グローバル量子暗号通信網構築のための研究開発

基本計画書

１．目　的

近年の量子コンピュータ研究の加速化により、実用的な量子コンピュータが実現されることで、現代暗号で守られて

いたデータが全て解読されてしまう事態が懸念されている。従って、量子コンピュータ時代においても、国家間や国内重要機関間で機密情報を安全にやりとり可能とするため、国として、広域的な量子暗号通信ネットワーク技術を確立し、極めて堅牢性の高いサイバー空間を実現する必要がある。

現在、量子暗号通信の基盤となる技術の確立に向けて、100km 圏内を対象とした地上の２地点間の量子暗号通信技術やトラステッドノード技術の研究開発（内閣府 SIP 第二期）、及び衛星通信における量子暗号技術の研究開発（総務省委託研究）に取り組んでいるところである。特に、SIP 第二期では、長期にわたって守るべきデータを扱う医療分野や生体認証分野等のユーザニーズを基にした、実用性の高い量子暗号通信ネットワーク技術の研究開発と社会実装を進めている。

さらに、グローバル規模での量子暗号通信ネットワークの実現に向けて、数百 km～数千 km といった通信の長距離化へのニーズも存在しているが、地上系のみでは、量子暗号通信の直接伝送の距離・速度限界のため、多地点を含む広域化とスケール性確保には課題がある。一方、衛星系では、宇宙空間において通信品質が劣化せず長距離化が容易である反面、高度な衛星捕捉追尾技術が必要、かつ長期の悪天候時に地上局と通信できなくなる恐れがある等の課題がある。従って、前述の実施中の研究プログラムで開発している地上系及び衛星系の個々の要素技術の高度化に加え、双方を組み合わせた統合ネットワーク化が不可欠である。

本研究開発では、グローバル規模で量子暗号通信（情報理論的安全性が保証されているものに限定。以下、同じ。）が可能なネットワークの実現に向けて、国家間や国内重要機関間、また医療・金融分野等での機密情報のやりとりをユースケースとした要素技術の確立に向けた研究開発を実施する。具体的には、実用性が高く、かつ通信のさらなる高速化・長距離化が可能な（１）量子通信・暗号リンク技術、（２）トラステッドノード技術、（３）量子中継技術、及び（４）広域ネットワーク構築・運用技術を確立する。

２．政策的位置付け

『統合イノベーション戦略 2019』（令和元年 6 月 21 日閣議決定）において量子技術

が主要分野とされているところ、その個別戦略である「量子技術イノベーション戦略（最終報告）」（令和２年１月 21 日）において、重点領域として、量子通信、量子暗号、光通信チャネルとの並存技術等に関する総合的かつ戦略的取組を強力に推進する、とされている。

『成長戦略 2019』（令和元年６月 21 日閣議決定）において、量子に関する主要技術領域におけるファンディング・研究機関の取組の重点化・強化、国際研究開発拠点の推進、人材育成の推進、とされている。

『世界最先端デジタル国家創造宣言・官民データ活用推進基本計画』（令和元年 6 月 14 日閣議決定）において、量子通信技術等の研究開発を強化するとともに、その成果のビジネス支援やオープンイノベーションを促進する環境整備を行い、海外展開を見据えた我が国技術優位性を確保する、とされている。

『デジタル変革時代の ICT グローバル戦略懇談会報告書』（令和元年５月 31 日）において、量子 ICT 技術が、オープンイノベーションによるキーテクノロジーとして位置づけられており、その高度化にむけた方向性の１つである安全安心なデータ主導社会の実現に向けて、盗聴できないことが数学的に保証された秘匿性の高い通信を地球規模で実現することにより通信の安全性が大幅に向上する、とされている。

『経済財政運営と改革の基本方針 2019～「令和」新時代：「Society 5.0」への挑戦～』（令和元年６月 21 日閣議決定）において、全ての科学技術イノベーションに影響する最先端の基盤的技術であるＡＩ、バイオテクノロジー、量子技術の研究開発を戦略的に進める、とされている。また、生活習慣病・認知症対策、防災・減災、再生医療、ゲノム医療、ＡＩ、量子、革新的環境エネルギー等の社会的課題解決に資する研究開発を官民挙げて推進するとともに、政府事業・制度等の一層のイノベーション化を進める、とされている。

３．目　標

（１）政策目標（アウトカム目標）

高い可用性（盗聴攻撃や災害等への高い耐性）のもとでグローバル規模の量子暗号通信を実現するためには、今までに開発してきた 100km 圏量子暗号通信ネットワークよりもさらに通信の長距離化が可能な技術が必要であり、量子暗号装置や中継器等の性能を向上し、そしてまだ世界でも実現していない多地点間メッシュ型の大規模ネットワークを構築するための管理制御技術等を確立する必要がある。

そこで、Tokyo QKD（Quantum Key Distribution）Network のような既存の量子暗号通信ネットワークの大規模化、具体的には数百 km 圏で実用性の高い量子暗号通信を実現するための要素技術として、２地点間の（１）量子通信・暗号リンク技術、中継としての（２）トラステッドノード技術と（３）量子中継技術、及び多地点間通信のための（４）広域ネットワーク構築・運用技術を確立することによって、グローバルな量子暗号通信ネットワークの実現に寄与する。

また、開発成果の国際標準化や市場展開を推進し、我が国の量子暗号通信技術の国

際的な競争力を強化する。

（２）研究開発目標（アウトプット目標）

グローバル規模の量子暗号通信ネットワークの構築を目指し、地上系の数百 km 圏において、ノード数が２桁以上で、万単位のユーザ端末の収容及び鍵供給を可能とし、100kbps 以上の暗号鍵生成スループット、及び高い安全性と可用性を同時に可能とする技術を実現する。また、都市圏距離において 1Mbps 程度の暗号鍵生成速度を達成する量子暗号装置を実現する。

さらに、衛星系ネットワークと地上系ネットワークを組み合わせることで、既存の量子暗号通信ネットワーク（例：Tokyo QKD Network）の 10 倍以上の大規模化、具体的には 1,000km 圏で実用性の高いネットワークを構築可能な技術について、基礎調査も含めた検討を行う。

４．研究開発内容

（１）量子通信・暗号リンク技術

① 概要

地上系量子通信チャネルにおける通信のさらなる長距離化及び高速化に資する新たな量子鍵配送（QKD）方式や、高効率単一光子検出器や広帯域光検出器といったデバイス技術等を開発し、それら開発技術を組み込んだ量子暗号装置を作製する。

② 技術課題

ア）量子暗号通信の高性能化技術

グローバル規模の量子暗号通信ネットワークの実現のためには、ネットワークの各リンクで要求される速度・距離等に応じた量子暗号通信の高速化や長距離化が必須である。高速化は、デコイ BB84 や CVQKD（Continuous-Variable QKD）など既存の量子鍵配送方式における送信機や検出器の高速化、量子暗号通信チャンネルの多重化などにより実現できると期待される。一方、伝送距離の長距離化は、検出器の低雑音化や、新たな量子鍵配送方式（例えば、Twin-Field QKD）などの開発により実現できると期待される。そこで、これらをそれぞれ実現するための要素技術に関する研究開発を行った上で、光源や検出器、符号器、復号器等で構成された量子暗号装置に開発技術を組み込むシステム化を行う。

イ）光子検出技術

上記課題の実現において、以下の検出器開発が重要となる。

a）低雑音光子検出技術

量子暗号通信の長距離化及び高速化のためには、２地点間の量子通信リンクの受信側における単一光子検出精度（雑音耐性等）の向上が必要である。

b）広帯域ホモダイン検出技術

単一光子検出による方式と比較して、性能面（通信の距離及び速度）よりも、コスト面や早期実現が求められる場合、通信波長帯（1310nm または 1550nm 帯）における既存の光ファイバー及び関連機器の活用など（例えば波長多重等の非量子暗号通信チャネルとの並存等）によって、安価に量子暗号通信を実現できる広帯域ホモダイン検出技術が必要である。

③ 到達目標

ア）量子暗号通信の高性能化技術

現在の敷設環境で動作している量子暗号装置と比較して、同一距離のもとで３倍程度の高速化（例えば敷設ファイバー45km で鍵生成速度１Mbps 程度）を実現可能な技術を開発し、それを組み込んだ新たな量子暗号装置を作製する。

また、同一の速度のもとで、現在敷設環境で動作している量子暗号装置の量子鍵配送方式では原理的に不可能な長距離化（例えば、超低損失ファイバーで 500km 相当）及びメンテナンスの容易化等を実現可能な技術に関する研究開発を行う。

イ）光子検出技術

a）低雑音光子検出技術

量子暗号通信の長距離化を可能とするため、半導体素子検出器の高性能化等により、従来の 1/4 以下のタイムウィンドウ（100ps 程度）で光子検出可能な技術について、実用に適した検出技術の研究開発を行う。

b）広帯域ホモダイン検出技術

量子雑音限界に近い信号/雑音特性での広帯域光ホモダイン検出（帯域２GHz 以上、ショット雑音/回路雑音比９dB 以上）が可能な技術の研究開発を実施する。

（２）トラステッドノード技術

① 概要

安全保障関連やゲノム・医療情報等の世紀単位の超長期間にわたるセキュリティを確保する必要があるデータには、トータルシステムとして、情報理論的安全性を保証する必要がある。本課題では、ハードウェア面及びソフトウェア面の双方で、量子暗号通信による情報理論的安全性を保つことを前提とした鍵の生成・配送・保管・消去等が可能なシステムを新たに開発する。

地上系の実用的な量子暗号通信ネットワークでは、盗聴者が電気的・物理的にアクセスできない環境を有する局舎、いわゆるトラステッドノードを設け、その中に量子暗号装置を設置し、生成された暗号鍵を安全に分割・統合、保管、及び鍵リレー中継（いわゆる鍵管理）し、ネットワーク化・長距離化を実現する方式が用いられている。トラステッドノード内でこのような鍵管理を行うのが鍵管理サーバであ

り、実際的なセキュリティ脅威が集中する部分でもあり、その高信頼化は依然、実用上重要な課題となっている。そこで、高信頼な鍵管理サーバのシステム実装技術の研究開発を行う。

また、量子暗号通信ネットワーク上で暗号鍵や重要データを複数の経路とトラステッドノードに秘密分散しながら配送・保管し、また秘匿性を保ったままマルチパーティー計算することにより、サービス停止攻撃やネットワーク障害があっても機密性・完全性を損なわず可用性の高いネットワーク運用やセキュリティサービスを実現することが可能になる。また、ネットワーク符号化技術等と組み合わせることで配送効率やスケール性を向上させることができると期待される。そこで、秘密分散技術、マルチパーティー計算技術、ネットワーク符号化技術等を活用した新たな量子暗号通信ネットワーク技術を研究開発し、有効性を実証する。

② 技術課題

ア）鍵管理サーバ技術の高信頼化

鍵管理サーバでは、量子暗号装置で生成された暗号鍵が電気的に保管・処理されておりその安全性、いわゆる耐タンパー性の確保が極めて重要である。特に、サイバー攻撃や災害等によって中継点の局舎が機能不全状態に陥っても鍵管理サーバ内では安全に鍵の管理・処理・保管・消去等が実行できる技術は実運用上、重要となる。そこで、鍵管理サーバのシステム全体を堅牢化し、さらには、不正開封時の情報漏えい防止や、トラステッドノードの障害の状況をリアルタイムで把握するためのモニタリング技術等、耐タンパー性を保証する技術の研究開発を行う。

イ）高度分散化技術

量子暗号通信ネットワークで繋がれた複数のデータサーバに原本データを秘密分散保管することにより、一定数以下の分散データが、盗聴されるか、もしくは棄損しても、原本データの機密性を長期間にわたって守り、かつ必要時に復元することができ、さらに無意味化された分散データのまま情報処理を行うマルチパーティー秘匿計算技術も実現できる。さらに、暗号鍵自体を複数のトラステッドノードと経路に秘密分散しながら配送・保管・マルチパーティー処理することにより、サービス停止攻撃やネットワーク障害に強く可用性の高い鍵配送・供給サービスが可能になる。

秘密分散技術、マルチパーティー計算技術を活用した機密性・完全性・可用性の高い量子暗号通信ネットワーク技術、及び供給された暗号鍵を用いて重要な原本データを分散保管・処理するネットワークアプリケーション技術の研究開発を行う。

さらに、ネットワーク符号化技術等を導入することで、大規模ネットワーク上でもスケール性を保持し高効率に暗号鍵やデータを安全にリレー配送・保管・処理する新しい技術の研究開発を行う。

③ 到達目標

ア）鍵管理サーバ技術の高信頼化

鍵管理サーバへの具体的な攻撃としては、例えばサイドチャネル攻撃、フォールトベース攻撃、侵入型・非侵入型攻撃等が考えられる。また、災害等による局舎の機能不全化も想定される。これらを含めた想定される攻撃手法の分析を行った上で、攻撃の防止、検知、データ消去等の攻撃への反応、攻撃の痕跡を残す仕組み等、適切な対策を具備した高信頼鍵管理サーバ技術を確立し、ハードウェアモジュールを作製する。

イ）高度分散化技術

サービス停止攻撃やネットワーク障害への可用性を高めるため、従来の単一経路リレー方式に対して、３倍程度の経路・ノード冗長性を有する分散型リレー中継方式を開発し、情報処理機能としては３パーティ以上の秘匿計算を１Mbps 以上の速度で実行する技術を開発する。さらに、ネットワーク符号化技術等を導入した高スケール性・高効率化に関しては、基礎理論の構築とシミュレーション等による実証を行い、基本設計を確立する。

（３）量子中継技術

① 概要

地上系において、量子暗号通信の更なる長距離化、及びトラステッドノードよりも安全な暗号鍵の中継を実現するため、量子中継技術に関する研究開発を行う。量子中継技術として、ネットワークの中継点において量子状態を一定時間保持できる量子メモリ技術やその周辺技術の開発、また全光量子中継や波長多重量子中継等の新方式の基盤技術開発を対象とする。

② 技術課題

ア）量子メモリの光リンク技術

情報の損失による伝送距離の限界を破るためには、量子状態を保持できる量子メモリ技術を実現し、量子メモリ内での量子操作や光との量子メディア変換、量子波長変換等を駆使して十分離れた中継点に置かれた量子メモリの間を光でリンクする必要があるが、このリンク技術は確立されていない。そこで、量子メモリ技術の研究開発に加え、十分な長さの光ファイバーでつながれた複数の量子メモリを光で接続し、量子メモリ間での量子ビットの中継（転送）操作（量子もつれ等）を実現するための研究開発を行う。

イ）量子中継基盤技術

量子メモリ間のリンクを大規模化していくためには、量子メモリの研究開発に加えて、量子波長変換、波長多重化、量子メモリと光のインターフェース等の周

辺技術の高度化や、量子メモリを使わない全光量子中継方式や複数モードを用いる波長多重化方式等、新しい量子中継方式の検討が重要である。そこで、これら量子中継の基盤技術を確立するための研究開発を行う。

③ 到達目標

ア）量子メモリの光リンク技術

独立して動作する２個以上の量子メモリ間を 10km 以上の光ファイバーで接続し、量子ビットの中継（転送）操作を１秒に 10 回以上の頻度で生成するための技術を確立する。

イ）量子中継基盤技術

量子メモリ以外に重要となる量子波長変換、波長多重化、量子メモリと光のインターフェース等に関する基盤技術を確立する。また、全光量子中継方式や波長多重量子中継方式など、新しい量子中継の方式に関する研究開発を実施し、その基本動作を実証する。

（４） 広域ネットワーク構築・運用技術

① 概要

量子通信・暗号リンク技術やトラステッドノード技術、量子中継技術等を組み合わせて多地点間通信を可能とするため、量子暗号通信ネットワークの広域化に資するネットワーク制御管理技術の研究開発を行う。

② 技術課題

ア）ネットワーク制御管理技術

量子暗号通信ネットワークの大規模化のためには、多地点間通信を可能とするためのメッシュ型ネットワークの構築・運用技術、さらには複数方式の量子暗号通信を連携して動作させるための制御技術、及び複数方式の量子暗号通信ネットワークにまたがる安全な広域鍵管理技術等が必要である。

ハードウェア面では、異なる QKD 方式の暗号装置及び異なるベンダ装置を、いかに相互接続するかが課題である。ソフトウェア面では、送受信間で複数の QKD 方式のネットワークをまたいで暗号鍵を共有するために、各々の QKD 方式の特徴（例えば、伝送距離やシステム全体の消費電力、セキュリティ、動作の安定性等）を考慮に入れて、例えば、送受信間の通信経路の動的な設定や、ユーザ（パーティ）毎の鍵配送速度の柔軟な設定・変更、量子鍵配送用の波長等のリソースの柔軟な割り当て等、量子暗号通信技術に特化した制御管理技術を開発する必要がある。

③ 到達目標

ア）ネットワーク制御管理技術

ノード数が２桁以上で、万単位のユーザ端末の収容及び鍵供給を可能とする量子暗号通信ネットワークを構築するための要素技術を開発する。異なる QKD 方式の暗号装置及び異なるベンダ装置の相互接続を実現する。また、動的な経路設定や、鍵配送速度の動的設定、量子鍵配送用リソース割り当て等、ネットワーク内で３種類以上の方式の量子暗号装置の連携動作を可能とし、かつ複数方式のネットワークにまたがる安全な広域鍵管理の技術等を確立する。また、QKD ネットワークを効率的に運用するための新たな制御管理技術等を確立する。

５．研究開発期間

令和２年度から令和６年度までの５年間

６．その他　特記事項

（１）特記事項

提案者は、下記課題（１）-ア)、（１）-イ）、（２）-ア)、（２）-イ)、（３）-ア)、（３）-イ)、（４）-ア）のいずれか又は複数の課題に提案することができる。
ただし、課題（１）-イ）についてはさらに小さい課題単位(例：課題（１）-イ)-a))の提案も可能とする。

課題（１）-ア）の受託者は課題（１）および本研究開発課題全体のとりまとめ、課題（２）-ア）の受託者は課題（２）のとりまとめ、課題（３）-ア）の受託者は課題（３）のとりまとめ、課題（４）-ア）の受託者は課題（４）のとりまとめを行うものとする。

但し、本研究開発課題全体のとりまとめについては、課題（１）とは別の課題（(２)、（３)、もしくは（４)）をとりまとめとする提案も可とする。

（１）量子通信・暗号リンク技術
　　ア）量子暗号通信の高性能化技術
　　イ）光子検出技術
　　　　a) 低雑音光子検出技術
　　　　b) 広帯域ホモダイン検出技術
（２）トラステッドノード技術
　　ア）鍵管理サーバ技術の高信頼化
　　イ）高度分散化技術
（３）量子中継技術
　　ア）量子メモリの光リンク技術
　　イ）量子中継基盤技術
（４）広域ネットワーク構築・運用技術

ア）ネットワーク制御管理技術

（２） 提案及び研究開発に当たっての留意点

① 提案に当たっては、基本計画書に記されているアウトプット目標に対する達成度を評価することが可能な具体的な評価項目を設定し、各評価項目に対して可能な限り数値目標を定めること。また、アウトカム目標の達成に向けた適切な研究成果（アウトプット等）の取扱方策（研究開発課題の分野の特性をふまえたオープン・クローズ戦略を含む）について提案すること。

② 実用化については、量子暗号通信ネットワーク及び関連技術に関するこれまでの内外の成果動向を記載のうえ、その点をふまえて実用化目標年度、実用化に至るまでの段階を明示した取組計画等を記載し、提案すること。また、製品・サービスの実現に向けたアプローチが考えられる場合には、製品として実装する際のコスト等（メンテナンス等の後年度負担やソフトウェア産業への展開も含む）への配慮を含め、具体的な取組計画を記載しつつ、提案すること。

③ 目標を達成するための具体的な研究方法、実用的な成果を導出するための共同研究体制又は研究協力体制について研究計画書の中にできるだけ具体的に記載すること。複数機関による共同研究を提案する際には、分担する技術間の連携を明確にし、インターフェースを確保すること。

④ 研究開発の実施に当たっては、関連する要素技術間の調整、成果の取りまとめ方等、研究開発全体の方針について幅広い観点から助言を頂くと共に、実際の研究開発の進め方について適宜指導を頂くため、学識経験者、有識者等を含んだ研究開発運営委員会等を開催する等、外部の学識経験者、有識者等を参画させること。なお、本件について不明点がある場合は、本研究開発の担当課室まで問い合わせること。

（３） 人材の確保・育成への配慮

① 研究開発によって十分な成果が創出されるためには、優れた人材の確保が必要である。このため、本研究開発の実施に際し、人事、施設、予算等のあらゆる面で、優れた人材が確保される環境整備に関して具体的に提案書に記載すること。

② 若手の人材育成の観点から行う部外研究員受け入れや招へい制度、インターンシップ制度等による人員の活用を推奨する。また、可能な限り本研究開発の概要を学会誌の解説論文で公表するなどの将来の人材育成に向けた啓発活動についても十分に配慮すること。これらの取組予定の有無や計画について提案書において提案すること。

（４） 研究開発成果の情報発信

① 本研究開発で確立した技術の普及啓発活動を実施すると共に、実用に向けて必要と思われる研究開発課題への取組も実施し、その活動計画・方策については具体的に提案書に記載すること。

② 研究開発成果については、原則として、総務省としてインターネット等により発信を行うとともに、マスコミを通じた研究開発成果の発表、講演会での発表等に

より、広く一般国民へ研究開発成果を分かりやすく伝える予定であることから、当該提案書には、研究成果に関する分かりやすい説明資料や図表等の素材、英訳文書等を作成し、研究成果報告書の一部として報告する旨の活動が含まれていること。さらに、総務省が別途指定する成果発表会等の場において研究開発の進捗状況や成果について説明等を行う旨を提案書に記載すること。

③ 本研究開発終了後に成果を論文発表、プレス発表、製品化、Web サイト掲載等を行う際には「本技術は、総務省の「グローバル量子暗号通信網構築のための研究開発」（令和２年度一般会計予算）による委託を受けて実施した研究開発による成果です。」という内容の注記を発表資料等に都度付すこととする旨を提案書に明記すること。