

量子セキュリティ／量子ネットワークの産業の 今後について

東芝デジタルソリューションズ株式会社
村井 信哉
2021年12月6日

01

諸外国における社会実装の状況

量子鍵配送(QKD)ネットワークの社会実装が進む



サマリー

- 中国が広域網を拡大中
- 韓国と欧州が大規模QKDネットワークの構築に動き出す
- 米国エネルギー省が量子インターネット研究を推進

中国：既に広域インフラを構築

- 世界最大規模の量子暗号ネットワークを構築、国営企業が利用
 - 北京－上海間の政府向けバックボーン(2000km)。金融通信などに利用。
- 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)
- 量子メトロネットワークの実証も進む (2021、合肥市46ノード*1)

韓国：国家政策として推進

- SK Telecomが、2019年に自社の5G/LTEネットワーク(ソウル・デジョン地区)への適用を発表
- 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

欧州：キャリアの動き活発化、テストベッドが進行

- 2019年に欧州各国参画のテストベッド構築プロジェクトOPENQKDが始動、2022年に終了予定
- 2022年よりEU諸国でEuroQCI (Quantum Communication Infrastructure) 基盤整備事業が開始される見通し。

米国：エネルギー省がQKD、量子インターネットの研究を推進

- エネルギー省配下で17の研究機関が量子関連技術の研究開発を推進
- Qubitekk社が電力システム向けなどにQKDを事業化中
- 2021年には全米規模の量子インターネット整備5か年計画を発表

*1 <https://www.nature.com/articles/s41534-021-00474-3.pdf>

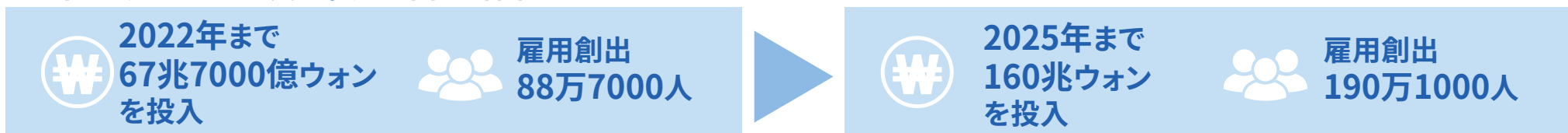


通信大手3社が公共・医療分野で量子暗号通信網を構築

(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



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

<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。

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)

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。

当社事例：EUのQKD実証実験へ参加（2019年～2022年）

ドイツ、ポーランド、オーストリア、イタリア、スペイン、英国のOpenQKD Testbedに参画中

OpenQKD Testbeds OPEN QKD

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
Partners: UNIVERSITY OF CAMBRIDGE, ADVA, BT, fragmentX
- Padua**
Combining satellite communications with terrestrial QKD infrastructure
Partner: POLITONICA
- Madrid**
Securing end-to-end communications for business-to-business & 5G networks
Partners: redi madrid, Telefónica
- Berlin**
Secure communication for 5G networks, with QKD and post-Quantum crypto
Partner: Deutsche Telekom
- Poznan**
Securing data centre communications for banking, healthcare and government
Partner: PSNC
- Graz & Vienna**
Secure secret sharing between hospitals & securing government ministry communications
Partner: AIT

© 2021 Toshiba Digital Solutions Corporation 17

OpenQKD: 汎欧州レベルでのQKDのTestbed。2019年9月より2022年8月末までの期間で実施。予算約18M Euroのうち、EUが約15M Euroを負担。テスト対象は13か国(オーストリア、チェコ、フランス、ドイツ、ギリシャ、イタリア、オランダ、ポーランド、スペイン、スイス、UK)で実施されており、東芝欧州社は6件のTestbedに参画している。

引用元；

<https://cordis.europa.eu/project/id/857156>

欧州動向 #2 EUの量子暗号通信イニシアティブ EURO QCI

2019年6月、7か国で欧州における量子通信インフラ(EURO QCI)の実現に向けて取り組むことに合意
2021年11月公募が開始



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

参加国

計25か国が共同声明に署名

概要

2019年6月のDigital Assemblyで、12か月にかけてEU地域での今後10年間のQCI(Quantum Communication Infrastructure)の開発、展開に関して協議することに合意。2021~2027の間、量子技術はHORIZON EUROPEと共にDigital Europe Programmeによってサポートされることが背景にある。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年中にQCIのフィージビリティ検証を終え、2022年より推進予定。

02

量子鍵配送ネットワークの今後について

今後の展開

- ネットワークの大規模化
 - 都市圏、全国網から、衛星網と地上網が結合したグローバル網へ
- 利用形態の変化
 - 専用システムから複数のユーザが利用する共用型鍵配送ネットワークサービスへ
- 新規技術の順次導入
 - 長距離化技術、装置の小型化技術、衛星、量子中継などが、既存のネットワークに導入・結合されていく。

量子鍵配送ネットワークの拡張のステップ

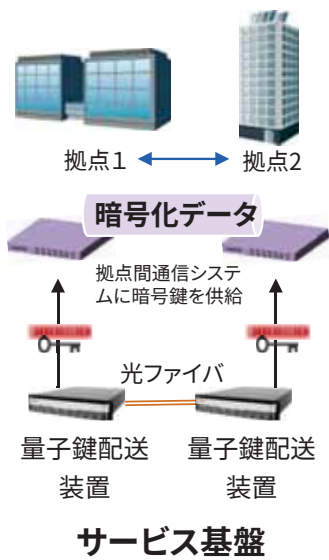
現在

1対1システム
(単一ユーザ専用)

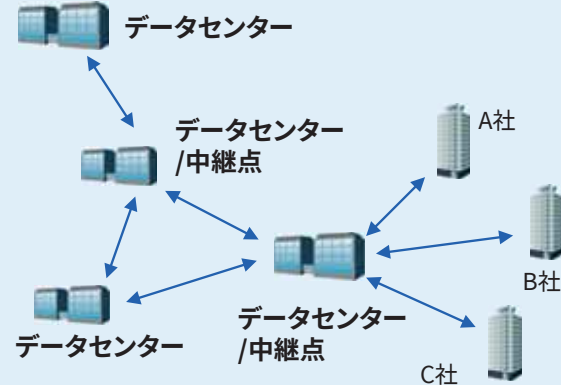
大都市圏・大都市間
(複数ユーザが顧客)

全国網

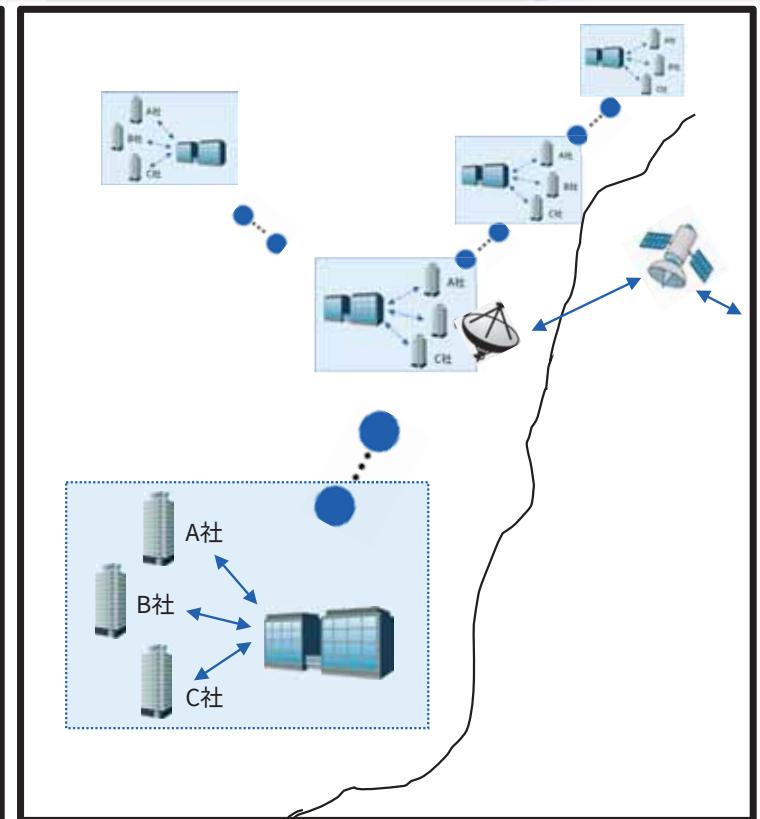
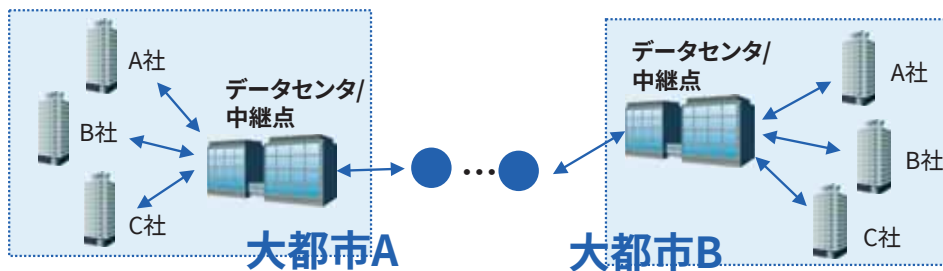
グローバル網



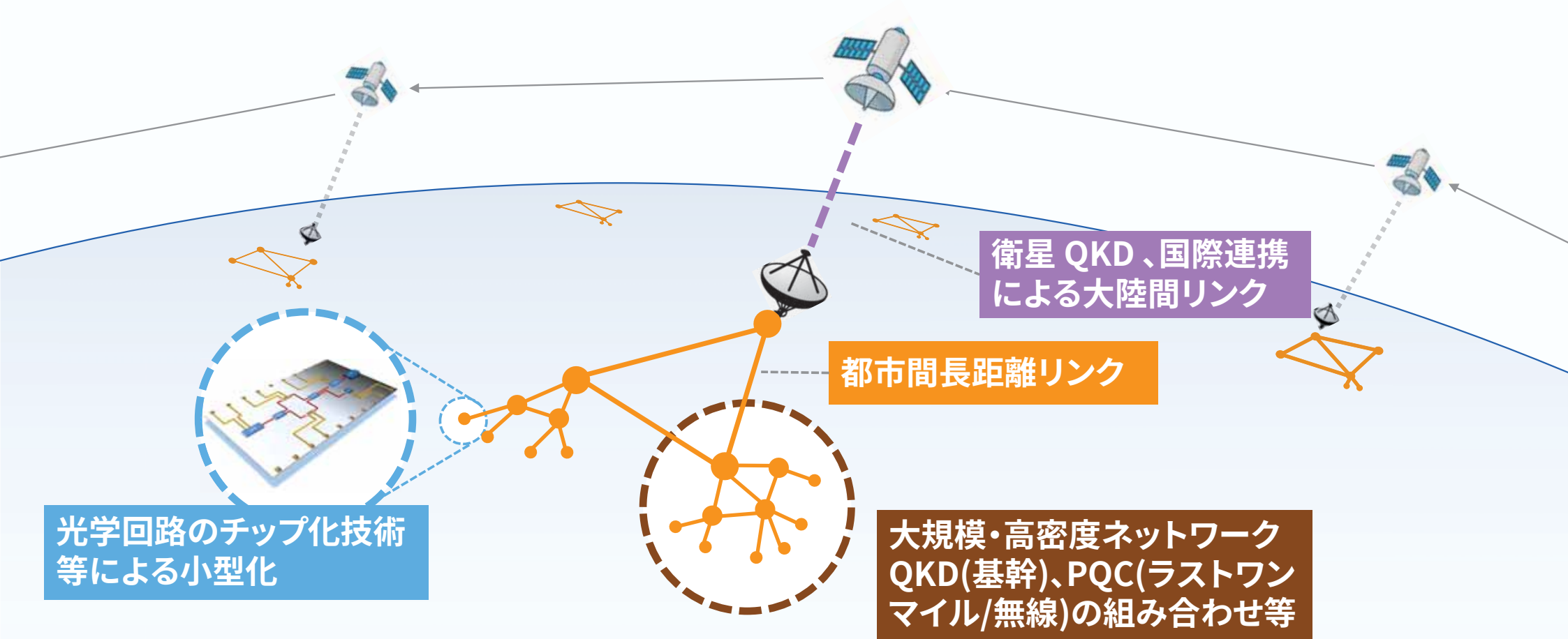
大都市圏



大都市間



グローバル網の姿



光学回路のチップ化技術等による小型化

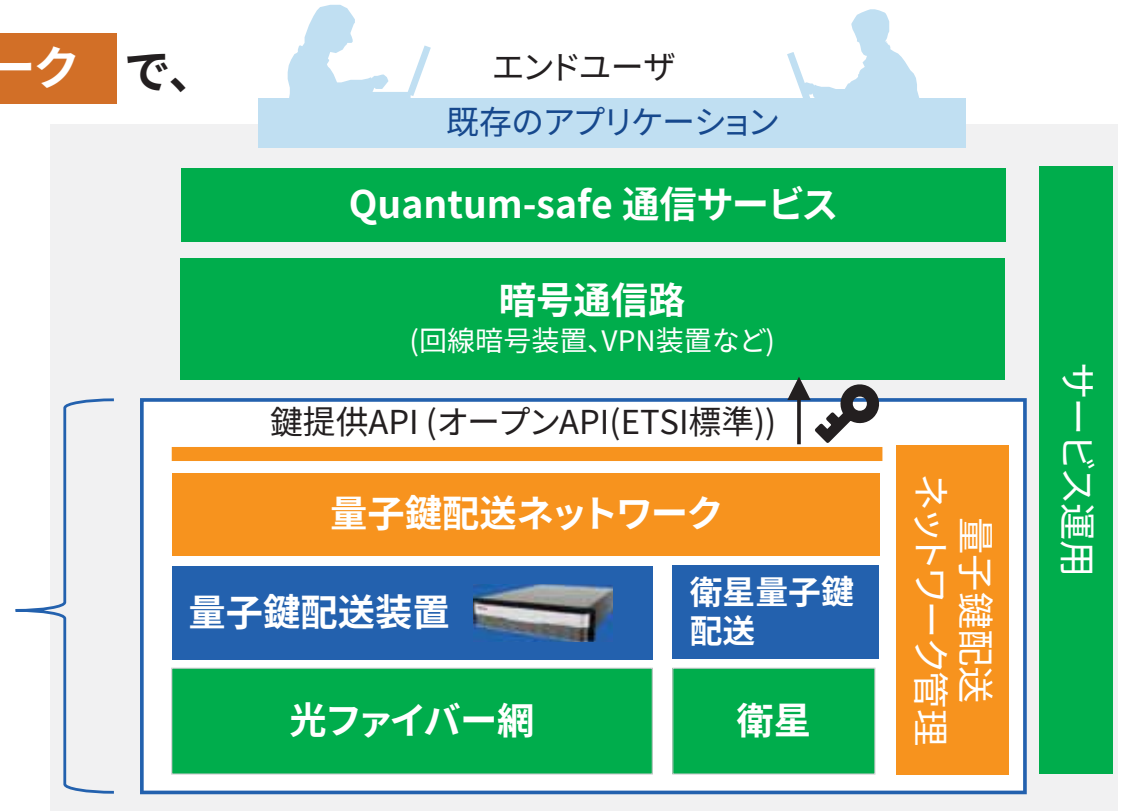
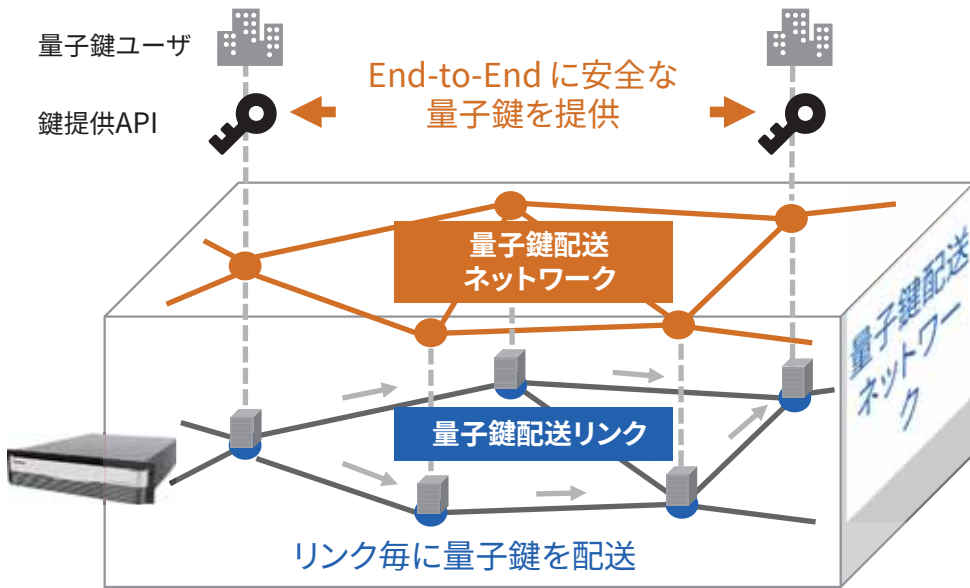
衛星 QKD、国際連携による大陸間リンク

都市間長距離リンク

大規模・高密度ネットワーク
QKD(基幹)、PQC(ラストワンマイル/無線)の組み合わせ等

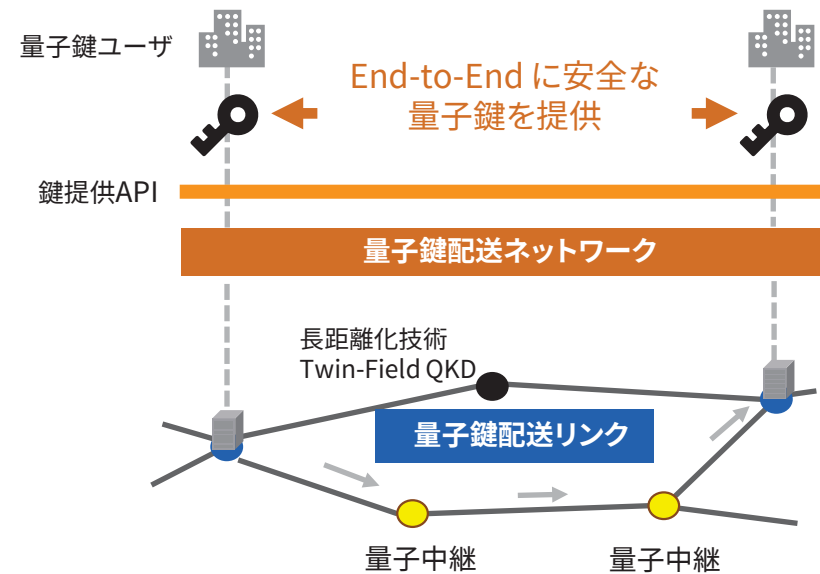
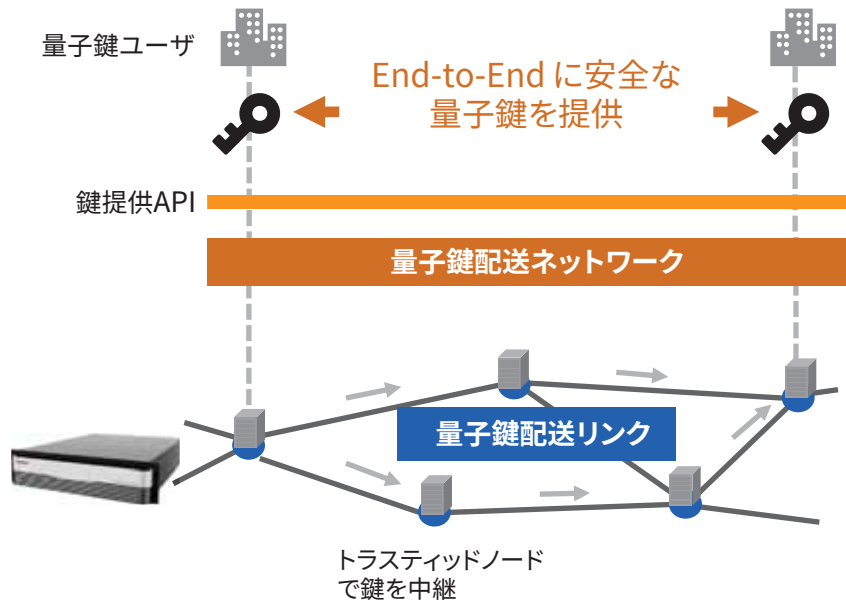
産業化には技術視点でなくユーザ視点が必要

量子鍵配送リンク + 量子鍵配送ネットワーク で、
量子鍵配送ネットワークサービスを構成



ユーザが簡単に量子暗号通信を利用できるサービス

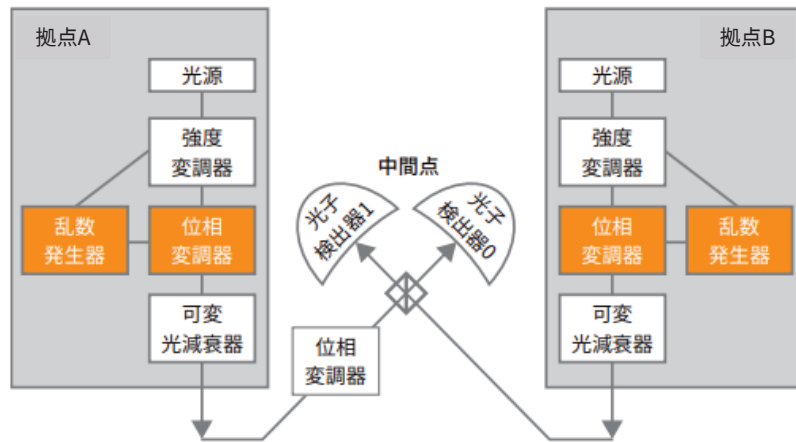
量子鍵配送技術の進化に伴うネットワークの変化



インターフェースは変わることなく、その結果アプリケーションも変わらず、量子鍵配送ネットワークの下で、徐々に新規技術が適用されていく

当社新規技術例: 長距離化 Twin Field QKD (TF-QKD)

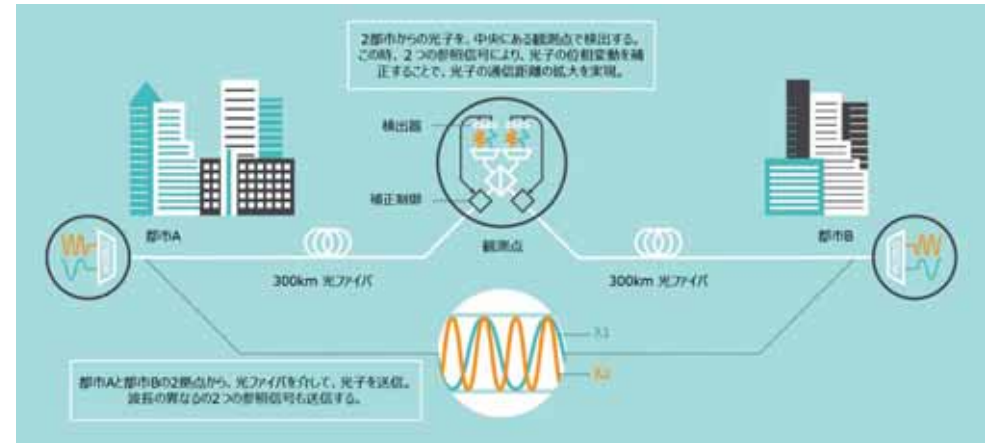
- 一式の量子暗号装置によって通信(量子鍵配送)可能な距離は、従来技術では最大100~200kmに限られる。これは、光子が光ファイバー上で減衰してしまう物理的な制約によるもの。
- 量子暗号の新しいプロトコルを考案し、光ファイバーを使った量子暗号で500kmを超える暗号鍵共有が可能となることを示した(2018年)。さらに、600km以上の通信距離を実証(2021年)
- 光子送信を両端の拠点から行い、中央の拠点で光子検出を行う構成。



TF-QKDの構成

量子暗号通信で世界最長600km以上の通信距離を実証2021.6.9

<https://www.global.toshiba/jp/technology/corporate/rdc/rd/topics/21/2106-02.html>



社会実装フェーズにある量子鍵配送で重要なこと

各国での社会実装が始まりつつある状況であり、コアコンポーネントの改良(長距離化・小型化等)だけではなく、周辺技術含めた実用化技術も重要な技術課題

実用化技術例

- スケーラビリティ(プラグ・アンド・プレイ、QoS等含む)
- 社会実装やエコシステム構築のためのアーキテクチャ・フレームワーク・インタフェース

【考慮すべき観点】

- 精緻なユースケース(アーリーアダプタの業界ごとの要件等)
- 社会実装のしやすさ(既存の通信インフラ・システム・アプリケーションとの整合性)
- 標準化(オープン・クローズ)

実用化技術でフォロワーとなると、他国にアーキテクチャ・フレームワーク・インタフェースで先手をとられ、それらに合わせるための技術開発に多くの労力を費やすことになる。

実フィールドで鍛えられた技術をもとに、**自身の強みを生かせるアーキテクチャ・フレームワーク・インタフェース**を策定し、**標準化を推進し、実用化技術においてもリーダー**となるのが、産業としての国際競争力の確保にとって極めて重要



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。



新しい未来を始動させる。

We turn on the promise of a new day.

- 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。
- 本資料に記載されている数値および表現は2021年12月現在のものです。
- 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。