TOSHIBA

量子技術の実用化推進WG 2022.11.10

資料2-1

量子未来社会ビジョンの実現に向けて

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
シニアフェロー
村井　信哉

グローバルで量子暗号通信の実証・協業を推進中

米**JPモルガン・チェース**と、
金融ブロックチェーンに関するPoC実施
(2022年2月)

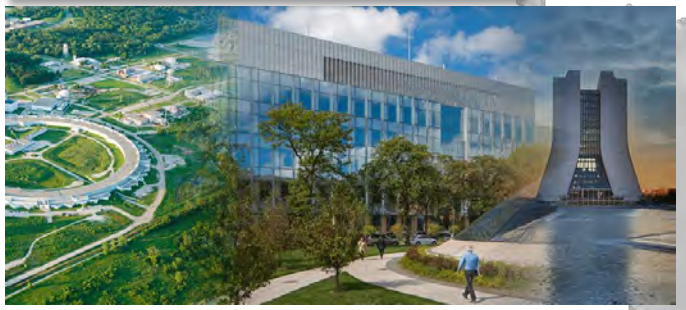
英**BT**と、産業用ネットワーク向けトライアル実施
(2020年10月)

汎欧州プロジェクト**OpenQKD**にて、
6か国のトライアルに参画中

NTTと、大容量・低遅延な「IOWNセキュア光トランスポートネットワーク」の検証に成功
(2021年11月)

米**ベライゾン**と
トライアル継続中

米量子技術コミュニティ**CQE**の量子テストベッドに参画(2021年6月)



CHICAGO QUANTUM EXCHANGE

英**BT**と、ロンドンで世界初の量子暗号通信の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開始(2022年4月)

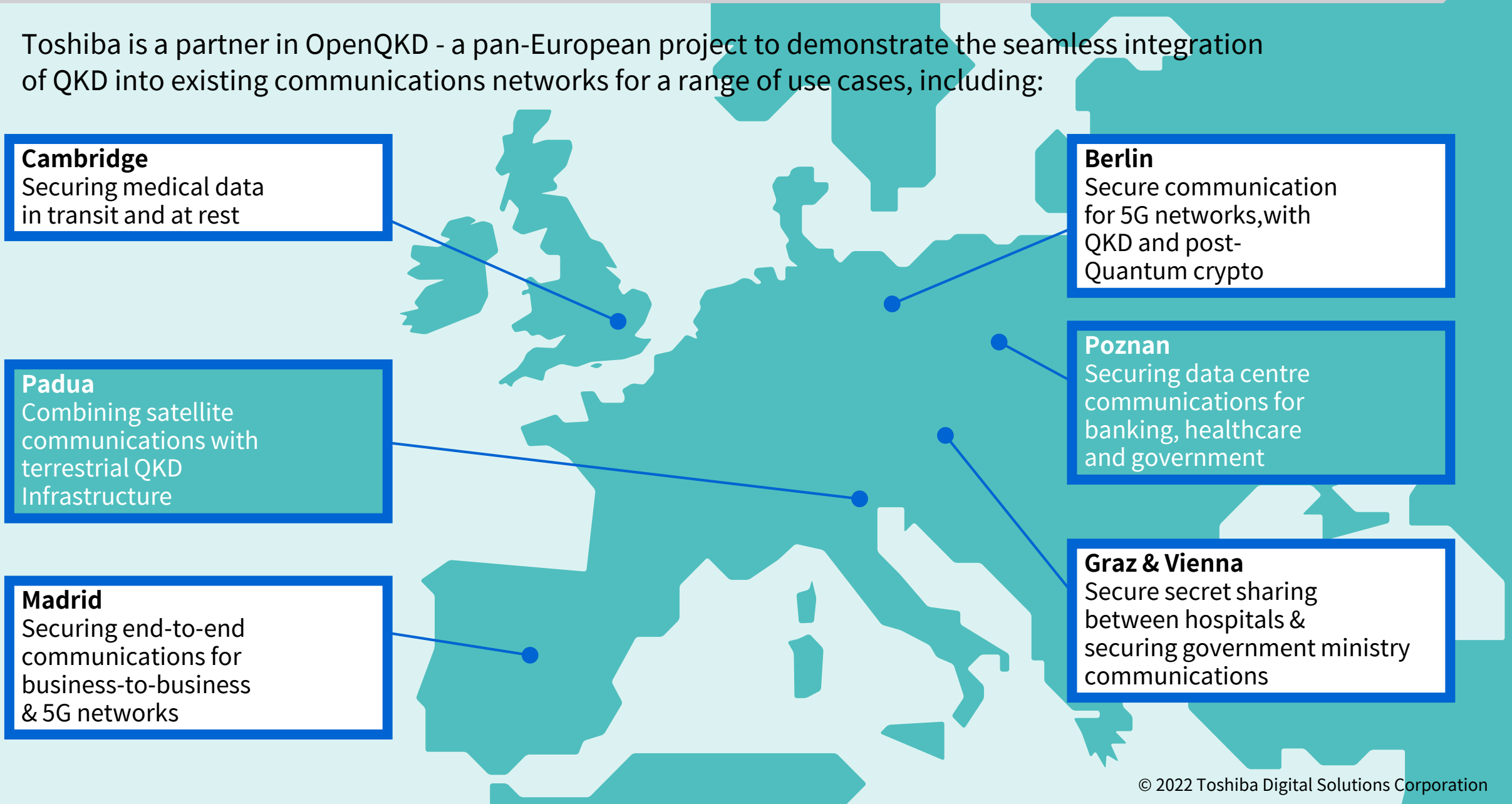
韓**KT**と、ソウルと釜山間の約490kmにおいて、長距離ハイブリッド量子暗号通信ネットワークを実証
(2022年3月)

シンガポール**SpeQtral**と、東南アジアにおける量子暗号通信ビジネスで協業を開始(2021年8月)

SPEQTRAL TOSHIBA

EU OpenQKD Testbedsへ参画

Toshiba is a partner in OpenQKD - a pan-European project to demonstrate the seamless integration of QKD into existing communications networks for a range of use cases, including:



Cambridge
Securing medical data in transit and at rest

Berlin
Secure communication for 5G networks,with QKD and post-Quantum crypto

Poznan
Securing data centre communications for banking, healthcare and government

Padua
Combining satellite communications with terrestrial QKD Infrastructure

Graz & Vienna
Secure secret sharing between hospitals & securing government ministry communications

Madrid
Securing end-to-end communications for business-to-business & 5G networks

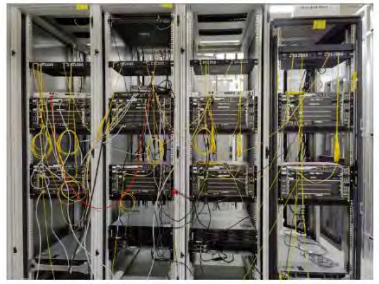
OpenQKD: オーストリアにおける医療ユースケーストライアル例

Medical use-case in Graz

OPEN QKD

Deployment finalized in Graz:

- ❑ Test of QKD links (4 from IDQ, 2 from Toshiba) and completed under realistic conditions
- ❑ Fiber infrastructure characterized
- ❑ Interface to encryptors (ADVA) implemented
- ❑ Storage solution by FragmentiX



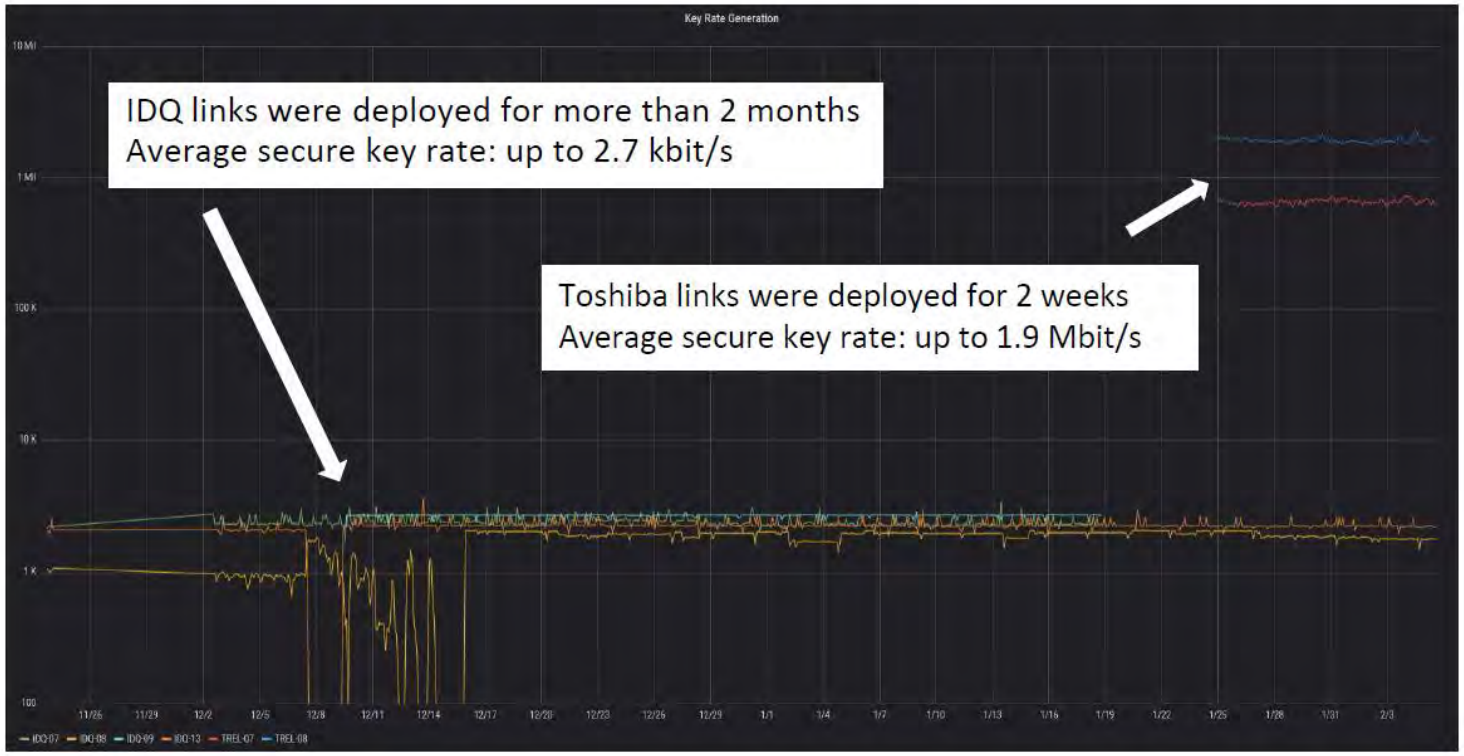
Dry-run of optical network

Geographic layout

競合と比較し、当社QKDが、数百倍の鍵配送可能であることが示された。

Secure Key Rates from the Field Test

OPEN QKD



16

https://www.itu.int/en/ITU-T/webinars/20210526/Documents/Andreas%20Poppe_Presentation.pdf?csf=1&e=ol42va

事例：英国BT社と、量子鍵配送の商用メトロネットワークのトライアルを開始

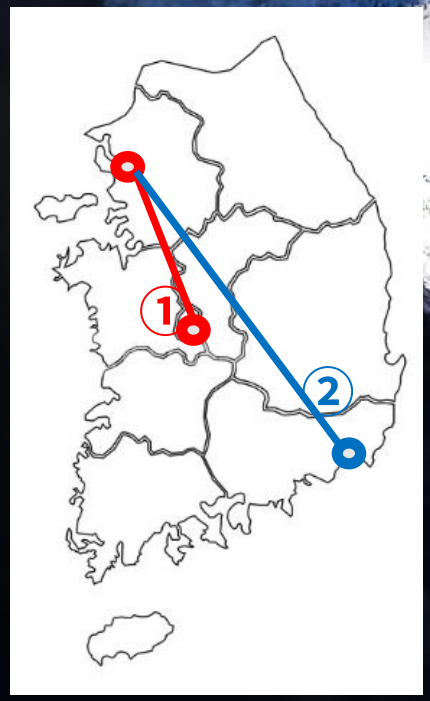
- EY が最初の商用顧客として参画し、ロンドンの主要な拠点間でセキュアなデータ通信の検証を開始

https://www.global.toshiba/jp/news/corporate/2022/04/news-20220427-01.html

事例：韓国KTと量子鍵配送の実証プロジェクトを共同で実施

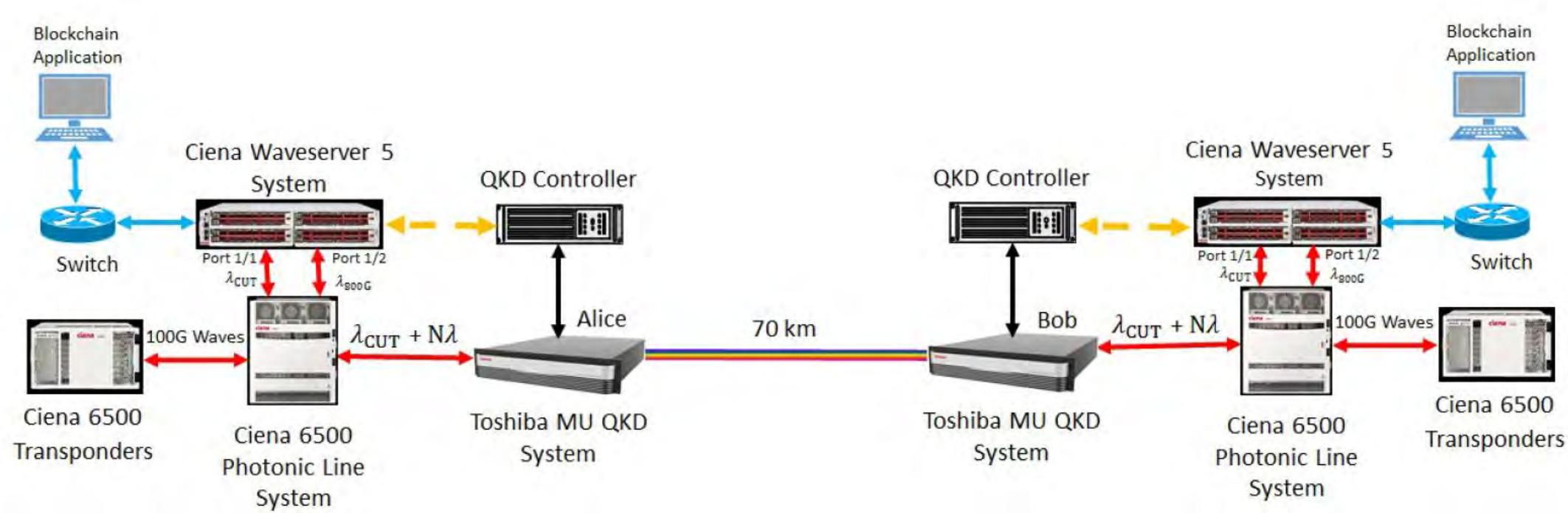
- 韓国ソウル特別市と釜山市間の約490kmにおいて、異機種の量子鍵配送システムをつないだ長距離ハイブリッド量子鍵配送ネットワークを実証
- ソウル特別市と大田市間において、量子産業エコシステム拡張に向けたオープンなQKD-as-a-Service(QKDaaS)のテストベッドを運用予定

https://www.global.toshiba/jp/company/digitalsolution/news/2022/0328.html



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

米国CQEとQKDネットワークリンクの実証を開始

Short Term

- Develop Testbed with CQE to demonstrate Toshiba quantum innovations to U.S. government and enterprises.

Mid Term

- Expansion of DOE laboratory quantum internet program to universities and cities

Long Term

- Industrial collaboration in Quantum Internet development and enablement

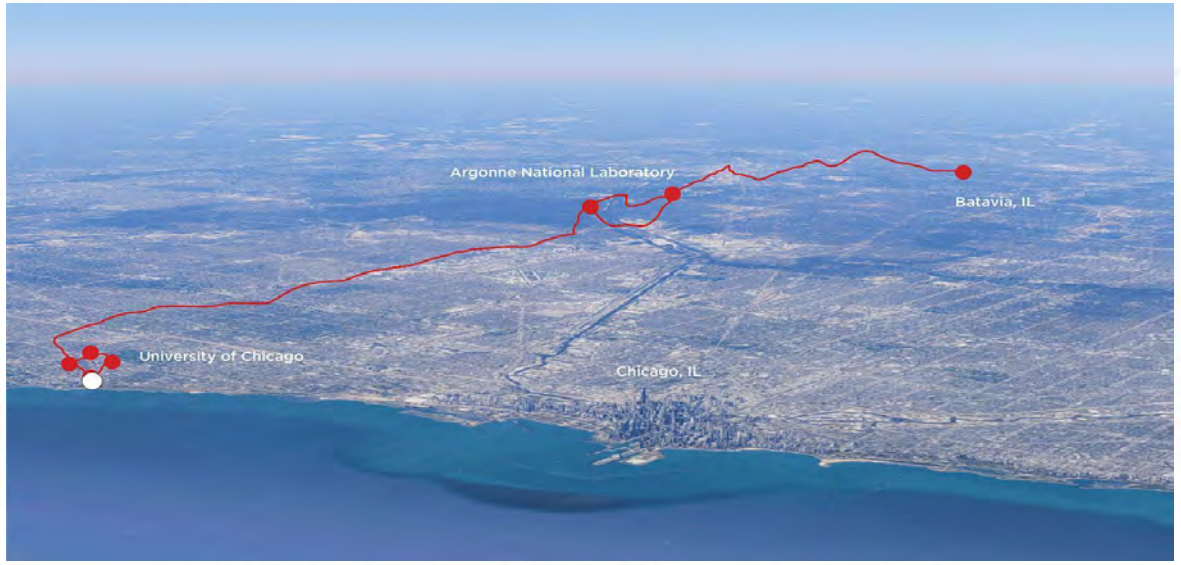
Quantum Network Testbed

Backbone for Quantum Internet Network

TOSHIBA

CHICAGO QUANTUM EXCHANGE

*Image courtesy of Chicago Quantum Exchange



Telecom Fiber Multi-node Metropolitan Network

- Real world operating conditions
- Solid state nodes
- GPS disciplined clock synchronization
- Plug and play platform

2022年4月28日発表：https://www.global.toshiba/jp/company/digitalsolution/news/2022/0428.html

量子ネイティブ育成へ　～シカゴの高校生が量子暗号を実体験～

“この量子ネットワークは研究者の技術・デバイス検証や、次世代量子技術者を育成するための貴重な教育ツールを開発するプラットフォームです。学生がこの投票デモを通じ、量子技術の現実世界への適用に参加した体験で、将来の量子コミュニティのメンバになることを願っています”
（CQEディレクター　David Awschalom氏）

Chicago Quantum Exchange（本部：シカゴ）で開催された量子技術体験学習に市内の高校生が参加、量子暗号通信を用いた投票デモを実体験した
（2022年10月18日）

当日はオバマ元大統領もサプライズ参加、高校生を驚かせた

https://chicagoquantum.org/news/chicago-high-schoolers-become-first-members-us-public-use-ultra-secure-quantum-technology-mock

量子未来社会ビジョンの実現に向けて

「国内の量子技術の利用者を1,000万人に」向けて
多くの利用者を巻き込む仕掛け
ご提案：現在、国内の民間機関や政府機関が個別に有する機微な情報を、
安心して保存・管理・利活用可能な国内量子セキュアクラウドの整備

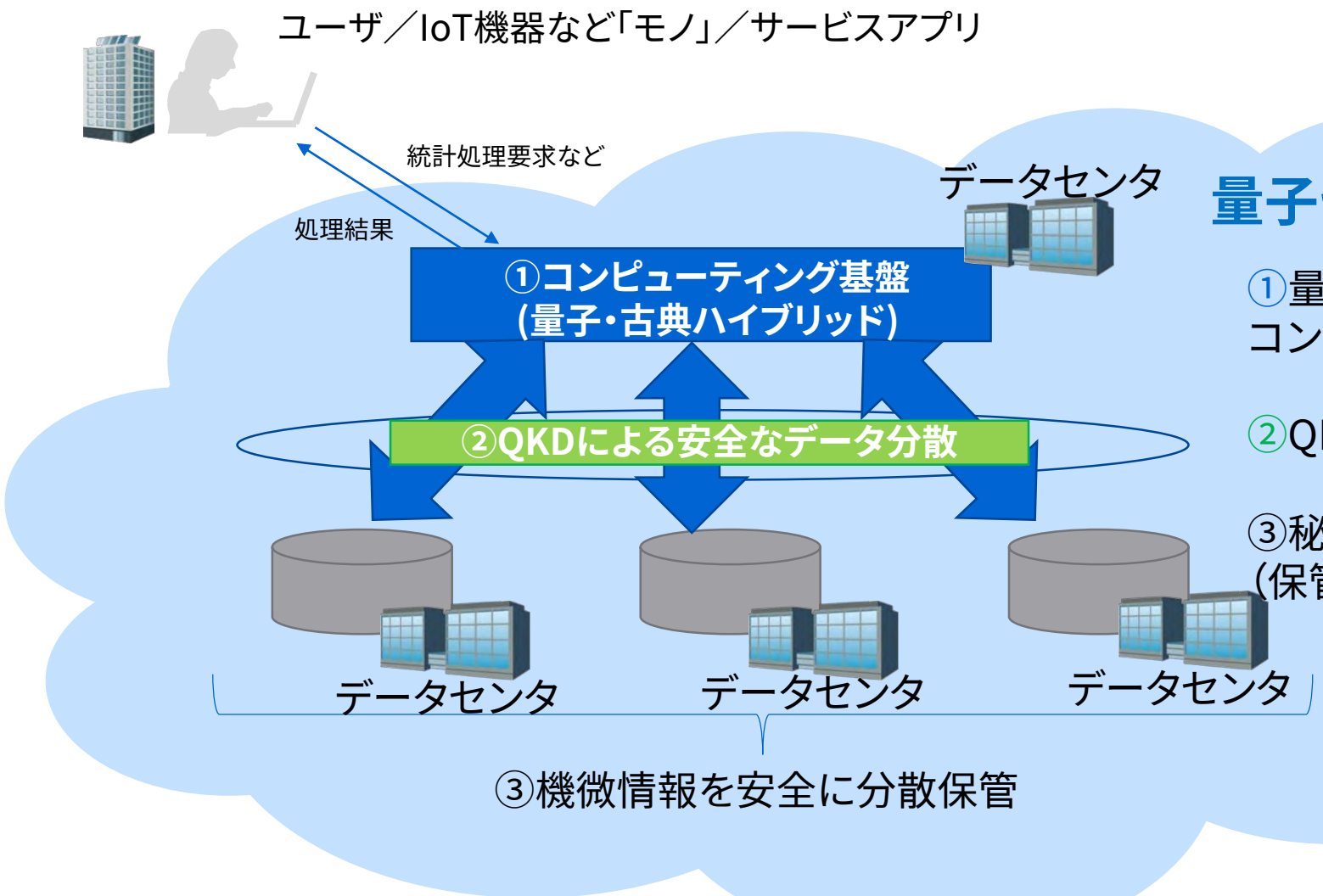
NICT様が中心に研究開発が進められている「量子セキュアクラウド」を、
拡充・広域化・実用化し、
多くのユーザを巻き込む、量子技術活用基盤としてはどうか？

「実利用」「ユースケース開拓」「技術検証・改善」のプレイグラウンド

論点：量子暗号通信の広域テストベッドの充実・強化の在り方
論点：主要拠点であるNICTについて、産業界から期待される取組強化の在り方

最新量子技術をフル活用した国内クラウド

ユーザは、機微情報の個別管理から解放され、最新量子技術を利用できる



量子セキュアクラウド

①量子・古典ハイブリッドによる強力・柔軟なコンピューティング基盤

②QKDによる安全なデータセンター間通信

③秘密分散等による安全なデータ分散保管
(保管データの漏洩対策、災害対策)

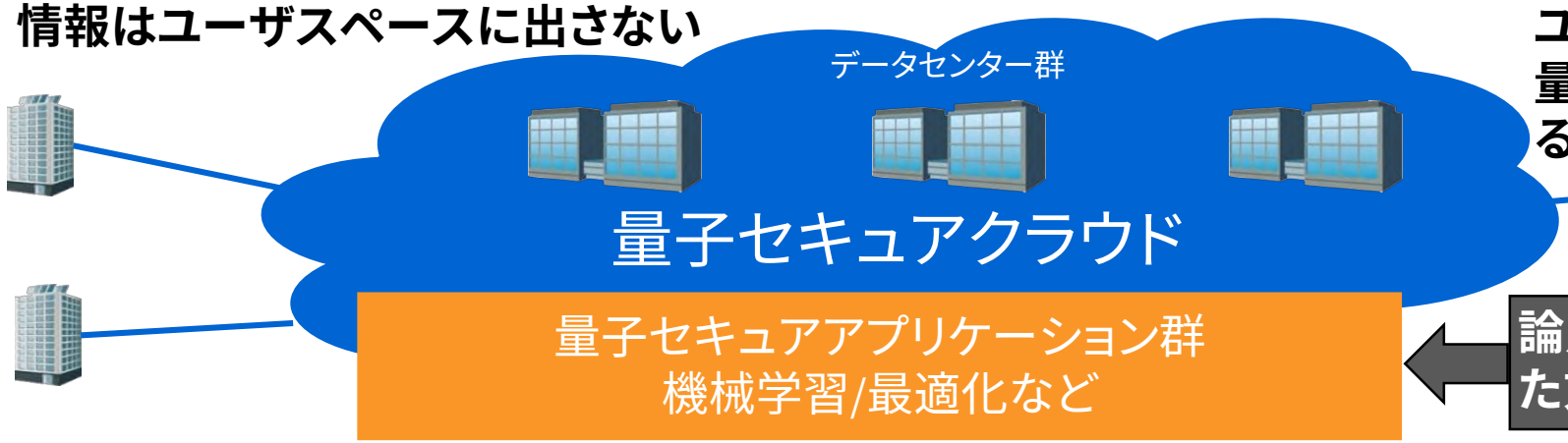
多くの利用者・アプリケーションを巻き込む仕掛け・フレームワーク

インターネット等古典インフラをから量子セキュアクラウド上のデータを利用

量子セキュアスペース

ユーザスペース

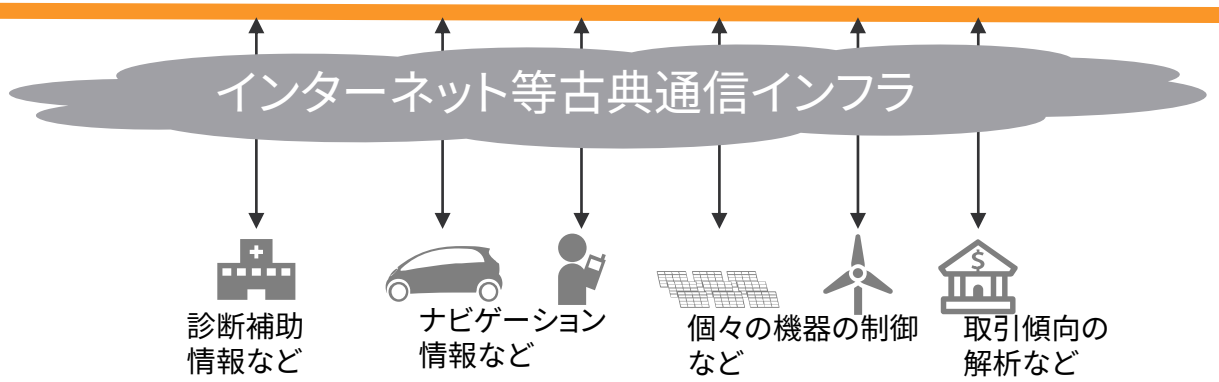
ポイント：長期に機密保持が必要な情報はユーザスペースに出さない



機密情報を直接扱う重要拠点やユーザは、QKDで直接つなぎ、量子セキュアスペース側に入れる。

論点：新たな企業の参画に向けた方策はどうあるべきか

論点：古典暗号との共存の在り方



データ利活用API

レガシーなユーザスペースから量子セキュアスペースへのアクセスを可能にするデータ利活用APIを定義し、提供する。

コンセプト実現のポイント

■簡便性
- 「量子」の特殊性を意識せずにデータ利活用が可能なAPIとアプリケーション

■安心&オープン性
- 「国のお墨付き」を得たシステム、利用者にオープンな運用・管理体制
  - QKD装置は機器認証制度を活用
  - その他必要な運用ガイドラインの整備など

論点：利用支援サービス（アプリケーション）を提供する民間事業者のビジネスモデルや主体の在り方

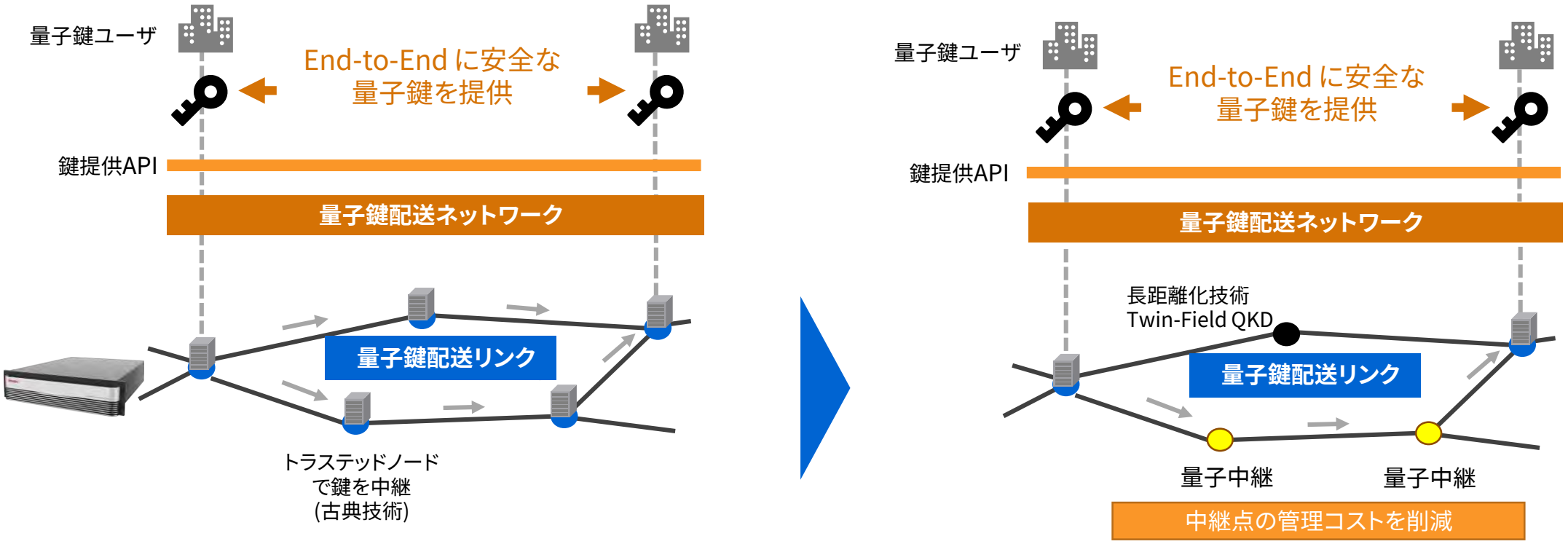
■拡張性・発展性
- スケーラブル（主要都市圏から全国へ。衛星QKD網整備が必要）
- 最新量子技術を、シームレスに取り込むことのできるフレームワーク・IF定義

論点：古典アーキテクチャからのマイグレーション、古典暗号との共存の在り方

発展性・拡張性：　最新技術を取り込むフレームワーク

適切なインターフェースの定義により、アプリケーションを変えずに、徐々に新規技術にマイグレーションできる。

鍵提供インターフェースの例：



論点：国内ベンダー企業の勝ち筋となるビジネスモデル、熾烈な国際競争に劣後しないための国際競争力強化等の在り方

鍛えられた実装実績をもとに標準化を先導し、諸外国のプレーヤを自らの土俵に引き込む

実用化技術を強化し、持続的な国際競争力を獲得するために

実装を鍛えて標準化に持ち込む

①実装強化
システムの構成要素を提供するベンダ・オペレータ、そしてユーザが一体となって、アジャイルに、柔軟に、トライ・アンド・エラーを重ねて実用化技術を成長させることができる大規模オープンテストベッドにより実装を鍛える。
【期待できる効果】
- 実用化における課題がリアルに把握できる。
- 全体最適を図れる。
- 課題解決のための技術を次々と試すことができ、継続的な技術成果の産業化に繋がる。

②標準化
鍛えられた実装実績をもとに、諸外国のプレーヤを自らの土俵に引き込む。
- ◆ システム全体のフレームワーク
  - エコシステムを構成する各プレーヤのポジション・役割を明確にでき、分業が容易になる。
- ◆ 既存システムとの接合部分のインターフェースプロトコル
  - 量子鍵配送ネットワークの導入を容易にし、既存システムベンダを巻き込むことができる。

活動中の標準化団体

ITU-T
ネットワーク要件、アーキテクチャ等

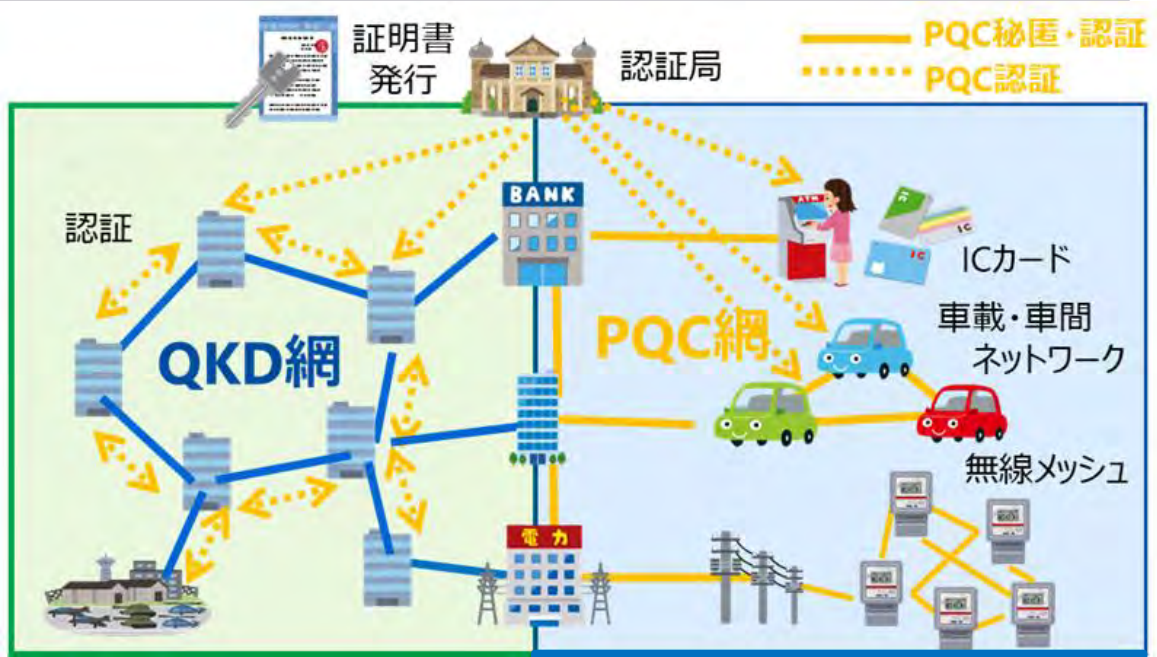
ISO/IEC
QKD装置の実装安全性評価

ETSI(欧州電気通信標準化機構)
部品・モジュール・インターフェース・ネットワーク等

QKDとPQCのハイブリッドについて

	量子鍵配送(QKD)	耐量子計算機暗号(PQC)
	物理的アプローチ	**数学的アプローチ** 量子計算機でも計算困難な問題に基づく暗号
秘匿	**無条件安全**	計算量的安全
認証	他の技術と組み合わせる前提	あり
通信距離	制約あり⇒ネットワーク化で延伸	制約なし
実装	専用HWが必要	**SWで実装可**

コンピュータの発展によらず安全な鍵配送を提供
→**“Store now, decrypt later”** 攻撃(*)に対しても安全 (*)通信路上を流れるデータを傍受し、保存しておき、後で解読する攻撃

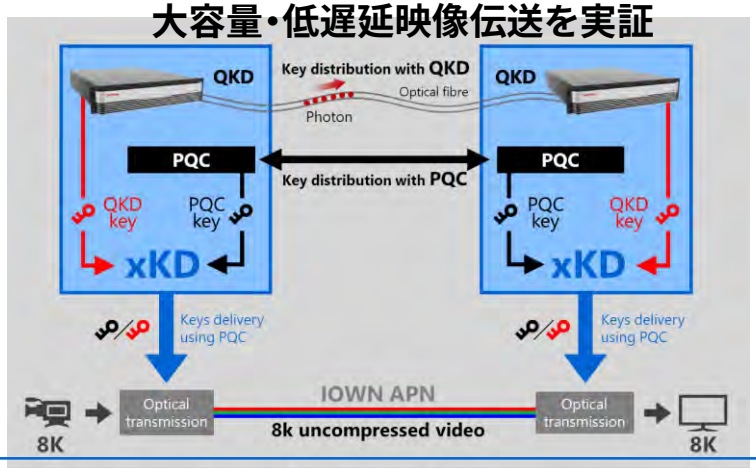


長期的に機密保持が必要な情報が流れる通信路など

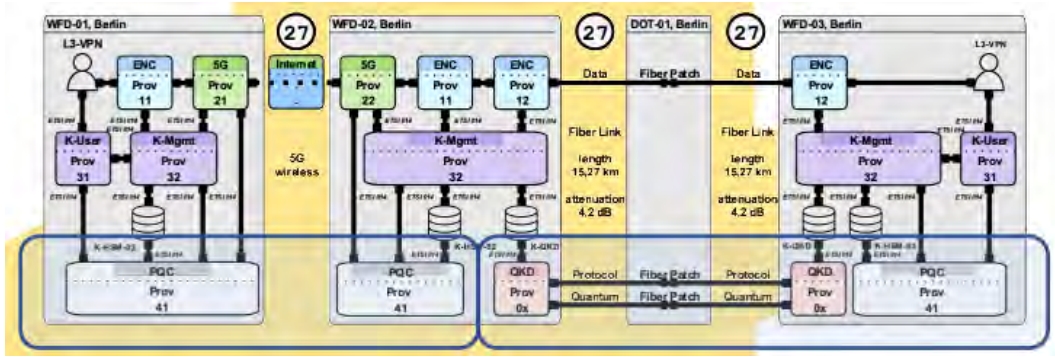
IOT・モバイル機器との通信、公開情報・機密保持が短期で良い情報の通信など

事例

NTT社と共同で、PQCとQKDを組み合わせた大容量・低遅延映像伝送を実証



DT社(ドイツテレコム)、IDQ社と共同で、PQCとQKDを組み合わせた鍵配送ネットワークを実証



https://www.itu.int/en/ITU-T/webinars/20210526/Documents/Andreas%20Poppe_Presentation.pdf?csf=1&e=ol42va

TOSHIBA

ご清聴ありがとうございました。

- 本資料は無断複製、無断改編、無断転載、無断使用（転用）を禁じます。
- 本資料に表記されている数値および表現は2022年11月現在のものです。
- 本資料の内容は予告無く変更されることがあります。
- 本資料に掲載の社名及び商品名はそれぞれ各社が商標または登録商標として使用している場合があります。