

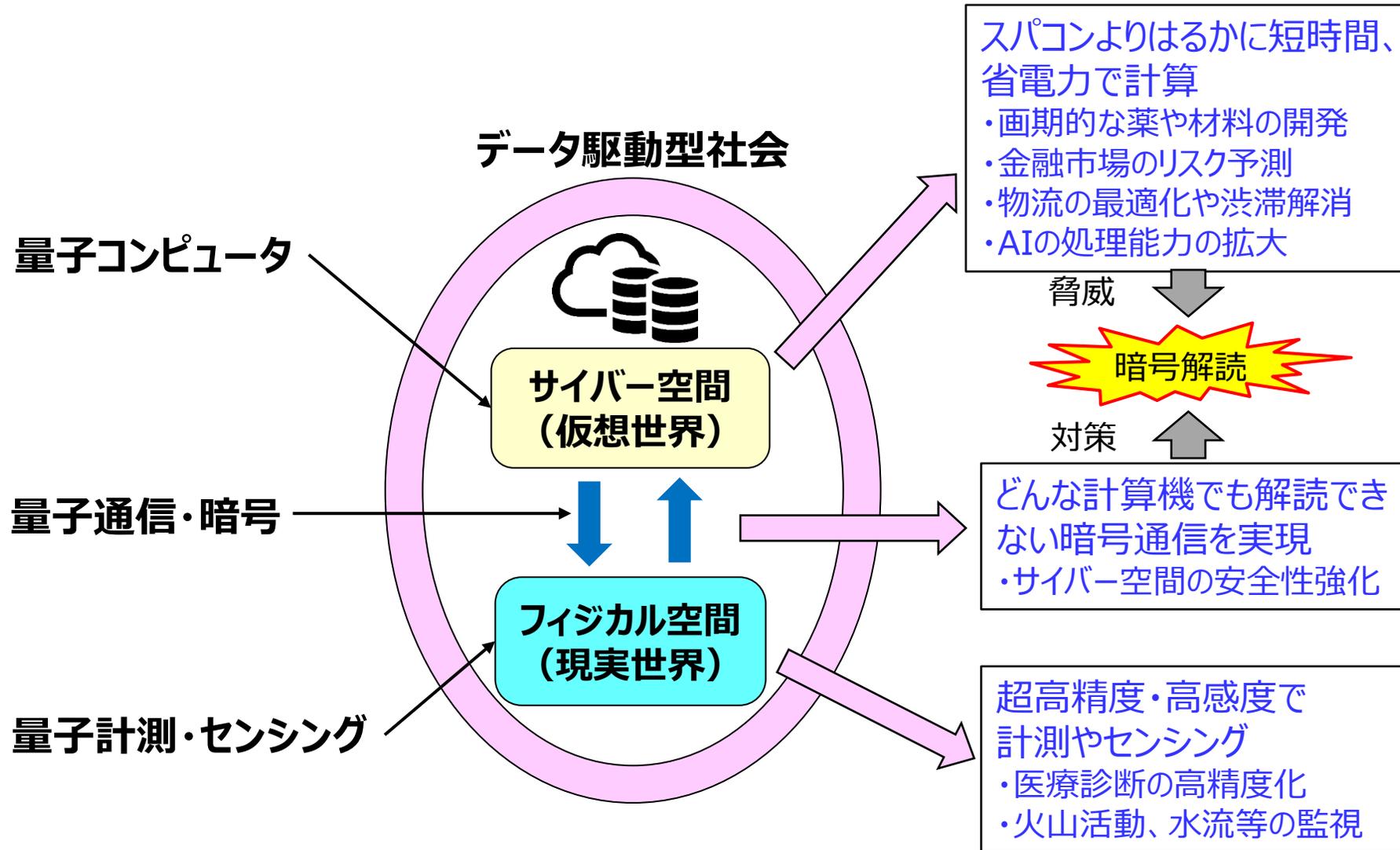
量子技術分野の動向と今後の課題

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

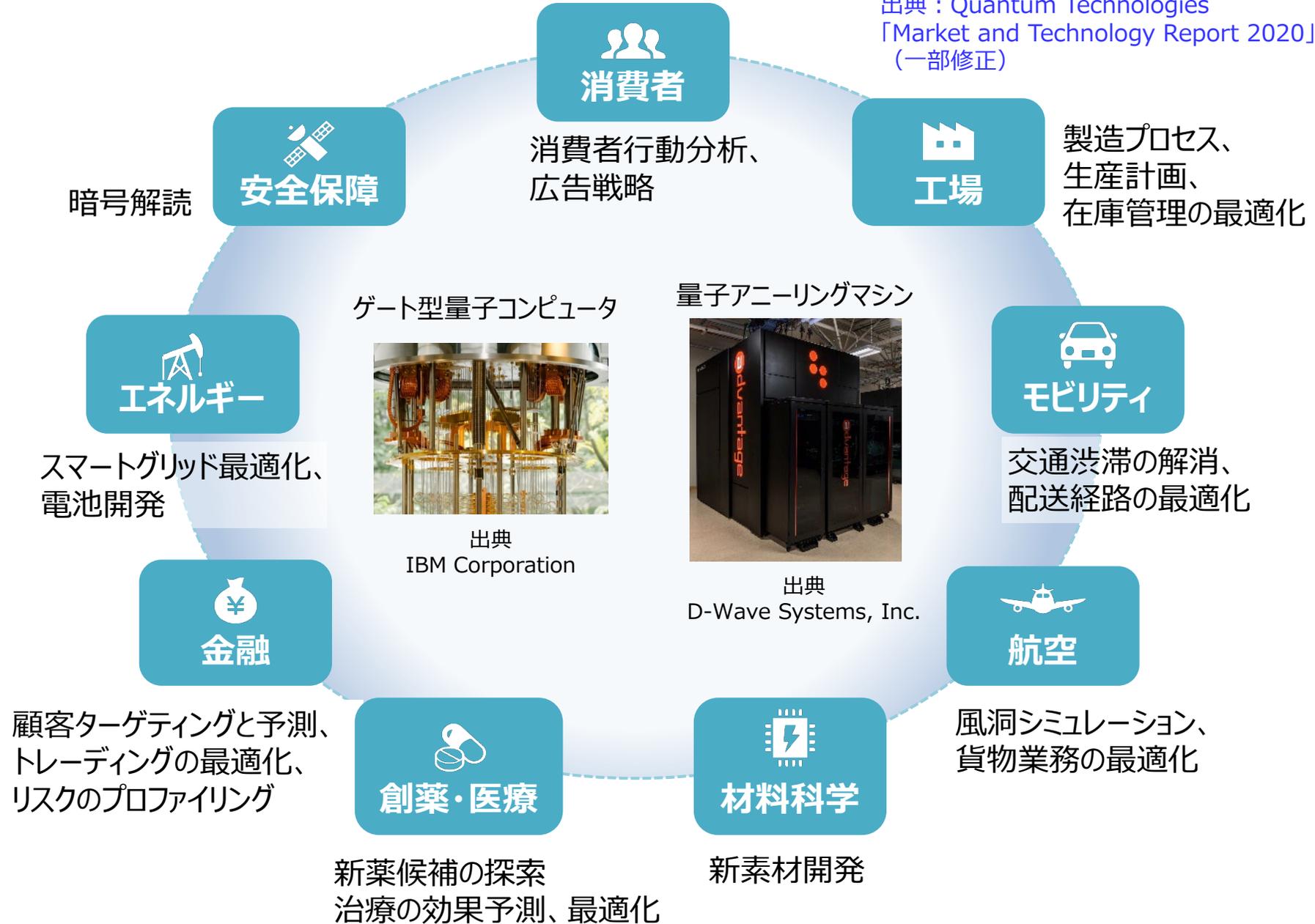
研究センター長 佐々木 雅英

量子技術の概要、社会的インパクト



量子コンピュータの適用領域

出典：Quantum Technologies
「Market and Technology Report 2020」
(一部修正)



量子通信・量子暗号

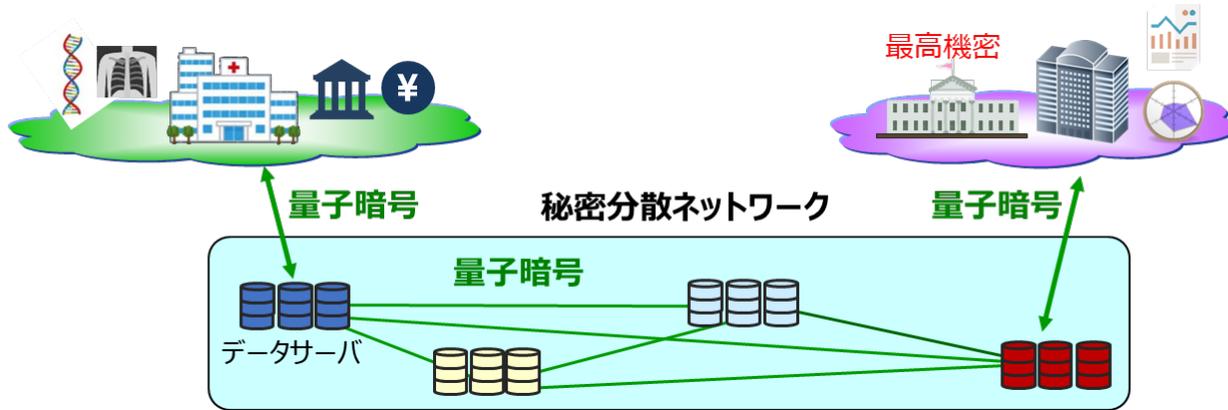
盗聴やハッキングが理論上不可能な暗号通信を実現

重要情報の安全な通信、保管、2次利用

- ・ 国家機密
- ・ 金融情報
- ・ 個人のゲノム、医療・生体情報
- ・ 企業の顧客情報、技術情報

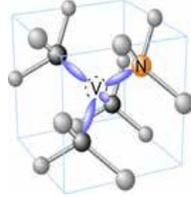
衛星通信網による重要情報の通信

- ・ 外交機密
- ・ 衛星センシング情報
(安全保障分野、商社等の重要情報)
- ・ データセンタ間でのマスタ鍵の交換



量子計測・センシング

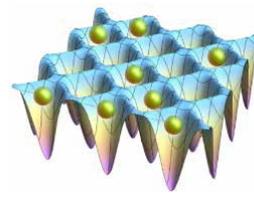
固体量子センサ



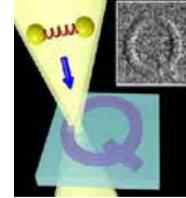
量子慣性センサ



光格子時計

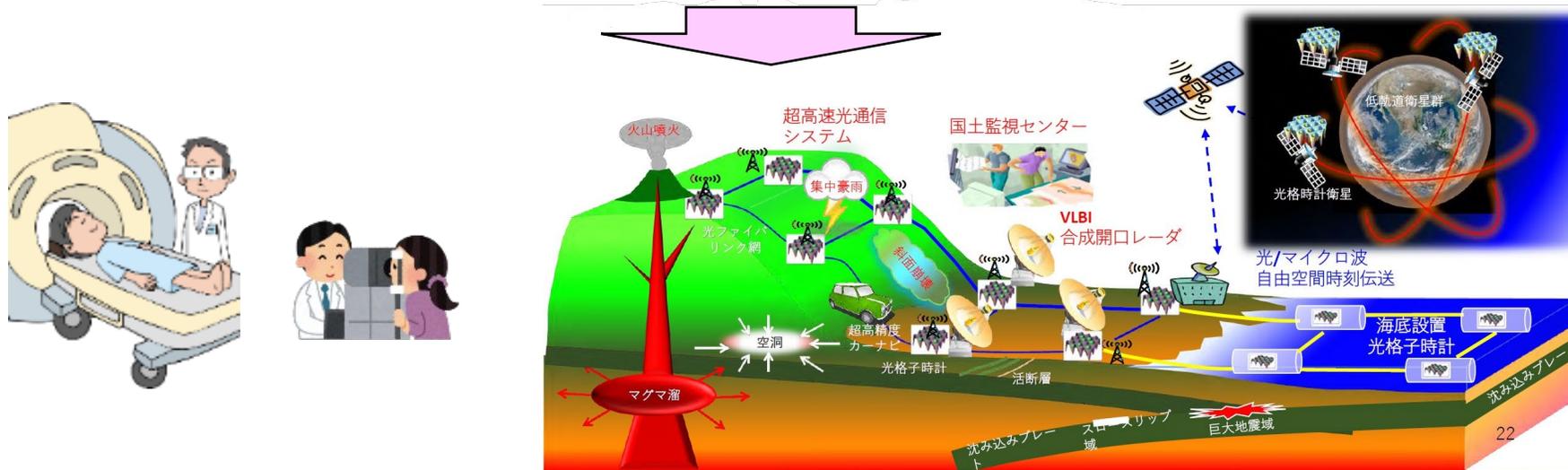


量子もつれ
光センサ



様々な量子系
(スピン、超伝導、
イオントラップ、
NMR、…)

図： 内閣府「量子技術イノベーション戦略」



図： 東大・香取教授のご発表スライド

2030年頃から生命科学、医療、姿勢制御、時空間ビジネス、全球測位システム、計量標準、国土監視、光計測、磁場計測等で実用化が本格化すると予想

諸外国の政府の取組

諸外国は「量子技術」を経済・社会に大きな変革をもたらす革新技術と位置づけ、研究開発投資を大幅に拡充、拠点形成や人材育成等の戦略的取組を展開



- ✓2018年12月、**国家量子イニシアティブ法**が成立。
2019年より5年間で最大13億ドル(約1,400億円)規模の投資。
- ✓**“Science First”**の方針のもと、**研究開発や人材育成の長期戦略を推進**



- ✓2017年6月、欧州委員会が**「量子技術フラッグシップ最終報告書」**を策定
- ✓2018年から**10年間で、10億ユーロ(約1250億円)規模**のプロジェクトを開始
- ✓欧州各国は、独自の国家プロジェクトも平行で推進



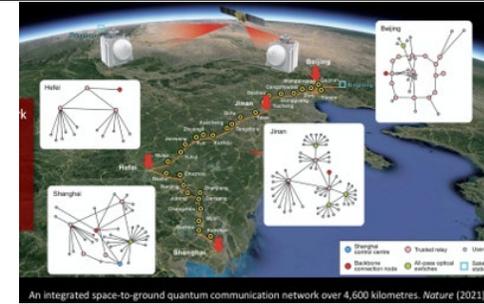
- ✓「科学技術イノベーション第13次五カ年計画(2016年)」において、**量子通信と量子コンピュータを重大科学技術プロジェクト**と位置づけ、積極投資
- ✓「量子情報科学国家実験室」を安徽省合肥市に**約70億元(約1,200億円)かけて建設中**(2020年末、第1研究棟完成)
- ✓**衛星量子暗号**を世界で初めて実証するなど、**暗号・通信分野でも躍進**

諸外国の動向：量子通信・量子暗号分野



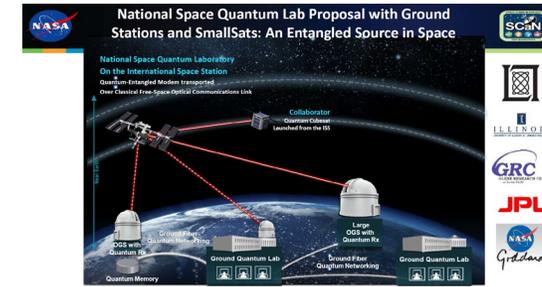
スピード、規模で他国を圧倒し先行

- ✓世界最大規模の量子暗号ネットワークを構築、運用
- ・2025年までに全国規模のネットワーク構築を計画
- ✓衛星量子暗号を世界で初めて実証(2017)



Science Firstの方針のもと長期戦略を推進

- 電力供給網向け量子暗号ネットワーク(LANL、電力会社)
- エネルギー省が全国規模の量子インターネット構築を推進
- 米国は衛星光通信で圧倒的な技術力を有し、衛星量子通信でも主導権を握ることは確実

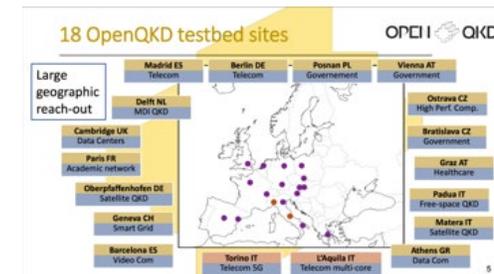


2022年、ISS-地上間で量子もつれ交換実験を計画



通信事業者、衛星事業者の動きが活発化、インフラ構築に向けた動き

- ✓『OpenQKD』(2019-2023)
 - ・13カ国38機関、18のテストベット、50以上のUse case
- ✓『EuroQCI』(2021-2027)。
 - 欧州全土で量子通信インフラを構築する計画。
 - ①ドイツテレコム、オーストリア技術研究所、タレス、テレフォニカ
 - ②エアバス、レオナルド、オランジュ、イタリア国立計量研究所など



量子技術イノベーション拠点整備

- 基礎研究から技術実証、オープンイノベーション、人材育成等に至るまで産学官で一気通貫に取り組む拠点を形成
- 国内外から優れた研究者・技術者を結集、産業界から積極的な投資を呼び込み

量子コンピュータ開発拠点（理化学研究所）

量子デバイス開発拠点（産業技術総合研究所）

量子コンピュータ利活用拠点（東京大学－企業連合）

量子ソフトウェア研究拠点（大阪大学）

量子セキュリティ拠点（情報通信研究機構）

量子生命拠点（量子科学技術研究開発機構）

量子マテリアル拠点（物質・材料研究開発機構）

量子センサ拠点（東京工業大学）

発足式典 2021年2月26日

量子セキュリティ拠点 (情報通信研究機構)

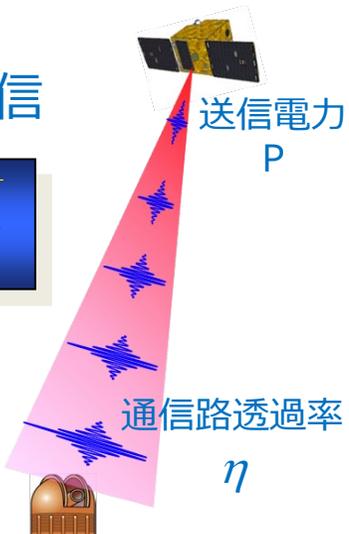
基礎となる要素課題

量子通信

① 長距離・大容量通信

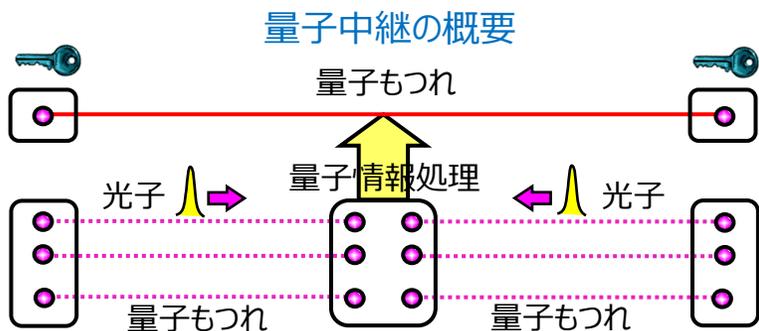
$$C = \frac{\pi}{\ln 2} \sqrt{\frac{2\eta P}{3h}}$$

Plank定数
 $h = 6.6 \times 10^{-34} \text{J} \cdot \text{s}$



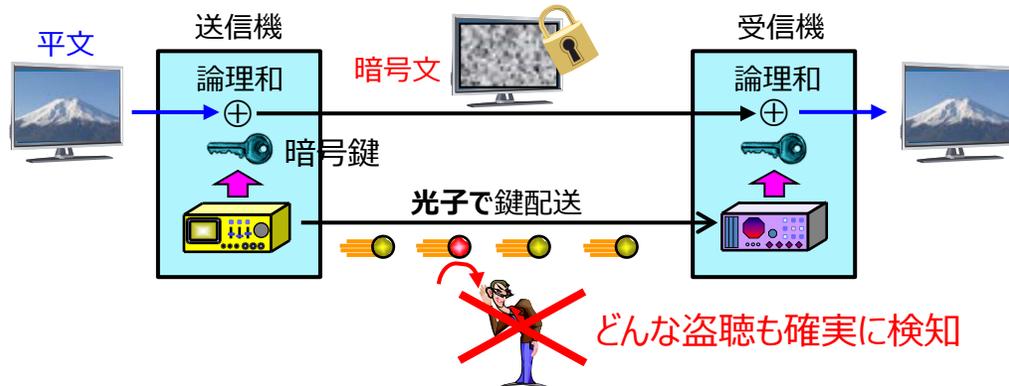
② 量子中継などの新プロトコル

量子もつれを用いた量子ネットワークの構築



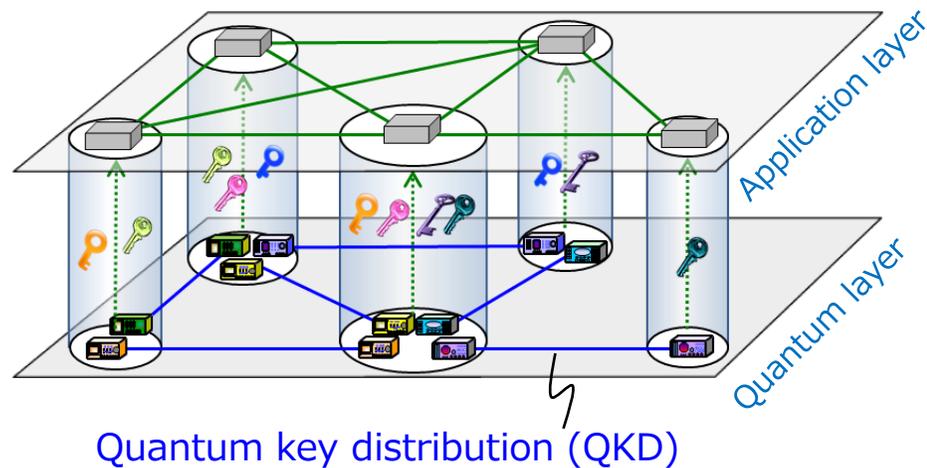
量子暗号

どんな計算機でも解読できない暗号通信



・50km圏で1Mbps程度の鍵配送速度

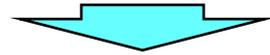
・トラステッドノードを介した鍵リレーによりネットワーク化



量子セキュリティ分野の必要性

- ・現在の量子暗号、量子中継は1対1の通信プロトコル
⇔ 公開鍵暗号は1対100万規模での電子署名、鍵交換を実行
- ・量子暗号、量子中継は、盗聴され続けると『鍵や量子もつれを確立できない』
⇒ サービス停止(DoS)攻撃への耐性がない

『量子』のみでは広域・多地点のセキュリティインフラ構築は不可能



量子と古典を組み合わせたネットワーク冗長化が必須
(未踏課題)

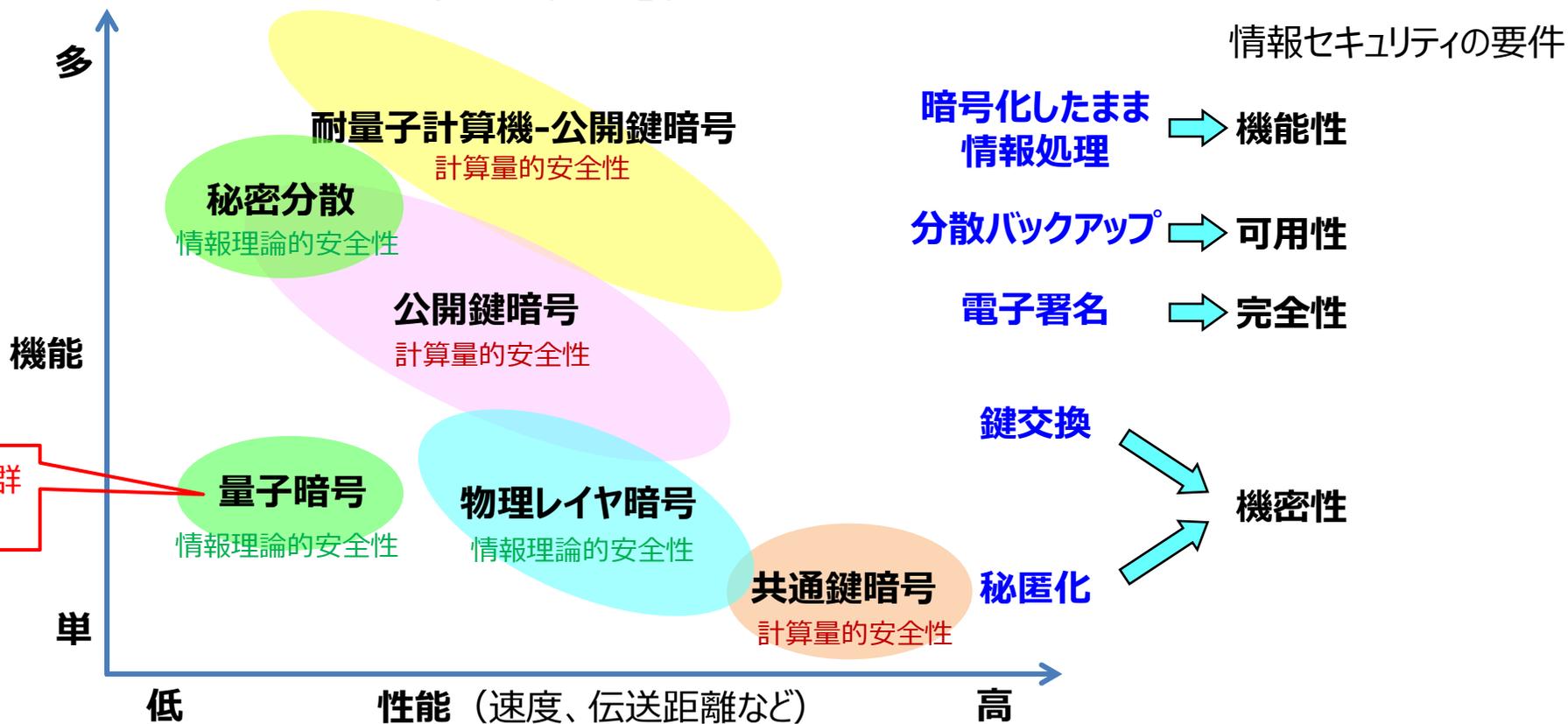


量子セキュリティ分野

この融合領域の技術体系構築が、学術創成と実用化の鍵

様々な暗号技術

「機能-性能」視点でのマッピング



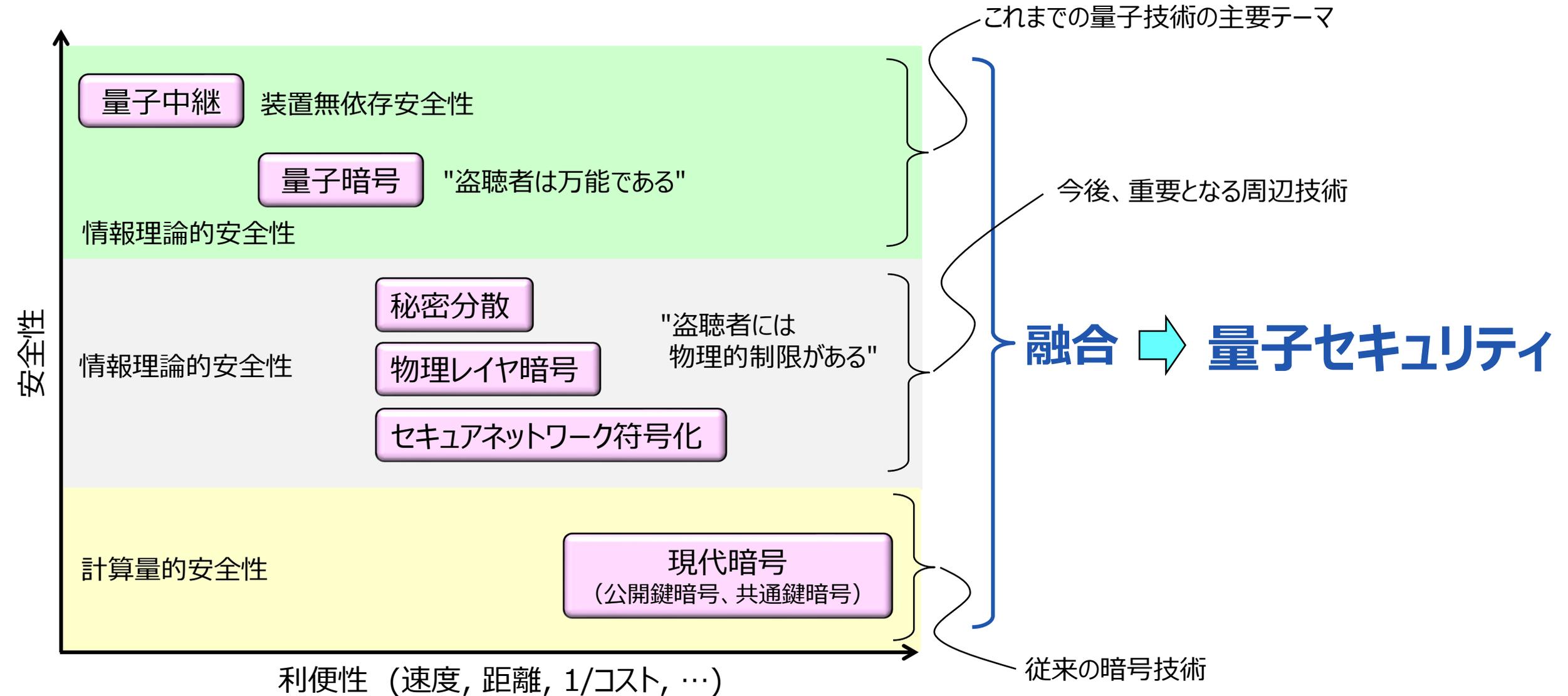
量子暗号は多くの暗号技術群のほんの一角に過ぎない

機密性、完全性、可用性、機能性の全ての要件を満す全能の暗号技術は存在しない

様々な暗号技術を適材適所で組合せ、総合的にセキュリティを強化

様々な暗号技術

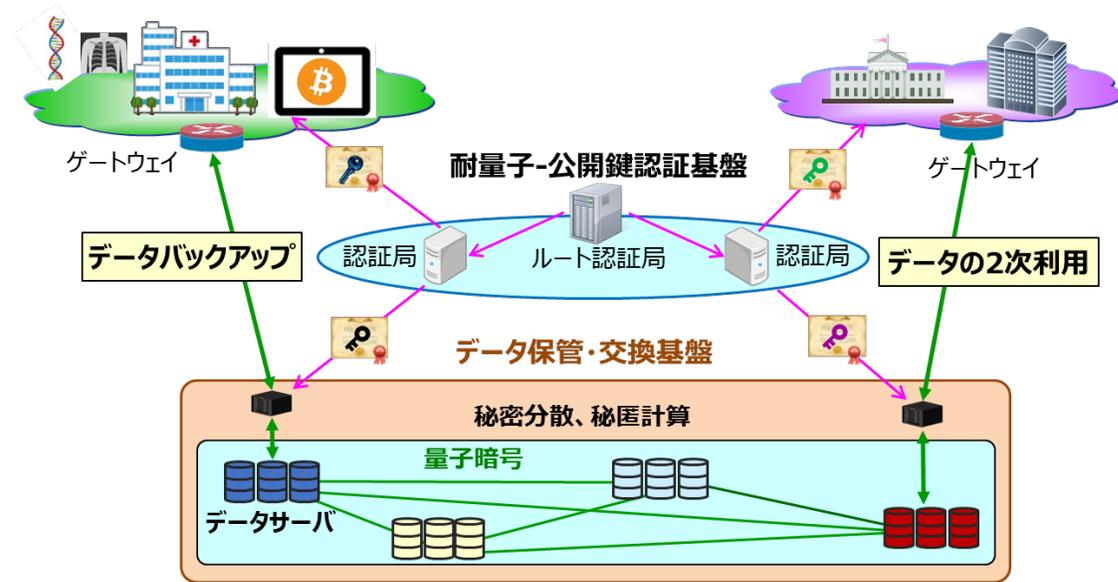
「安全性-利便性」視点でのマッピング



量子セキュリティ分野の主な出口イメージ例

量子セキュアクラウド

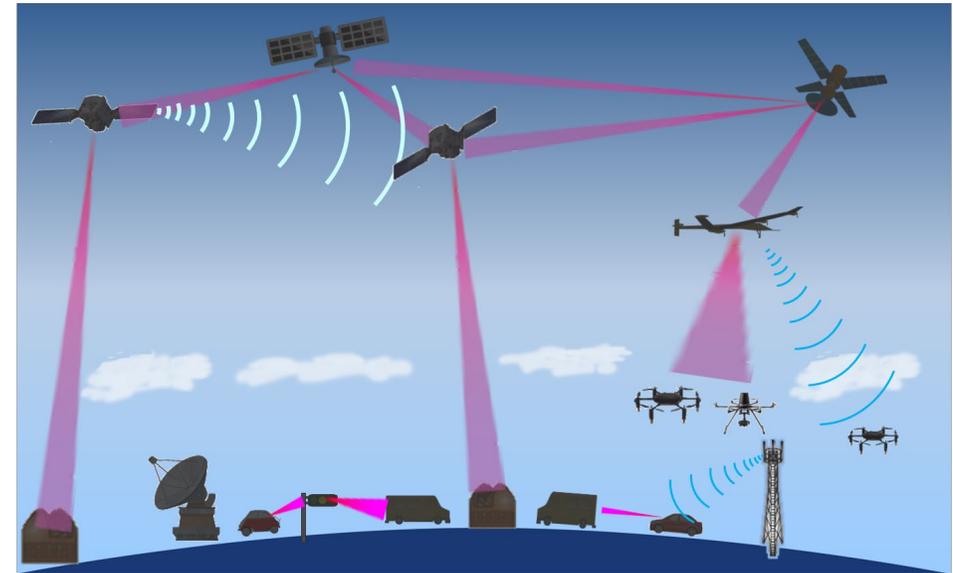
将来にわたり盗聴や改竄を防ぎ、
秘匿化したまま計算を実行



内閣府SIP『光・量子を活用したSociety 5.0実現化技術』
(2018年度～2022年度)
NICT、NEC、東芝、学習院、ZenmuTech、北大、東大

量子セキュア移動通信ネットワーク

宇宙から地上網まで網羅する大容量
かつ安全な移動通信ネットワークを実現



特許6923151 (NICT、プロドローン)

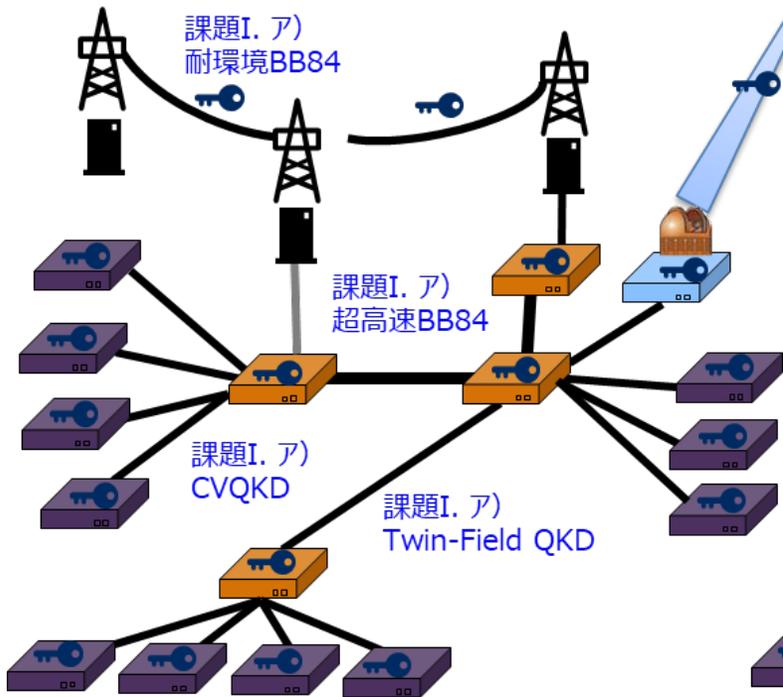
総務省『衛星通信における量子暗号技術の研究開発』
(2018年度～2022年度)
NESTRA、NICT、ソニーCSL、スカパーJSAT、東大
総務省『グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発』
(2021年度～2025年度)
スカパーJSAT、NICT、NEC、東芝

グローバル量子暗号通信網構築のための研究開発

東芝、NICT、NEC、北大、横国大、学習院大、東大、三菱電機、古河電工、浜ホト、AIST、NIMS
(2020年度～2024年度)

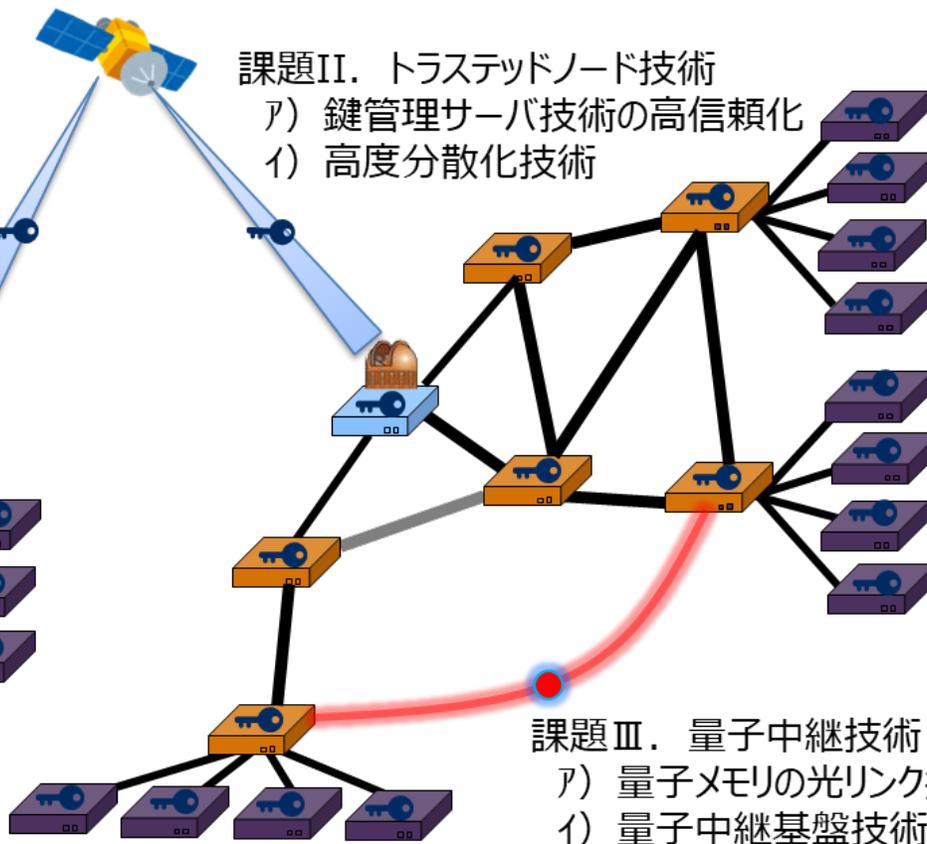
課題I. 量子通信・暗号リンク技術

- ア) 量子暗号通信の高性能化技術
- イ) 光子検出技術



課題II. トラストドノード技術

- ア) 鍵管理サーバ技術の高信頼化
- イ) 高度分散化技術



- ・量子暗号
- ・量子中継

X 融合

- ・秘密分散
- ・物理レイヤ暗号
- ・セキュアネットワーク符号化

課題IV. 広域ネットワーク構築・運用技術

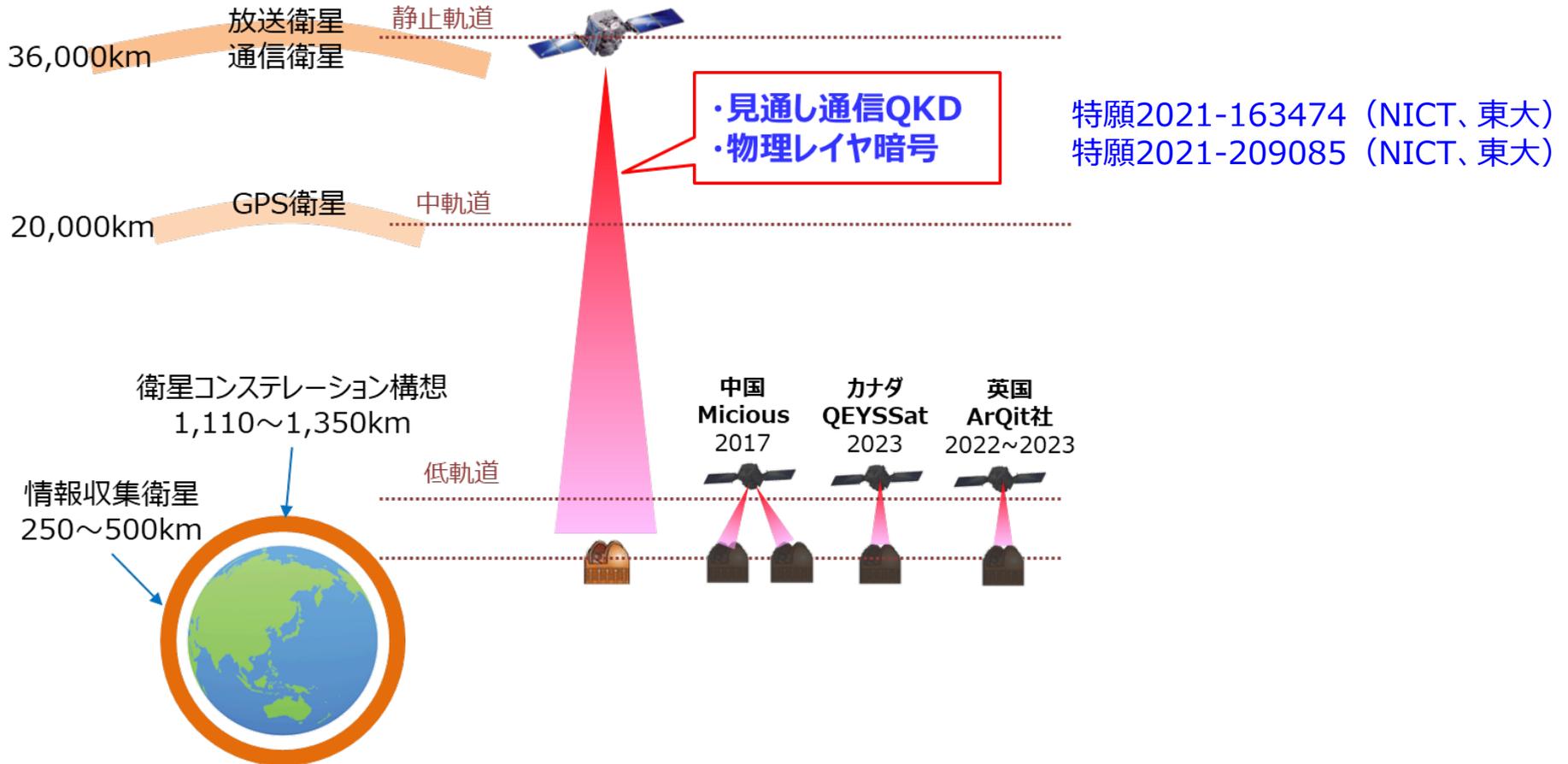
- ア) ネットワーク制御管理技術



総務省 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

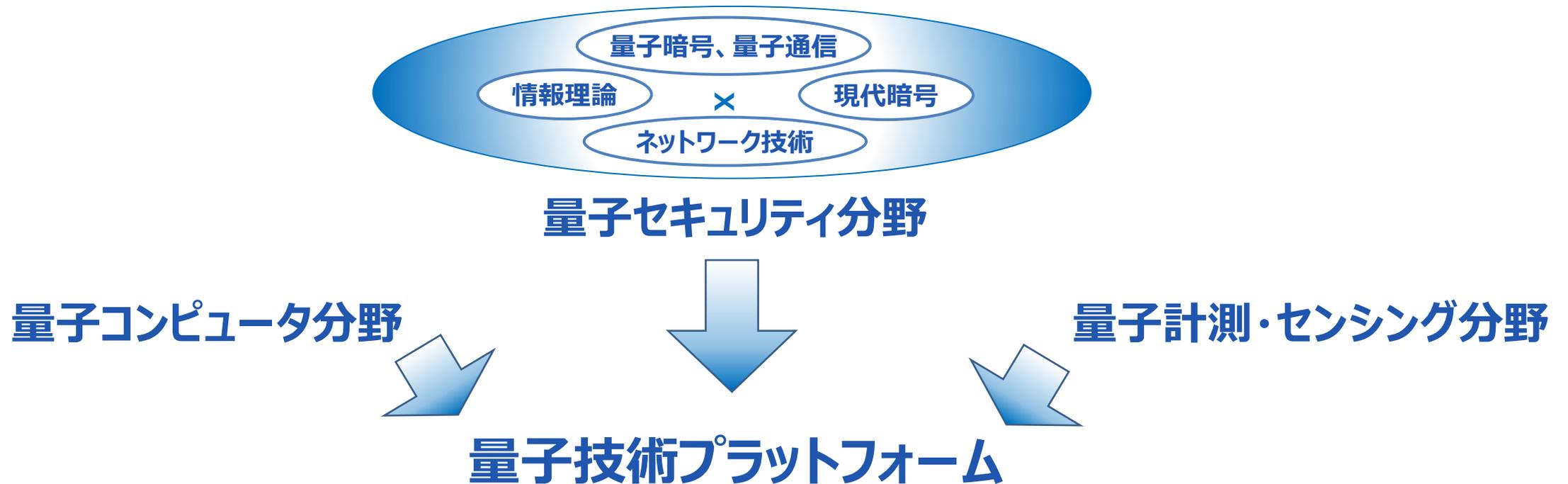
スカパーJSAT、NICT、NEC、東芝（2021年度～2025年度）

安全性と伝送効率のバランスを自在に制御できる新方式『見通し通信QKD』や『物理レイヤ暗号』を開発し、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を実現



今後の課題と戦略案

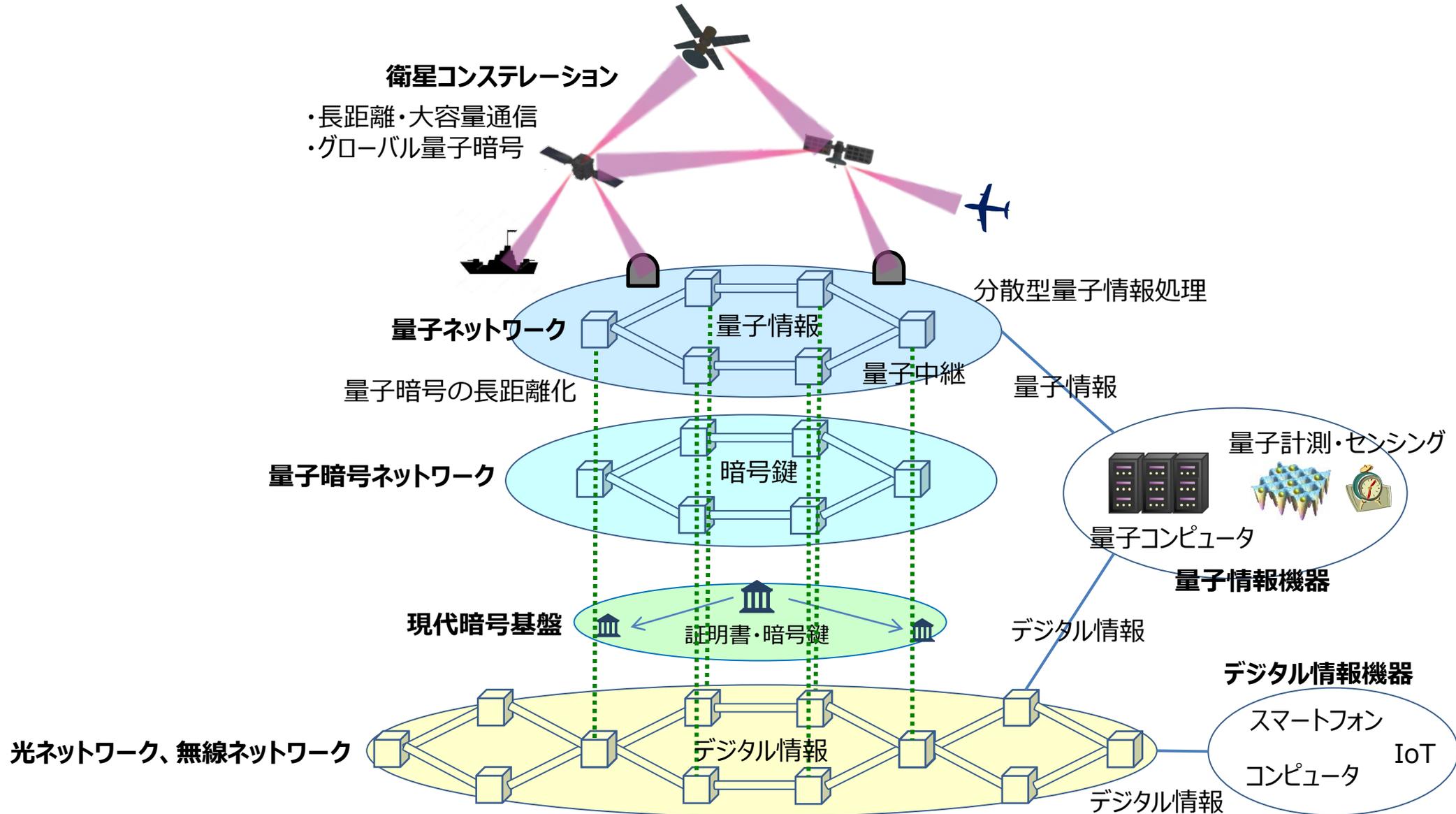
様々な量子技術の融合を図り、情報通信インフラに導入・統合し、
量子技術に基づく新たなサービスを提供するインフラを構築



高度な計算処理、計測・センシング、通信・暗号の機能を提供する新たな基盤

量子技術プラットフォーム

高度な計算処理、計測・センシング、通信・暗号の機能を提供する新たな基盤



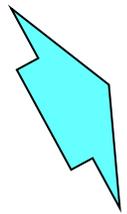
ロードマップ

令和3年度(2021年度)
補正予算事業



2023年頃

ユーザ拠点に量子暗号回線を伸長。
ベンダー、通信事業者による
量子暗号サービスの提供。



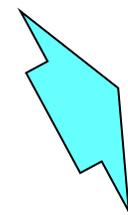
2025年頃

都市間の量子暗号通信網

- ・装置の量産化
- ・国産APD生産体制の整備
- ・評価・認証制度の確立

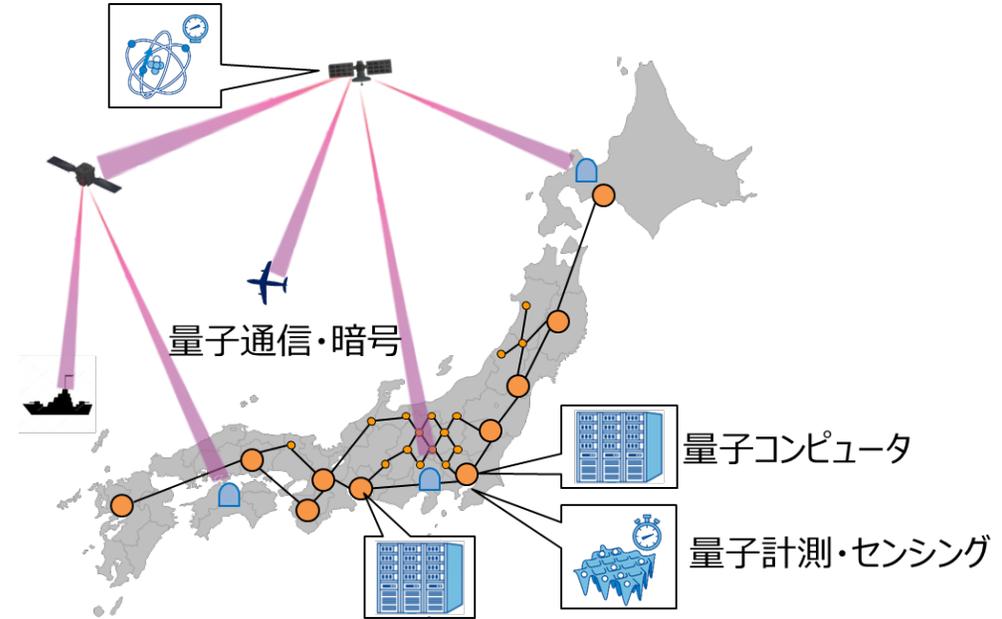
様々な量子技術の集約

- ・量子セキュアクラウドの実用化
- ・量子中継のフィールド実証



2030年頃

衛星・地上網の統合
本格普及、ビジネスエコシステムの確立



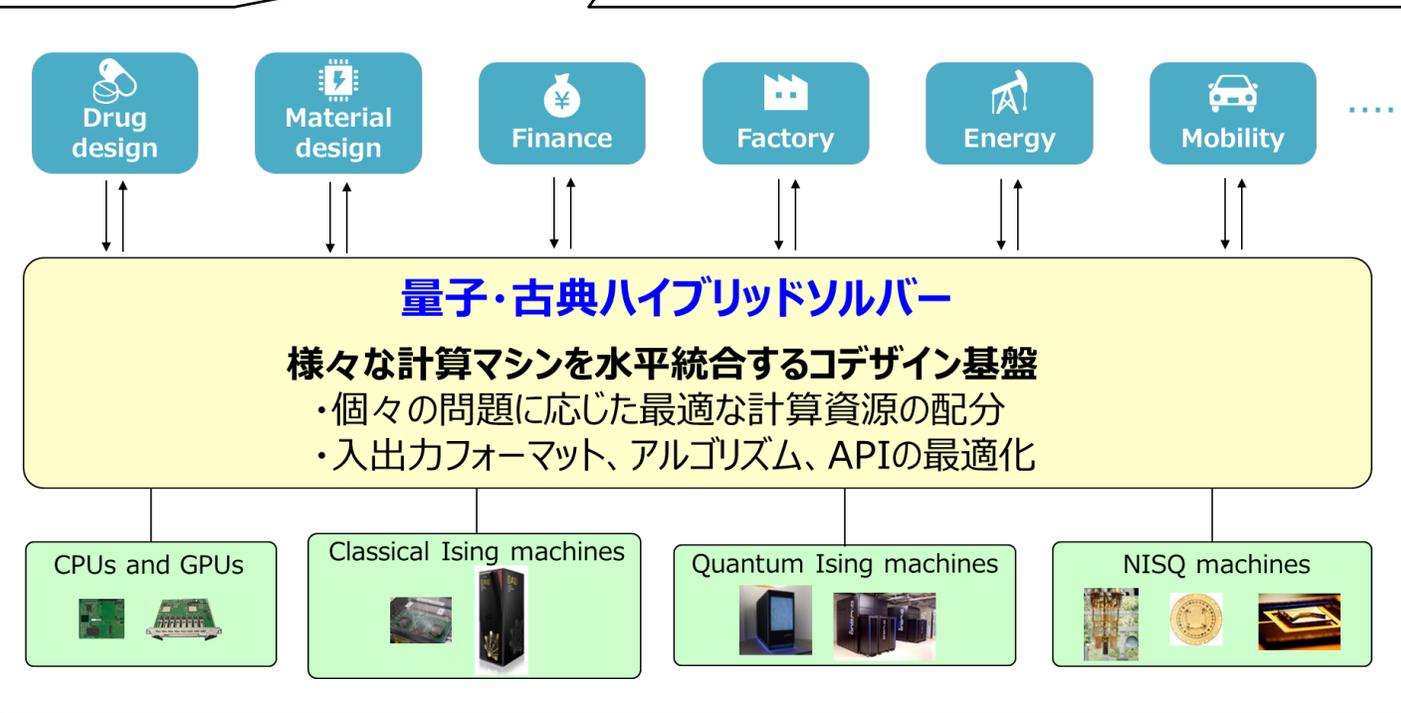
次世代コンピューティング基盤

X

超長期セキュリティを 保証する次世代暗号基盤

- 量子・古典ハイブリッドソルバー

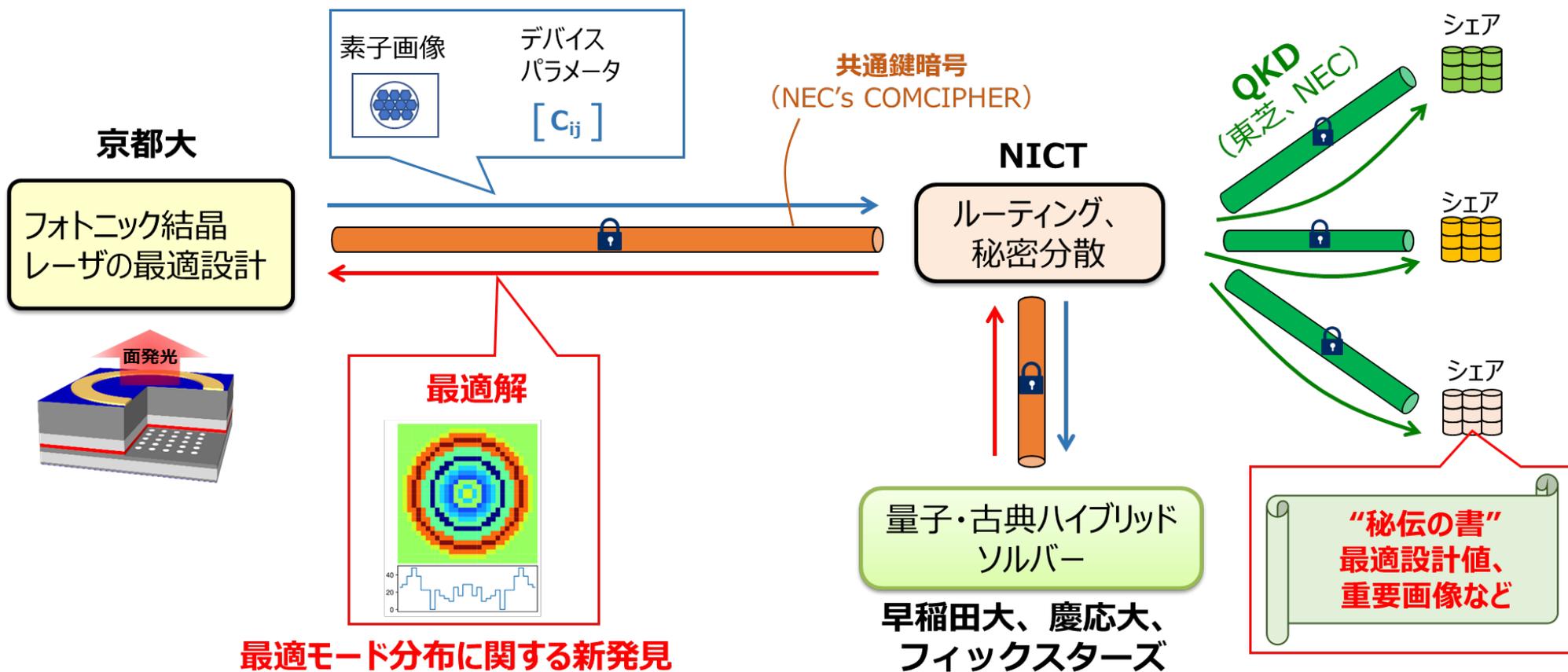
- 耐量子計算機-暗号
- 量子暗号
- 秘密分散



実証例：フォトニック結晶レーザのスマートデザイン

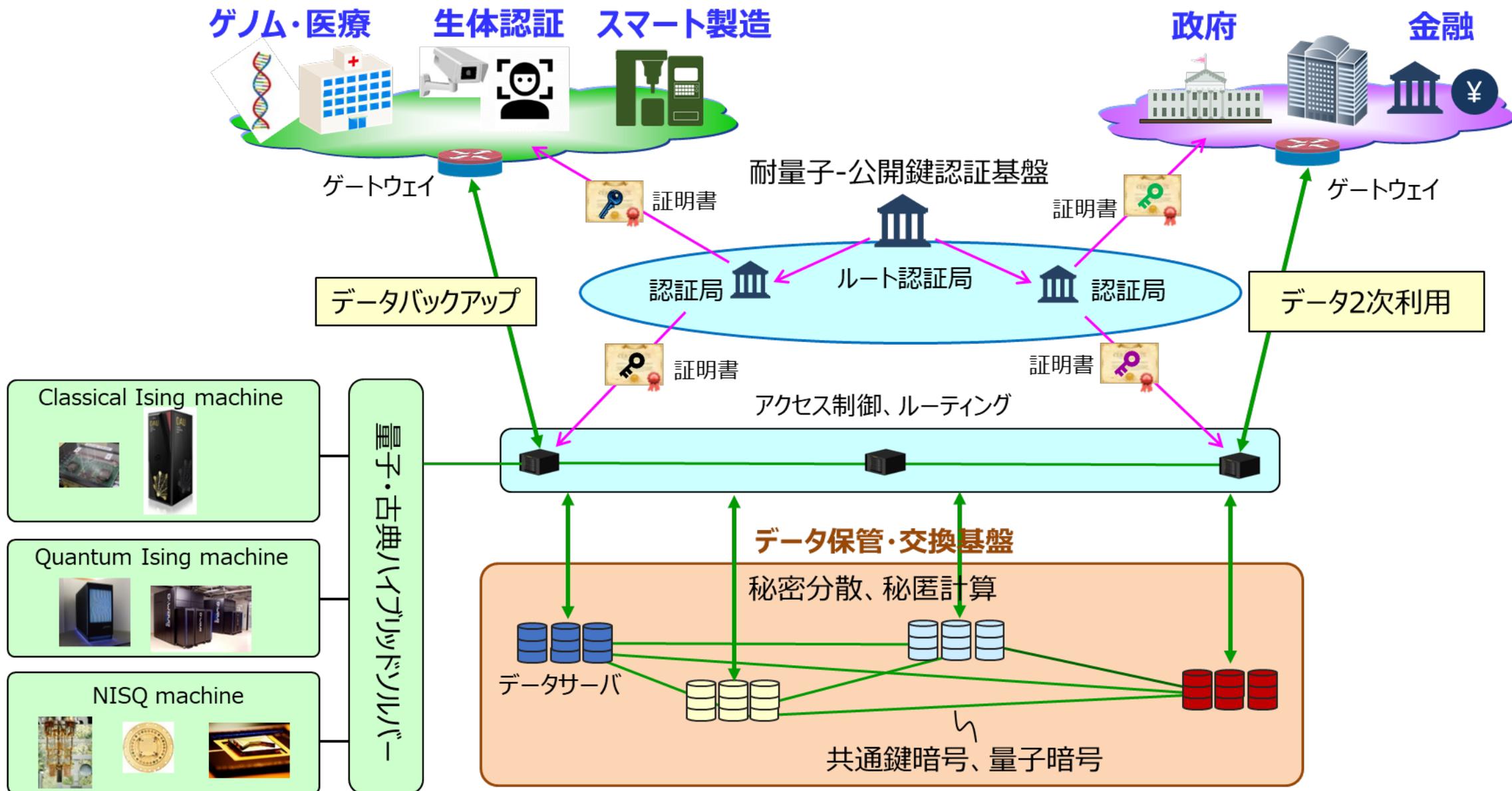
内閣府SIP『光・量子を活用したSociety5.0実現化技術』

- 量子・古典ハイブリッドソルバーを使い、最適設計パラメータの導出時間を劇的に短縮（約1か月⇒約1日）
- 設計に関する“秘伝の書”を超長期間、安全にバックアップ保管



2025年頃、実用化

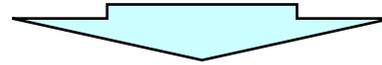
量子セキュアクラウド



2025年頃までに 評価・検定・認証制度の整備

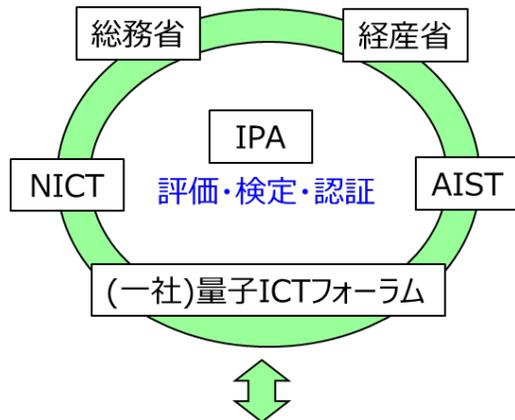
量子暗号装置の調達には国際規格（**コモンクライテリア:CC**）準拠の認証が必要。
しかし、**まだ世界にその実例はない。**

ETSI、ISO/IEC JTC1へ日本から膨大な寄書を提出、主導権を握っている



日本の取るべき戦略

CC認証を取得した量子暗号装置を世界に先駆けて市場投入する



Q-STAR等のコンソーシアムとの連携

- ・セキュリティ要求仕様（**プロテクションプロファイル:PP**）の草案を作成
- ・認証機関（日本のIPA、ドイツのBSIなど）による審査を経てPPが成立
- ・評価機関（ECSEC等の企業、NICT、AISTなど）による量子暗号装置の評価
- ・認証機関による認証
- ・CC認証された量子暗号装置をユーザが調達
⇒ ベンダによる市場展開と量産化（**2025年頃**）



日本がルールメイキングを主導、国際市場のシェア拡大に繋げる

量子インターネットに向けた研究開発基盤の整備

総務省『グローバル量子暗号通信網構築のための研究開発』

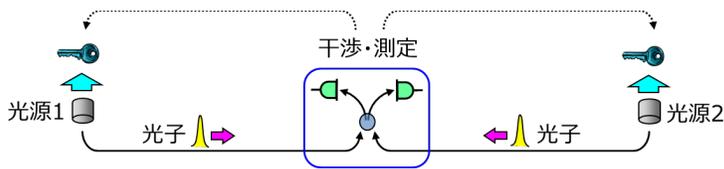
(2020年度～2024年度)

一方向型QKD

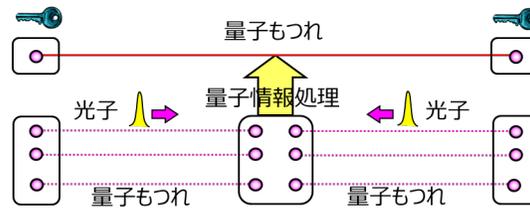
BB84、CV-QKDなど

測定支援中継型QKD

Twin field-QKD、MDI-QKD など



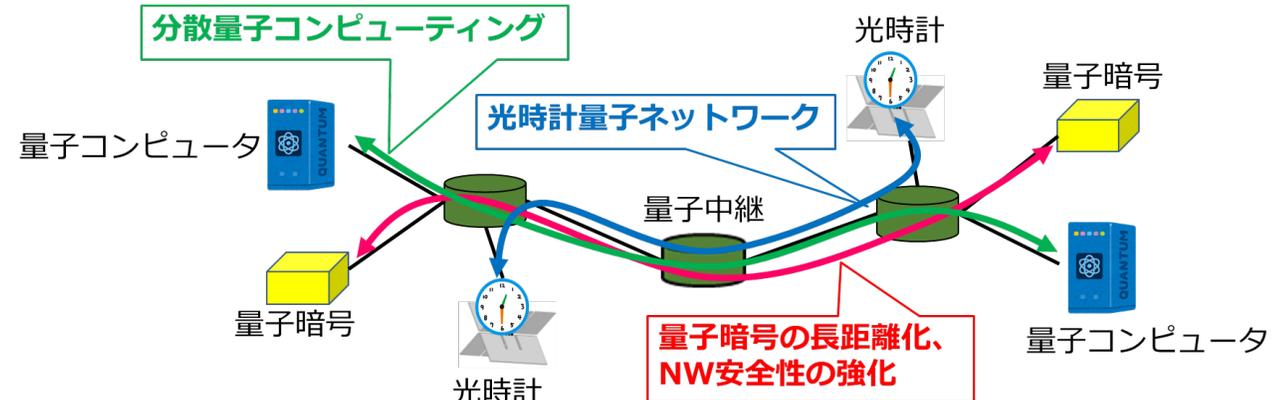
量子中継



文科省

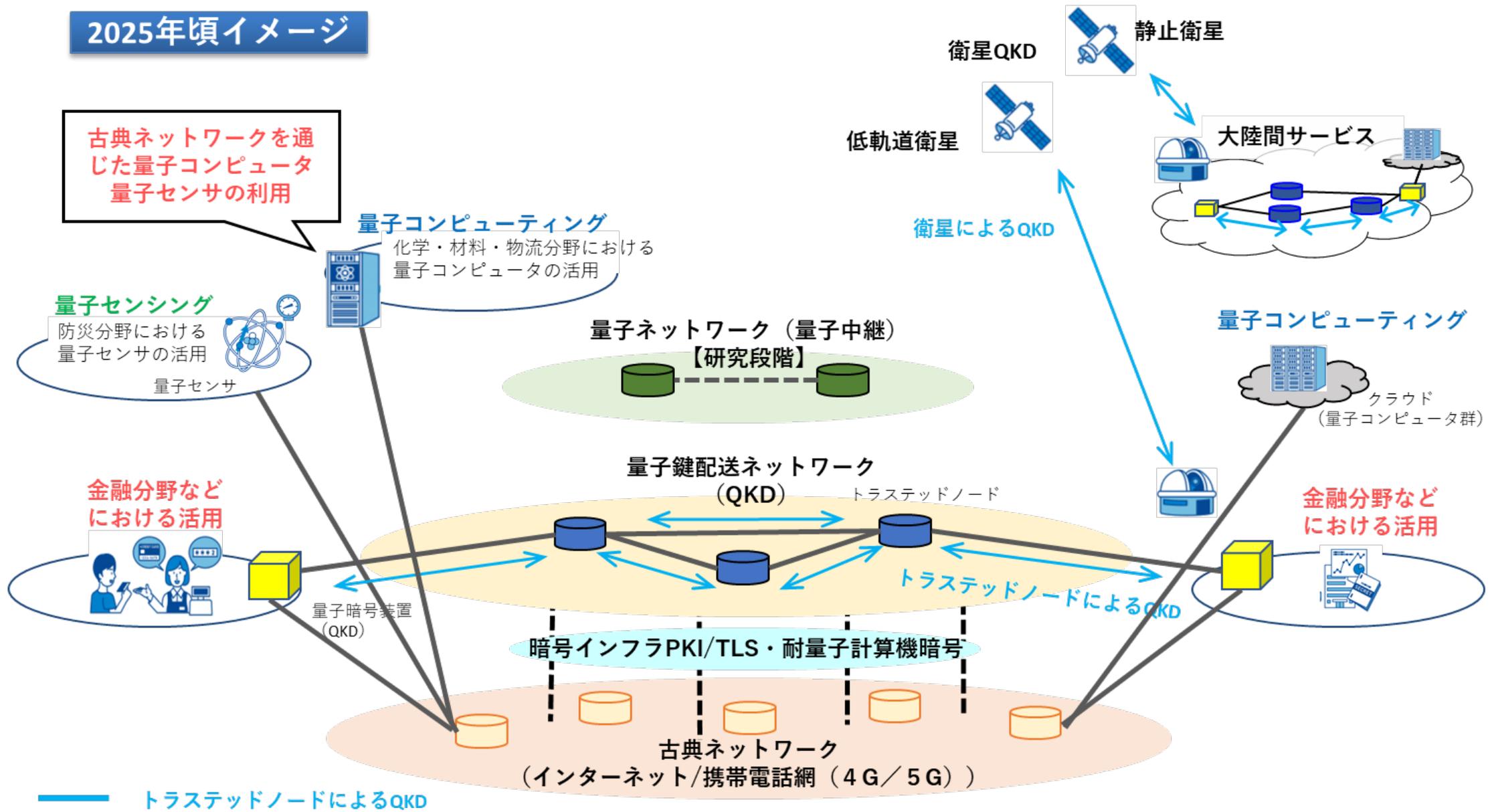
・Q-LEAP

・ムーンショット型研究開発制度
目標6：量子コンピュータ社会の
実現に向けた抜本的な加速

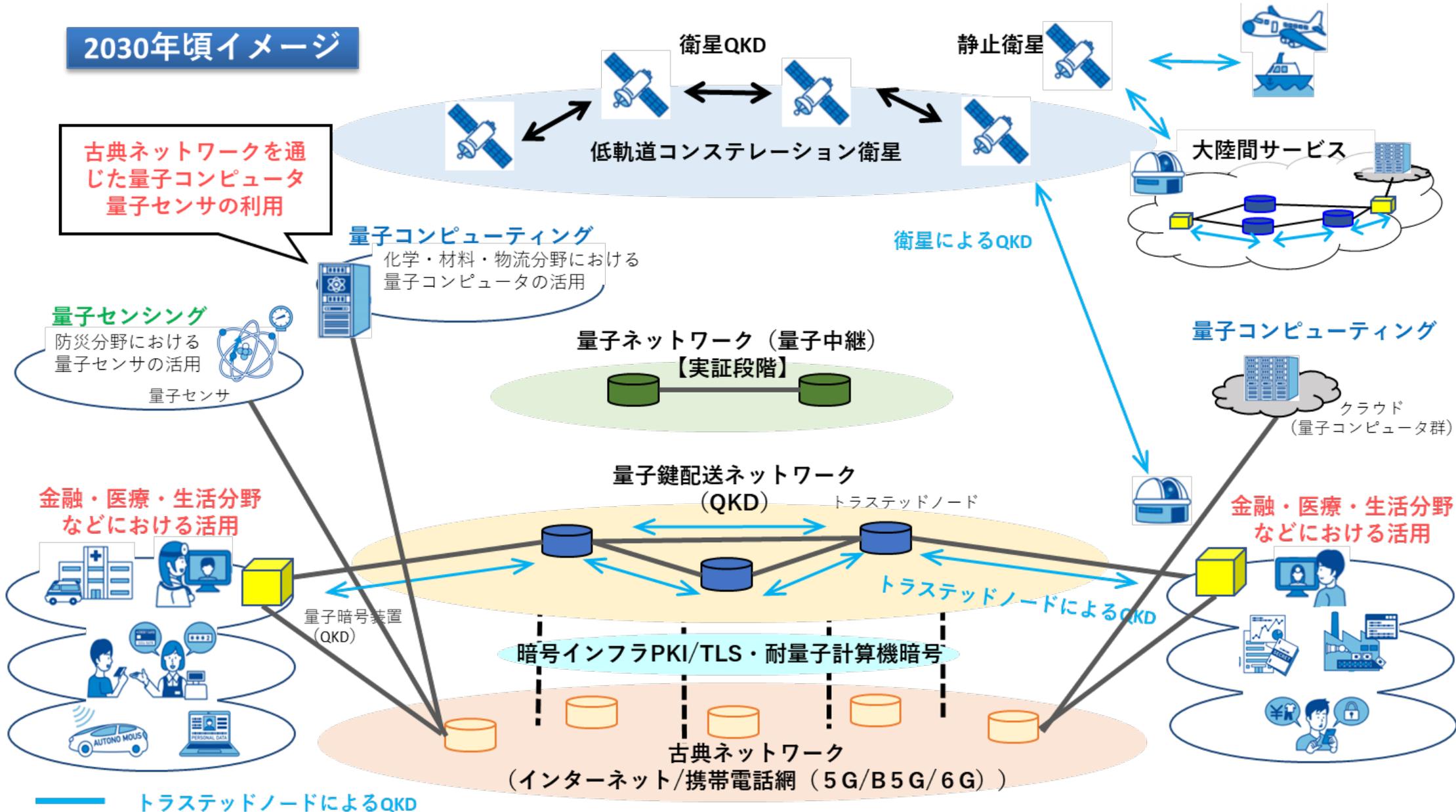


最終的なゴールイメージ

2025年頃イメージ



2030年頃イメージ



古典ネットワークを通じた量子コンピュータ
量子センサの利用

量子コンピューティング
化学・材料・物流分野における
量子コンピュータの活用

量子センシング
防災分野における
量子センサの活用
量子センサ

金融・医療・生活分野
などにおける活用

量子暗号装置
(QKD)

暗号インフラPKI/TLS・耐量子計算機暗号

古典ネットワーク
(インターネット/携帯電話網 (5G/B5G/6G))

大陸間サービス

衛星によるQKD

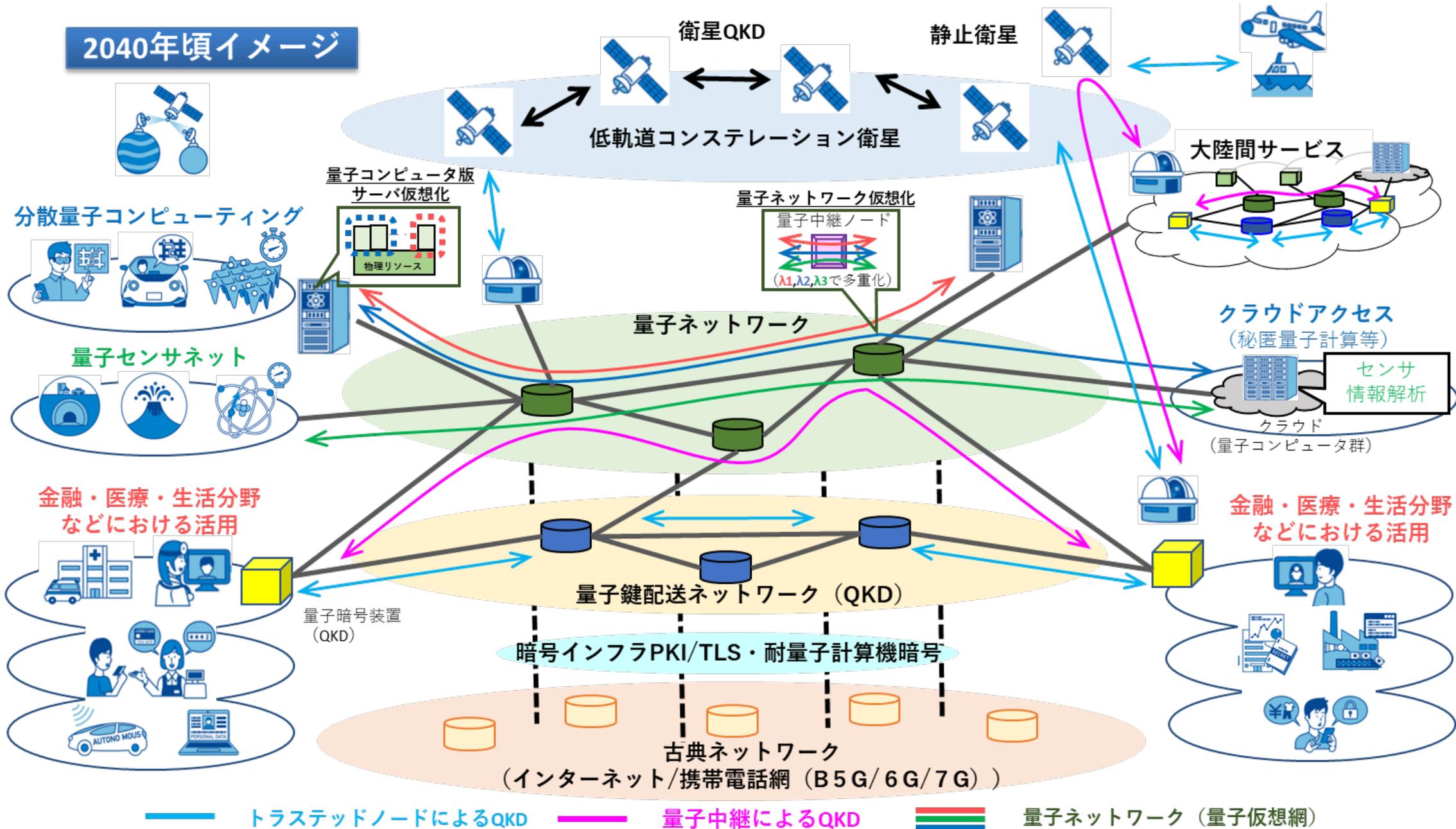
量子コンピューティング
クラウド
(量子コンピュータ群)

金融・医療・生活分野
などにおける活用

トラステッドノードによるQKD

トラステッドノードによるQKD

2040年頃イメージ



人材育成

NICT量子ICT人材育成プログラム “NICT Quantum Camp”

● 産学官連携による実践的なプログラム

高専生、大学生、大学院生等を対象に量子ICTネイティブ人材を育成。

2020年度、30名が卒業。

2021年度

① 講習会

座学、演習（量子コンピュータ IBM-Q）

⇒ 75名の応募者から50名の受講生を採択

② 探索型/課題解決型研究

課題提案、研究実施、成果発表（研究作業支援費を支給）

⇒ 8件の応募から5件を採択

⇒ 昨年度の修了生がアシスタントとして参加。

自主勉強会や進学相談会を自発的に開催。

⇒ 修了生の一部は、NICTインターンシップ制度でさらに研究開発を実施



まとめ

- 量子技術による情報通信インフラのアップデートが始まっている。
- 量子技術は、
2025年頃から量子暗号等で量産化・低価格化が始まり、
2030年頃から、コンピューティング、通信・暗号、計測・センシング
を統合した形で本格普及期に入ると予想される。
- 並行して、量子技術と周辺技術の融合による新たな学際領域が創成されてゆくと期待される。

情報収集や交流の場として、[\(一社\) 量子ICTフォーラム](#)
人材育成の場として、[NICT Quantum Camp](#)
もぜひご活用ください。

謝辞

本講演の内容の一部は、以下のプロジェクトの研究開発の成果に基づいています。

内閣府SIP『光・量子を活用したSociety 5.0実現化技術』

総務省『ICT重点技術の研究開発プロジェクト(JPMI00316)』のうち、
『衛星通信における量子暗号技術の研究開発(JPJ007462)』
『グローバル量子暗号通信網構築のための研究開発(JPJ008957)』
『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
(JPJ010277)』

本発表資料の一部は、発表者が関わっている以下の活動・資料から引用しています。

- 統合イノベーション戦略推進会議/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」有識者
- 一般社団法人 量子ICTフォーラム・技術担当理事
- 内閣府 SIP第2期「光・量子を活用したSociety 5.0実現化技術」
サブプログラムディレクタ（光・量子通信担当）

ご清聴ありがとうございました

