# 平成22年度 「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
## ～ 課題イ 量子暗号ネットワーク技術の研究 ～

### 1. 施策の目標

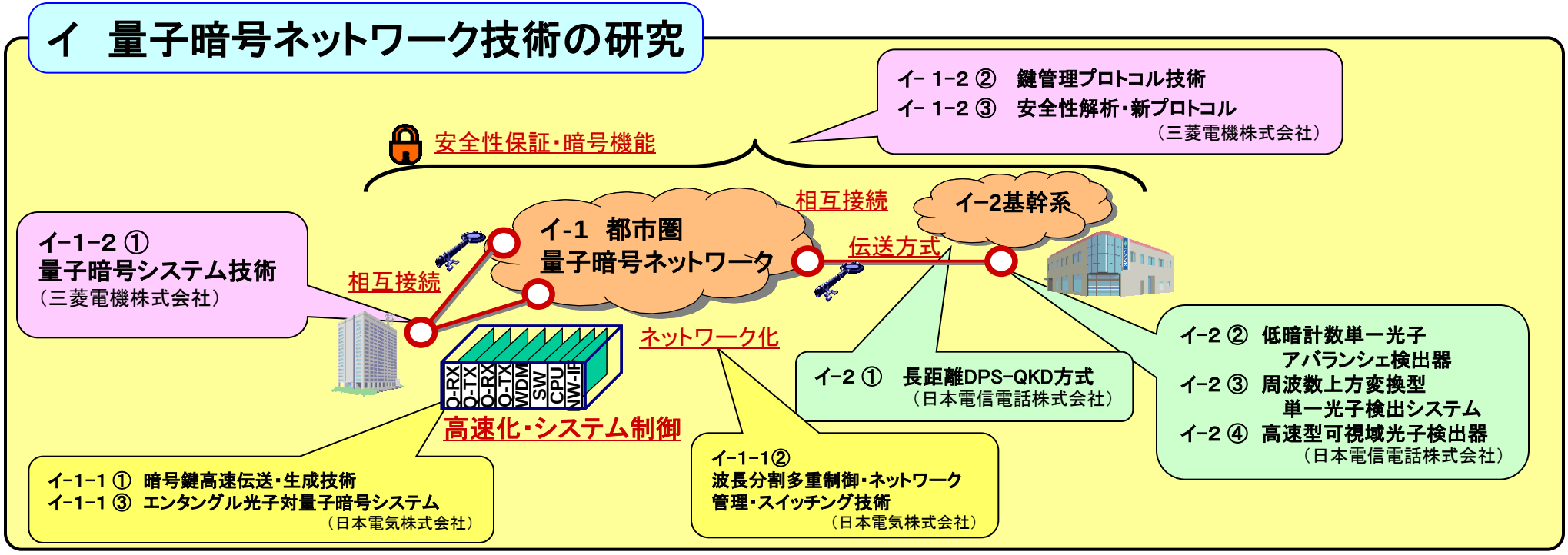
– 高性能単一光子検出技術を利用して、無条件安全性が理論的に保証された高速な量子鍵配送プロトコルを都市圏ネットワークで実現するためのシステム技術の開発および量子鍵配送を基幹回線ネットワークへ適用していくための基盤技術の開発を行い、都市圏ネットワークと基幹回線ネットワークが接続したネットワーク上における量子鍵配送システムを開発して、その性能を実証することを目的とする。

### 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。



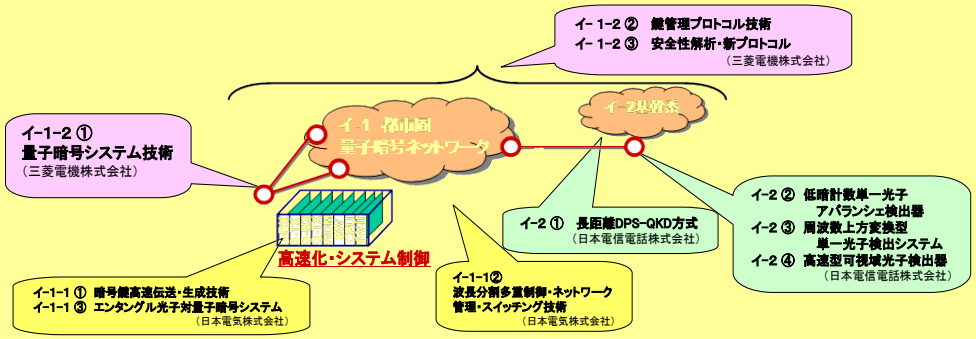

### 4. 研究開発の期間及び体制

– 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

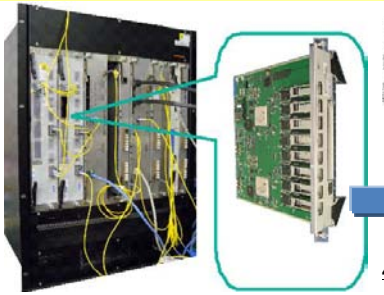
## イ　量子暗号ネットワーク技術の研究

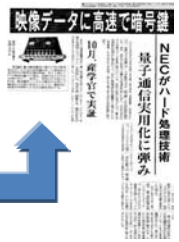
イ-1：都市圏対応型量子鍵配送システム技術の研究開発
　イ-1-1：都市圏量子暗号ネットワーク技術（日本電気株式会社）
　イ-1-2：都市圏量子セキュリティ技術（三菱電機株式会社）
イ-2：基幹回線対応型量子鍵配送技術の研究開発
（日本電信電話株式会社）



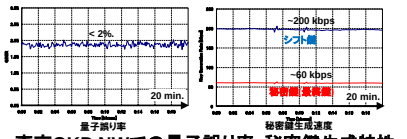

## イ - 1 - 1：都市圏量子暗号ネットワーク技術（日本電気㈱）

- 8波長の量子信号WDM状態で多重による劣化が無いことを確認。鍵蒸留基板も8波長分の信号処理が可能であること、1Mbps以上の鍵速度が可能であることを実証。
- 本課題で試作した量子光基板/同期基板/制御基板/鍵蒸留基板、課題(ア)の成果である光子検出基板、NICT製のSSPDを組み合わせ、1GHz駆動高速QKDシステムを確立した。
- 14dB損失リンクにおいて1波長で80kbpsの最終鍵を達成。8波長多重時に10dB損失換算で鍵速度1Mbps以上に相当する性能を実証した。

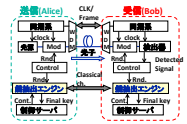

量子暗号装置



4/16日刊工業新聞
（1面、右上トップ、
カラー写真付）



東京QKD NWでの量子誤り率・秘密鍵生成特性

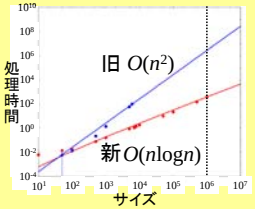


QKD装置ブロック図

## イ - 1 - 2：都市圏量子セキュリティ技術（三菱電機 ㈱）

- デコイ方式を用い偏波補償機能を有する100MHz駆動の量子暗号装置を開発した。また秘匿性増強用のアルゴリズムを新たに提案し、専用ハードウェアを用いずとも、ソフトウェア(PC)のみで鍵蒸留処理をすべて高速に行えることを実証した。
- 大手町−白山間の往復敷設ファイバ24km（JGN2plus）において、本装置を適用し鍵配送に成功した。また、Tokyo QKD Networkにおいて、NICT, NEC,三菱,NTTおよび海外研究機関と共同で鍵リレーやそれを用いたTV会議システムなどネットワーク実験に成功した。（広報発表およびライブデモ）
- 量子鍵配送を用いたワンタイムパッド携帯電話ソフトウェアを開発し、量子暗号の身近なアプリを実現した。（広報発表およびデモ展示）
- 量子暗号の安全性に関する理論研究を行い、その結果を用いて鍵蒸留アルゴリズムを高速化した。またその成果を論文として発表した。


量子暗号装置とワンタイムパッド携帯電話アプリケーション

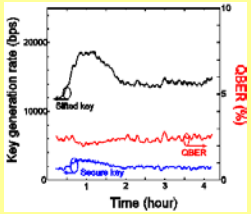


鍵蒸留アルゴリズムの新旧速度比較

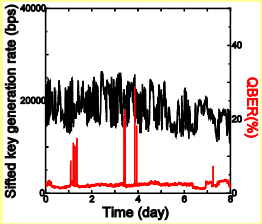
## イ - 2：基幹回線対応型量子鍵配送技術の研究開発（日本電信電話 ㈱）

- 差動位相シフト量子鍵配送（DPS-QKD）をシステム化し、NICTが開発した超伝導単一光子検出器、NECが開発した鍵蒸留基板と組み合わせることにより、実環境敷設光ファイバー約90km(損失27dB)（JGN2plus）上で安定した鍵配送が行えることを示した。
- 4時間に渡る連続最終鍵生成と8日間に渡る安定したシフト鍵生成を行い、最終安全鍵生成レート約2kbps、シフト鍵生成レート　約18kbps、ビット誤り率 約2%であった。
- 暗計数雑音をさらに低減した周波数上方変換モジュール（1810nm励起）を新たに製作. コントローラを一体化した光子検出器として最大効率で暗計数率 $10^{-7}$ Hz/nsec 台を達成した。高速クロック(～GHz)のQKDシステムに適合する。

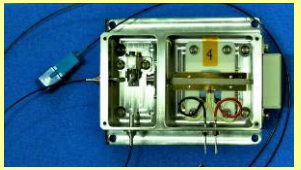

小金井に配置した送受信装置



4時間に渡る最終鍵
生成実験



8日間に渡る連続シフト鍵生成実験


長波長ポンプUCD 新モジュール：
全域で暗計数率 $10^{-7}$ Hz/nsec 台

## 5. これまで得られた成果（特許出願、論文発表等）

| | 国内出願 | 外国出願 | 研究論文 | その他研究発表 | 報道発表 | 展示会 | 標準化提案 |
|---|---|---|---|---|---|---|---|
| 量子暗号の実用化のための研究開発　課題イ | 46<br>(5) | 8<br>(0) | 59<br>(10) | 95<br>(19) | 12<br>(2) | 7<br>(4) | 0<br>(0) |

※累計件数を記載。括弧内は、平成22年度の件数。特許は、取得予定を含む。

## 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）

UQCC2010にて動態デモ、発表など

- UQCC2010にて、高速QKDシステム及び生成鍵を用いた高秘匿TV会議システムの動態デモを実施、同システムの技術に関する招待講演を行い、日本のQKD技術の先進性をアピールした。また、空間伝送デモンストレーション会場にて、ポスター掲示による成果発表を行った。
- 電子情報通信学会英論文誌、QIT研究会、OCS研究会、IEICE総合大会にて各々1件発表を行い、成果アピールを行った。
- 高速鍵蒸留技術について日刊工業新聞に掲載(4/16 1面)、高速量子暗号技術についてOptcomに掲載(6月号)。

■ イ-1-2：都市圏量子セキュリティ技術（三菱電機株式会社）

研究論文 2件、国際会議発表 3件、広報発表 2件、TV取材 2件、取材掲載 30件以上など

- 2010/09/02に広報発表（「量子鍵配送を用いたワンタイムパッド携帯ソフトウェアの開発」）を行った。これにより、世界で初めて通話の解読が原理的に不可能な携帯電話ソフトウェアが実現した。（日経新聞をはじめ、新聞雑誌、WWWなど掲載10件以上。また、9/2テレビ東京WBSで放送。）
- 2010/10/14に広報発表（「量子暗号ネットワークの試験運用開始」）をNICT, NEC, NTTと共同で行った。（新聞、雑誌、WWWなど掲載20件以上。10/29テレビ東京WBSで放送。）
- 国際会議UQCC2010において、Tokyo QKD Networkのライブデモを実施し、また装置開発および安全性に関する口頭発表およびポスター発表を行った。また、量子暗号を用いた携帯電話のデモ展示も同時に実施した。
- 電子情報通信学会（SCIS2011, QIT, ISEC等）などに参加し、成果をアピールした。
- 日経サイエンス2011年1月号にNICT, NEC, 三菱, NTT,海外研究機関によるTokyo QKD Network実験に関する記事が掲載された。
- 量子暗号の安全性に関する理論研究を行い、その成果を安全性の向上および鍵蒸留処理の高速化に役立てた。また国際会議でのポスター発表や(QCMC2010, UQCC2010ほか)、論文投稿も行った(arXiv.org, IEEE Trans. ITほか).

■ 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）

国際会議、国内研究会、及び学会にて発表

- Int. Symp. Physics of Quantum Technology および QIT22 でノイズの元でのQKDの安全性証明に関して報告した。
- UQCC2010 及び光通信システム研究会で基幹網量子鍵配送実験について報告した。
- 応用物理学会のシンポジウムに参加し、基幹網QKDと安全性証明に関し報告した。