参考資料２

量子セキュリティ・ネットワークの研究開発・産業動向

JST CRDS
量子チーム（赤木、嶋田、眞子）

2021.12.6
量子技術イノベーション戦略見直し検討WG

国立研究開発法人科学技術振興機構 研究開発戦略センター
Center for Research and Development Strategy Japan Science and Technology Agency

1. 量子通信の研究開発・技術の現状

具体的な研究開発課題

量子コンピューティング 量子シミュレーション

NISQマシンのキラーアプリ探索
- 量子化学計算/機械学習
- 量子超越性
- 古典-量子ハイブリッドアルゴリズム

ゲート型量子コンピュータ実機の試作
- 超伝導量子ビット系

エラー耐性量子コンピューター基盤技術
- 量子ソフトウェア
- 量子誤り訂正方式
- 様々な量子ビット系

複雑系の計算が可能な量子シミュレータ開発

量子計測 センシング

ダイヤモンドNV中心作製技術
- 大型・高品質化（T_2向上）
- 新材料探索

ダイヤモンドNV中心と量子もつれ光センサの医療・診断応用
- プロトタイプ製作
- 脳磁計・心磁計
- イメージング技術

原子干渉計・光格子時計の実用性探索
- 小型化・可搬化
- 高精度化
- 「秒」の再定義・標準化

量子暗号・通信

QKDの社会実装と一般普及の促進
- BB84運用・品質保証
- 市場投入・キラーアプリ探索
- 低価格化

標準化活動への積極的寄与
- ETSI & ITU-T
- 耐量子-公開鍵暗号

高速化・長距離化に向けた量子中継技術、ネットワーク技術
- 量子メモリー・全光量子
- 量子望遠鏡
- 量子インターネット

量子マテリアル

トポロジカル量子物質
- トポロジカル量子コンピュータ
- トポロジカル絶縁体
- ワイル磁性体

スピントロニクス材料
- 半導体スピントロニクス
- スピンMOSFETデバイス

エネルギー変換材料
- スピン-ゼーベック効果
- スピン流

フォトニクス材料
- メタマテリアル
- シリコン／ナノフォトニクス

共通量子技術基盤

原子・分子・光科学
量子光学
量子エレクトロニクス

単一光子制御技術
- 効率化・室温動作・光子検出器
- 量子もつれ光子、多体量子もつれ制御

異種の量子ビット間結合（ハイブリッド量子科学）
- 固体量子ビット & 光 など

量子ビット基盤技術
- 様々な量子ビット系

材料設計・製造、計測技術

研究開発の国際比較（量子暗号・通信）

	量子暗号・通信			
	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	• 量子暗号通信の理論的研究は、東京大学、名古屋大学、富山大学、慶應義塾大学、NICT、NII、産総研、三菱電機などで実施。 • 実験的研究も、QKDではNICT、北海道大学と学習院大学で、量子中継では大阪大学と横浜国立大学で活発に進展。
	応用研究・開発	○	→	• NICTを中心に、SIPにおいてネットワークと量子セキュアアプリケーションの研究が進められている。 • 衛星量子通信についても実証に向けた研究がソニー、スカパーJSATも参加して進められている。
米国	基礎研究	◎	↗	• DOE傘下の国立研究所や大学において古くから量子技術・量子情報科学の基礎研究が続けられてきた。 • 最近では量子中継ネットワークについての研究も進展。
	応用研究・開発	○	→	• Quantum XchangeがId Quantiqueと協業し、QKD ネットワークサービスを開始した。 • 各地でフィールドテストのための量子ネットワークテストベッドが作られ、衛星量子通信も量子もつれ共有をターゲットにプロジェクトが始まっている。
欧州	基礎研究	◎	↗	• オランダQuTechを中心とした量子ネットワーク研究Quantum Internet Allianceやジュネーブ大・東芝ケンブリッジ研究所ではQKD研究が行われている。 • 予算規模1300億円を超えるEU Quantum Technology Flagshipプロジェクトがスタートし、第一次の採択が決定。
	応用研究・開発	◎	↗	• 英国Quantum Communication Hubによる量子暗号ネットワークが建設されている。EUにおけるOPENQKD、スペインでのCVQKDによるネットワーク、ドイツでのQuNet Initiativeなど各国で量子ネットワーク開発が進む。衛星量子通信の研究開発もドイツなどで行われている。 • ETSIによる標準化活動も進展している。
中国	基礎研究	○	↗	• 中国科学技術大学のグループは量子暗号でも新しいプロトコルの実証実験を素早く行っている。 • Atomic ensemble量子メモリでも進んでいる。
	応用研究・開発	◎	↗	• 世界初の衛星量子通信を成功。人工衛星と量子通信ネットワーク用いた広域量子暗号通信ネットワークが完成。 • 量子専業企業の株式が上場され量子が投資の対象に。 • ITU-Tのネットワーク標準化、ISOの実装安全性標準化でリード。

〈現状〉
◎ 特に顕著な活動・成果が見えている
○ 顕著な活動・成果が見えている
△ 顕著な活動・成果が見えていない

〈トレンド〉
↗：上昇傾向
→：現状維持
↘：下降傾向

JST-CRDS「研究開発の俯瞰報告書　ナノテクノロジー・材料分野（2021年）」
「研究開発の俯瞰報告書　システム・情報科学技術分野（2021年）」

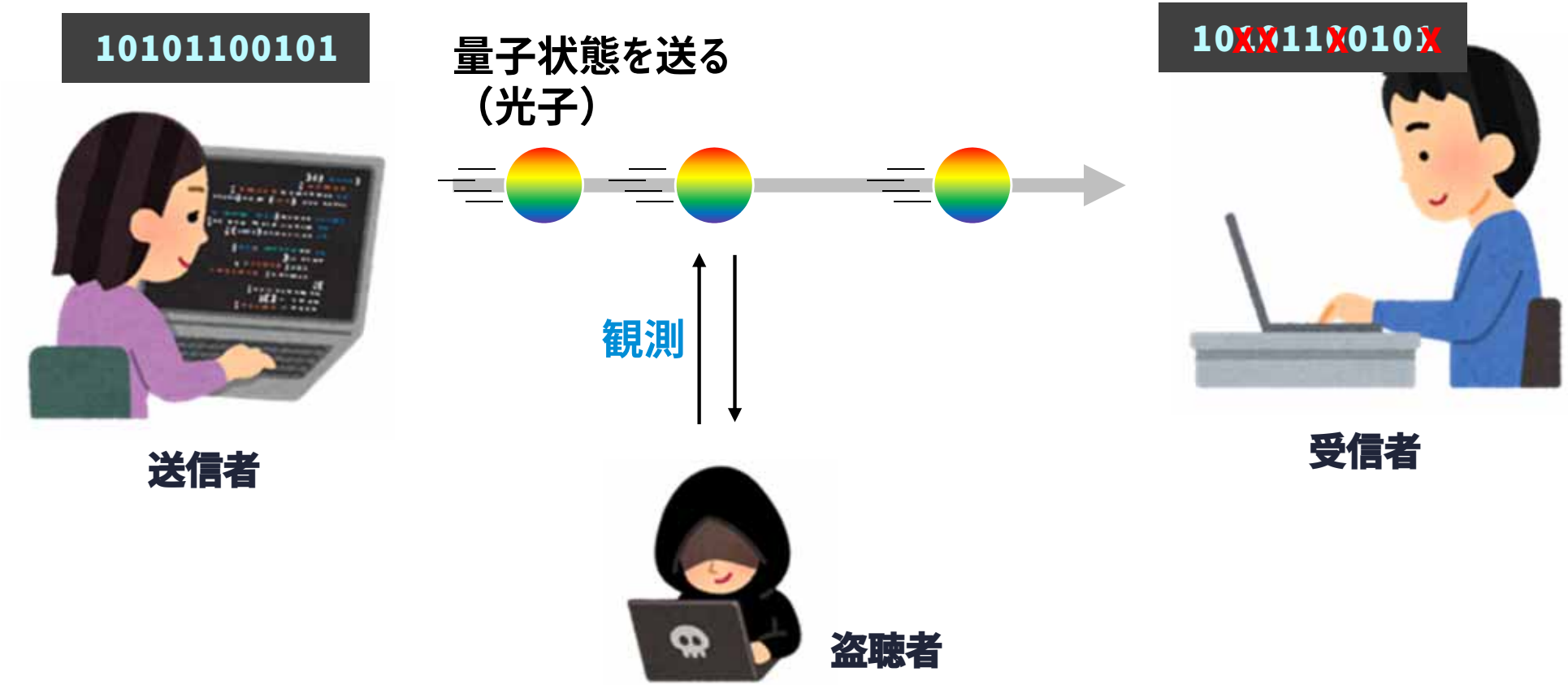
量子暗号鍵配送（QKD）

BB84（第１世代QKD）

観測に依って量子状態が変化する性質を利用して、盗聴を検知する。

BBM92（量子もつれ型）

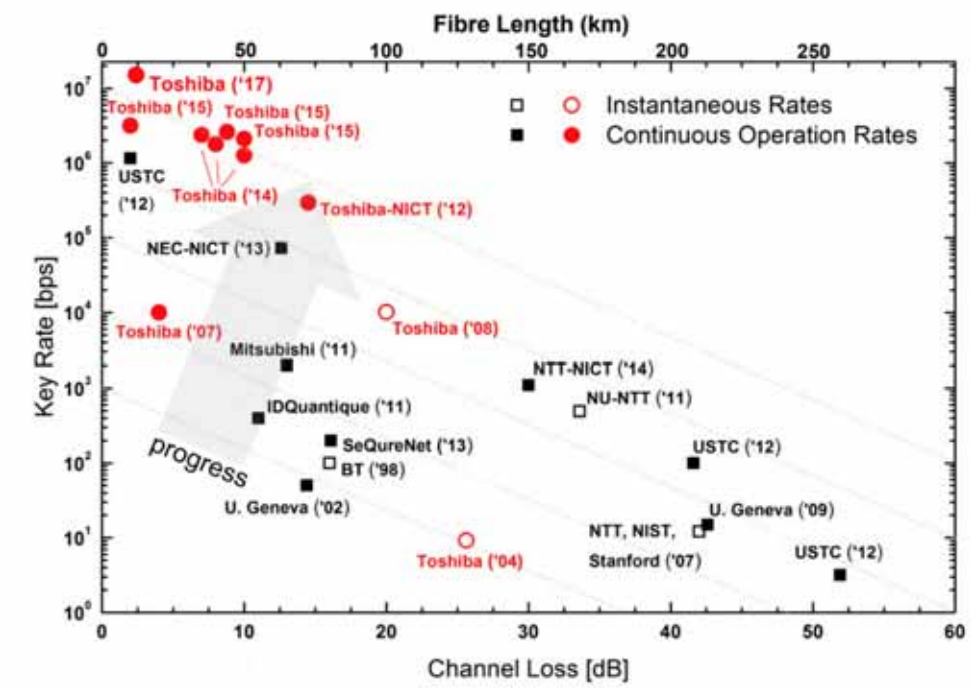
エンタングルした光子対を送信者と受信者が測定することで安全に鍵を共有する。



物理法則が通信システムの安全性を担保。

量子暗号・量子通信

	量子もつれ型		光子型	光波型
安全性	極めて高	高	高	中
プロトコル	デバイス独立QKD, MDI-QKD	E91, BBM92	BB84, DPS, RR-DPS等	CV-QKD
コスト	極めて高	高	中	低
現状	実験室段階	50bps@20km	300kbps@50m 1kbps@100km	10kbps@25km



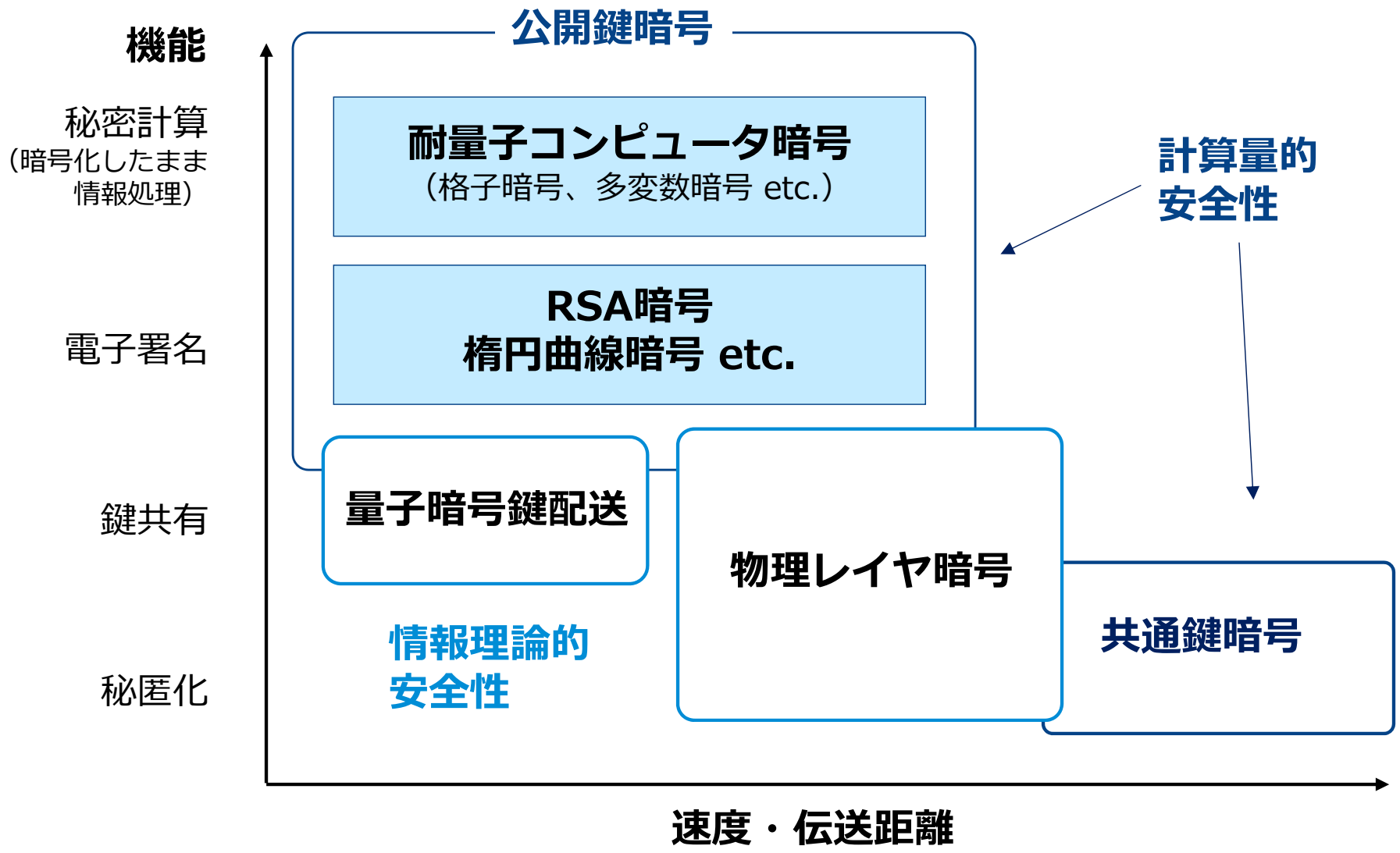
佐々木雅英「量子通信、量子暗号の研究動向と今後の戦略」 量子科学技術委員会（2016.6.20）

斉藤史郎「産業界から見た量子暗号通信の現状と政府に対する期待」イノベーション政策強化推進のための有識者会議「量子技術イノベーション」（2019.5.16）

量子暗号・量子通信の長距離化

方式	概要
信頼できる局舎（trusted-node）	社会実装段階。現状のQKDの性能は光ファイバを通じた通信で約100kbps@50km。プロトコルはおとり信号つきBB84が用いられる。信頼できる局舎を介して、暗号鍵をカプセルリレーし、ネットワーク化する。任意の局舎間で安全な通信が可能。
Twin-Field QKD	原理実証段階。光子の送信を両端の拠点から行い、中間にある拠点で光子検出を行う構成のため、距離を倍にすることが可能。500kmを超える暗号鍵共有が可能。異なる光源間での位相同期など、実用化への障害は残っている。
衛星利用	中国の「墨子」衛星による原理実証実験が報告されている。衛星利用は、現時点でグローバルな鍵配送を可能にする唯一の方法（地上で大陸横断するには他国の領土に局舎を置く必要がある）。光子レベルでの光ビームの捕捉追尾が重要課題。
量子中継・量子インターネット	原理実証段階。隣接するノード間の量子もつれを、離れたノード間の量子もつれに変換する。物質量子メモリでは原子、キャビティQED、ダイヤモンド色中心などの提案があるが、性能指標は一長一短。物質量子メモリを用いない全光方式も提案されている。プロトコル・ソフトウェアに関するシミュレータの研究開発も進められている。

量子暗号鍵配送と耐量子コンピュータ暗号



佐々木雅英、MEXT量子科学技術委員会（H28第４回）「量子通信、量子暗号の研究動向と今後の戦略」（2016/6/20）を参考にCRDS作成

耐量子暗号（PQC） ＝ 耐量子コンピュータ暗号

量子暗号鍵配送（QKD）とは異なることに注意

	代表例	量子アルゴリズム	対策
共通鍵暗号	**AES**	**グローバー検索** （共通鍵を総当たりで探索）	鍵長を２～３倍に延伸
公開鍵暗号	**RSA暗号** **楕円曲線暗号**	**ショアのアルゴリズム** （素因数分解・離散対数問題が容易に解ける）	**耐量子暗号への移行**

耐量子暗号の標準化

赤字：日本からの提案
太字：Round2
太字青：Round3 finalists
太字緑：Round3 alternates

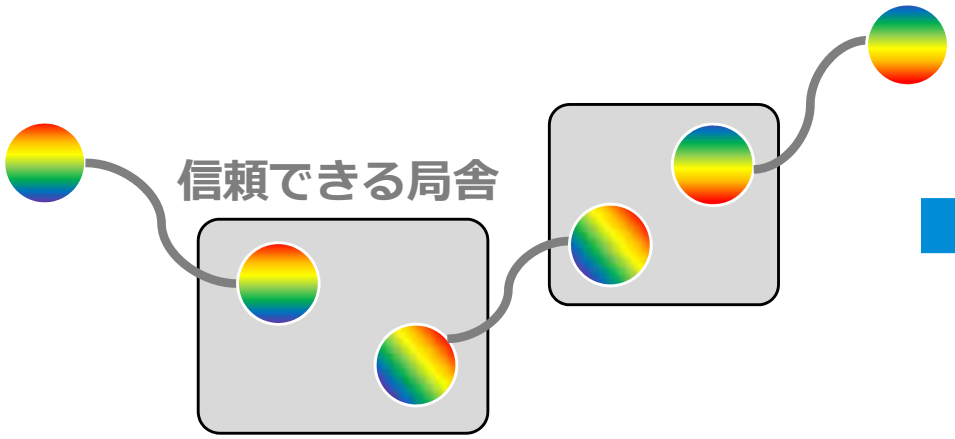
	格子暗号	符号暗号	多変数多項式	その他
暗号化・鍵確立	Compact LWE, **CRYSTALS-KYBER**, Ding Key Exchange, EMBLEM and R.EMBLEM, **FrodoKEM** Giophantus, KCL, KINDI, **LAC**, Lima, Lizard, LOTUS, **NewHope**, **NTRU**(NTRUEncrypt + NTRU-HRSS-KEM), **NTRU Prime**, Odd Manhattan, **Round5**(HILA5+Round2), **SABER**, **Three Bears**, Titanium	BIG QUAKE, **BIKE**, **Classic McEliece**, DAGS, Edon-K, **HQC**, **LEDAcrypt**(LEDAkem+LEDApkc), Lepton, McNie, **NTS-KEM**, QC-MDPC KEM, Ramstake, RLCE-KEM, **RQC** **ROLLO**(LAKE+LOCKER+Ouroboros-R)	CFPKM, DME, SRTPI	GuessAgain, HK17, Mersenne-756839, Post-Quantum RSA-Encryption, RVB, **SIKE**
デジタル署名	**CRYSTALS-DILITHIUM**, DRS, **FALCON**, pqNTRUsign, **qTESLA**	pqsigRM, RaCoSS, RankSign	DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**, SRTPI	Post-Quantum RSA-Signature, WalnutDSA, Gravity-SPHINCS, **Picnic**, **SPHINCS+**

https://csrc.nist.gov/Projects/post-quantum-cryptography/

量子中継技術

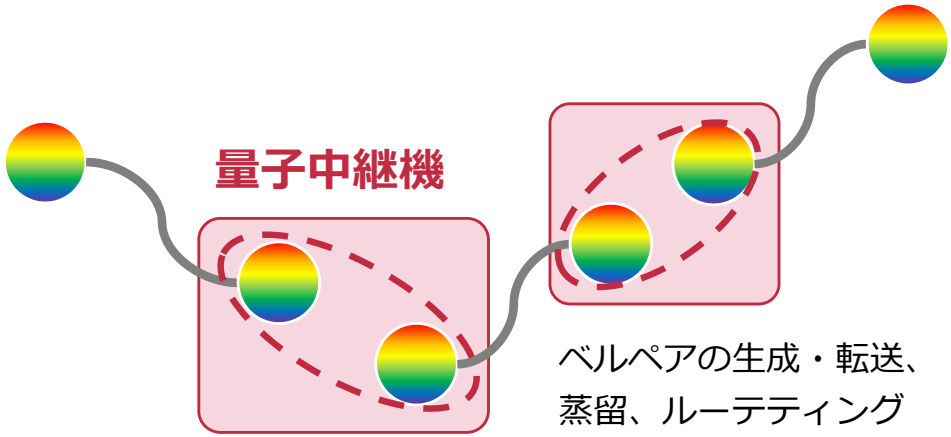
量子暗号鍵配送（QKD）

「信頼できる局舎」によるリレー



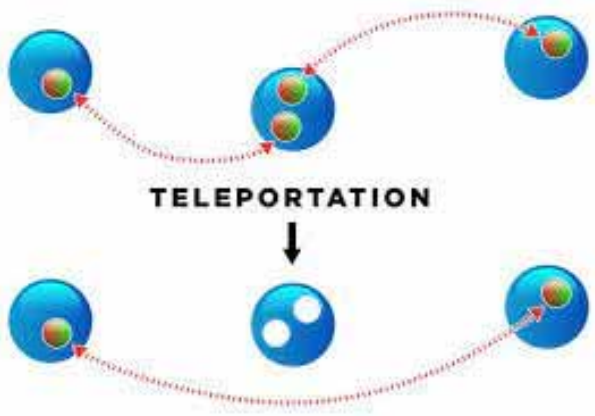
量子インターネット

量子中継機による量子情報ネットワーク



量子中継機（Quantum Repeater）

- エンタングルメントペア（ベルペア）の生成・転送
- 蒸留によるフィデリティの確保
- ルーティングなどのネットワーク管理



量子暗号鍵配送と量子インターネット

		共有されるデータ	
		デジタルデータ （非量子）	量子データ （量子状態）
通信	ビット （非量子）	インターネット 送信者 デジタルデータ 11010… 0 1 0 1 1 ビット 受信者 デジタルデータ 11010…	
	量子 ビット	**量子暗号鍵配送** 送信者 デジタルデータ 11010… ? ? ? ? ? 量子ビット 受信者 デジタルデータ 11010…	**量子インターネット** 送信者 量子データ 00101… ? ? ? ? ? 量子ビット 受信者 量子データ 00101…

量子ネットワークのユースケース

	ユースケース例	量子ネットワーク技術の進展	量子コンピューティング・センシング技術の進展
2020年代	● 医療:電子カルテやゲノム情報など、漏洩することで生涯にわたって影響がある生体情報のやり取り ● 製造:企業の営業秘密・ノウハウ、重要技術など、漏洩することで企業活動に大きな影響がある情報のやり取り ● 金融:金融システム等に係る情報などのやり取り	• QKD(関東圏→全国規模)	• NISQ量子コンピュータ
2030年代	● 行政・外交・安全保障:行政における個人情報のやり取り、在外公館における機密情報の通信、機密情報のやり取り ● 生活:モバイル端末向け暗号自動販売機などの活用による家庭レベルでの超セキュアインターネット(個人の医療情報・金融情報などのやり取り)	• QKD(全国規模→グローバル規模) • 衛星 QKD/ 物理レイヤ暗号 • 量子ネットワーク	• NISQ 量子コンピュータ • 小規模エラー耐性量子コンピュータ • 量子センサ
2040年代	◆化学・材料・創薬など:量子ネットワークに接続された量子コンピュータによる新素材・新薬等の発見 ■ 防災・災害対応:量子ネットワークに接続された量子センサーによる微弱な重力変動などの監視 ● 資源開発:月・火星における掘削ロボットの大容量画像伝送(シャノン限界越え量子符号化)	• QKD(グローバル規模) • 衛星量子通信 • 量子ネットワーク(グローバル規模)	• エラー耐性量子コンピュータ • 分散量子コンピューティング • 量子センサ

●:QKD、◆量子コンピュータ、■:量子センシングによるユースケース例

NICT IDI, “量子ネットワークホワイトペーパー” (2021年3月).

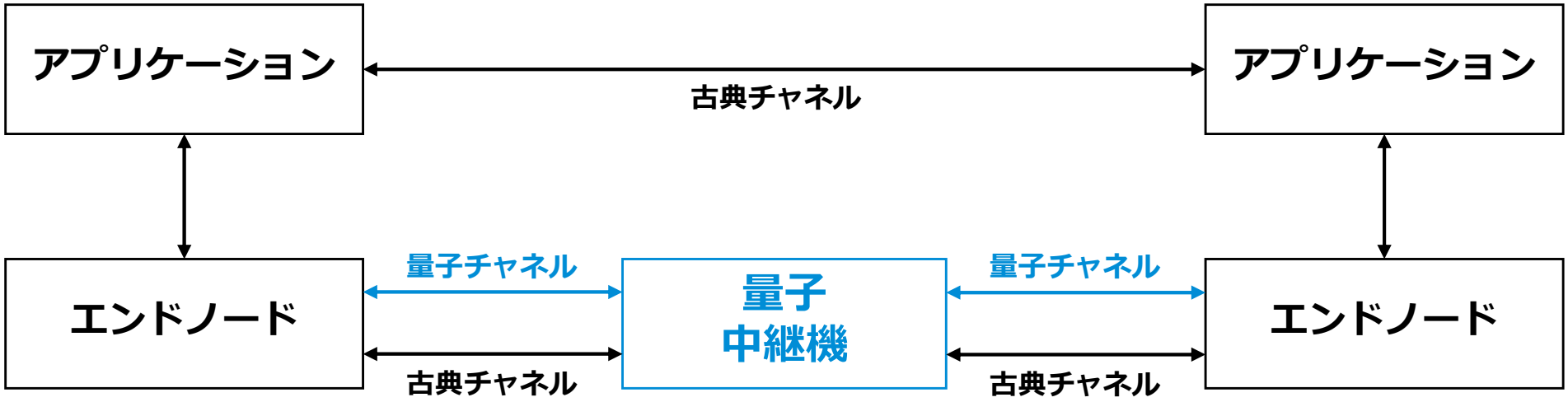
量子インターネットの概念モデル

Internet Research Task Force (IRTF)

- インターネット技術標準化委員会（IETF）の姉妹団体。研究に特化。

Quantum Internet Research Group (QIRG)

- 2018年11月設置。チェアはR. Van Meter（慶應大）とW. Kozlowski（QuTech）



ノードの種類

- **量子ルータ**：制御信号により制御される量子ノード。E2Eでの交換ベルペアを決めるなど。
- **自動量子ノード**：量子チャネルのみを中継し、延伸化する。
- **エンドノード**：エンタングルメントペアを受信する。量子メモリは持たない。
- **非量子ノード**：古典チャネルの制御を行う。

IRTF-QIRG “Architectural Principles for a Quantum Internet”
NICTイノベーションデザインイニシアティブ活動報告（2020-R1）

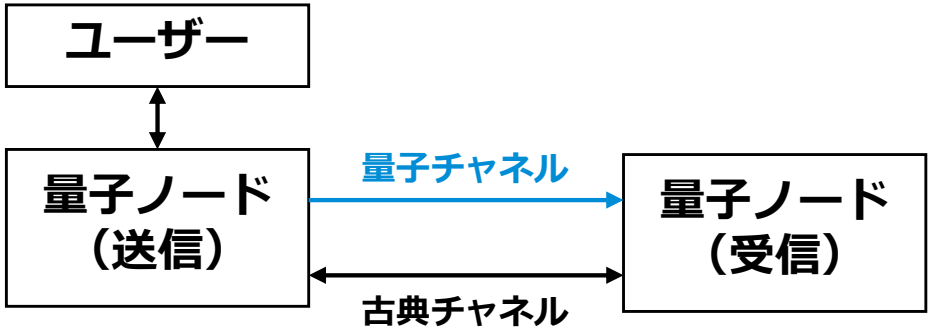
量子インターネットのユースケース

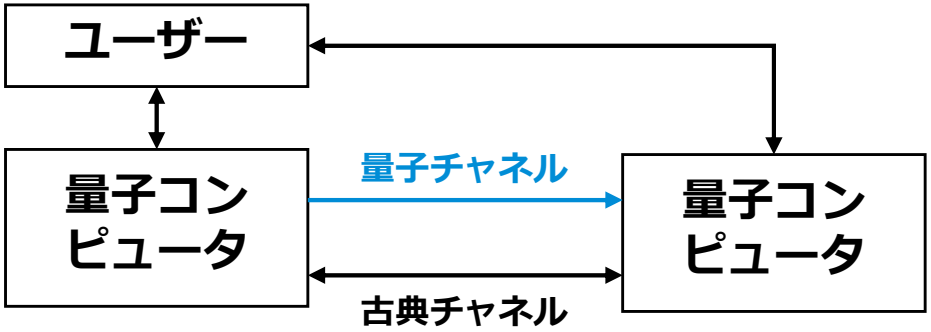
量子セキュア通信

- 複数のエンドノード間のQKD
- ブロックチェーン

分散量子計算

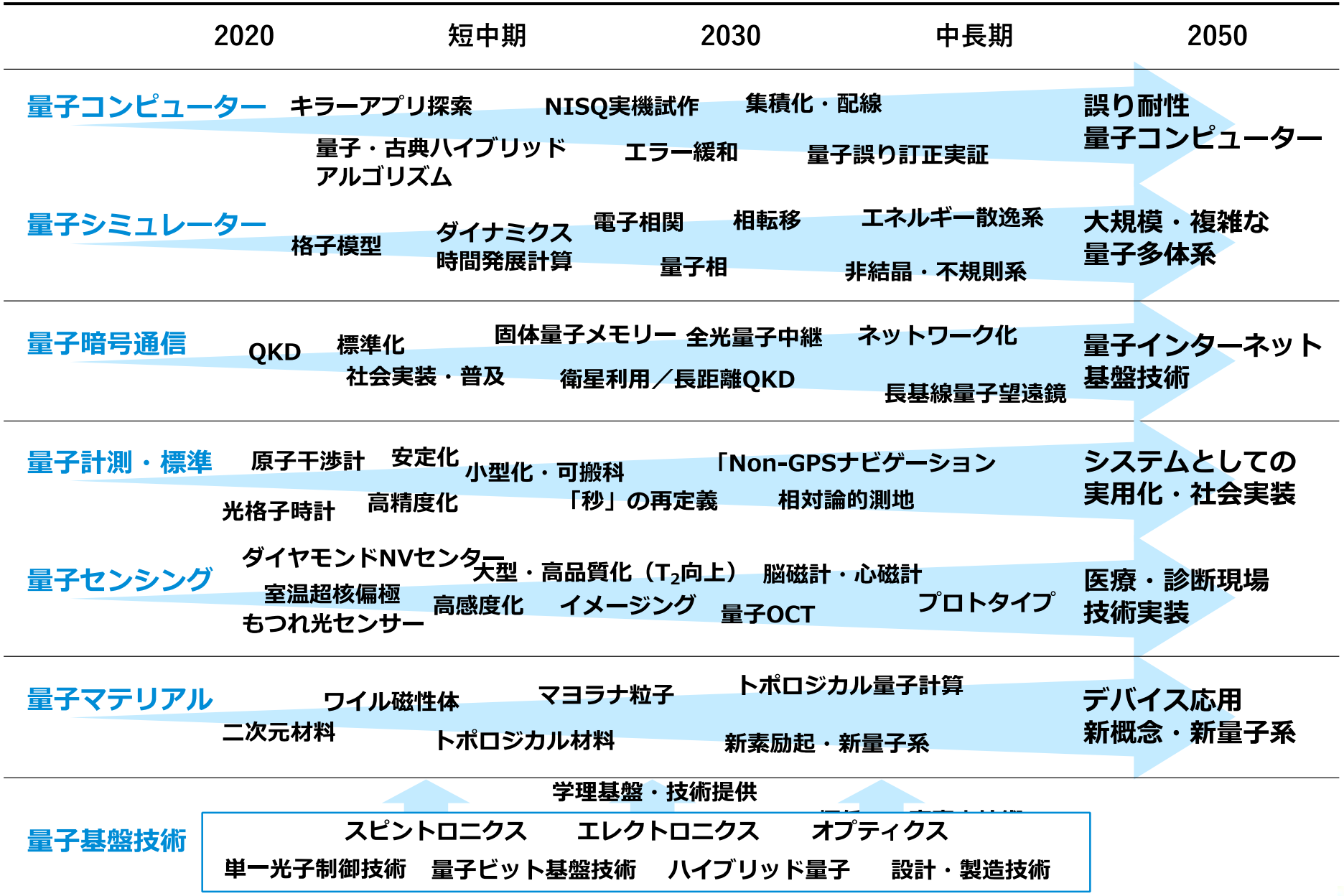
- 複数の量子コンピュータの協同動作により大きな量子計算を実行
- プライバシー保護をしながらセキュアな量子計算





IRTF-QIRG “Architectural Principles for a Quantum Internet”
https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/

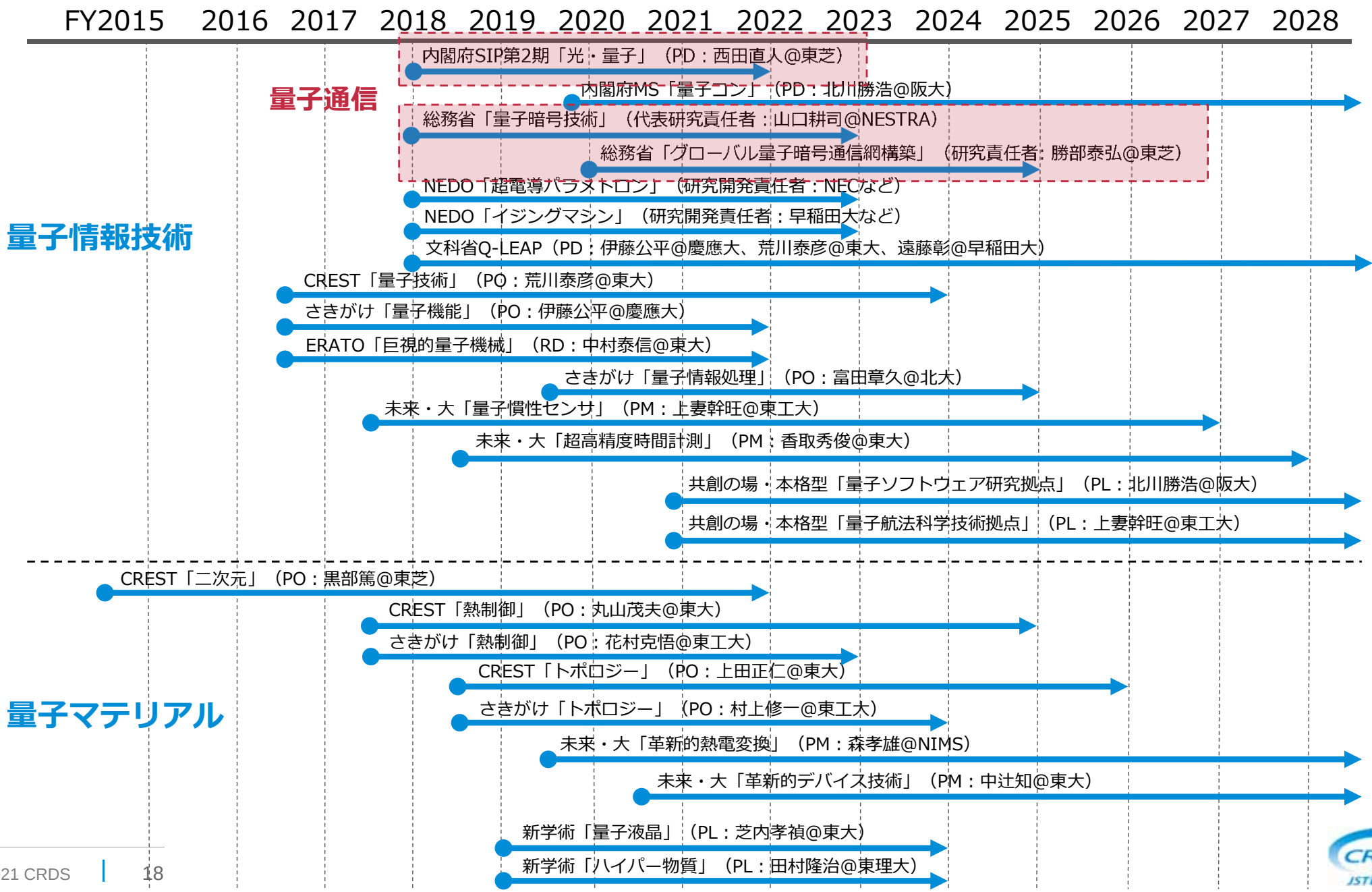
量子技術 現状と展望



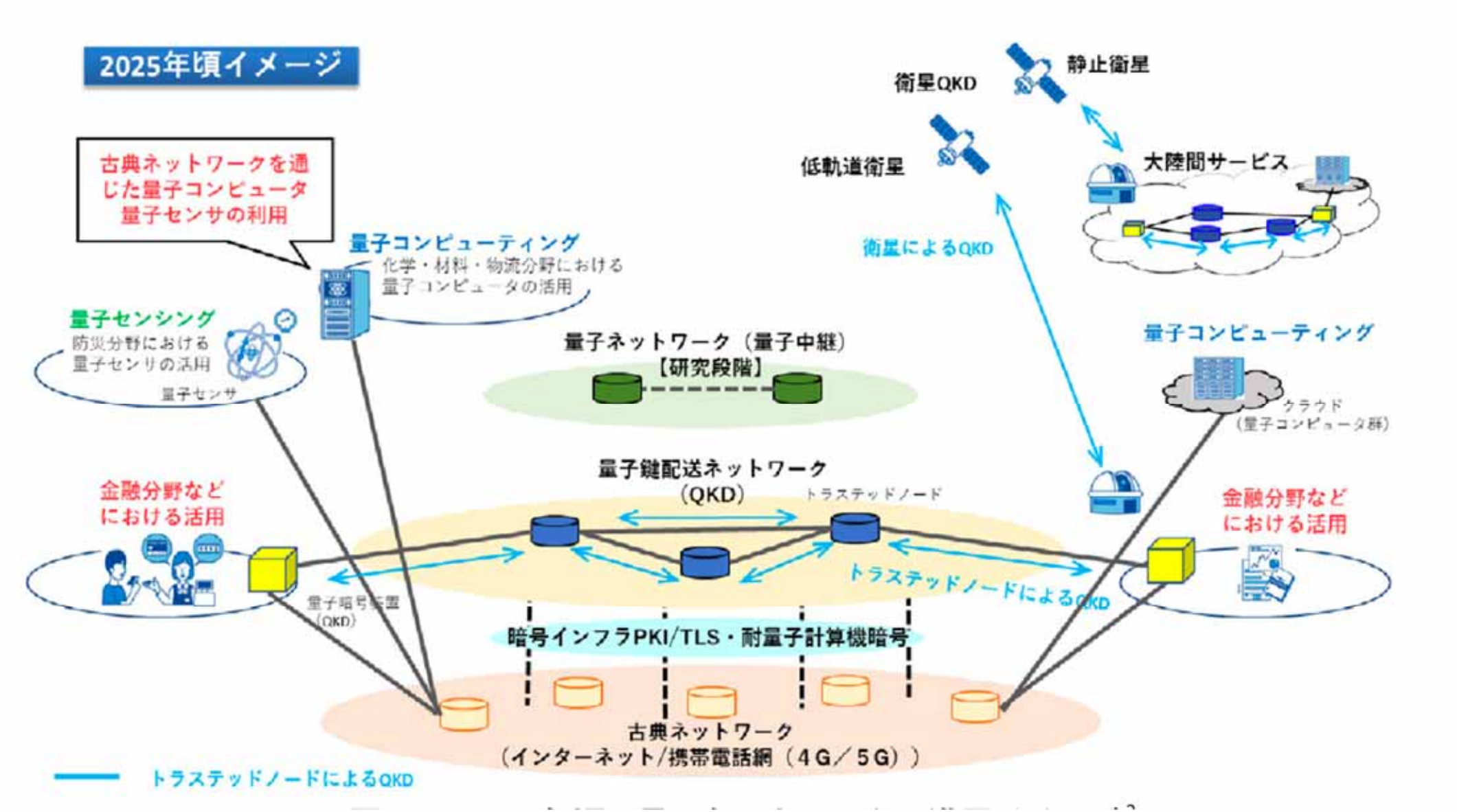
CRDS 戦略プロポーザル「量子2.0 ～量子科学技術が切り拓く新たな地平～」（2020）

2. 国際競争・各国の量子通信政策・PJ

日本の量子科学技術関連PJ



QKDネットワークサービスイメージ（2025年頃）



NICT IDI, “量子ネットワークホワイトペーパー” (2021年3月).

量子通信・量子インターネット研究動向

日本

- グローバル量子暗号通信ネットワーク

中国

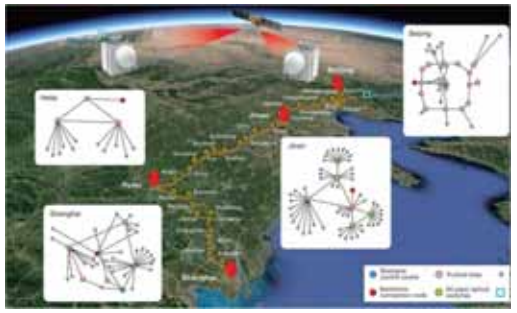
- National quantum secure communication backbone network（京滬幹線）

米国

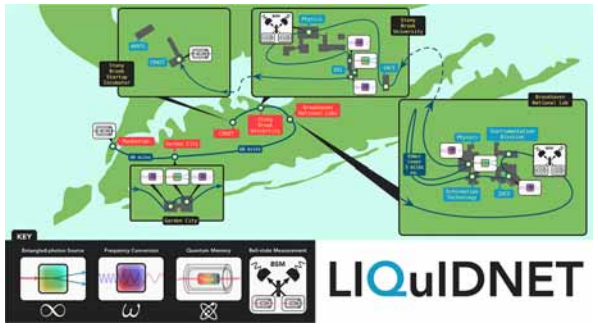
- Center for Quantum Networks (NSF)
- Long Island Quantum Repeater Network
- Chicago Quantum Network

欧州

- Quantum Internet Alliance (オランダ)
- Q.Link.X（ドイツ）
- OpenQKD （スペイン）



YA Chen, et al. ”An integrated space-to-ground quantum communication network over 4,600 kilometres”, Nature 589, 214-219 (2021).



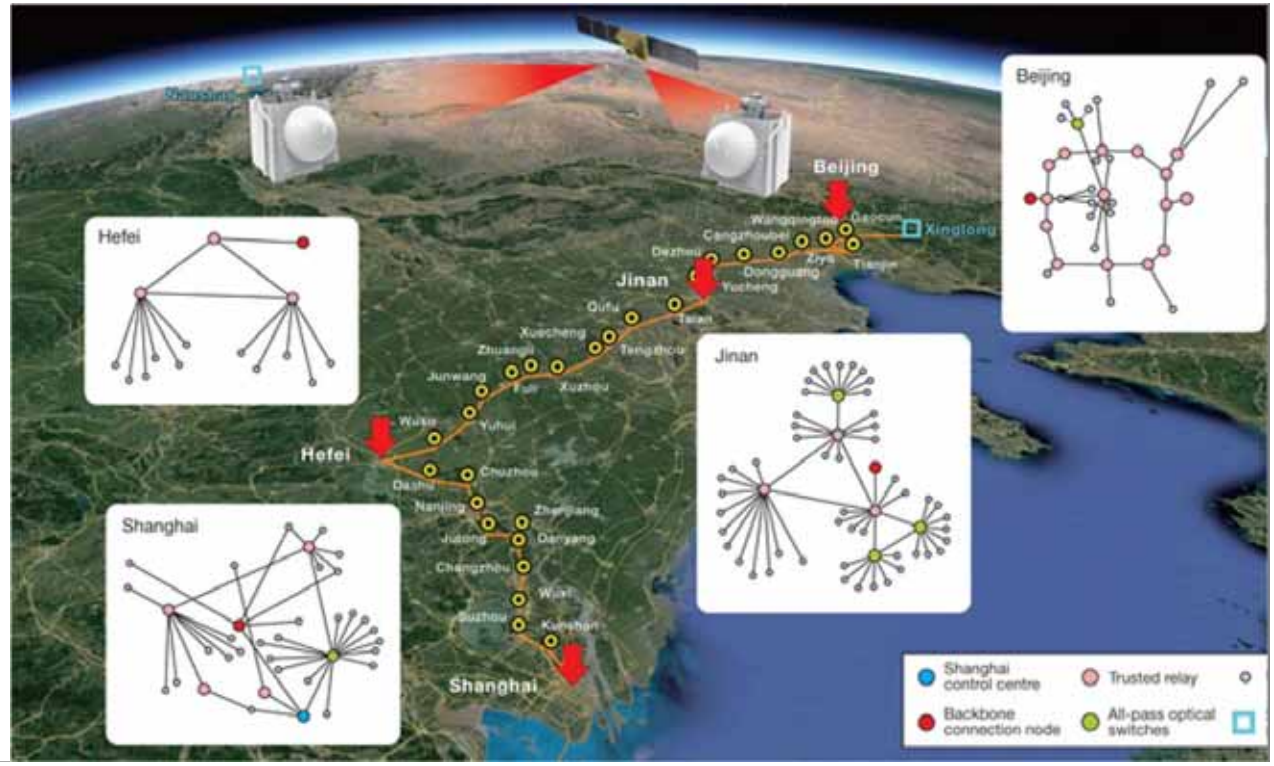
http://qit.physics.sunysb.edu/wordpress/?page_id=485

https://labs.ripe.net/author/becha/introduction-to-the-quantum-internet/

実証実験@中国

地上・衛星統合量子通信ネットワーク

- 地上の光ファイバーと衛星リンクを組み合わせたQKDネット（のべ4600km）
- 衛星から地上へのQKD鍵生成レートは47.8kbps（以前の40倍向上）。地上ベースのQKDもツインフィールドQKD方式により500kmを達成。
- 量子通信衛星「墨子」による実験（2016）、北京-上海間の光ファイバーネットワーク（2017）に続く、アップデート。

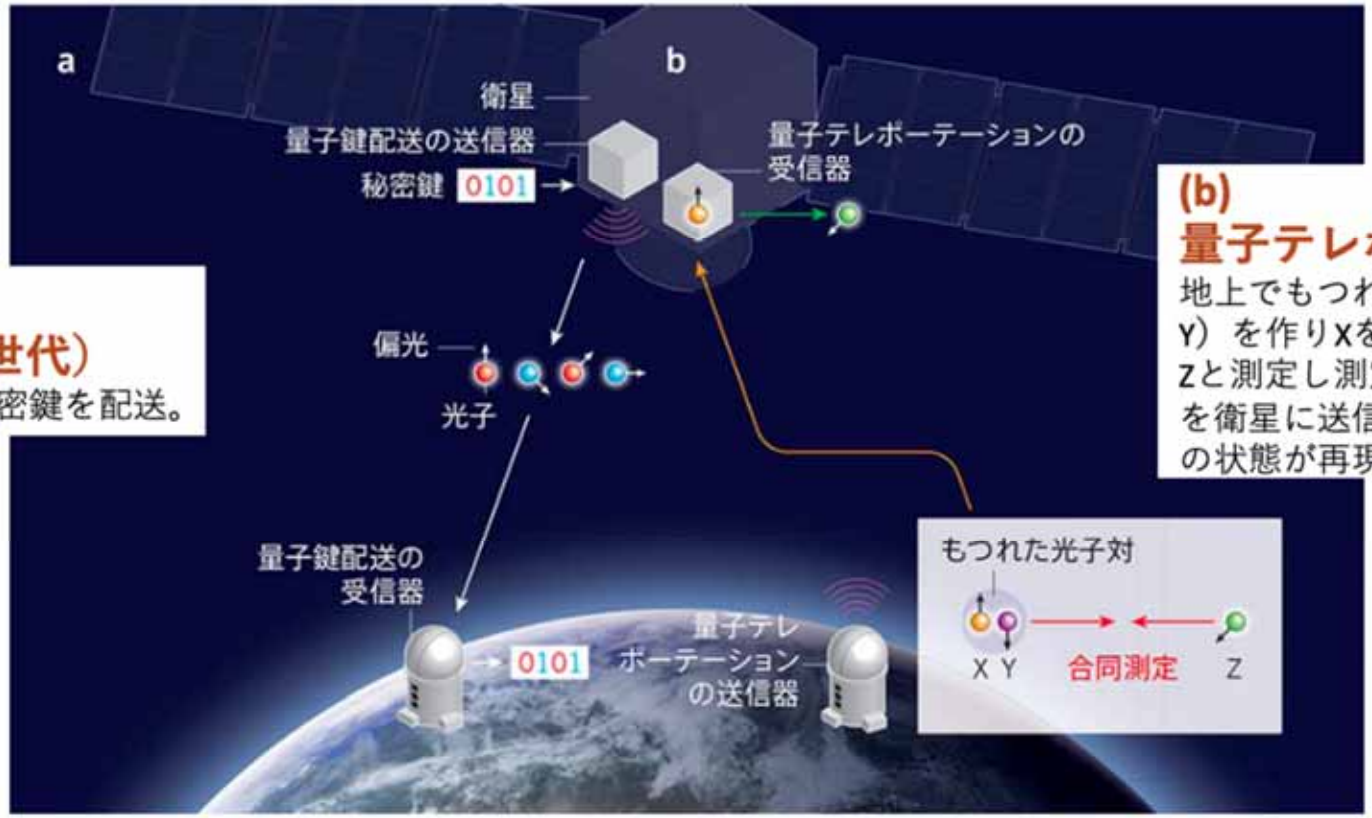


Chen, YA., Zhang, Q., Chen, TY. *et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589,** 214–219 (2021). https://doi.org/10.1038/s41586-020-03093-8

量子通信衛星

人工衛星Micius（＝墨子）

- 2016年８月打ち上げ。地球規模の量子通信ネットワーク実証実験。
- 衛星からエンタングル光子対を地上局に送信。
- 衛星から地上局への鍵配送。地上から衛星への量子テレポーテーション。



(a)
QKD（第１世代）
衛星→地上で秘密鍵を配送。

(b)
量子テレポーテーション
地上でもつれ状態の光子対（XとY）を作りXを衛星に送る。地上のZと測定し測定結果（古典情報）を衛星に送信すると、衛星上でZの状態が再現される。

Sheng-Kai Liao, et al, Satellite-to-ground quantum key distribution, Nature 549, 43-47 (2017). Ji-Gang Ren, Ground-to-satellite quantum teleportation, Nature 549, 70-73 (2017).

量子ICT実用例@中国

中国工商銀行

- ネットバンキングのデータの北京・上海間量子暗号通信に成功。
- 量子乱数発生器を利用して、ユーザー管理・認証のセキュリティ向上。

http://finance.people.com.cn/n1/2021/0512/c1004-32101145.html

徽商銀行（HQ：安徽省・合肥）

- 主データセンターとバックアップセンターの間でのQKD利用。
- 支店と中国金融認証局（CFCA）の間でのデジタル証明書の発行・送信。

https://www.cfca.com.cn/20171106/100002298.html

海南省

- 衛星利用で政府データセンタ、産業商業管理局の科学技術部門、地域の人的資源社会保障局間で量子通信実証PJ。

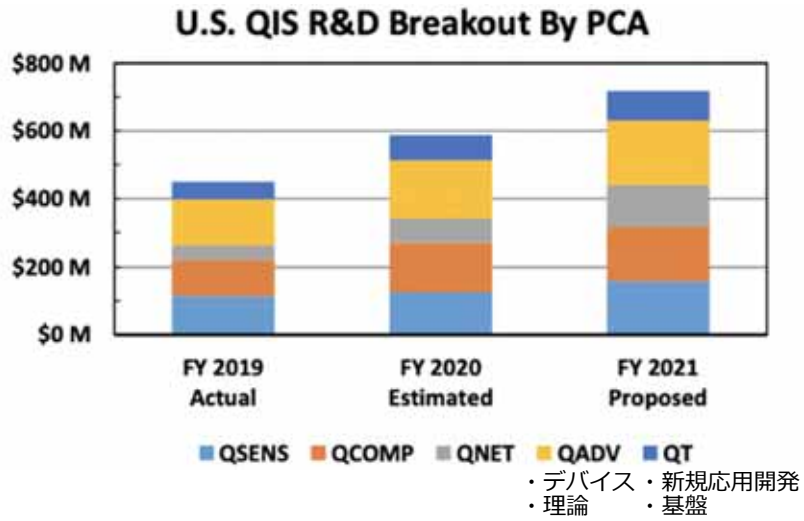
https://www.yicaiglobal.com/news/hainan-enters-quantum-communications-era-with-demonstration-project

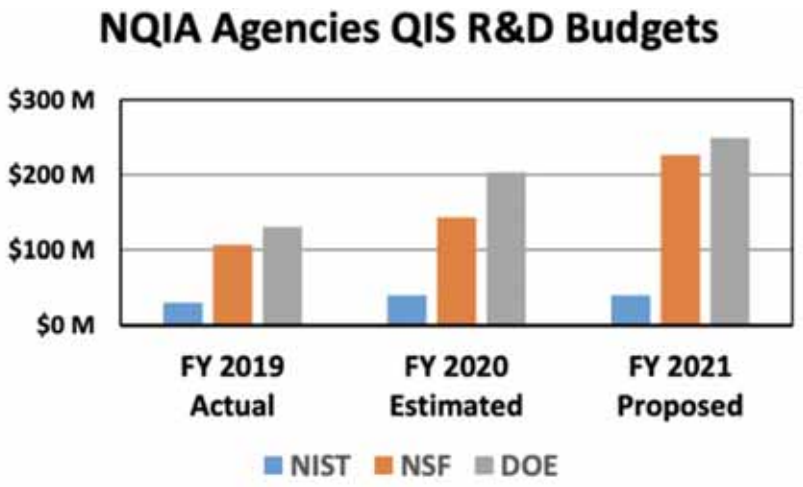
米国政府の動向（2021年～）

量子情報科学の研究開発費2021～22年度に倍増の計画（2021年1月）

- 2019年はNQIプログラムの立ち上げ、2020年には複数のNQIセンターとコンソーシアムの設立などが行われた。
- QIS研究開発のための実際の予算は4億5000万ドル（FY2019）、5億8000万ドル（FY2020 概算）、FY2021は7億1000万ドル（要求額）。

https://www.quantum.gov/wp-content/uploads/2021/01/NQI-Annual-Report-FY2021.pdf





量子ネットワークの協調的アプローチに関する報告書の発表（2021年1月）

国家科学技術会議（NSTC）は、量子ネットワーク（QN）推進のための技術的勧告と制度的勧告を行い、政府機関がとるべき方向性を提示。

技術的勧告（TR）

TR1：QNのユースケース研究を継続
TR2：QNの有益なコアコンポーネントの優先順位付け
TR3：QNをサポートする古典技術の改善
TR4：適切なサイズのQNテストベッドの開発

制度的勧告（PR）

PR1：QN研究開発に関する省庁間連携の強化
PR2：QN研究開発インフラのタイムテーブルの確立
PR3：QN研究開発の国際協力の促進

https://www.quantum.gov/wp-content/uploads/2021/01/A-Coordinated-Approach-to-Quantum-Networking.pdf

NSF傘下PJ

Quantum Leap Challenge Institutes (QLCI-CI)（各$25M/5年, 2020-25, Round I）

Q-SEnSE: Quantum Systems through Entangled Science and Engineering

代表：U. Colorado Boulder。量子センサー技術の設計、構築、採用を行い、精密測定の幅広い応用の実現を目指す。

http://amophysics.berkeley.edu/news/2020/7/21/establishment-of-the-quantum-leap-challenge-institute-for-present-and-future-quantum-computation

HQAN: Hybrid Quantum Architectures and Networks

代表：U. Illinois。小規模な量子プロセッサーを相互に接続したネットワークを構築し、分散型量子処理による量子プロセッサーのスケーリングの実現を目指す。

https://mrl.illinois.edu/news/prof-brian-demarco-and-iquist-lead-new-25m-nsf-hybrid-quantum-architectures-and-networks

BQIC・Berkeley Quantum Information and Computation Center

代表： UC Berkeley。先進的で大規模な量子コンピューターの設計、効率的なアルゴリズムの開発を通じ、最終的には量子コンピューターが最高の古典コンピュータを凌駕することを実証することを目指す。

http://amophysics.berkeley.edu/news/2020/7/21/establishment-of-the-quantum-leap-challenge-institute-for-present-and-future-quantum-computation

NSF Engineering Research Center (ERC)（$26M（追加$24.6/5年）, 2020-25 ）

CQN・Center for Quantum Networks

代表： U. Arizona。量子リピーターを実現し、完全に誤り訂正された量子接続を100kmの距離を10M量子ビット／秒の速度で実現する量子ネットワークを世界で初めて構築することを目指す。

https://news.arizona.edu/story/university-arizona-awarded-26m-architect-quantum-internet
https://cqn-erc.org/

NSFの量子拠点： CQN

Center for Quantum Networks（CQN）[1)]

NSF Engineering Research Centers (ERC) の１つ（代表：U. Arizona）
（2020～2025年、$26M（追加オプション 5年 $24.6））[2)]

- 量子リピーターを実現し、誤り訂正された量子接続を、100kmの距離に対して10M量子ビット／秒の速度で実現する量子ネットワークを世界で初めて構築することを目指す。
- アリゾナ大キャンパス内に敷設されたエンタングルドフォトン配信ネットワークを利用したTucson Testbedでは、マルチユーザー10M量子ビット／秒誤り耐性エンタングルメント配信を実証。
- MITとLincoln laboratoriesを42kmのファイバでつなぐBoston Testbedでは、1M量子ビット／秒でのQKD実験により、量子中継器の有用性を実証。
- アリゾナ大、ハーバード大など米国内10大学をはじめ、14企業、2つの国立研究所、7名の海外共同研究者が参画

1) https://cqn-erc.org/
2) https://news.arizona.edu/story/university-arizona-awarded-26m-architect-quantum-internet

DOE傘下の量子研究センター

（各センターに $125M（最大）/5年）

Quantum Information Science (QIS) Research Centers （2020～2025年）

- **Q-NEXT・Next Generation Quantum Science and Engineering**（アルゴンヌ国立研究所）
  - 量子暗号・通信開発を含む、量子科学技術のためのエコシステム構築。量子デバイスのためのマテリアル研究からネットワークテストベッド構築まで幅広く行う。
- **C²QA・Co-design Center for Quantum Advantage**（ブルックヘブン国立研究所）
  - 高エネルギー・核物理、化学、マテリアル科学、コンデンスドマター物理のためのコンピューテーション研究。量子優位性を持つハード、ソフト、量子誤り訂正などを開発。
- **SQMS・Superconducting Quantum Materials and Systems Center**（フェルミ国立加速器研究所）
  - 量子コンピュータ、量子センサのための優れた量子デバイス開発を目指した超伝導デバイスのデコヒーレンス機構の理解と除去の研究、および量子デバイスファウンドリー構築。
- **QSA・Quantum Systems Accelerator**（ローレンスバークレー国立研究所）
  - 科学研究応用のための、量子優位性を満たす量子デバイス、量子アルゴリズムなどの設計。量子デバイス（原子、イオン、超伝導回路）とアルゴリズムを組み合わせて最適な応用を実証。
- **QSC・The Quantum Science Center**（オークリッジ国立研究所）
  - レジリエンス、制御性、スケーラビリティのある量子デバイスを実現するための、革新的トポロジカル量子材料とアルゴリズム、センサーを発見、設計、実証することを目指す。

https://science.osti.gov/Initiatives/QIS/QIS-Centers

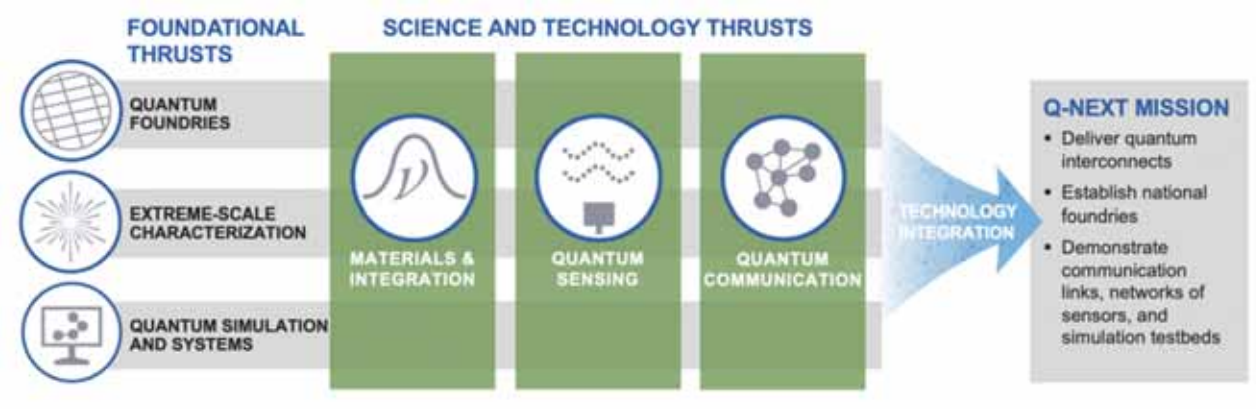
DOEの量子拠点： Q-NEXT

Next Generation Quantum Science and Engineering（Q-NEXT）[1)]

DOE Quantum Information Science (QIS) Research Centersの１つ
（代表：アルゴンヌ国立研究所）

（$115M（DOEの予定額、2020～2025年）
$ 93M（パートナ団体から）
$200M（イリノイ州から、2020年）[2)]

- 量子暗号・通信開発を含む、量子科学技術のためのエコシステム構築。量子デバイスのためのマテリアル研究から量子センシング、ネットワークテストベッド構築まで幅広く行う。Chicago Quantum Networkはこの枠組みに含まれる様子。[3)]
- ミッションは、
  - 量子材料ファウンドリ構築
  - 量子インターコネクト確立
  - 量子通信リンク、量子センサーネットワーク、量子シミュレーションテストベッドの実現



- 3つのDOE研究所、9つの大学、12の米国量子関連企業が参画。

1) https://www.q-next.org/
2) https://www.anl.gov/article/department-of-energy-selects-argonne-to-lead-national-quantum-center
3) https://news.uchicago.edu/story/argonne-uchicago-scientists-take-important-step-developing-national-quantum-internet

欧州の状況

European Quantum Communication Infrastructure（EuroQCI）initiative

- ヨーロッパ全域における量子通信インフラの構築を目指すために、2019年6月に7ヶ国の合意で発足。2021年6月にEU全加盟国（27ヶ国）の合意完了。
- 欧州域内の拠点をQKDネットワークで結ぶ大規模テストベッドPJ。
- OpenQKD projectの成果を活用。Digital Europe programme、Connecting Europe Facility、Horizon Europeなどのプログラムでサポート。
- 2027年までに、地上ネットワークおよび衛星を使った完全に安全な通信ネットワークの構築を目指す。
- まずはQKD。将来的には量子インターネットのバックボーン想定
- アプリは金融、安全保障、医療情報など。

https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

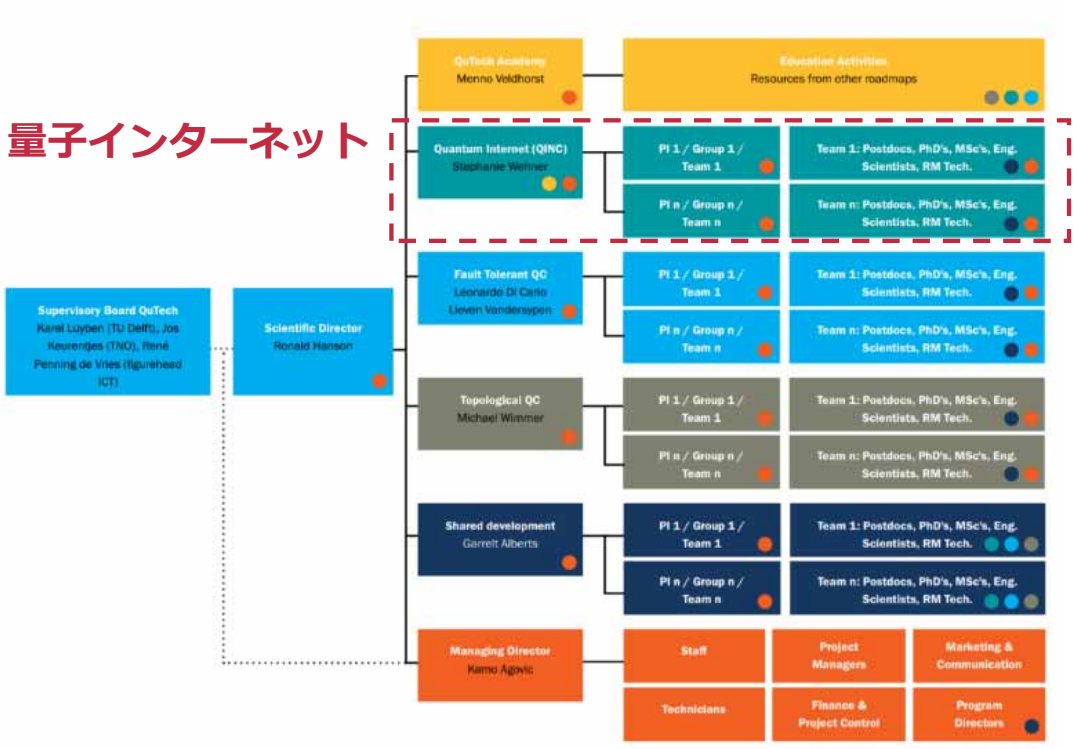
欧州「Quantum Flagship」

Basic Science					**€ 20,090,951.25**
	2D-SIPC	Dmitri Efetov	ICFO, Spain	二次元光集積回路量子デバイス	2,976,812.50
	MicroQC	Nikolay Vitanov	Foundation for Theoretical and Computational Physics and Astrophysics, Bulgaria	イオントラップ量子コンピュータ	2,363,343.75
	PhoG	Natalia Korolkova	The University Court of the University of St Andrews, United Kingdom	単一光子源	2,761,866.25
	PhoQuS	Alberto Bramati	Sorbonne Universite, France	光量子シミュレータ	2,999,757.50
	QMiCS	Frank Deppe	Bayerische Akademie der Wissenschaften, Germany	量子通信プロトコル	2,999,595.00
	S2QUIP	Klaus Jöns	Kungliga Tekniska Hoegskolan, Sweden	二次元光集積回路量子デバイス	2,999,298.75
	SQUARE	David Hunger	Karlsruher Institut fuer Technologie, Germany	希土類イオン量子ビット	2,990,277.50
Quantum Communication					**€ 33,547,307.25**
	CiViQ	Valerio Pruneri	ICFO, Spain	物理レイヤ量子暗号通信	9,974,006.25
	QIA	Stephanie Wehner	Technische Universiteit Delft, Netherlands	量子インターネット	10,406,113.50
	QRANGE	Hugo Zbinden	Universite de Geneve, Switzerland	量子乱数ジェネレータ	3,187,282.50
	UNIQORN	Hannes Hübel	AIT Austrian Institute of Technology GmbH, Austria	光集積回路量子デバイス	9,979,905.00
Quantum Computing					**€ 19,924,645.00**
	AQTION	Thomas Monz	Universität Innsbruck, Austria	イオントラップ量子コンピュータ	9,587,252.50
	OpenSuperQ	Frank Wilhelm-Mauch	Universität des Saarlandes, Germany	超伝導量子コンピュータ	10,334,392.50
Quantum Simulation					**€ 18,593,150.00**
	PASQuanS	Immanuel Bloch	Max-Planck-Gesellschaft zur Forderung der Wissenschaften eV, Germany	プログラマブル冷却原子量子シミュレータ	9,257,515.00
	Qombs	Augusto Smerzi	Consiglio Nazionale delle Ricerche, Italy	量子カスケードレーザー周波数コム	9,335,635.00
Quantum Sensing & Metrology					**€ 36,718,102.50**
	ASTERIQS	Thierry Debuisschert	Thales SA, France	ダイヤモンドNVセンサ	9,747,888.75
	iqClock	Florian Schreck	Universiteit van Amsterdam, Netherlands	光格子時計	10,092,468.75
	macQsimal	Jacques Haesler	Swiss Center for Electronics and Microtechnology (CSEM), Switzerland	小型ガスセルセンサ	10,209,943.75
	MetaboliQs	Christoph Nebel	Fraunhofer Gesellschaft zur Foerderung der Angewandten Forschung eV, Germany	室温超偏極センサ	6,667,801.25
CSA (Coordination and support action)					**€ 3,478,996.25**
	QFlag	Markus Wilkens	VDI Technologiezentrum GmbH, Germany	コーディネーション・アウトリーチ	3,478,996.25
					€ 132,350,152.25

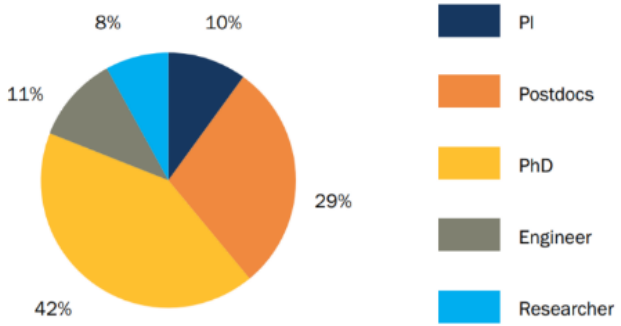
https://ec.europa.eu/digital-single-market/en/projects-quantum-technology

オランダQuTech

- 組織は主３テーマ＋教育チーム、共通基盤、管理の６部門
- 約180名がQuTechに勤務（2017年12月時点）。次の１年で340名程まで増える予定。
- 研究者の10%はPI（全体でのFacultyは30名ほど）、ポスドク、博士課程学生が70%
- オフィス約1500m^2、低温実験室約1500m^2、光学実験室約500m^2
- 2015年から10年間の予算総額は145.53 Mユーロの予定。



研究者の内訳



予算（2015年から10年間）

TU Delft in-kind	29	M€
TU Delft in-cash	20	M€
TNO in-cash*	50.75	M€
NWO/FOM*	36.18	M€
STW in-cash	9.6	M€
Total	**145.53**	**M€**

QuTech Annual Report 2017
https://qutech.nl/wp-content/uploads/2017/06/180507_qutech_jaarplan_2017_v7_online.pdf

EU QIA プロジェクト

Quantum Internet Alliance（QIA）[1)、2)]

Horizon 2020のPJ（代表： オランダ デルフト工科大）（2018～2022年、計 €10M）

- 全欧州にわたる量子インターネットの青写真を描くことを目標に、多ノード量子ネットワーク上で動作する完全に統合されたスタックを実現するプロジェクト。
- エンドノード（トラップ型イオンキュービット、ダイヤモンドNVキュービット、中性原子キュービット）と量子リピーター（希土類ベースのメモリ、原子ガス、量子ドット）の技術開発を行い、双方の統合を行う。それによって3～4の量子ネットワークノード間のエンタングルメントとテレポーテーションを実証し、マルチノードネットワークを実現。
- さらに、メモリベースの量子中継器を実現し、世界最長の中継器リンクを含む、長距離中継器リンクの原理実証を行う。
- 23のパートナー（大学、研究機関、企業）が参画。

1) https://quantum-internet.team/
2) https://cordis.europa.eu/project/id/820445

EU OpenQKD プロジェクト

Open European Quantum Key Distribution Testbed （OpenQKD） 1)、2)

Horizon 2020のPJ（代表： オーストリア AIT）　（2019～2022年、計 €18M）

- 欧州の量子通信技術のグローバルな地位の強化を目指し、EU全域にまたがる量子セキュリティ技術を統合することを目的とするプロジェクト。
- 具体的なターゲット
  - QKD対応実験プラットフォームの確立
  - インターフェース標準化
  - ユースケースの実証

  など
- EU域内13か国 38のパートナー（東芝など16の企業、22の研究機関）が参画。

1) https://openqkd.eu/
2) https://cordis.europa.eu/project/id/857156

ドイツ政府の動向（2021年～）

独連邦当局間の最初の量子通信リンクに成功（2021年8月）

- 教育研究省（BMBF）と連邦情報セキュリティ局（BSI）間で、QKDをベースにしたセキュアなビデオ会議を試験的に実施。
- 教育研究省（BMBF）が進めるQuNETイニシアチブの成果。QuNETイニシアチブの4つの中核機関は、フラウンホーファー応用光学・精密力学研究所（IOF, Jena）、フラウンホーファー ハインリッヒーヘルツ研究所（HHI, Berlin）、ドイツ航空宇宙センター通信・ナビゲーション研究所（DLR-IKN, Oberpfaffenhofen）、マックスプランク光科学研究所（MPL, Erlangen）

https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/2021/08/100821-Quantenkommunikation.html
https://www.qunet-initiative.de/

「未来パッケージ」で量子技術での主権確保を目指す（2021年1月）

- 連邦教育研究省（BMBF）発表。ポストコロナ対策「未来パッケージ」の最初の1.2億ユーロで、量子通信と量子コンピュータハードの主要技術の開発プロジェクトに注力。経済界と科学界の準備と活性化、ネットワーク化のために必要とされる体制構築を急ぐ。
- BMBFイニシアチブであるQuNET（量子通信）、2020年初頭に開始した量子コンピューティング戦略的イニシアティブをさらに加速する。

https://www.bmbf.de/de/karliczek-mit-quantentechnologien-zu-mehr-technologischer-souveraenitaet-13489.html

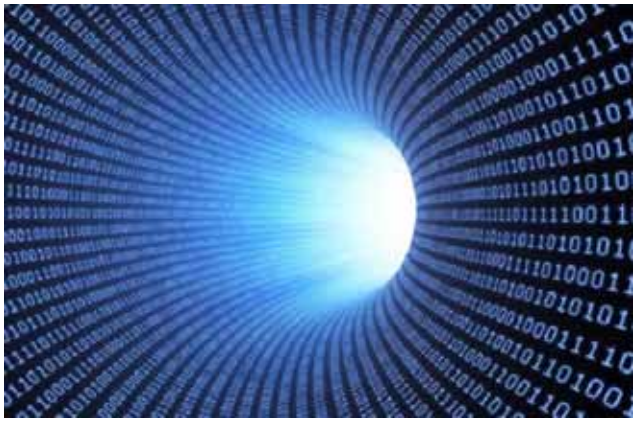
フランス政府の動向

国家量子戦略公表（2021年1月）

- 高等教育・研究・イノベーション省（MESRI）発表。
- 投資額 2,300億円（18億ユーロ）/ 5年以上
- マクロン大統領がフランスの量子戦略（Stratégie nationale sur les technologies quantiques）を発表
- 目的：産業のバリューチェーンを強化しながら、人材育成、科学研究、技術実験を大幅に強化すること。
- 目標：最終的にフランスの輸出の1～2%を占めること

量子戦略の7本の柱

- NISQシミュレータ・アクセラレータ（3億5200万ユーロ）
- LSQスケールに移行する量子コンピュータ（大規模誤り耐性量子コンピューター）（4億3200万ユーロ）
- 量子センサー技術・応用（2億5800万ユーロ）
- 耐量子計算機暗号（1億5600万ユーロ）
- **量子通信システム（3億2500万ユーロ）**
- 競争力のある実現技術（2億9,200万ユーロ）
- エコシステム構築



https://www.enseignementsup-recherche.gouv.fr/cid156616/strategie-nationale-sur-les-technologies-quantiques.html

3. 国内外ベンダーの動向

量子暗号通信　国内企業の動向

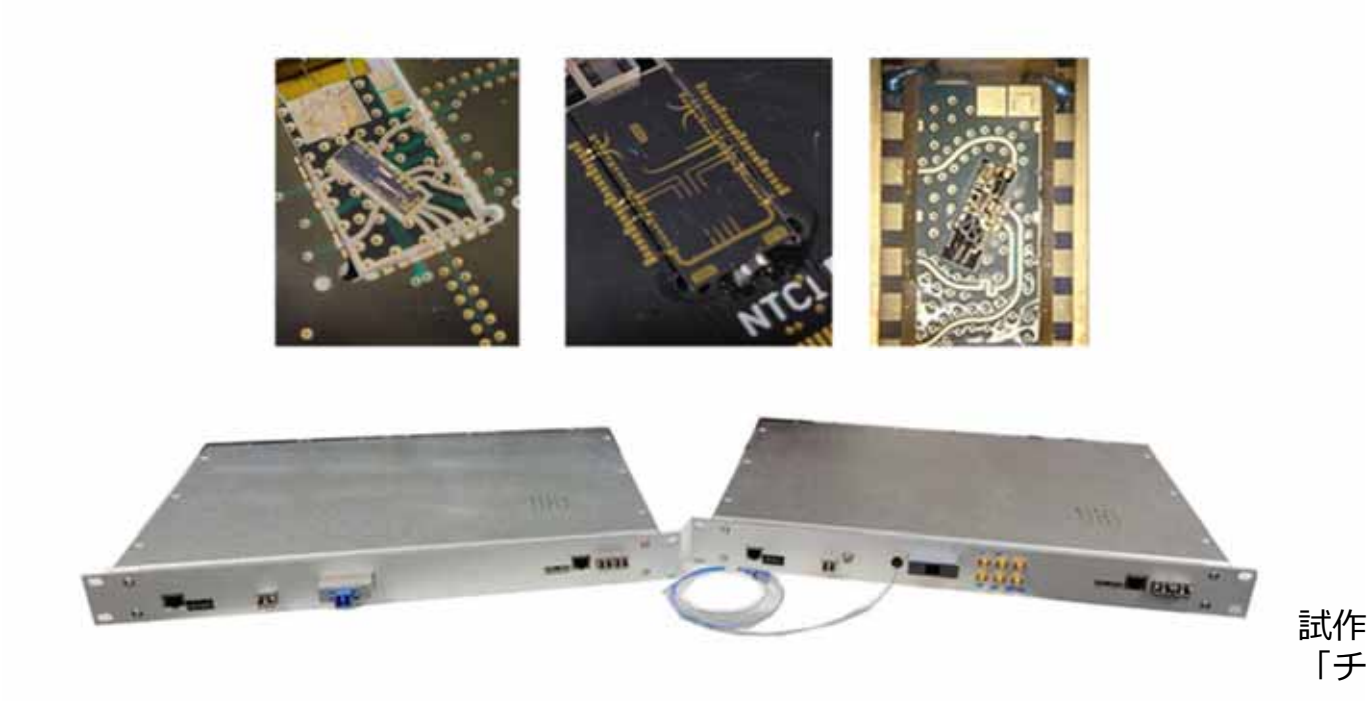
	概要
東芝	東芝欧州研究所傘下のケンブリッジ研究所で基礎技術開発し、実用化に向けた体制を日本に構築。2017年に、距離10kmで10Mbpsを超える鍵配信速度を達成（世界最速）。最長240kmの光ファイバーリンクを用いた鍵配送実用性の実証や、ゲノム解析データの暗号化通信の実証など、実用化に向けた実証実験を積極的に進める。2020年度より量子暗号システム提供開始。
	東芝独自開発の新しいプロトコル Twin-Field QKD を発明。2021年に600kmを超える暗号鍵共有を実証。実用化に向けた研究開発が進む。
NEC	NICTとの共同で、量子暗号（QKD）を用いて、顔認証システムでの特徴データの伝送と、特徴点などの認証用参照データの保存を高秘匿で実行できるシステムを構築。NICTの量子暗号研究開発用ネットワーク上に同システムを構築し、2019年から、日本代表選手が所属する様々なスポーツ分野のナショナルチームのデータサーバ管理のための試験利用を開始。
三菱電機	同種写像暗号などの耐量子計算機暗号の研究開発を長年行っている。
NTT	阪大、富山大との共同で、2019年に「全光」での量子中継の原理検証実験に成功。全光量子ネットワークの実現に向けた第一歩。
日立情報通信エンジニアリング	玉川大学、ソフトバンクテレコムとの共同で、量子揺らぎを利用したY-00方式を長年開発している。2017年にAPRESIA Systems(株)が、日立のY-00技術を活用して情報保護ソリューション分野に参入することを発表。
東芝・NEC・三菱電機・古河電気・浜ホト	東大・北大・横国大・学習院大・NICT・AIST・NIMSとの共同で、総務省委託事業「情報通信技術の研究開発に係る提案の公募－グローバル量子暗号通信網構築のための研究開発－」を受諾（上限14.4億円@令和2年）
NEC・東芝	NICTとの共同で開発してきた量子鍵配送ネットワーク技術の成果を盛り込んだ国際標準勧告が、国際標準化機関ITU-Tで承認（2019年）。

公開情報を基にJST-CRDSで作成

国内の最近の動き（2021年～）

東芝、量子暗号通信機能を数ミリ角にチップ化（2021年10月発表）

- チップベースの量子暗号通信システムを開発。量子送信チップ（2x6 mm）、量子受信チップ（8x8 mm）、量子乱数発生チップ（2x6 mm）を開発し、これらを実装した世界初の「チップベース量子暗号通信システム」の実証に成功。
- 2024年の実用化に向けて、研究開発を進める。



試作した光集積回路と
「チップベース量子暗号通信システム」

東芝プレスリリース「世界で初めて光集積回路化により小型化した量子暗号通信システムの開発・実証に成功　－プラントや工場間の機密データ通信への適用を目指す－」より
https://www.global.toshiba/jp/technology/corporate/rdc/rd/topics/21/2110-01.html

中国の量子通信関連企業

Quantum CTek Group (国盾量子) http://www.quantum-info.com/English/

- 政府、金融、エネルギー業界などでサービスイン（のべ6000 km 以上の通信）。
- 中国内の量子技術をリードする立場。ITU等の国際会議のメンバー。

Zhejiang Quantum Technologies Co. Ltd（QTEC) (九州量子) http://www.qtec.cn/

- 量子通信の専門企業。清華大学などと連携し、量子ネットワークに関する教育・訓練を行う共同ラボを設立。
- 量子乱数生成器やQKDの開発・サービス提供でIDQ（スイス）と協力

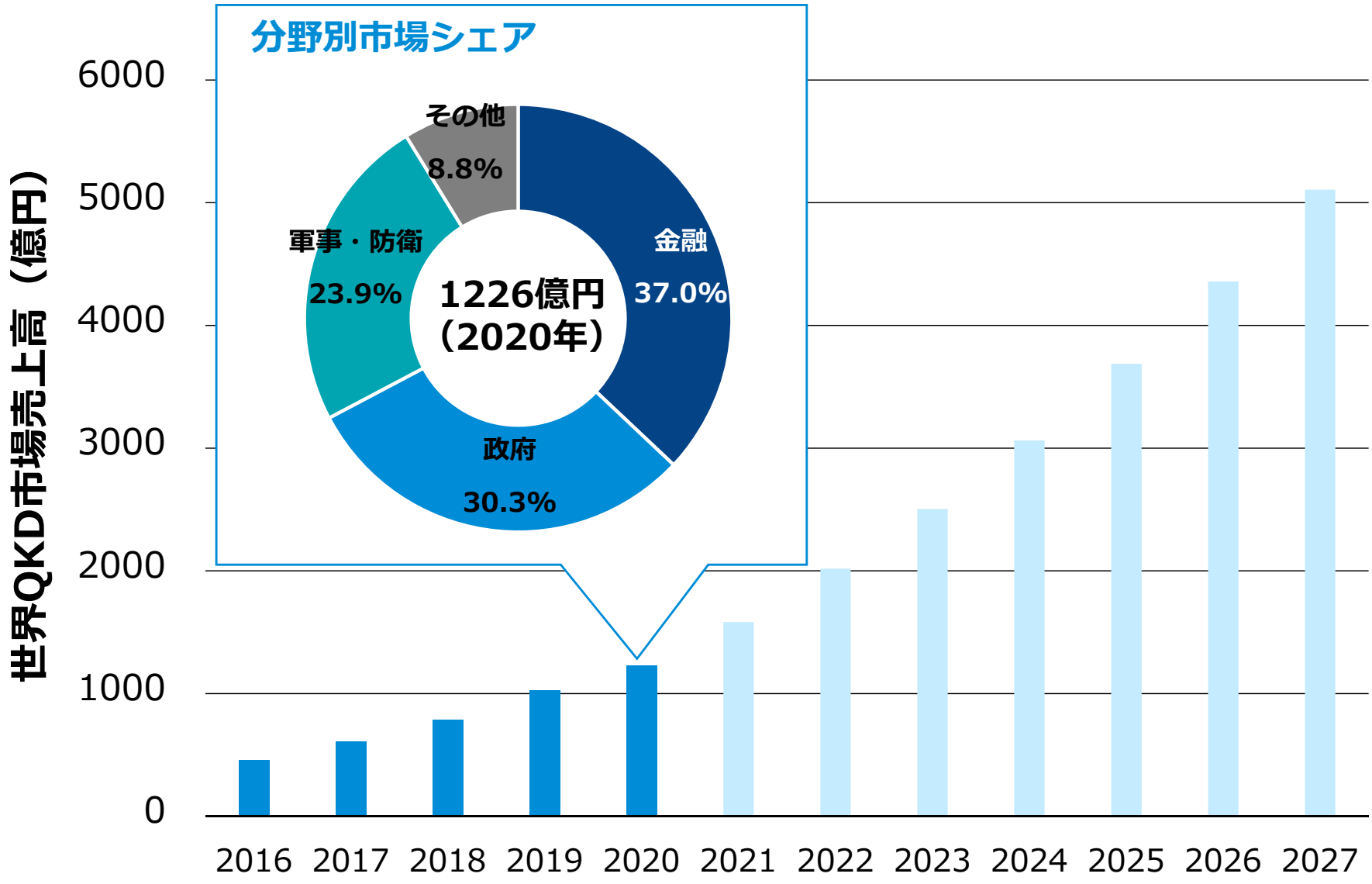
Anhui Qasky Quantum Technology Co., Ltd.(安徽問天量子)

http://www.qasky.com/en/

- 中国科学技術大学と投資会社が共同で2009年に設立。政府の国家暗号管理局認定の商用暗号製品の指定生産者・ライセンス販売者。
- 子会社として合肥 Liangxin Technology Co.、Ltd.を設立。 国内特許多数。量子情報セキュリティシステムのトータルソリューションを提供。

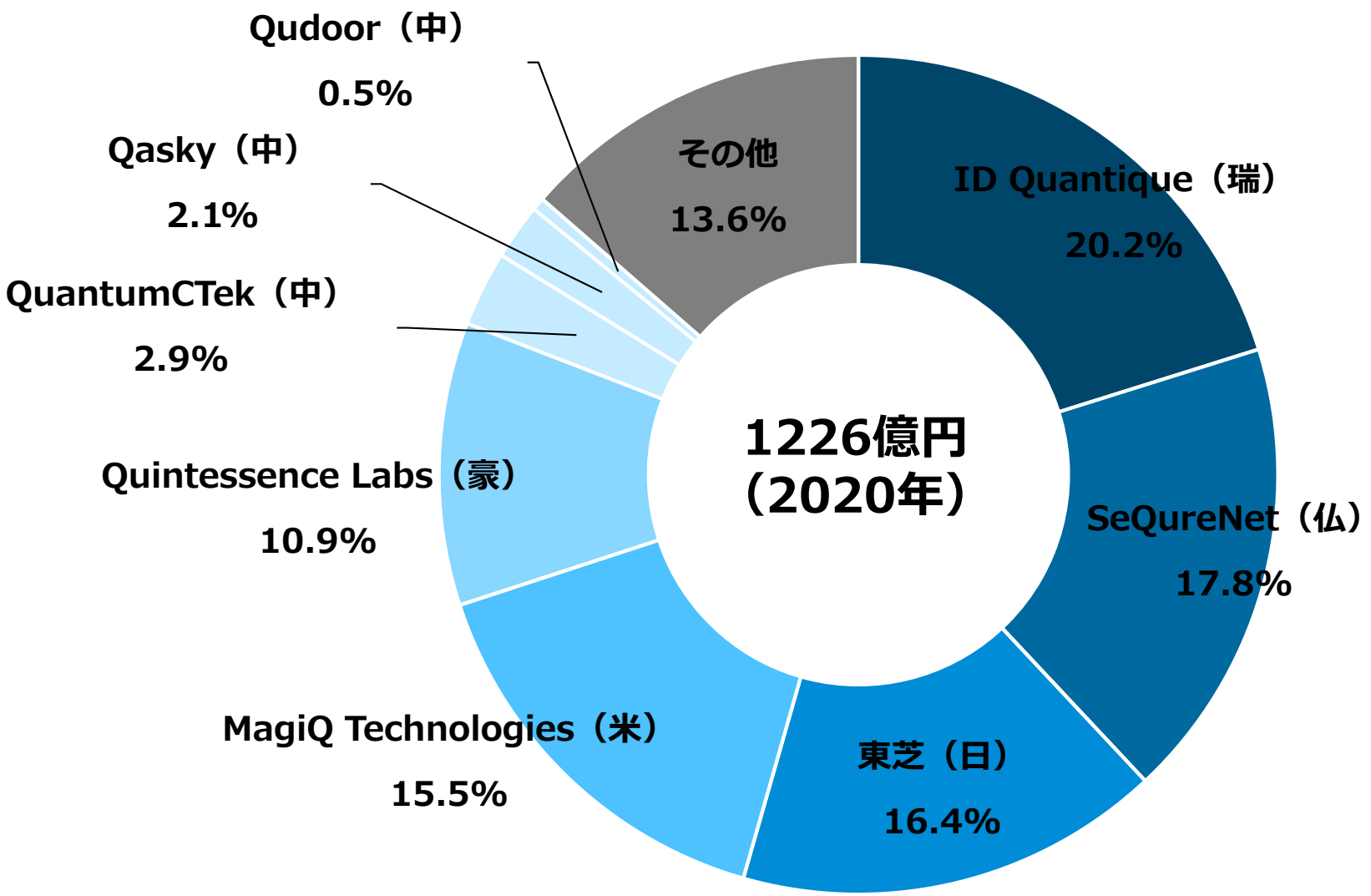
4. 量子通信市場予測

QKD市場の予測



QYResearch, “Global Quantum Key Distribution (QKD) Market Size, Status and Forecast 2021-2027” (2021).

QKD市場シェア（2020）



QYResearch, “Global Quantum Key Distribution (QKD) Market Size, Status and Forecast 2021-2027” (2021).