プログラム名：量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現
PM 名：山本 喜久
プロジェクト名：量子セキュアネットワーク

委 託 研 究 開 発

実 施 状 況 報 告 書（成果）

平成２８年度

研究開発課題名：

量子鍵配送プラットフォームの研究開発

研究開発機関名：

日本電気株式会社

研究開発責任者
津村 聡一

Ⅰ　当該年度における計画と成果

１．当該年度の担当研究開発課題の目標と計画

高秘匿量子光送信技術に関して、平成 28 年度では量子光送信の高秘匿化を実現するための技術についての研究開発を行う。当該期間は、前年度までに設計を終え試作に着手した高精度 Decoy を実現する高秘匿量子光送信部の単体およびシステム評価を行う。評価では、光パルス強度揺らぎをはじめとする重要パラメータの測定と分析を行い設計通りに動作することを確認する。

フレキシブル秘匿増強処理実装アーキテクチャに関して、平成 28 年度では秘匿増強処理の高秘匿化を実現するためのアーキテクチャについての研究開発を行う。当該期間では、前年度までに行った秘匿増強処理単位を拡大した場合の規模の見積もりおよび実行時間の見積もり結果に基づいて、リアルタイム処理を実現するための実装検討を行う。

スマート鍵管理実装技術に関して、平成 28 年度はネットワークアーキテクチャ全体を取りまとめる国立研究開発法人情報通信機構（以下、「NICT」）と連携し、実用性の高いスマート鍵管理システムの実装技術の研究開発を行う。当該期間では、前年度までに行ったアーキテクチャ、インタフェースの仕様の検討をさらに進め、検討結果を実現するための実装設計等を通して実用的な実装技術の策定を行う。

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、平成 28 年度は鍵管理層で生成された暗号鍵を情報端末や制御機器で要求されるセキュリティレベルや通信速度に応じて最適に活用するためのアプリケーションインタフェース技術の研究開発を行う。ベースモデルとして前年度までに評価環境を開発したアプリケーション、設計・開発中のアプリケーションを対象とし、当該期間は、評価試験を通して実利用時の運用面の向上等に関する課題点、更なる機能向上・拡張の可能性を抽出し、実用化への検討に繋げる。

２．当該年度の担当研究開発課題の進捗状況と成果

2-1 進捗状況

高秘匿量子光送信技術に関して、平成 28 年度は前年度までに行った設計に基づいて高精度 Decoy を実現するための光送信機を試作し、単体評価およびシステム評価を行った。その結果、目標とする精度を達成する良好な特性を得た。（計画通りに進捗）

フレキシブル秘匿増強処理実装アーキテクチャに関して、リアルタイム処理を実現するためのソフトウェア実装検討および詳細設計を行い、その設計に基づいて鍵蒸留ソフトウェアの試作を行った。（計画を上回る進捗）

スマート鍵管理実装技術に関して、実用性を向上する機能としてシステム間通信のセキュリティ強化機能、鍵供給インタフェースのセキュリティ機能の追加を行なった。また、鍵利用効率向上のための鍵管理方式の実現性について検討を行った。開発機能を実証検証するために高秘匿量子鍵配送装置を構築し、実証環境に組み込み稼働を開始した。（計画通りに進捗）

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、秘匿携帯アプリケーションの開発と動作確認を行った。また、L2 回線暗号装置によってポイントツーポイント接続された全拠点に対して、任意の二拠点間での暗号通信機能の開発と動作確認を実施した。(計画を見直した)

2-2 成果

高秘匿量子光送信技術に関して、光パルス強度を高精度に制御可能な光送信機（図１）を試作し、単体評価を行った。A/D コンバータの精度向上や強度モニタ回路の雑音抑制により、重要パラメータであるデコイパルス強度の調整誤差を従来の光送信機の 4.5%に比べて 1/3 以下の 1.2%に抑制することができた。これにより盗聴者に漏洩する情報量を制限して高安全・高効率な暗号鍵生成を行うことが可能となる。また、本光送信機を量子鍵配送システムに組み込み、実機環境でも正常に動作することを確認した。

図１　光送信機

フレキシブル秘匿増強処理実装アーキテクチャに関して、鍵蒸留ソフトウェアの実装検討および詳細設計を行い、その設計に基づいて鍵蒸留ソフトウェアの試作を行った。図２に試作した鍵蒸留ソフトウェアにおける鍵データ処理のフローおよび送受信機間の通信データを示す。平成 29 年度に実機評価を行う。

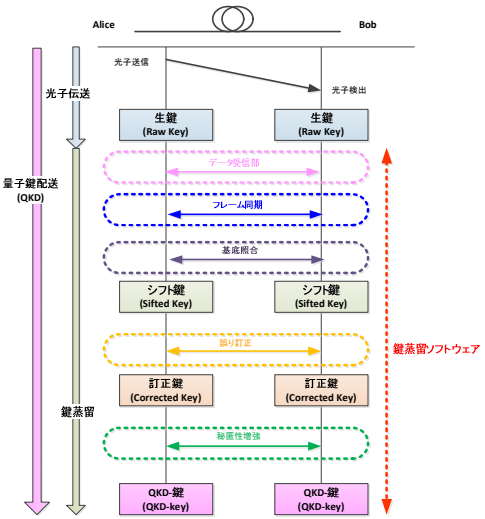

図２　鍵蒸留ソフトウェア

スマート鍵管理実装技術に関して、実運用を見据えてスマート鍵管理システムを構成する鍵管理エージェント（KMA）間などのシステム間通信としてこれまで用いてきた SSL 暗号化機能を量子鍵配送装置（QKD）から供給された鍵を用いた方式に変更した。また、鍵供給エージェント（KSA）とアプリケーション層のインタフェースに、端末（ユーザ）認証機能、データ暗号化を追加することでセキュリティ強化を図り、NICT が保有する評価環境（Tokyo QKD Network）に組み込んだ。

複数のユースケースを想定した鍵利用効率の検討を行った。一例として、アプリケーションの通信特性により暗号化鍵／復号化鍵の使用に偏りが発生し利用効率が悪化する場合を想定し、暗号化鍵と復号化鍵に分離した鍵管理方式から、暗号化鍵と復号化鍵を一元管理する方式に変更するための基本設計を実施した。平成 29 年度に開発を行い評価環境に実装する。

また、開発機能を実証検証するために必要となる高秘匿量子鍵配送装置を構築し、実証環境（Tokyo QKD Network）に組み込み稼働を開始した。

現代暗号と量子暗号の統合による新しいセキュリティ技術に関して、実利用に際し有用な多拠点間通信の実現のため、回線暗号化通信装置がポイントツーポイント接続された全拠点（４拠点）に対して、任意の二拠点間で暗号通信するための機能を開発し、機能評価環境構築と動作確認を実施した（図３）。

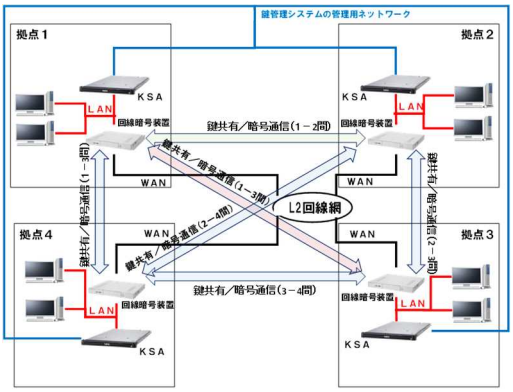

図３　任意の二拠点間での暗号化通信機能評価系

秘匿スマートフォンに関しては、音声、メールの運用から、データ通信まで範囲を広げた秘匿モバイルとしての運用を見据えて、現在の通信環境へのシステム適合、タブレット等への端末適用範囲拡大に必要な機能を追加開発した（図４）。平成 29 年度は、実証環境に組み込み評価試験を通して、鍵の使用量や管理方法、高負荷時の通信処理や実運用面での課題点を抽出し、実用化に向けた機能向上の検討を行う。

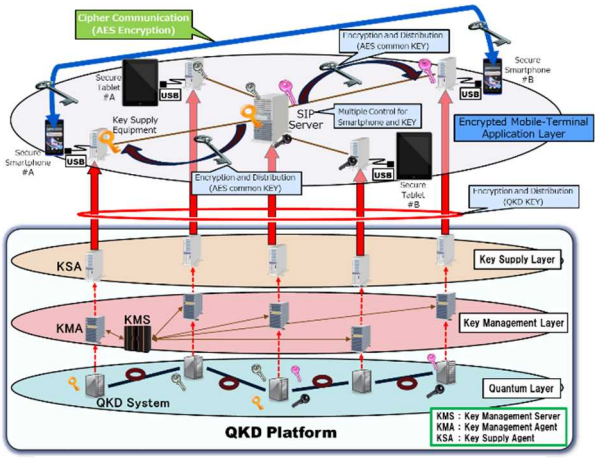

図４　秘匿モバイルを想定したシステムの拡張

2-3 新たな課題など

計画通りに進捗しており、新たな課題は特に生じなかった。

３．アウトリーチ活動報告

特になし。