量子鍵配送の最近の動向について

株式会社東芝
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

TOSHIBA

© 20XX Toshiba XXX Corporation
© 2026 Toshiba Corporation

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)

- 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

© 2026 Toshiba Corporation

量子コンピュータに対抗するソリューション

- ２種類の主要な技術

量子鍵配送 Quantum Key Distribution (QKD)

- 物理学的アプローチ(新しいアプローチ)
- “理論”による安全性 (情報理論的安全)
  ⇒コンピュータの発展によらず安全
  ⇒データ・ハーベスティングへの耐性がある
- 鍵交換のみ
- 専用のハードウェアが必要

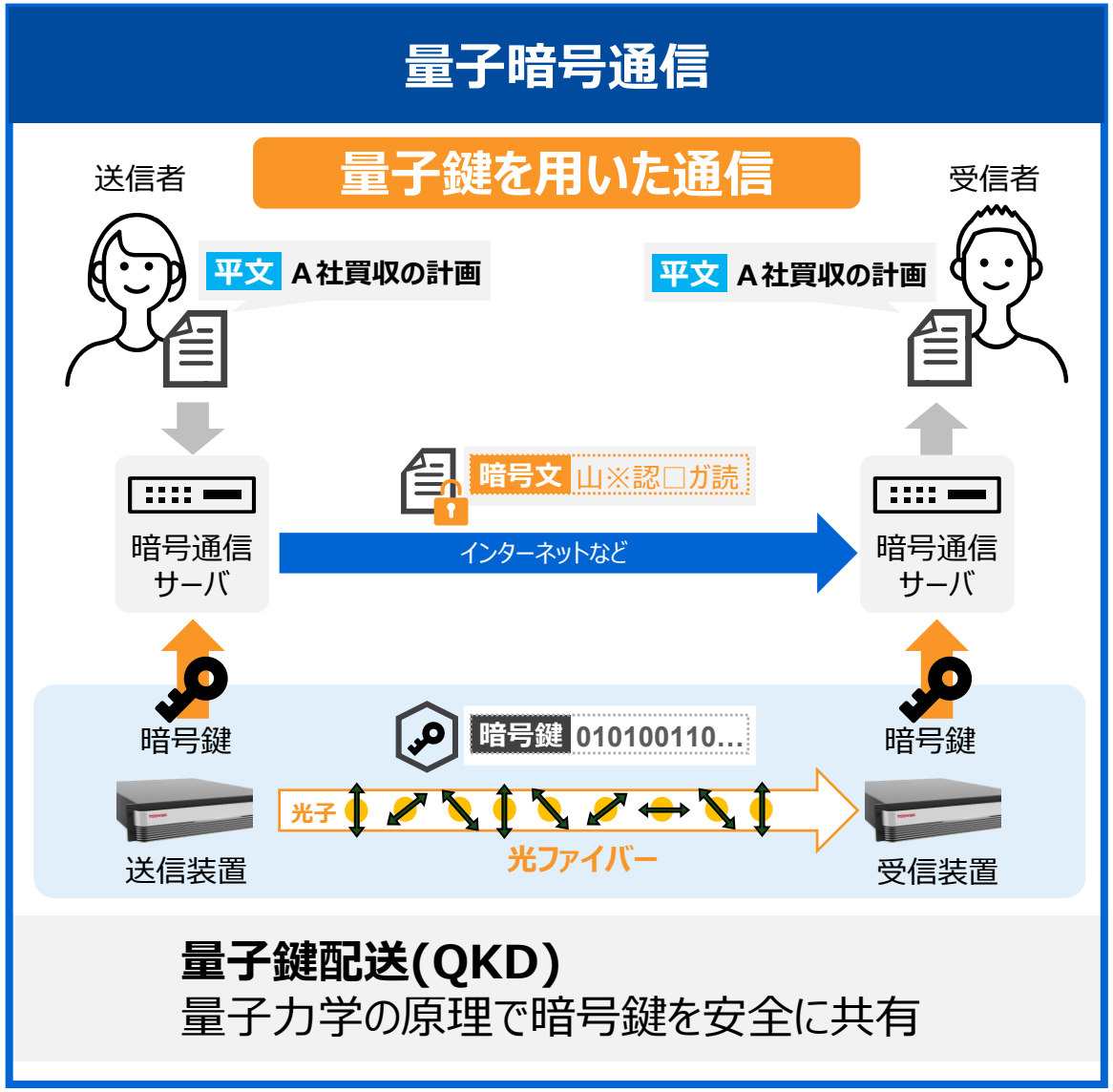
耐量子計算機暗号 Post Quantum Cryptography (PQC)

- 数学的アプローチ(従来と同じアプローチ)
- “解読に必要な計算量の膨大さ”による安全性(計算量的安全)⇒コンピュータや解読アルゴリズムの発展により破られる可能性を排除できない
- 多機能 (秘匿通信、電子署名)
- ソフトウェアで実装可能⇒実装が容易

それぞれの特長を活かしたハイブリッドなソリューションになっていく

© 2026 Toshiba Corporation

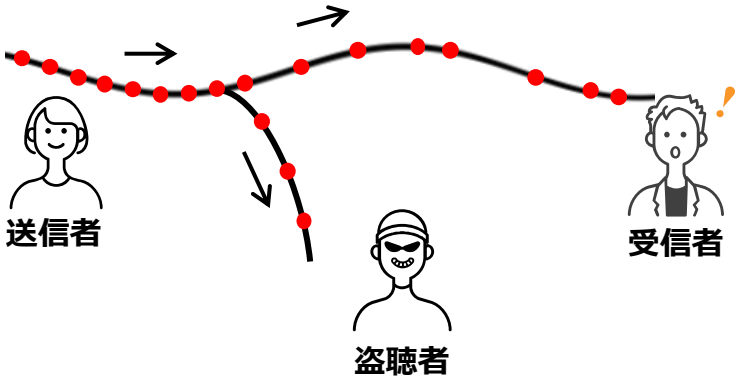
量子鍵配送(QKD)と量子暗号通信



© 2026 Toshiba Corporation

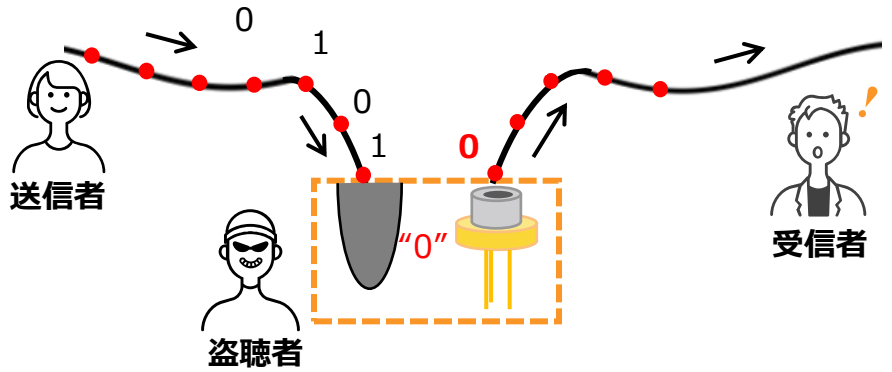
量子鍵配送：Quantum Key Distribution (QKD)

「光子は分割できない」



⇒ **受信した光子は安全**

「光子状態は完全にはコピーできない」



⇒ **異なる状態の光子が届く**

エラーを確認することで、確実に盗聴を検知できる

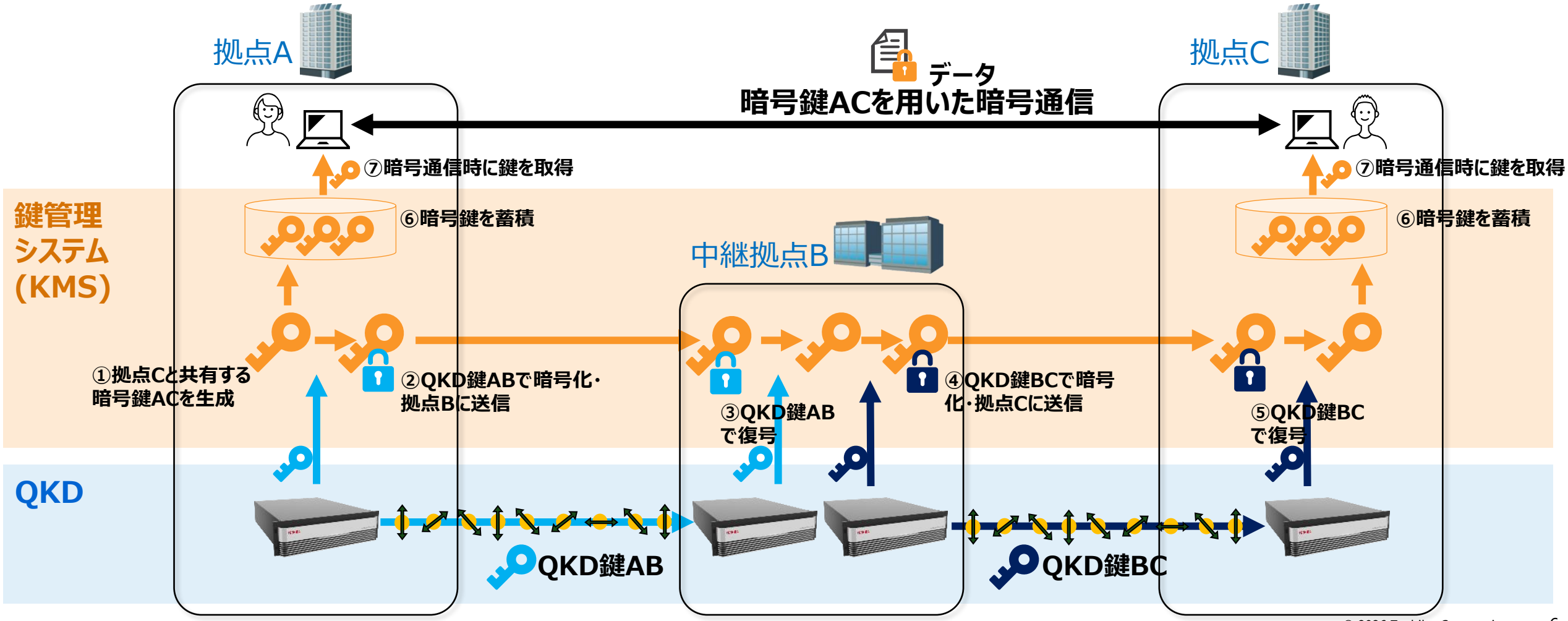
盗聴されずに交換された"光子"に乗せた情報に基づき「暗号鍵」を生成する

光子の量子力学的な性質を利用して、盗聴なしと保証された「暗号鍵」を共有

© 2026 Toshiba Corporation

量子鍵配送(QKD)の長距離化・ネットワーク化

複数の量子暗号装置を数珠つなぎにしてネットワーク化することで、任意の距離・拠点間で安全な暗号鍵共有が可能となる。暗号鍵は蓄積し、暗号通信時に利用する。



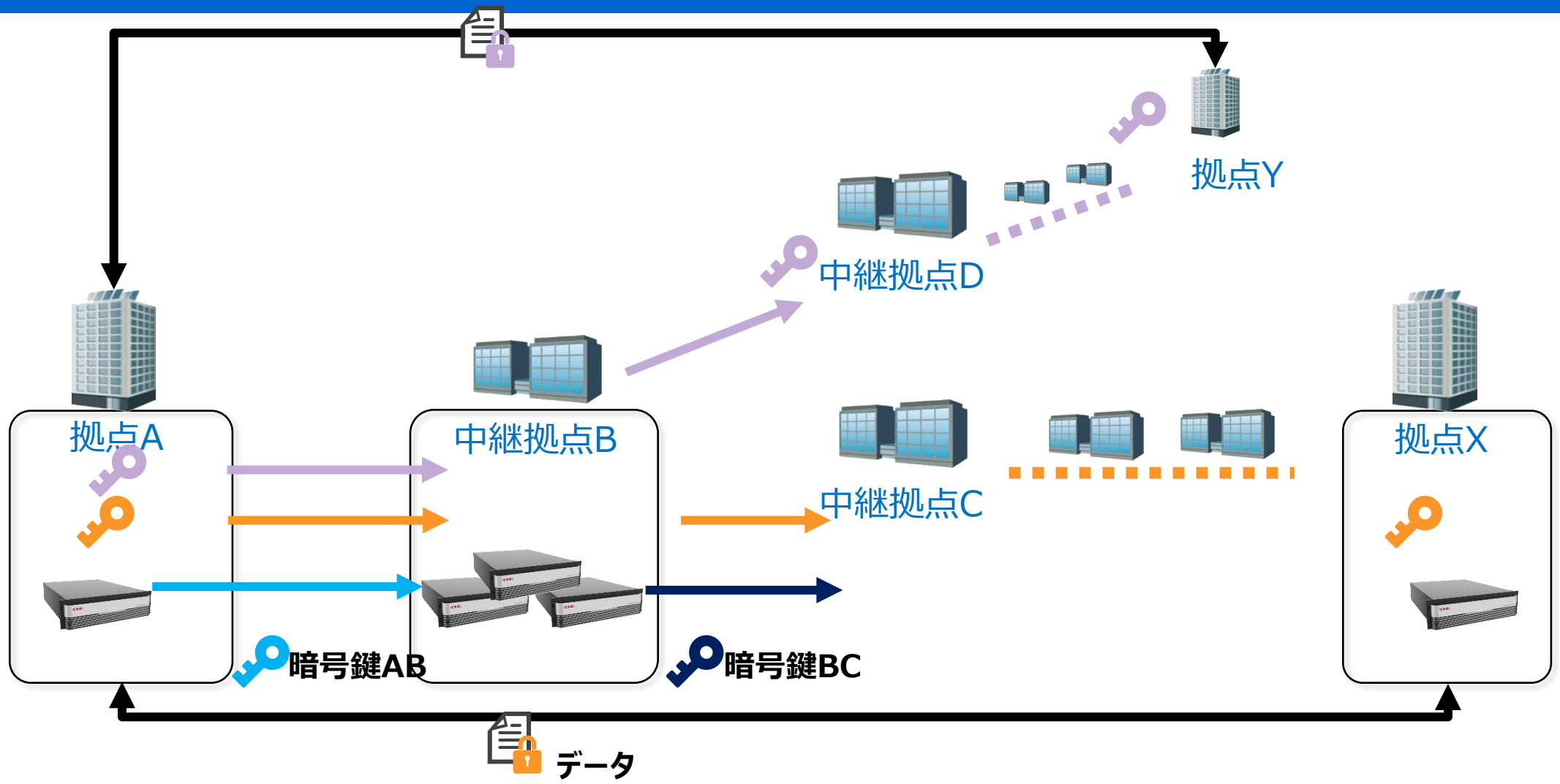
QKD: 光ファイバを直接接続可能な拠点間での鍵交換

QKD: 光ファイバを直接接続可能な拠点間での鍵交換

© 2026 Toshiba Corporation

量子鍵配送(QKD)の長距離化・ネットワーク化

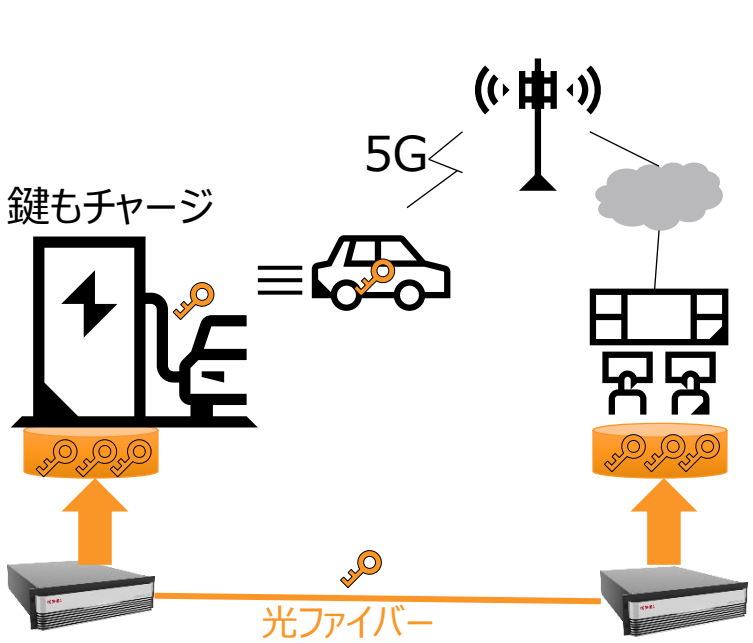
中継拠点を整備すれば、長距離化・多地点化が可能



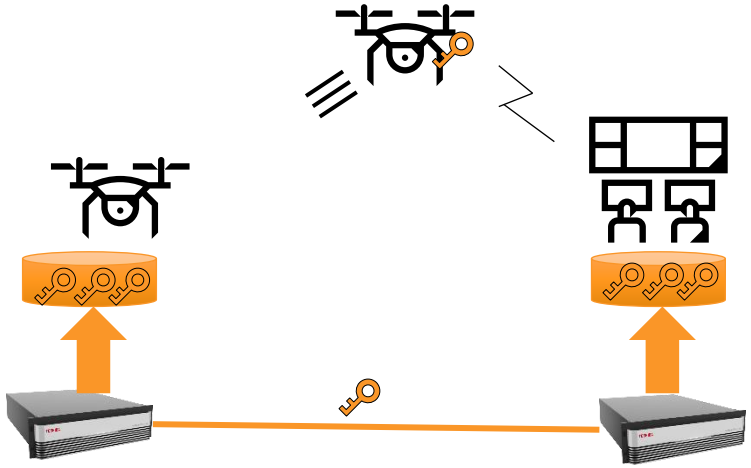
© 2026 Toshiba Corporation

移動体での活用

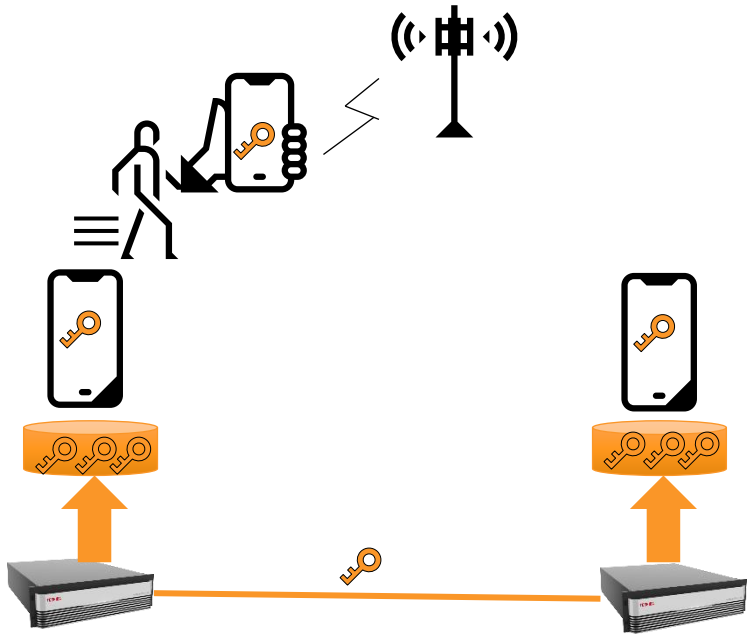
暗号鍵を事前に移動体に蓄積することで、移動中も通信が可能



自動運転



ドローンによる監視

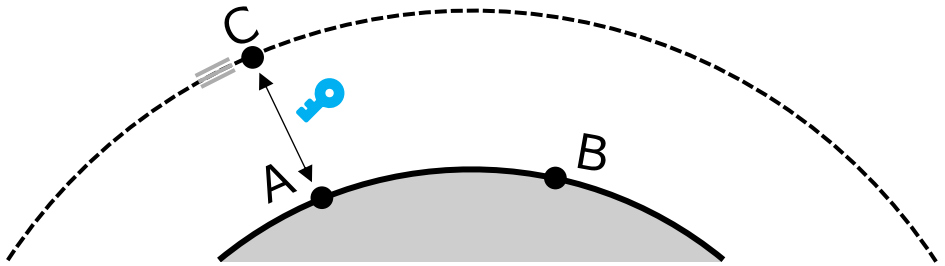


携帯電話

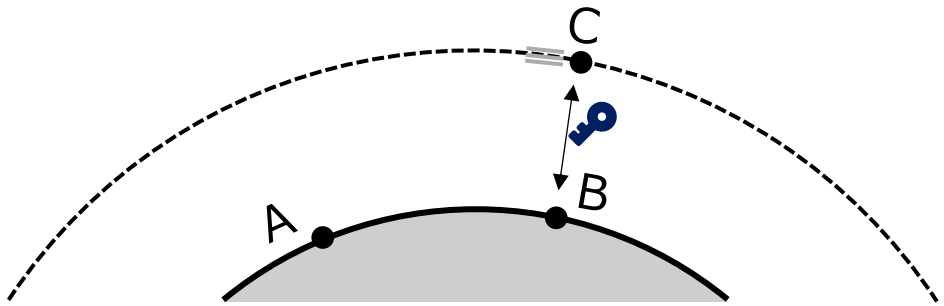
© 2026 Toshiba Corporation

衛星QKDを用いた暗号鍵共有の例

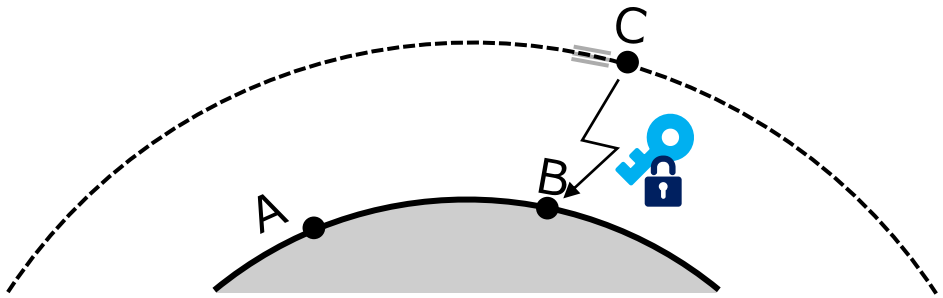
C: 低軌道衛星



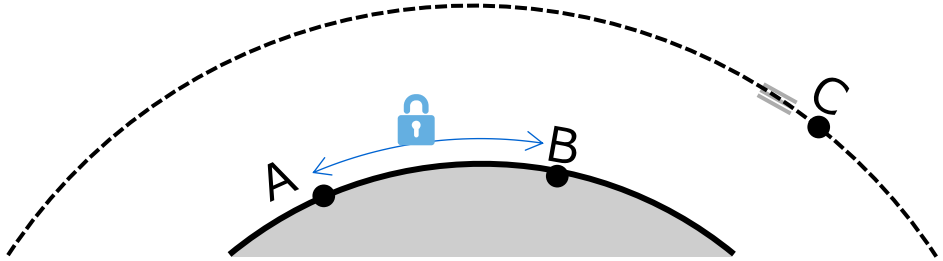
Step1: AとCが暗号鍵 をQKDで共有



Step2: BとCが暗号鍵 をQKDで共有



Step3: CがBに を で暗号化して送信
(通常の通信で良い)



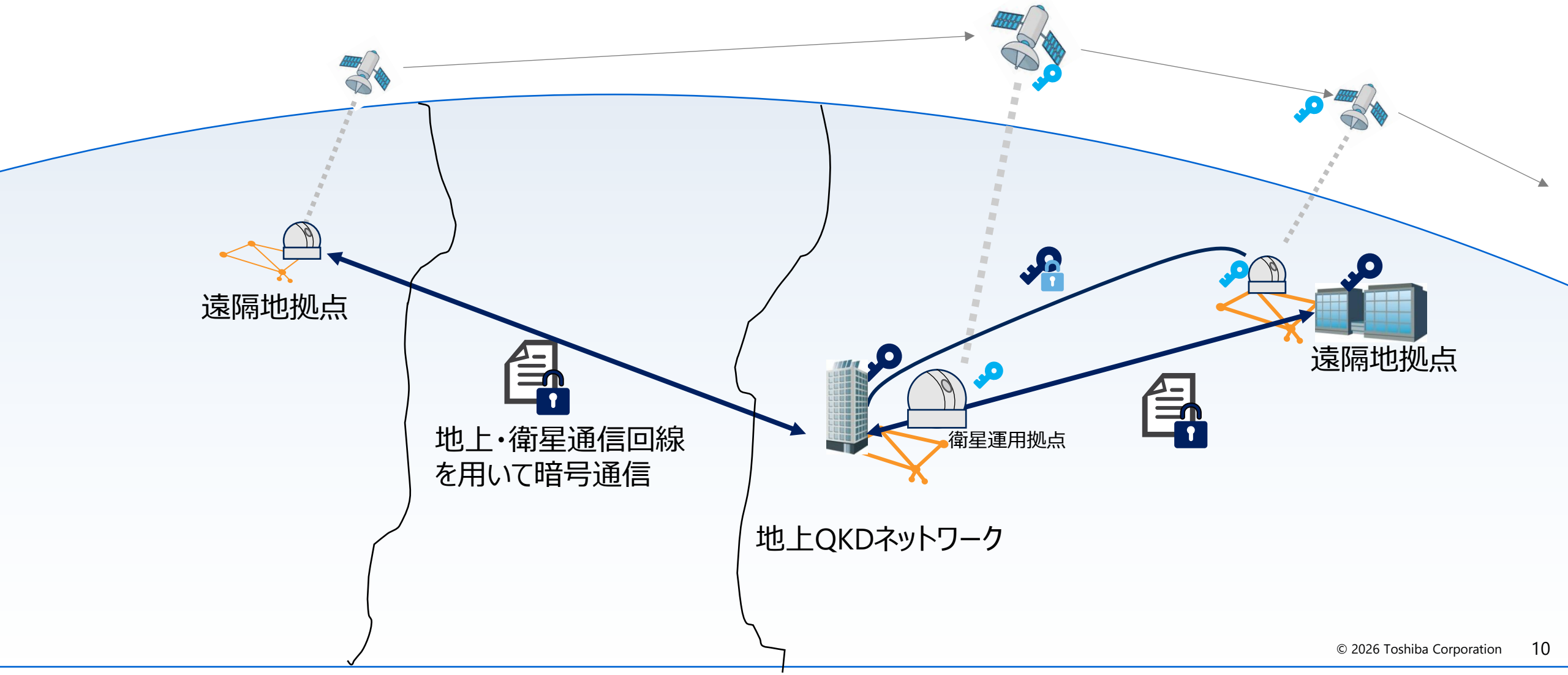
Step4: AとBが を使って暗号通信
(インターネットなど通常の通信で良い)

出典：https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf

© 2026 Toshiba Corporation

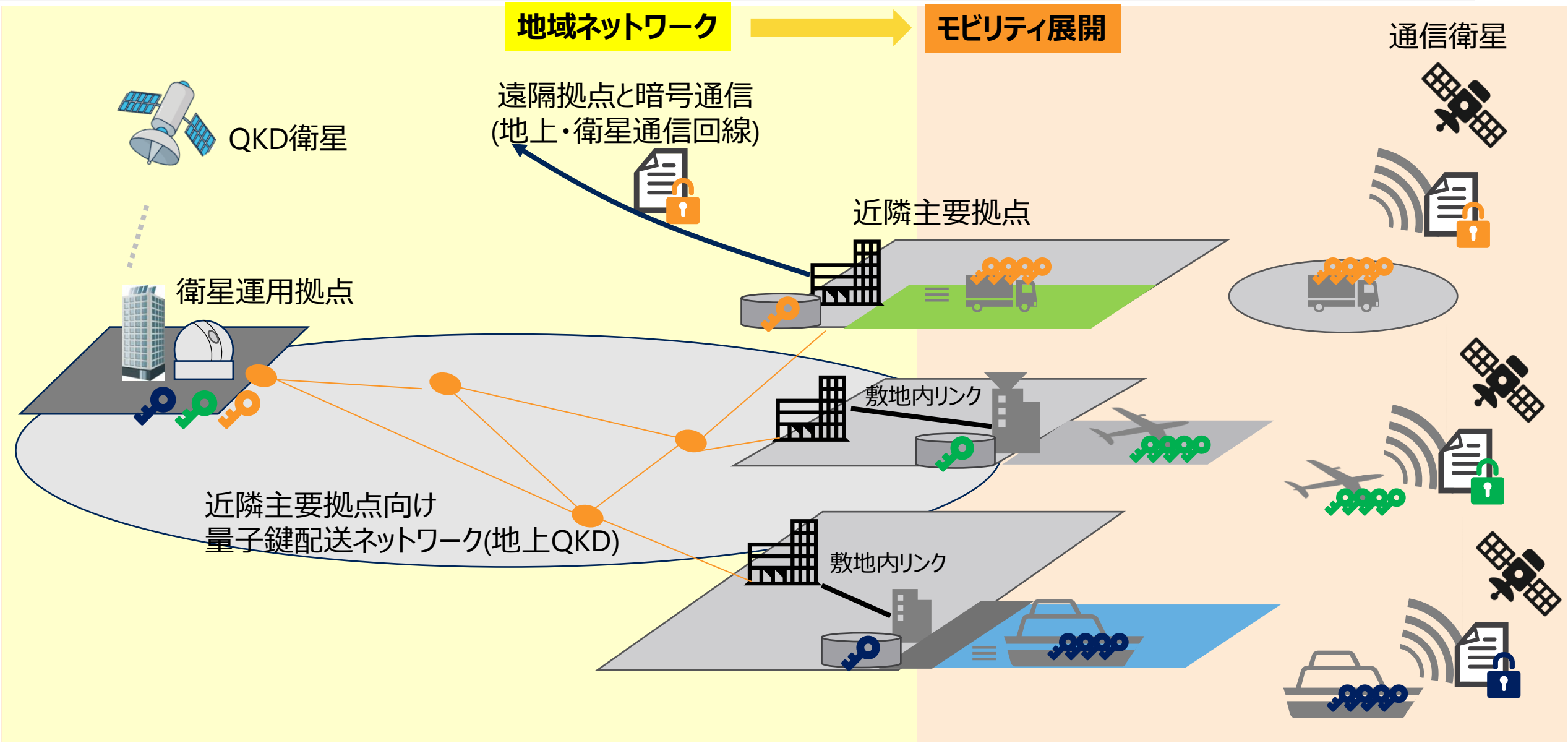
量子セキュア広域通信ネットワーク

遠隔地拠点に安全に暗号鍵を供給、地上・衛星通信回線を用いて暗号通信



© 2026 Toshiba Corporation

地域ネットワーク＋モビリティ展開



© 2026 Toshiba Corporation

先行国の動向

＊2026年10月時点

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

欧州：全域でQKDネットワーク実装活発化

- 2022年より**EU27ヵ国参画**のQKDの社会実装プロジェクトEuroQCI (Quantum Communication Infrastructure)が始動。

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

韓国：国家政策として推進

- 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

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 (NQSN+)が発表され、2024年に商業利用テストベッドが始まる

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

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

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

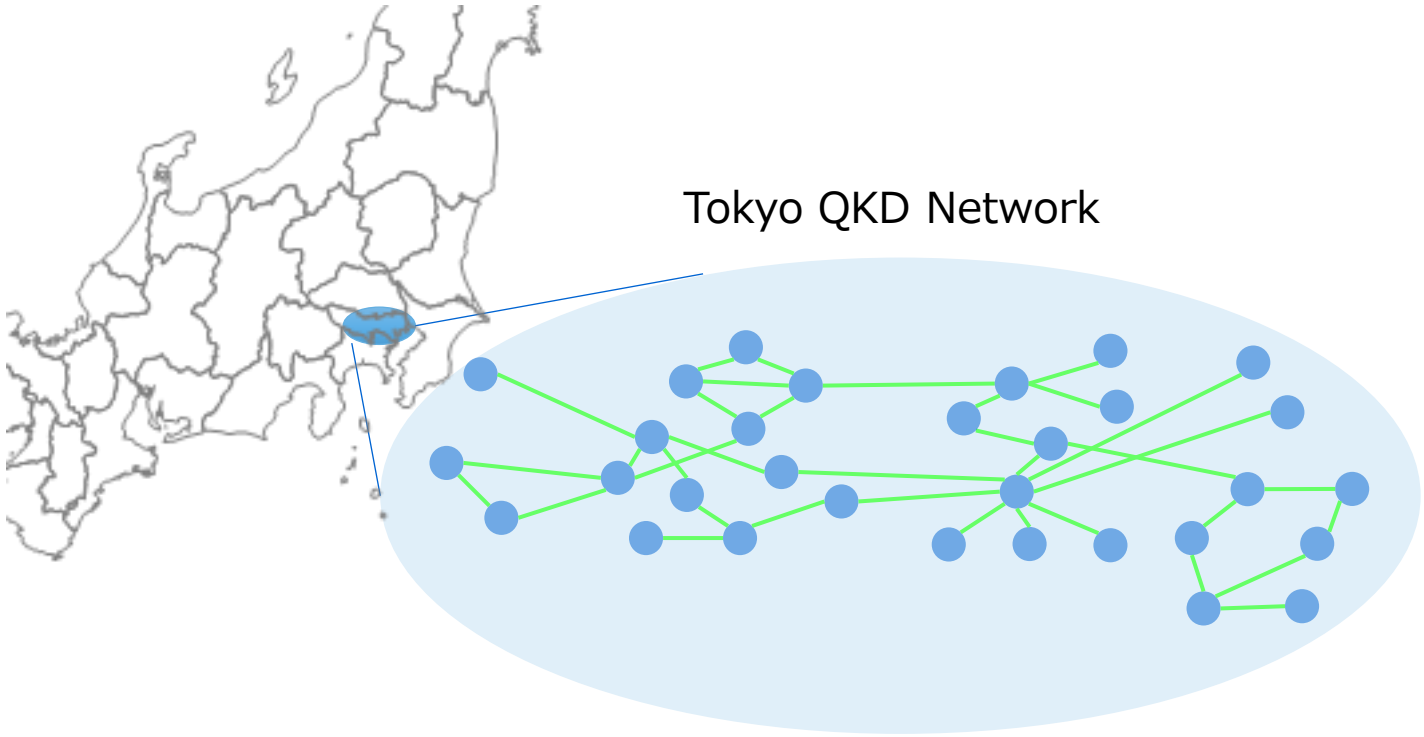
- NICTが中心となり運用される東京QKDネットワークをベースとした研究開発・実証や、金融・医療分野をターゲットとした社会実装PoCを、総務省・内閣府等の国家PJにより推進。国際標準化をリード。

日本、中国、欧州、韓国が技術開発を牽引
QKDネットワークの社会実装が進行

© 2026 Toshiba Corporation

東京QKDネットワーク(2023～)

- 国立研究開発法人情報通信研究機構(NICT) が、2023年より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
- 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

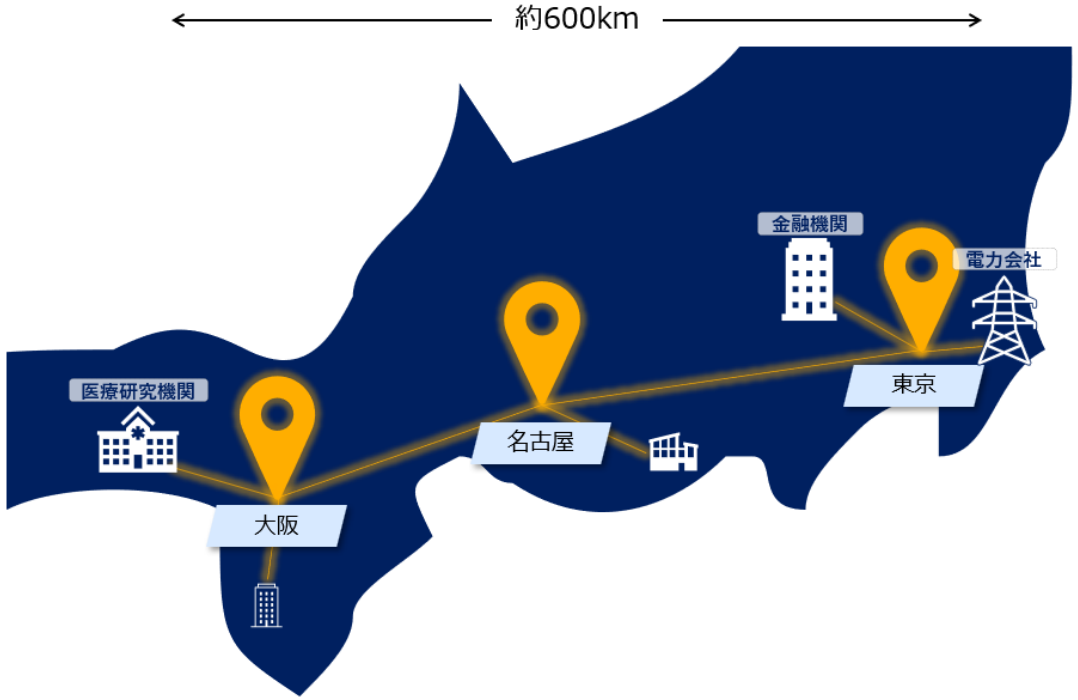


Quantum-inspired optimization solution
SQBM+™

© 2026 Toshiba Corporation

広域量子暗号通信ネットワーク

- 三大都市圏(東京、名古屋、大阪)を結ぶ約600kmの広域量子暗号通信ネットワーク構築を開始(2026年6月公表)
- 機密性の高いデータを扱う、医療、金融、電力業界などでの社会実装を見据え、量子技術による安全な通信技術の検証を進めることで、有望なユースケースの創出をめざす
- 東芝は、量子鍵配送装置の提供、量子鍵配送ネットワーク構築、技術検証・ユーザー実証を実施予定



広域量子暗号通信ネットワークの構築イメージ



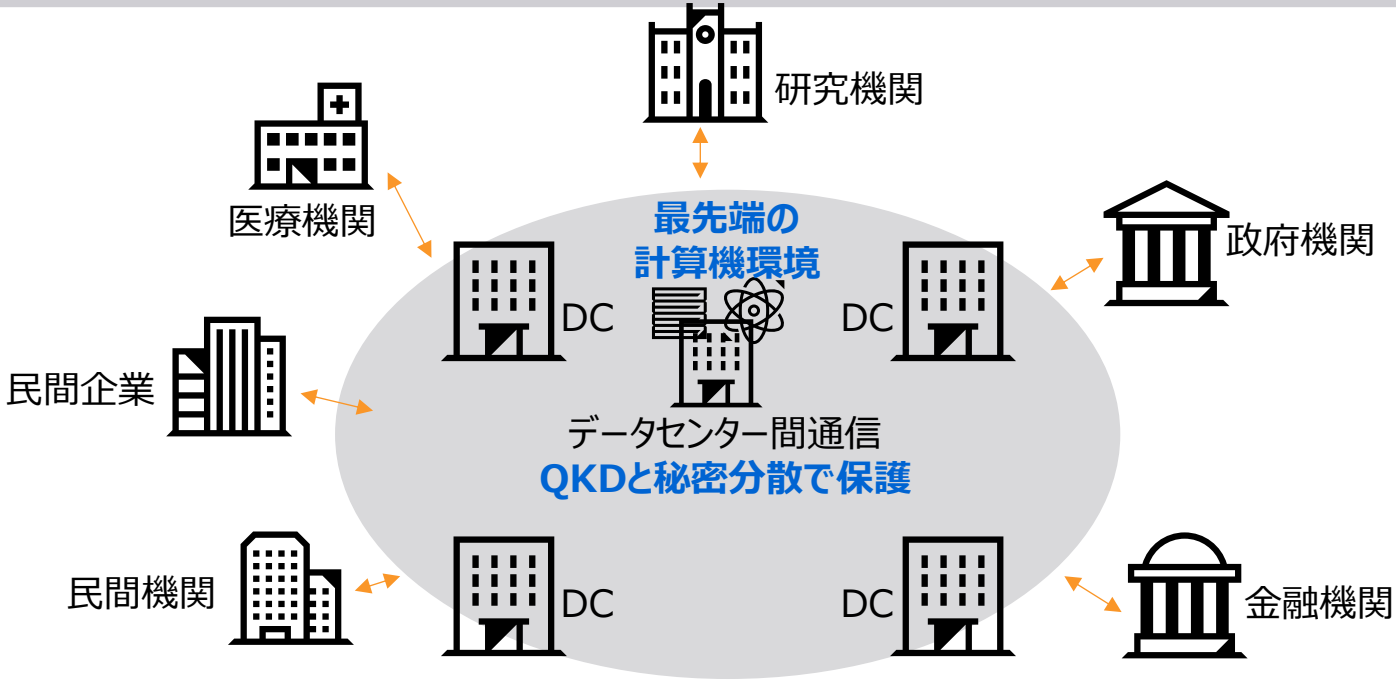
東芝QKDシステム

テストベッド構築参画企業
NTTドコモビジネス、東芝、日本電気、エクシオグループ、エクシオ・デジタルソリューションズ、エヌ・ティ・ティ エムイー、デロイトトーマツ、さくらインターネット

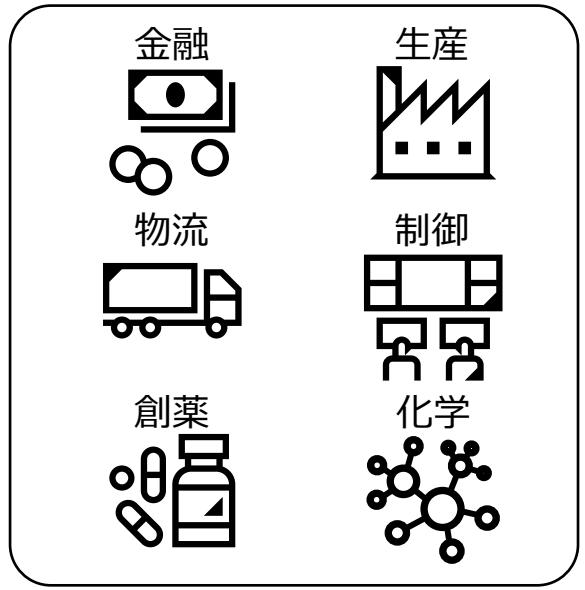
(東芝プレスリリース)
https://www.global.toshiba/jp/news/digitalsolution/2026/06/news-20260630-01.html

© 2026 Toshiba Corporation

量子セキュアクラウド



適用領域



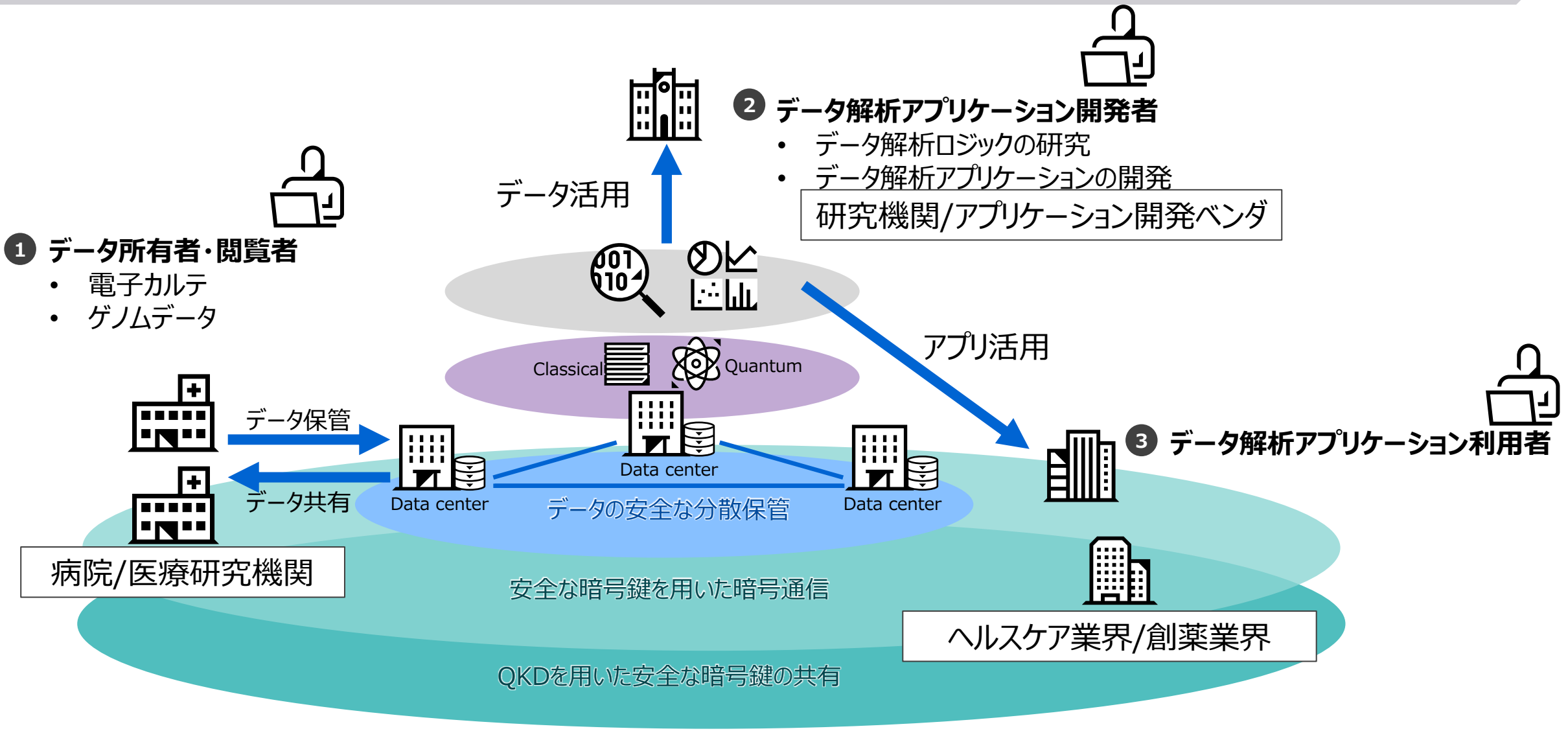
- 秘密分散を用いてデータを安全に分散保管⇒災害やサイバー攻撃に対する耐性
- データの分散・収集に伴う通信はQKDで保護
- 最先端の計算機環境(古典及び量子)を配備

長期に秘密保持が必要なデータを管理する負荷から解放される
複数機関とのデータ連携が容易になる
データ解析などに最先端の計算環境を利用できる

本研究開発は，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）「先進的量子技術基盤の社会課題への応用促進」（研究推進法人：QST）によって実施しています。

© 2026 Toshiba Corporation

医療分野における活用イメージ



© 2026 Toshiba Corporation

東芝における量子暗号通信の技術開発と実証試験

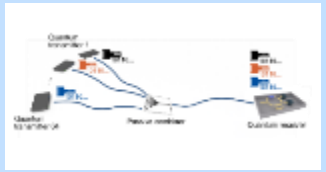
技 術 開 発



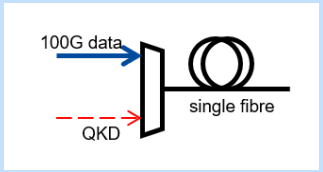
QKD>100km



QKD>1Mb/s



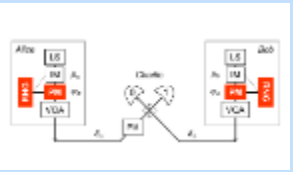
量子アクセス
ネットワーク



QKD 多重化



QKD>10Mb/s



Twin-field QKD



QKDチップ



QKD装置

事業開始

2004 2010 2013 2016 2018 2019 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+

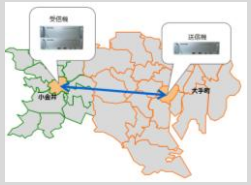
メトロネットワークの
商用トライアル
BT, 2022

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

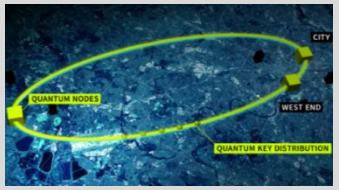
衛星搭載用
QKD送受信
システム実証,
英国,2026

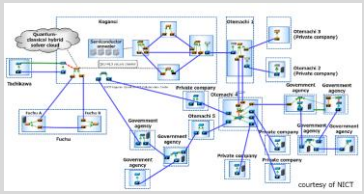


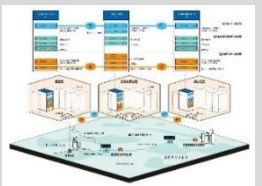


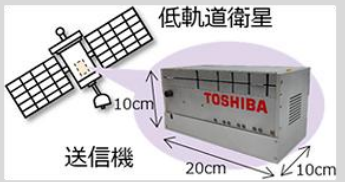












実 証 試 験

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

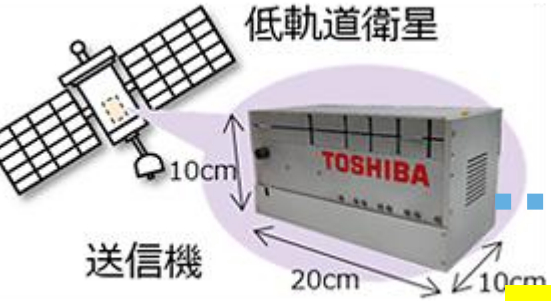
*2 https://openqkd.eu/

© 2026 Toshiba Corporation

最近の研究成果：衛星QKDへ向けた研究開発

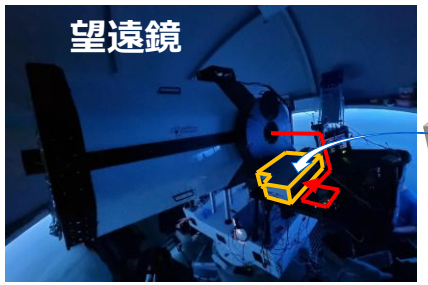
将来向け研究

望遠鏡と衛星向け装置を使った自由空間リンクとファイバー向け装置のリンクを接続して英国Heriot-Watt大学構内で量子暗号通信を実証 (2025)



衛星搭載を念頭に設計された
小型QKD送信機

1m 自由空間





衛星QKD受信機

LAN



ファイバーQKD受信機

1km 光ファイバー



ファイバーQKD送信機

HERIOT WATT UNIVERSITY

SINGLE-PHOTON GROUP



TOSHIBA

暗号化

HERIOT WATT UNIVERSITY

ワンタイムパッドで暗号化



暗号化されたデータを送信

復号

TOSHIBA

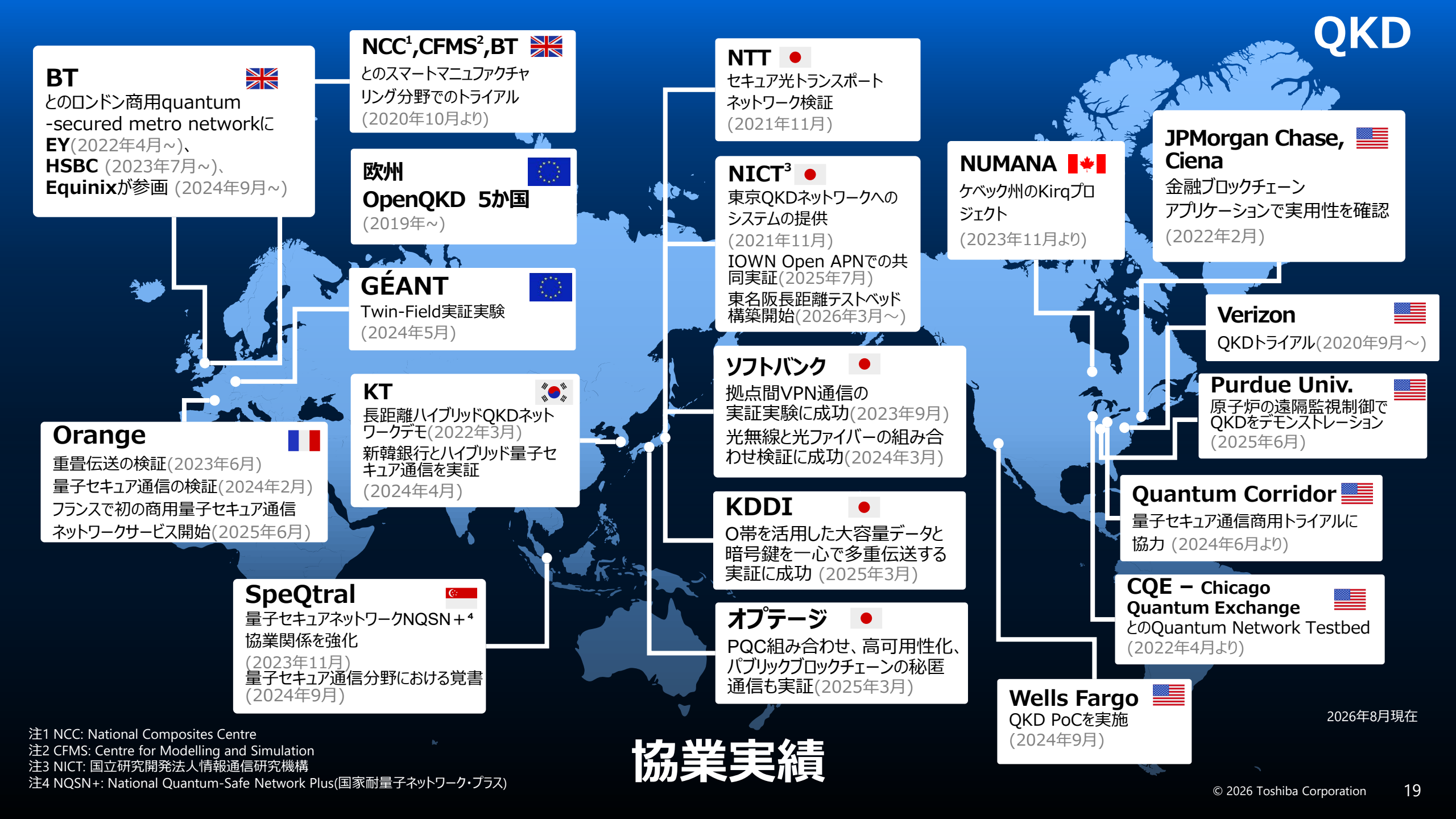
HERIOT WATT UNIVERSITY



ワンタイムパッドで復号した画像

R. Singh, et al., "*Integration of a Polarization based QKD Receiver Module to an Optical Ground Station*", IEEE ICSOS 2025.
This work has received funding from Innovate UK (project 10089202)

© 2026 Toshiba Corporation



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)
東名阪長距離テストベッド構築開始(2026年3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)

2026年8月現在

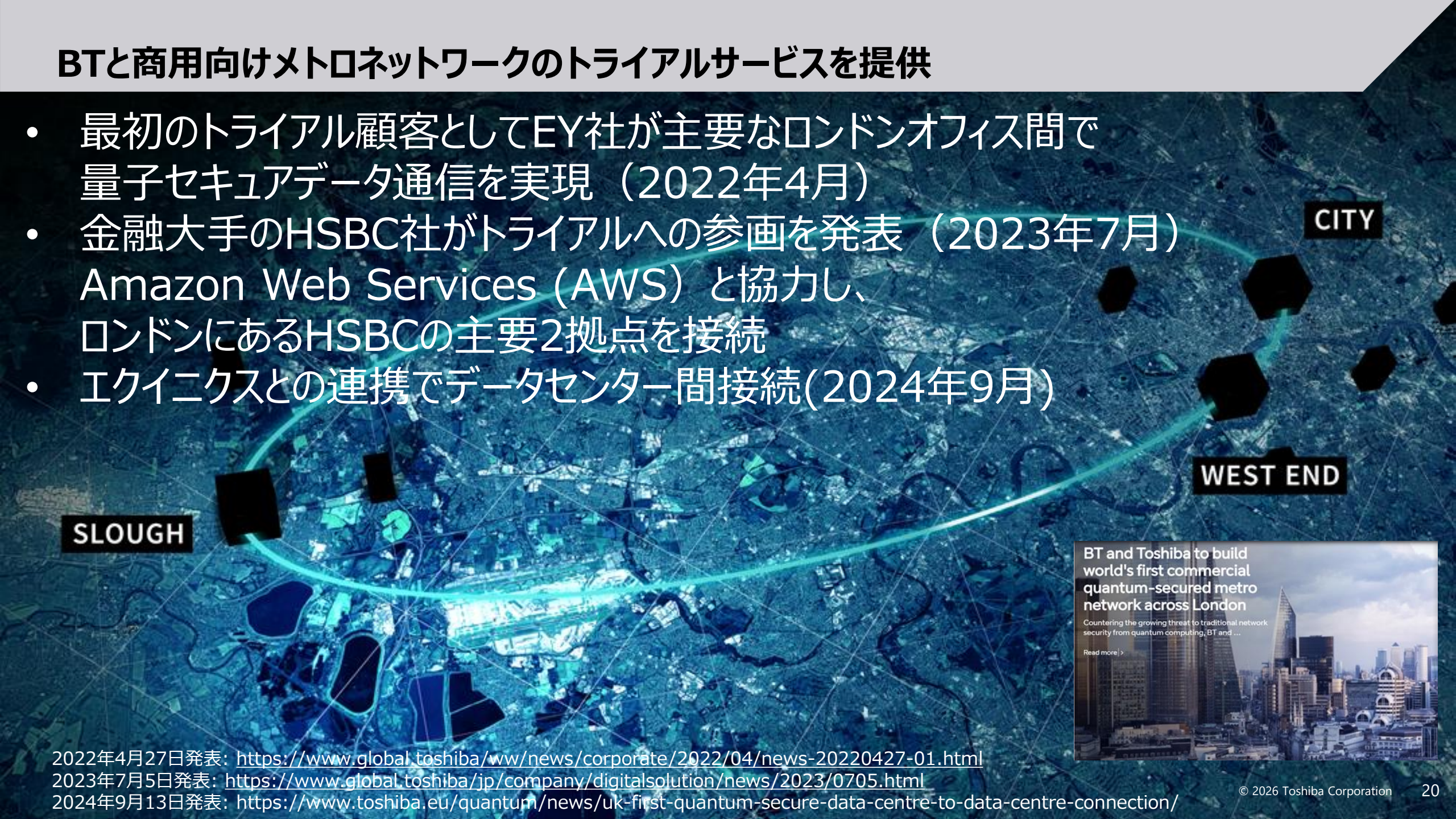
協業実績

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)

© 2026 Toshiba Corporation

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を発表（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
- エクイニクスとの連携でデータセンター間接続(2024年9月)



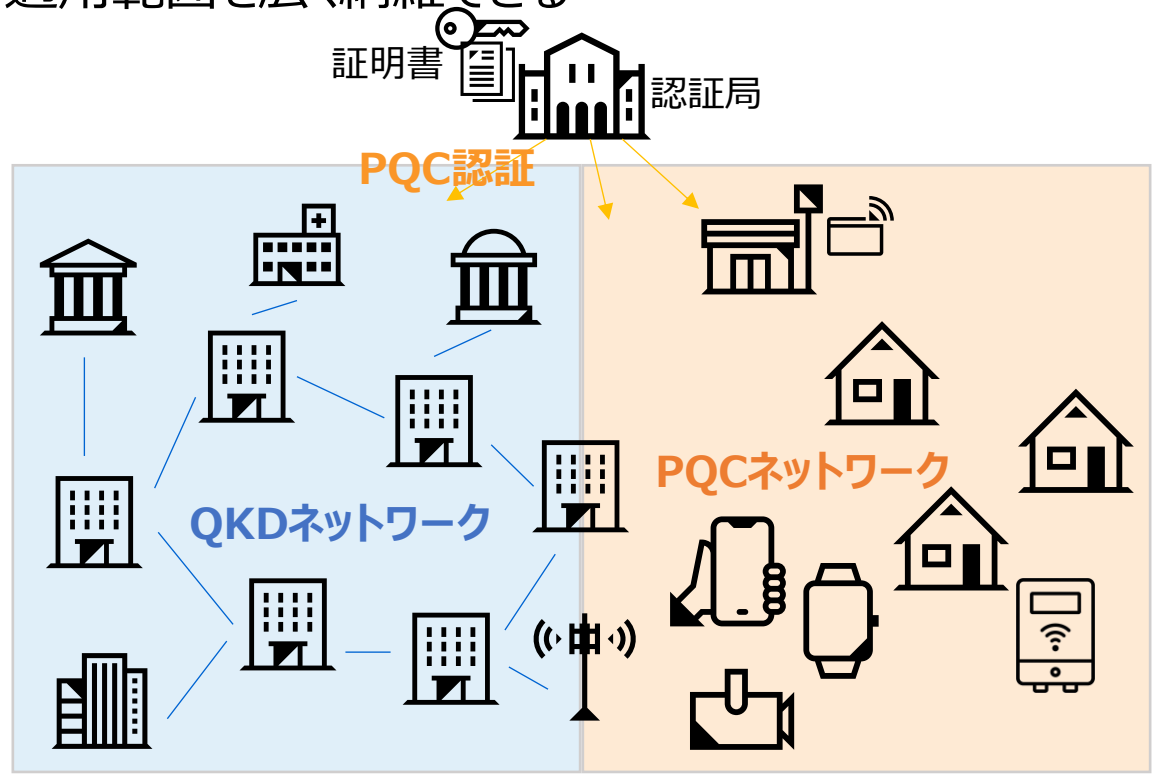
2022年4月27日発表: https://www.global.toshiba/ww/news/corporate/2022/04/news-20220427-01.html
2023年7月5日発表: https://www.global.toshiba/jp/company/digitalsolution/news/2023/0705.html
2024年9月13日発表: https://www.toshiba.eu/quantum/news/uk-first-quantum-secure-data-centre-to-data-centre-connection/

© 2026 Toshiba Corporation

QKDとPQCのハイブリッド

1. 適用先の特性に合わせて適切な技術を選択・統合し適用範囲を広く網羅できる

	QKD	PQC
通信データ	・長期利用データ ゲノム解析、医療カルテ、政府機関、安全保障、顧客情報、バックアップ ・重要社会インフラ 電力、ガス、鉄道、空港	・短期利用データ インターネットバンキング、制御信号 ・Webアクセス ・IoT機器 ・電子署名 ・デジタル署名
通信ネットワーク	・コアネットワーク ・データセンタ間接続	・アクセスネットワーク ・インターネット ・無線通信
機能	通信の機密保持	通信の機密保持+認証



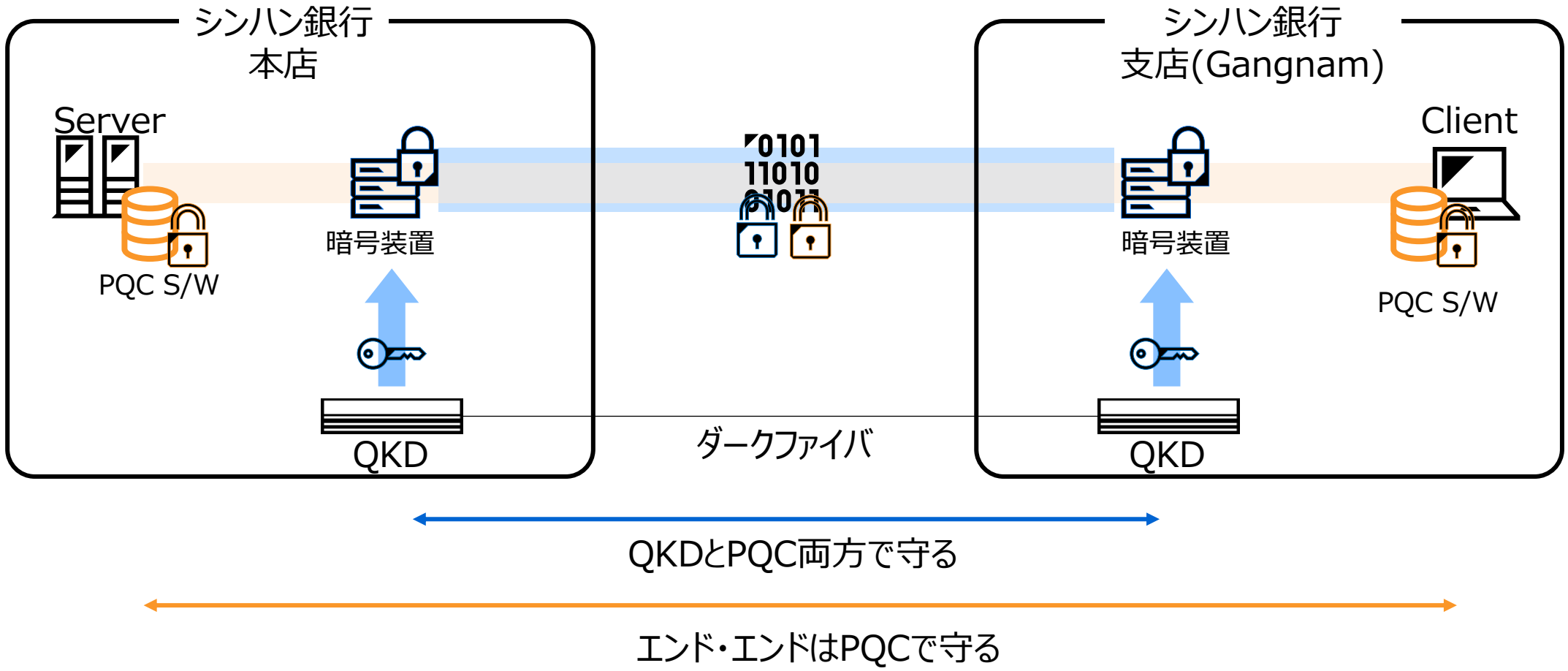
2. QKDとPQCによる保護で高可用性を実現
   - システム障害に対するロバスト性向上



© 2026 Toshiba Corporation

ハイブリッドの実証例(多重防御による高可用性)

韓国シンハン銀行とのPoC



https://www.global.toshiba/jp/news/digitalsolution/2024/04/news-20240419-01.html

© 2026 Toshiba Corporation

商用化　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を提供開始

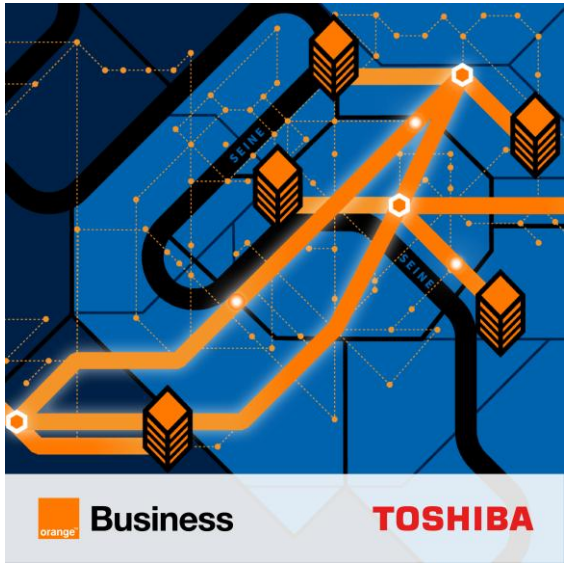
- 2025年6月11日、Orange Business 社（注）と、フランスで初となる量子セキュア通信ネットワークサービス「Orange Quantum Defender（OQD）」の**商用利用**をパリで提供開始した
- OQDサービスは、東芝の量子鍵配送（QKD）と耐量子計算機暗号（PQC）を組み合わせ多層防御した量子セキュア通信ネットワーク技術を利用している。
- 同サービスはパリ市とその周辺を含むパリ大都市圏で商用利用可能。フランスの大手金融サービス企業が最初の同サービスユーザーとなり、複数の拠点をつなぎ秘匿性の高い金融データのセキュリティを保ちながら通信を開始している。

注：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している。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11日発表：https://www.global.toshiba/content/dam/toshiba/jp/company/digitalsolution/news/pdf/news_20250611.pdf



«＝ 2025/6/11~13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、Orange Business社はOQDサービスを発表し、展示・デモを行った。

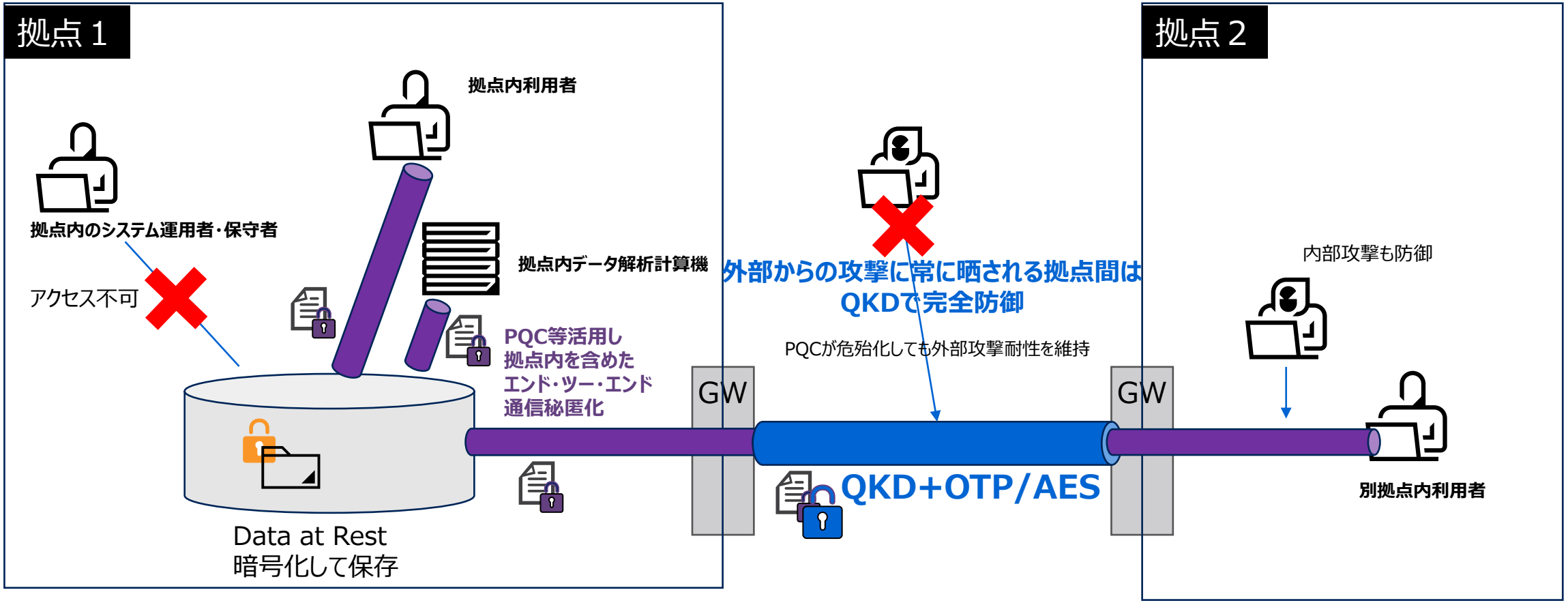


«＝ パリ量子セキュア通信ネットワークのイメージ図： QKD 3ノードで、リング状にコアネットワークを構成。各ノードよりユーザーアクセスリンクを張る。

© 2026 Toshiba Corporation

拠点内を含めたエンド･ツー･エンド防御

外部からの攻撃が容易な拠点間はQKDで完全防御⇒PQCが危殆化しても外部攻撃耐性を維持 ⇒ 基盤･インフラ
拠点内を含めたエンド･ツー･エンドはアクセス権に応じて適切に秘匿化(PQC等活用) ⇒ アプリケーション個別の対策
様々な暗号鍵の管理が重要⇒HSM(Hardware Security Module)を活用し保護



© 2026 Toshiba Corporation

- 本資料に表記されている数値および表現は2026年10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。