超長期秘匿性実現を目指して 量子鍵配送・量子セキュアクラウドのご紹介

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

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

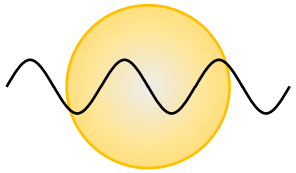
量子とは

・量子とは、粒子と波の性質をあわせ持った、とても小さな物質やエネルギーの単位のことです.
・量子の世界は、ナノサイズ（1メートルの10億分の1）あるいはそれよりも小さな世界です.
・このような極めて小さな世界では，私たちの身の回りにある物理法則は通用せず，
「量子力学」というとても不思議な法則に従っています.
・量子の特性を使うと，今までできなかったことができるようになります.

量子コンピュータ

計算に使う

現実的な時間で
不可能であった大規模な
計算を短時間で実現

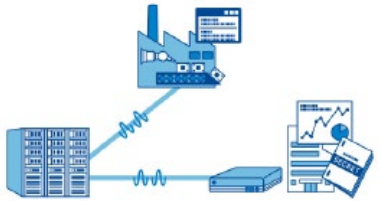


量子＝原子、電子、光子、、、

通信に使う

量子通信

完全秘匿通信が可能



センシングに使う

量子センサ

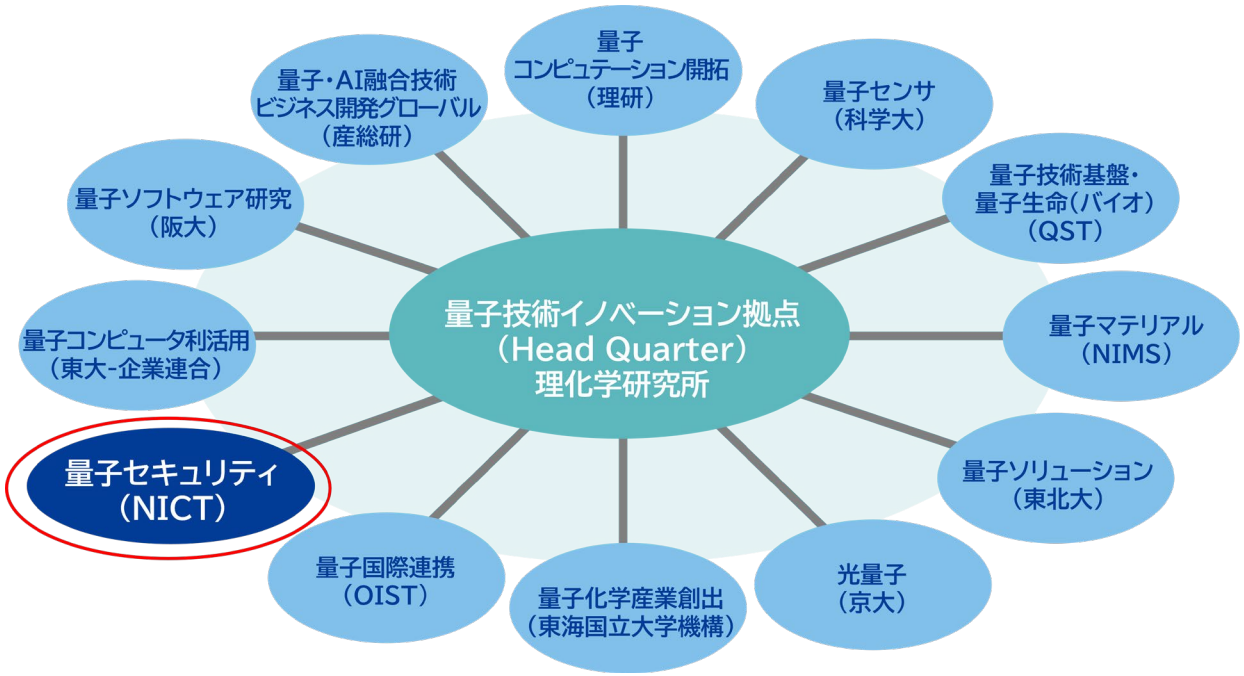
今まで見えなかったものが見えるようになる

医療への応用

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　内閣 統合イノベーション戦略推進会議報告）に基づき NICTは量子セキュリティ拠点に指定されました.
- 現在，12企業と連携規約を締結，量子セキュリティ技術に関する研究開発等を実施中です.

量子セキュリティ・協創棟（小金井）



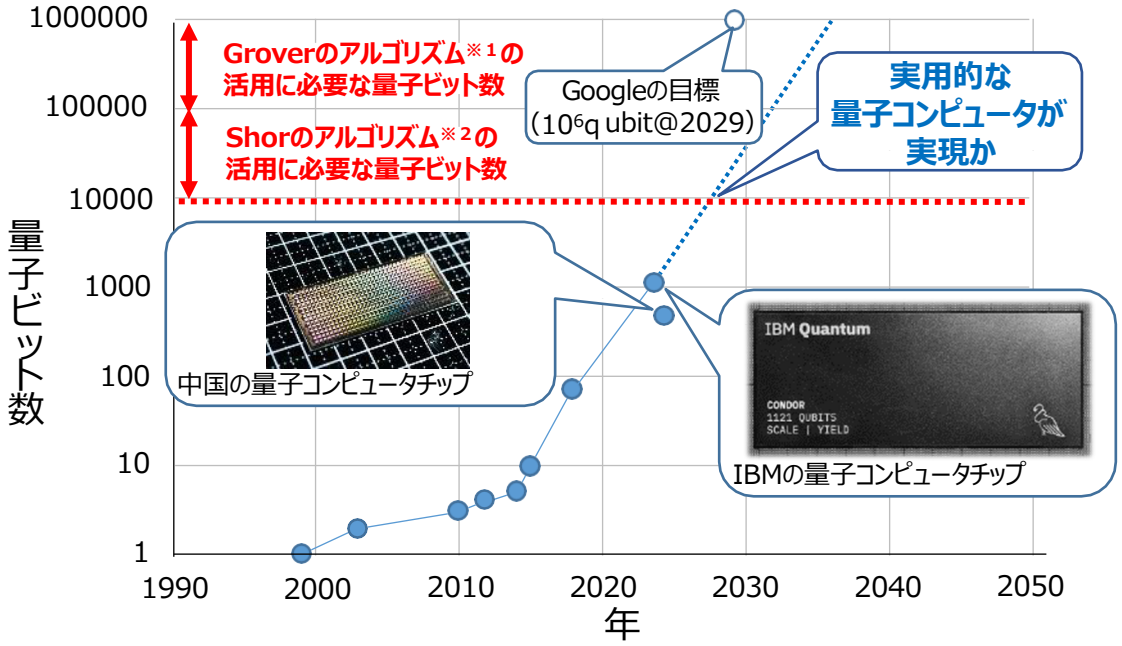
主に将来に渡り盗聴の脅威のない暗号通信を研究

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
- 京セラ株式会社
- 株式会社東芝
- 日本電気株式会社
- TOPPANデジタル株式会社
- 株式会社ワイ・デー・ケー
- 野村ホールディングス株式会社
- 株式会社大和証券グループ本社
- 株式会社みずほフィナンシャルグループ
- 株式会社マクニカ

暗号への脅威　進む量子コンピュータ開発

- ✓ 近年，**国際的な競争の激化に伴い、量子コンピュータに関する研究開発が加速しており，**米国NIST（国立標準技術研究所）は暗号鍵長2048ビットのRSA暗号を解読可能な**量子コンピューターが2030年頃に実現することを想定.**
- ✓ **攻撃者は**実用的な量子コンピュータの実現を見越して**既に暗号通信の盗聴・保存※を始めている**と考えられており，対策が急務となっている.
  ※Harvest now, decrypt later攻撃



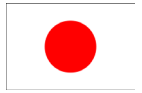
参考：https://www.jst.go.jp/crds/sympo/20190829/pdf/02.pdf

※１　Shorのアルゴリズム　：RSA等の公開鍵暗号方式の解読を**大幅に高速化**
※２　Groverのアルゴリズム　：AES等の共通鍵暗号方式の解読を高速化
※３　誤り訂正　：多数の量子ビットを用いて計算の精度を高める技術

国内外での最近の主な発表

- Googleが、2029年までに100万量子ビットを目指す計画を発表.　（2021年５月）
- Googleが、72量子ビットを用いて，量子コンピュータにおける誤り訂正※３を実証。（2023年２月）
- IBMが、1121量子ビットの量子コンピュータ「Condor」を発表。（2023年12月）

- 中国科学院が、504量子ビットの量子コンピュータチップをQuantumCTek社に納入.　（2024年４月）

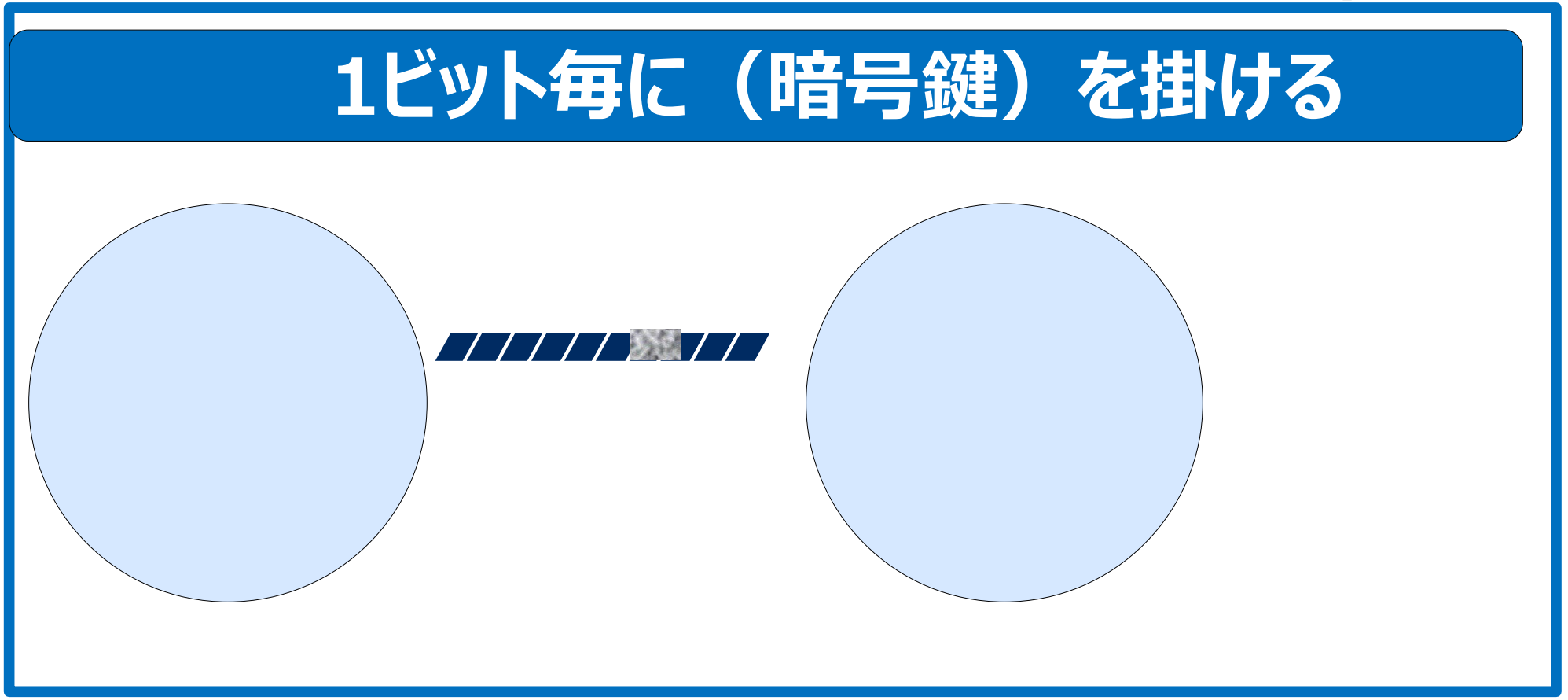


- 理化学研究所が、256量子ビットの国産量子コンピュータを開発。1000量子ビットに拡張可能な構造を採用.　（2025年4月）

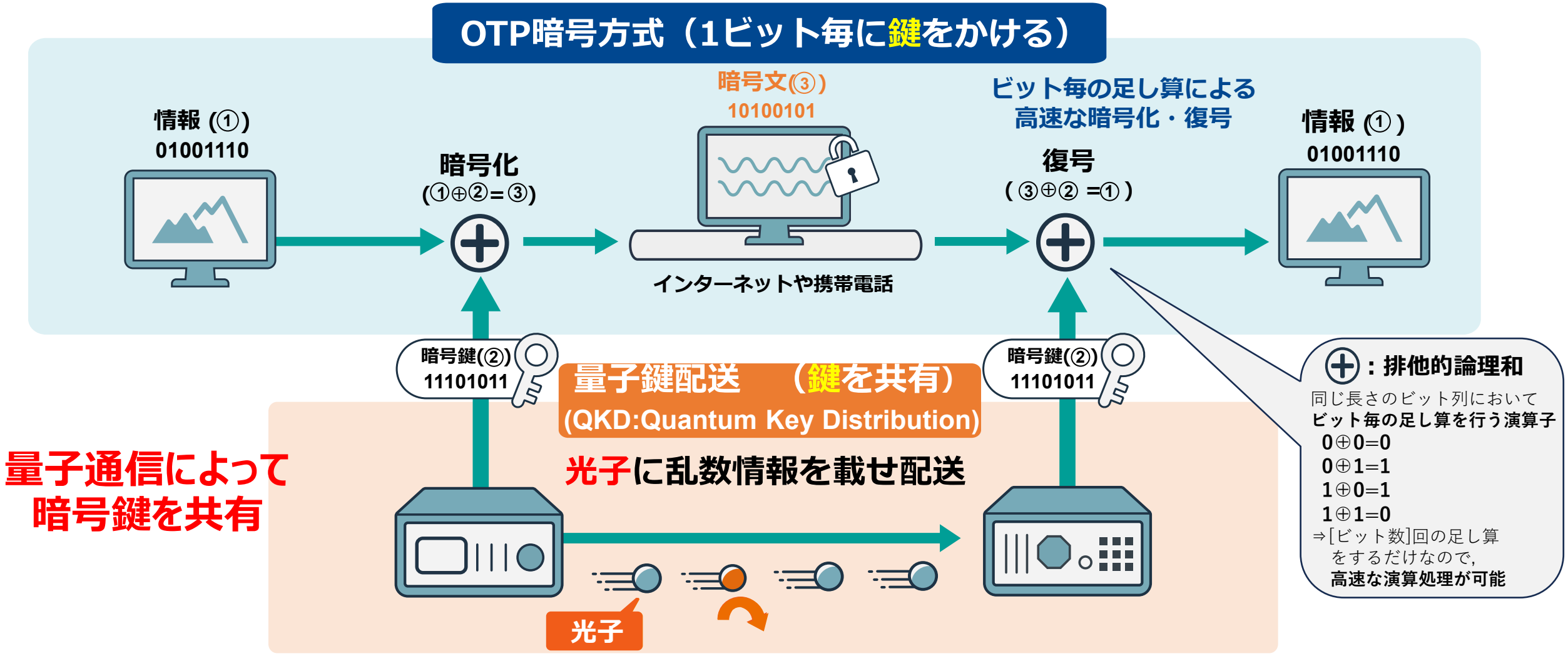
- フランスのPasqal社が2025年後半に、200量子ビットの量子コンピュータをサウジアラビアのアラムコ社に納入予定と発表.　（2024年５月）

完全秘匿通信　乱数表が共有できれば可能！

完全秘匿通信Vernam’s ワンタイムパッド（One-time pad）暗号



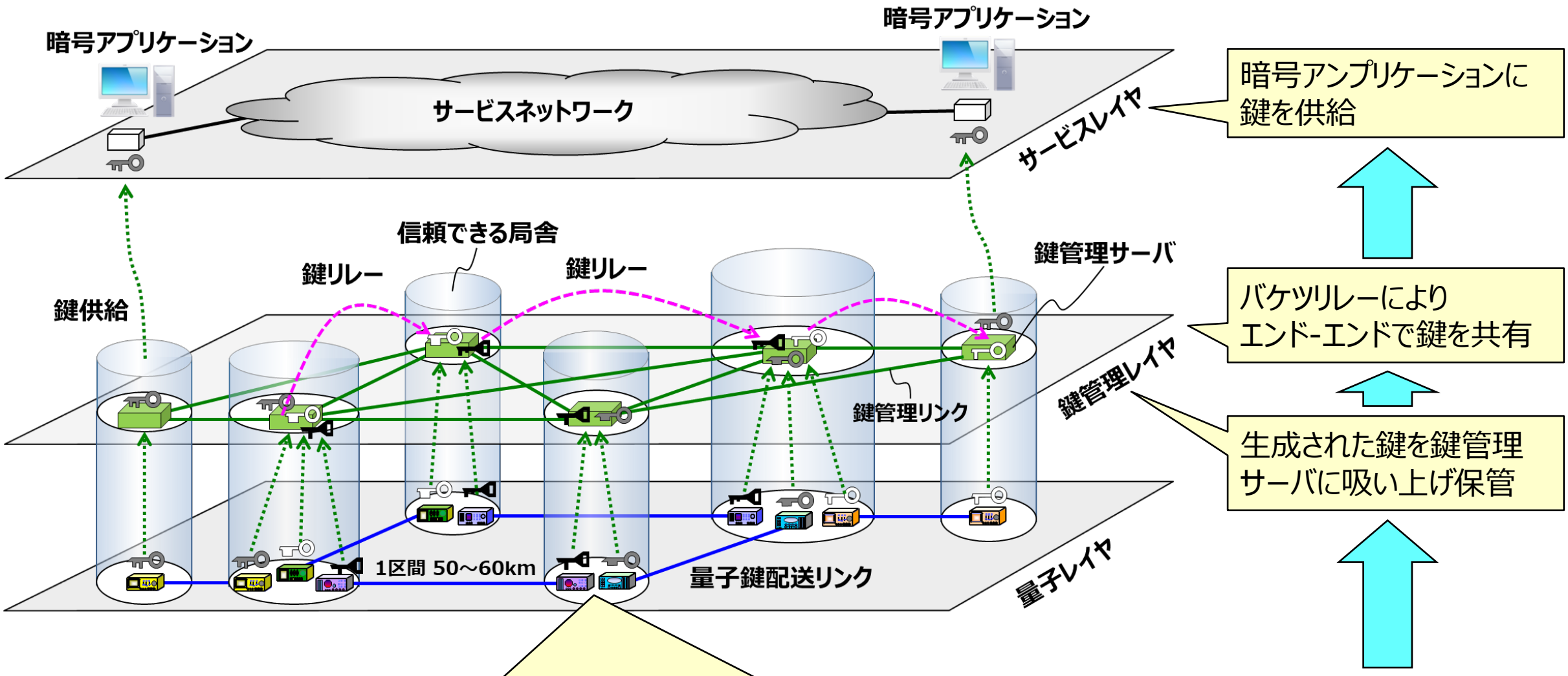
量子暗号 OTP暗号方式×量子鍵配送（QKD）



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、
盗聴を検知したらその乱数情報は捨てる
⇒信頼できる乱数情報のみを鍵として利用

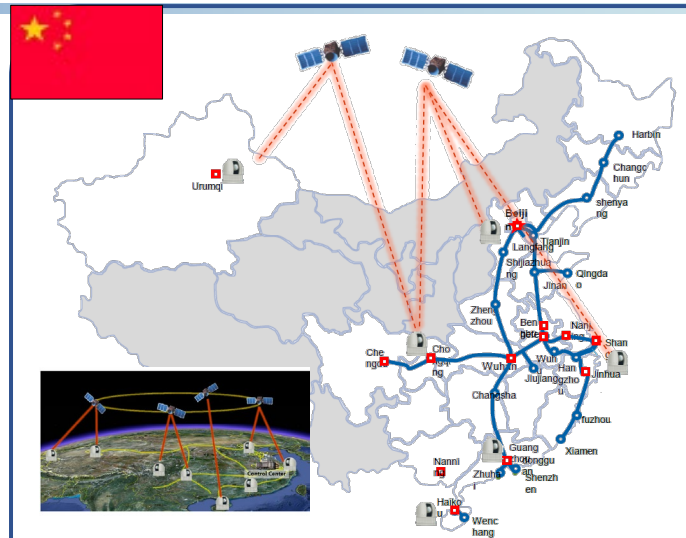
現在の量子暗号ネットワーク



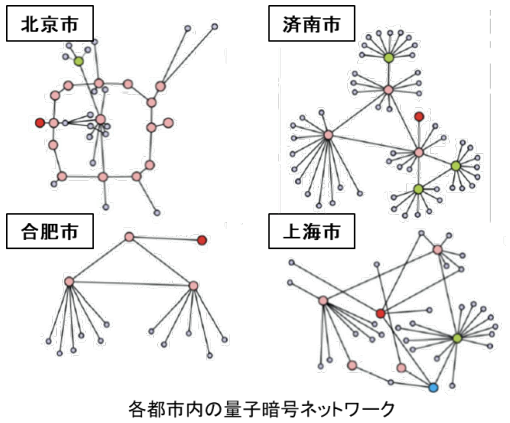
諸外国のQKDネットワーク整備

- ✓ CQE（米国の研究開発推進機関）は、エネルギー省アルゴンヌ国立研究所が2020年に構築した89mile（144km）のQKDネットワークを拡張し、124マイル（200km）のネットワークを整備。
- ✓ シカゴ南部（シカゴ大

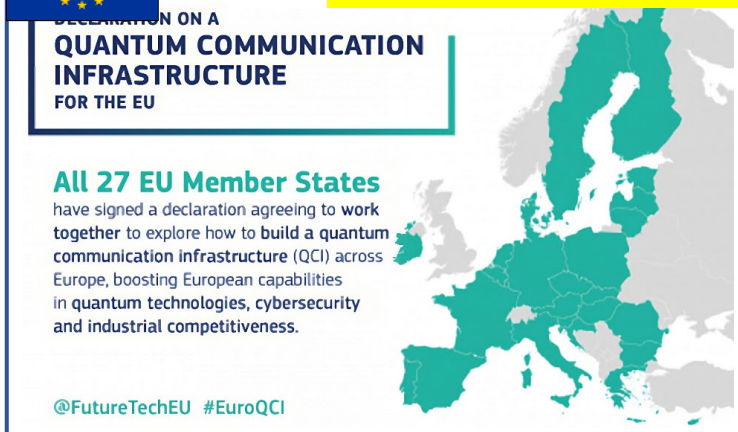
諸外国では、数100km以上の規模の広域ネットワーク化の動きが加速



基幹となる量子暗号ネットワーク
（総延長10,000km以上）

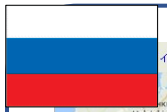


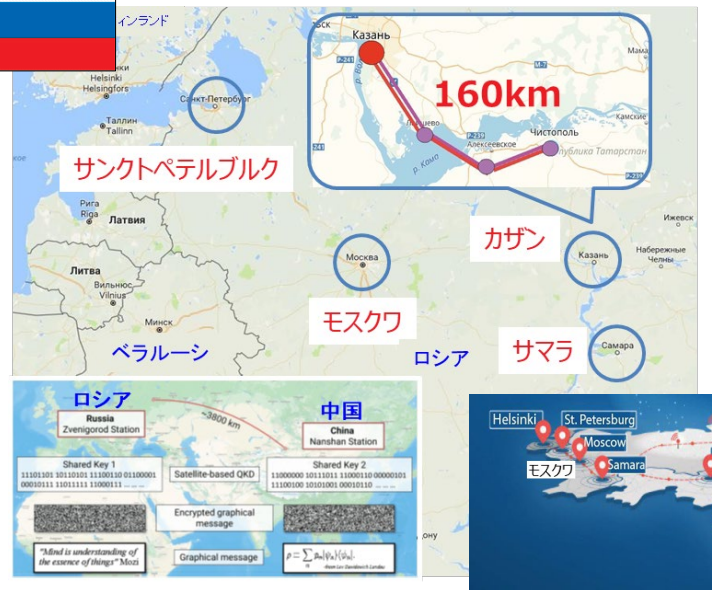
各都市内の量子暗号ネットワーク



- ✓ EuroQCI衛星の仕様を欧州委員会とESAが策定中。
- ✓ 試験衛星１号機のEagle-1は、2025年末もしくは、2026年初頭に打ち上げ予定。

- ✓ 2021年7月にアイルランドがEuroQCI宣言に署名し、全27加盟国の参加が確定。
- ✓ 2027年までにEuroQCIの構築を進める予定。



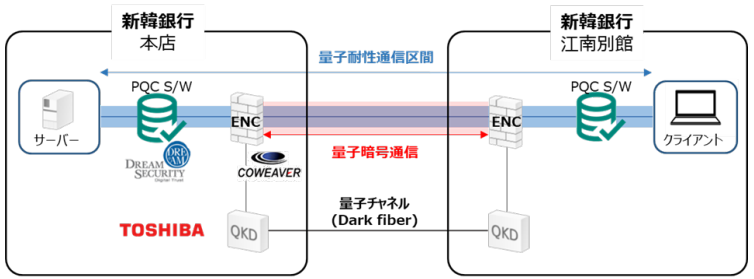


- ✓ 2019年、イトモ大学とカザン量子センターが、160kmのQKD網を構築。その他、サンクトペテルブルク、モスクワ、サマラにもQKD網を構築。
- ✓ 2023年12月、モスクワ近郊と中国ウイグル自治区間（約3800km）で、衛星を介した量子暗号通信を実施。

各国での金融関係での使用例

新韓銀行（韓国）
HPログイン（QKDとPQCを階層別に適用）

- 新韓銀行本店（ソウル）と江南別館の約22km区間を結ぶ実証網を構築
- 盗聴をブロックし光回線の物理層を保護するQKDと、インターネットセキュリティプロトコルに適用してホームページログインなどのアプリケーションサービスを保護するPQC公開鍵アルゴリズムによるハイブリッド量子セキュア通信の評価



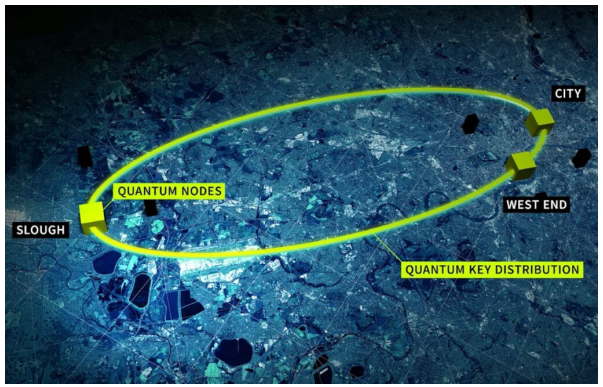
kt ： Quantum-Safe ネットワーク設計及び構築
： 量子保安性能/安定性試験検証

JPモルガン・チェース（米国）
データセンター間での機密データ伝送

- 東芝、Cienaとともに、シンガポールで敷設済みの46 kmの通信ファイバー上にQKDを用いたVPNトンネルを構成し、JPMorgan Chaseの２つのデータセンター間で45日間に渡って量子安全な通信を実現
- JPMorgan Chaseの研究施設内において金融取引（ブロックチェーンアプリケーションの転送）を量子安全にできることを実証

HSBC（英国）
金融取引・ビデオ会議・ワンタイムパッド暗号

- BT・東芝がロンドンに構築した商用量子セキュアメトロネットワークの実証にAWSと共同で参加。
- Canary Wharf本社とバークシャー州スラウ拠点のデータセンター（約62km）間を接続し、金融取引・ビデオ会議・ワンタイムパッド暗号など複数シナリオにおいてQKDを試用したセキュアな伝送を検証



Wells Fargo（米国）
:データセンター間での安全な鍵共有を想定（概念実証）

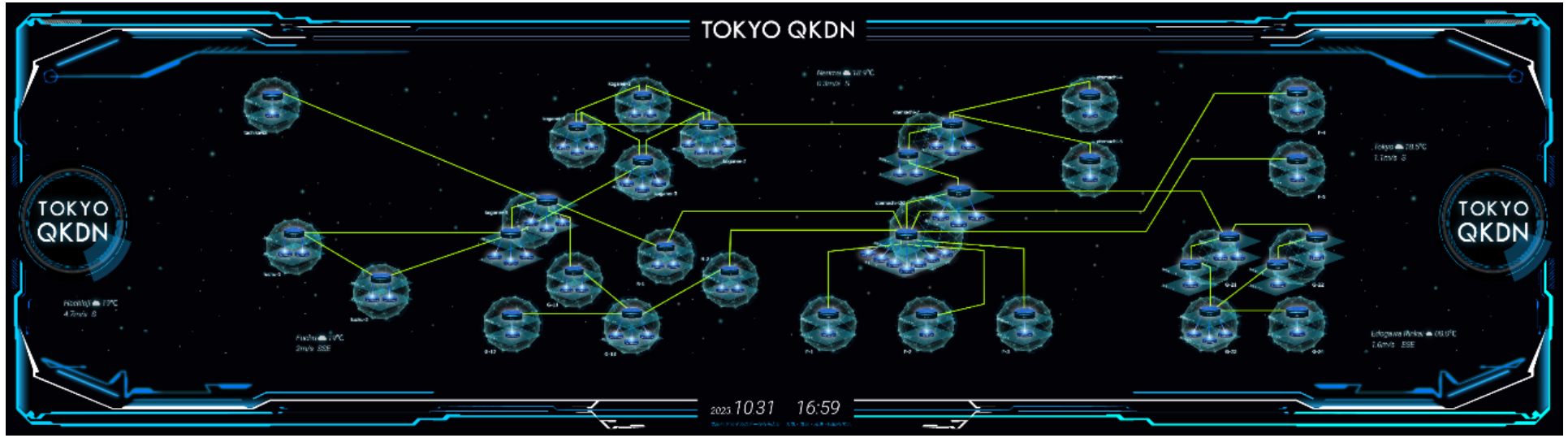
- 東芝QKD装置とCiena社の100Gbpsリンク機器を組み合わせ、2拠点間のデータセンター相互接続における鍵配送を想定し、同社の研究室内にて実証

複数金融機関（シンガポール）
金融サービスにおけるQKD導入可能性を検討（概念実証）

- シンガポール金融管理局(MAS)は2024年、DBS/OCBC/UOB/HSBCシンガポール支店など大手銀行や通信事業者と量子セキュリティ推進の覚書を締結しSpeQtralやSPTel提供のQKD装置による金融サービス向け概念実証を実施

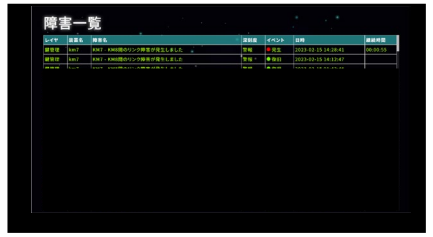
我が国におけるネットワーク　Tokyo QKD Network

- **NICT小金井本部を中核にQKDネットワークの運用実証等を行うため Tokyo QKD Networkを構築　～2011年より運用開始**
- **世界で最も運用実績の長いネットワーク（数10 km 規模）**
- 2023年12月野村ホールディングス株式会社、TOPPANデジタル株式会社、株式会社大和証券グループ本社、株式会社みずほフィナンシャルグループとも直接リンク形成

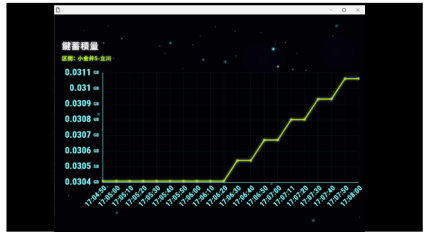


量子鍵配送ネットワーク制御画面

監視GUI(障害一覧)

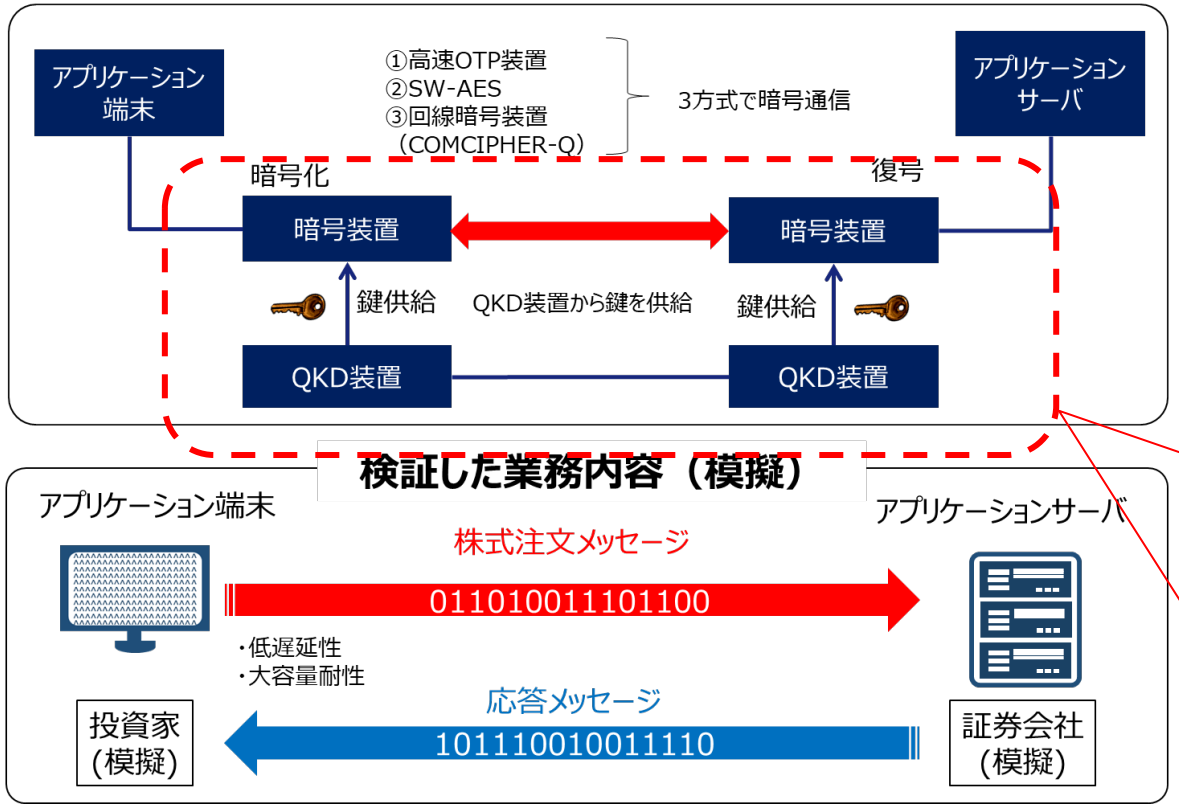


監視GUI(鍵残量)

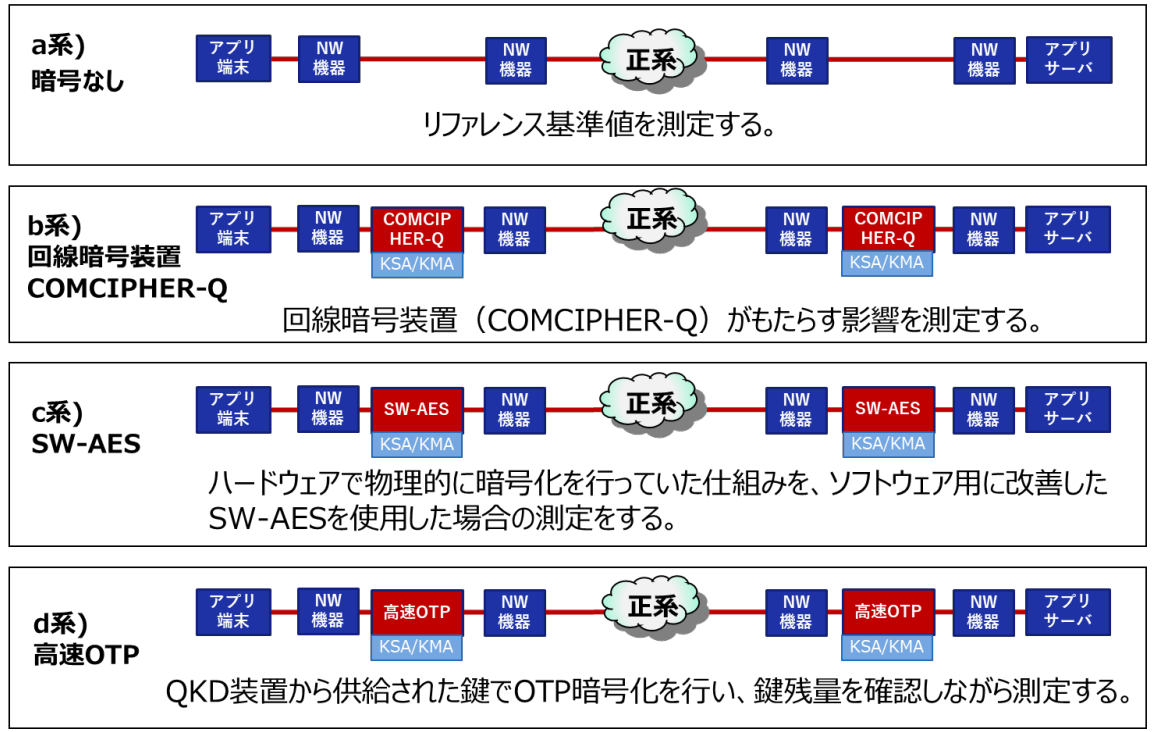


証券取引情報の暗号化信頼性試験

共同検証のシステム構成概要



各系ネットワークのシステム概要



野村HD様　野村證券様と共同で実証　通常の取引量の80倍のデータで実施

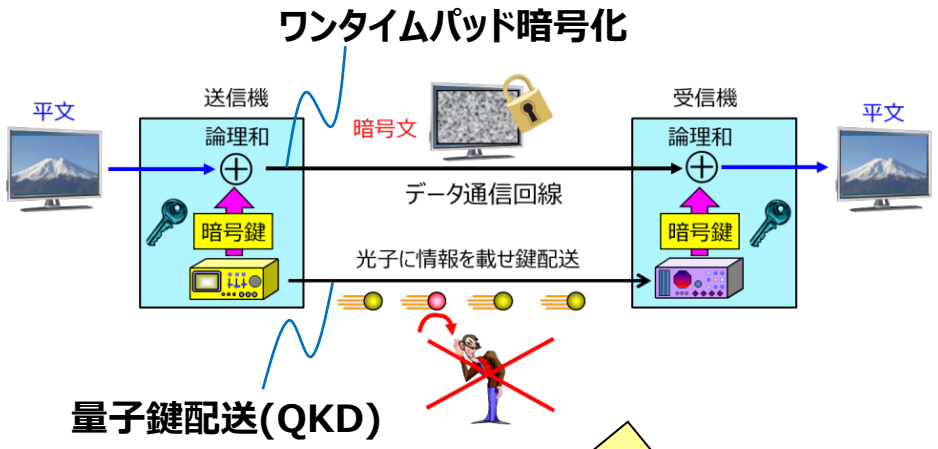
OTPだけでは鍵が不足する危険性があり，鍵の蓄積量が
一定割合を下回ると自動的にAES（例1分に1回鍵リフレシュ）モードに切り替え，運用の持続性を担保

低遅延性と大容量通信耐性を確認

安全なデータ保管　量子セキュアクラウド

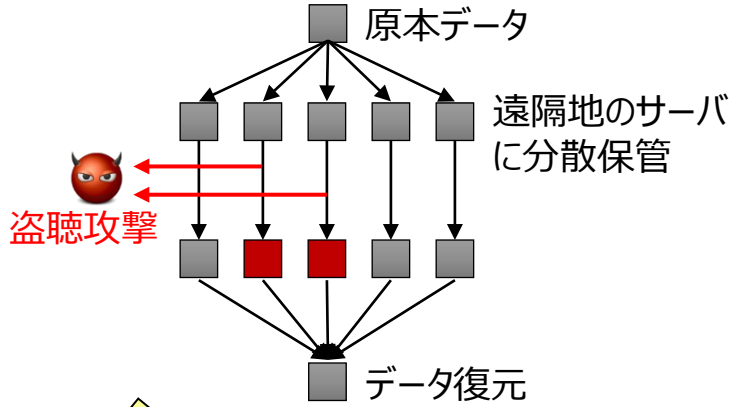
量子鍵配送網

『**どんな計算機でも解読できない**こと』を
証明できる現在唯一の暗号通信方式



秘密分散

原本データを一見乱数に見える複数の
データ（シェア）に**分散し保管**する手法



統合

Fujiwara, et al., Scientific Reports, 6:28988 (2016).
パスワード1つでも情報理論的安全な本人認証を実現（秘匿計算を応用）

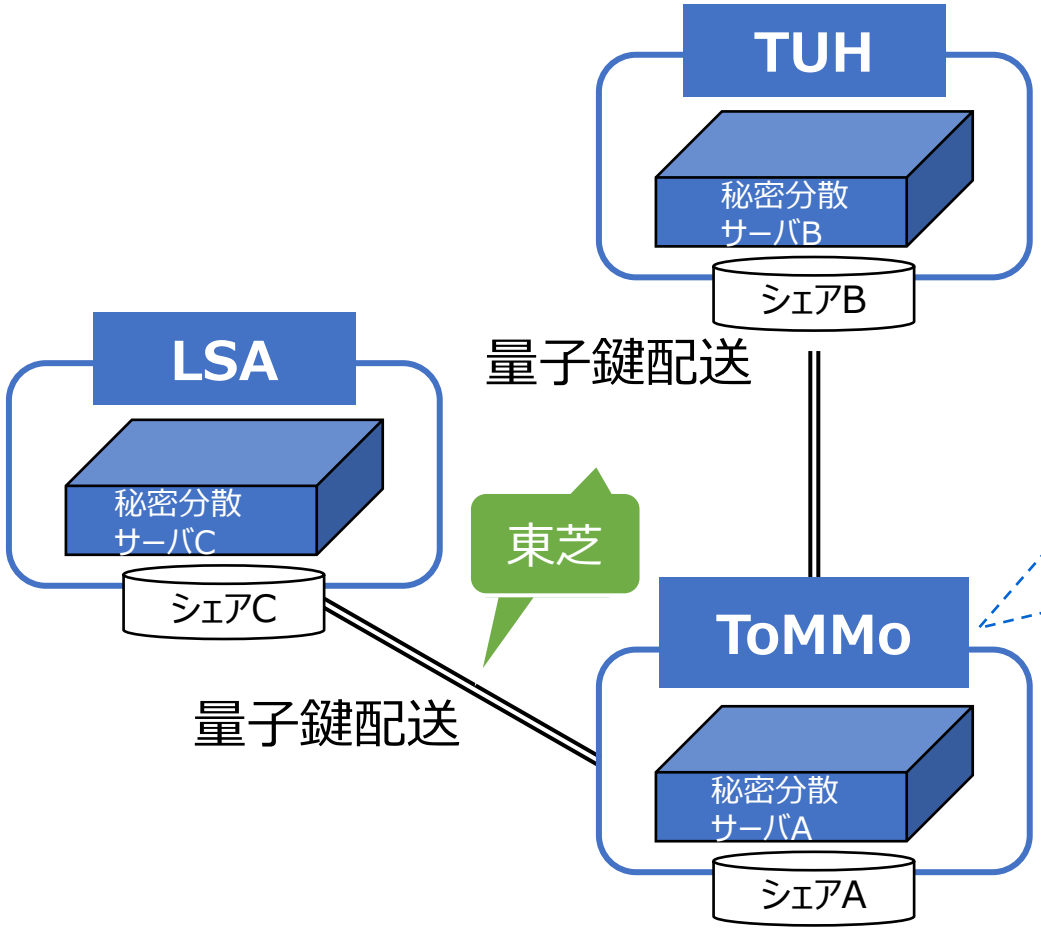
『量子セキュアクラウド』

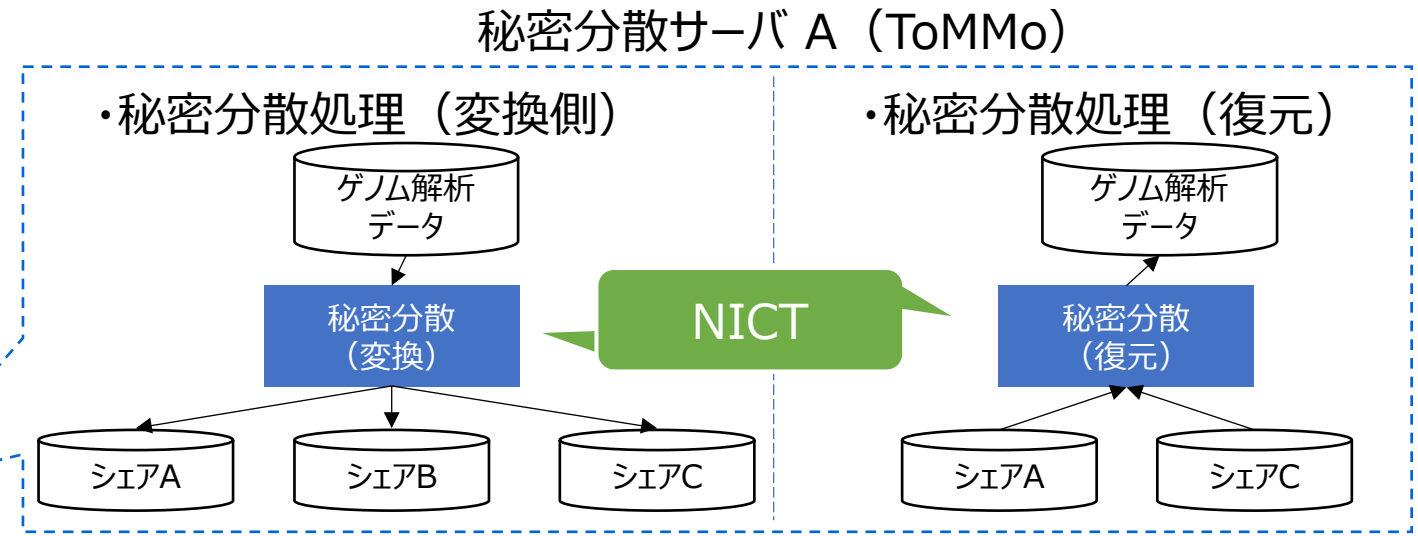
- ✓ **将来にわたり機密漏洩と不正改竄を防ぐ安全なデータ保管を実現**
- ✓ **一部のサーバが棄損した場合でも必要時に原本データを復元可能**
- ✓ **安全なデータの二次利用を実現**

ゲノム情報への適用

世界初　ゲノムデータの情報理論的安全な伝送と保管

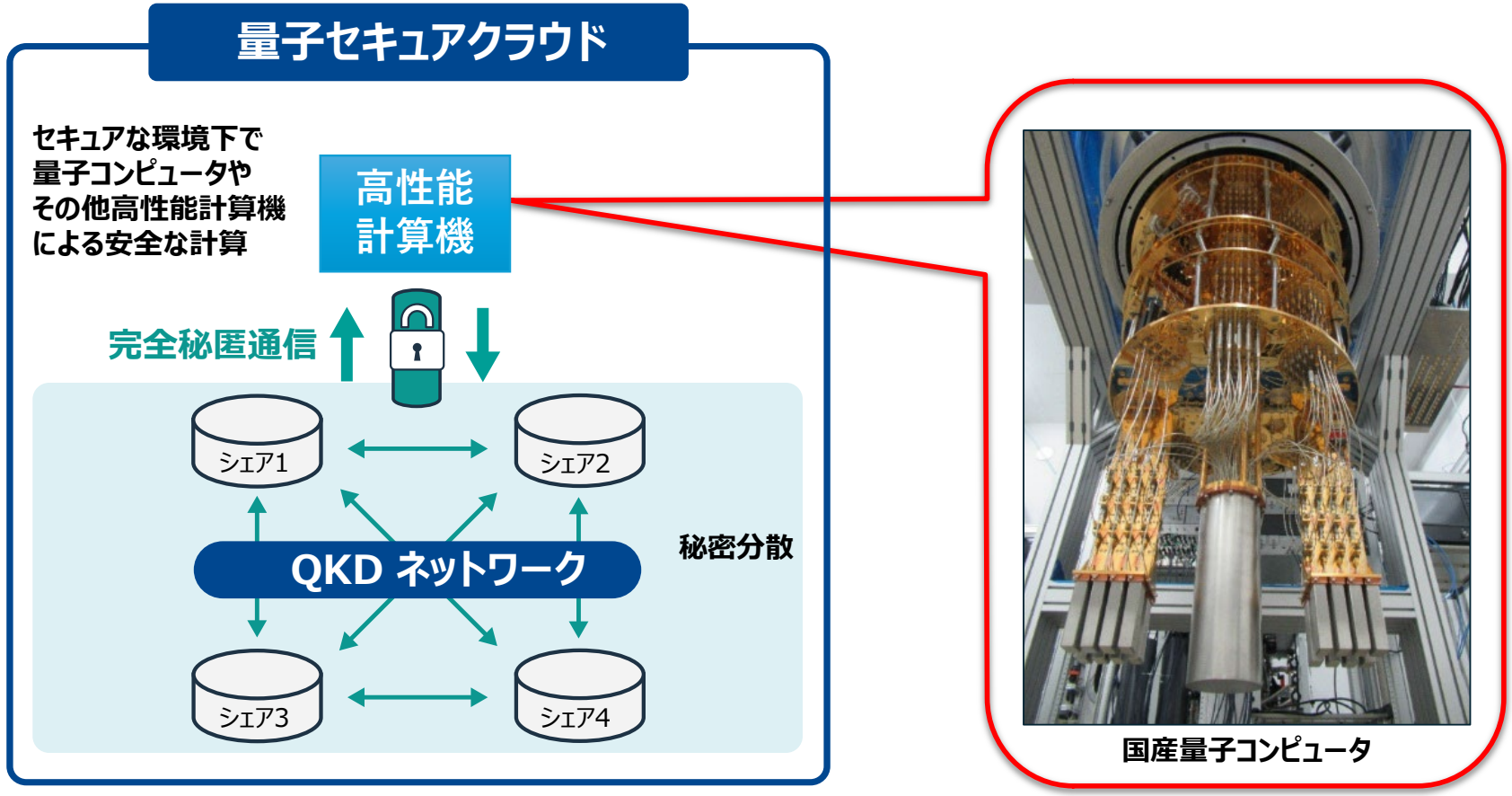
８０GBのデータを秘密分散で数時間で３か所に分散



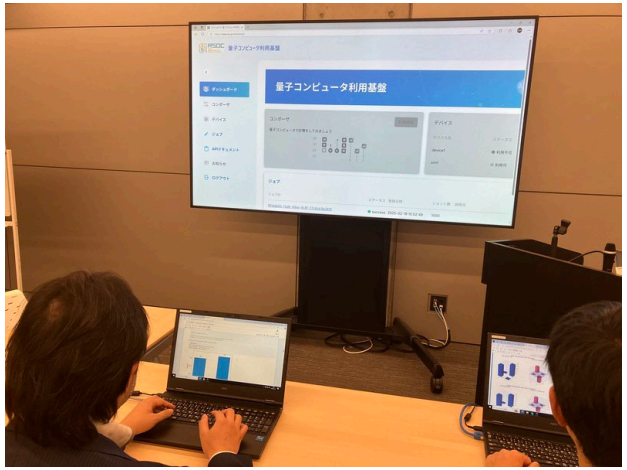


LSA：東芝ライフサイエンス解析センター
ToMMo：東北大学東北メディカル・メガバンク機構
TUH：東北大学病院
NICT：情報通信研究機構

量子セキュアクラウド　量子コンピュータ統合実証



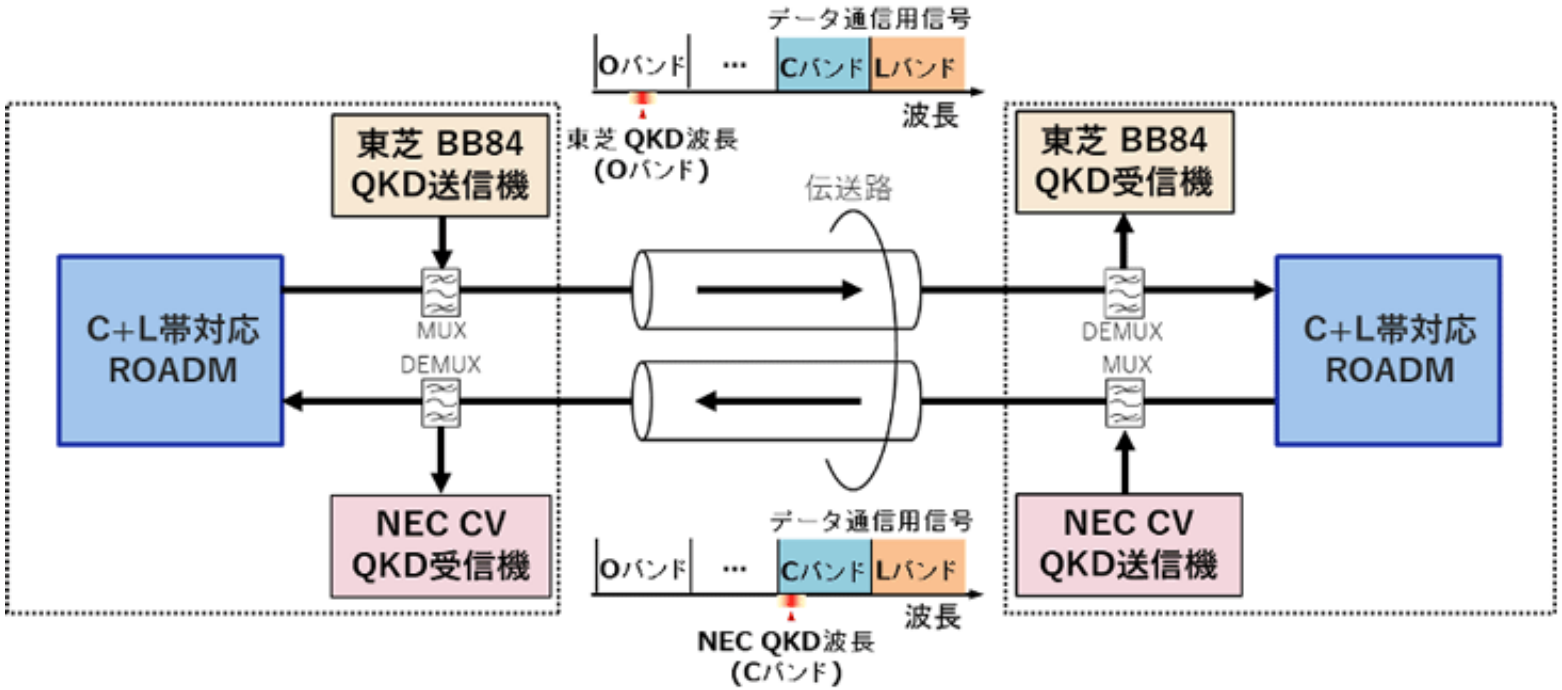
国産量子コンピュータ



NICTからの接続の様子

NICTが研究開発及び運用を進めている量子セキュアクラウドと，理研が中心となって開発した国産ゲート型量子コンピュータを接続し，国産ゲート型量子コンピュータを安全に利用するための相互接続環境を構築しました.
2025年3月13日プレスリリース

次世代通信インフラ化を目指して　IOWNとの統合実証



2025年7月28日
プレスリリース
株式会社東芝
日本電気株式会社
NICT

世界初，IOWN Open APN向け大容量光伝送システム実証環境に量子鍵配送システムを統合，高速データ通信と鍵生成との共存に成功

～通信キャリアの基幹系光ネットワークへ，低コストで安全な量子鍵配送サービスの導入を目指す～

直ぐに使える安全な暗号インフラとしてQKD技術への期待が高まっている

広域QKDNテストベッド構想

実ユーザを巻き込んだユースケースの検証が社会実装の加速に不可欠

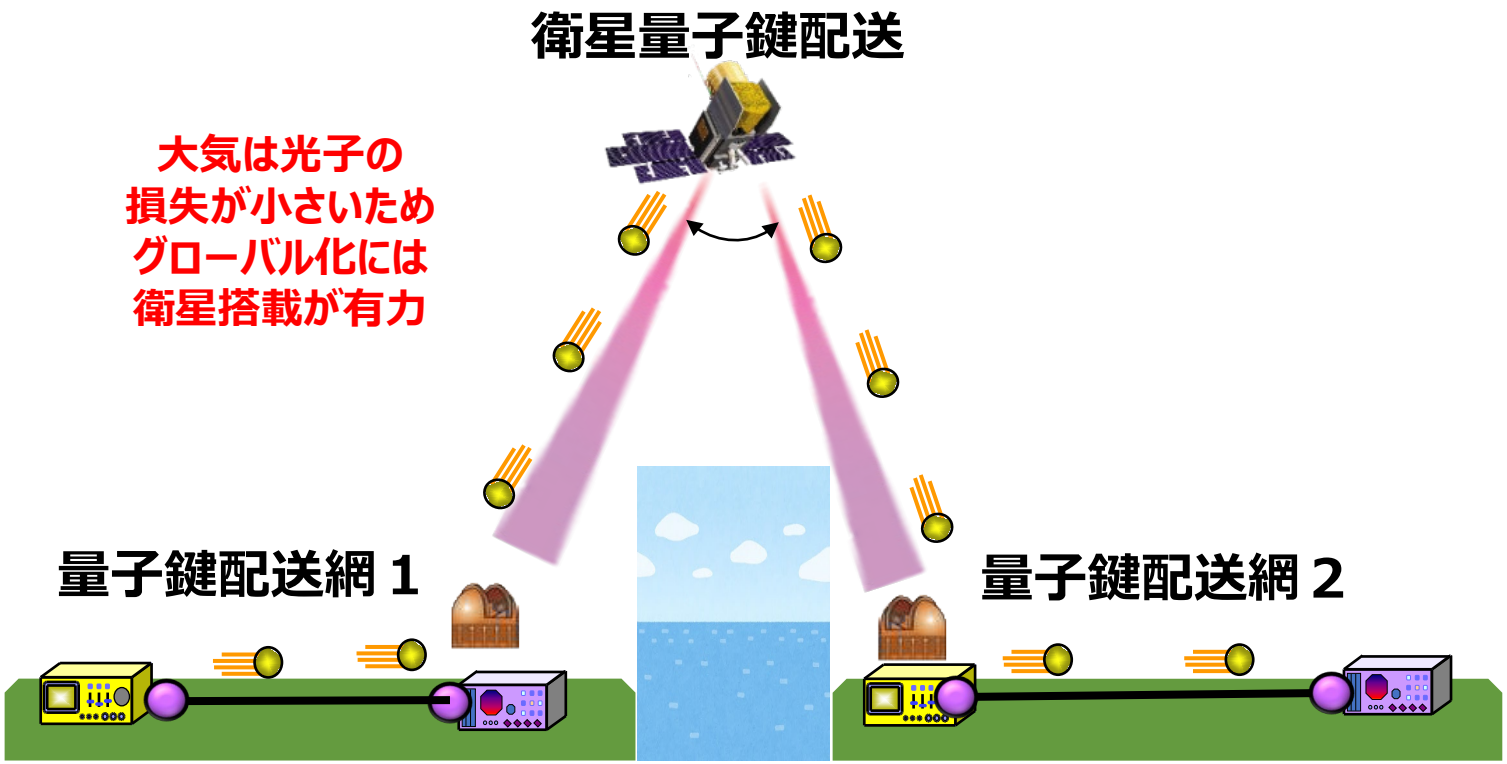
- **金融データの広域バックアップ**
- **ゲノムデータ，臨床データの共有**
- **要配慮情報の安全な解析**

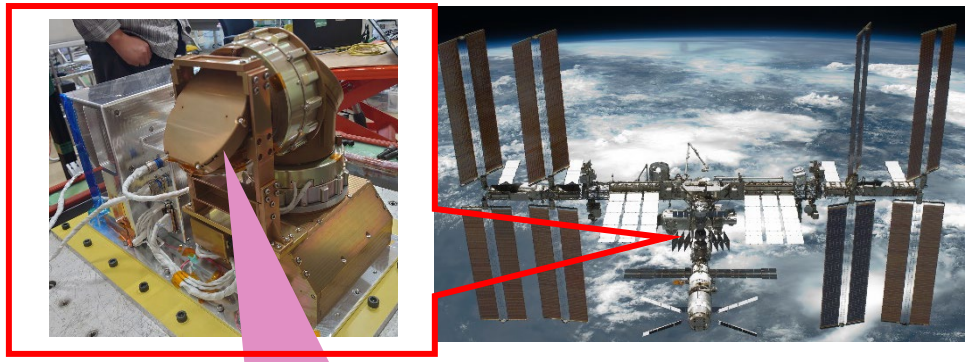
理化学研究所計算科学研究センター

国立循環器病研究センター

国立がん研究センター東病院

量子鍵配送装置を衛星搭載→　サービスエリア拡大





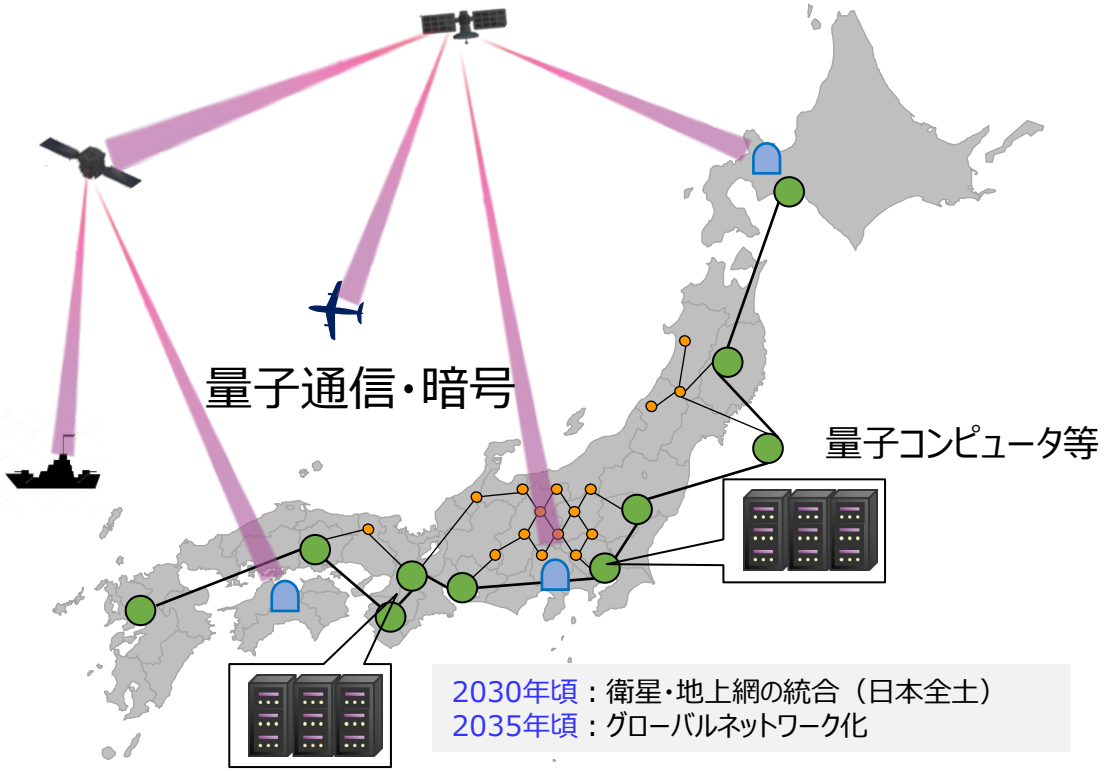
ISS－地上局での安全な鍵共有実験

- 衛星ー地上間で鍵を共有　衛星を介して地球上のあらゆる場所と鍵共有
- 衛星量子暗号の研究開発は中国が先行　EUや米国も開発を急ぐ
- NICTは2024年3月にISSと可搬地上局の間で安全な鍵共有実験に成功
- NICTが代表となり宇宙戦略基金事業を受託　2030年頃運用予定

量子暗号通信の早期社会実装に向けて

- 一度漏洩すると重大な影響がある安全保障・外交・個人のゲノム情報などは長期に渡って守ることが必要．これらの情報をネットワークにより共有する際には量子暗号通信網の活用が期待．
- 量子暗号通信の産学官連携テストベッドである「東京QKDネットワーク」で得た知見を活用し，テストベッドの広域化・高度化によりユースケースを創出，民間投資とユーザの拡大を加速化することが必要．

量子暗号通信ネットワークの将来像



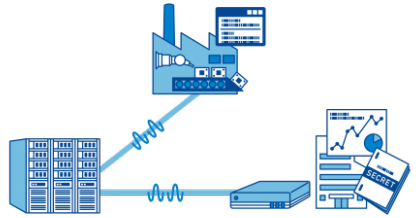
2030年頃：衛星・地上網の統合（日本全土）
2035年頃：グローバルネットワーク化

利用が期待される分野

● 医療分野

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医療情報のやりとり

● 産業・サービス分野



金融、製造分野等における重要技術情報、秘密情報などのやり取り

● 行政・外交・安全保障分野

政府の機密情報、在外公館における外交情報などのやりとり