資料2-4

量子セキュリティ拠点の概要紹介

2023年9月21日（木曜）

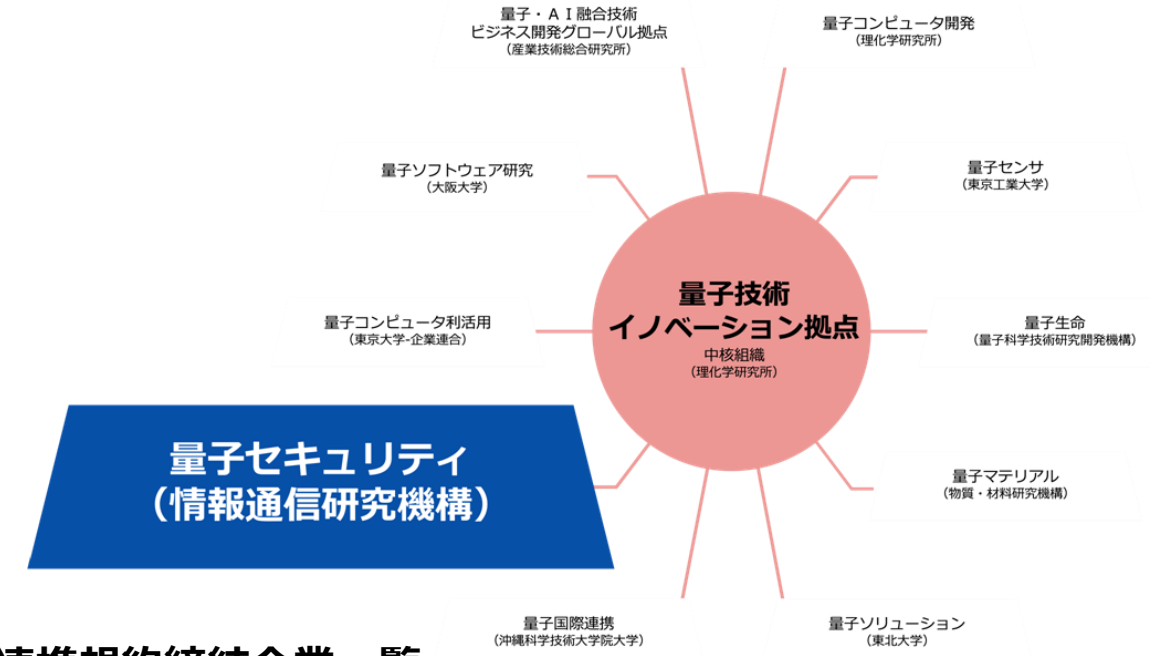
国立研究開発法人情報通信研究機構
量子ICT協創センター
研究センター長
藤原　幹生

量子セキュリティ拠点

- **量子技術イノベーション戦略（2020年１月）に基づき，NICTは量子セキュリティ拠点に指定されたところ，取組みの中核となる量子セキュリティ協創棟が2022年３月に竣工**
- **現時点で11企業と連携規約を締結し、量子セキュリティ技術に関する研究開発等を実施中**

量子セキュリティ・協創棟（小金井）

https://www2.nict.go.jp/qictcc/
にてオープンテストベッド利用方法について紹介



連携規約締結企業一覧

- KDDI株式会社
- さくらインターネット株式会社
- スカパーJSAT株式会社
- 株式会社大和証券グループ本社
- 株式会社東芝
- 凸版印刷株式会社
- 日本電気株式会社
- 野村ホールディングス株式会社
- 株式会社マクニカ
- 株式会社みずほフィナンシャルグループ
- 株式会社ワイ・デー・ケー

このほかにも連携に関する打診をいただいているところ

量子セキュリティ拠点における取組

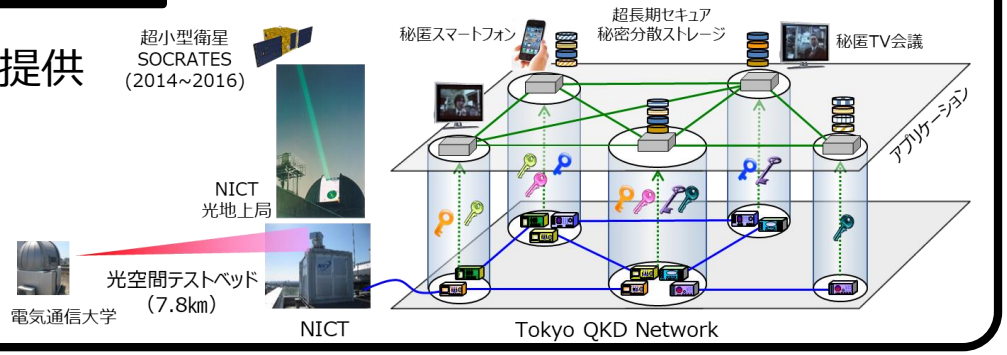
- **量子ICT協創センターを中核として，研究開発，オープンテストベッド構築，社会展開，人材育成等の取組を総合的に推進**

①研究開発

量子セキュリティ	量子暗号、現代暗号、ネットワーク技術、情報理論等との融合
衛星量子通信	量子技術の衛星搭載化
量子ネットワーク	地上網・衛星網の統合、グローバルネットワーク化
量子インターネット	量子もつれ中継、量子計測標準

②オープンテストベッド

- 産学官協創環境の提供
- 成果の実装、試験、企業への技術移転



③社会展開

- 標準化
- 知財
- 評価・認証制度
- 国際連携

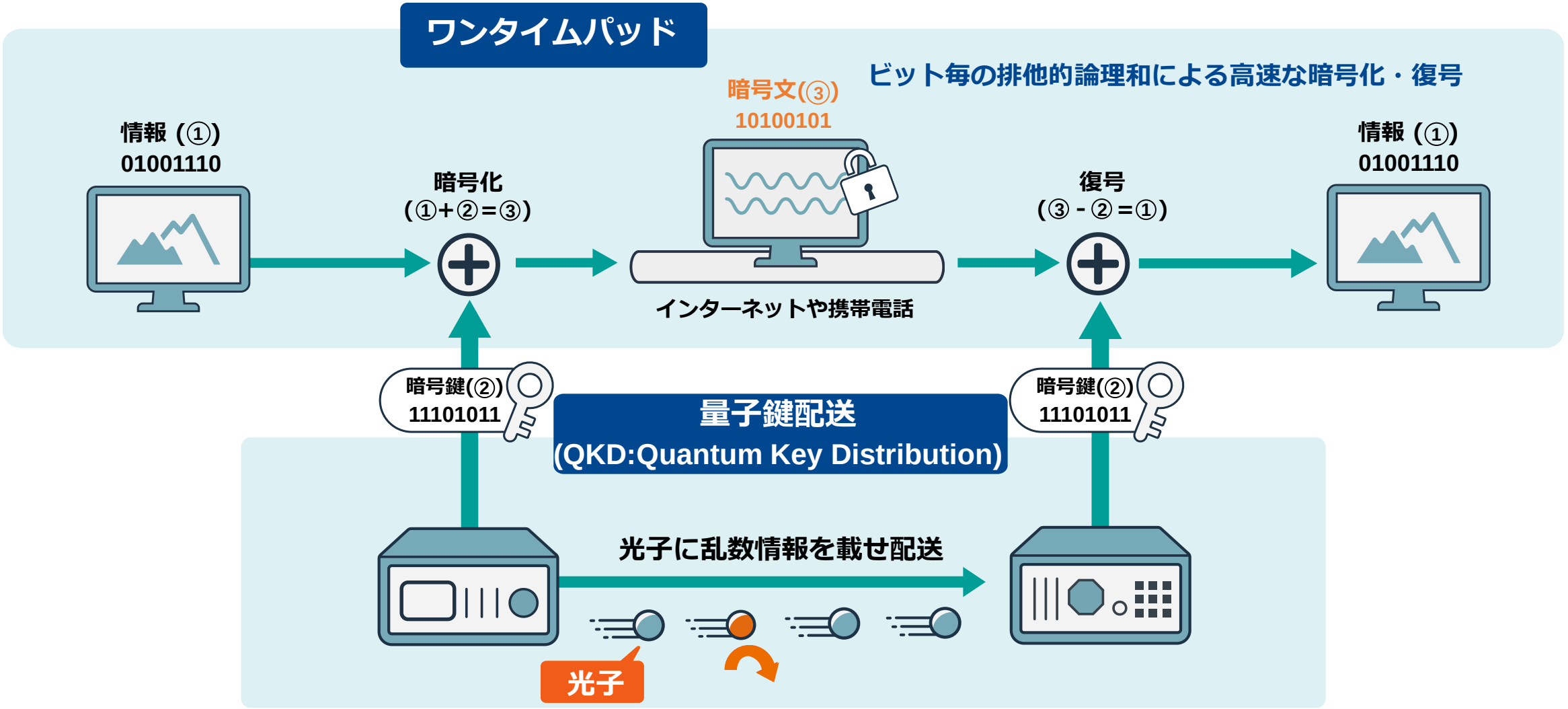
④人材育成

- NICT Quantum Camp
- 若手チャレンジラボ

・産学官連携による実践的なプログラム
・総合力のある量子ネイティブの育成

(※) **・総務省直轄委託研究　グローバル量子暗号通信網構築のための研究開発（R2-R6）**
・総務省直轄委託研究　グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発（R3-R7）
・総務省直轄委託研究　量子インターネット実現に向けた要素技術の研究開発（R5-R9）

（参考）量子鍵配送・量子暗号とは



将来の如何なる計算機による
盗聴脅威から解放

どのような盗聴でも確実に検知し
安全に鍵配送

（参考）量子セキュアクラウドとは

量子・古典ハイブリッドによる総合アーキテクチャ

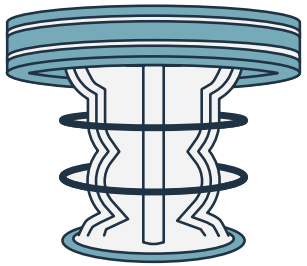
量子 ＋ **古典**

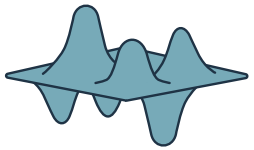
（量子鍵配送）　（秘密分散）

量子セキュアクラウド

optimization

Quantum computer/AI/ supercomputer





$$\frac{dx_i}{dt} = \frac{\partial H}{\partial y_i} = D y_i$$

$$\frac{dy_i}{dt} = -\frac{\partial H}{\partial x_i}$$

$$= -\left(D - p + x_i^2\right) x_i - c\alpha h_i + c\sum_{j=1}^{N} J_{i,j} x_j$$

QKD/OTP

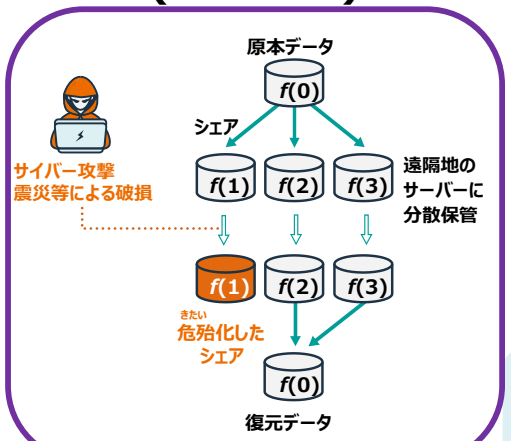
shere1　shere2

QKD network

shere3　shere4

Secret sharing

（秘密分散）



Secret data

QKD/OTP

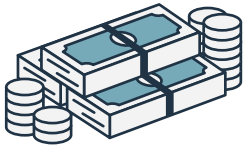
Analytical results

（量子鍵配送）

長期高秘匿を必要とするデータの安全な伝送・保管・二次利用

Users

Finance



Factory

Distribution

Control

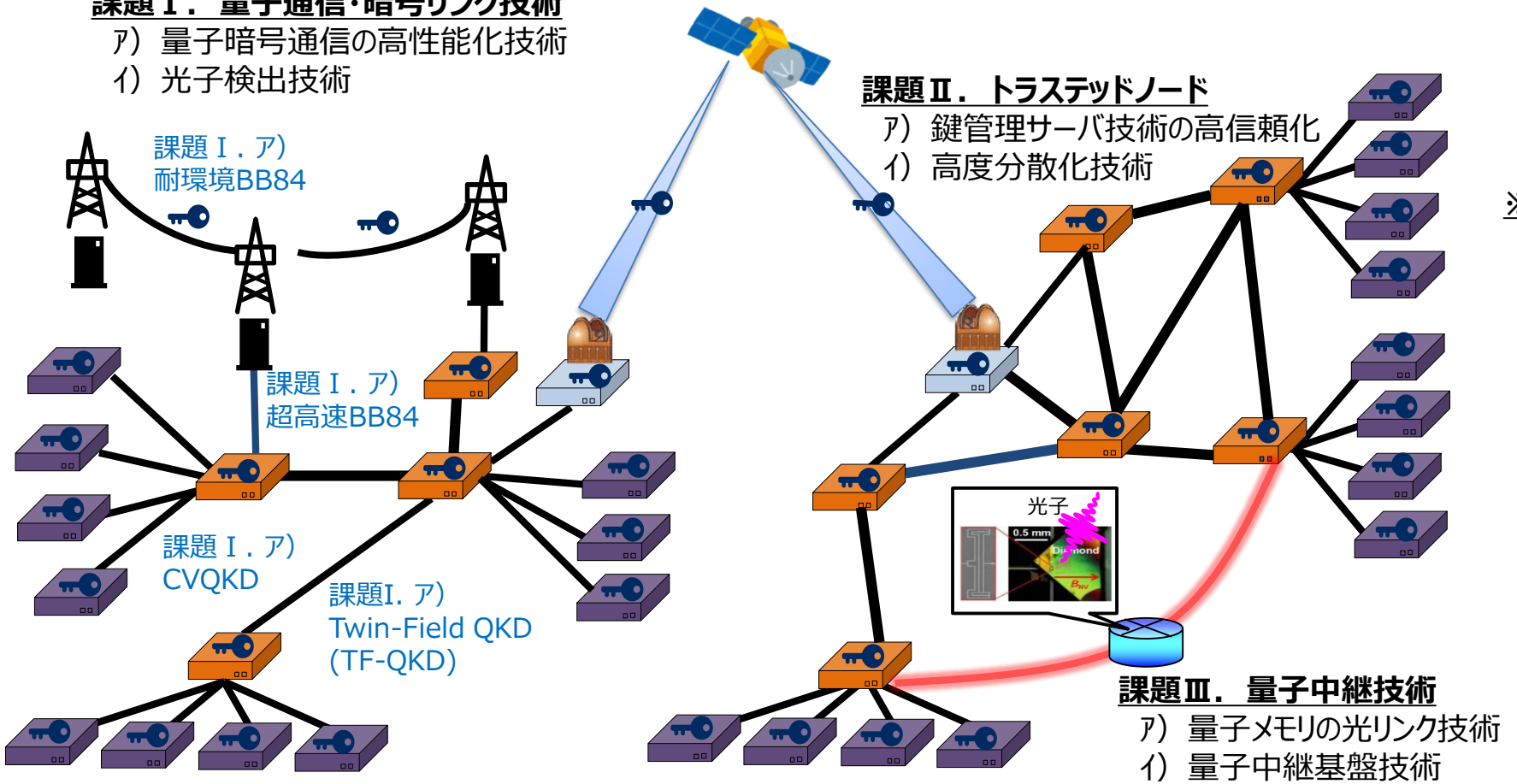
Drug develop

Chemical

研究開発：グローバル量子暗号通信網構築のための研究開発

- 「グローバル量子暗号通信網構築のための研究開発」を，産学官の12機関※で推進NICTは４課題の全てに参画

課題Ⅰ．量子通信・暗号リンク技術
ｱ）量子暗号通信の高性能化技術
ｲ）光子検出技術



課題Ⅲ．量子中継技術
ｱ）量子メモリの光リンク技術
ｲ）量子中継基盤技術

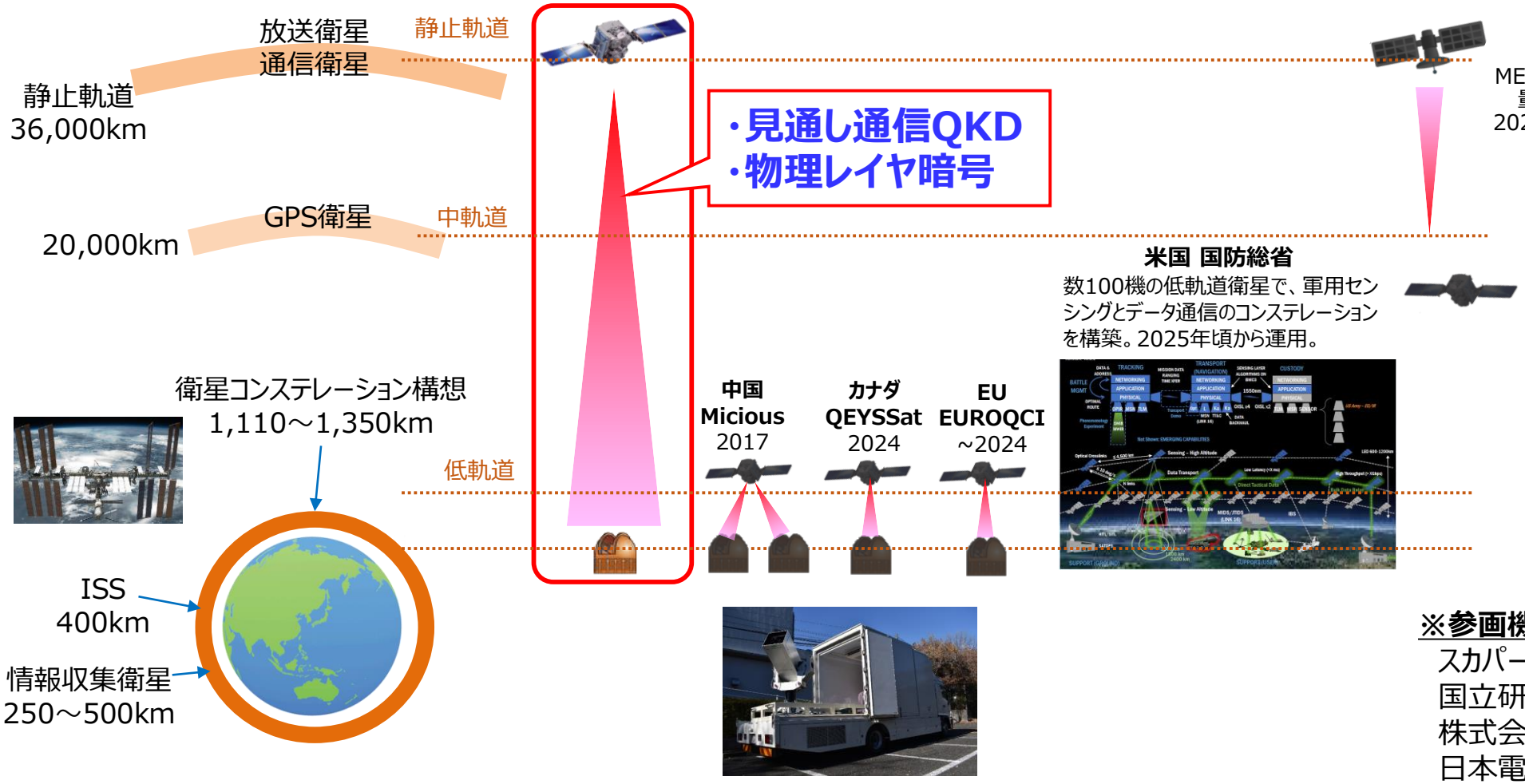
※参画機関一覧
株式会社東芝
日本電気株式会社
学習院大学
国立研究開発法人情報通信研究機構
国立大学法人北海道大学
国立大学法人 東京大学
浜松ホトニクス株式会社
三菱電機株式会社
国立大学法人 横浜国立大学
国立研究開発法人産業技術総合研究所
国立研究開発法人物質・材料研究機構
古河電気工業株式会社

課題Ⅳ．広域ネットワーク構築・運用技術
ｱ）ネットワーク制御管理技術

（提案概要資料より）

研究開発：グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発

- **中国が衛星量子暗号で先行(低軌道)．2026年頃、中軌道･静止軌道間で実証を計画.**
- **カナダ，英国がそれぞれ2022年頃から宇宙実証を計画（低軌道）.**
- **日本：地上局から静止軌道までカバーできる革新的な衛星量子暗号技術を開発**

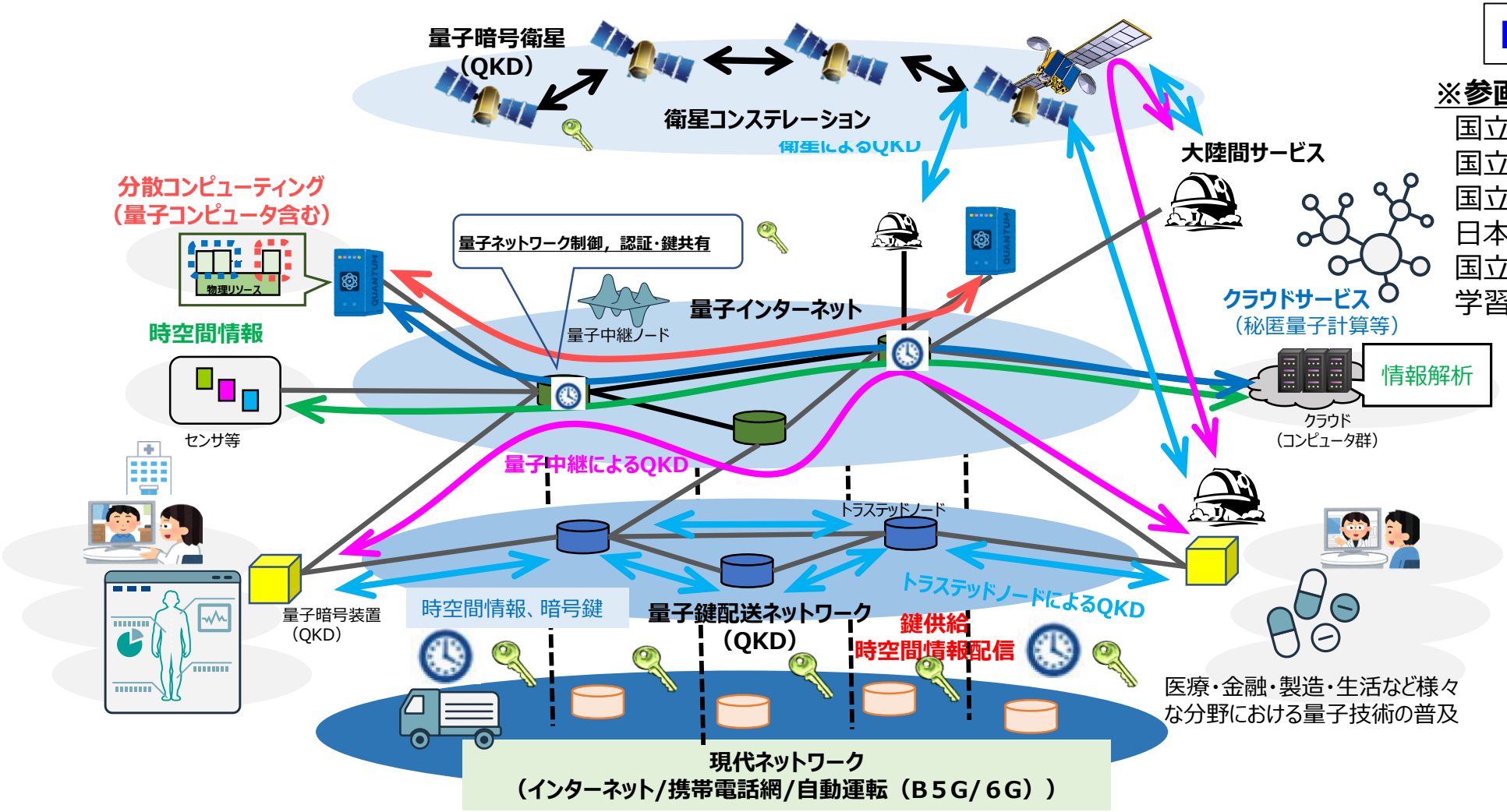


※参画機関一覧

スカパーJSAT株式会社
国立研究開発法人情報通信研究機構
株式会社東芝
日本電気株式会社

研究開発：量子インターネット実現に向けた要素技術の研究開発

- **量子状態（量子ビット）の流通及び量子通信ならではの機能・精度を可能とする「量子インターネット」の実現を目指す**



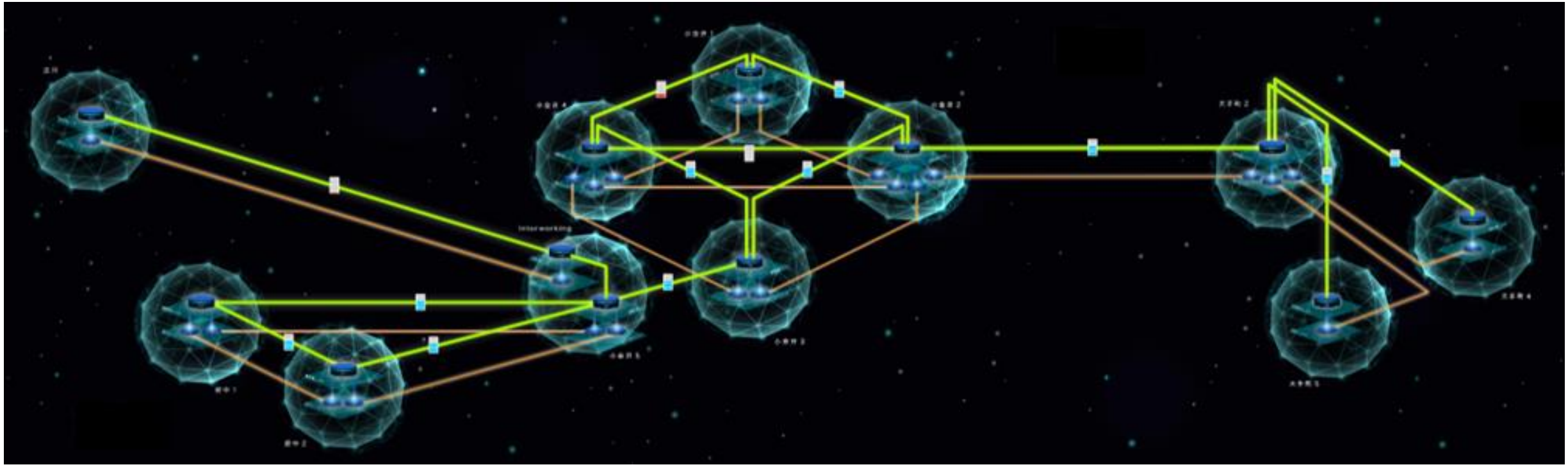
NICTが代表研究機関

※参画機関一覧

国立研究開発法人情報通信研究機構
国立大学法人　横浜国立大学
国立大学法人　大阪大学
日本電信電話株式会社
国立大学法人　東北大学
学習院大学

オープンテストベッド：Tokyo QKD Network

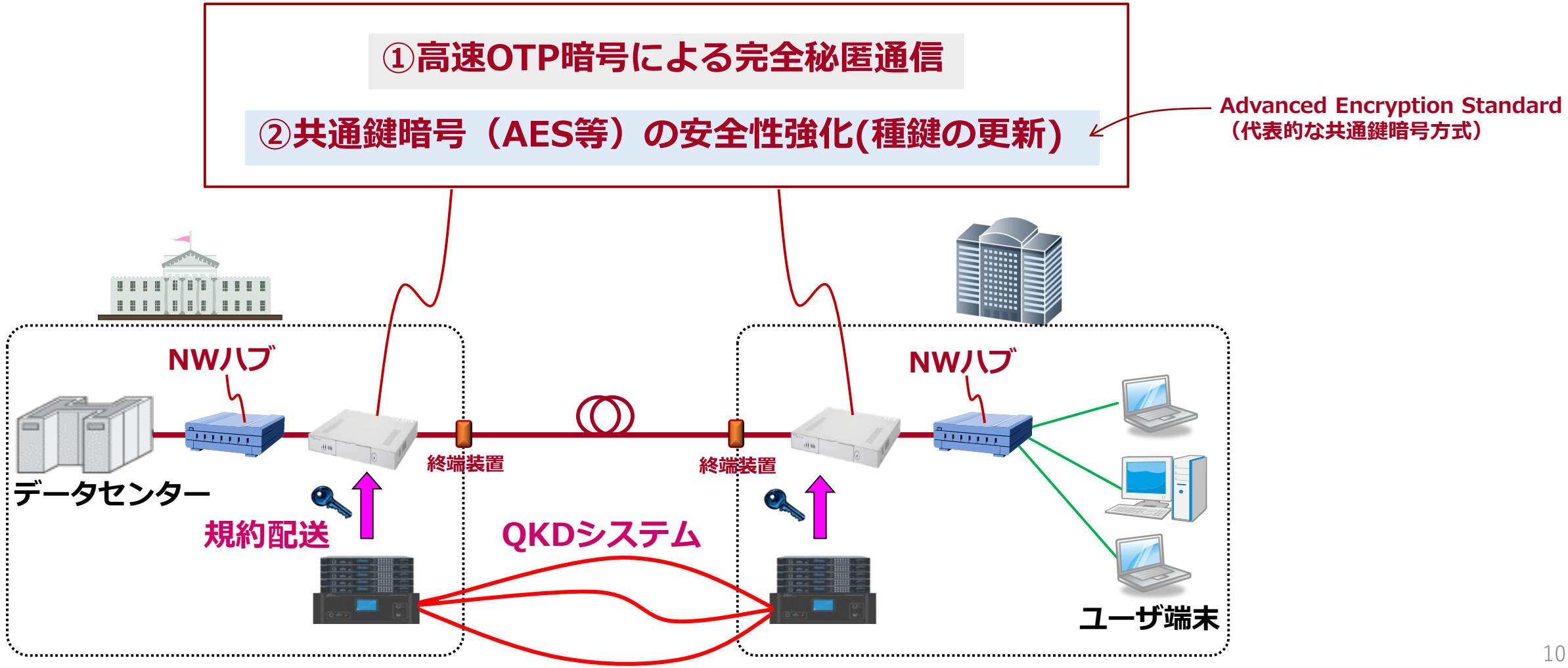
- NICT小金井本部を中核に，2010年より運用している世界で最も運用実績の長いQKDに関するオープンテストベッド
- Tokyo QKD Networkを活用し，QKD装置の運用や技術面での検証を実施をするとともに，本テストベッドでの運用実績を基にQKDプロトコルの標準化を主導



Tokyo QKD Networkのネットワーク構成のイメージ図

オープンテストベッドの活用例1

- QKD装置を用いてテストベッドに参加するユーザー企業とともに，秘匿通信の安全性を検証（ファイル転送，メール，TV会議等のアプリケーションを想定）

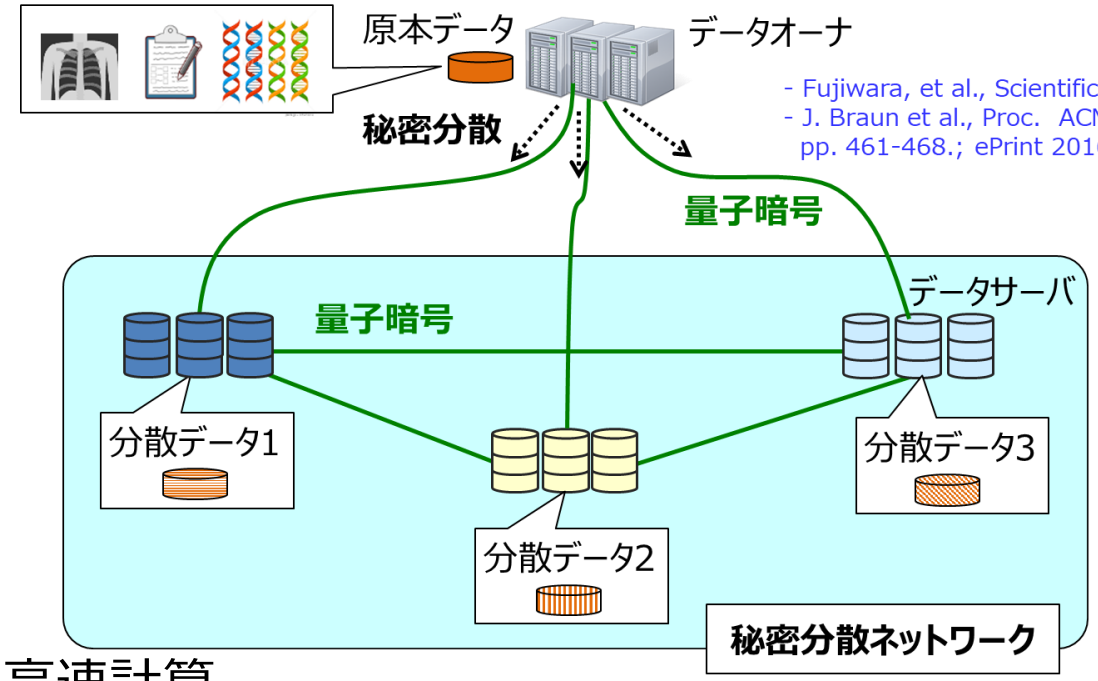


オープンテストベッドの活用例２

- **量子暗号通信と秘密分散の組合せにより，複数の拠点に安全なデータの保管分散を実現する量子セキュアクラウドの検証**

・量子セキュアクラウド（秘匿性＋可用性）

→　３つのシェア（乱数データにしか見えない状態）に分散，データ復元時には２つのシェアを集めて計算（排他的論理和）し復元.



- Fujiwara, et al., Scientific Reports, 6:28988 (2016).
- J. Braun et al., Proc. ACM Asia CCS2017, pp. 461-468.; ePrint 2016/742

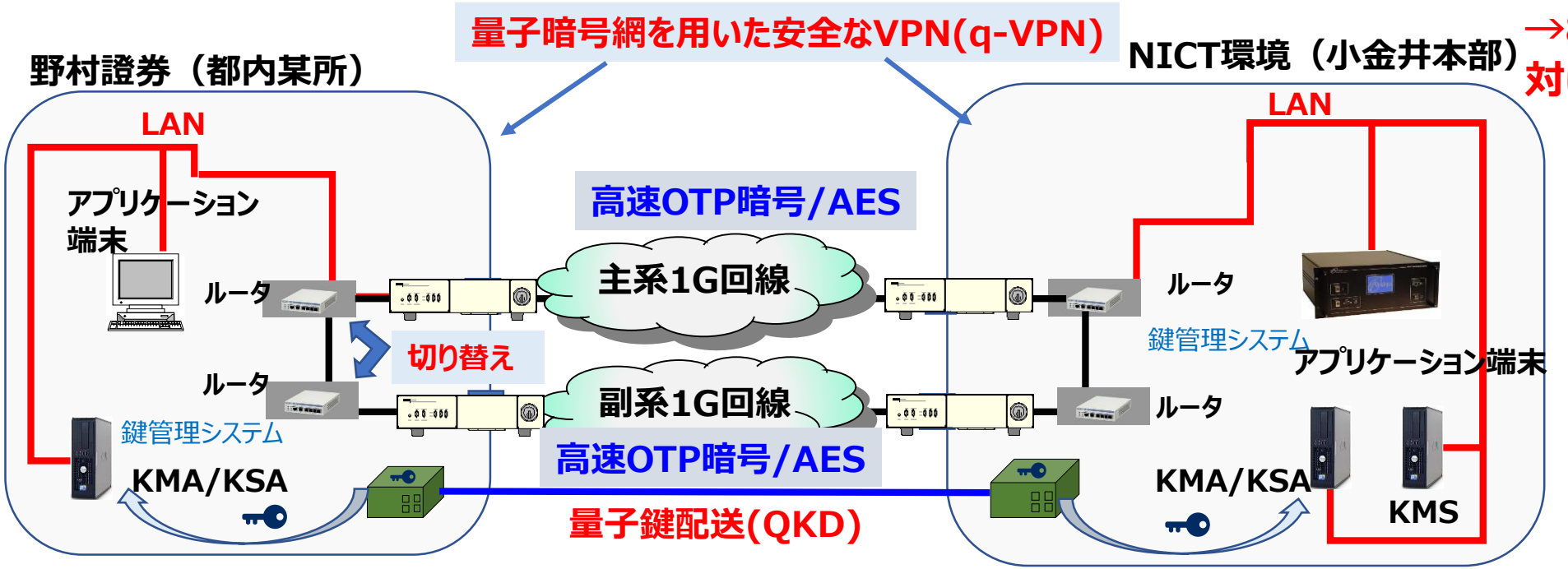
・安全なクラウド高速計算

→遠隔地に設置された高性能計算機（疑似量子アニーラーを導入予定）によるクラウド高速計算を安全なネットワーク（国内サーバー＋量子暗号通信）環境で実施可能.

オープンテストベッドの実際の実証事例

- **内閣府戦略的イノベーション創造プログラムSIP第２期において，産学官の７機関※で量子セキュアクラウド技術を開発し，証券会社との共同実証を実施**

金融分野では専用線を用いるケースが多く，量子暗号との親和性が高い



✓ **野村證券 野村HDと共同実証**

→80倍のボリュームのデータに対し，40msの付加的遅延

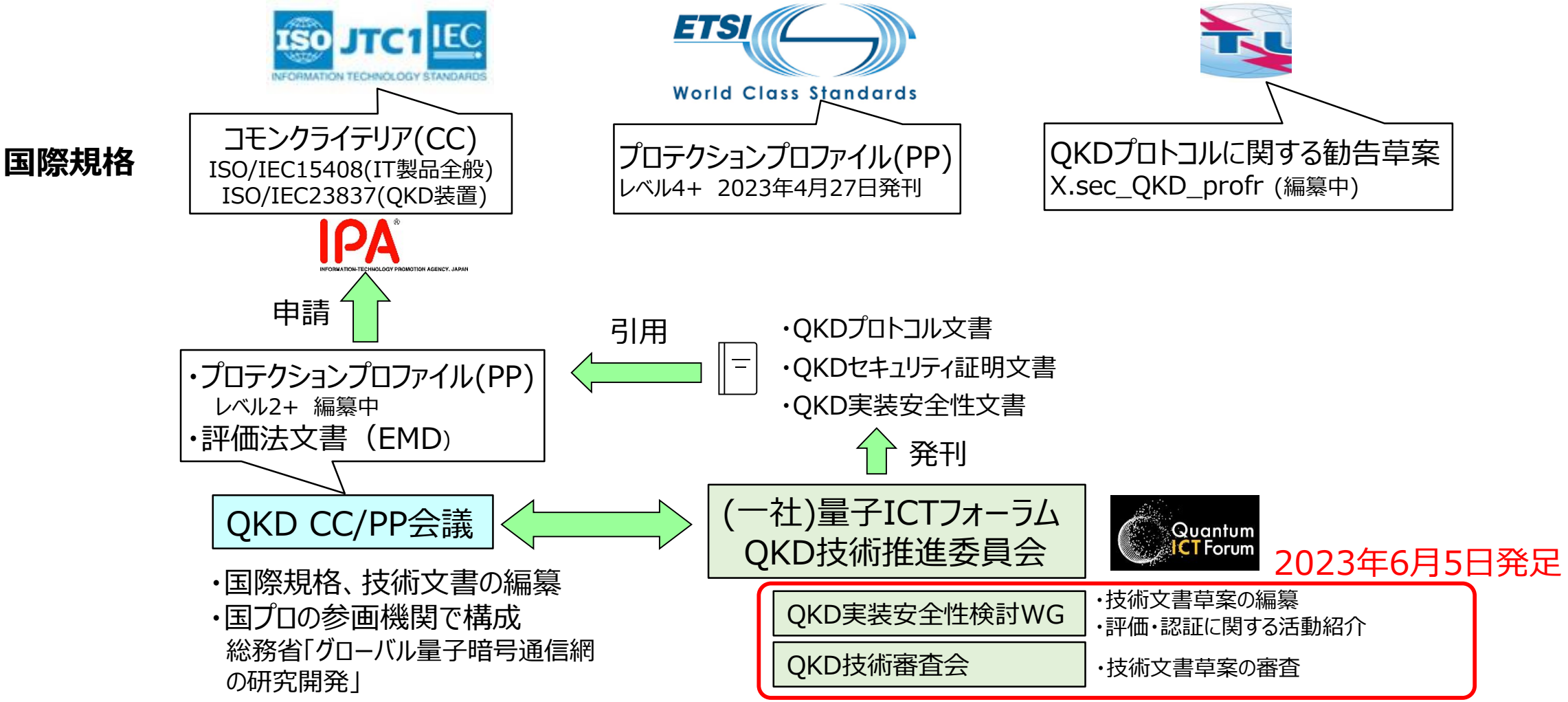
・技術的な評価に成功
→個人情報保護への適用などガイドラインの整備も含め実施予定

2022年1月14日プレスリリース
https://www.nict.go.jp/press/2022/01/14-1.html

※参画機関一覧
国立研究開発法人情報通信研究機構、日本電気株式会社、
株式会社東芝、学習院大学、北海道大学、東京大学、
株式会社 ZenmuTech

③社会展開：装置の評価・認証に向けて

- **QKD装置の国際的な普及展開を進めるためには，QKD装置の国際認証制度が必要**
- **情報技術セキュリティの観点からIT製品の設計・実装を評価するCC認証の枠組みを活用し，QKD装置の認証制度を検討**

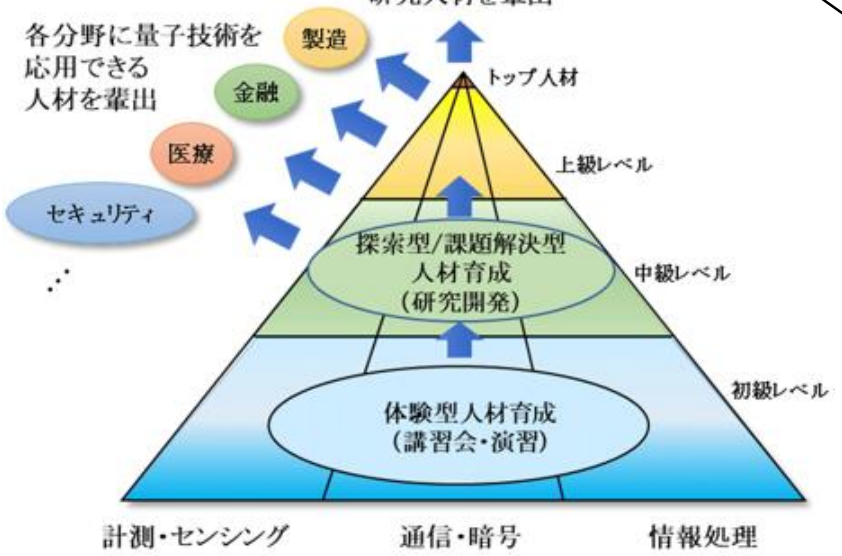


④人材育成：量子人材育成

- **量子ICT人材育成プログラムNQC（NICT Quantum Camp）を通じて産学官連携による実践的なプログラムを提供し，総合力のある量子ネイティブを育成**
- **NICTのリサーチアシスタントやインターン生による自律的な研究開発を支援（若手チャレンジラボ）**

人材育成

研究人材を輩出



若手チャレンジラボ（2022年度～）

NICTのリサーチアシスタントやインターン生として、
先端的な研究開発に挑戦。
産学官の協創環境の中で多様なメンバーと連携、交流。

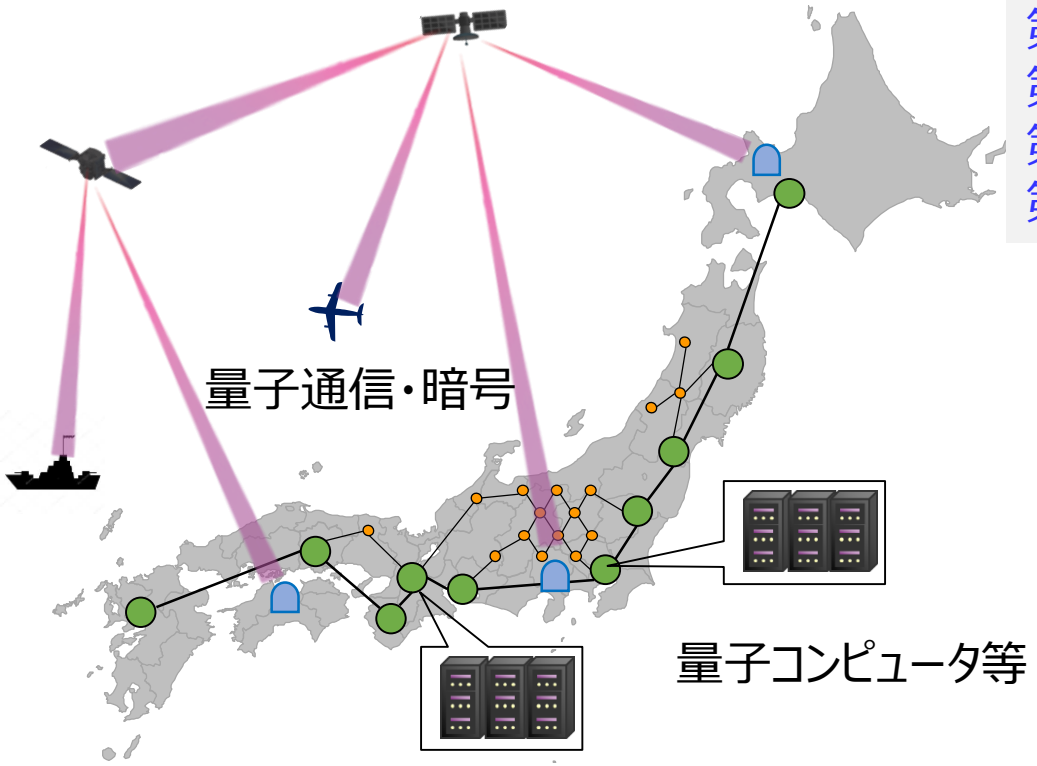
NICT Quantum Camp
（2020年度～）

探索型プログラム
研究作業支援費を受給し講師らの指導の下、研究を実施。

体験型プログラム
高校生、高専生、大学生、大学院生、社会人。
（講義）量子セキュリティ、量子計算、量子計測標準
（演習）量子コンピュータ実機（IBM Q）を利用
（講師）機構内外のトップ研究者17名

量子セキュリティの社会実装に向けたロードマップ

- **量子セキュリティ拠点の活用や，Tokyo QKD Networkの産学官共同利用を通じて，民間投資とユーザの拡大を図る**
- **2023年から段階的に量子暗号通信の普及･社会実装を推進し，グローバルネットワーク化を目指す**



第1段階（2023年頃）：関東圏での量子セキュアクラウド形成
第2段階（2025年頃）：各都市での量子セキュアクラウドコロニー形成
第3段階（2030年頃）：衛星･地上網の統合（日本全土）
第4段階（2035年頃）：グローバルネットワーク化