資料1

量子セキュリティ・量子ネットワークの論点等

量子技術の実用化推進WG　第一回、第二回
令和4年11月10日、11月24日

量子セキュリティ・量子ネットワークの論点等

①量子セキュリティ・量子ネットワークの産業振興

1．ユーザ産業の振興・拡大

- 量子セキュリティ・量子ネットワークを利用する様々なユーザ産業の発掘・拡大（参画促進、裾野拡大によるマーケット創造）、産業振興に向けた方策はどうあるべきか。
- 新たなユーザを訴求する**魅力的なユースケース**づくりの在り方はどうか。

2．量子セキュリティ・量子ネットワークの事業化支援・国際競争力強化

- 今後、国内ベンダー企業の**勝ち筋となるビジネスモデル**、熾烈な国際競争に劣後しないための国際競争力強化等の在り方はどうか。
- 利用支援サービス（アプリケーション）を提供する民間事業者の**ビジネスモデルや主体の在り方**はどうか。

3．量子暗号通信機器の国内認証基盤構築の推進

- 国内認証制度、**特に評価機関**はどうあるべきか。
- 国内認証制度を**エコシステムとして自律化**するための方策はどうあるべきか。

②量子セキュリティ・量子ネットワークの利用環境整備と利用実証の拡大

1．量子・古典ハイブリッドによる総合的アーキテクチャの検証

- 古典アーキテクチャからの**移行（マイグレーション）**はどうあるべきか。
- 量子暗号、耐量子計算機暗号、量子ストリーミング暗号等の多様な**量子・古典暗号のベストミックスと検証環境**の在り方はどうか。

2．量子暗号通信の広域テストベッドの充実・強化

- 総務省・NICTが展開している量子暗号通信の広域テストベッドの充実・強化、利用促進のあり方はどうか。
- **衛星を含む都市間の量子暗号通信ネットワークの構築**をどう推進すべきか。また、**都市間～全国規模**への拡大につなげる方策の在り方はどうか。

③量子セキュリティ・量子ネットワークの高度化

1．量子インターネットの研究開発の方向性

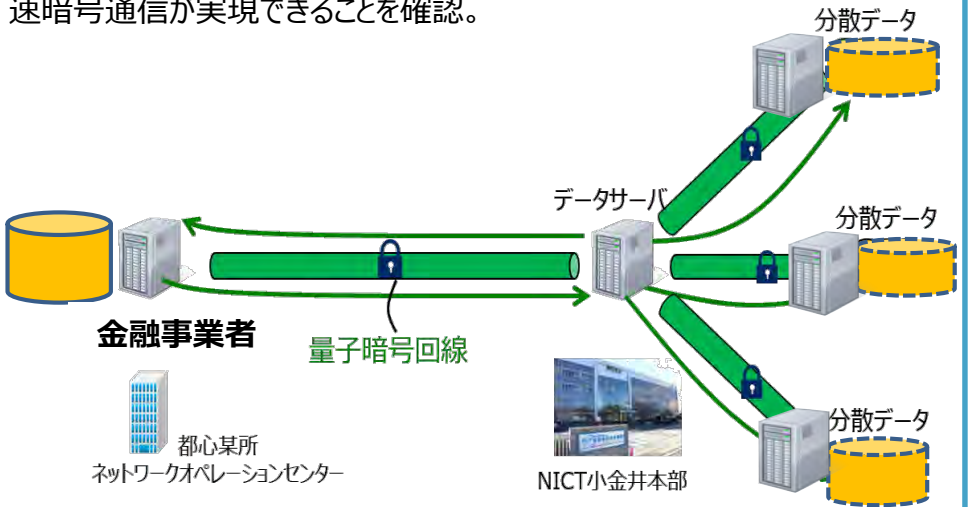
- 量子暗号通信や量子コンピュータを接続できる量子インターネット等を含む将来技術の研究開発・導入ロードマップはどうあるべきか

①－１　量子セキュリティ・量子ネットワークのユーザ産業の振興・拡大

- 量子セキュリティ・量子ネットワークを利用する様々なユーザ産業の発掘・拡大（参画促進、裾野拡大によるマーケット創造）、産業振興に向けた方策はどうあるべきか。
- 新たなユーザを訴求する魅力的なユースケースづくりの在り方はどうか。
- 金融や医療・ゲノム等の個別の事業領域における産業振興・利用促進のあり方。
- アンカーテナンシー/アーリーアダプタの役割を担う行政機関への利用促進のあり方。
- 日本企業が、海外ユーザに向けたサービス提供をサポートする取り組みはどうあるべきか。

実証事例（金融領域）

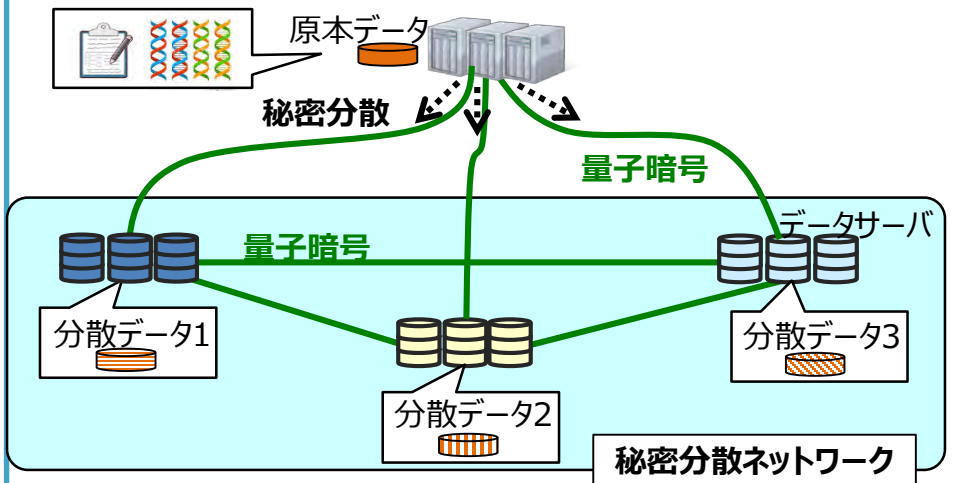
金融分野において、野村ホールディングス、野村證券、NICT、東芝、NECは、金融機関が保有する顧客情報、**株式取引情報等の疑似データの秘匿伝送実証、遠隔の複数サーバでの分散保管実証**を行い、高秘匿・高速暗号通信が実現できることを確認。



・NICTプレスリリース,大容量金融取引データの量子暗号による高秘匿通信・低遅延伝送の検証実験に成功,2022年1月14日, https://www.nict.go.jp/press/2022/01/14-1.html

実証事例（医療・ゲノム領域）

医療・ゲノム分野において、東芝、東北大学東北メディカル・メガバンク機構、東北大学病院、NICTは、**量子暗号通信技術と秘密分散技術を組み合わせたデータ分散保管技術を開発**し、大規模ゲノム解析データを複数拠点に分散して安全にバックアップ保管する実証実験に世界で初めて成功。



・NICTプレスリリース,量子暗号通信技術と秘密分散技術を活用しゲノム解析データの分散保管の実証に成功～ゲノム研究・ゲノム医療分野における安全なデータ管理に貢献～,2021年８月26日, https://www.nict.go.jp/press/2021/08/26-1.html

産業界における協議会設立

・産業界では、量子技術の応用を通じた中長期的な新産業を創出するために、2021年に量子技術における新産業創出協議会（Q-STAR）が設立

Quantum STrategic industry Alliance for Revolution
Q-STAR

①－2 量子セキュリティ・量子ネットワークの事業化支援・国際競争力強化

- 今後、国内ベンダー企業の勝ち筋となるビジネスモデル、熾烈な国際競争に劣後しないための国際競争力強化等の在り方はどうか。
- 利用支援サービス（アプリケーション）を提供する民間事業者のビジネスモデルや主体の在り方はどうか。
- 新たな企業の参画に向けた方策はどうあるべきか。

事業化への取り組み（国内ベンダー）

・東芝は世界No1性能の量子暗号通信の商用機をリリース。
（300kbps@50km）

東芝製QKD装置

（東芝ウェブサイトより）

・NECは試作機を用いて厳しい環境での長期安定動作を実証中。

NEC製QKD装置試作機

（NECウェブサイトより）

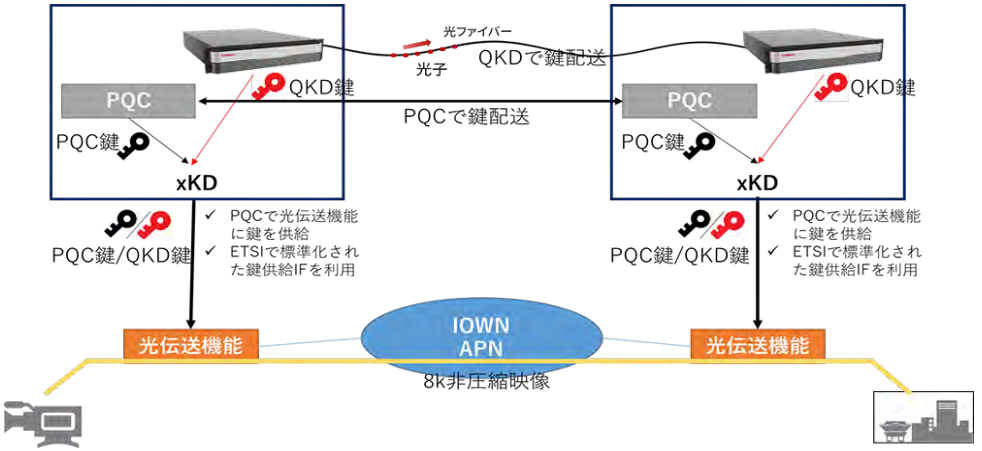
・量子インターネットの実用化を目指すLQUOMは量子もつれを用いた量子暗号通信装置を開発。
（10 kbps @ 10 dB loss）

LQUOM製量子暗号通信装置

（LQUOMウェブサイトより）

事業化への取り組み（サービスプロバイダ）

・東芝デジタルソリューションズとNTTは共同で、 量子計算機に対しても安全な技術として量子力学の原理に基づき情報理論的に安全性を担保するQKDと、計算量的複雑さにより安全性を担保する耐量子計算機暗号PQCを組み合わせた、大容量・低遅延光トランスポートネットワークの実装と動作検証に成功。



・東芝デジタルソリューションズ プレスリリース,量子鍵配送と耐量子計算機暗号を組み合わせた大容量・低遅延光トランスポートネットワークの検証に成功～量子計算機に対しても安全なオール光ネットワークの実現へ～,2021年11月5日,
https://www.global.toshiba/jp/company/digitalsolution/news/2021/1105.html
・日本電信電話株式会社,次世代の高安全な暗号技術を適用した光トランスポートネットワーク技術を開発～IOWNを支える高安全・大容量・低遅延な光伝送の実現へ～,2021年11月5日,
https://group.ntt/jp/newsrelease/2021/11/05/211105b.html

①－3　量子暗号通信機器の国内認証基盤構築の推進

- 世界初のQKD装置のCC評価認証に向けて、国内認証制度、特に評価機関はどうあるべきか。
- 国内認証制度をエコシステムとして自律化するための方策はどうあるべきか。
- 認証制度に関わる国際連携の在り方はどうか。

CC評価認証

・CC (Common Criteria) とは、情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための**国際標準規格**。

・CCによって、情報技術製品のセキュリティの度合いを、仕様書やガイダンス、開発プロセスなど様々な視点から系統的に評価できるようになる。消費者（調達者）は、導入を検討している製品を**共通の基準で比較すること**ができ、必要なセキュリティレベルに応じて必要な機能を具備し、運用や管理まで考慮した製品やシステムを、適正なコストで導入することが可能となる。

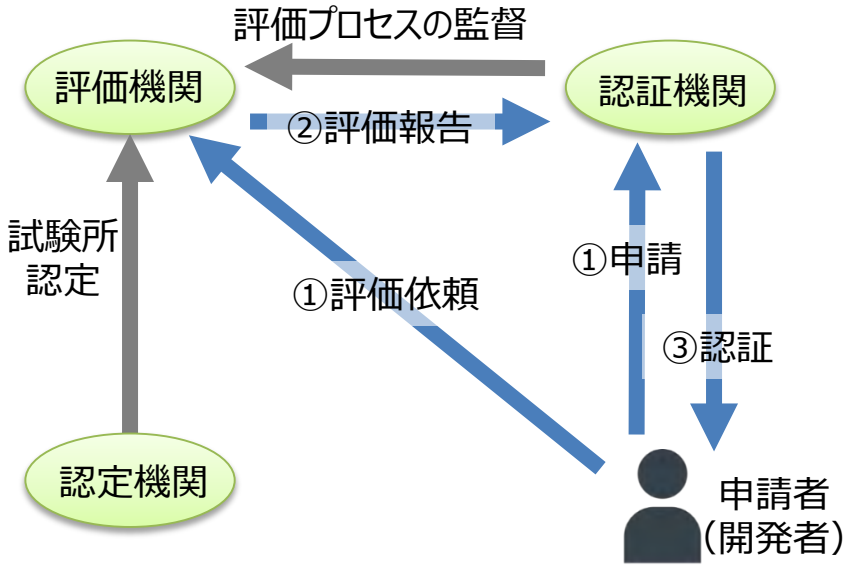
IPA「CC(ISO/IEC 15408)概説」より

CC評価認証制度確立に向けた現状と課題

・セキュリティ要求使用書（PP:Protection Profile）の作成
・装置のセキュリティ評価手法書（EMD:Evaluation Methodology Documents）の作成
　・PP及びEMDはETSIにおいて日本が主導して策定中。

・継続的な運用とそのための**エコシステムの構築**
　・製品**評価（認証）施設と装置**
　・製品**評価・認証人材**の育成
　・**ビジネスモデル**

（参考）既存のCC評価認証制度（JISEC）



IPA「評価認証制度（JISEC）概要)」をもとに総務省作成

②－１　量子・古典ハイブリッドによる総合的アーキテクチャの検証

- 量子暗号、耐量子計算機暗号、量子ストリーミング暗号等の多様な量子・古典暗号のベストミックスと検証環境の在り方はどうか。
- 古典アーキテクチャからの移行（マイグレーション）はどうあるべきか。
- 量子セキュアクラウド、量子暗号、量子計算機まで含む量子統合アーキテクチャ（量子技術プラットフォーム）の在り方はどうか。

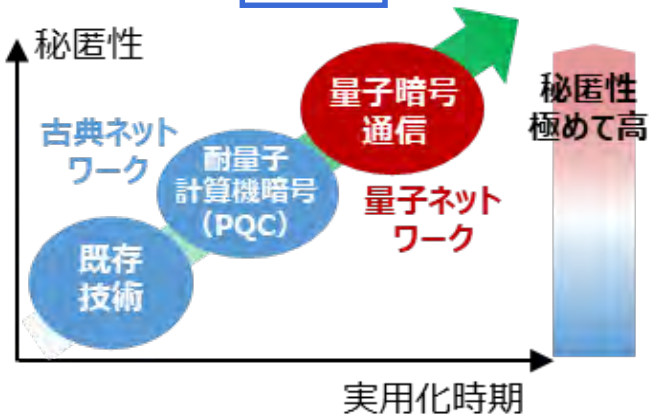
QKD性能の見通し

・現在、世界最速のQKD装置の性能は、
300kbps@50km。

・量子技術イノベーション戦略における目標では、
2040年までに1Gbpsで数100km程度(*)

(*)量子技術イノベーション戦略 ロードマップ(令和４年４月22日改訂)より

用途に応じた各暗号方式の効果的な使い分け



【将来の総合的なセキュリティのイメージ】

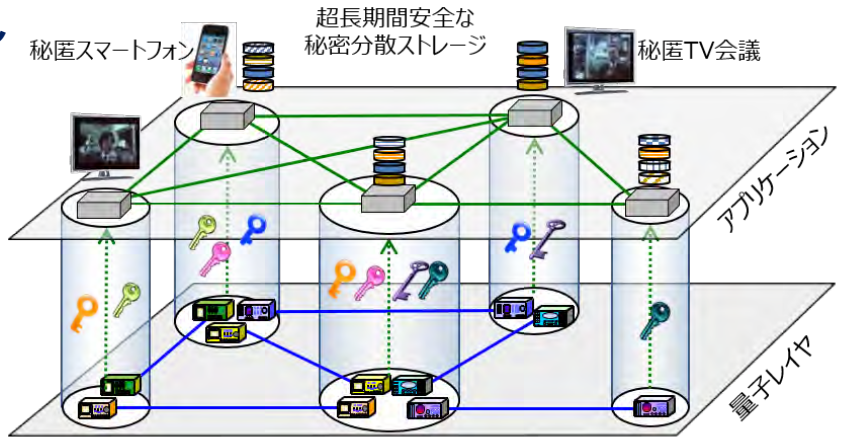
量子未来社会ビジョン（概要）（令和４年４月22日決定）より

②－2　量子暗号通信の広域テストベッドの充実・強化

- 総務省・NICTが展開している量子暗号通信の広域テストベッドの充実・強化、利用促進の在り方はどうか。
- 利用実証拡大を事業化につなげる方策の在り方はどうか。
- 衛星までを含む都市間の量子暗号通信ネットワークの構築をどう推進すべきか。

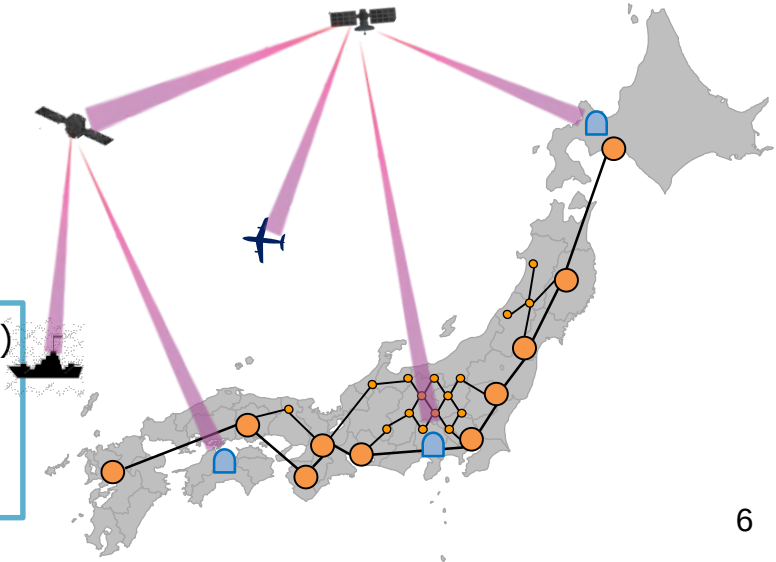
量子暗号通信の広域テストベッド　～東京QKDネットワーク～

- 2010年に構築された「東京QKDネットワーク」は**量子暗号通信テストベッド**として、**都市間(大手町～小金井　45km)**を敷設光ファイバで実際に結ぶとともに、**複数の環境・通信方式**を想定した環境を用意し、我が国の量子暗号通信に係る研究開発の基盤的設備として活用
- R3年度補正事業では、複数拠点間を結び商用網に見立てた量子暗号通信の広域テストベッドを構築
- 東京QKDネットワークにおける量子暗号装置の長期運用や開発された仕様を**国際標準**（ITU-T Y.3800シリーズ）に反映



量子鍵配送ネットワーク
(Tokyo QKD Network)

衛星までを含む都市間の量子暗号通信ネットワークの構築をどう推進すべきか。



例　NICTにおける拡張ロードマップ案

第1段階（2022年頃）：関東圏（量子コンピュータ、量子暗号・中継、光格子時計）
第2段階（2025年頃）：都市間（仙台、東京、大阪など、量子技術の集約）
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

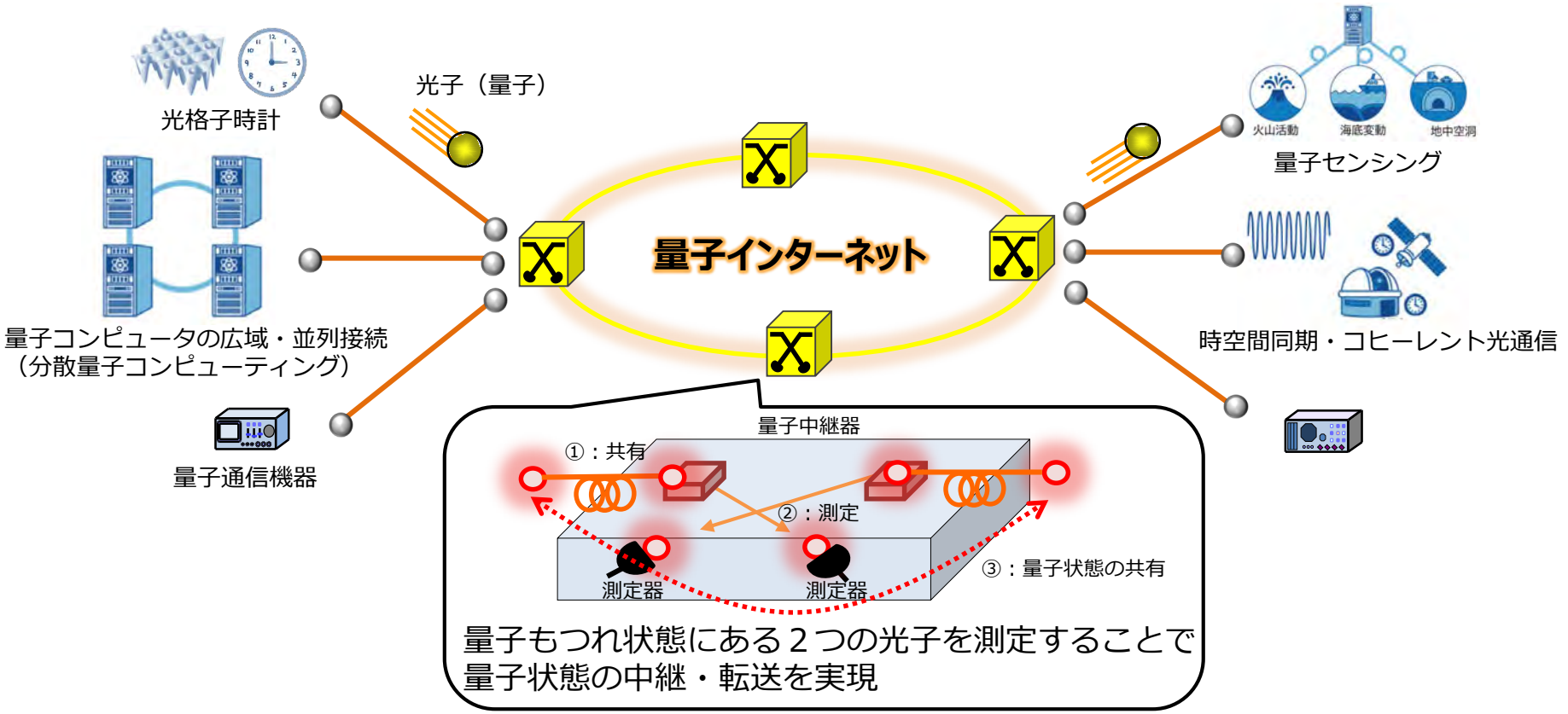
NICT量子ネットワークホワイトペーパーより

③－1　量子インターネットの研究開発の方向性

- 量子暗号通信や量子コンピュータを接続できる量子インターネット等を含む将来技術の研究開発・ロードマップはどうあるべきか。

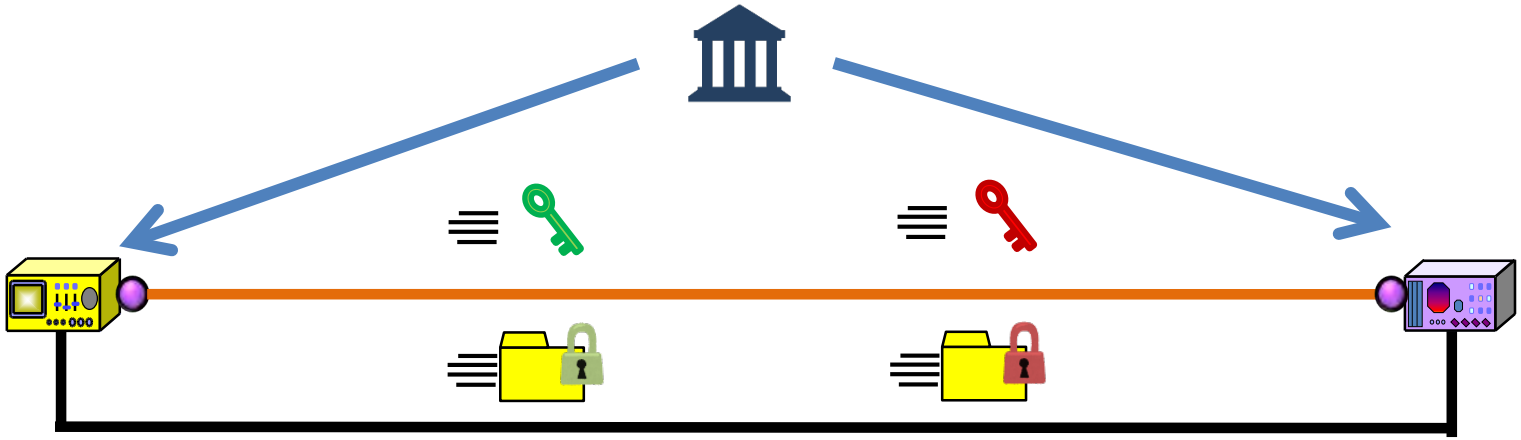
量子インターネットとは

- 量子コンピュータ・センサ等の量子情報を生成・処理する**量子通信機器・デバイスを相互に接続**し、**大規模な量子情報の広域ネットワーク上での流通を円滑化。**
- 量子状態は**複製することが不可能**なので、通信路の損失による信号の減衰を増幅で回復することはできない。そのため**量子通信の長距離化には量子中継が重要なコア技術の一つとなる。**



（参考） 用途に応じた暗号方式の例

- データの送受信の際には、様々な暗号方式を用いて、鍵交換、データ暗号化、デジタル署名等が行われる
- データの重要度やコストに応じて暗号方式を適切に組み合わせることで、より安全かつ効率的なデータ送受信が可能となる。



名前	暗号方式	主な用途
RSA等	公開鍵暗号	デジタル署名、鍵交換
CRYSTALS-Kyber等	公開鍵暗号	デジタル署名、鍵交換
BB-84,CV-QKD等	量子鍵配送（QKD）	鍵交換
AES	共通鍵暗号	データ暗号化
OTP	共通鍵暗号	データ暗号化
QNSC（Y-00等）	量子ストリーミング暗号	データ暗号化