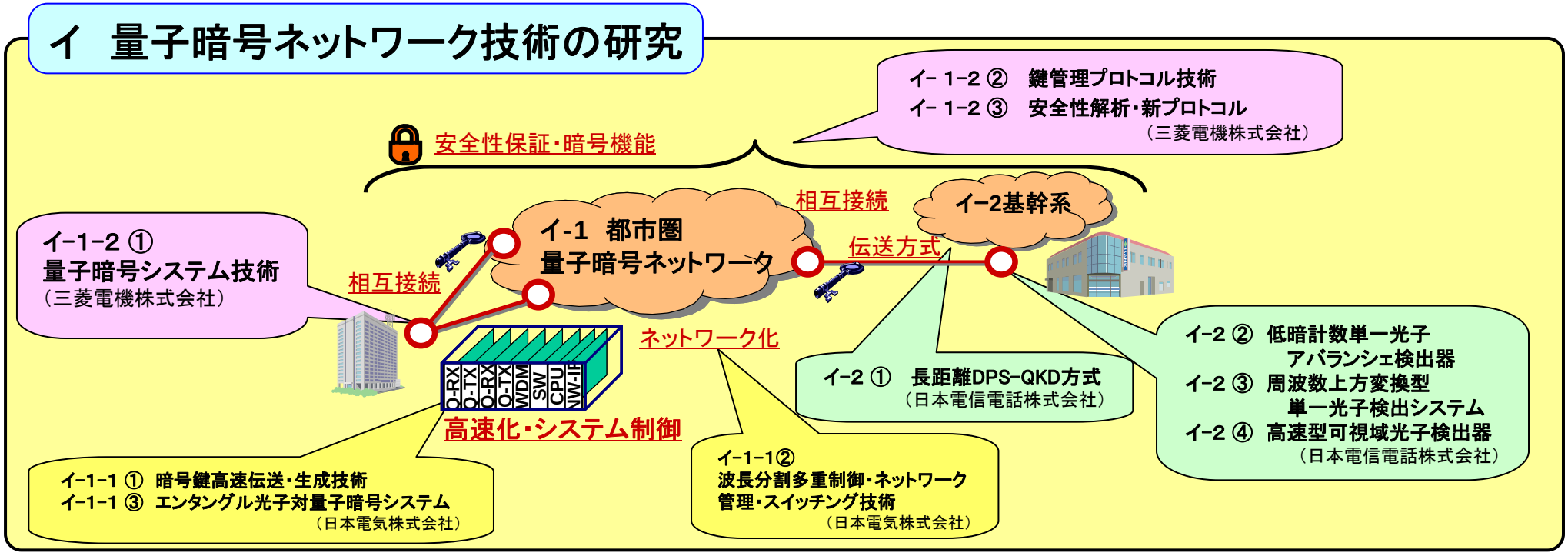
「量子暗号の実用化のための研究開発」の開発成果について
～イ　量子暗号ネットワーク技術の研究～

1. 施策の目標
– 高性能単一光子検出技術を利用して、無条件安全性が理論的に保証された高速な量子鍵配送プロトコルを都市圏ネットワークで実現するためのシステム技術の開発および量子鍵配送を基幹回線ネットワークへ適用していくための基盤技術の開発を行い、都市圏ネットワークと基幹回線ネットワークが接続したネットワーク上における量子鍵配送システムを開発して、その性能を実証することを目的とする。

2. 研究開発の背景
– 安心・安全な社会を実現するためのインフラストラクチャーとして、ネットワークは、ユーザが盗聴・改ざん・成りすましなどのさまざまな危険から解放され、通信の安全性が保証されたサービスなどを利用できることが求められている。

3. 研究開発の概要と期待される効果
– 都市圏ネットワークに対応した高速な量子鍵配送技術と、基幹回線ネットワークに対応した量子鍵配送技術、さらに両ネットワーク間の接続技術を開発することにより、都市圏ネットワークから基幹回線ネットワークまでのシームレスな量子鍵配送が実現できる。

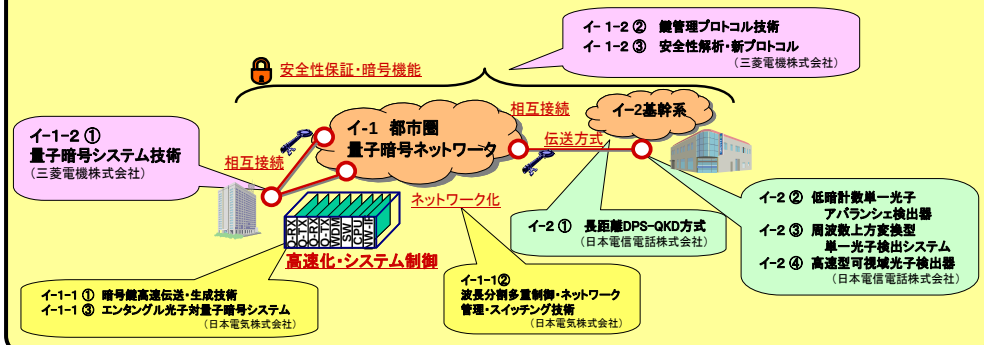


4. 研究開発の期間及び体制
– 平成18年度～平成22年度（5年間）
– NICT委託研究（日本電気株式会社、三菱電機株式会社、日本電信電話株式会社）

イ　量子暗号ネットワーク技術の研究の主な成果

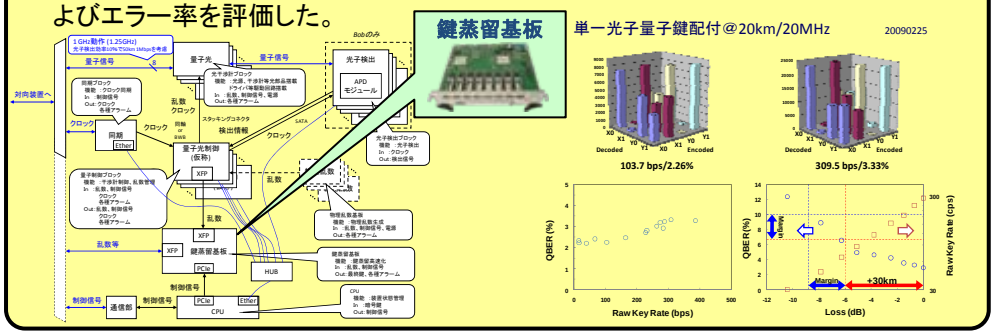
イ　量子暗号ネットワーク技術の研究

イ-1：都市圏対応型量子鍵配送システム技術の研究開発
　イ-1-1：都市圏量子暗号ネットワーク技術（日本電気株式会社）
　イ-1-2：都市圏量子セキュリティ技術（三菱電機株式会社）
イ-2：基幹回線対応型量子鍵配送技術の研究開発
　（日本電信電話株式会社）



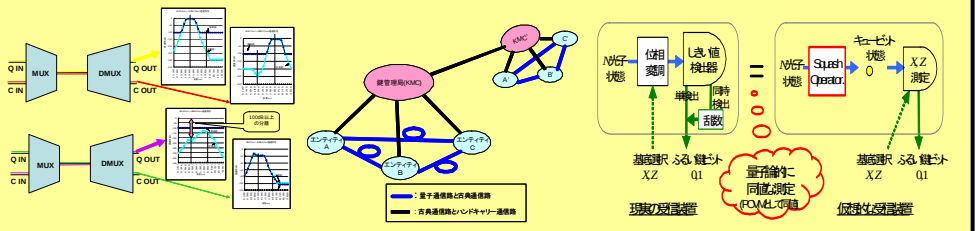
イ-1-1：都市圏量子暗号ネットワーク技術（日本電気 ㈱）

- 50 km 1Mbpsの最終鍵生成を実現する量子暗号装置の開発を進め、鍵蒸留高速化基板/同期基板/制御基板の試作を行い、各基板の基本動作評価を完了した。
- 東京大学ナノエレクトロニクス研究機構ならびに関係諸機関と連携し、世界初の1.5um帯単一光子量子鍵配付の実証に成功した。
- 鍵の使い捨てを想定し、暗号鍵の生成と消費に追従する鍵管理方式の提唱、実験を行い、実証した。
- 2波長光子対量子鍵配付の時間基底における動作を確認し、光子検出レート、およびエラー率を評価した。



イ-1-2：都市圏量子セキュリティ技術（三菱電機 ㈱）

- 古典信号と量子信号を100dBの強度差を持って波長多重分離するMUX・DEMUXを開発、動作検証に成功し、さらに古典・量子波長多重伝送が可能な古典光強度限界を確認した。
- 鍵管理センタの機能分析を行い、量子通信路から分離された鍵管理センタの形態が、柔軟なネットワーク構成を低コストで実現できることを示した。
- 「デコイ方式」における重要なパラメタである「イールド」の最大値と最小値を厳密に求めることに成功し、これによってQKDの通信距離および速度を向上させた。
- BB84方式の安全性証明における新手法（squash演算子）を開発し、これによって、従来問題となっていた理論と実験とのギャップ(しきい値検出器)の解消に成功した。



イ-2：基幹回線対応型量子鍵配送技術の研究開発（日本電信電話 ㈱）

- DPS-QKDが高速な鍵配送を実現できる点に着目して、短ジッタの特徴を持つハイブリット光子検出器を用い短距離での高速な鍵生成レートの確認を行うと供に高速・大容量のデータ処理を実現できるプロトタイプシステムの開発を進めた。
- レーザカオスを用いた高速物理乱数を用いたQKD実験に成功した。
- 周波数上方変換型の光子検出器（UCD）の開発をさらに進め、長波長ポンプシステムで低雑音化が可能なことを確認した。
- 単一光子光源を用いた DPS-QKD　方式の無条件安全性を示すことができた。

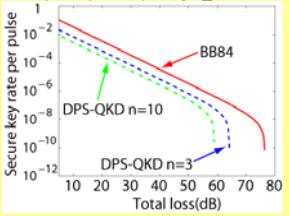


図1、単一光子を用いたDPS-QKDの鍵生成率とBB84の鍵生成率の比較

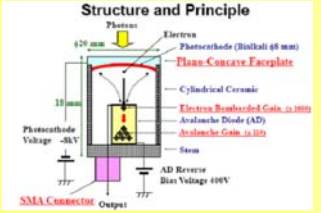


図2：Hybrid photon detectorの構造

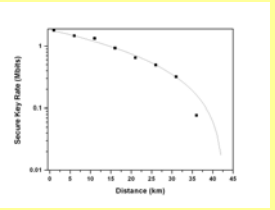


図3：HPDを用いたUCDによる安全鍵生成率と光ファイバ伝送距離

5. これまで得られた成果（特許出願、論文発表等）

	特許出願	論文	研究発表	報道発表
イ 量子暗号ネットワーク技術の研究	35件	55件	58件	8件

6. 研究成果発表会などの参加について

■ イ-１：都市圏対応型量子鍵配送システム技術の研究開発

■ イ-１-１：都市圏量子暗号ネットワーク技術（日本電気株式会社）

ECOC2008（ブリュッセル）にて2件、SECOQC（ウィーン）にて1件発表、UQC2008での講演など

- ECOCにて、NICT、NISTとの連携による世界最速の長距離フィールド実験及び量子鍵の安全性に関して招待講演を行うと共に、量子鍵配付ネットワークの方式提案と実証実験について発表を行った。
- SECOQCにおいて発表を行うことで、ヨーロッパ勢に対し日本の技術力をアピール。
- ICQO08でも量子暗号装置の高速化について招待講演を行い、主にロシア・東欧圏の研究者に日本の技術水準の高さを示した。
- Photonic Westにて量子暗号装置の試験に関する招待講演で標準化に向けた考え方を示した。
- UQC2008において日本における量子鍵配付研究と標準化に向けた活動の報告を行うことで、国際連携に向けたアピールに成功。
- Information security in a quantum world（IQC，カナダ）と量子情報未来テーマ開拓研究会に講師として参加し、委託研究の成果を紹介すると共に、量子暗号研究の活性化に向けて若手研究者にアピールした。

■ イ-１-２：都市圏量子セキュリティ技術（三菱電機株式会社）

SCIS2009暗号と情報セキュリティシンポジウム（滋賀大津）にて2件発表

情報セキュリティの分野で国内で最も権威のあるシンポジウムにて，サブ課題「安全性と新プロトコル提案」の成果として，2件発表した．1件はsquash operatorに関するもので光子検出器不完全さによる安全性証明の不備を解消するもの．もう1件は擬似乱数を用いるプロトコルの脆弱性について指摘したもの．

■ イ-２：基幹回線対応型量子鍵配送技術の研究開発（日本電信電話株式会社）

The Telecommunication Standardization Sector of ITU (ITU-T) together with the Organizaing Committee of the ITU-T "Innovations in NGN" Kaleidoscope Academic Conference Geneva, 12-13 May 2008

国際電気通信連合(ITU)主催の国際会議にて、Differential Phase Shift Quantum Key Distribution と題して最近の NICTでの実験の成果をアピールし、論文賞（second best award)を受賞した。