平成２３年度研究開発成果概要書
「セキュアフォトニックネットワーク技術の研究開発」
（課題エ　セキュアフォトニックネットワークアーキテクチャ）

（１） 研究開発の目的

情報の安全な共有を実現するための基盤としてのセキュアフォトニックネットワークを構築するにあたっては、安全な通信網の構築技術として、量子鍵配送ネットワーク制御技術、量子暗号安全性評価論、連続量量子鍵配送技術及びその他、最新のネットワーク理論、認証技術等の周辺関連技術を有機的に融合させ、高度化、多様化している盗聴攻撃や撹乱法に対抗可能なセキュアなネットワークアーキテクチャの研究開発を実施する必要がある。このため、量子暗号技術の安定化等の研究を進めるとともに、実際の環境における周辺関連技術との融合、動作検証等を実施し、各種研究成果を有機的に融合させセキュアなネットワークアーキテクチャとして確立する必要がある。

（２） 開発期間

平成２３年度から平成２７年度（５年間）

（３） 委託先企業

日本電気株式会社＜幹事＞
国立大学法人北海道大学

（４） 研究開発予算（百万円）

平成２３年度	３０（契約金額）
平成２４年度	２９（　〃　）
平成２５年度	２７（　〃　）
平成２６年度	２５（　〃　）
平成２７年度	２４（　〃　）

（５） 研究開発課題と担当

課題エ-1　ベースラインモデルの研究（日本電気株式会社）
課題エ-2　周辺関連技術の適用研究（日本電気株式会社）
課題エ-3　量子暗号技術の適用研究（国立大学法人北海道大学）
課題エ-4　環境構築／動作検証（日本電気株式会社）

（６） これまで得られた研究開発成果

（累計）件　　（当該年度）件

特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	2	2
	プレスリリース	0	0
	展示会	0	0
	標準化提案	0	0

具体的な成果

(1)日本電気

量子暗号技術の概要とこれまでの歴史、最近の技術動向について概要説明を実施した。今後、量子コンピュータの実現等により、公開鍵暗号方式などの現代暗号のみでの秘匿性確保が困難になることが想定される。そのため、量子鍵配送技術と既存の技術の融合実現の必要性について説明し、現在実施中の研究における匿名認証技術等の認証技術と量子鍵配送技術融合実現の有効性についての期待感の確認ができた。

(2)北海道大学

量子リレーにおける中継点の信頼度に関する要求を緩和するため、量子グループ秘密分散技術と分散コンピューティング技術を用いた量子リレーのプロトコルを提案した。このプロトコルでは、中継点で鍵に関する情報が分散され、中継点を構成する全てのメンバーが一致しない限り鍵を得ることはできない。また、鍵共有に必要な乱数は中継点の数に対してスケーラブルである。

（７） 研究開発イメージ図

※別添をご参照くださいますよう、お願いいたします。