平成23年度「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
量子暗号技術を活用した安全な通信網の構築技術の研究

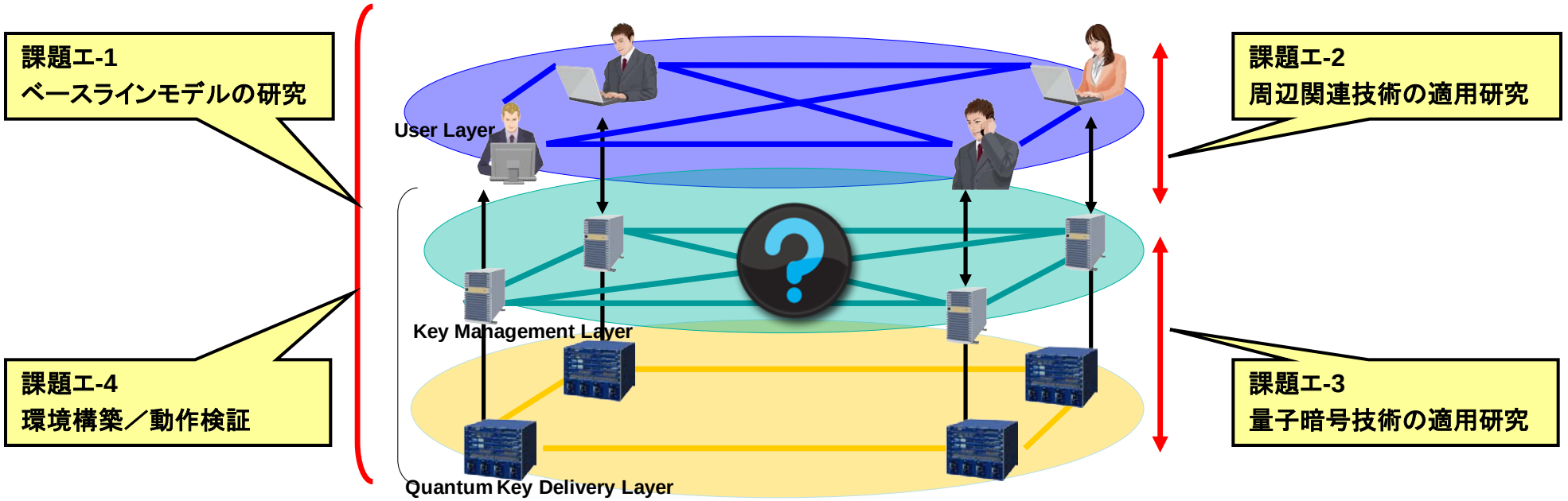
1．実施機関・研究開発期間・研究開発費

■実施機関　　日本電気株式会社（幹事者）、北海道大学
■研究開発期間　　平成23年度から平成27年度（5年間）
■研究開発費　　総額 133百万円（平成23年度30百万円）

2．研究開発の目標

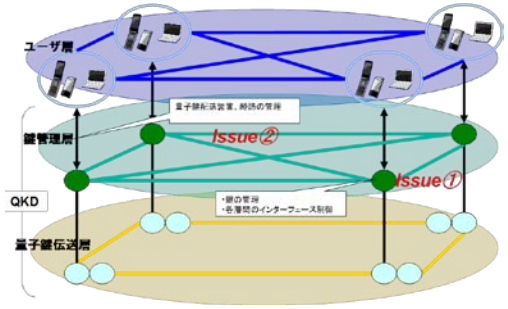
研究開発課題全体の目標としては、物理的安全性が理論的に保証された量子鍵配送技術をベースとして50km圏内の都市圏ファイバネットワーク上に量子鍵配送ネットワークを構築し、500kbps以上の速度で半年以上にわたって鍵を生成し続け長期運転実績を積むと共に信頼性の確立を行う。
そのため、量子鍵配送ネットワーク制御技術を実現する要件より課題エ「(1)ベースラインモデルの研究　(2)周辺関連技術の適用研究　(3)量子暗号技術の適用研究(4)環境構築／動作検証」の4つの技術課題を抽出し、研究開発を遂行する。

平成23年度の目標としては、セキュアフォトニックネットワークアーキテクチャ構築のための第一段階として、社会インフラを構成する典型的な通信環境における暗号通信網の構成方式を定義する。このため、1対1の通信モデルと1対多の通信モデルを定義する。このモデルと具体的利用場面を想定し、「実現のための課題の抽出」「活用周辺関連技術の抽出」を定義する。また、平成24年度以降の検証環境として必要な環境を定義し、課題ア、ウで開発する量子暗号鍵配付装置を用いた（情報通信研究機構殿所有の）ネットワークに必要な市販暗号装置等を活用した検証環境を構築する。



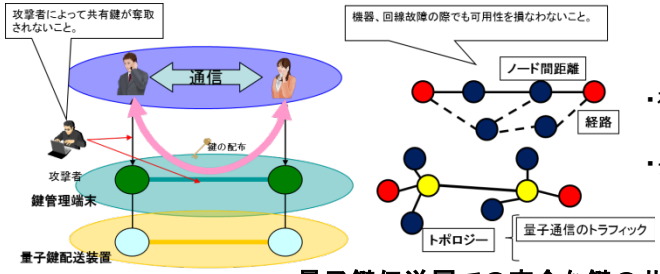
3. 研究開発の成果

課題エ-1 ベースラインモデルの研究 （日本電気株式会社）



大容量データ伝送用鍵の
管理、共有、供給方式

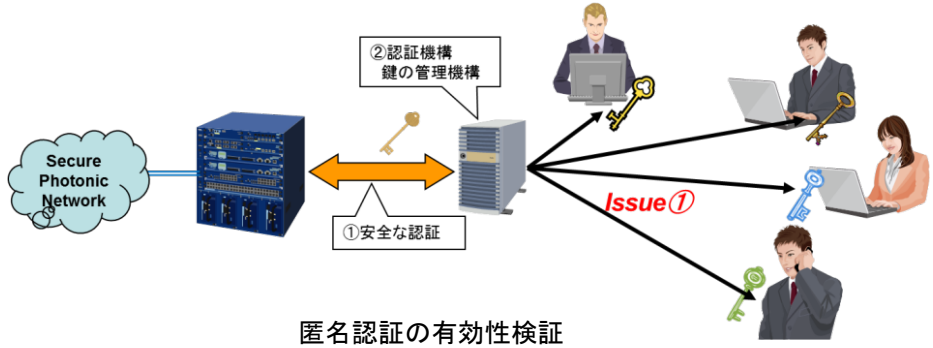
安全な鍵の共有方式と各層の網管理方式



・複数拠点間での
鍵共有方式
・長距離鍵配送方式

量子鍵伝送層での安全な鍵の共有のための要件定義

課題エ-2 周辺関連技術の適用研究 （日本電気株式会社）



匿名認証の有効性検証
（課題アとの連携）

鍵配送に関するアプリケーションインタフェース方式の策定

研究開発成果：ベースラインモデルの開発

【課題】

・残存性を地理的に確保するため、100Km程度の距離を確保してバックアップサイトを構成するデータセンタにおいて、理論上の完全な秘匿性を確保した鍵共有の実現が必要である。
・理論上の完全な秘匿性の確保が保証できないことに起因し、安全な鍵共有を人手に頼っている。この、鍵配送の無人化／自動化の実現が必要である。

【成果】

ベースラインモデルの確定

・典型的な通信モデルを具体的に想定することにより、ネットワークアーキテクチャの妥当性評価が可能なようにベースラインモデルを策定した。
・残存性を地理的に確保する目的のため、１対１のセキュアフォトニックネットワークのベースラインモデルを定義した。具体的には大容量データの伝送用鍵の管理、共有、供給方式を検討するためのベースラインとして、生成した鍵の消費量を局限する方策を検討するためのモデルを定義した。
・鍵配送の無人化／自動化を検討するため、１対多のセキュアフォトニックネットワークのベースラインモデルを定義した。具体的には複数拠点間の鍵共有方式を検討するためのベースラインとして４拠点での鍵共有方式を検討するためのモデルを定義した。

研究開発成果：周辺関連技術の適用研究

【課題】

複数拠点での鍵共有を考えた場合、鍵の配送先の正当性を確認して配送する必要があると共に、中間装置に必要以上の情報を渡さないことを考慮する必要がある。具体的には、相手先の確実な認証と鍵管理機構の検討が必要である。

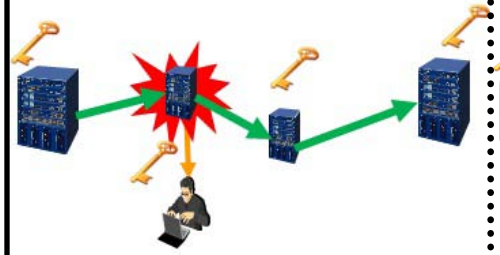
【成果】

周辺関連技術の適用研究

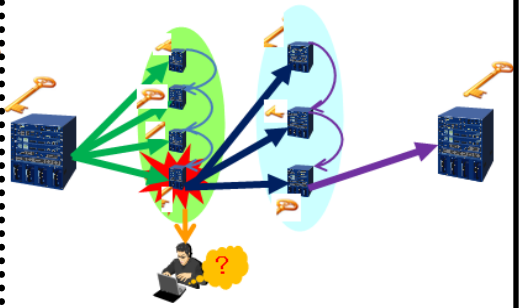
・典型的なベースラインモデルにおける課題を解決するための既存技術を周辺関連技術として抽出した。この抽出された周辺関連技術と量子暗号技術との融合方式を各研究課題受託部門と調整することにより全体課題の解決方式を定義した。
・量子暗号技術活用範囲外の経路におけるエンド-エンドの通信の安全性を匿名認証技術の適用を基準とした検討を行い課題に対応する活用可能な周辺関連技術を抽出した。具体的には匿名認証方式の有効性を確認し、その実現性を検証した。
・ユーザと鍵管理端末間の認証の課題を明確化した。具体的には匿名認証方式の適用方法を検証した。

3. 研究開発の成果

課題エ-3　量子暗号技術の適用研究　（北海道大学）

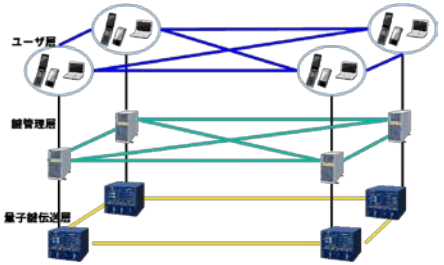


量子リレーにおける中継点のリスク



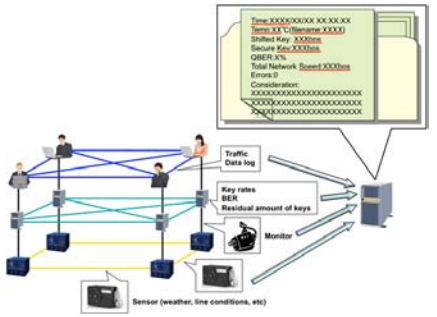
量子グループ秘密分散による解決

課題エ-4　環境構築／動作検証　（日本電気株式会社）



既存装置への鍵供給方式
既存通信網との親和性

全課題(ア、イ、ウ、エ)の課題解決方法の実証環境の確立



温度等の影響の検証環境

温度の影響性の確認環境の確立

研究開発成果：量子暗号技術の適用研究

【課題】

・典型的なベースラインモデルにおいて、認証、(論理)鍵の複数拠点間における効率的な伝送と共有、鍵の有効性管理が課題であり、解決のため活用可能な量子暗号技術・量子通信技術を抽出する。抽出された量子技術を元にしたネットワーク管理方式を提案し、実効性を評価する。さらに、周辺関連技術と融合しネットワーク全体として課題を解決するために必要な量子暗号技術の改変を課題アーウの研究者と共同して行う。最終的に課題エ-2と協力し、安全性とネットワークリソースの両面から最適な方式を選択する。

・量子暗号技術の適用により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ことを検討した。量子リレーで鍵を中継していく際、中継点では鍵情報が古典情報として得られるため、中継点は完全に信頼できるものと仮定する必要がある。

【成果】

量子秘密分散の量子リレーへの適用

・典型的なベースラインモデルにおける課題を解決するために活用可能な量子情報技術として量子グループ秘密分散技術を抽出した。

・抽出された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。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。また、鍵共有にあたり中継点間で伝送される古典情報はパリティのみでこの情報から外部の盗聴者が鍵を再現することはできない。

研究開発成果：周辺関連技術の適用研究

【課題】

・量子鍵配送の仕組みの実用化に向け、既存技術と量子暗号技術の有機的な融合の実現が課題となっている。このため、具体的検証環境を構築する必要がある。

・量子鍵配送装置の長期運転実績の確立、および公開のためには、量子鍵配送装置から統計情報を環境データと供に定期的に収集し、公開サイトに反映させるソフトウェア作成の必要がある。

【成果】

実証環境の構築

・課題エ-1で定義した１対１の通信モデルの検証環境として準備すべき装置構成等を特定し、検証環境を構築した。具体的には、既存Ｌ２暗号装置及びスマートホン等を検証環境に追加した。

・平成24年度以降に実施する通信モデルの検証環境の構築を可能とするため、既存の回線暗号装置等へのインタフェース追加の試作を実施した。具体的にはＬ２暗号器等へ鍵を供給するためのインタフェースを試作した。

・移動端末等を含んだ秘匿通信網の構成モデルを実現するための検証環境の構築を行った。具体的には３Ｇ回線とのインタフェースとしてインターネットアクセスモデルを構築した。

温度の影響性の確認環境

量子鍵配送装置の鍵生成に影響を与える要因として、周囲の温度変化が想定される。この基礎データを収集するため、赤外線サーモグラフィーを検証環境に導入し、周囲の温度変化を記録する仕組みを検証環境として構築した。

4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
量子暗号技術を活用した安全な通信網の構築技術の研究	0 (0)	0 (0)	0 (0)	2 (2)	0 (0)	0 (0)	0 (0)

5. 研究成果発表会等の開催について

（1）某省庁　技術動向調査報告

・課題エ（全般）：　2011年10月～11月、某省庁　技術動向調査報告会（研究企画部門、システム運用部門等が参加）：
技術動向として、量子暗号技術の必要性、セキュアフォトニックネットワーク構築の委託研究の目的及び計画等に関する概要を口頭説明

（2）電子情報通信学会 2012年総合大会

・課題エ-3：　20120年3月21日　電子情報通信学会2012年総合大会
量子グループ秘密分散を用いた量子リレー方式を口頭発表

6. 今後の研究開発計画

この成果により、今後、どのような研究を行うのかを例示を上げながら、具体的、かつ簡潔に記載して下さい。

課題エ-1　ベースラインモデルの開発

周辺関連技術の動向及び量子暗号技術の動向を反映した構成方式の改善案を平成24年度中に実施する方式検討を踏まえ順次改定ベースラインとして提案する。

課題エ-2　周辺関連技術の適用研究

ネットワーク環境を構築する際における具体的な課題を解決するための最新技術動向に基づき周辺関連技術の適用方法を改善策として抽出する。

課題エ-3　量子暗号技術の適用研究

量子リレーにおける課題を解決するための量子グループ秘密分散技術に関し、安全性の検討と実際の通信網に用いる場合の問題点を明らかにし、
安全性の高い量子リレー方式を提案する。

課題エ-4　環境構築／動作検証

課題エ-1で定義したベースラインモデルの拡張に対応することを考慮し、検証環境としての要件を特定し、検証環境を拡張して構築する。
（今後の追加環境として、気象センサー、温度センサーの追加等を含む）