\Orchestrating a brighter world NEC

資料2-2

量子技術の実用化推進WG

量子セキュリティ／ネットワーク産業の課題や今後の産業振興方策について

2022年11月10日

NEC　アドバンストネットワーク研究所
浅井　繁

講演者紹介

浅井　繁(あさい　しげる)

所属・役職	NEC グローバルイノベーションユニット アドバンストネットワーク研究所長
経歴	1998年 4月　日本電気株式会社　入社 2012年10月　防衛ネットワークシステム部　第一システム部 陸自将来システム　提案・開発等に従事 2016年　4月　ナショナルセキュリティ・ソリューション事業部　システム部長 2018年　4月　同　事業部長代理　ネットワーク事業統括 2020年　4月　技術シナジー創造本部長 2022年　4月　アドバンストネットワーク研究所長

説明内容

I.　量子セキュリティ／ネットワークを取り巻く環境
II. NECの量子暗号研究の取り組み
III.今後の産業振興方策について（提言）

Ⅰ 量子セキュリティ／ネットワークを取り巻く環境

量子コンピューティングの進化に対して現代暗号への対策が急務

現代暗号の安全性

【安全性の根拠】 現在の計算機で解読するには天文学的な時間がかかる

量子コンピュータによる

RSAなど現代暗号の危殆化

耐量子計算機暗号

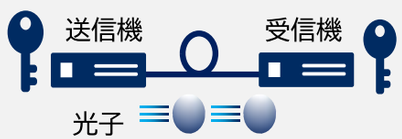
格子暗号

鍵配送
デジタル署名

計算量に基づく安全性（評価中）

- ソフトウェアだけで実現可能
- 量子コンピュータが苦手なアルゴリズムを採用

量子暗号



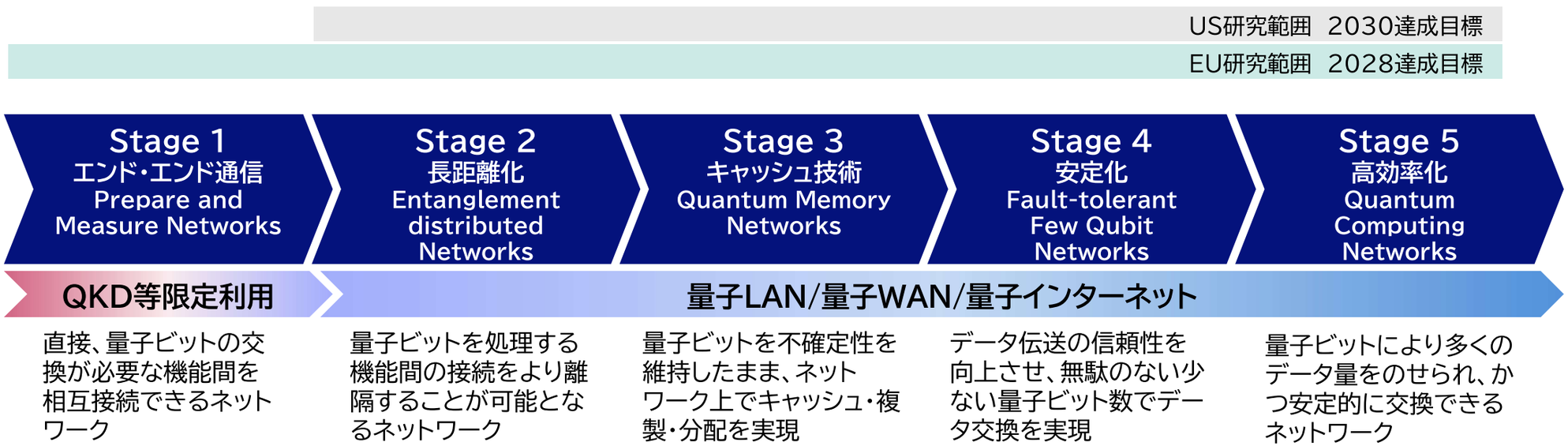
情報理論・量子力学に基づく安全性

- 専用の量子鍵配送装置が必要
- **量子コンピュータ含め未来の計算機でも解読不可**

各国の量子暗号通信の戦略

量子暗号通信は、将来の量子インターネットの戦略的な位置づけ（EU/US）

- 量子鍵配送に関する技術要素が量子ネットワーク・量子インターネットにつながる
- 量子のままビット交換する技術として、QKDは量子ネットワークの第1ステップとされている



Quantum internet: A vision for the road ahead, 2018を参考にNECにて作成
https://science.sciencemag.org/content/362/6412/eaam9288

量子暗号通信の普及が期待される市場

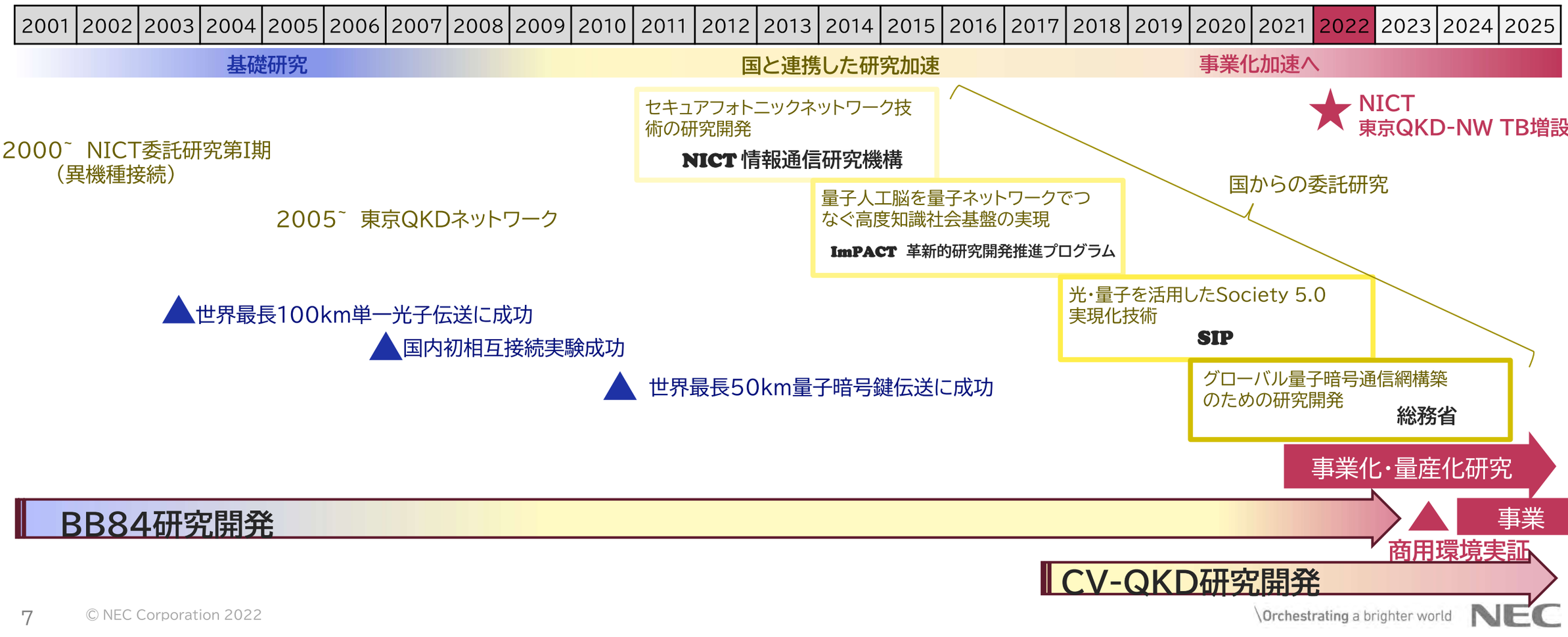
- 量子暗号通信は、DX化が進む社会を安全・安心に担保するためのインフラ技術となる
- 社会を下支えするためには量子暗号通信網の普及が必須

安全保障	行政	製造業	金融	医療
機密情報	個人情報	設計情報	取引・与信情報	遺伝子情報
認証情報	認証情報	サプライチェーン改竄保護	認証情報	創薬開発情報

量子暗号通信

Ⅱ NECの量子暗号研究開発の取り組み

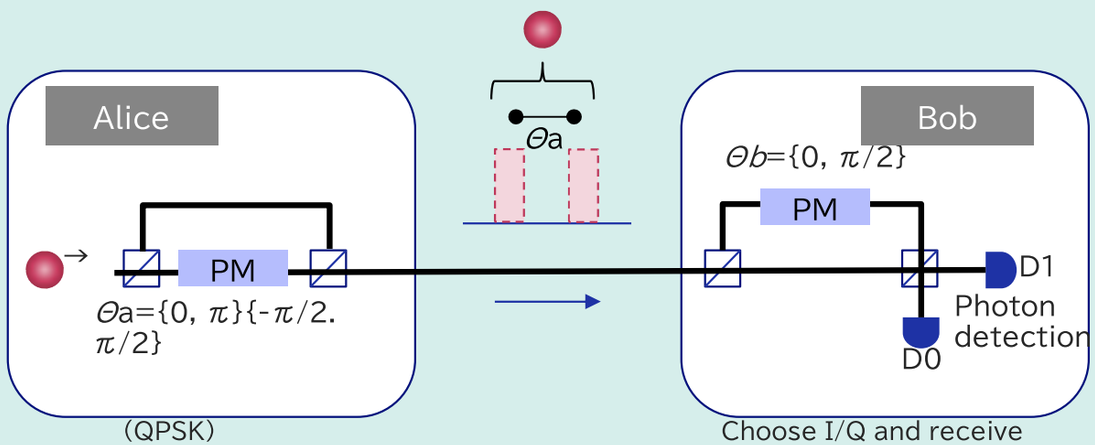
NICTを中心に国内のICT企業と共に20年間にわたり研究を継続。NECは国内に主要研究拠点を持つ唯一の企業として量子暗号通信技術開発を牽引。商用化に向けて技術実証から量産化にシフト中。



2つのQKD技術の特徴

DV-QKD(BB84)

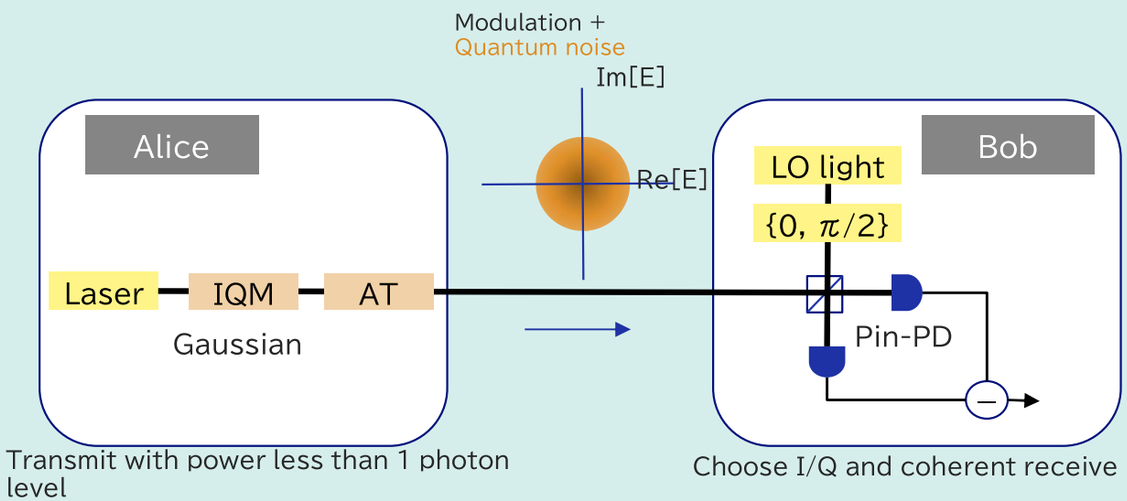
単一光子に対して、暗号鍵の論理ビットに対応するように位相変調を付与して装置間で送受する。



光子検出用の高感度デバイスが必要なため高コストだが、距離の延伸化で中継数を削減

CV-QKD

微弱光波に対し、受信側が暗号鍵の論理ビットに対応した信号レベルで受信できるように、送信側でIQ変調と減衰を付与して装置間で送受する。

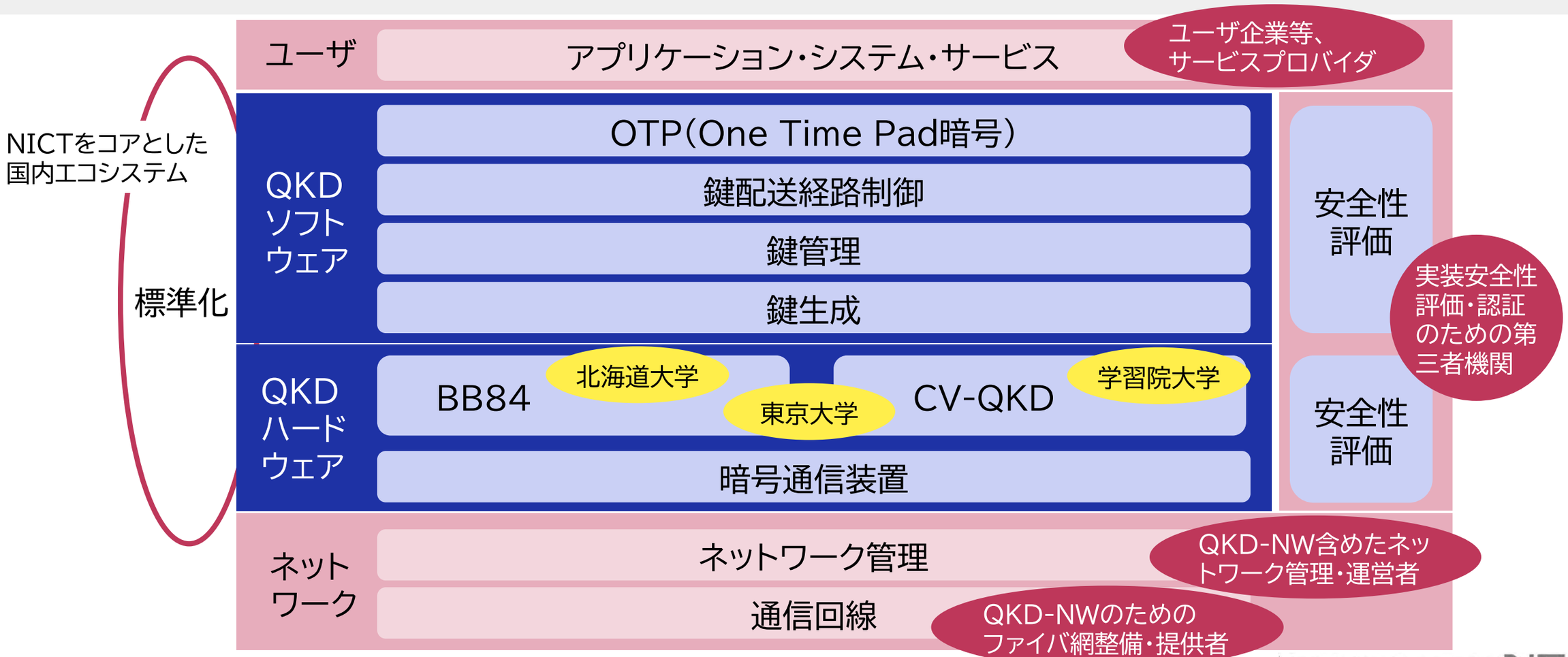


一般的な光通信用デバイスが活用可能で、既存の光ファイバー通信との共存(同時利用)が可能

Ref) http://www1b.comm.eng.osaka-u.ac.jp/com02adm/pdf/lecture_inoue/20190226.pdf

NECの研究開発体制

ハードからソフトまで一気通貫した研究開発・製造体制を国内に構築



Ⅲ 今後の産業振興方策について

- 今後の産業振興方策の方向性（提言）

今後の産業振興方策の方向性

量子暗号・通信技術を社会経済システムに組み込むための事業化促進策と研究開発の推進

1. ユーザ産業の発掘・拡大（活用促進）

2. 量子暗号通信の利用環境整備

3. 量子暗号通信技術の知財化・標準化促進

今後の産業振興方策の方向性(1)

1. ユーザ産業の発掘・拡大(活用促進)

市場導入を加速するため政府がファーストユーザとなり次世代暗号へ移行

① 優先的に保護すべき情報の指定

次世代暗号導入すべき情報・区分を選定し、次世代暗号への切替をルール化

② 調達要件への適合

量子暗号(QKD+OTP(One Time Pad)等を政府推奨暗号とするため、CRYPTRECでの検討を促進

③ 全国ネットワークの構築と民間共用(転用)の推進

デジタル基盤の安全性アピールと、規模拡大による導入コスト低減と高信頼化を両立を図る

民間市場の導入推進

① 市場・産業の発掘

政府との共用化で新たな利活用策の発案、実証のハードルを低減し、早期の知財獲得、人材育成を促進

② ユーザ産業の導入拡大

指定された情報を扱うシステムでの利用推奨・ルール化に加えて、税制優遇や助成金などで導入を支援

例　遺伝子情報、金融取引等

CRYPTREC(クリプトレック): Cryptography Research and Evaluation Committees

今後の産業振興方策の方向性(2)

2. 量子暗号通信の利用環境整備(QKDネットワーク拡充)

① 大規模量子暗号通信のテストベッドを整備し、実用・安全性を検証

② 地方のデジタル活性化のためのセキュアネットワークとして利活用

③ 民間との共用ネットワークとして投資効率化と利用促進を両立

東京QKD-NWから

東海道に沿って大都市圏へQKD-NWを延伸

東京ー大阪のQKD-NWを構築(2025)

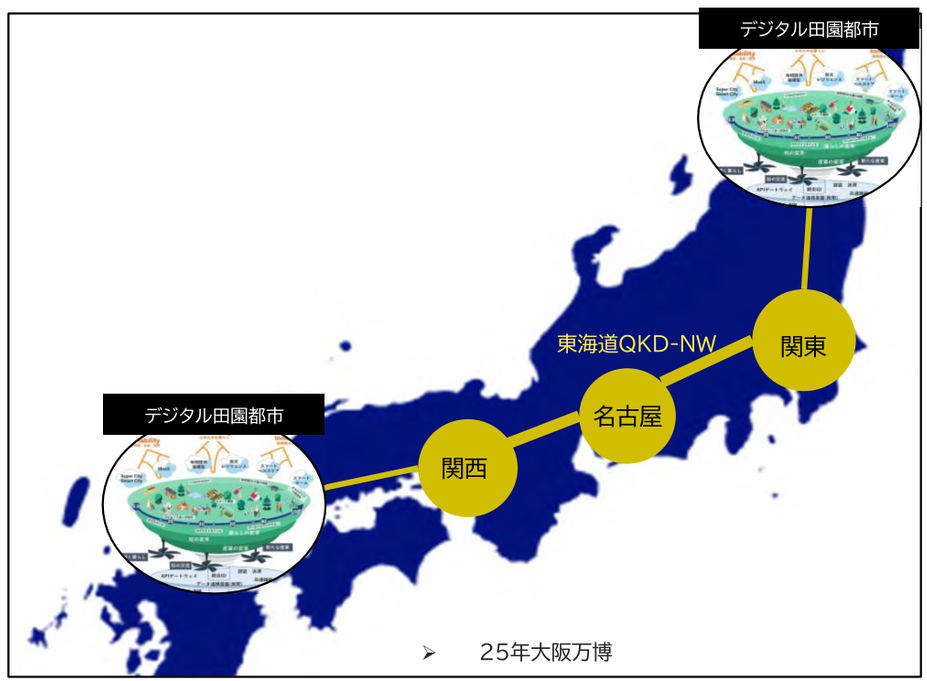
↓

デジタル田園都市のデジタル・インフラへ

重要情報保護、プライバシー保護に寄与

↓

世界に先駆けて
全国版量子セキュアクラウドの構築と実用化



商業の中心かつ重要データが集積される東海道で長距離量子暗号ネットワークを構築し、レジリエントなデジタル基盤として地方へ拡大していく

今後の産業振興方策の方向性(3)

3. 量子暗号通信技術の知財化・標準化促進

ベンダの競争・協力を促し、国の技術水準の底上げを図り、グローバル競争力を強化

① グローバルで技術仕様策定をリードし、技術水準を底上げ

知財化と標準化、技術実証と事業化を並行させ、日本が先行者利益を獲得

② インターオペラビリティ(相互接続性)の確保

ベンダの機器が相互接続できることで、ユーザが安心して構築できる

(ベンダが権益を保持できる仕組みも準備) 例 :公開用リファレンス機・コードを開発

③ 機器の安全性認証体制の構築

第三者による装置・ソフトウェアの安全性検証の仕組み(人材育成も含む)を構築

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC