Tokyo QKD Network: 量子暗号ネットワークテストベッドの構築と利活用

情報通信研究機構 未来ICT研究所
量子ICT先端開発センター
武岡 正裕

国立研究開発法人 情報通信研究機構

内容

1. 量子暗号とは

2. Tokyo QKD Network
   ーJGNの量子技術への活用と成果

3. まとめ

量子暗号とは

「（量子計算機を含む）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方式***

*ただし直接手渡しを除く

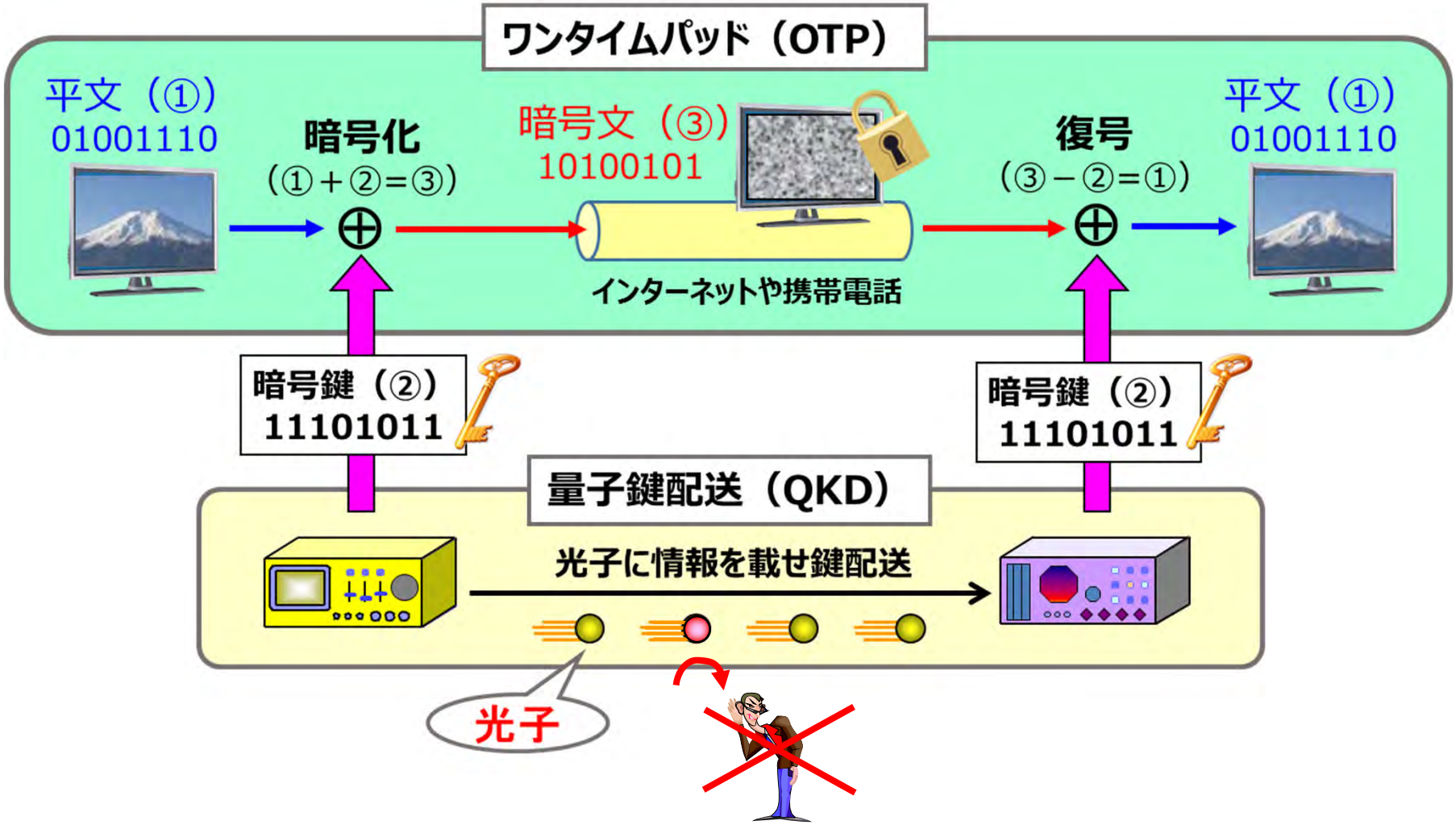
1．情報理論的安全性
→ あらゆる計算アルゴリズムを使っても解読不可
（量子計算や未来の新しい計算技術も含む）

2．（鍵共有）通信路への盗聴攻撃に対する安全性
→ あらゆる盗聴攻撃を検知

現在の暗号（数理暗号）の安全性：解読計算の困難さに立脚（計算量的安全性）
例：RSA暗号　　・・・素因数分解の困難さ
　　耐量子公開鍵暗号・・・現在知られている量子計算アルゴリズムでも解読困難

量子暗号

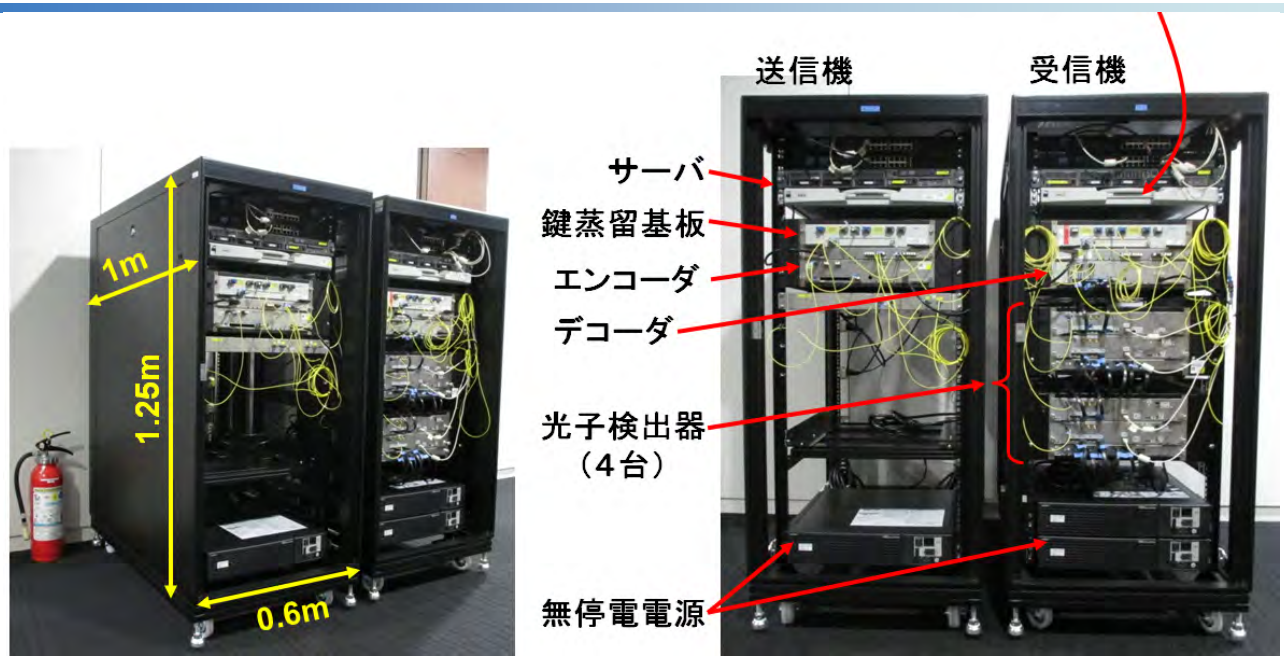
・量子鍵配送（QKD）により、平文と同じサイズの暗号鍵を共有
・最も安全な暗号化（情報理論的安全性）：送りたい情報と暗号鍵を1ビットずつ
足し算し暗号化（1度使った鍵は2度と使い回さない → ワンタイムパッド暗号：OTP）

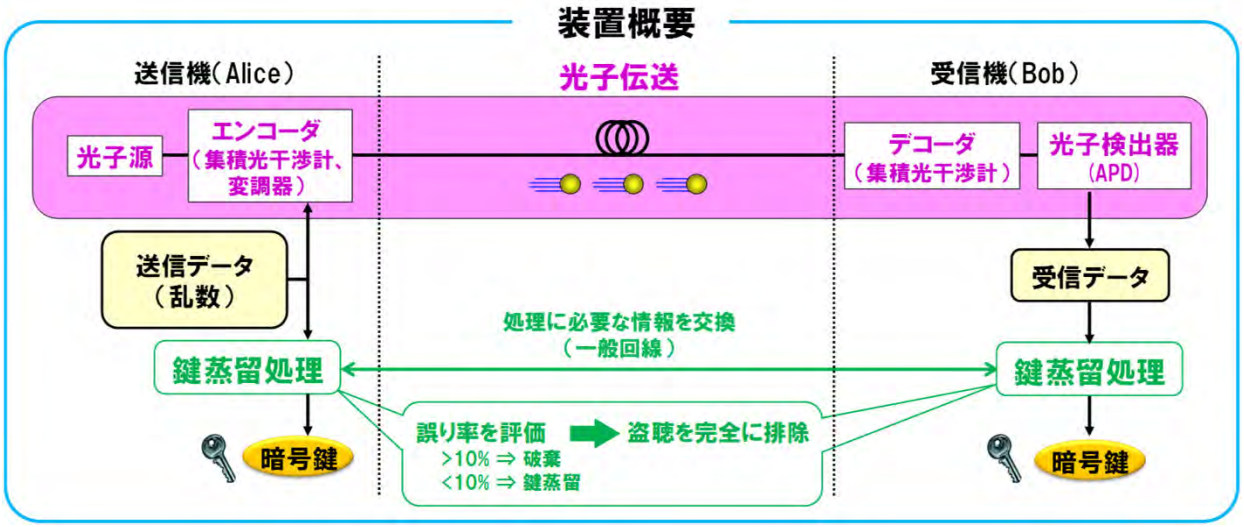


QKD: Quantum Key Distribution

どんな盗聴も確実に検知し、安全に鍵配送

QKDシステムの実装例（NEC社開発事例）

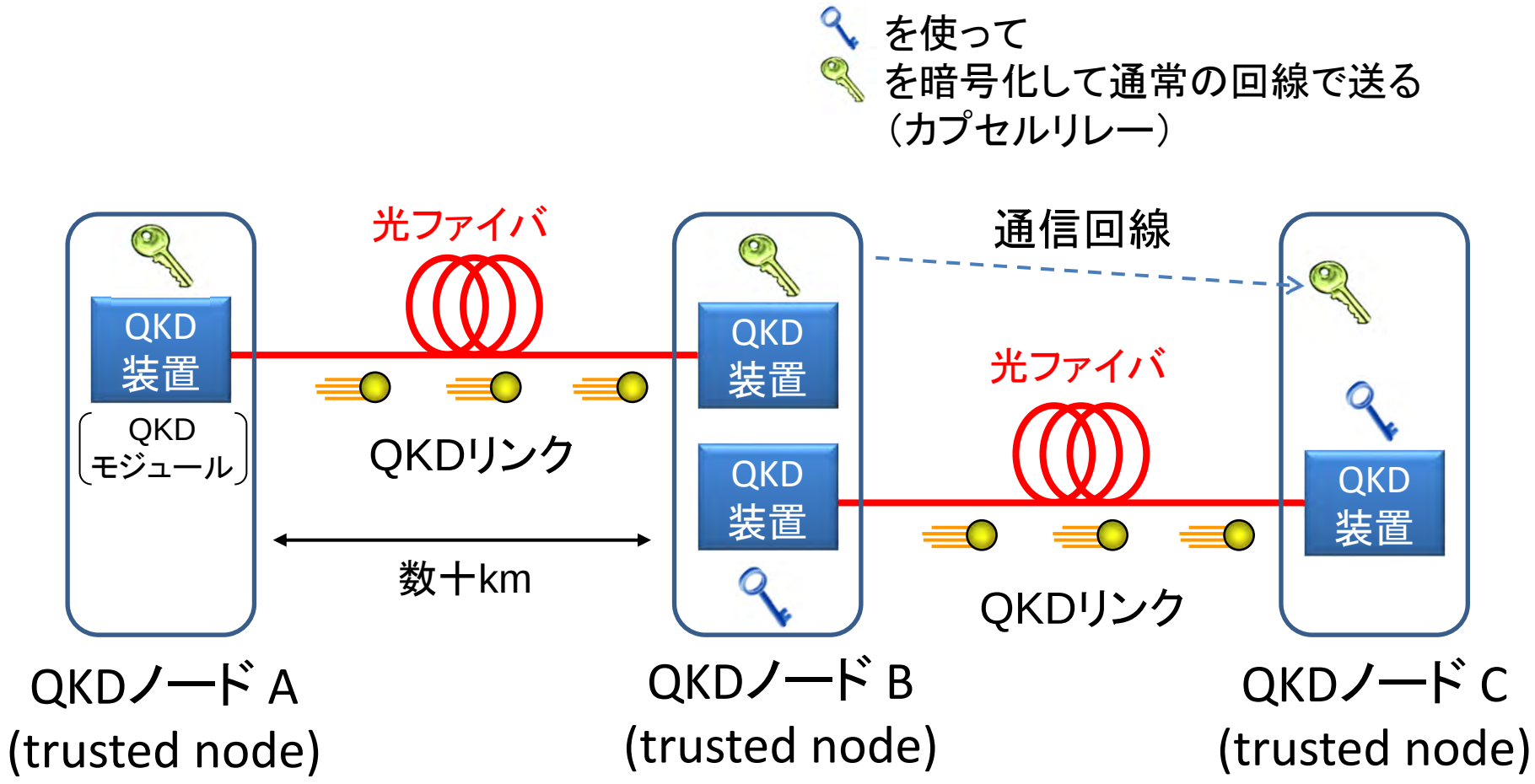




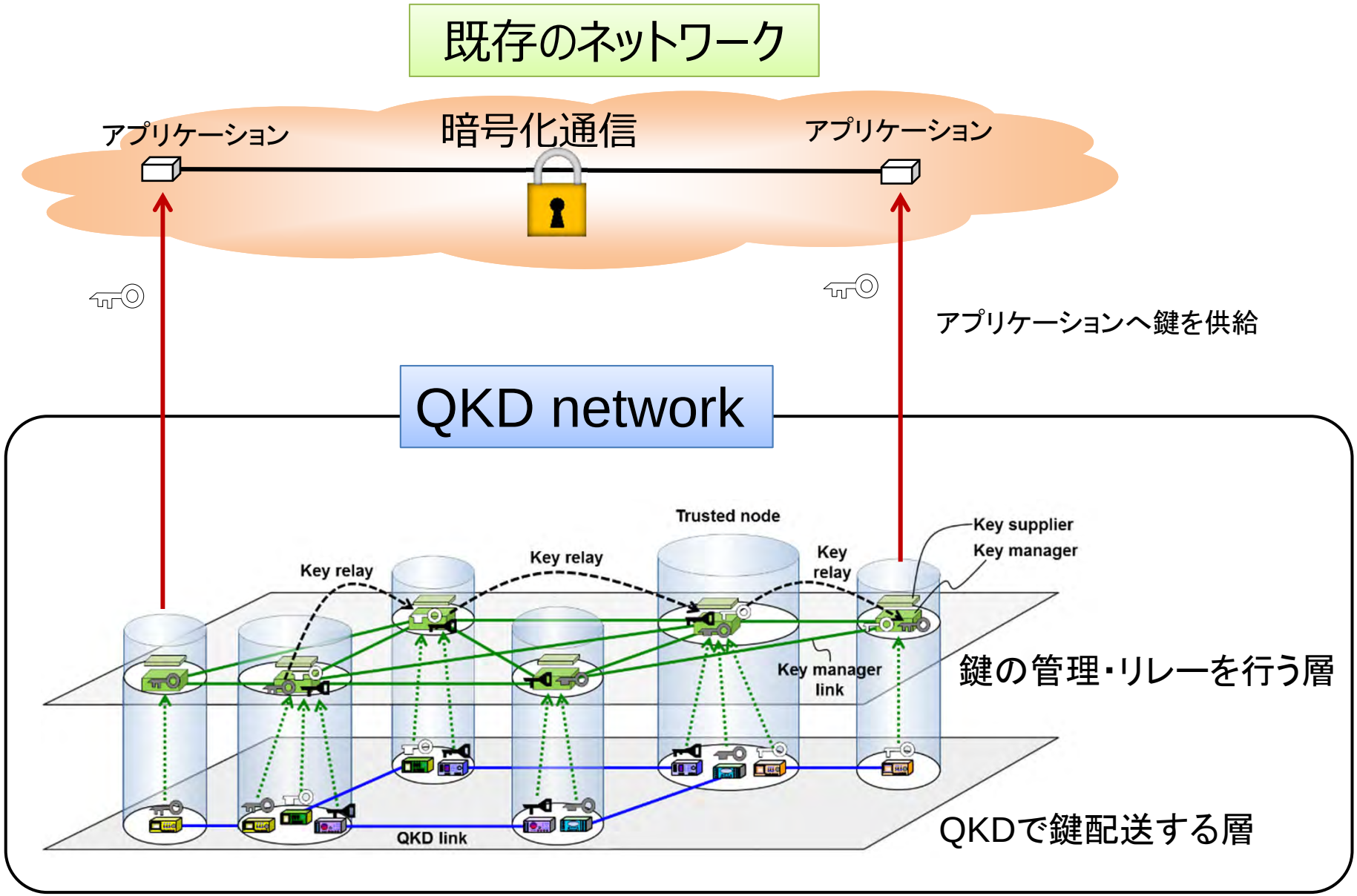
〇ハードウェア：
最先端光通信技術＋光子検出器（APD）
〇ソフトウェア：
QKD特有のデータ処理技術

長距離化・ネットワーク化の方法：鍵リレー

安全な局舎（trusted node)を介して鍵をリレーする



量子鍵配送ネットワーク（QKD network）



内容

1. 量子暗号とは

2. Tokyo QKD Network
   ーJGNの量子技術への活用と成果

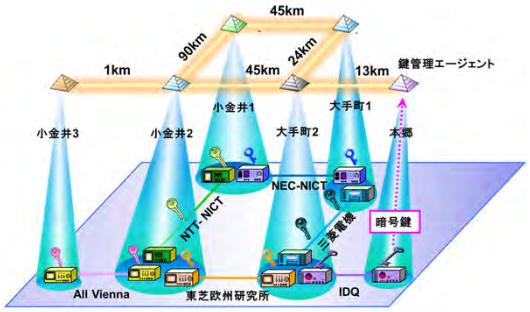
3. まとめ

日本の取り組み

2010年　　2018年　　2023年

NICT委託研究 → **ImPACT** → **SIP第2期**

2010年、量子暗号テストベッド「東京QKDネットワーク」を構築

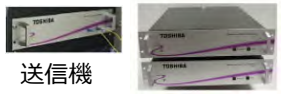


✓ 動画の量子暗号化を世界で始めて実現

NEC
100kbps@45km

送信機　受信機

東芝
300kbps@45km



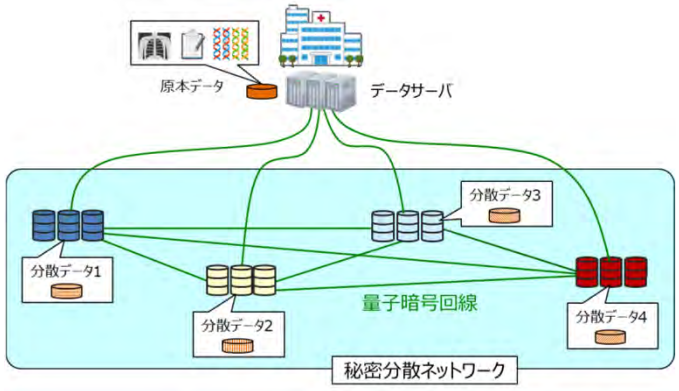
送信機　受信機

✓ **世界最高速**の装置を開発
300kbps @45km　（東芝）

海外製の**10倍高速、2倍長距離**

✓ 新たなキラーアプリ
『**量子セキュアクラウド技術**』
の原理実証
(**量子暗号x秘密分散**)

『光・量子を活用したSociety5.0実現化技術』

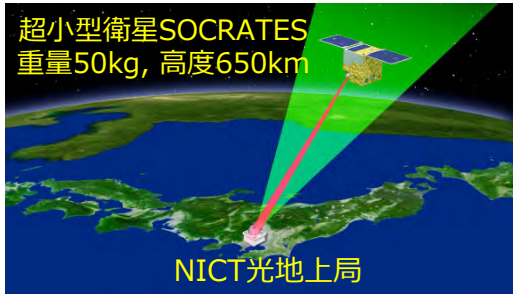


➢ 政府重要拠点間等での量子暗号サービスの準備開始

量子セキュアクラウド技術の開発と社会実装

総務省・委託研究

グローバル量子通信網の構築



✓ NICTが超小型衛星で量子通信を実証（2017年）

総務省・委託研究

衛星通信における量子暗号技術

テストベッド構築のためのリンクの要件

QKDのパフォーマンスを最大限発揮するためには。。

〇中継増幅器を使えない、光-電気信号変換不可

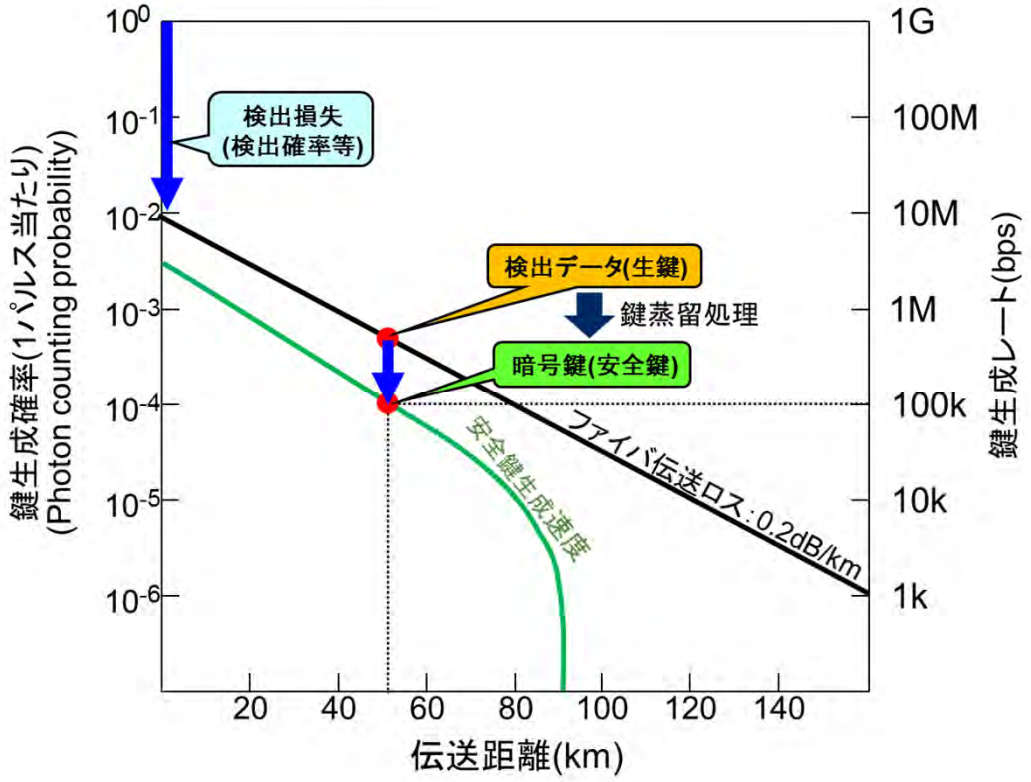
〇リンク間の距離は50km程度まで。

〇（現状技術で最高性能を出すためには）
ダークファイバーが好ましい。

QKDの技術的な制限

- 光子のほとんどはファイバーや検出器の損失で失われる
- 中継増幅器は量子状態を破壊するため使えない
- 光子は超微弱なため、クロストークに弱い

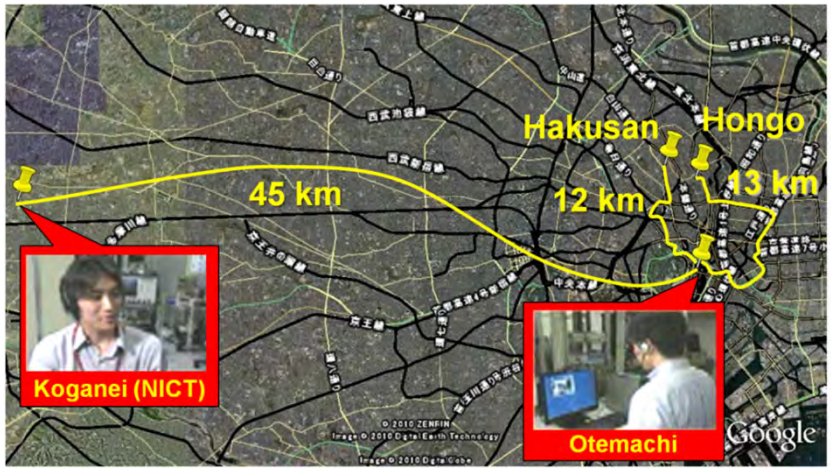
1 対のQKD送受信機では鍵の伝送距離・速度が制限される

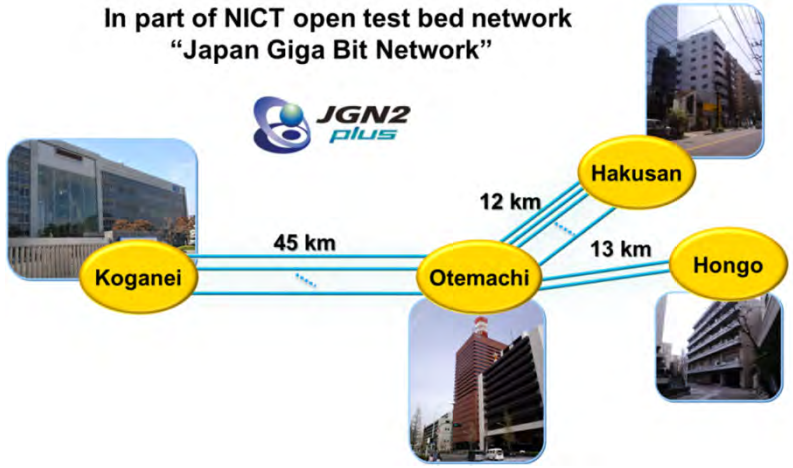


鍵生成レート
試算の一例

Tokyo QKD Network

・2010年にテストベッド「東京QKDネットワーク」を構築。
NICT委託研究参画機関を中心に、フィールド実証を実施





〇東京都心と郊外（小金井市）をつなぐテストベッド光回線"JGN"
を利用したQKDネットワークテストベッド
〇NEC、東芝、NTT、学習院大等の産学機関、及び一部海外機関が
それぞれのQKD装置を導入しネットワークを構成。
〇2010年、世界初となるQKDによる秘匿動画配信（TV会議）の実証に成功
〇現在も実証実験を継続中。世界で最も長い運用実績。

http://www.tokyoqkd.jp/

テストベッド上での研究開発成果とその展開

研究開発成果

1. 技術開発

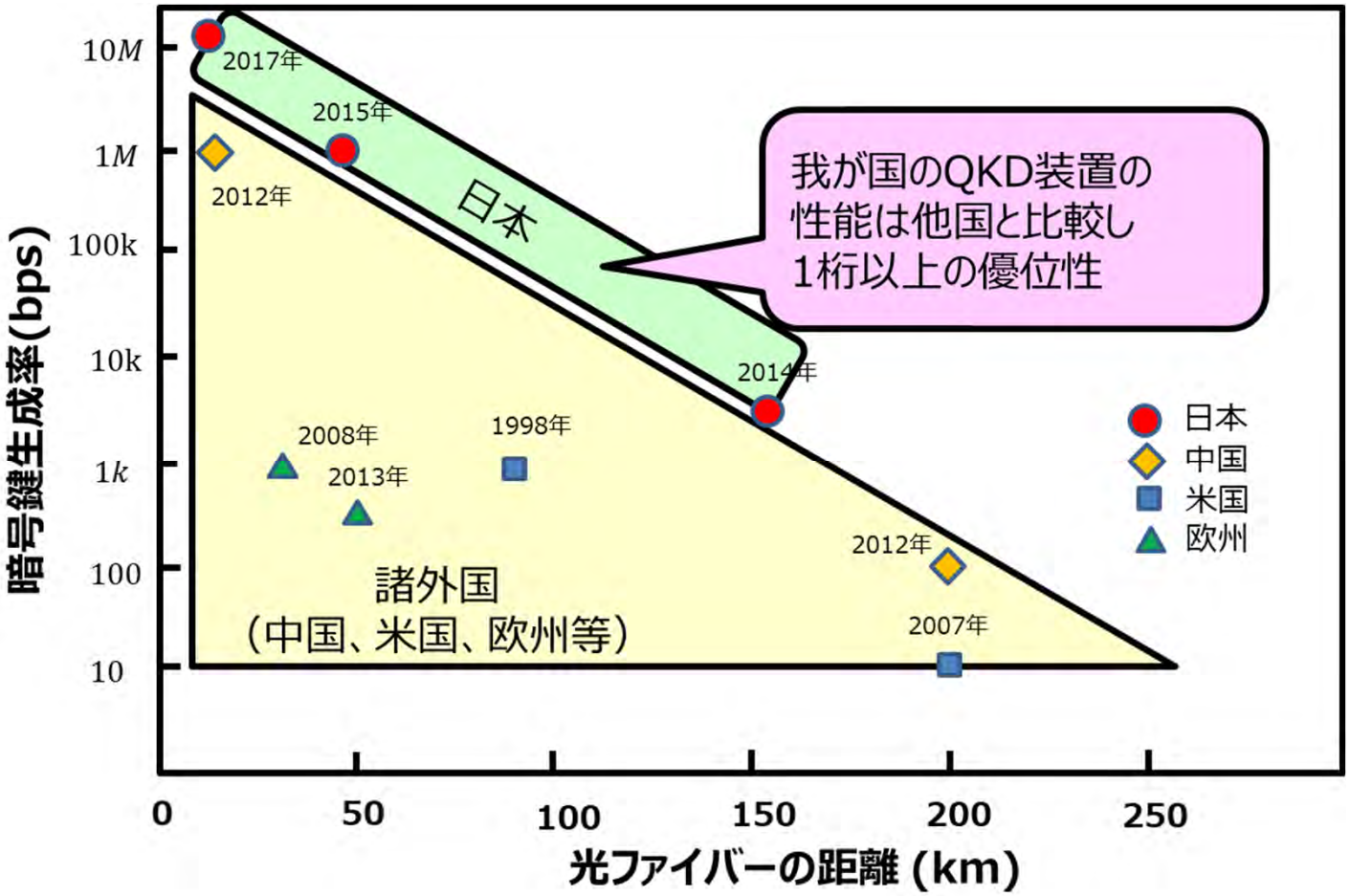
2. 社会実証実験（PoC）

成果の展開

3. 実用化

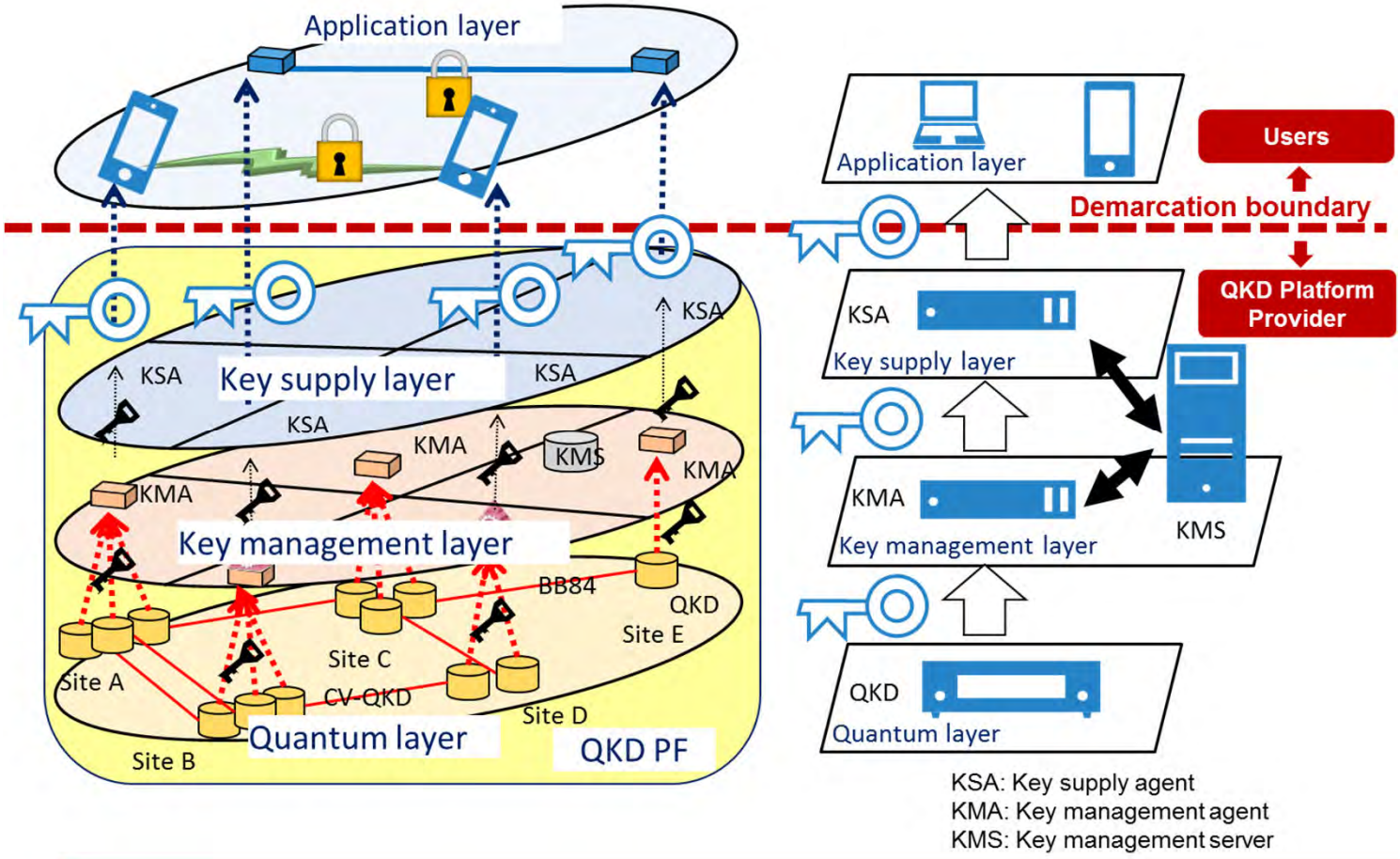
4. 国際標準化

鍵生成速度比較（QKD装置の高性能化）



QKDプラットフォームの開発

QKDネットワーク全体の制御と鍵管理、アプリケーションへの提供を安全に行う「QKDプラットフォーム」技術を開発



QKD装置の開発が始まった時期に、世界に先駆けて
QKDネットワーク全体の開発・実装を推進

テストベッド上での研究開発成果とその展開

研究開発成果

1. 技術開発

2. 社会実証実験（PoC）

成果の展開

3. 実用化

4. 国際標準化

実証実験・ネットワーク化の現在の取り組み

(1) 電子カルテ（模擬）の秘密分散保管（量子暗号の要素技術、量子暗号、量子セキュアクラウド）
(2) ゲノムデータ（模擬）の秘密分散保管（量子暗号技術、量子セキュアクラウド）
(3) レーザ加工拠点の重要回線の秘匿化（量子暗号技術、量子セキュアクラウド）
(4) 生体認証の参照データの秘密分散保管（量子暗号技術、量子セキュアクラウド）

高知医療センター

電子カルテの標準データ交換規格に基づく模擬データを提供

(1) 高知～東京 800km圏、電子カルテ模擬データを共通鍵暗号で秘匿化

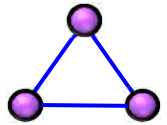
大阪拠点

名古屋拠点

共通鍵暗号による秘匿化
（量子暗号回線の敷設はまだ）

(3) レーザ加工拠点の重要回線の秘匿化

仙台 10km圏



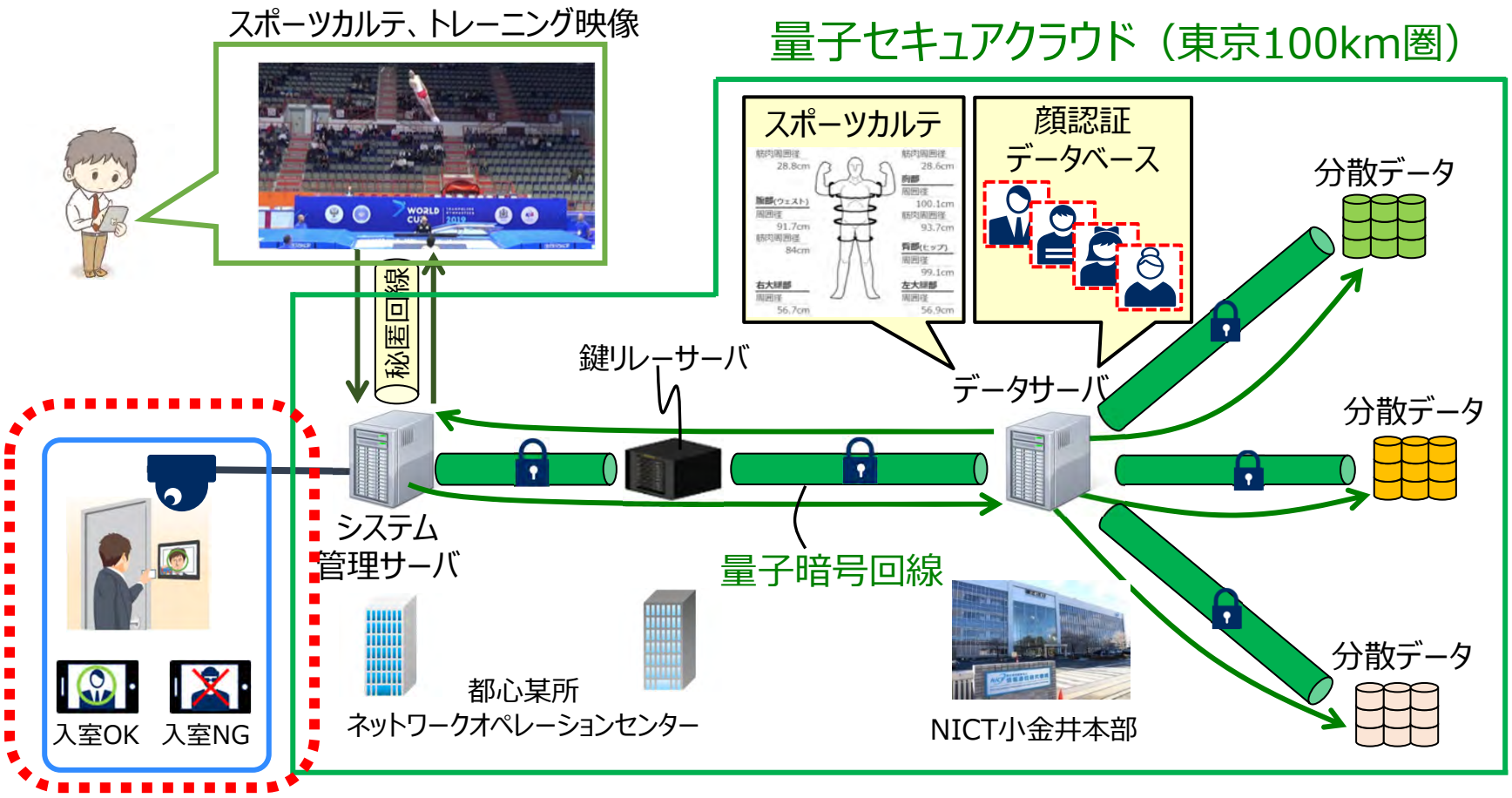
(2) ゲノム解析データの暗号通信、秘密分散

東京 100km圏

(1) 電子カルテ模擬データを量子暗号で秘匿化
(4) 生体認証の実データを量子暗号で秘匿化　参照データの分散バックアップ

実証実験の例：生体認証システムへの適用

- ✓ 顔認証用参照データ，スポーツカルテの秘密分散保管
- ✓ 日本代表選手が所属する団体で利用中



2019年10月　報道発表（NICT, NEC）

テストベッド上での研究開発成果とその展開

研究開発成果

1. 技術開発

2. 社会実証実験（PoC）

成果の展開

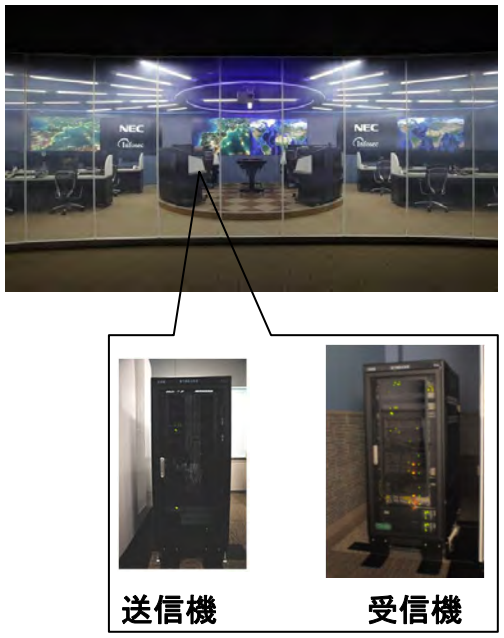
3. 実用化

4. 国際標準化

実運用試験

- NEC

「サイバーセキュリティ・ファクトリー」内で実運用評価試験を開始（2015年7月～）

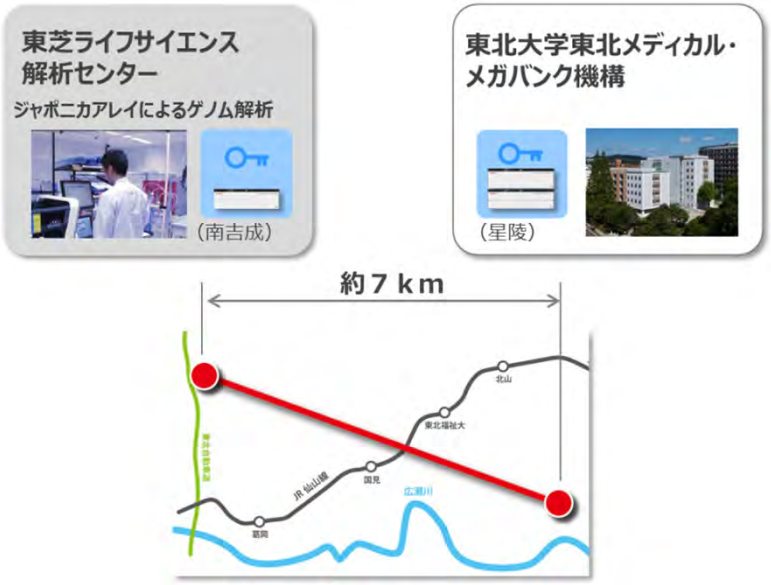


プレスリリース

http://jpn.nec.com/press/201509/20150928_03.html

- 東芝

仙台の自社ー東北大間を結ぶQKD回線を構築。ゲノム解析データの暗号通信を開始（2015年8月～）



プレスリリース

http://www.tqccs.com/cl/tech/qccs/

製品化（国内初）

TOSHIBA Japan 検索

製品・サービス | 企業情報 | ニュース | お問い合わせ

東芝トップページ > ニュース&トピックス > 量子暗号通信システム事業を開始

ニュースリリース

ニュースリリースに掲載されている情報（製品の価格／仕様、サービスの内容及びお問い合わせ先など）は、発表日現在の情報です。予告なしに変更されることがありますので、あらかじめご了承ください。最新のお問い合わせ先は、東芝全体のお問い合わせ一覧をご覧下さい。

量子暗号通信システム事業を開始

2020年度より順次国内外で積極的に事業を展開し、量子暗号通信の実用化を牽引

2020年10月19日

当社は、2020年度第4四半期より、国内外での量子暗号通信システムのプラットフォームの提供およびシステムインテグレーション事業を順次開始することを決定しました。

2020年10月

https://www.toshiba.co.jp/about/press/2020_10/pr_j1901.htm

テストベッド上での研究開発成果とその展開

研究開発成果

1. 技術開発

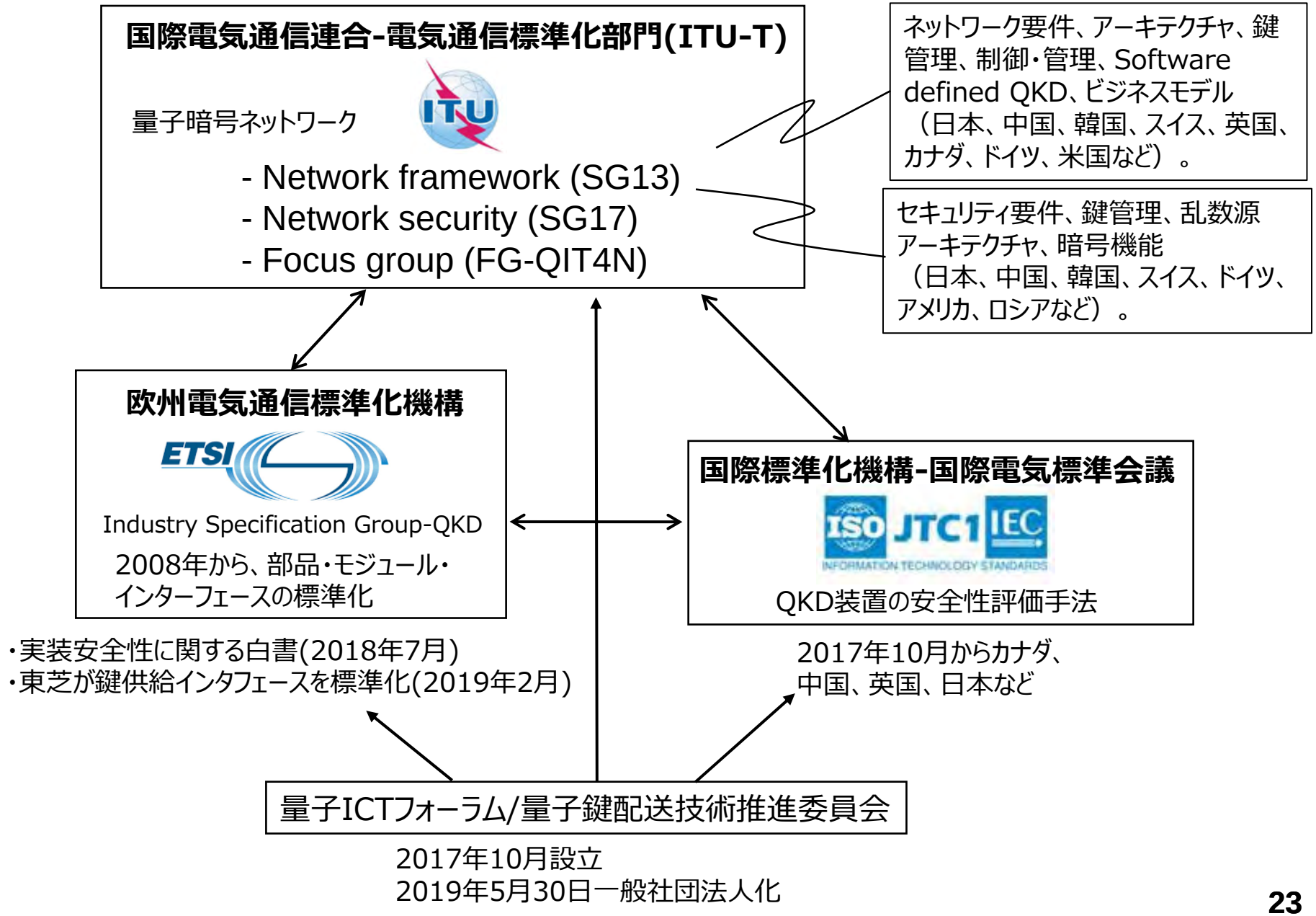
2. 社会実証実験（PoC）

成果の展開

3. 実用化

4. 国際標準化

量子暗号に関する標準化活動動向



国際標準化例: ITU-T

ITU-Tにおける量子暗号分野に関する初の勧告Y.3800が成立（2019年10月25日）

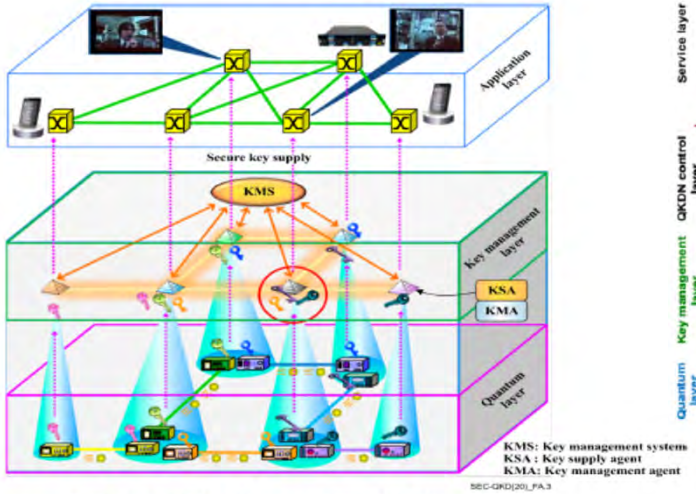
ITU-T **Y.3800**
(10/2019)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

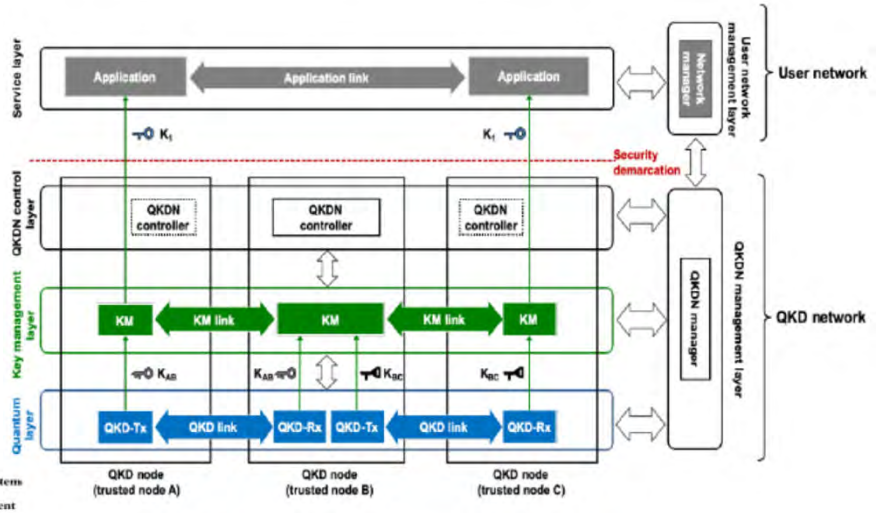
SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,
NEXT-GENERATION NETWORKS, INTERNET OF
THINGS AND SMART CITIES
Cloud Computing

Overview on networks supporting quantum key distribution

・量子暗号ネットワークの基本構成を定義
・日本（NICT、NEC、東芝）が文書作成を主導
→ 日本の技術仕様を入れ込み



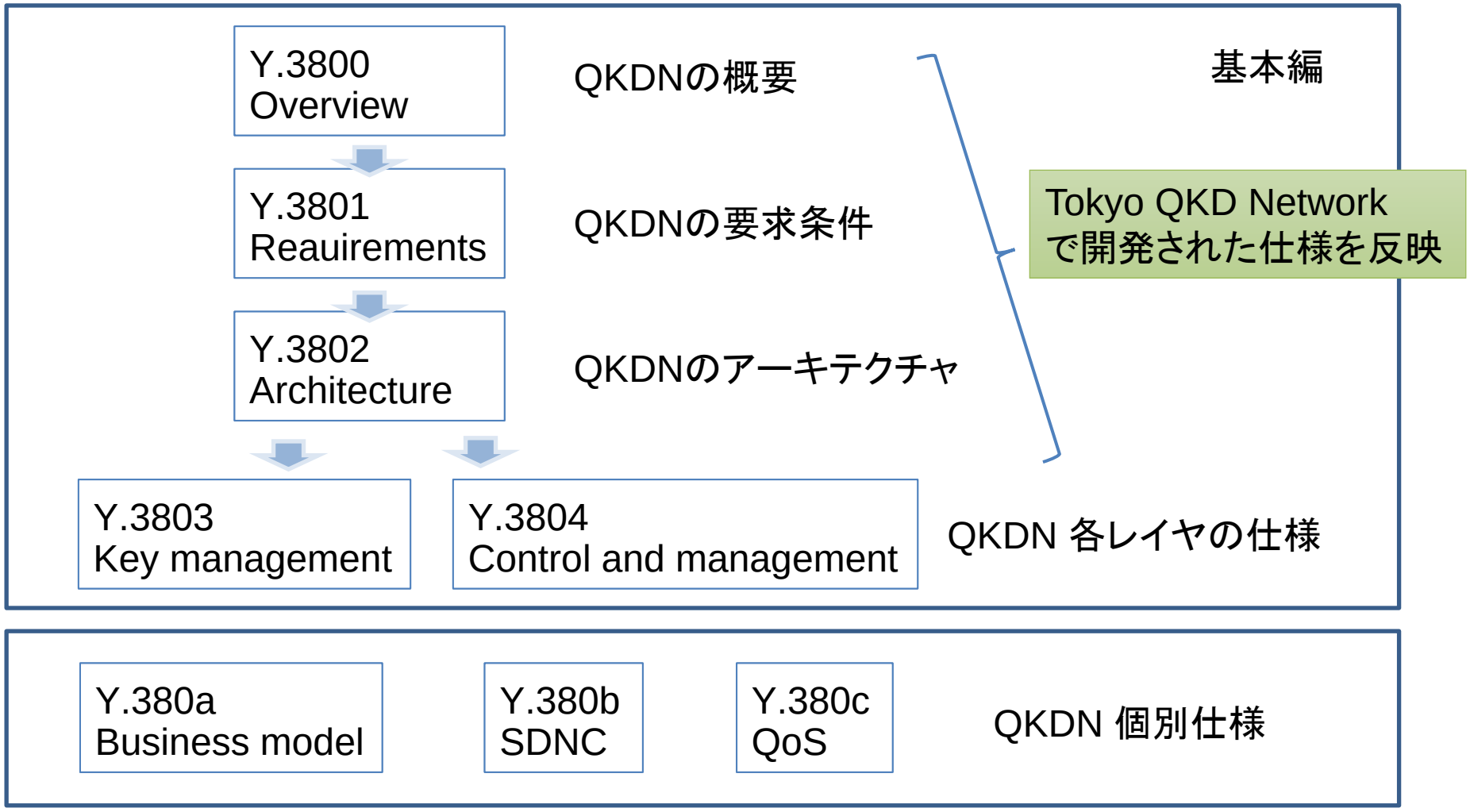
Tokyo QKD Networkの構成



Y.3800 QKD Networkの概念的構造

国際標準化例: ITU-T

SG13（ネットワークアーキテクチャ）、SG17（セキュリティ）で勧告化が進展



SG13で成立、及び審議中の勧告シリーズ

グローバルネットワークに向けて

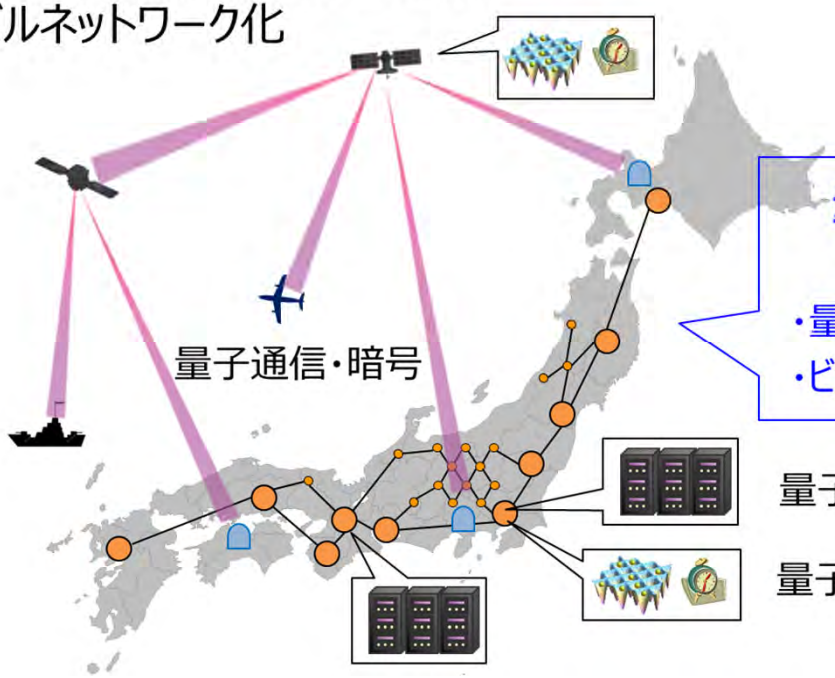
・NICTに国際的な『量子セキュリティ拠点』を整備中
・産学官共同利用のオープンテストベッド化を検討中

⇒ **民間投資とユーザの拡大**

第1段階（2022年頃）：関東圏（量子コンピュータ、量子暗号・中継など）
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

政府アーリーアダプタ
✓ 2020年度、量子暗号

NICT本部に国際的な研究開発拠点（**量子セキュリティ拠点**）の整備をR2年度より開始



量子技術プラットフォームの構築
・量産化、低価格化
・ビジネスエコシステムの構築

量子コンピュータ

量子計測・センシング

まとめ

- 量子暗号ネットワーク

〇量子コンピュータを含むあらゆる計算機で解読不可能なことが
厳密に証明されている唯一の暗号技術

〇JGNを活用し、東京圏にテストベッド「Tokyo QKD Network」を構築
量子暗号ネットワークとしては世界最長期間の運用・開発実績
（一方、海外でも大規模実証プロジェクトや通信事業者参入が近年本格化）

〇テストベッドの成果：世界最高速QKD装置の開発と実用化
医療、金融、安全保障分野等での実証
日本仕様の国際標準化への反映

〇今後の課題：QKD装置性能の向上（既存インフラにも一部乗り入れ可能に）
QKDと既存セキュリティ技術の融合とトータルセキュリティシステムの開発
（日本独自技術「量子セキュアクラウド」の開発を進行中）
グローバル量子ネットワークの実現へ（長期課題）