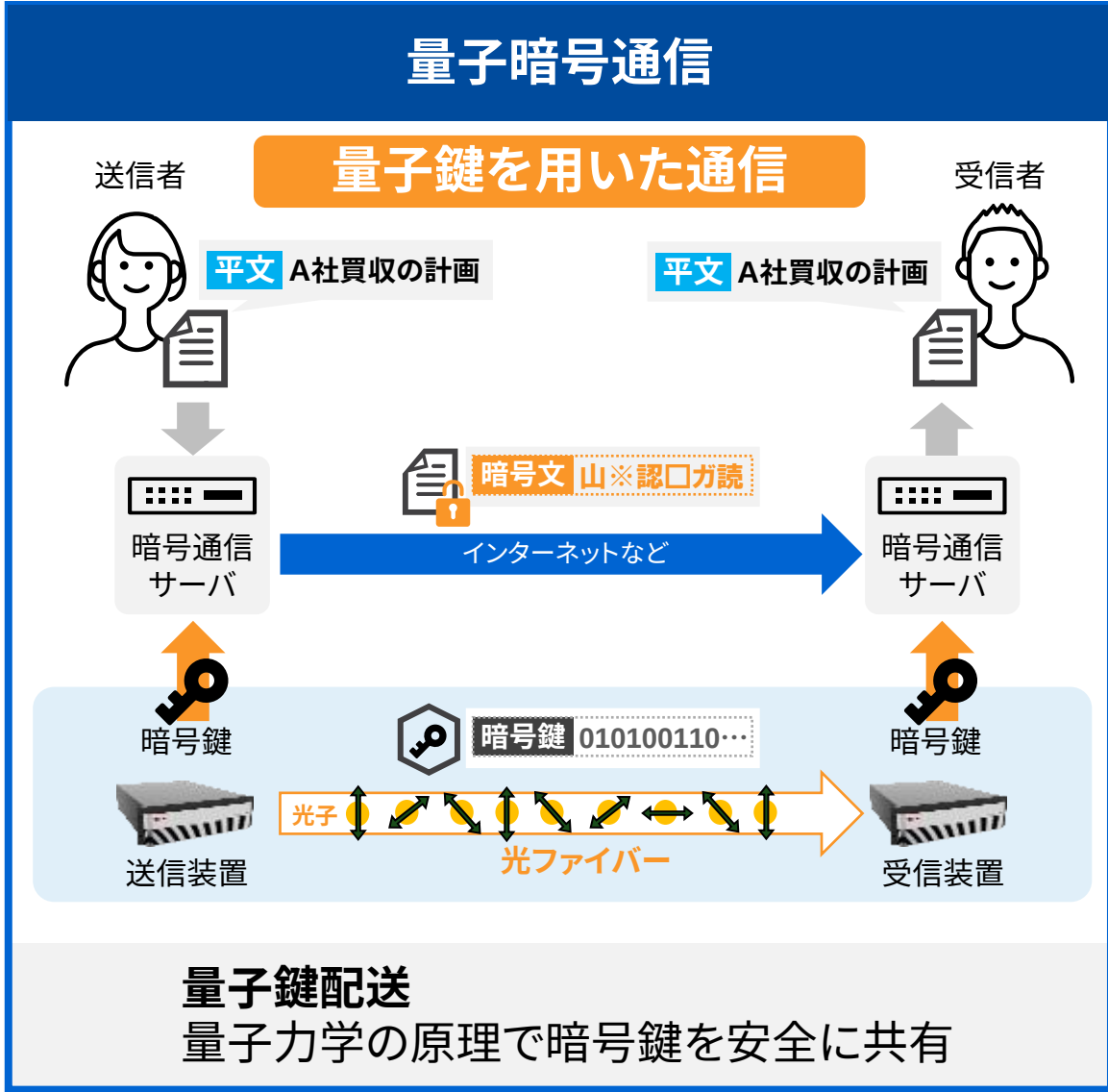
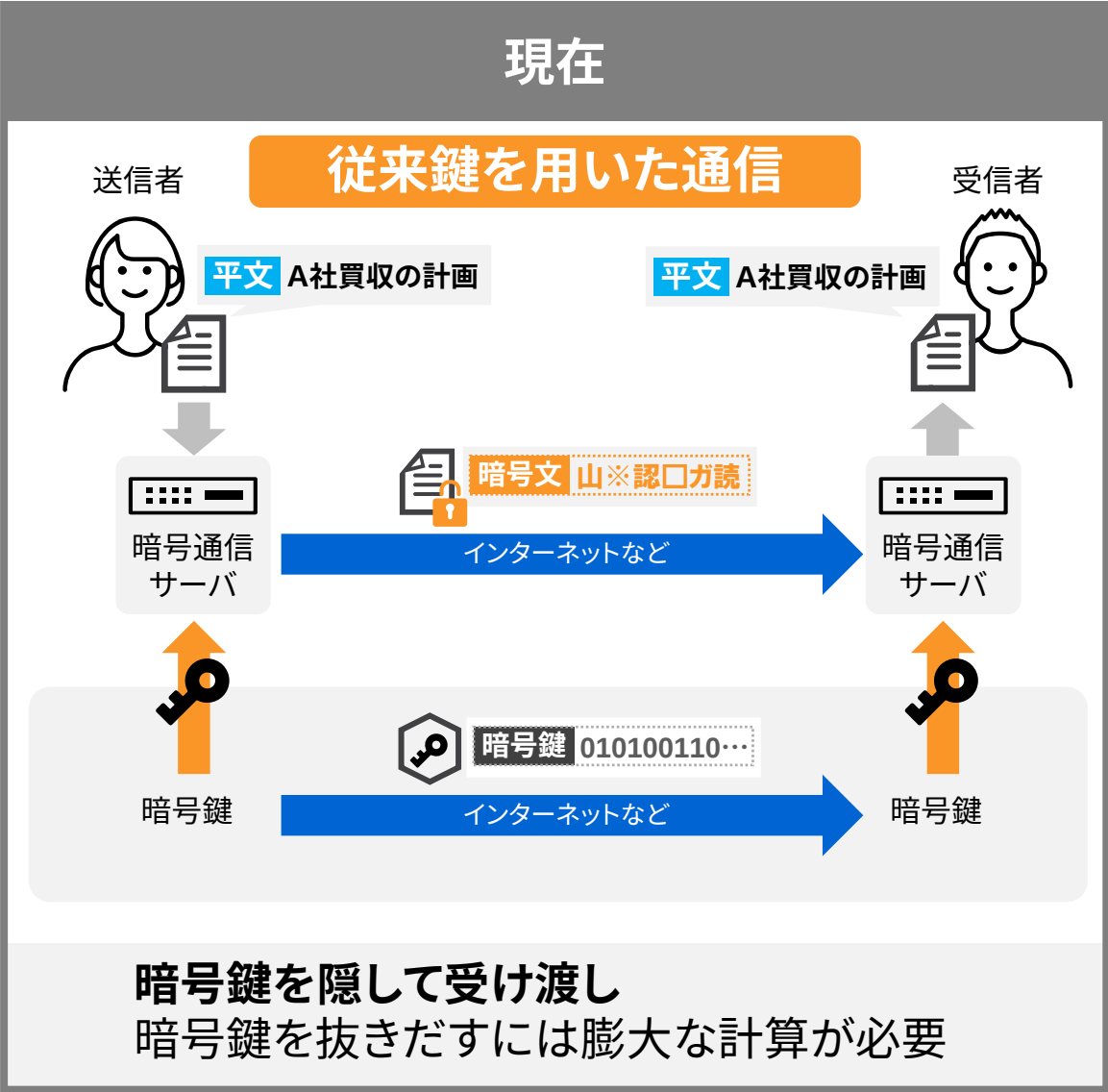
現在の課題

データ・ハーベスティング (Harvest Now, Decrypt Later: HNDL attack)

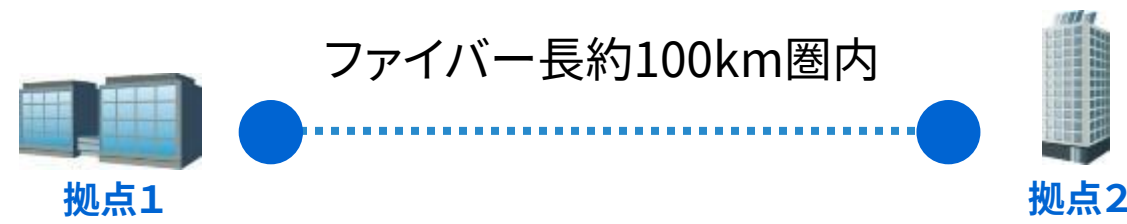
- 暗号化されたデータを傍受し保存しておき、時間をかけて解読する攻撃
- 「**現在の通信データ**」も将来**解読される可能性**

量子コンピュータに対抗できるソリューションが今から必要
量子力学に基づく新しいセキュア通信 = 「量子暗号通信」

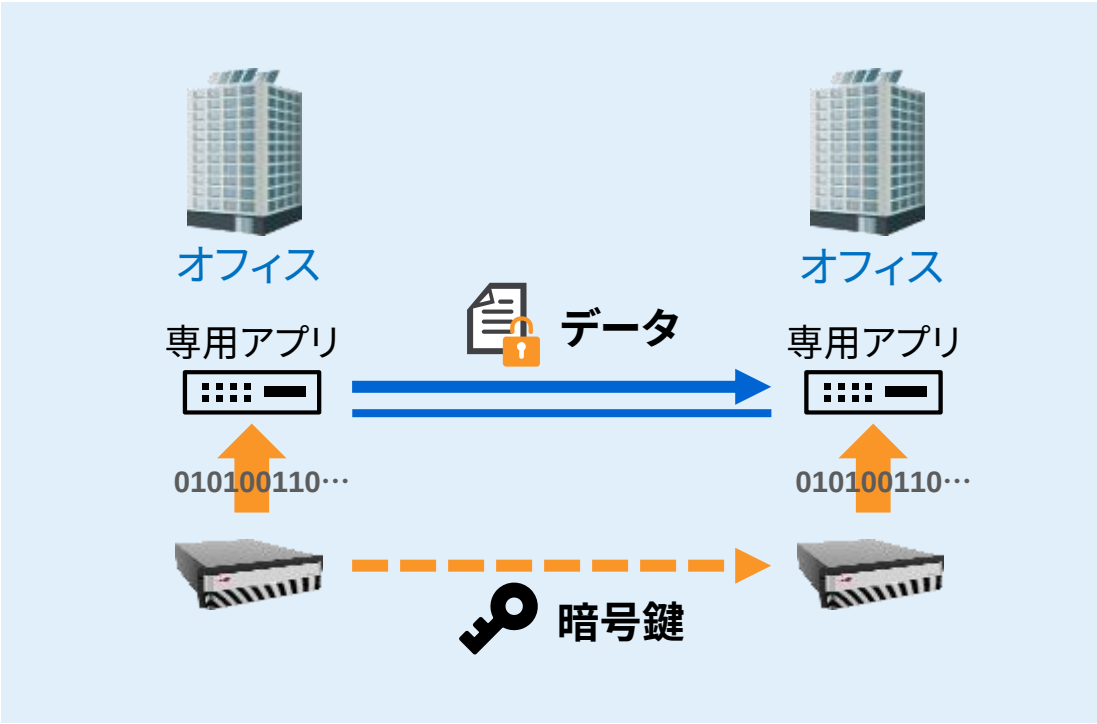
現在の暗号通信方式との比較



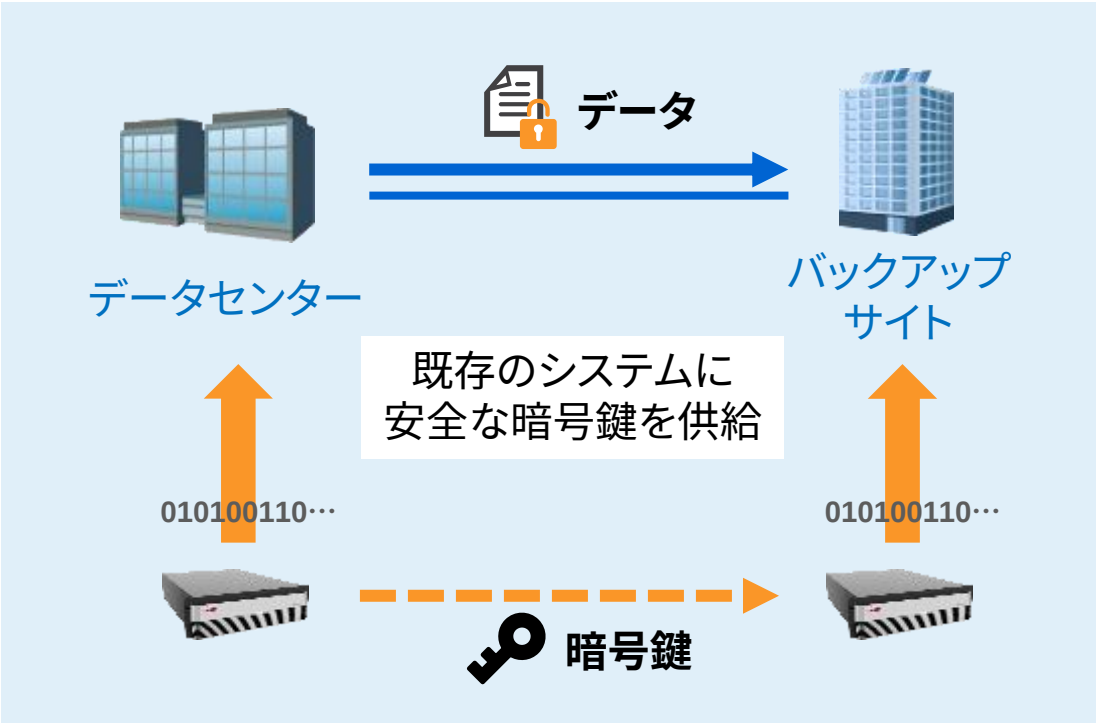
構成例1：ファイバーで直接接続可能な2拠点間の通信



アプリケーションも含めた専用のシステム



既存の暗号通信システムへの組み込み

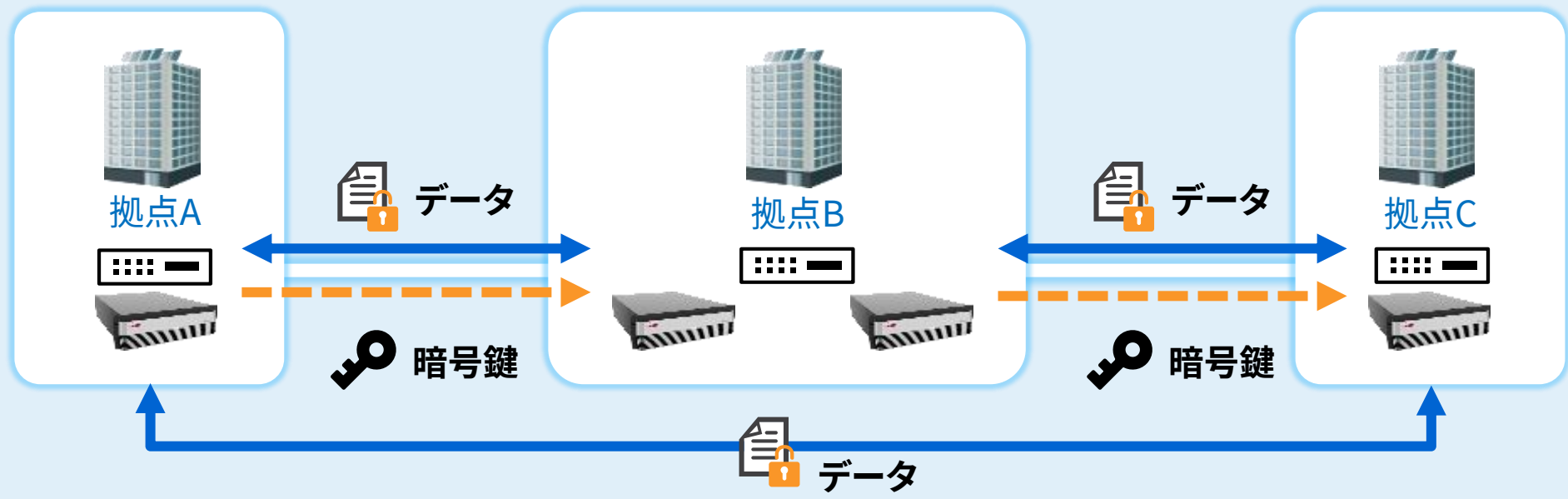


構成例2：長距離化・ネットワーク化(1/2)



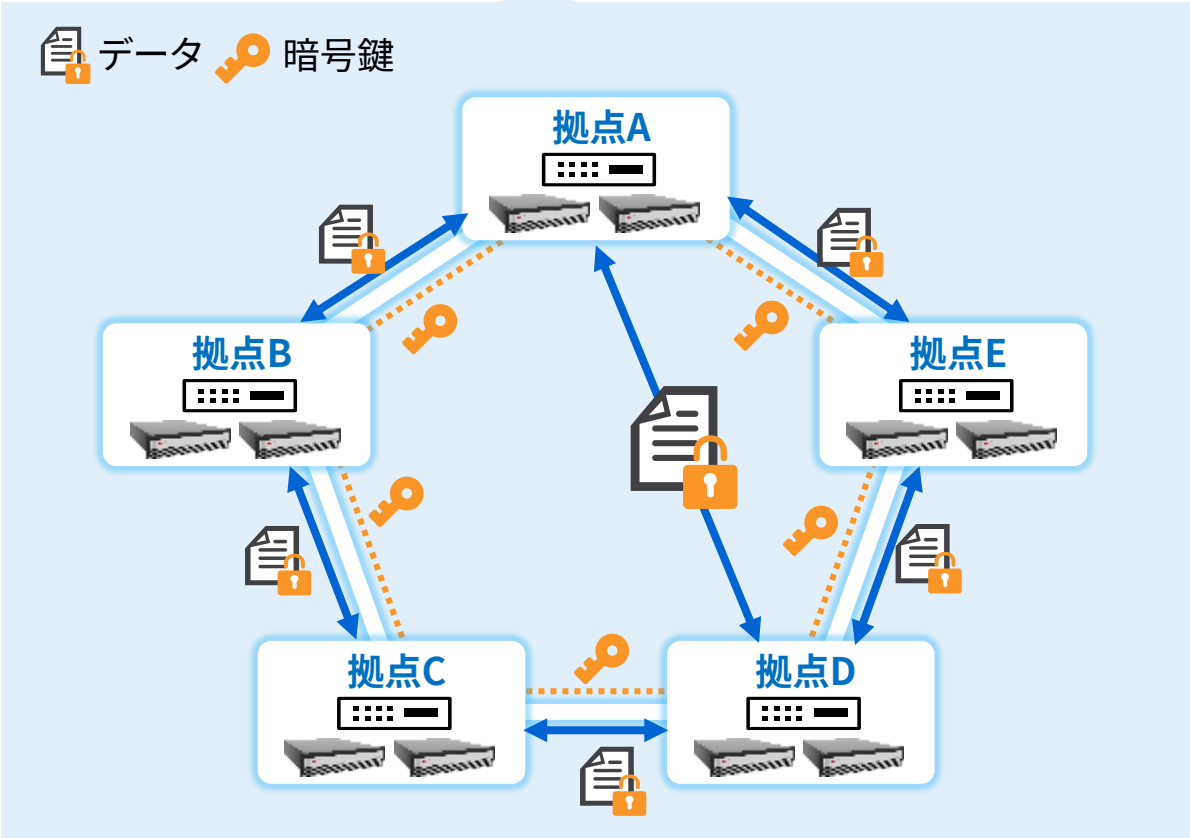
量子暗号通信は、通信距離に制約がある(100km程度)

複数の量子暗号装置を数珠つなぎにする等してネットワーク化することで、
任意の距離・拠点間で暗号鍵共有・暗号通信が可能となる。



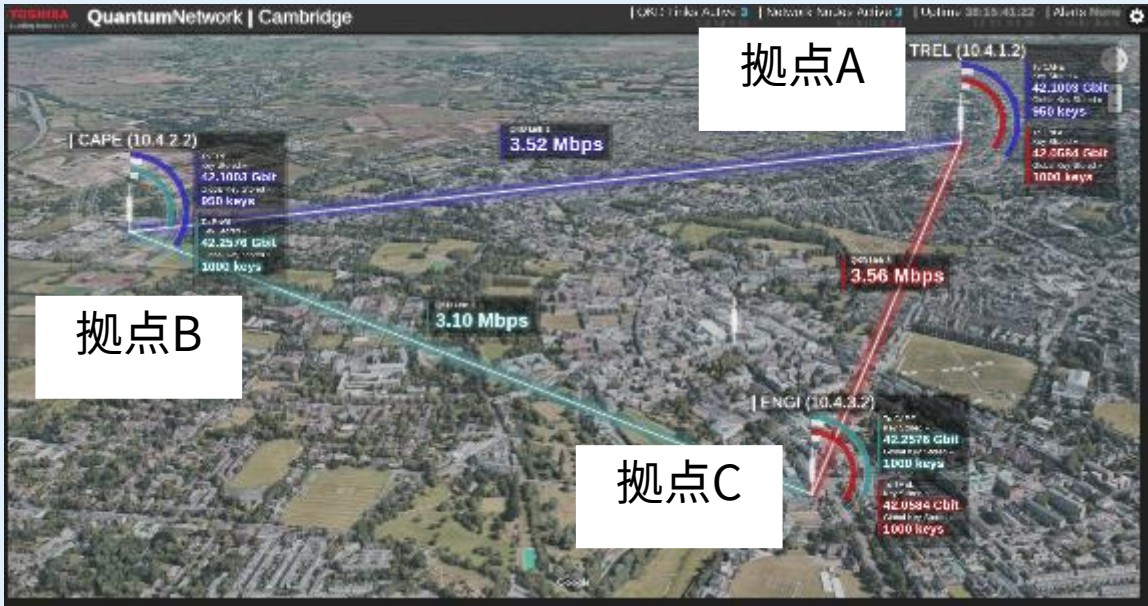
構成例2：長距離化・ネットワーク化(2/2)

5拠点リングネットワークの例



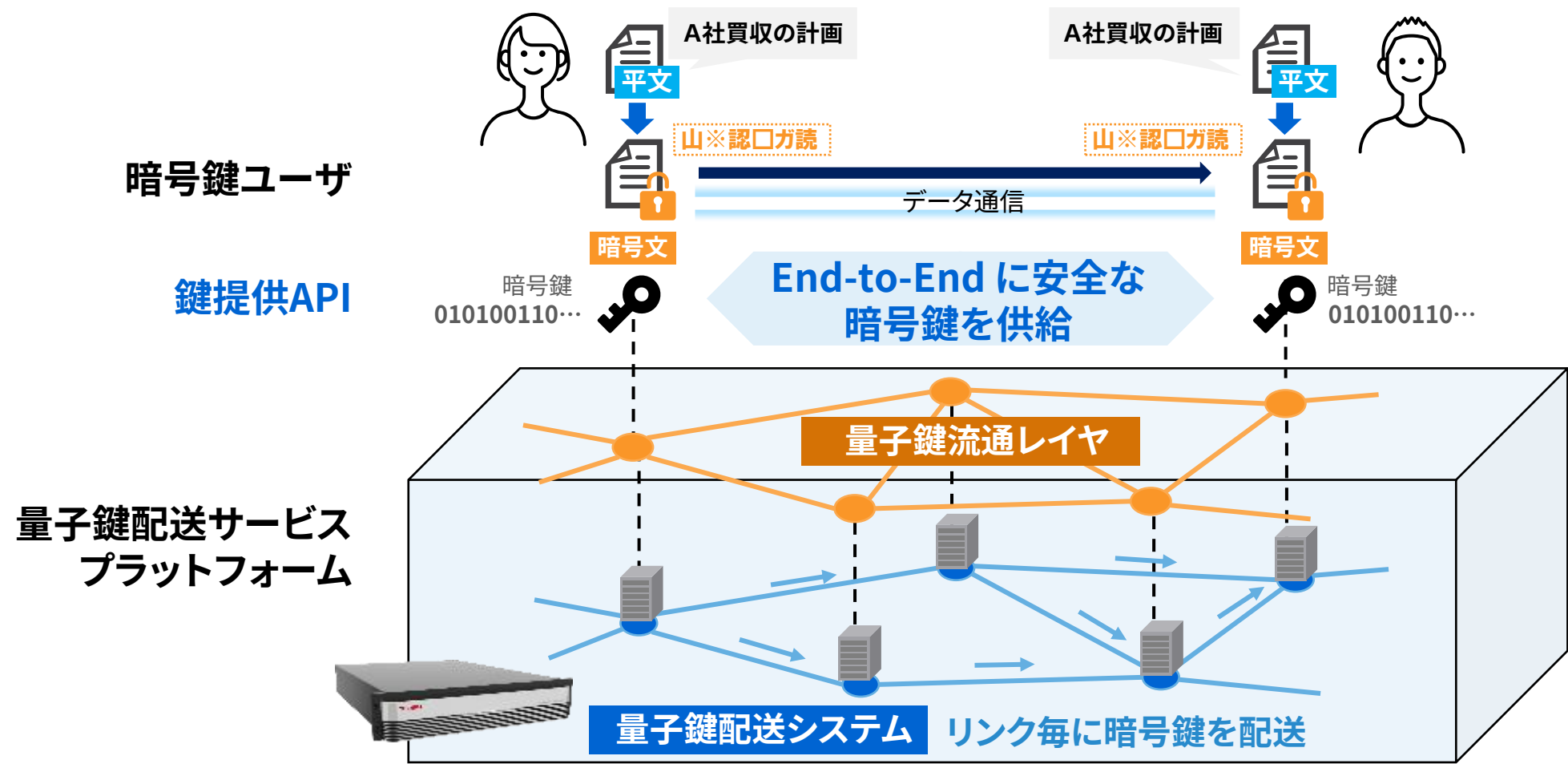
3拠点リングネットワークの例

英国のプロジェクトにて3拠点のリングネットワーク等を検証(2017年~)



アプリケーション・ユースケースに応じて、
様々なネットワーク形態(リング・メッシュ・二重化等)が実現可能

構成例3：暗号鍵供給インフラとして



安全な暗号鍵を供給するサービスプラットフォーム
任意の2地点に安全な暗号鍵を供給

02

市場動向

量子インターネット時代の到来

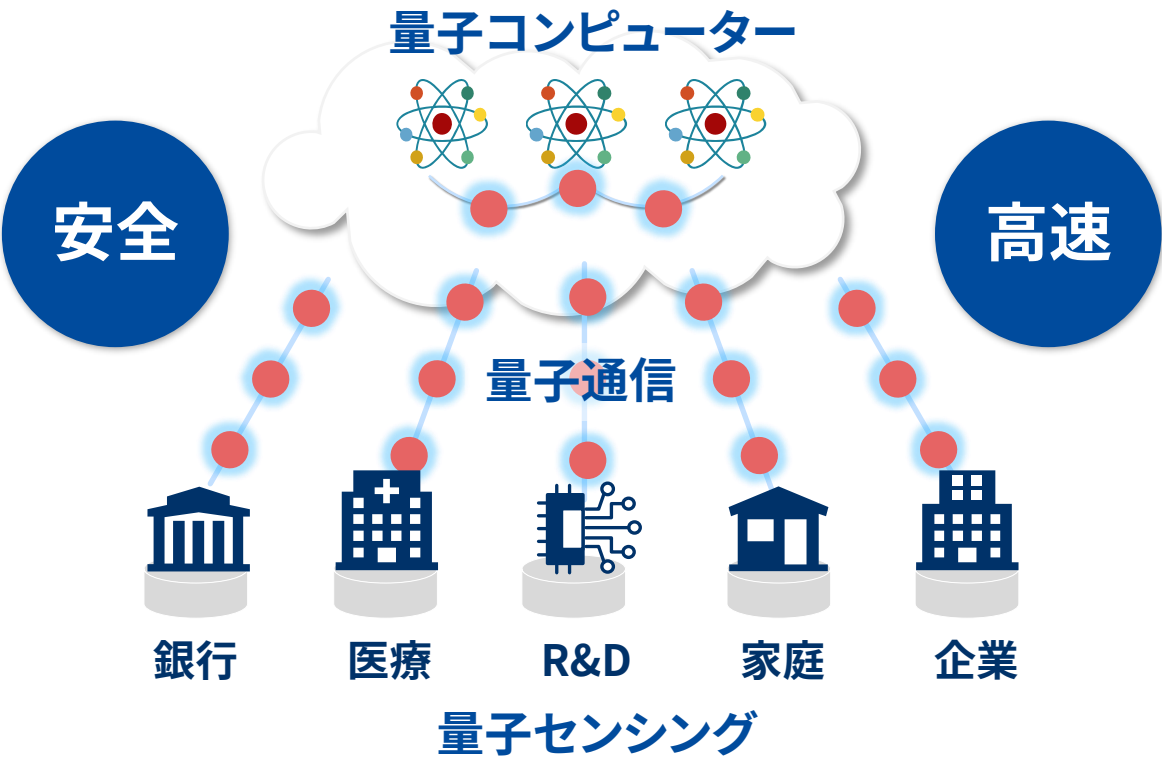
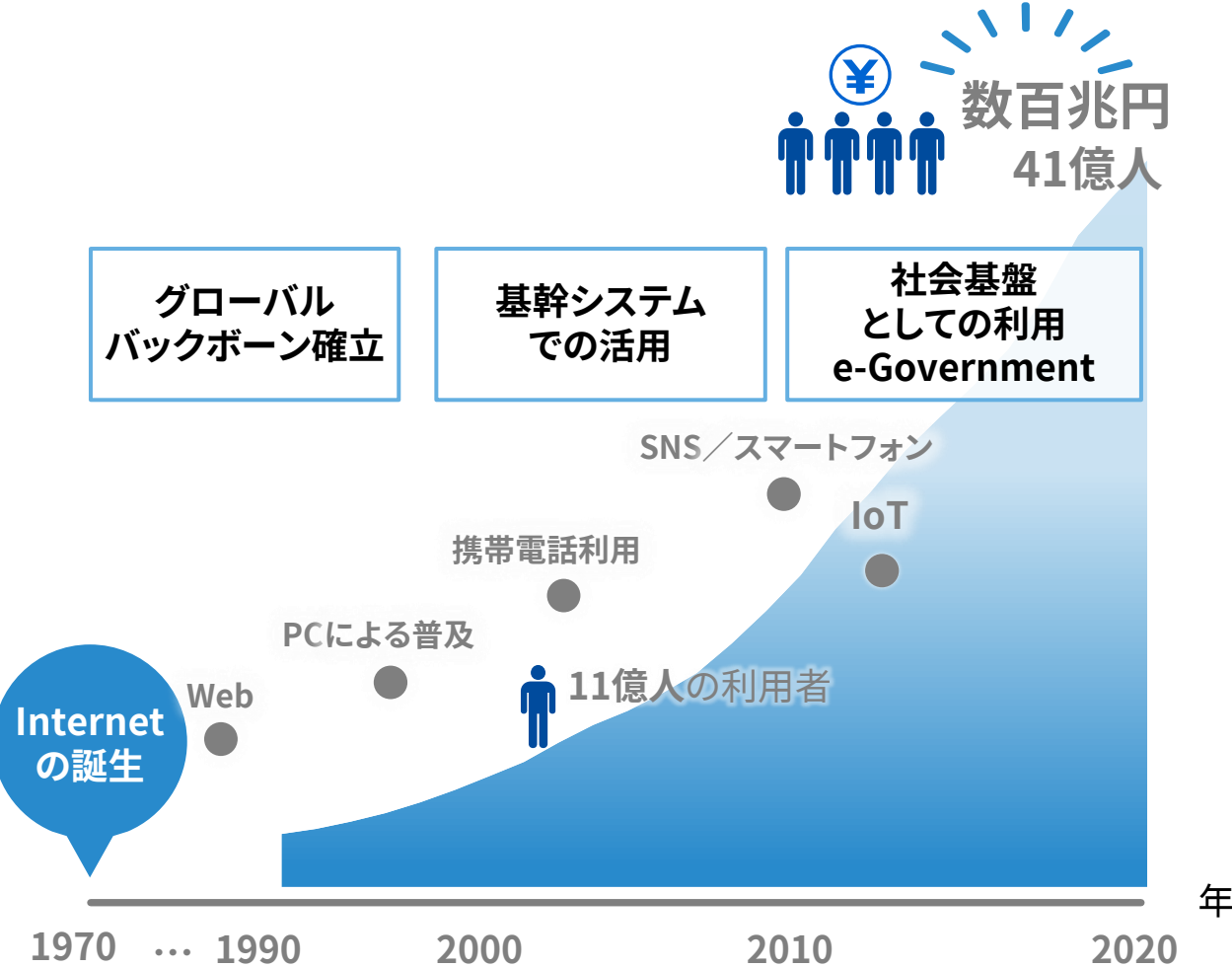
インターネット

50年で数百兆円の産業を創出

次の50年

量子インターネット

量子コンピュータ、量子センシング
量子通信・暗号の融合による、
安全で高速な情報インフラ



先行国の動向

* 2024年11月時点

ロシア：中国連携の動き

- 2024年にモスクワ近郊と中国ウルムチ近郊の間で、中国製衛星を使った量子鍵配送に成功

中国：広域インフラを構築

- 2017年世界初の衛星地上間での量子鍵配送実験に成功(距離1200km)
- 北京・上海・他、中国全土に10,000kmを超えるQKDネットワークを敷設

日本：量子技術イノベーション戦略に基づく、研究開発・実証を推進

- NICTが中心となり運用される東京QKDネットワークをベースとした研究開発・実証や、金融・医療分野をターゲットとした社会実装PoCを、総務省・内閣府等の国家PJにより推進

米国：DOEやDARPAが量子インターネットの研究推進

- エネルギー省(DOE)配下で17の研究機関が量子関連技術の研究開発を推進
- 2020年に量子インターネットのブループリントを公開
- 2023年DARPAがQuantum Augmented Network (QuANET)開発への参画公募を開始

欧州：全域でQKDネットワーク実装活発化

- 2022年よりEU27カ国参画のQKDの社会実装プロジェクトEuroQCI (Quantum Communication Infrastructure)が始動。デンマークでは、防衛省・外務省も参画

韓国：国家政策として推進

- 韓国版ニューディール政策の一環で、「K-サイバー攻撃防疫」の中で「量子暗号通信網構築モデル事業」を策定し推進中
- ドローンと組み合わせた非武装地帯警備トライアル等を実施
- 2022年7月に通信大手のKTとSK Broadbandが相次ぎ量子暗号専用回線サービスを発表
- 2022年、SK BroadbandとIDQが総延長800kmに渡る48の政府機関を結んだQKD網を構築開始

インド：防衛利用が進む

- 防衛省(MoD)がQKD実証に成功。陸軍が調達プロセスを開始

シンガポール：国家規模のQKD網を構築

- 2023年に商用実証プロジェクト National Quantum Safe Network Plus (NQSNet+)が発表され、2024年に商業利用テストベッドが始まる

QKDネットワークの社会実装、防衛用途の利用検討が進行



中国動向#4 中国全域の量子暗号通信基幹網を構築中



National Wide-area Quantum Secure Communications Backbone Network



Finance

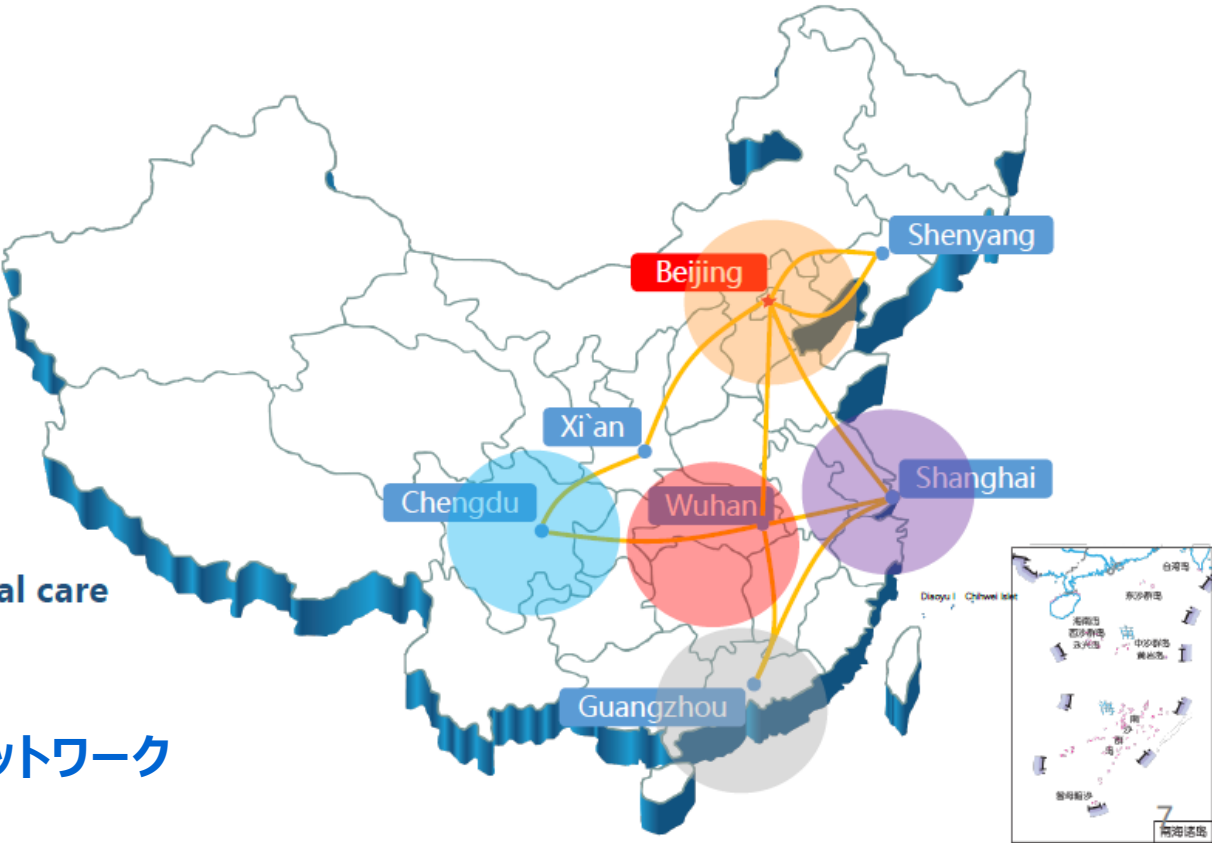


Customs

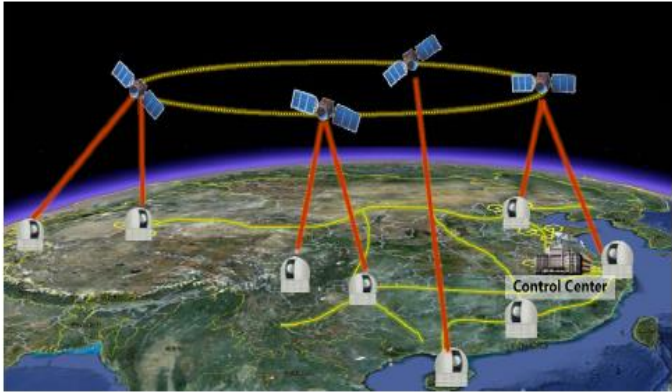


Health and medical care

地上系量子暗号ネットワーク



衛星量子暗号ネットワーク



Our Plan

- ~2022: 2 Satellites, 10 Ground Station
- ~2030: 5~8 Satellites, 100 Ground Station

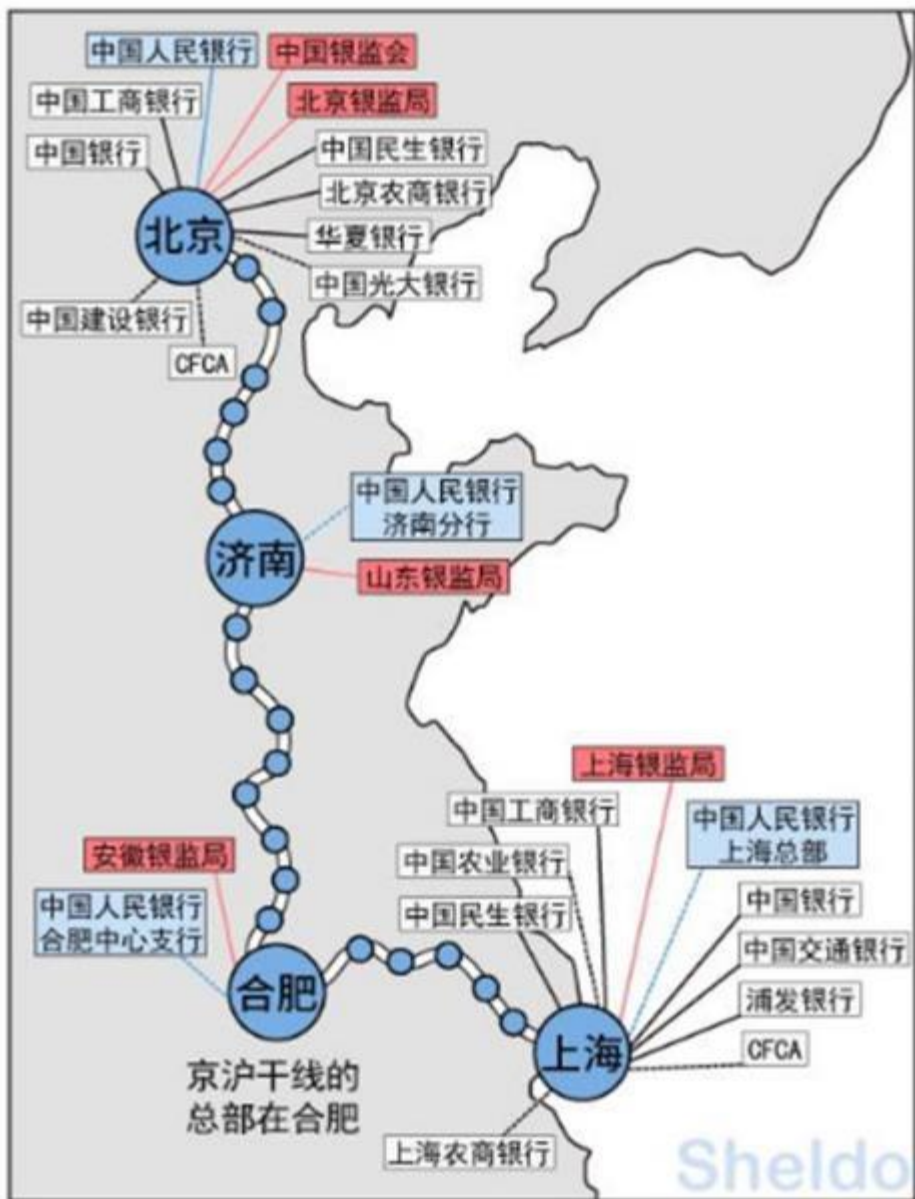
将来の量子インターネットでの覇権を見据え、地上＋衛星で着々と準備中



中国动向#3 中国大都市圏の量子暗号通信インフラ整備状況

出典: "Large-scale quantum network: From Intra-city to Inter-city to Global", Yu-Ao Chen, QCrypt 2018





QKDの用途

各種規制情報の収集 (Regulatory Information Collection)

外国取引情報の収集 (Foreign Transaction Information Collection)

長距離のデータバックアップ (Long-distance Disaster Recovery)

インターネットバンキング取引 (Real-time Internet Banking Transaction)

システム保全情報の暗号化 (System Maintenance Key Encryption)

各拠点内でのデータバックアップ (Area Network Data Transmission for Disaster Recovery)

Source (Chinese): https://www.sohu.com/a/195807595_177021



(2020/09/11付けHerald経済記事より抜粋)

韓国政府は2020年7月14日、covid-19以降の景気回復のための国家プロジェクト 「韓国版ニューディール政策」を確定・発表

該当する分野への投資と雇用創出の計画



2022年まで
67兆7000億ウォン
を投入



雇用創出
88万7000人



2025年まで
160兆ウォン
を投入



雇用創出
190万1000人

この政策に沿って量子暗号通信網を推進

KT、SKブロードバンド、LGU+等が公共・医療・産業分野の量子暗号通信網事業者として選定

(9月11日 韓国科学技術情報通信部「K-サイバー防疫」3次補正予算事業着手報告会にて表明)

<量子暗号通信モデル事業 選定結果>

分野	主管機関	需要先
公共	SKブロードバンド	広州市長
	KT	全羅南道庁(海軍3艦隊)、江原道長(春川市長)
医療	SKブロードバンド	延世医療院
	KT	ソウル聖母病院、恩平聖母病院
	LGU+	ウルジ大学病院
産業	SKブロードバンド	Hanhwaシステム、ウリ銀行、CJオリーブネットワークス
	KT	現代重工業
	LGU+	LGイノテック

「K-サイバー攻撃防疫」とは？

サイバー安全網を構築する事業である。この中で「量子暗号通信網構築モデル事業」は高度なセキュリティを要する公共・医療及び産業部門に量子暗号通信網を構築することが骨子である。これを通じて応用サービスを発掘、実証を支援し、公募を通じて選定された8つのコンソーシアムで事業を推進する計画。公共部門はKTとSKブロードバンドが主管する。医療、産業部門はKT、SKブロードバンド、LGU+が担当する。情報通信技術(ICT)の中小企業がコンサルティング費用及び最大1500万ウォンの製品導入費用を支援される「ICT中小企業情報保護力量強化事業」も今回の補正予算に含まれた。

量子通信の欧州の地位を強化するための量子鍵配送テストベッド



目的

量子通信の最前線で欧州の世界的な地位を強化する

期間

2019年9月～2022年9月(3年間)

予算

1,797万€(EU助成金:1,500万€) by HORIZON EUROPE 2020

概要

欧州13か国の主要通信機器メーカー、エンドユーザー、ネットワークオペレーター、QKD機器プロバイダー、科学者などが結集し、量子通信分野での欧州の地位を最前線で強化する。長距離リンク、衛星を用いた量子鍵配送の研究など、汎欧州の量子ネットワークの土台を作る。

EUの通信インフラを量子鍵配送で耐量子化するプロジェクト



目的

研究分野での欧州地域のリーダーシップの統合、優位性の拡張、競争力の確保

期間

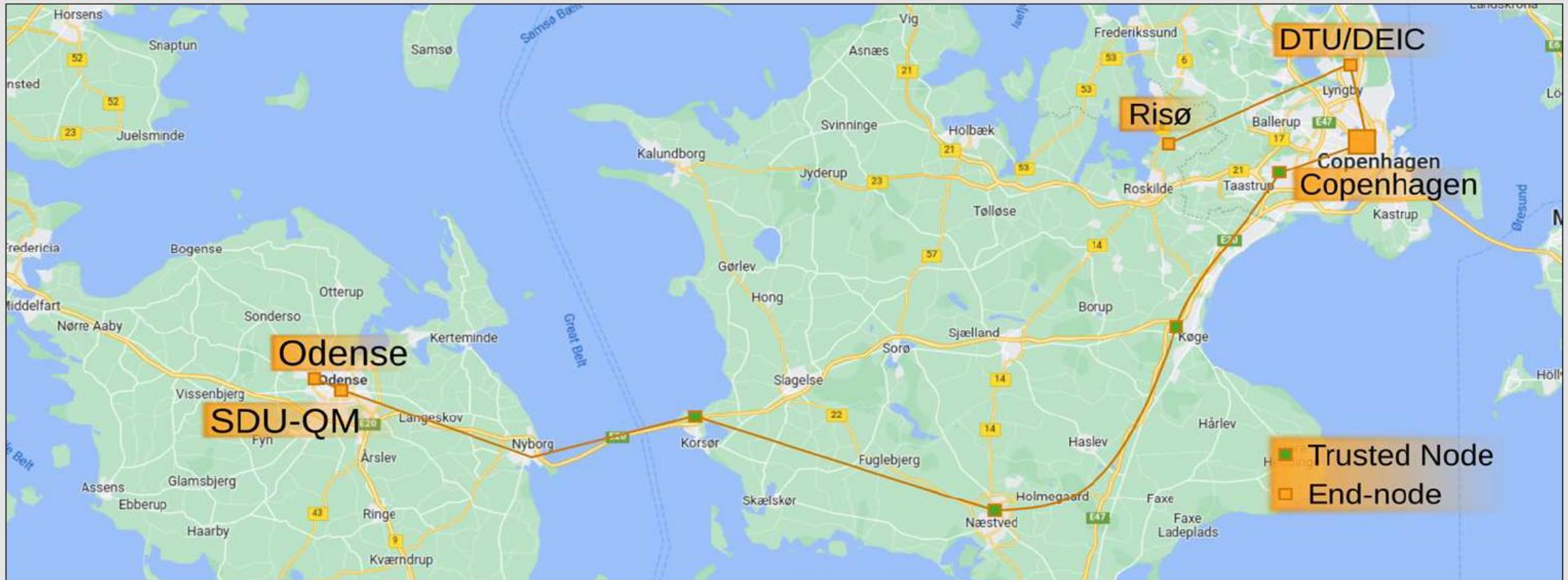
2022年～2027年

概要

最初のサービスは量子鍵配送で初期のユーザーはEU加盟国の官庁・政府機関を想定し、欧州の重要産業施設をサイバー攻撃から守ることを図る。
2021年11月にプログラム実施概要が発表され、2023年中に推進される見込み。



長距離 QKD ネットワーク (EuroQCI デンマークの例)



- ・コペンハーゲンとオーデンセ間の接続
- ・~200 km
- ・信頼できるnodeのネットワーク

NQSN (National Quantum-Safe Network) が立上がる

- NQSN (2022~);
 - 量子暗号通信基盤の構築とユースケース実効性実証を行う

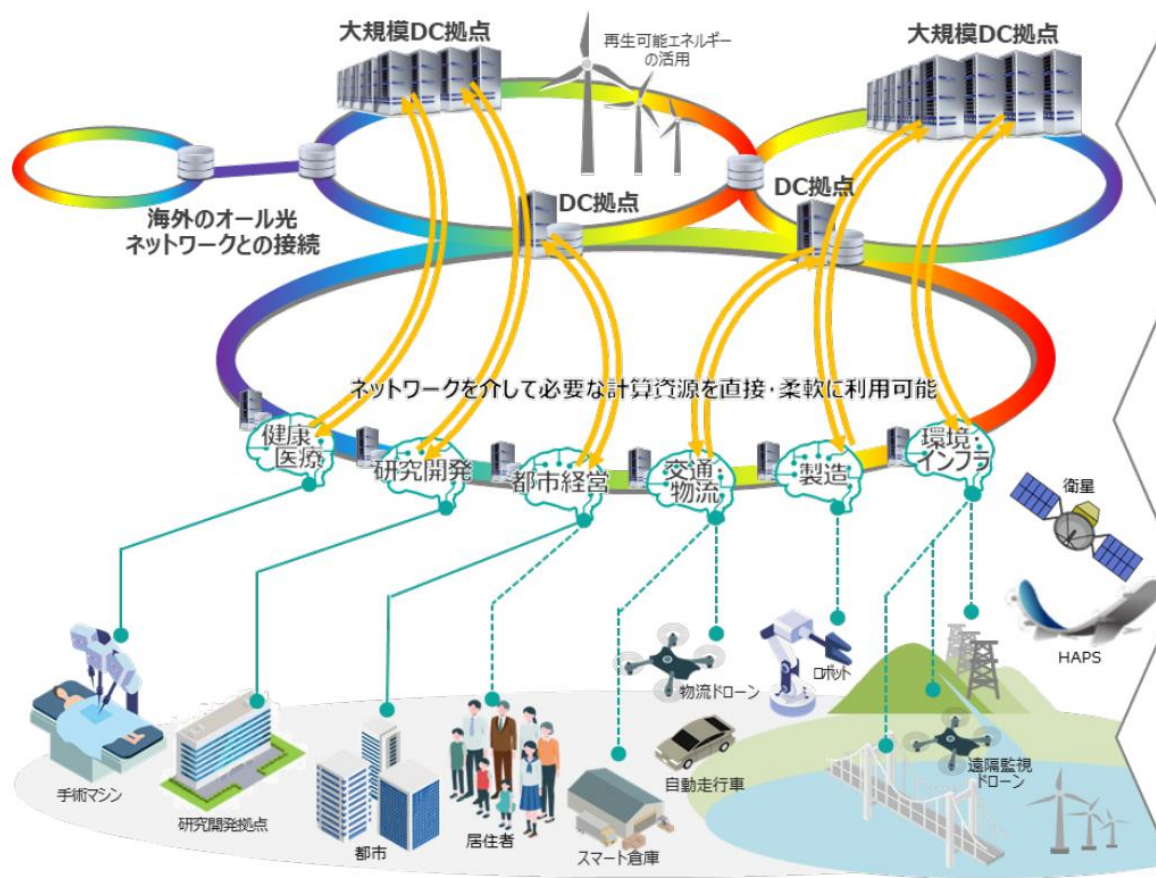


出典:<https://www.nqsn.sg/>

- NQSN Plus (2023~);
 - 政府機関と企業が一体となり参加し、商業利用を促進する
 - ✓ IMDA発表:<https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-launches-southeast-asias-first-quantum-safe-network-infrastructure-to-help-businesses-tap-on-quantum-safe-technologies>

日本の取り組み ～ 2030年代のAI社会を支えるデジタルインフラ像

2030年代のAI社会を支えるデジタルインフラとして、個別分野に特化した小規模・分散化した多数のAIや、これを駆動するデータセンター等の計算資源群を連携させ、モノ（自動車、ドローン、ロボット等）やセンサーを含む多様なユーザとを場所を問わずに繋ぐことが可能な、低遅延・高信頼・低消費電力な次世代情報通信基盤（Beyond 5G）が求められている。



データセンター等の計算資源

- ・オール光ネットワーク等と一体的に運用されるデータセンター等の計算資源が、様々な分野で利用される多数のAIを駆動
- ・オール光ネットワークで繋ぐことにより距離の制約が緩和され、現在、大都市圏に集中するデータセンター拠点を、再生可能エネルギーが活用可能な地域等へと分散化が可能

オール光ネットワーク（APN）

- ・今後増大が予想される大量のデータを低遅延・高信頼・低消費電力で流通させるための基幹的なインフラとして位置付け
- ・特に、計算資源・ユーザ等を連携させ、必要な計算資源を直接・柔軟に利用可能とすることで、我が国のAI開発力の強化やAI利用を促進するゲームチェンジャーとなることが期待

非地上系ネットワーク（NTN）

無線アクセスネットワーク（RAN）

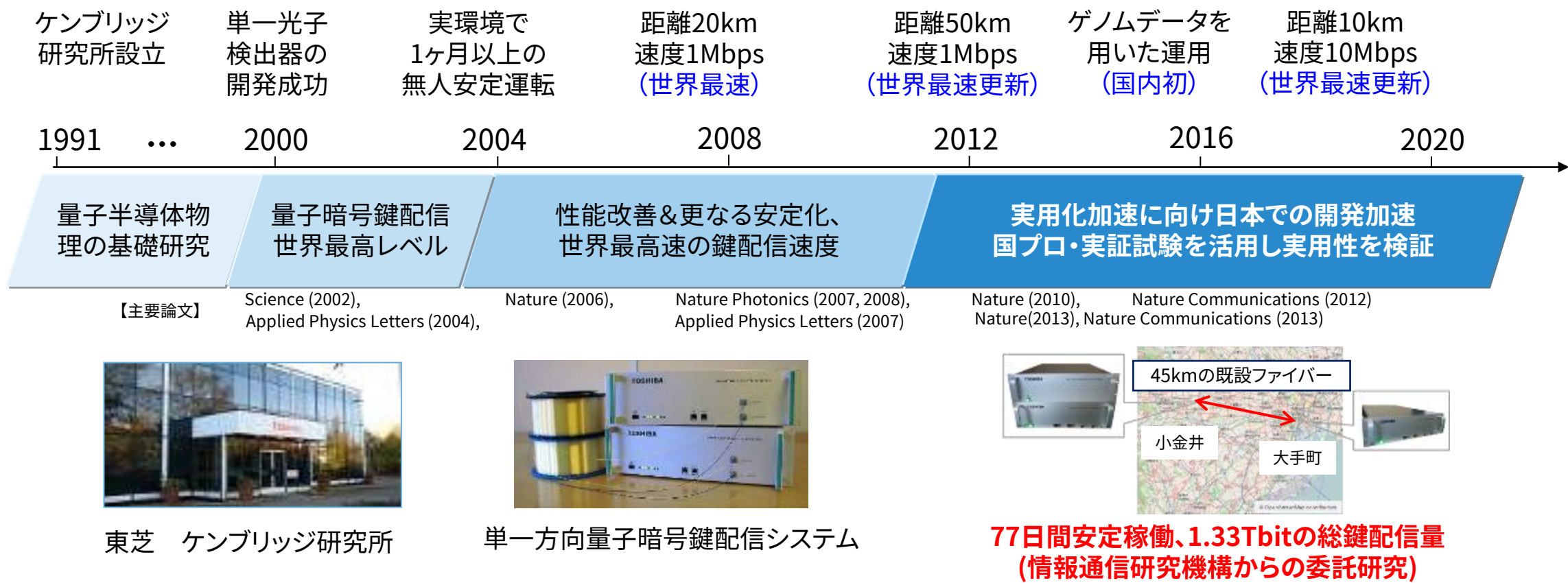
- ・ヒトよりも、モノ（自動車、ドローン、ロボット等）や、環境を把握するセンサー等が主たる端末となって、「産業のワイヤレス化」を加速
- ・RANやNTN（衛星・HAPS等）等からなる複層的なネットワークにより、非居住地域も含め、どこでも繋がる環境を実現

低環境負荷（グリーン）で安全・安心で信頼できるAIが社会全体で提供され
社会課題の解決や我が国の競争力に繋がるイノベーションを加速

03

東芝の取り組み

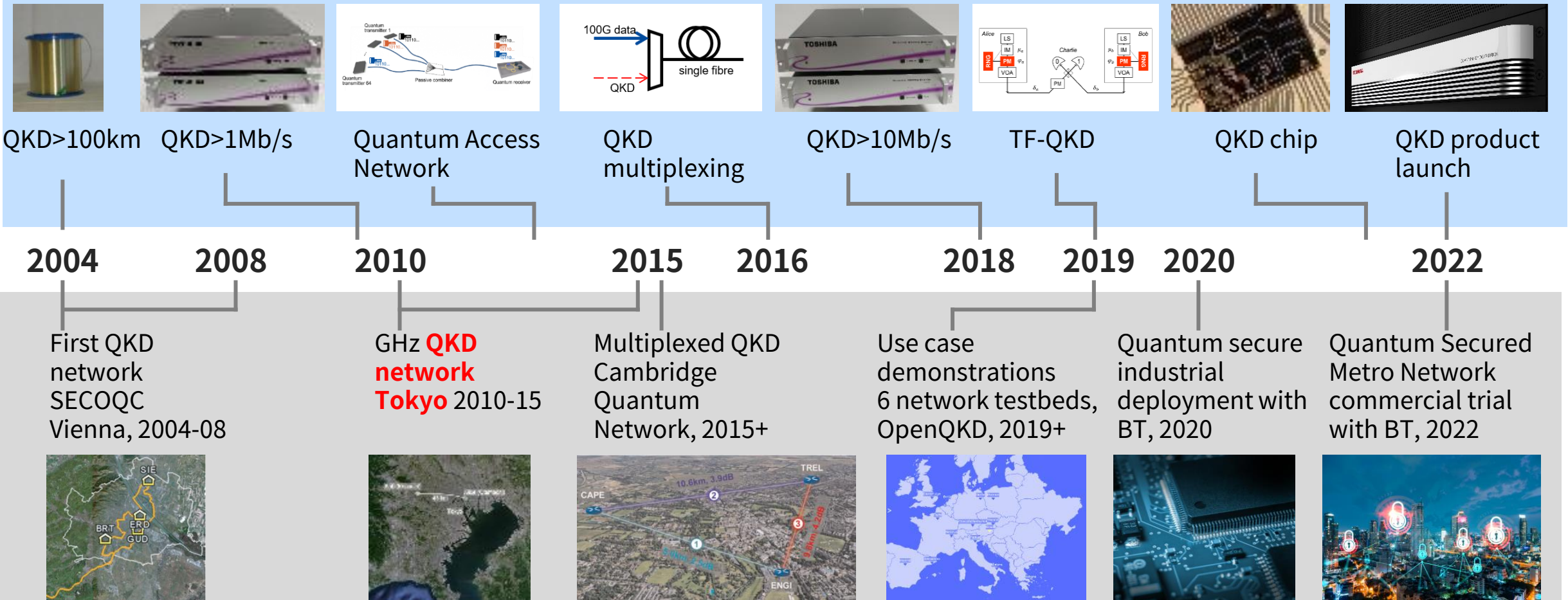
東芝における量子暗号研究開発の歴史



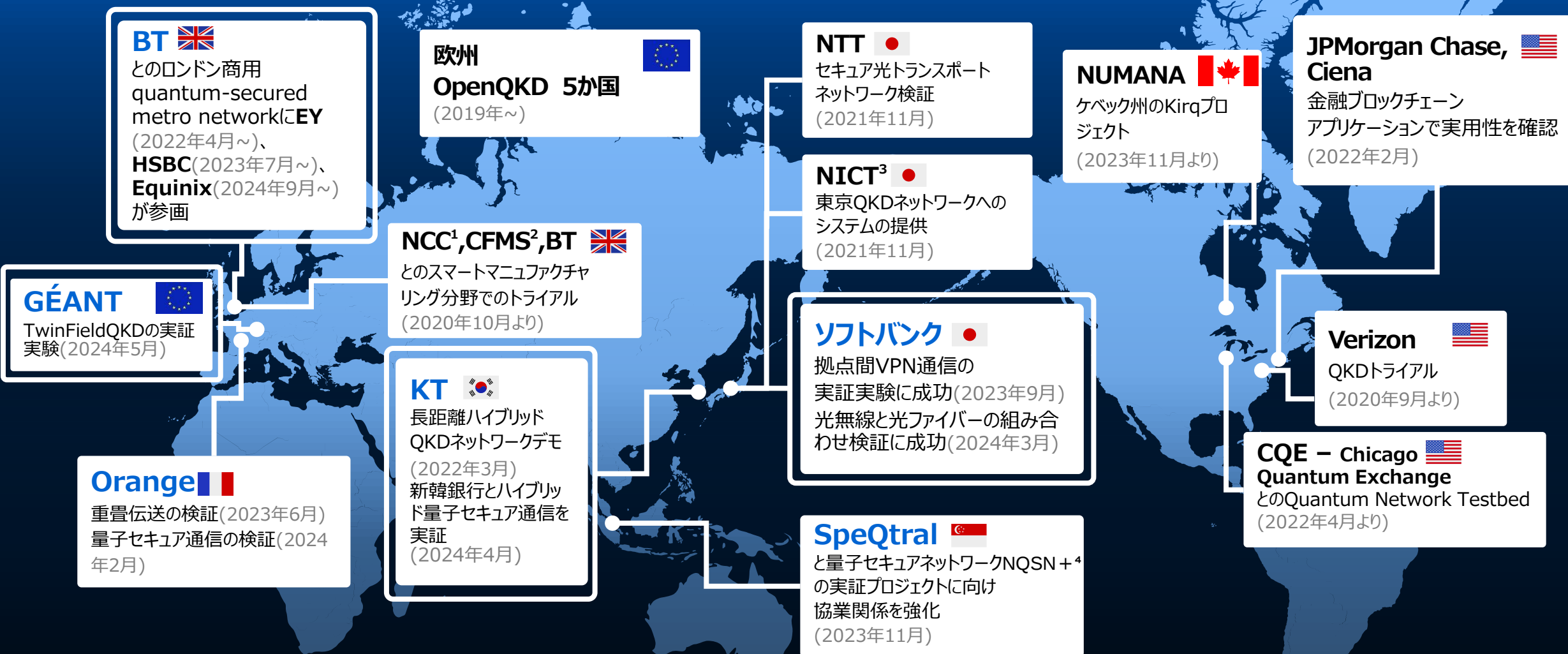
英国での基礎研究をベースに日本で実用化研究を推進
多くの顕著な世界初となる技術を実証

東芝の量子暗号技術実証の経緯

Technology Development



Technology Validation



豊富な協業実績

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)

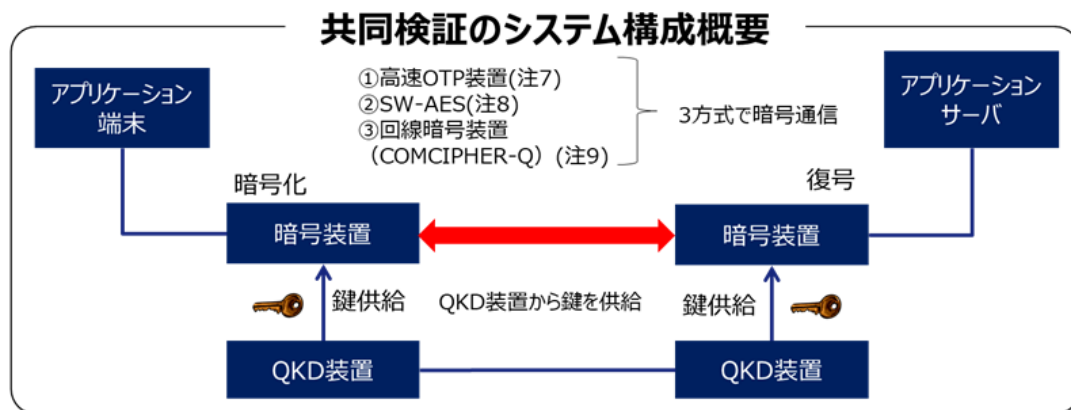
2024年11現在

直近のトピックス

公開情報より主要な実績を掲載

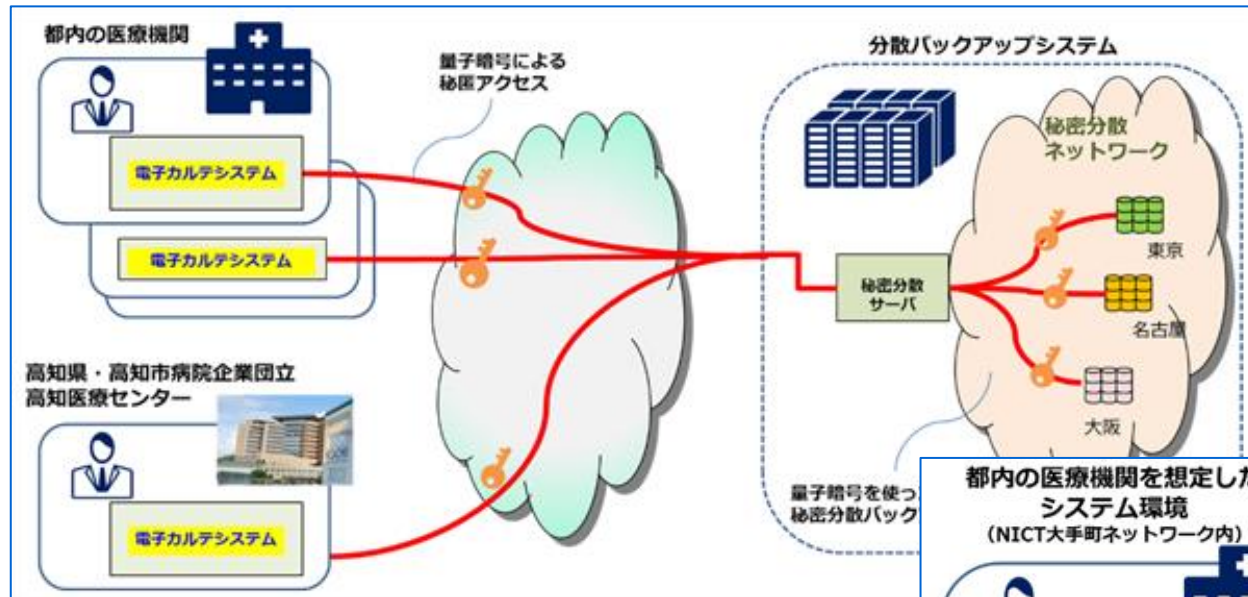
© 2024 Toshiba Digital Solutions Corporation

- 野村HD、野村證券、NICT、東芝、NECの5者による共同検証
- 図の3種類の方式（高速OTP装置、SW-AES、COMCIPHER-Q）のいずれかの暗号化方式を用いることで、① 量子暗号通信を適用しても従来のシステムと比較して遜色のない通信速度が維持できること、② 大量の株式取引が発生しても暗号鍵を枯渇させることなく高秘匿・高速暗号通信が実現できること、を確認
- 検証結果は、暗号化レベルや暗号通信速度などについて、将来的に様々な顧客ニーズに対応できるシステム構成について、柔軟に提案可能となることを示唆

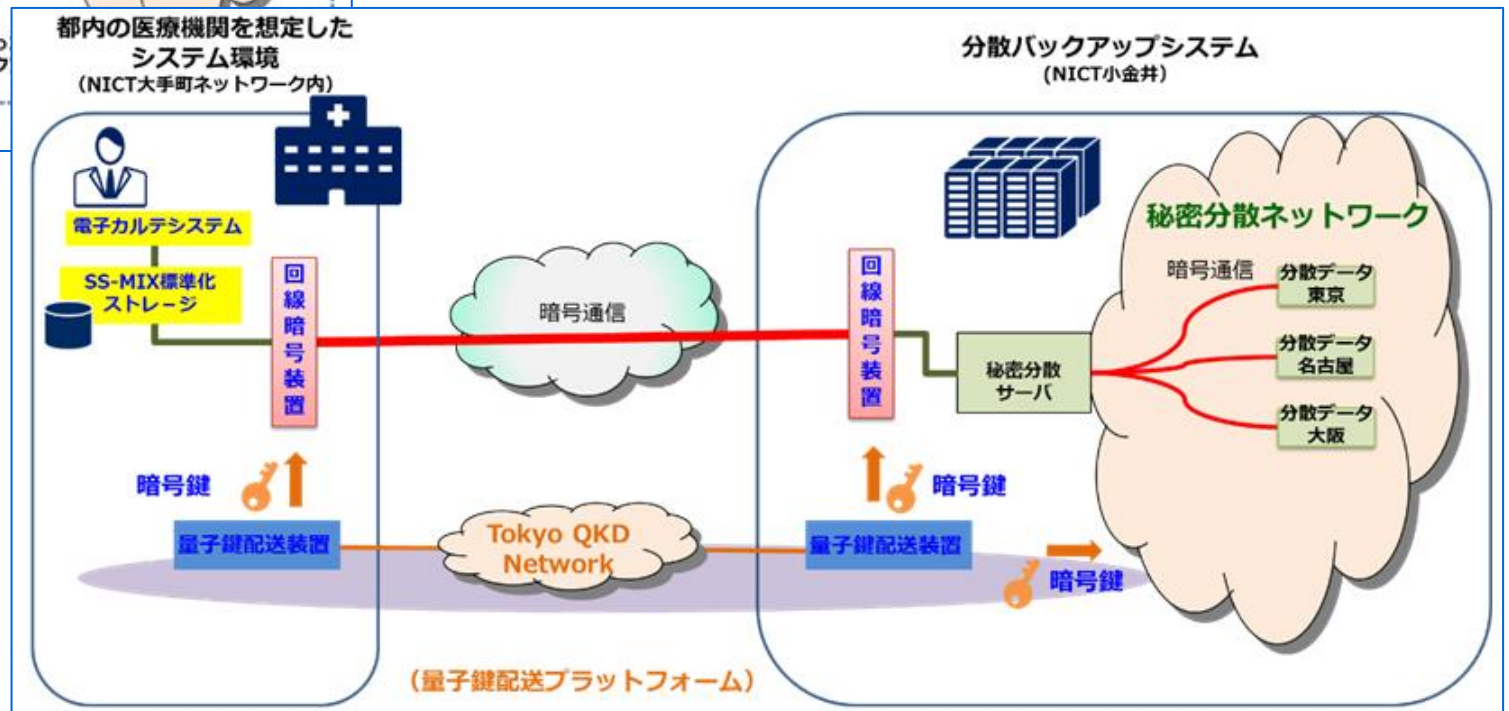


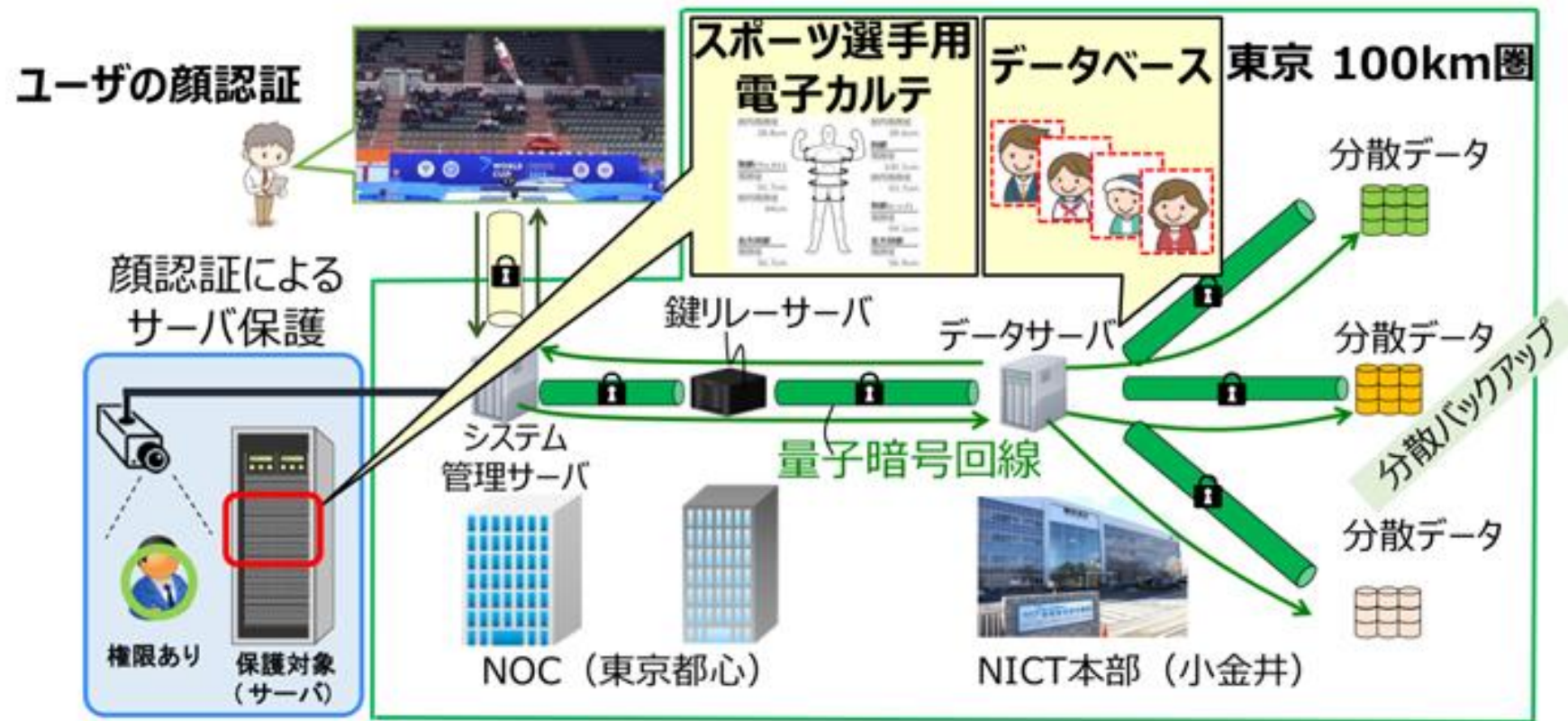
＊本研究の一部は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム(SIP)「光・量子を活用したSociety 5.0実現化技術」(管理人:量子科学技術研究開発機構)によって実施されました。





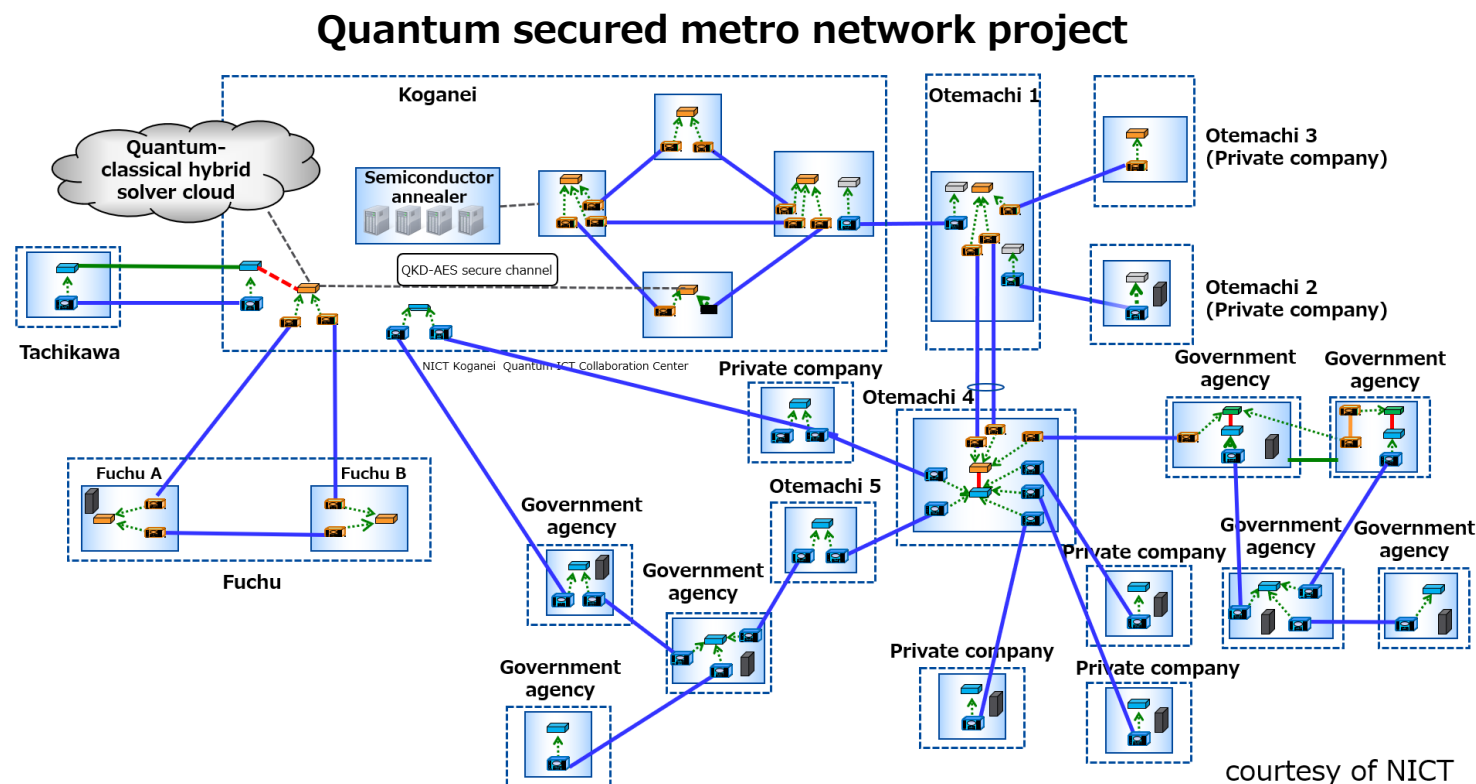
https://jpn.nec.com/press/202010/20201022_01.html





東京QKDネットワーク拡張(2023～)

- 国立研究開発法人情報通信研究機構(NICT) が世界最先端の量子ネットワーク技術を集結した東京QKDネットワーク(量子セキュアクラウド)を拡張
- 官民の複数機関が試験利用予定 野村ホールディングス、TOPPANデジタル、大和証券グループ、みずほフィナンシャルグループの参画が報道発表(2023年12月18日)
- 当社はQKDシステムと量子インスパイアード最適化ソリューションSQBM+を提供



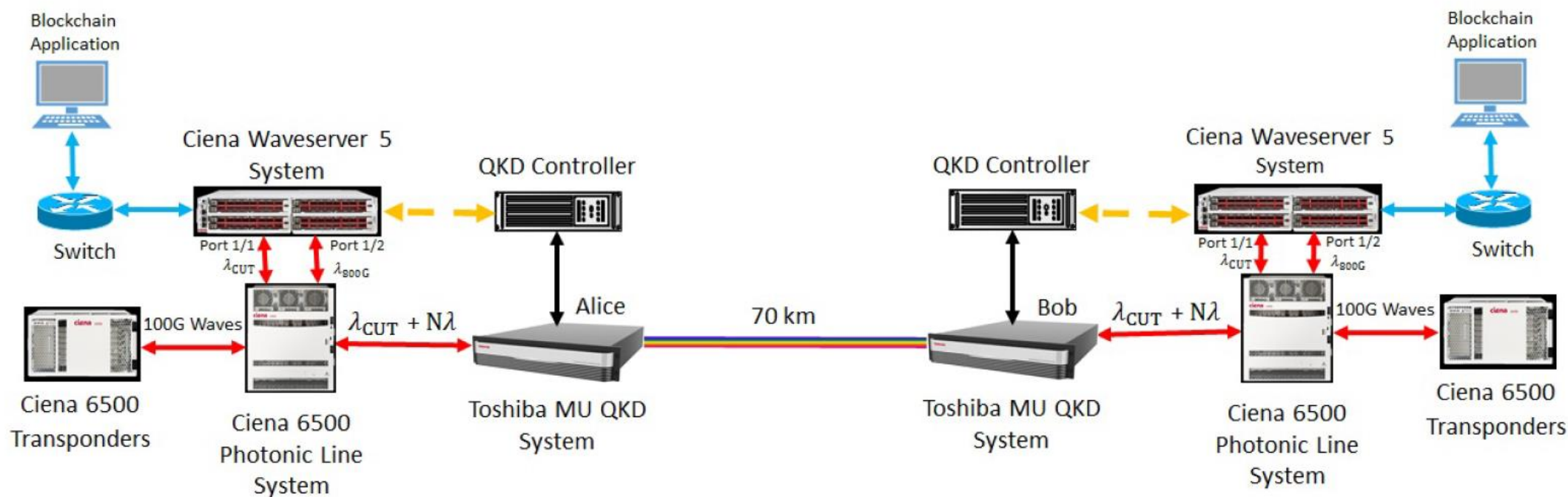
Toshiba QKD System



Quantum-inspired optimization solution **SQBM+**TM

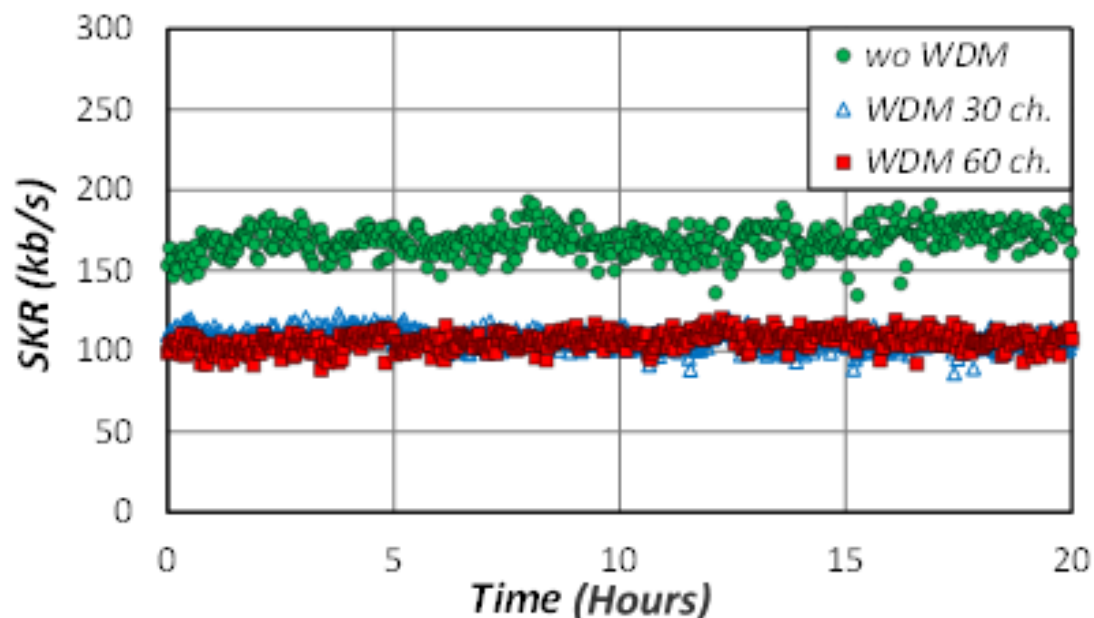
金融アプリケーションで量子暗号通信の実用性を確認

- 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100km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

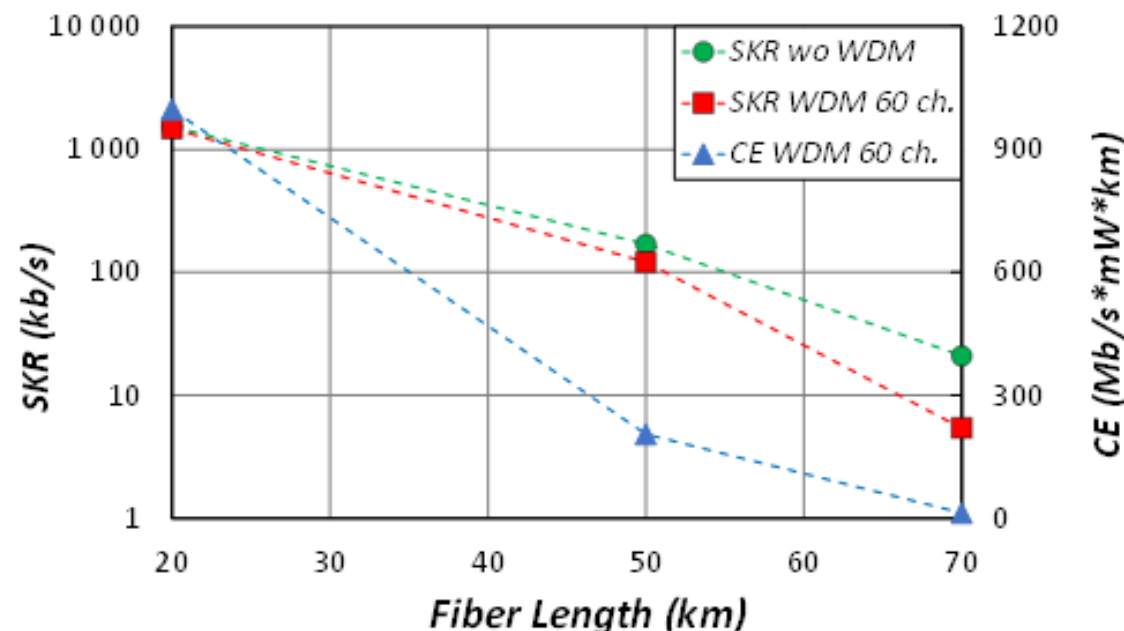


- **2022年2月18日発表:** <https://www.global.toshiba/jp/company/digitalsolution/news/2022/0218.html>
- 本実証実験の技術成果 (英文): <https://arxiv.org/abs/2202.07764>

- 東芝欧州社と仏オレンジ社によるPoC
- 東芝の商用 QKD 技術を用い、オレンジ社の既存の光ファイバーネットワーク上で、現行のデータサービスとともにQKD 技術を導入することが可能であることを実証
- これにより、オレンジ社のようなネットワーク事業者が、量子専用のファイバーインフラに投資する必要がなくなり、QKD の導入コストを削減できることを示す



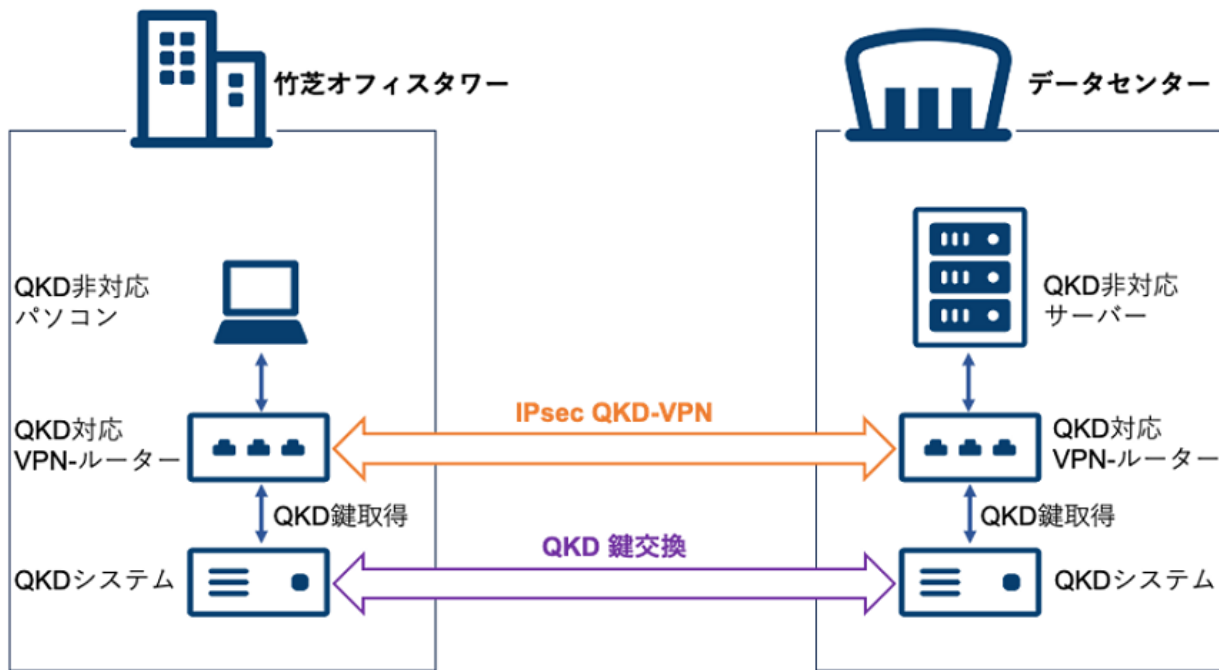
WDMを採用することでSKRは低下するが、
チャンネル数の影響は少ないことを示すグラフ



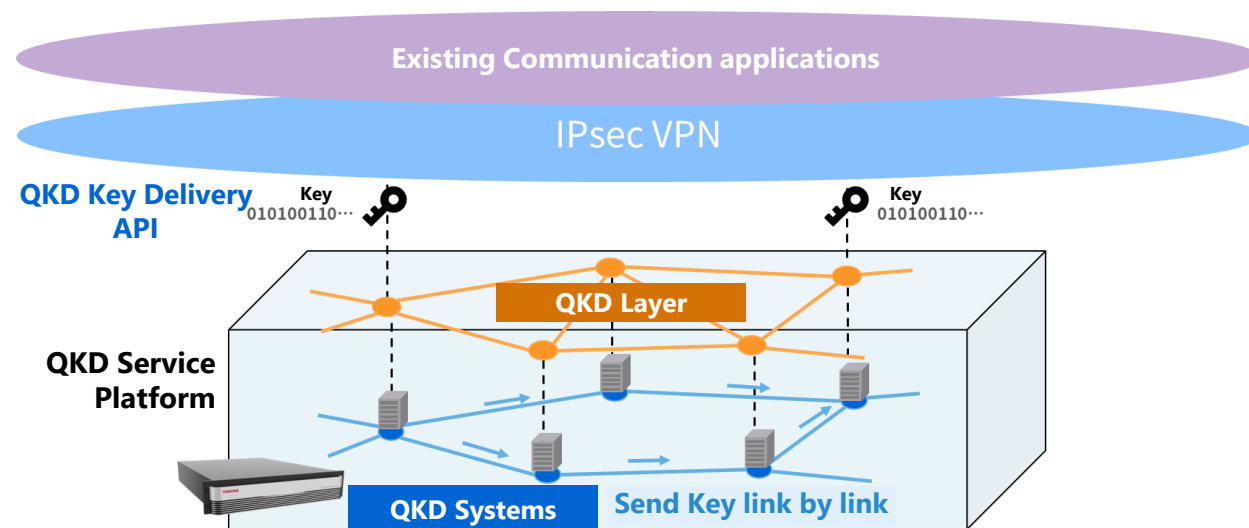
新メトリクス「Co-propagation Efficiency (CE)」が、
SKRと同様に距離に応じて減少することを示すグラフ

- 2023年6月6日発表: https://www.global.toshiba/content/dam/toshiba/jp/company/digitalsolution/news/pdf/news_202306.pdf
- 本実証実験の技術成果 (英文): <https://arxiv.org/abs/2305.13742>

今回の実証実験



今後の可能性



2023年9月20日発表: <https://www.global.toshiba/jp/news/digitalsolution/2023/09/news-20230920-01.html>

QKDを意識することなく既存の通信アプリケーションをそのまま利用できる

- World first(注) commercial QSMN trial
- EY as first commercial customer to connect quantum secure data transmission between its major London offices since April, 2022
- HSBC as first bank to join the trial, in collaboration with Amazon Web Services (AWS), connecting their global HQ in Canary Wharf and a data centre in Berkshire since July, 2023

SLOUGH

CITY

WEST END

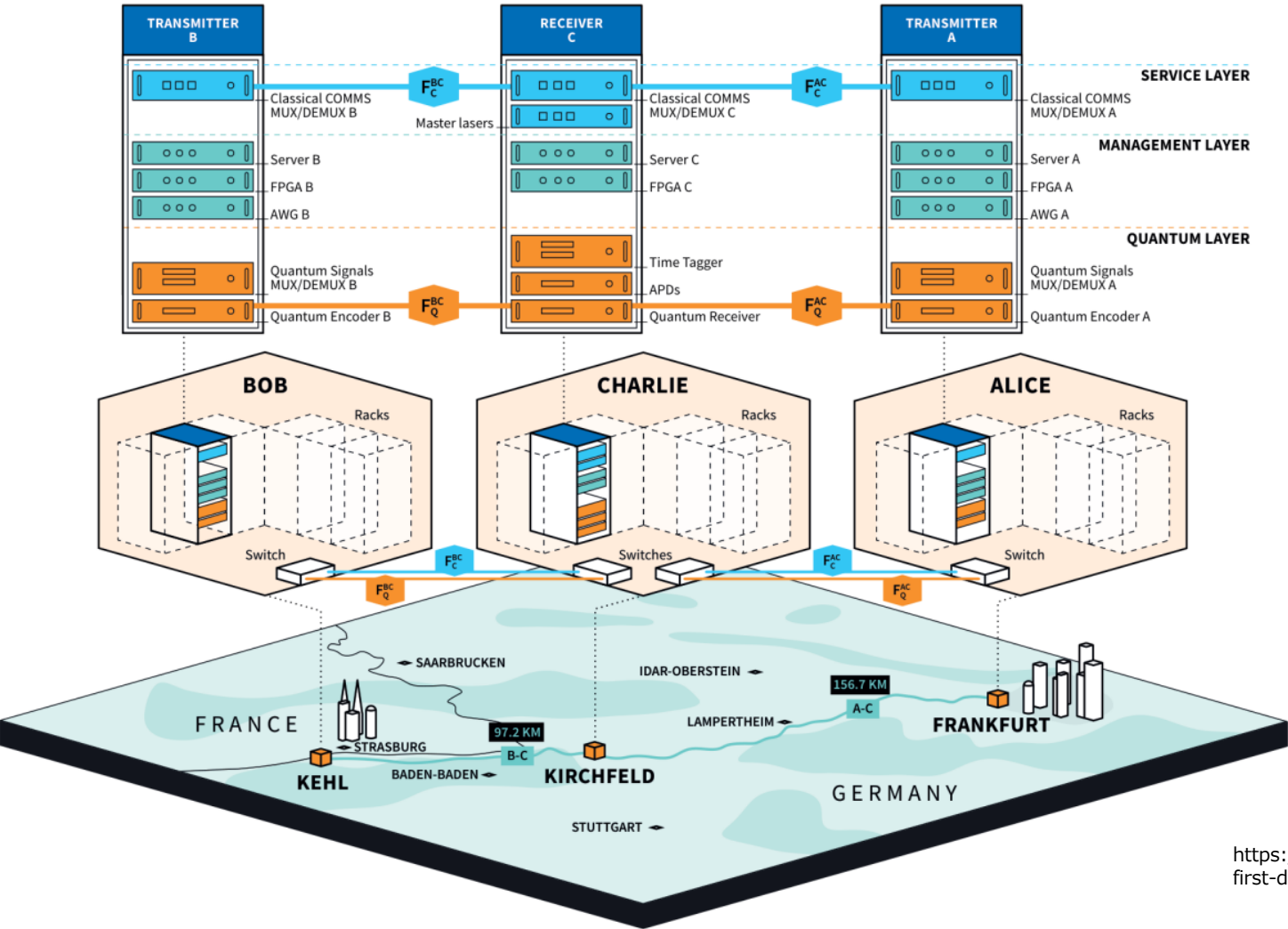


2022年4月27日発表: <https://www.global.toshiba/www/news/corporate/2022/04/news-20220427-01.html>

2023年7月5日発表: <https://www.global.toshiba/jp/company/digitalsolution/news/2023/0705.html>

注(株)東芝およびBT調べ

フランクフルト～キール間254kmで接続検証(2024)



Toshiba Europe, GÉANT, PSNC and Anglia Ruskin University announce the first demonstration of Quantum Key Distribution within commercial telecommunication networks.

Quantum communications harness quantum phenomena like superposition and entanglement to enhance information transfer between remote nodes. The key benefits of these techniques are the ability to be able to detect if communications have been intercepted or modified en-route. Which makes these techniques ideal for highly sensitive data interchange.

However, coherent quantum communications, essential for typically phase-based quantum internet architectures, require optical coherence among nodes and typically involve single-photon interference. Within laboratory environments the challenges of preserving optical coherence and integrating advanced single-photon detectors can be managed through careful implementation and isolation techniques (even vibrations of the fibre optics can affect coherence). However commercial telecommunications implementations cannot easily provide this highly controlled environment and so the deployment in existing telecommunication networks has been extremely difficult to achieve and often limited to metro-scale implementations – particularly in the financial services sector where the costs of dedicated infrastructure can be supported.

<https://network.geant.org/toshiba-europe-geant-psnc-and-anglia-ruskin-university-announce-the-first-demonstration-of-quantum-key-distribution-within-commercial-telecommunication-networks/>

04

今後の課題

各国の状況と今後の技術開発課題

各国の状況：QKDネットワークの実装が活発化

中国	既に国家規模のQKDネットワークを運用中 衛星QKD、Twin-Field QKDの開発も積極的
欧州	EuroQCIにより、EU各国でQKDネットワークの社会実装が開始 スタートアップが複数出現。EuroQCIへの適用を睨んだ動きの模様
韓国	SK Telecomが自社サービス、政府ネットワークにQKDを適用 KTがQKDネットワークの複数トライアルを実施
シンガポール	NQSN+プロジェクトが開始。SingTel、SPTelが参画し、国家規模のQKDネットワークを構築

今後の技術トレンド：

開発競争の中心が、QKD装置だけでなく、**QKDネットワーク**、さらにQKDを活用する**サービス**に広がっていく。

QKDネットワーク本格普及に向けた課題と必要となる技術

QKDネットワークを用いた安全なサービスを、多くのユーザがICT基盤として利用するために

暗号鍵配送の効率化

- ・QKDネットワークの最適制御

通信インフラ共通化：データ通信NW(オール光NW)とQKDネットワークの融合

- ・データ通信ファイバへの量子信号多重化など

経済安全保障

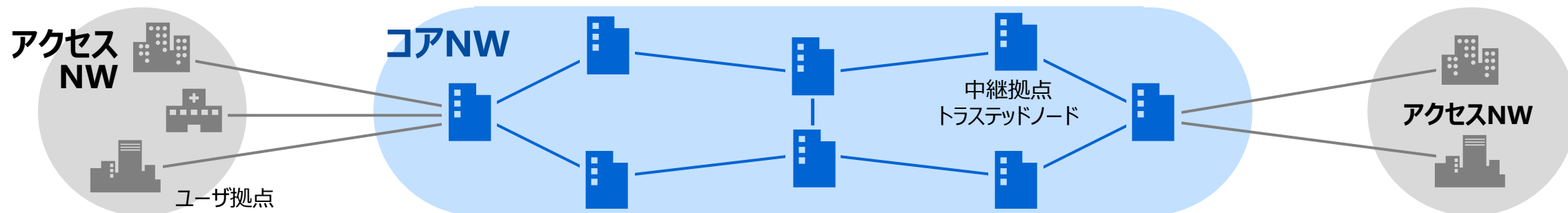
- ・キーデバイスの国産化、国産QKDシステムの高度化・低コスト化とフィールド実証

量子技術ならではの共通サービスの開発

- ・量子セキュアクラウドを用いた高度情報処理基盤
(超長期に秘匿性を必要とするデータの利活用基盤として)
- ・高精度時空間情報の安全な流通
(自動運転など、社会インフラ向けサービスとして)

秘匿通信の信頼性向上

- ・秘密分散・ネットワーク符号化



ユーザの導入障壁低減：

小型化・低コスト化

- ・CV-QKD
- ・チップベースQKD
- ・小型・低コスト光子検出器

インフラ整備コストを削減：トラステッドノード(古典技術で守る中継拠点)数最少化

- ・長距離QKD(TF-QKDの実用化・高度化)
- ・量子中継長距離化、量子もつれ光子配信
- ・量子中継ネットワーク基礎技術(量子もつれ転写(通信・メモリ間)、宛先制御等)

多くのユーザを収容：鍵配送大容量化

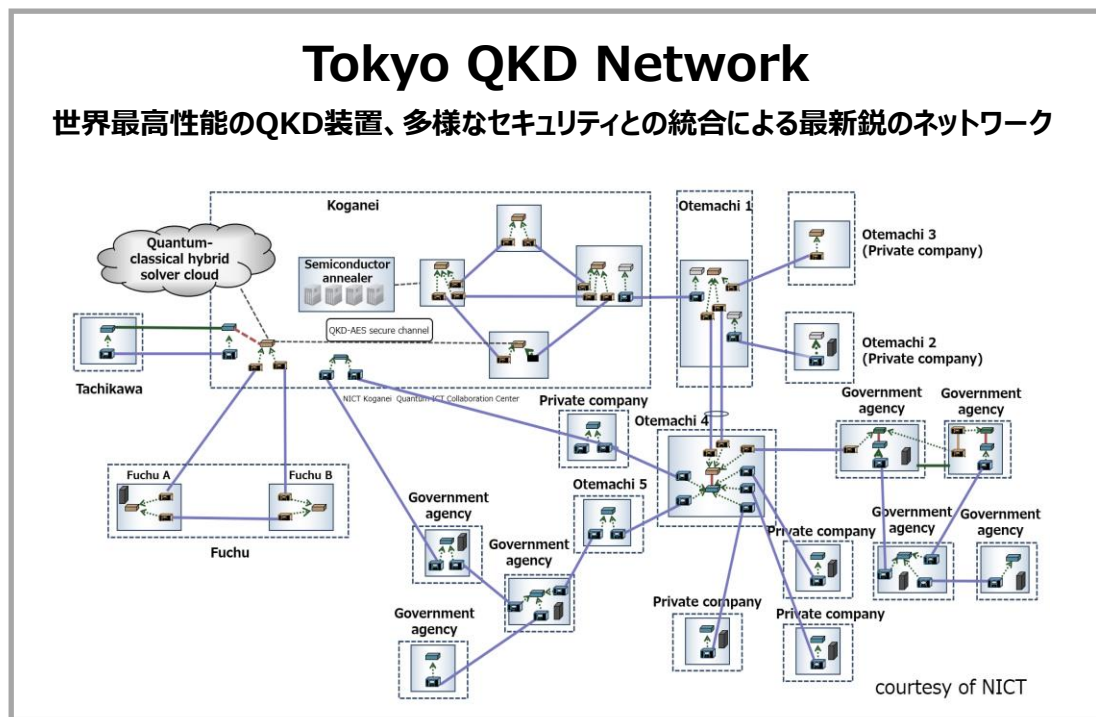
- ・マルチチャネル光集積回路
- ・大容量光子検出器(チップ並列化)

ネットワークの広域化：

- ・衛星QKDと地上QKDの融合

量子暗号通信テストベッドの拡張に向けて

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)



QKD: Quantum Key Distribution

NICT: National Institute of Information and Communications Technology

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

主要都市間への拡大
東名阪など主要都市路結ぶネットワーク拡張
国際標準の実装と実利用で競争力を磨く
PQC方式との混在利用



全国ネットワークの実現

研究開発が進む衛星QKDと地上網の実装
本格導入を進める

PQC: Post Quantum Cryptography

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

05

NICT様への期待

量子情報通信の高度化・普及に向け、量子セキュリティ拠点として
中長期的なビジョンを示し、基礎的・基盤的な研究開発を主導する等、
今後も引き続き本分野を牽引することを期待します

①研究開発

世界のトップレベルの技術力の確保に向けた量子通信（量子暗号通信、量子インターネット）の基礎的・基盤的な研究開発の取り組みの強化

②テストベッド

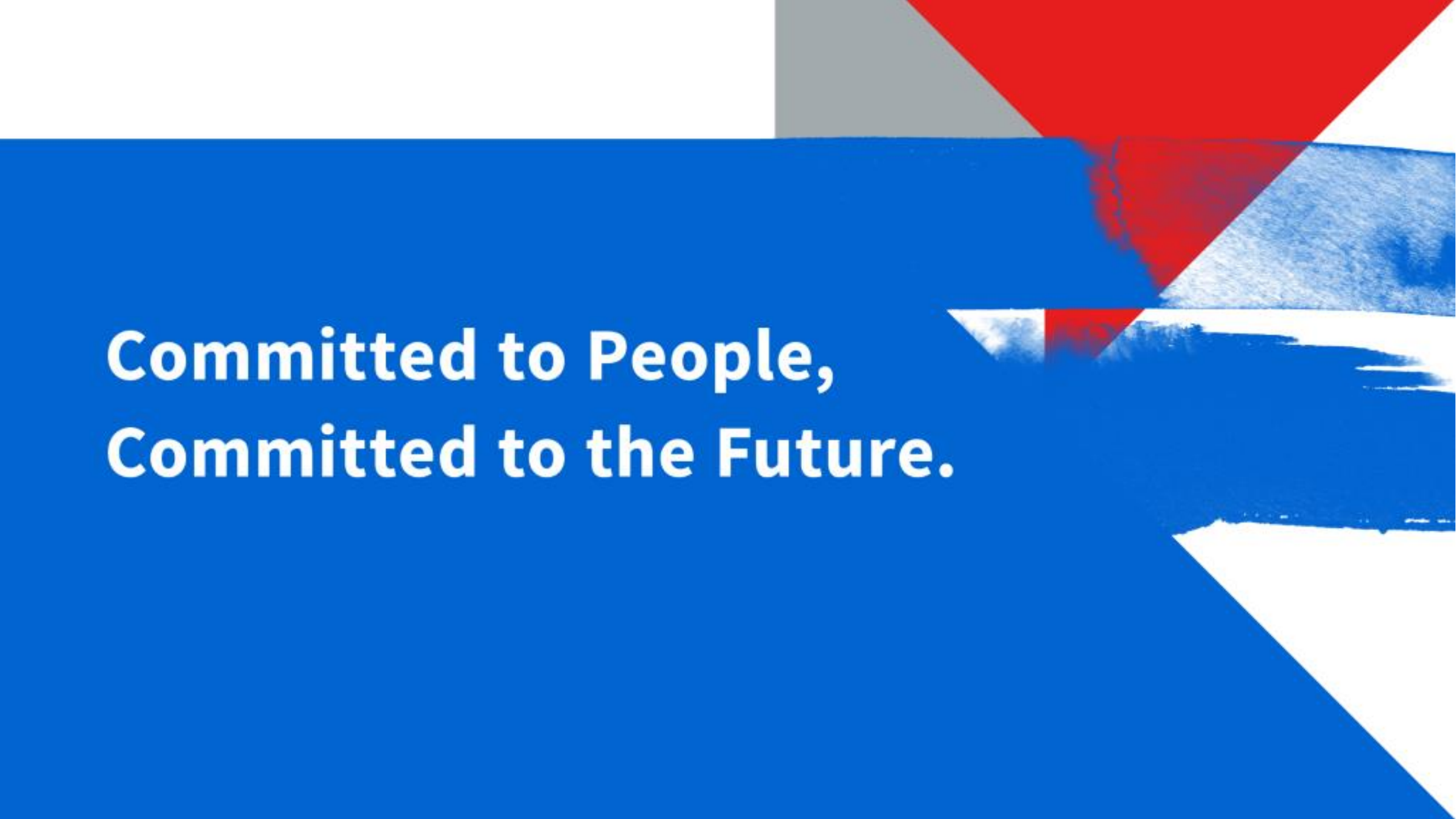
量子暗号通信の早期実用化に向けたアーリーアダプタの取り込みとQKDテストベッドの拡充（長距離テストベッドなど）

③国際標準化

国際市場への円滑な展開、サプライチェーンの確保等を可能にするため、量子暗号通信等の国際標準化や量子暗号通信装置の安全性に関する認証枠組みの議論のリード

④人材育成

日本の量子通信に関する研究や技術開発を担う量子ネイティブの育成

The background features a large, solid blue area on the left. To the right, there are several overlapping geometric shapes: a red triangle pointing downwards, a grey triangle pointing upwards, and a blue triangle pointing upwards. These shapes are layered over a background of horizontal bands of white and blue, some of which have a textured, brush-stroke-like appearance.

**Committed to People,
Committed to the Future.**

TOSHIBA