日本総研
The Japan Research Institute, Limited

量子暗号通信に関する動向

株式会社日本総合研究所
先端技術ラボ
2021年2月1日

Copyright (c) 2021 The Japan Research Institute, Limited

目次

1. 量子暗号通信とは
概要 / 必要となる背景 / （参考）鍵配送問題 / （参考）主な暗号方式

2. 原理
量子暗号通信の原理 / ワンタイムパッド（OTP） / 量子鍵配送（QKD） / QKD方式の代表例：BB84方式

3. ユースケース
① 2拠点間の情報交換 / ② 複数拠点間の情報交換

4. 技術・市場動向
市場動向サマリ / 中国・韓国 / 欧米 / 国内 / （参考）東芝の取り組み概況 /
（参考）量子暗号通信・暗号リンク技術のロードマップ /
（参考）製品動向：量子鍵配送の装置ベンチマーク /
量子暗号技術の現状 / 標準化の動向 / （参考）耐量子暗号

5. 今後の展望
社会実装に向けた課題 / 今後の展望（仮説） / まとめ

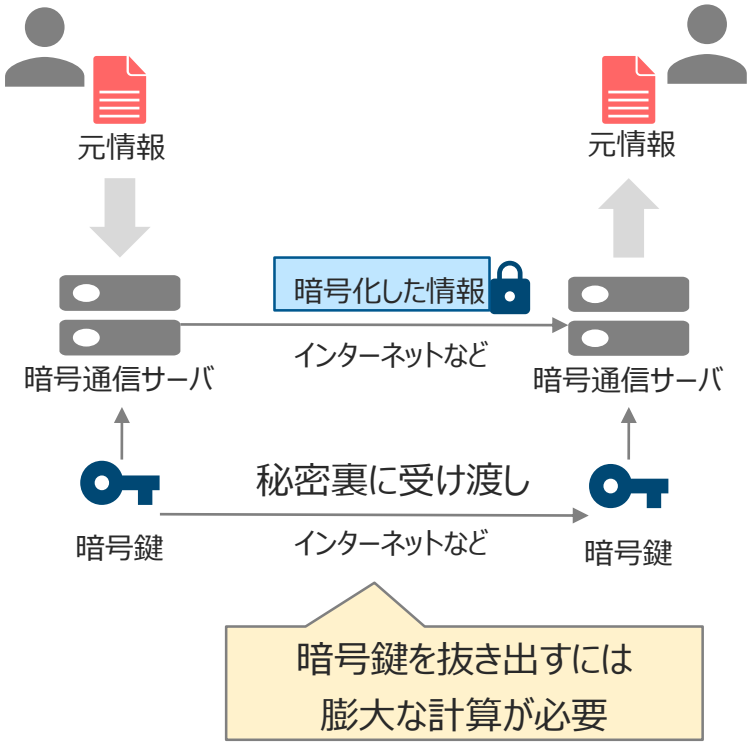
（注記）
暗号というと広義には、秘密通信以外にもデジタル署名(digital signature)や認証(authentication)も含む。しかし現在の量子暗号研究において、実現可能性が見えている暗号機能は量子鍵配送(quantum key distribution, QKD)のみであり、署名や認証用の量子暗号プロトコルの研究は発展途上である。そこで本レポートでは量子鍵配送についてのみ示す。

Copyright (c) 2021 The Japan Research Institute, Limited

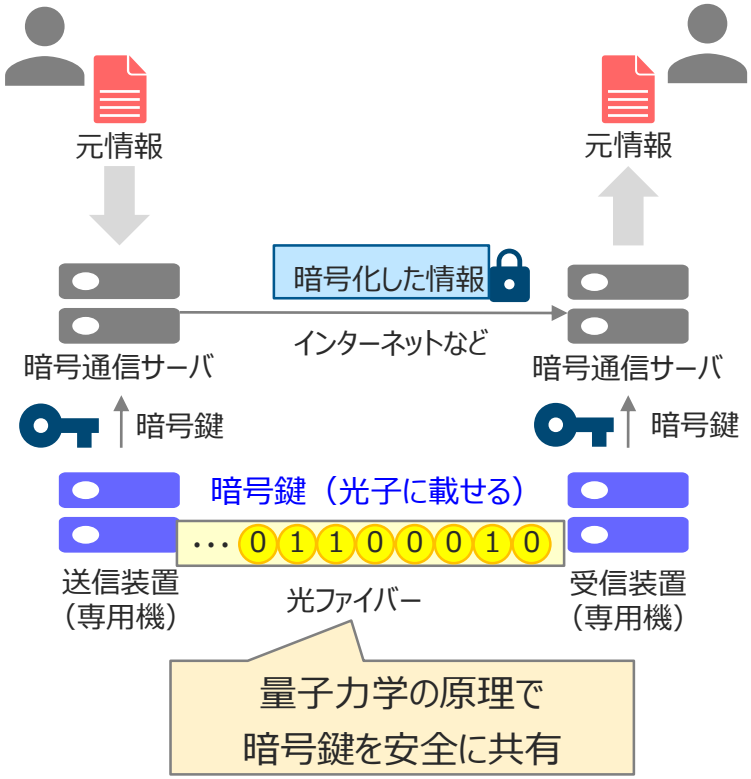
1.1 量子暗号通信の概要

- 量子暗号通信とは、暗号鍵を分割して量子の一種である「光子」（光の最小単位）に載せて送ること。
- 光子が持つ量子力学の性質(観測すると状態が変わる性質)を用い、盗聴検出時は鍵を無効化し再生成する。
  暗号鍵が盗聴不可能であることが理論上証明されていることを安全性の根拠としている。
- 量子暗号通信を行うには、双方の専用機器を光ファイバーで接続する。
  光子は極小かつ不安定であるため、安定して取り扱えるようにするための技術開発が進められている。

現在の暗号通信方式



量子暗号通信



Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

1.2 量子暗号通信が必要となる背景

- 量子コンピュータの実現により、RSAなどの一部の公開鍵暗号方式が危殆化すると考えられる。
- 対抗技術として、「耐量子暗号」や「量子暗号通信」が研究開発されている。

量子暗号通信が必要となる背景

量子コンピュータ時代の到来

- Googleが、量子超越性（Quantum Supremacy）を実証したと発表
- 世界各国で研究開発が加速する中、実用規模の量子コンピュータが2030年頃に登場する予測。

既存暗号通信技術の危殆化

- RSAなどの既存暗号は、量子コンピュータを使うと短時間で破られる可能性
- 暗号化されたデータを傍受・保存し、時間をかけて解読する攻撃（データ・ハーベスティング攻撃）も存在。現在の通信データの長期安全性も保証されない。

量子コンピュータへの対抗技術

量子コンピュータでも破られない セキュリティ技術の実現

量子暗号通信

- 量子力学に基づく、情報理論的安全性を実現
- 光ファイバー網と専用機器が必要
- 高機密情報に適する（国家機密、ゲノム医療データなど）

耐量子公開鍵暗号

- 既存暗号技術のアルゴリズム更新
- 計算量的安全性
- ネットワーク種別によらずソフトで実現
- 汎用通信（ウェブ閲覧、電子商取引）に適する

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研
The Japan Research Institute, Limited

（参考）鍵配送問題

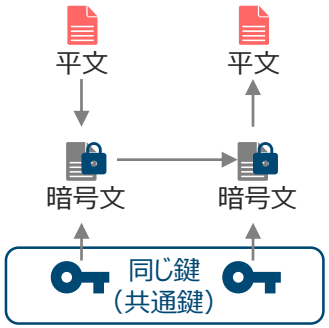
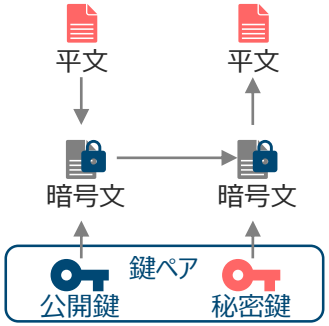
- どれだけ強固な暗号アルゴリズムを用いても、鍵が漏洩すればデータの秘匿性は失われる。
「いかに安全に暗号鍵を届けるか」が、暗号技術の大きな課題（鍵配送問題という）。
- 大きく３つの手段が存在。このうち電子的な手段によるものは、量子コンピュータの実現により危殆化が懸念される。

手段1 **物理的な手段による配送**	• 物理デバイス（HDDやUSBメモリ）などに鍵情報を保管し、デバイスを送受信者が直接渡すことや、信頼できる者に配送を依頼するなどの方法 • 鍵の共有者に対する本人認証が必要 • 参加者が増えるにつれ、膨大な鍵を作成・管理する必要があり、負荷が大きい
手段2 **Diffie-Hellman鍵共有** 危殆化の懸念	• 盗聴のおそれがある通信路でも、暗号鍵を共有できる方式 • 送受信者間で、他人に知られてもよい情報を交換した後に、双方が交換情報をもとに共通鍵を生成 • 安全性は離散対数問題の計算困難性に依るため、量子コンピュータによって解かれる可能性 • 通信の間に割り込んで盗聴・改竄する中間者攻撃に弱い
手段3 **公開鍵暗号方式** 危殆化の懸念	• 鍵交換が不要となり、配送問題を解決できる • 共通鍵暗号方式と比べ、演算処理がケタ違いに遅い • 一般に、データサイズが小さい鍵情報は公開鍵暗号方式で交換し、データ自体は共通鍵暗号方式でやり取りするハイブリッド方式が用いられる （例：ウェブサイトにおけるSSL通信） 鍵交換　：公開鍵暗号方式 データ交換　：共通鍵暗号方式 公開鍵の証明：デジタル署名／デジタル証明書

Copyright (c) 2021 The Japan Research Institute, Limited

（参考）主な暗号方式

- 暗号方式には、「公開鍵暗号方式」と「共通鍵暗号方式」の大きく２種類が存在する。
- 量子コンピュータの実現で脅威となる暗号方式は、公開鍵暗号のうちRSA暗号・楕円曲線暗号が対象。

		共通鍵暗号方式	公開鍵暗号方式		
概略図					
概要		• 同じ鍵を用いる（共通鍵） • 暗号化する人と復号する人の間で鍵を事前に共有する	• 公開鍵を用いて暗号化、秘密鍵を用いて復号する		
メリット		• 暗号化が高速 (公開鍵暗号の1/1000以下)	• 鍵の事前共有が不要 • 公開鍵を知る人は誰でも暗号化できる		
デメリット		• 安全な鍵共有が困難	• 計算速度が遅い		
主な用途		• データ自体の暗号化	• 鍵の共有、デジタル署名		
方式例	暗号名	AES暗号、ワンタイムパッド暗号	**RSA暗号**	**楕円曲線暗号**	準同型暗号
	安全性の根拠	ー	素因数分解	離散対数問題	最短格子問題
	耐量子性	有り	無し	無し	有り

Copyright (c) 2021 The Japan Research Institute, Limited

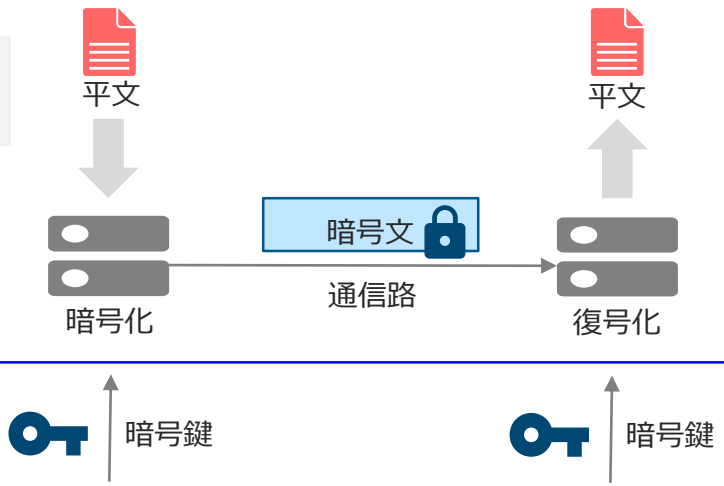
2.1 量子暗号通信の原理

- “光子”の量子的ふるまいに基づき、盗聴されていないことが保証された「暗号鍵」を共有する。
- “光子”の特殊なふるまい（分割できない、コピーできない）を利用し、「盗聴」を検出する。
- これにより、どのような計算機でも解読できない（＝情報理論的安全性を持つ）暗号通信を実現している。

量子暗号通信の原理

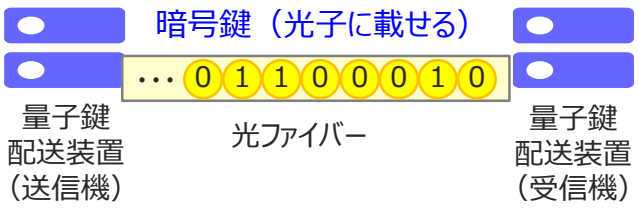
ワンタイムパッド（OTP）

平文と同じサイズの鍵で暗号化し、毎回使い捨て



量子鍵配送（QKD）

光子1個に暗号鍵1ビットを載せて伝送し、双方で同じ鍵を持つ

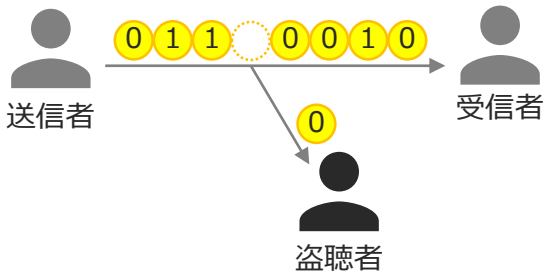


- 光子に（暗号鍵に限らず）情報を載せて伝送することを、単に「量子通信」という。

（参考）「光子」の性質

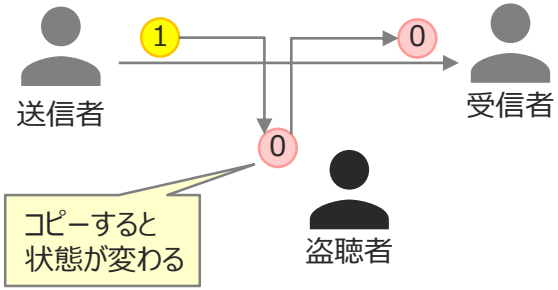
1) 光子は分割できない

⇒ 数が減ったら盗聴されている証拠



2) 光子状態は完全にはコピーできない

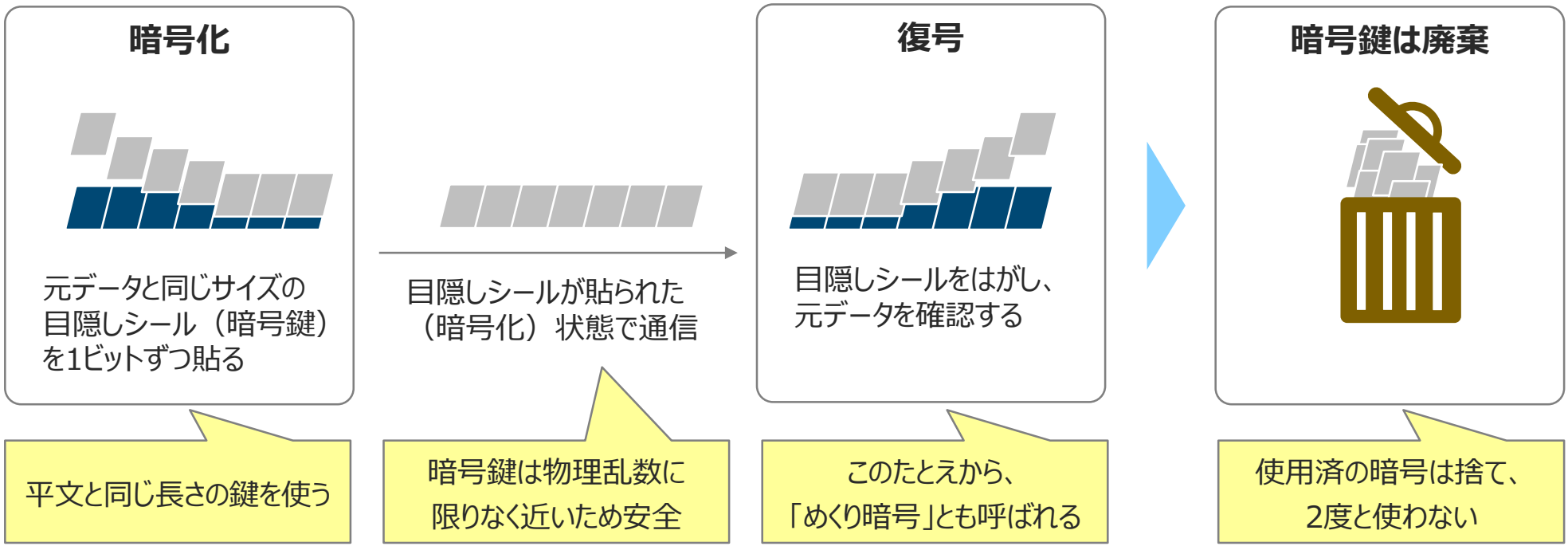
⇒ 光子の状態が変化したら盗聴の疑いあり



Copyright (c) 2021 The Japan Research Institute, Limited

2.2 ワンタイムパッド（OTP）

- ワンタイムパッド（One Time PAD; OTP）とは、送信者および受信者が、送受信するメッセージと同じ長さの鍵を事前に共有しておき、その鍵を用いてメッセージの暗号化・複合化を行う暗号方式。
- 量子暗号通信におけるOTPは、平文と同じ長さの暗号鍵で暗号化し、用いた暗号鍵は廃棄するため、永続的に解読が不可能となる。



出所）情報通信研究機構（NIST）の資料をもとに日本総研作成

- ワンタイムパッド自体は、1882年に概念が生まれ、第二次世界大戦でも利用された。暗号鍵を確実に廃棄することが運用上の課題であった。盗聴や複製によって暗号鍵が壊れるという量子暗号の考えが、確実な鍵廃棄の実現というワンタイムパットの要件と合致し、量子暗号通信で用いられるようになった。

Copyright (c) 2021 The Japan Research Institute, Limited

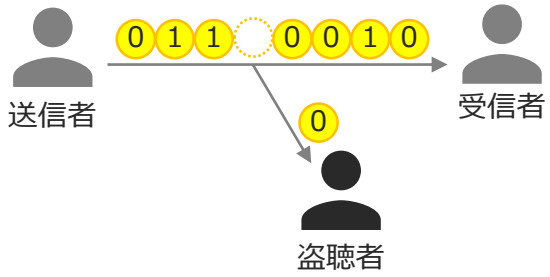
2.3 量子鍵配送（QKD）

- 量子鍵配送（Quantum Key Distribution; QKD）とは、光ファイバー伝送路において、1ビットあたり1個の光子に鍵情報を載せて伝送することで、2者間で安全に暗号鍵を共有する技術。盗聴を検知・防止できる。

（参考）「光子」の性質（再掲）

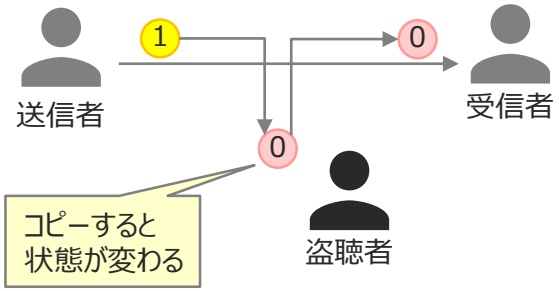
1) 光子は分割できない

⇒ 数が減ったら盗聴されている証拠



2) 光子状態は完全にはコピーできない

⇒ 光子の状態が変化したら盗聴の疑いあり



量子鍵配送（QKD）のポイント

［ポイント1］盗聴者は通信者と同じ鍵情報を取得できない

- 通常の光通信では、1ビットに数万の光子を用いるため、数個無くなっても分からない
- 量子鍵配送は、1ビットに光子1個を用いる
- 盗聴された場合、光子の個数が合致しない。
  ⇒盗聴されたと結論づけ、プロトコルを最初から再実行する

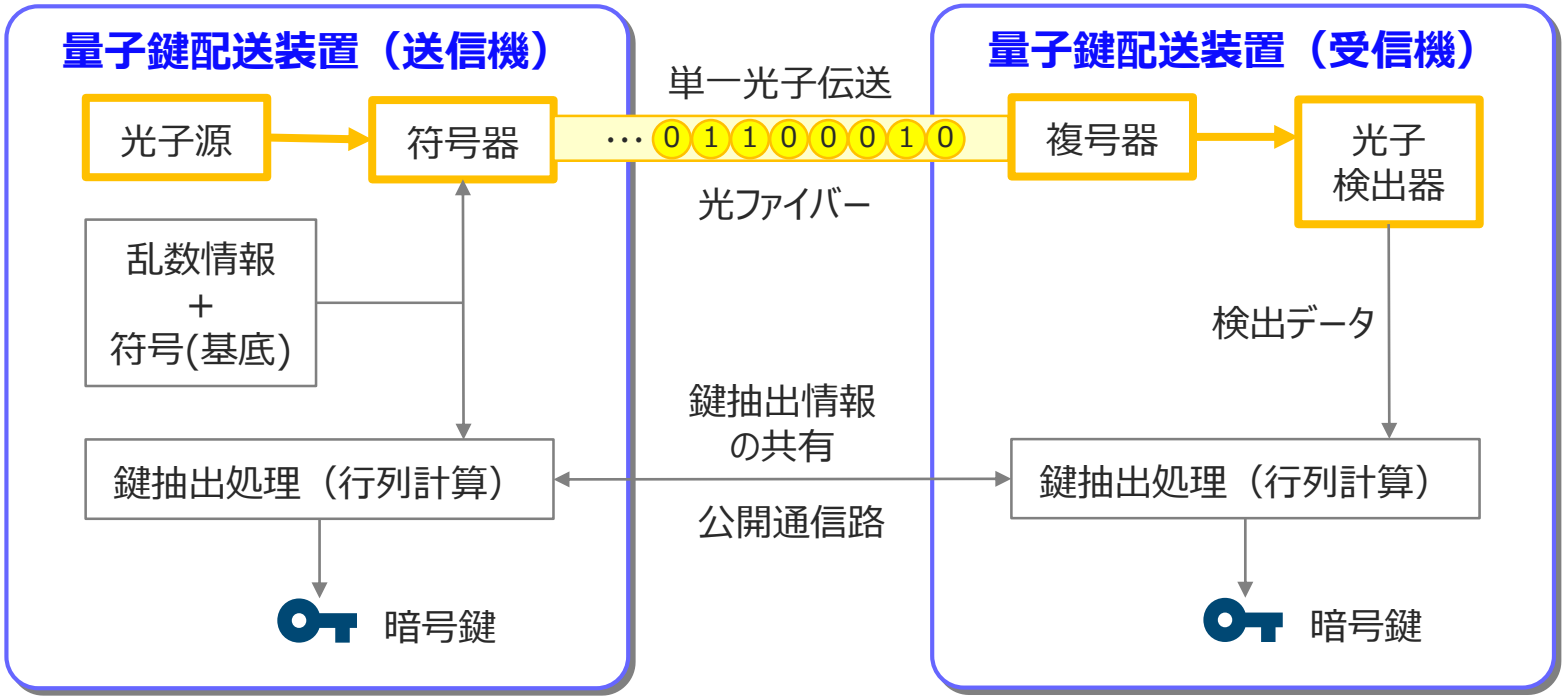
［ポイント2］変化した光子は使用しない

- 量子力学的に、光子は観測すると状態が変化する
- 盗聴された場合、受信者が得るチェックビットに誤りが乗る。
  ⇒盗聴されたと結論づけ、プロトコルを最初から再実行する

Copyright (c) 2021 The Japan Research Institute, Limited

2.4 QKD方式の代表例：BB84方式

- BB84方式：光子1個（単一光子）に鍵（乱数）情報を載せた伝送・共有する方式。
- 受信した乱数情報のみを用いて鍵を生成することで、鍵の安全性を担保する（盗聴・盗難された乱数情報は使わない）。
- 量子通信路（光ファイバー）は専有する。

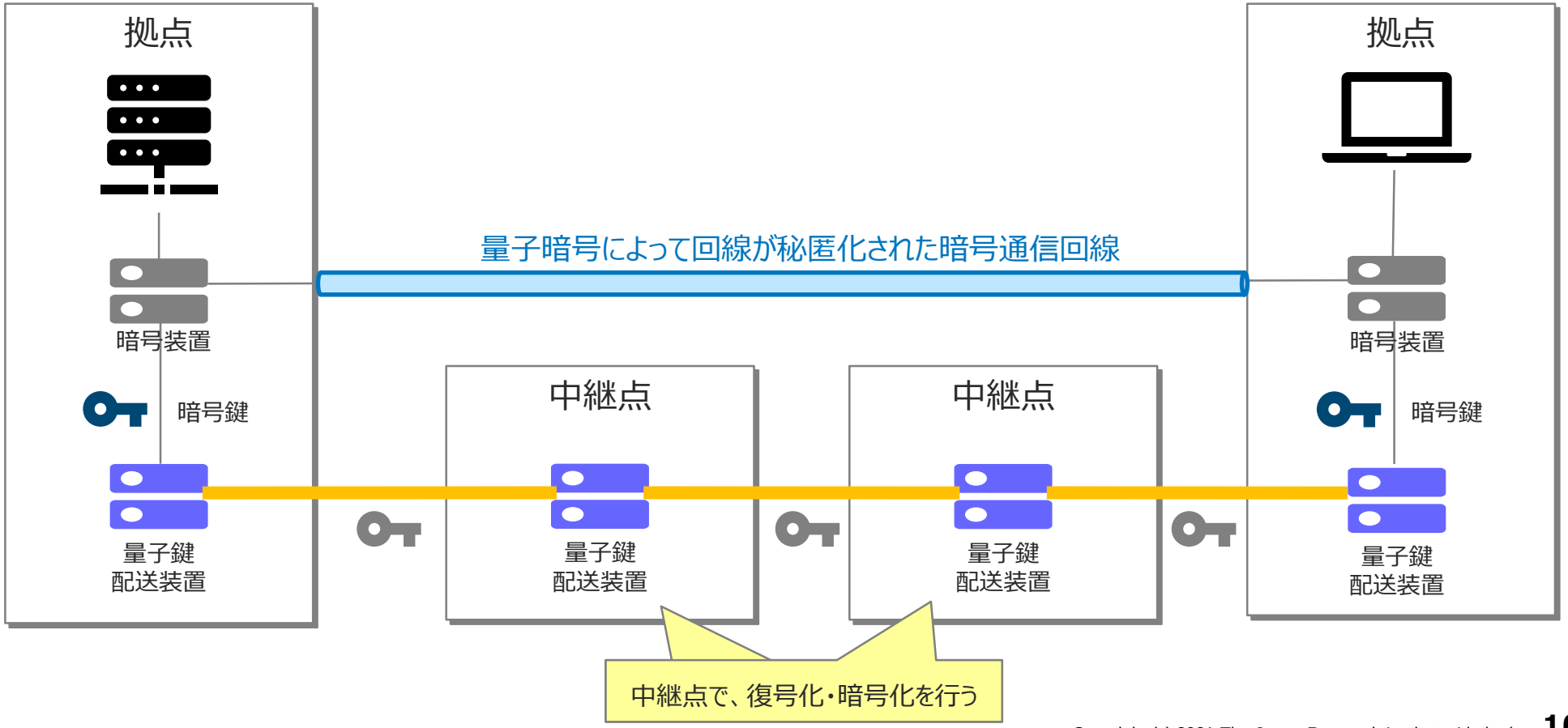


- BB84（Bennett and Brassard [1984]）は、1984年に Charles H. Bennett と Gilles Brassard が提案した量子暗号の方式。初代量子暗号といえる。BB84以外にも、B92（Bennett [1992]）や量子もつれ（エンタングルメント）を利用するE91（Ekert [1991]）等が提案されている。ここでは、原理を理解するうえで最も分かりやすいBB84を例にとる。

Copyright (c) 2021 The Japan Research Institute, Limited

3.1 ユースケース①｜2拠点間の情報交換

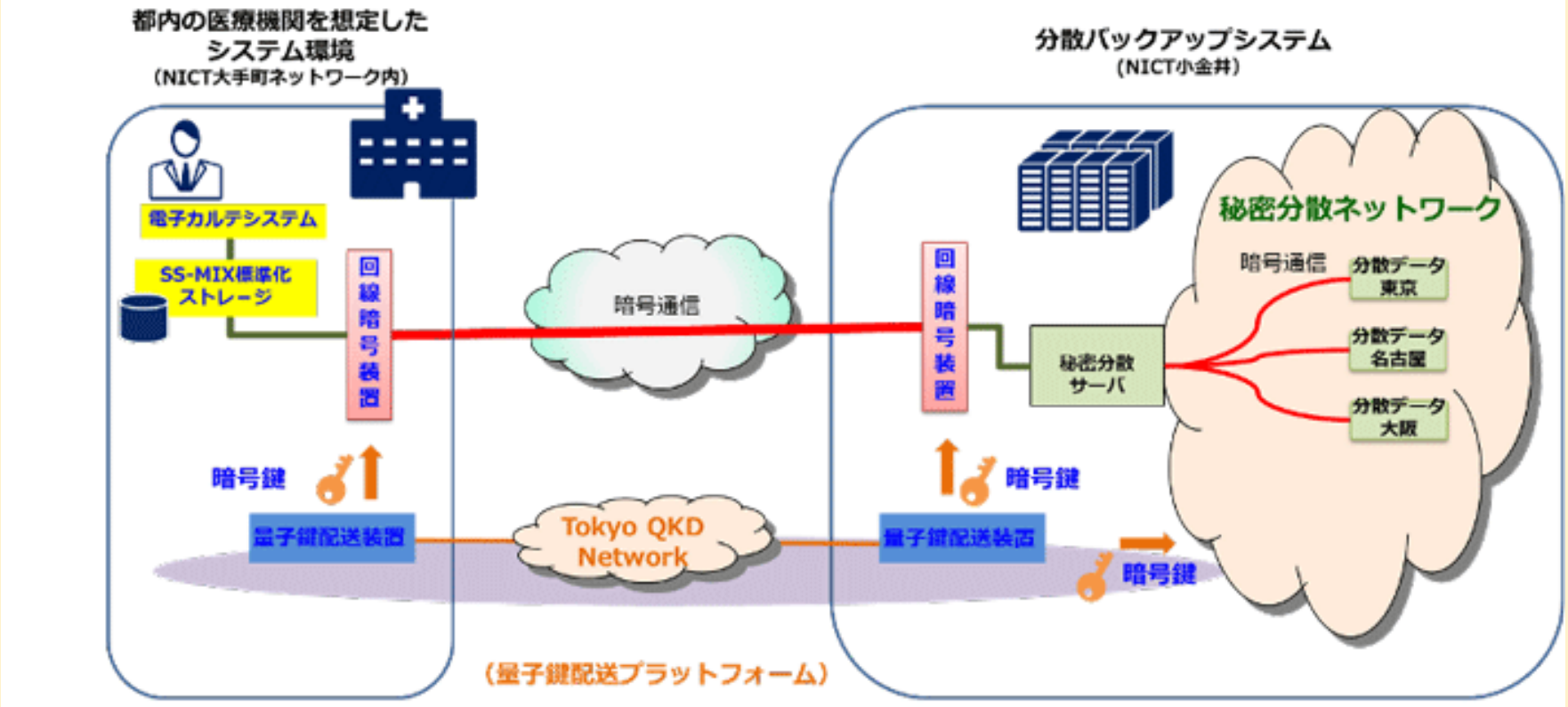
- 拠点間で、秘匿性の高い情報を交換する。遠距離（数十km以上）の場合は、中継点が必要となる。
  中継点で鍵が盗聴されないことが前提であり、中継点が信頼点となる。これを解決する量子中継技術の研究も進められている。
- 量子力学の干渉の性質を用いた「ツインフィールドQKD」方式を採用することで、量子暗号の到達距離を約2倍（実験最大値は約500km）に伸ばす技術も登場している。



Copyright (c) 2021 The Japan Research Institute, Limited

（参考）2拠点間の情報交換｜NECの事例

- NEC、NICT、株式会社ZenmuTechは、電子カルテのサンプルデータを量子暗号で伝送そのものを秘匿し、広域ネットワーク経由で秘密分散技術を用いてバックアップするシステムの実験に成功（2020年10月22日発表）。
- 約1万件の電子カルテのサンプルデータの伝送を量子暗号で秘匿化。ネットワーク経由で安全なデータ伝送および秘密分散を用いたバックアップを行うシステムを開発。
- 電子カルテデータを、安全に遠隔地保管したり医療従事者間で共有したりする仕組みを実現。

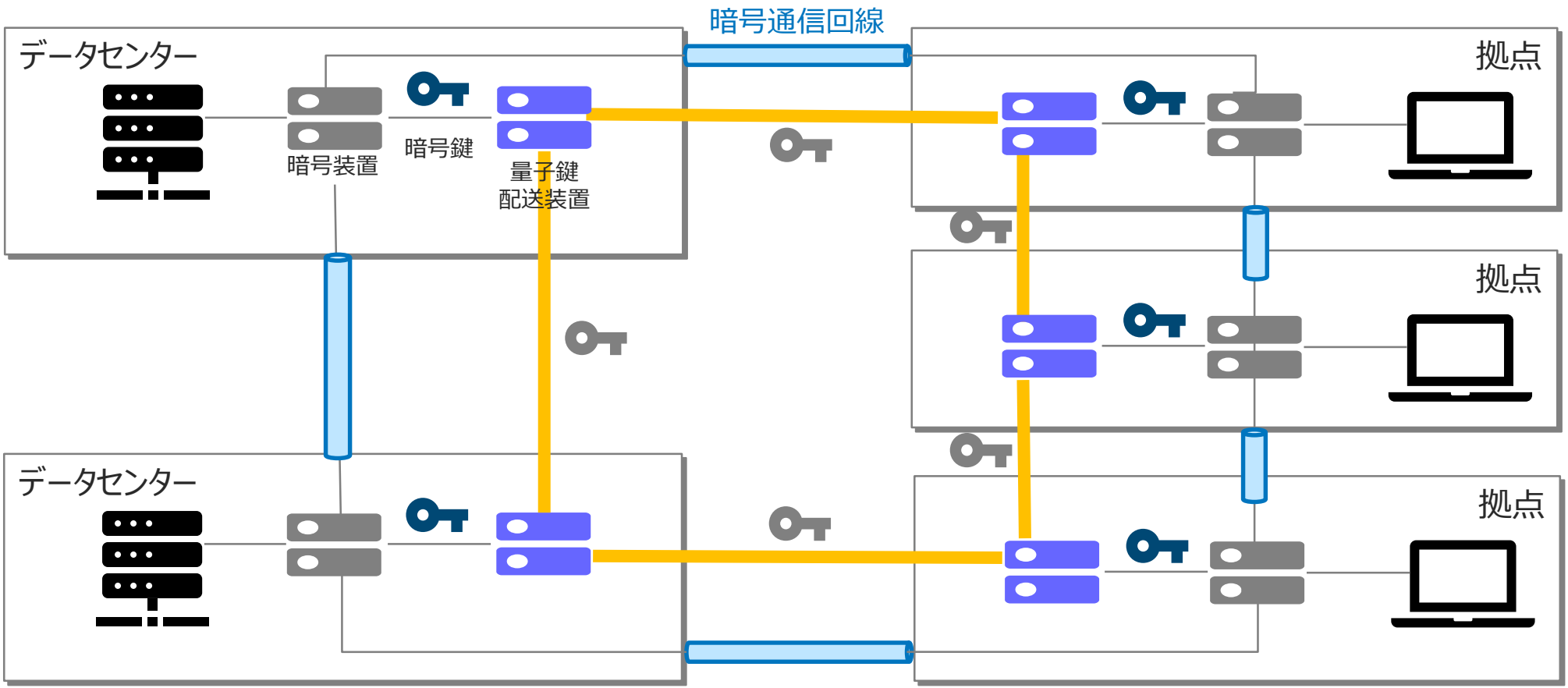


出所）情報通信研究機構　https://www.nict.go.jp/press/2020/10/22-1.html

Copyright (c) 2021 The Japan Research Institute, Limited

3.2 ユースケース② | 複数拠点間の情報交換

- 量子暗号通信は基本的には2点間の通信であるが、複数拠点間でも共通鍵をリレーすることで、情報の機密性を保証したうえで通信できる。



Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

4.1 市場動向｜サマリ

- 社会実装面では、中国がスピード・規模で先行。金融・司法分野で実用化済、2025年までに量子暗号通信ネットワークを中国全土に広げる計画。
- 韓国とドイツが大規模QKD網の構築に動き出す。米国、英国、日本は小規模・局地的な取り組みにとどまる。

量子暗号通信ネットワーク化先行国の動向

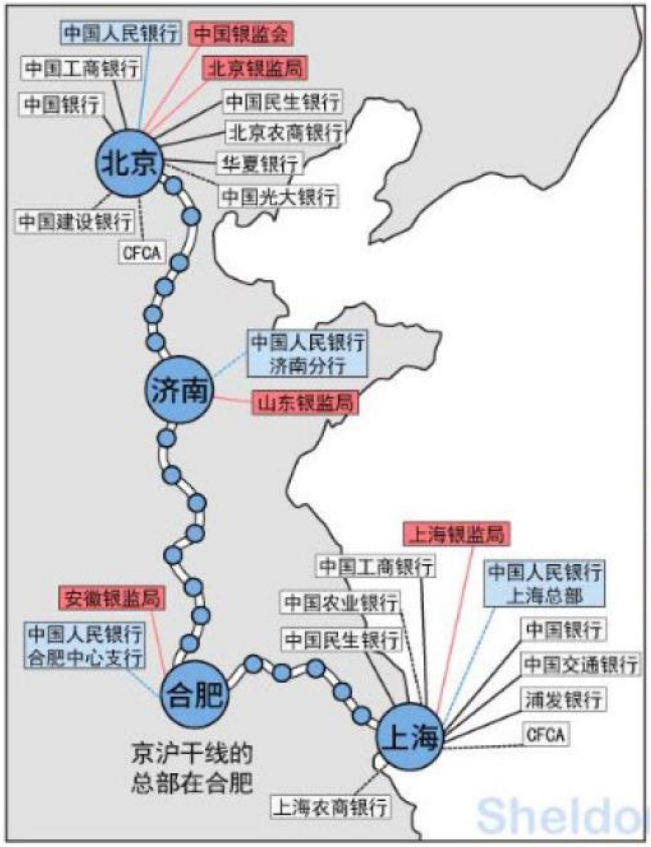
中国	既に広域インフラを構築	• 2016年までに、上海・合肥・洛南・北京の4都市間ネットワーク（全長2,000km）を構築 • 2017年、世界初の衛星・地上間での量子鍵配送（距離1,200km、1kbps）に成功（独自開発の衛星「墨子」） • 2018年、世界最大の量子暗号ネットワークを構築。新華社通信、中国工商銀行、国家電網公司などが利用 • 2025年までに、全国規模のネットワーク構築を計画
韓国	国家政策として推進	• SK Telecomが、2020年に自社5G/LTEネットワーク (ソウル・デジョン間）へ適用 • 韓国版ニューディール政策の一環で、「K-サイバー攻撃防疫」の中で「量子暗号通信網構築モデル事業」を推進（2020年9月発表） • 2025年までに160兆ウォン(約15兆円)を投じ、約190万人の雇用創出を目指す
欧州	キャリアの動き活発化	• 2019年、欧州各国参加のテストベッド構築プロジェクトOPENQKDが始動 • [ドイツ]ドイツテレコムの実証通信網にSK Telecom/ID Quantiqueがシステムを提供して2019年商用網へ拡張 • [イギリス]2018年、British Telecomが同国初の量子暗号通信網をケンブリッジ-イプスウィッチ間に構築
米国	スタートアップ中心に展開	• 2018年、Quantum Xchangeが同国初の量子暗号サービスを発表 (New York-New Jersey間(32km)。ウォール街の金融市場が狙い。東芝も参画)
日本	NICTを中心に研究開発	• 2010年から、NICTを中心に量子暗号ネットワークテストベッドの構築に関する研究開発。ImPACT「量子セキュアネットワークプロジェクト」にて、都市圏QKDネットワーク「Tokyo QKD Network」(小金井-大手町間45km)の実証 • 2018年度から、内閣府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Society5.0実現化技術」にて、量子暗号と秘密分散を統合した社会実装に取組み • 2020年10月、NEC、NICT、ZenmuTechは、電子カルテのサンプルを量子暗号で伝送そのものを秘匿し、広域網経由で秘密分散技術を用いてバックアップ成功

Copyright (c) 2021 The Japan Research Institute, Limited

（参考）市場動向｜中国・韓国

中国

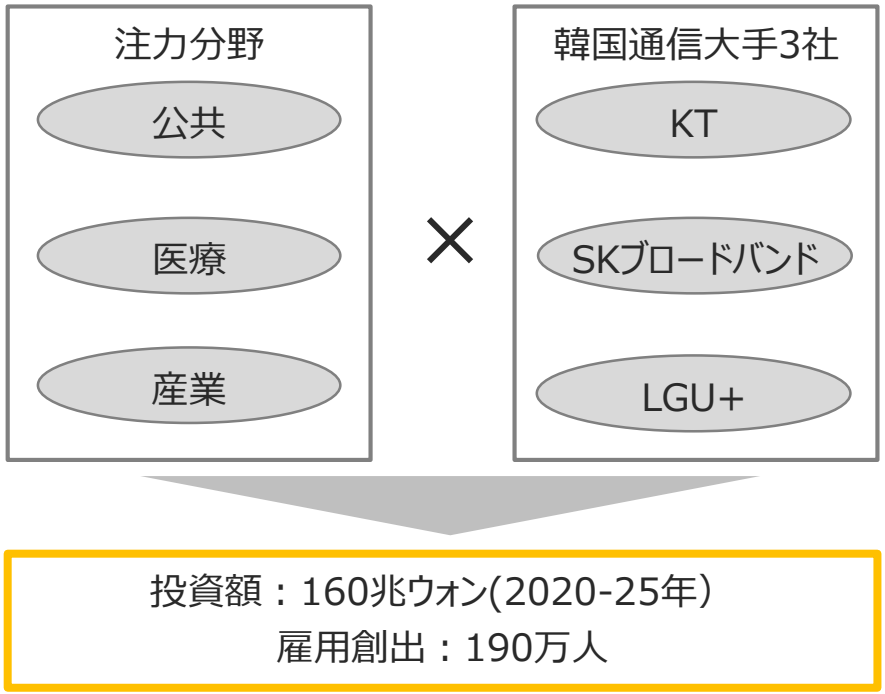
- 北京＝上海のQKDサービス網に銀行も接続。
- 情報収集（各種規制、外国取引）、データバックアップ、ネットバンキング、システム情報の暗号化などへの活用を企図（詳細不明）。



出所）東芝 https://www.itmedia.co.jp/business/articles/2012/09/news022_3.html

韓国

- 韓国政府は2020年7月14日、COVID-19後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」を発表。
- この政策のうち、サイバー安全網を構築する「K-サイバー攻撃防疫」の中に、「量子暗号通信網構築モデル事業」を開始。

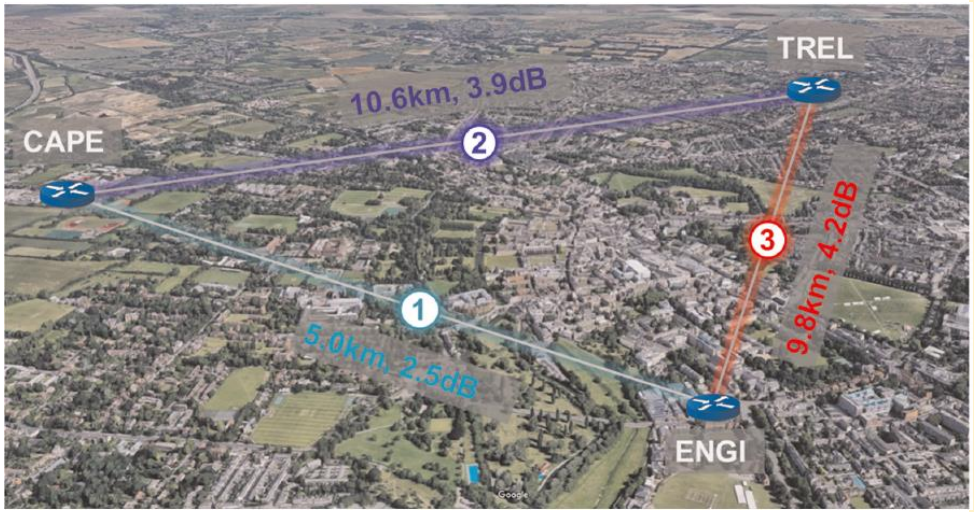


Copyright (c) 2021 The Japan Research Institute, Limited

（参考）市場動向｜欧米

欧州

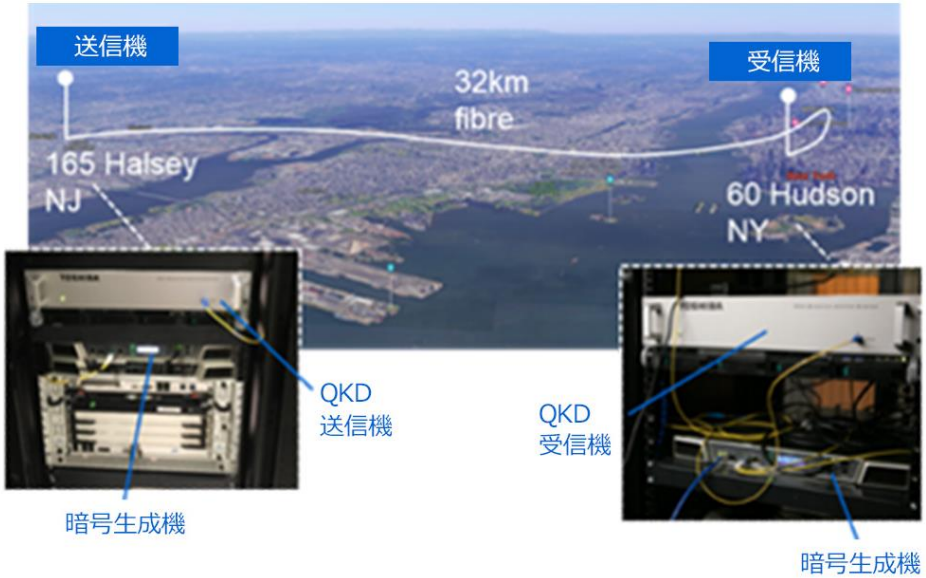
- 英国ケンブリッジに、3拠点からなるリングネットワークを設置し、検証。通信距離は、各10km程度。東芝も参画。



出所）Dynes, J.F., Wonfor, A., Tam, W.W.S. *et al.* Cambridge quantum network. *npj Quantum Inf* **5,** 101 (2019). https://doi.org/10.1038/s41534-019-0221-4

米国

- 米Quantum Xchange社の金融向け耐量子ネットワークで、東芝の量子暗号通信を実験。
- 通信距離：32km（ニューヨーク州・ニュージャージー州間）
- 1本の光ファイバーで、量子鍵配送とデータ通信の両方を実現。光ファイバーのコスト削減につながる。



出所）東芝 https://www.toshiba.co.jp/qkd/case2.htm

Copyright (c) 2021 The Japan Research Institute, Limited

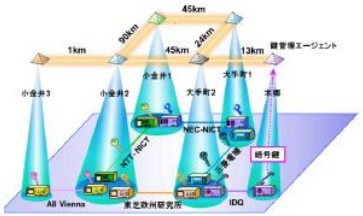
4.2 市場動向｜国内

- NTTが早くから研究に着手し、NEC、東芝、情報通信研究機構（NICT）などで研究開発が進められる。
- ImPACT「量子セキュアネットワークプロジェクト」で都市圏QKD網が実証され、2018年からは、内閣府の戦略的イノベーション創造プログラム（SIP）にて、量子暗号と秘密分散を統合した社会実装に取り組み中。
- 政府（防衛・警察）通信ネットワークのセキュリティ対策として、2021年度から実証事業が開始。

2010年　　2018年　　2023年

NICT委託研究 → **ImPACT** → **SIP第2期**

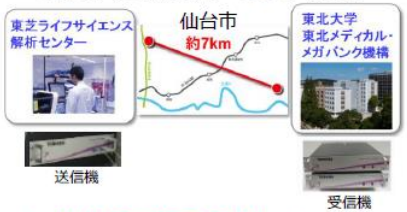
2010年、東京量子暗号ネットワークテストベッドを構築



✓ 動画の量子暗号化を世界で始めて実現

NEC：サイバーセキュリティ関連施設で試験運用

東芝：ゲノム解析データの暗号通信

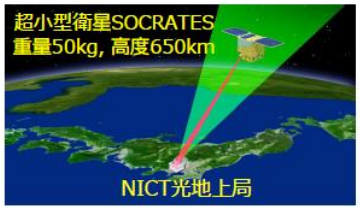


✓ **世界最高速の装置**を開発
300kbps @45km （東芝）
海外製の**10倍高速、2倍長距離**

✓ 鍵管理アーキテクチャ確立

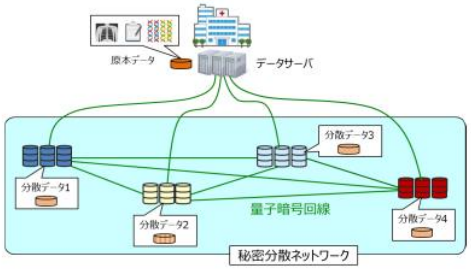
✓ 新たなアプリの開発
「超長期セキュアデータ保管」
（**量子暗号x秘密分散**）

✓ NICTが超小型衛星で量子通信を実証（2017年）



光・量子を活用したSociety5.0実現化技術

量子セキュアクラウド技術を開発し、将来にわたり安全なデータ保管と利活用を実現



➢ 専用用途での量子暗号サービス

政府重要拠点間等での利用を検討
⇒ 民間用途への展開

➢ 標準化、運用ガイドライン案を策定

➢ 量子セキュアクラウドシステムの社会実装

総務省・委託研究

衛星通信における量子暗号技術

6

出所）情報通信研究機構　https://www.nisc.go.jp/conference/cs/kenkyu/dai11/pdf/11shiryou02.pdf

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

（参考）東芝の取り組み概況（2020年10月19日報道発表を中心に）

- 東芝は2020年度第4四半期から、量子暗号通信システムのプラットフォーム※の提供、およびシステムインテグレーション事業を順次始める。（2020年10月19日報道発表）（※量子鍵配送(Quantum Key Distribution, QKD)）

量子暗号通信システムのプラットフォーム提供

- 2種類の量子鍵配送プラットフォームを開発
  「多重化用途」：データ通信用光ファイバーを共有する
  「長距離用途」：鍵配送の速度と距離を最大化
- 国内外で量子鍵配送ネットワークを構築し、金融機関を中心とした顧客向け量子鍵配送サービスを2025年度までに本格開始予定
- 英ケンブリッジに製造拠点を置き、2020年内に特定ユーザ向けサービスを提供開始
- 2035年度に、全世界の量子鍵配送サービス市場（推定約200億米ドル＝約2.1兆円）の約1/4（2030年度で約30億米ドル＝約3,150億円）の獲得を目指す
- 2019年の量子暗号関連特許数世界一
- 競合他社が提供中の量子鍵配送装置のベンチマークを引き合いに、「鍵共有速度」「最大距離」の両方が優れることをアピール

システムインテグレーション事業

- 専用光通信回線を用いる顧客向けに、量子暗号通信システムを一括納入し、運用・保守サービスを提供
- 国内では東芝デジタルソリューションズが事業展開。海外では地域のパートナーと共同で事業展開

地域		取組状況
国内		・2021年4月から、情報通信研究機構（NICT）と複数拠点間の量子暗号通信実証事業を開始予定（事業展開は国内初）
海外	英国	・BTグループ（大手通信事業者）との共同実証試験を2020年9月開始。研究機関向けネットワークに適用。それまで、ポータブルストレージに格納し人手で搬送していたものを、オンライン伝送可能に
	米国	・Verizon Communicationsの量子暗号通信試験にQuantum Xchange（スタートアップ）と共同参加。１本の光ファイバーで鍵配送とデータ通信を行う
	その他	・2021年度以降、欧州、アジアの主要国でも現地事業パートナーと量子暗号通信システム事業を推進予定

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

（参考）野村HDの取り組み概況（2020年12月21日報道発表を中心に）

- 野村ホールディングス、野村証券、NICT、東芝、NECは、金融分野におけるデータ通信・保管のセキュリティ強化に向けて、量子暗号技術の有効性と実用性に関する国内初の共同検証を12月開始。
- 内閣府主導の戦略的イノベーション創造プログラム「光・量子を活用したSociety 5.0実現化技術」の一環として実施。（2020年12月21日報道発表）

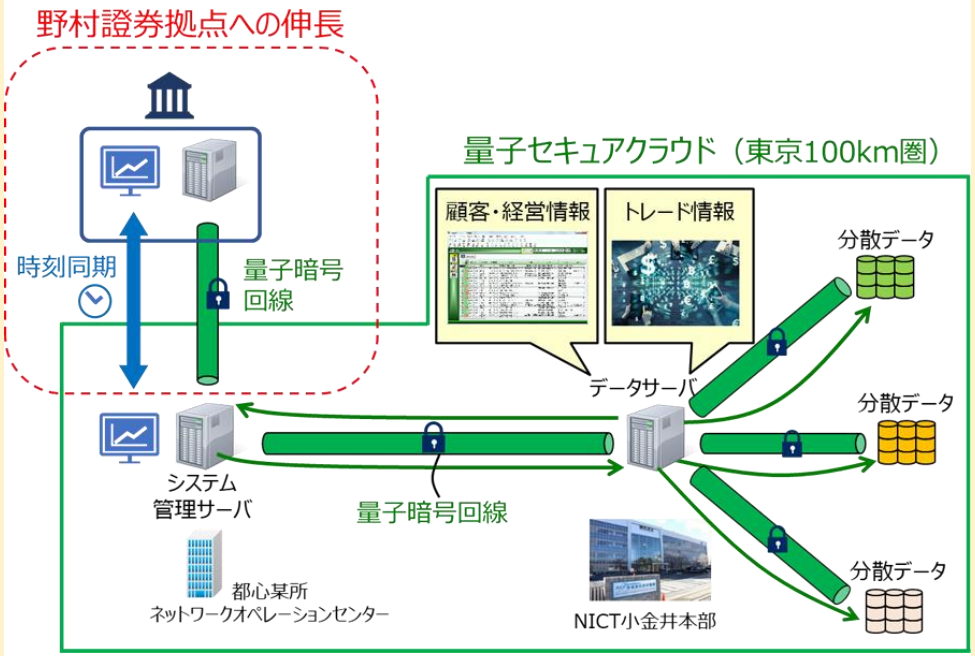
検証内容

- 野村証券が持つ顧客情報や株式取引情報（疑似データ）を量子暗号により秘匿伝送する実験
- 遠隔地の複数のデータサーバまで秘密分散を用いて、バックアップ保管や安全な計算処理を行う、量子セキュアクラウドシステムの動作検証　など
- 1年以上かけて検証。結果をもとに、数年後の実用化を展望

参加者	実施内容
野村HD・野村証券	• 自社システムの提供、テストデータの生成 • 金融実務への適用可能性検証、など
NICT	• Tokyo QKD Networkの運用・管理 • 量子セキュアクラウドシステムの提供 • 金融環境における機能検証
東芝	• 量子暗号装置の導入・運用支援 • 量子暗号と暗号通信アプリとの連携システムの検討・構築
NEC	• 量子暗号装置の開発・運用支援 • 量子暗号装置とアクセス管理のための認証技術との連携システムの検討・構築

検証環境

- 量子暗号装置（東芝製）を野村証券の拠点に導入
- NICTが運用する量子暗号ネットワーク「Tokyo QKD Network」を、野村証券の拠点まで延長



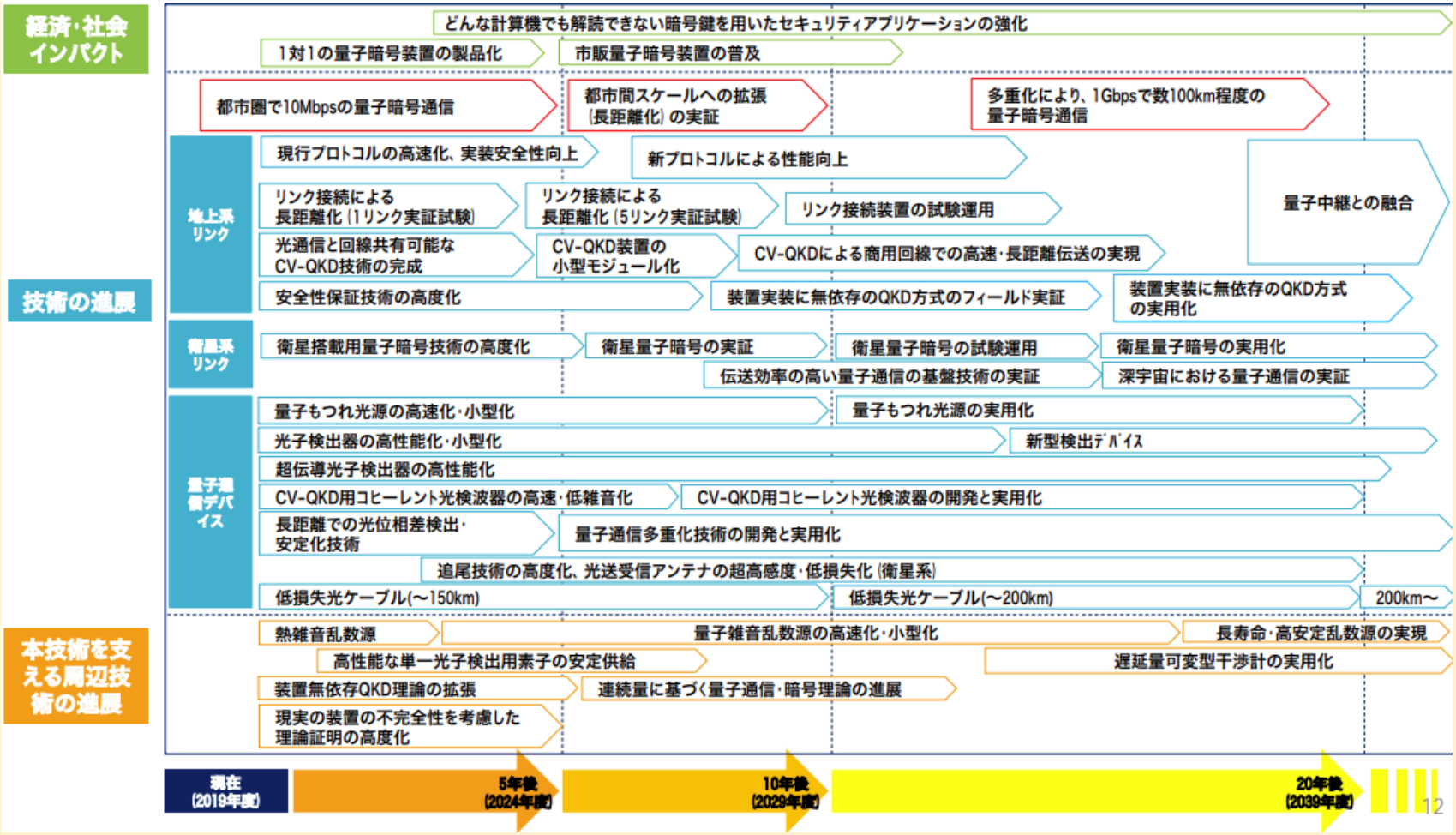
出所）野村ホールディング他　https://www.nomuraholdings.com/jp/news/nr/holdings/20201221/20201221.html

Copyright (c) 2021 The Japan Research Institute, Limited

（参考）量子暗号通信・暗号リンク技術のロードマップ

⑪量子通信・暗号リンク技術

○量子暗号装置の製品化によって、様々なセキュリティアプリケーションの安全性を強化
○5年後までに都市圏で10Mbpsの量子暗号通信、10年後までに都市間スケールへの拡張（長距離化）の実証
○高性能な単一光子検出器や量子もつれ光源、乱数源等の研究開発。加えて、QKDの新方式の研究開発



出所）内閣府「量子技術イノベーション戦略（最終報告）」2020年1月21日 https://www8.cao.go.jp/cstp/siryo/haihui048/siryo4-2.pdf

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

（参考）製品動向：量子鍵配送の装置ベンチマーク

- 機器市場について、中国を除くと、スイスIDQuantique社（韓国SK Telecom傘下）が先行する。
- ベンチマーク値は、最新製品ということもあり、東芝が優れる。

	東芝	スイス IDQuantique	中国 QuantumCTek	中国 Qasky
外観		https://www.idquantique.com/quantum-safe-security/products/cerberis3-qkd-system/	http://www.quantum-info.com/English/product/quantum/2017/1013/407.html	http://www.qasky.com/en/display.asp?id=781
鍵共有速度	300 kbps @50km	6 kbps @60km	15 kbps @50km	40 kbps @50km
最大距離(最大ロス)	120km (24dB)	75km (18dB)	85km	～100km
事業実績	なし	10年超の実績	中国国内で実績あり	中国国内で実績あり

出所）東芝などの情報をもとに日本総研作成

- IDQuantique（IDQ）：ジュネーブ大学からのスピンオフ企業。ジュネーブ投票システムや金融機関のネットワークへの適用など、実証実績多数。欧州のR&Dプログラムに参加することで学術機関と関係をもち、最先端プロジェクトで主要な役割を果たしている。2018年韓国SK Telecomが買収。
- QuantumCTek（QCT）：2009年に中国科学技術大学（USTC）と個人投資家によって設立。北京・上海間の長距離ネットワークに参画。中国の量子情報技術標準化団体のリーダーを務める。
- Qasky： 2009年設立。Wuhu Construction Investment（蕪湖県建設投資有限公司）とUSTCが共同出資。P2Pの量子暗号通信技術、量子暗号通信ネットワーキング技術、量子暗号通信コアデバイスを提供。中国の150km超のQKDネットワーク実証に参画。

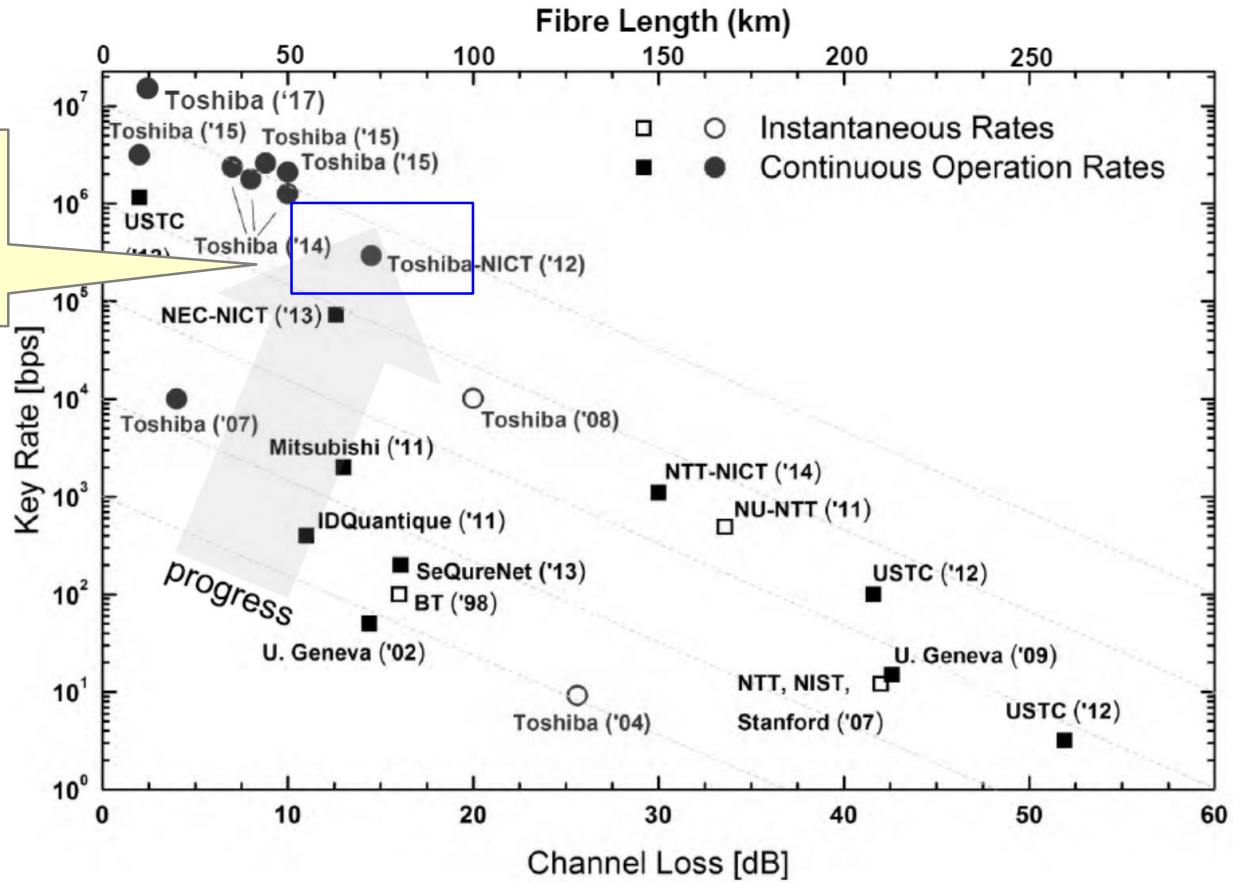
Copyright (c) 2021 The Japan Research Institute, Limited

4.3 量子暗号技術の現状

- 光子は極小かつ不安定であるため、伝送距離を延ばすのが難しい。距離を伸ばすと速度が落ちる。伝送距離・速度・ノイズ耐性とのバランスによって決定される。
- 現在は、伝送距離:数十キロ、速度:数百kbpsが妥当な水準。今後の製品開発によって性能向上が望まれる。

伝送距離・速度・ノイズ耐性の性能向上の推移

伝送距離:数十キロ
速度:数百kbps
の領域



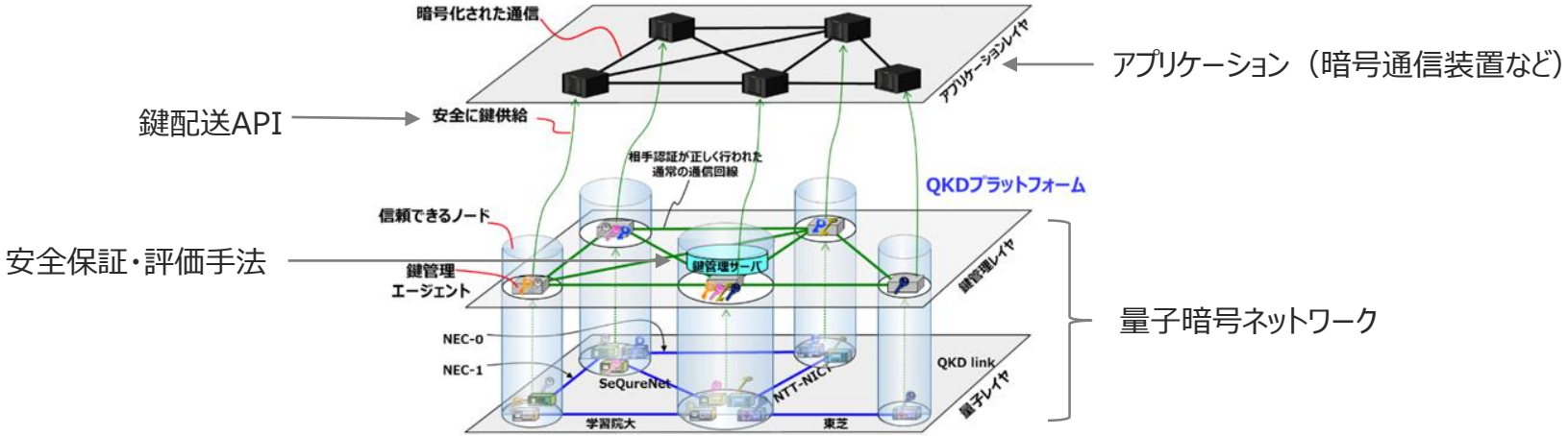
出所）東芝
https://www.kantei.go.jp/jp/singi/ryoshigijutsu_innovation/dai3/siryo2.pdf

Copyright (c) 2021 The Japan Research Institute, Limited

4.4 標準化の動向

- 相互運用性、ネットワーク親和性、装置の安全性の各観点から、国際機関で標準化活動が進められている。

区分	内容	標準化活動
相互運用性 (多様なアプリと接続して利用できる)	鍵提供APIを標準化	・ETSI QSD GS 014(2019)
ネットワーク親和性 (既存ネットワークに容易に導入できる)	量子暗号ネットワークの構成を標準化	・ITU-T SG13 Y.3800(2019) ・ITU-T SG17
装置安全性	安全性保証・評価手法を標準化	・ISO/ISC JTC1 SC27 WG3 ・ETSI



出所）情報通信研究機構の資料（https://www.nict.go.jp/press/2019/07/02-1.html）に日本総研にて追記

- ETSI：欧州電気通信標準化機構（European Telecommunications Standards Institute）。EUが後援する標準化組織。
- ITU-T：国際電気通信連合 電気通信標準化セクタ（International Telecommunication Union Telecommunication Standardization Sector）国連機関。
- ISO/ISC：国際標準化機構（International Organization for Standardization）／国際電気標準会議（International Electrotechnical Commission）。ISOはスイス本部の非営利組織。

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研 The Japan Research Institute, Limited

（参考）耐量子暗号｜2022―24年に標準化策定へ

- 現在汎用されている2048ビットRSA暗号は、2030年頃に危殆化する（暗号が解読可能となる）ことが想定されている。2030年頃までに耐量子暗号に移行できるようにするために、暗号の標準化作業が進められている。
- 一方、2048ビットの合成数を量子コンピュータで素因数分解する場合、理想的環境下でも4098量子ビットで数兆回（10の12乗）の計算量が必要であり、CRYPTRECは近い将来に危殆化する可能性は低いと指摘している。

耐量子暗号の標準化スケジュール

2020年
NIST標準化ラウンド３
- 最終候補（7つ）と代替候補（8つ）を選定

2022年～24年
NIST標準化ドラフト発行

2025年頃～
耐量子暗号への移行
CRYPTRECから移行指針発表（見込み）

鍵長がRSA2048の数十～数百倍になる見込みであり、ICカードに導入する際、IC容量を拡大する必要あり

2030年
耐量子暗号への移行完了

2048ビットRSA暗号の危殆化（暗号解読される）

＜参考＞ Michele Mosca方程式

耐量子暗号技術への移行検討判定式。
カナダ・ウォータールー大学量子コンピューティングセンター共同創設者のミッチェル・モスカ教授が提唱。

- x＝今後生成される情報の安全性を保ちたい年数
- y＝耐量子暗号アルゴリズムへの移行に必要な年数
- z＝大規模量子コンピュータが完成するまでの年数

x＋y＞z ならば，移行検討を要する。

y年後に「安全保存期間：x年間」と暗号化した暗号文は，x年未満に量子コンピュータによって破られる可能性があるため。

出所）NTTジャーナル https://www.ntt.co.jp/journal/1902/files/pdf/JN20190223.pdf

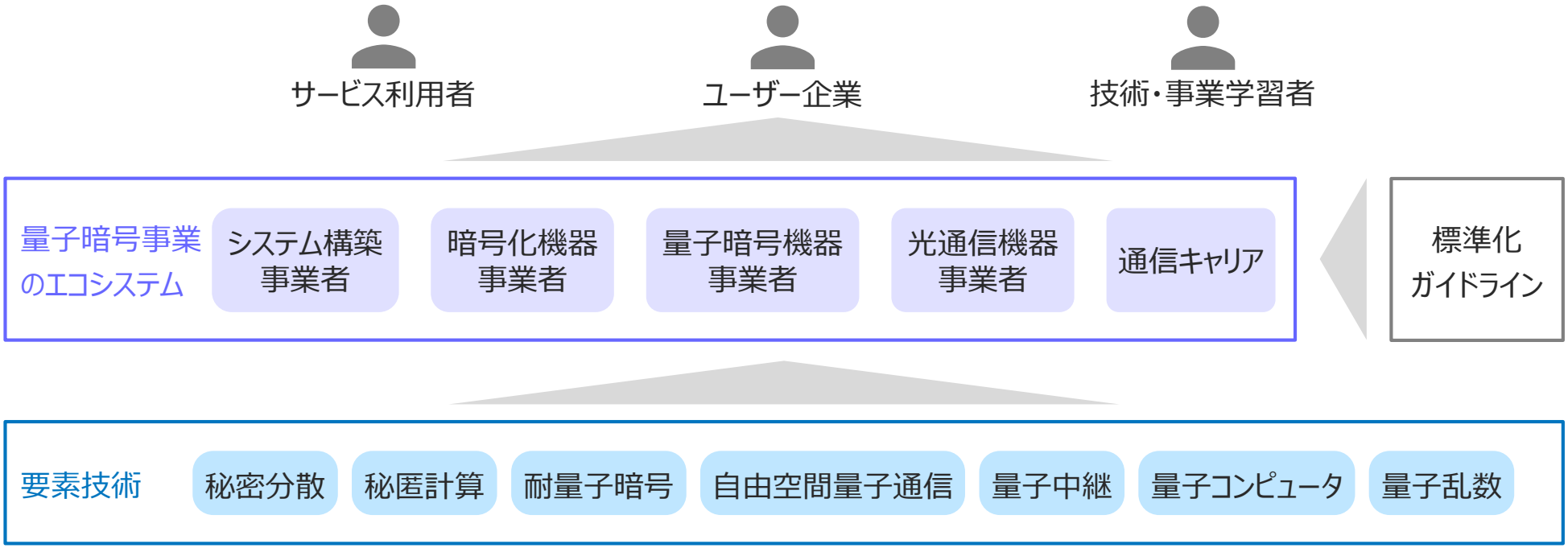
- NIST：The National Institute of Standard and Technology。アメリカ国立標準技術研究所。

出所）CRYPTREC https://www.cryptrec.go.jp/report/cryptrec-mt-1421-2019.pdf
https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2019.html

Copyright (c) 2021 The Japan Research Institute, Limited

5.1 社会実装に向けた課題

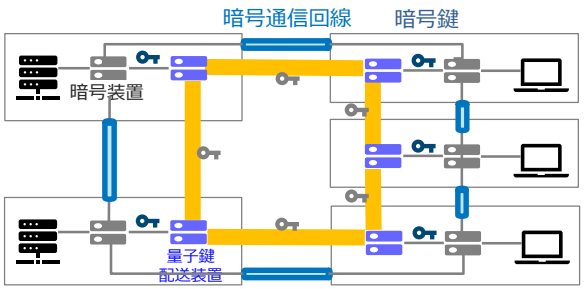
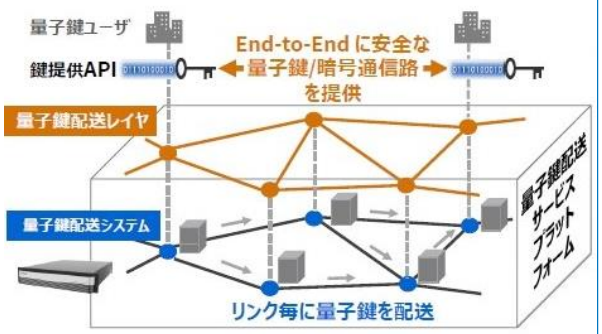
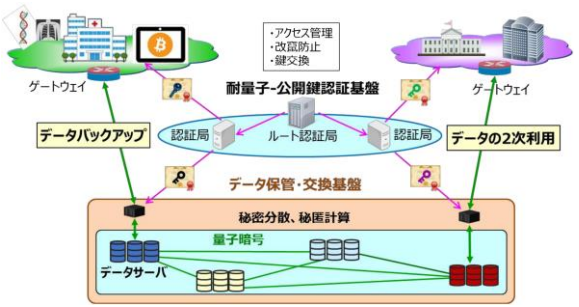
- 現状、設備投資に多額の費用を要するため、民生向けは普及に時間がかかる。ITメーカーは、行政機関内の機密データ共有などの運用実績を得て、民生用途へ展開・普及を図る戦略。扱う情報の漏洩リスクが膨大である、国防・警察・医療などから導入が進むと考えられる。
- 量子暗号の普及には、ガイドライン・標準の策定も待たれる。標準規格を採用した複数のネットワークが相互接続することで、通信網を拡大し、用途やユーザの拡大につながる。
- サービス提供事業者側も今後、量子暗号システム事業のエコシステムを構築し、裾野の広い通信インフラ事業として展開するため、量子暗号技術だけでなく、秘密分散、秘密計算、耐量子暗号といった複数の要素技術を組み合わせた分野横断の「量子セキュリティ技術分野」を創出し、産官学連携での試験運用を通じた人材育成が求められる。



Copyright (c) 2021 The Japan Research Institute, Limited

5.2 今後の展望（仮説）

- QKDの技術が進化し実用化が進むにつれて、周辺技術との融合により利活用が進んでいく。
- インターネットやクラウドサービスのインフラとして、普及していくと見込まれる。

	専用網でのQKDの利用拡大 （2021年～2025年）	パブリックなエコシステム形成 （2025年～2030年）	量子セキュアクラウドの実現 （2030年～）
概略図		 出所）東芝 https://eetimes.jp/ee/articles/2010/19/news035.html	 出所）情報通信研究機構 https://www.nisc.go.jp/conference/cs/kenkyu/dai11/pdf/11shiryou02.pdf
概要	• 専用の機器・回線を用いて、1対1または、特定メンバー間に閉じた環境で鍵交換を行う • 実証実験の事例あり	• キャリアやクラウド事業者との連携が拡大。QKDサービスがプラットフォーム化し普及 • ミドルウェア・ソフトウェア・APIが整備され、広範なユーザが利用できる環境が整備される	• QKDに加え、秘密計算、耐量子暗号なども実用化し、セキュアなクラウド環境が実用化される • 耐量子-公開鍵認証基盤なども整備され、インターネットのインフラとして広く普及する

Copyright (c) 2021 The Japan Research Institute, Limited

日本総研
The Japan Research Institute, Limited

5.3 まとめ

- 量子暗号通信とは、暗号鍵を量子の一種である「光子」に載せて送る通信方法。量子コンピュータが実現するとRSA暗号などが危殆化する懸念があり、その一解決策として、実用化が研究されている。

- 【原理】光子が持つ量子的ふるまい（分割不能性・複製不能性）を根拠に、盗聴されていないことが保証された暗号鍵を共有する。これにより、いかなる計算機でも解読不能であるという、情報理論的安全性を持つ暗号通信を実現する。量子暗号通信には、量子鍵配送（QKD）とワンタイムパッド（OTP）と呼ばれる要素技術を用いるが、量子鍵配送が直接可能な数十km程度より遠距離の通信には中継点を要する。中継点における鍵の盗聴リスクを解決するための、量子中継技術の研究も進められている。

- 【市場動向】中国がスピード・規模で先行。韓国とドイツが大規模網の構築に着手。米、英、日本における取り組みは小規模・局地的。日本では、NEC、東芝、情報通信研究機構などで研究開発が進められ、2021年度からは防衛・警察の通信網のセキュリティ対策として実証事業が始まる予定。

- 【普及への展望】光ファイバー網の整備といった大規模な設備投資を要するため、民生向けは時間を要する。ITメーカーは、国防・警察・医療分野の機密データ共有などで運用実績を得て、民生用途へ展開・普及を図る戦略。標準規格を採用した複数の網が相互接続することで、用途・ユーザ拡大につながる。サービス提供事業者も今後、通信インフラ事業として展開するため、量子暗号技術に、秘密分散・秘密計算・耐量子暗号といった要素技術を組み合せた、量子セキュリティ技術分野を創出し、産官学連携での人材育成が求められる。それらの結果、中長期的にはインターネットやクラウドサービスのインフラとして普及すると見込まれる。

Copyright (c) 2021 The Japan Research Institute, Limited

お問い合わせ

■本レポートは、作成日時点で弊社が信頼できると考えた資料に基づき作成したものですが、情報の正確性・完全性・有用性・安全性等を保証するものではありません。また、実際の技術動向等は、経済情勢等の変化により本レポートの内容と大きく異なる可能性もあります。ご了承ください。

本件に関するお問い合わせ・ご確認は、以下までお願いいたします。

株式会社日本総合研究所　先端技術ラボ
101360-advanced_tech@ml.jri.co.jp

金子　雄介　エキスパート／シニア・リサーチャー　kaneko.yusuke@jri.co.jp
間瀬　英之　リサーチャー　mase.hideyuki@jri.co.jp
身野　良寛　シニア・スペシャリスト　mino.yoshihiro@jri.co.jp

株式会社
日本総合研究所

東京本社
〒141-0022
東京都品川区東五反田2丁目18番1号
大崎フォレストビルディング

本資料の著作権は株式会社日本総合研究所に帰属します。