量子暗号通信網の早期社会実装に向けた研究開発

基本計画書

１．目　的

国際的な量子コンピュータ開発競争の激化による技術的な進展により、現在インターネット等で広く使われている公開鍵暗号（RSA 暗号、楕円曲線暗号等）アルゴリズムが 2030 年代には危殆化する可能性が指摘されている。また量子コンピュータが実用化されるまでの間に暗号処理されたデータを盗聴などにより収集しておき、量子コンピュータが実現したタイミングで一気にデータの解読を行う事が懸念されており、対策が急務となっている。そのため、これらの対応策として、量子力学的性質を活用した「量子暗号」の重要性が高まってきている。

量子暗号では、暗号鍵の共有に「量子鍵配送（QKD）」を用いるため、盗聴を確実に検知することが可能である。また、量子鍵配送による鍵共有技術と、量子コンピュータを用いても絶対に解読できないことが証明されているワンタイムパッド暗号化方式を組み合わせることで、原理的にどんな計算機でも解読することができない「情報理論的安全性」を有する量子暗号が実現できる。一度漏洩すると重大な影響がある安全保障や外交に関する情報、個人のゲノム情報などをはじめとした情報の安全な伝達を実現するためには、量子暗号を用いた高秘匿通信網「量子暗号通信網」の高機能化及び早期社会実装に向けた研究開発が必要である。量子鍵配送装置については、鍵生成速度や最大伝送距離等の観点から我が国のベンダーが世界トップレベルの技術を有しており、装置の製品化も実現している。しかしながら、社会実装に向けては、鍵生成速度や伝送距離の更なる向上や、広域網を中継・制御するネットワーク化技術の確立のほか、データ通信回線との統合や通信相手及び内容の検証のための運用・認証技術の開発が求められている状況にある。また、世界各国においても、量子鍵配送技術の研究開発、量子鍵配送網の構築・運用に向けた取組が加速している。こうした状況の中、量子暗号通信分野における我が国の優位性を維持し、国際的な競争力を確保するためには、産学官の総力を結集してこれらの技術のさらなる研究開発を行い、社会実装を加速することが必要である。また経済安全保障の観点からも自国において競争力の高い量子鍵配送技術を有しておくことが重要である。

本事業では、量子暗号通信の 2030 年頃までの社会実装に向けた研究開発を目的とする。

２．政策的位置付け

「統合イノベーション戦略 2024」（2024 年６月４日閣議決定）において、「量子技術に関する基礎研究や応用研究に着実に取り組むとともに、量子技術と基盤技術（AI 技術や古典計算基盤等）の融合を推進する。さらに、グローバルサプライチェーンの構築・強靭化、国際標準化活動の推進、量子計算資源や量子暗号通信等の利用環境の整備を進め、バイオ、マテリアル等の多様な分野における実用的なユースケースの創出・実証、スタートアップや新事業等の創出を支援する」などとさ

れている。

「新しい資本主義のグランドデザイン及び実行計画2024改訂版」(令和６年６月21日閣議決定)において、「量子コンピュータや量子暗号、量子センサ等のテストベッド利用環境の充実を加速・強化する。さらに、我が国が不可欠なグローバルサプライチェーンの構築に向けた研究開発、研究・専門人材の育成、国際標準化活動の推進、グローバル展開・連携機会の創出、ユースケースの創出・実証に取り組む」とされている。「経済財政運営と改革の基本方針 2024」(令和６年６月21日閣議決定)においては、「新たな産業の芽となるフュージョンエネルギーや量子、経済社会を支える基盤的な技術・分野であるAI、バイオ、マテリアル、半導体、Beyond 5G (6G)、健康・医療等について、分野を跨いだ技術の融合による研究開発、産業化、人材育成を俯瞰的な視点で強力に推進するとともに、グローバルな視点での連携を強化し、市場創出等に向けた国際標準化などの国際的なルールメイキングの主導・参画や、Ｇ７を始めとした同志国やASEAN・インドを含むグローバル・サウスとの国際共同研究、人材交流等を推進する」とされている。「デジタル社会の実現に向けた重点計画」(令和６年６月21日閣議決定)においては、「AI、量子コンピュータ、デジタルツイン、Beyond 5G (6G) 等の実装フェーズに入った技術については、先んじて徹底的に利用していくことが重要となる。政府調達や政府による利用が果たす役割も極めて大きいため、官民の役割を整理した上で、利用促進に向けた所要の措置を講じていく」とされている。

また、我が国が世界に先駆け量子技術イノベーションを牽引すべく、量子コンピュータや量子暗号通信、量子センシング等について研究開発から社会実装までの幅広い取組を推進すべく「量子技術イノベーション戦略 (最終報告)」(令和２年１月 21 日統合イノベーション戦略推進会議) が策定され、その後の国際的な量子技術に係る投資・開発の拡大を踏まえ「量子未来社会ビジョン」(令和４年４月22日統合イノベーション戦略推進会議)、「量子未来産業創出戦略」(令和５年統合イノベーション戦略推進会議) が策定された。さらにその３戦略を補完するものとして策定された「量子産業の創出・発展に向けた推進方策」(令和６年４月９日量子技術イノベーション会議) においては、「量子未来社会ビジョン」に掲げた2030年目標の実現に向け、国際連携に関する取組をさらに強化し、官民一体となった量子技術イノベーションに関する総合的かつ戦略的な取組を強力に推進することとされている。

３．目　標

（１）政策目標（アウトカム目標）

鍵生成速度の高速化・伝送距離の長距離化等技術の確立により、実利用環境においても高機能な量子鍵配送装置を実現し、量子コンピュータが実用化された際にも、重要データの安全な保管や秘匿通信等を可能とする。また、大規模な量子鍵配送網の情報理論的安全な運用・管理を実現するための最適制御・高信頼化技術や、マルチユーザに対応した相手認証等の量子暗号通信網の高機能化技術等の確立により、高い実用性を有した高秘匿通信インフラを構築する。これらの開発成果により、量子暗号通信網の早期の社会実装を実現し、国際競争力強化・サイバー空間の安全性を確保することを政策目標（アウトカム目標）とする。

（２）研究開発目標（アウトプット目標）

本研究開発により、技術課題（１）量子鍵配送技術の高度化、（２）量子鍵配送網における鍵管理技術の高度化、（３）量子暗号通信網の高機能化と統合実証、を実施し当該技術を確立する。本研究開発に係る特許の取得や国際標準の獲得、また量子鍵配送装置の実装安全性を証明するための認証制度を確立し、本研究開発成果の製品化や国際市場への展開を研究開発目標（アウトプット目標）とする。

４．研究開発内容

（１）量子鍵配送技術の高度化

①　概要

プロジェクト終了時に世界トップレベルの性能を有する実用性・信頼性の高い量子鍵配送装置を実現するため、量子鍵配送における鍵生成速度の高速化、伝送距離の長距離化及び広域化、オール光ネットワークとの統合技術の研究開発及び実用性検証を実施する。

②　技術課題

ア）鍵生成速度の高速化技術

量子鍵配送の利用を拡大するためには、鍵生成レートの高速化と装置の小型化を実現するとともに、暗号通信機器としての堅牢性・安定性・信頼性・可用性の向上が必要である。そのため、安全性証明や装置が満たすべき物理的要件である実装安全性の検討において最も充実しているデコイ BB84 型の量子鍵配送装置に関し、波長多重、光子検出器の性能向上等により鍵生成レートの高速化を実現する。また、量子乱数発生器のさらなる高速・高精度化のための技術開発や量子鍵配送装置構成部品の小型化・モジュール化を実現し、実装安全性検証を容易とする構成を実現するとともに、実環境でも安定した鍵生成を可能とする技術を確立する。

イ）伝送距離の長距離化・広域化技術

トラステッドノードを介さず量子鍵配送の長距離化を実現する技術として Twin Field QKD（TF-QKD）方式の実用化が期待されており、低雑音光子検出器による性能向上と最適化に重点が置かれた研究が世界中で加速している。そのため、耐環境性能を備えた装置の研究開発及び実用性検証を実施する。さらに、広域化によるユーザ数やサービスエリアの効率的拡大を図るため、多拠点の時分割切り替えを可能とするスター型の TF-QKD 装置の研究開発を行う。タイムスロット毎に、ユーザノードの中間に位置する検出ノードを異なるユーザペアに割り当てることで、多数のユーザペア間で検出ノードを共有する機能を開発する。これらの研究開発により TF-QKD による長距離化・広域化の実証を行う。

また、ファイバリソースが制限されるメトロ・アクセス網におけるユーザ拠点への導入を想定し、データ信号との同一ファイバ内での共存に優れたデジタルコヒーレント CV-QKD 方式について、光集積回路の適用による小型実装で、実装安全性と運用容易性を高めた構成を実現する。また、高密度な大都市部でのアクセス網では、ルータ・スイッチを介さず、ユーザ間をダイレクトに接続するダークファイバを自由に追加敷設することは困難とされ、新たに管路建

設を工事することは膨大なコスト増加を引き起こす可能性が想定されるため、そのような過密な都市環境での通信を高秘匿化する技術として、背景光の影響を受けにくいCV-QKD方式による空間 QKD の研究開発を行い、地上間における自由空間を介した量子鍵配送を実現することにより、量子鍵配送ネットワークの広域化の実証を行う。

ウ）量子鍵配送とオール光ネットワークの統合技術

量子鍵配送網を広域展開するためには、専用のダークファイバインフラを用いるのではなく通信事業者で広域展開されることが想定されるオール光ネットワークにオーバレイする形で実現するアプローチが効率的である。そのため、オール光ネットワークにおける様々な光パス形態の上での波長多重伝送による量子鍵配送、及び鍵リレーによるエンドーエンド鍵共有方式を開発する。オール光ネットワークと量子鍵配送ネットワーク間の制御・管理情報の共有・連携方式を確立し、フィールド実証を通じてその実用性の検証を行う。

③ 到達目標

ア）鍵生成速度の高速化技術

デコイ BB84 方式を用いて、チップベース QKD 技術を用いた小型化・集積化、波長多重による高速化（光ファイバ損失 0.2dB/km のもとで 50km に相当する伝送損失 10dB の環境で 4Mbps を超える鍵生成）を実現する。また、受動的基底選択を用いた耐環境性能の向上と高速化（光ファイバ損失 0.2dB/km のもとで 50km に相当する伝送損失 10dB・架空線率 50%以上の環境で１Mbps 以上の鍵生成）を実現する。

イ）伝送距離の長距離化・広域化技術

TF-QKD 方式を用いて、敷設ファイバを含む伝送距離 500km での鍵生成を 10bps 以上で実現する。また、３拠点以上を接続するスター型 TF-QKD を構築し、250 km以上離れた任意の２拠点間での鍵共有を実現する。

デジタルコヒーレント CV-QKD 方式を用いて、既存データ用チャネルとの波長多重伝送条件下で伝送距離 20km で 50kbps 以上の鍵生成を実現し、19 インチラック高さ１U、横 19 インチ、奥行き 19 インチ程度のサイズを実現する。また、空間 CV-QKD 方式を用いて、対向設置した光アンテナを利用し、地上付近の距離１km での自由空間伝搬を行い、環境影響下で 10kbps 以上の量子鍵配送を実現する。

ウ）量子鍵配送とオール光ネットワークの統合技術

オール光ネットワークにおける様々な光パス形態の上での波長多重伝送による量子鍵配送、及び鍵リレーによるエンドーエンド鍵共有方式を開発し、アクセス網～中継網～アクセス網を含む３ホップ以上の鍵リレーを専用ダークファイバ使用時の鍵生成速度と比較し、50%未満の速度劣化で実現する。 さらに、敷設ファイバ環境下での長期安定性（１ヵ月以上の安定動作）を実現する。

（２）量子鍵配送網における鍵管理技術の高度化

① 概要

大規模な量子鍵配送網の高信頼な運用・管理を実現するため、複数のユーザが利用することを想定した鍵管理システムの構築を行い、大規模量子鍵配送網における鍵管理の最適制御・高信頼化技

術や、高秘匿・高信頼な鍵リレー技術の研究開発を実施する。

② 技術課題

ア）大規模量子鍵配送網における鍵管理の最適制御・高信頼化技術

大規模量子鍵配送網の実用環境では、鍵需給状況が時々刻々と変化するため、鍵需給状況やネットワーク状態の動的変化への追従かつ需要予想による、最適な鍵供給サービスを行うためのプロアクティブ制御技術を、単一の組織が量子鍵配送網を占有するケース（オンプレミス型）と複数のユーザで量子鍵配送網を共有するケース（クラウド型）について開発・実証を行う。また、異なる量子鍵配送網管理システム（集中管理型及び分散管理型）同士での鍵リレーを円滑に実施するための管理手法・プロトコルを確立する。

イ）高秘匿・高信頼鍵リレー技術

現在の量子鍵配送網における鍵リレーは“信頼できるノード”による鍵のカプセルリレー方式で実装されている。一方、量子鍵配送網が大規模化するにつれ、全てのノードを“信頼できるノード”として管理・運用すると、管理コストが膨大に増加する可能性がある。それに対し、ノードが危殆化する危険性がある場合でも、その危険性や秘匿性・信頼性への影響を評価し適切なレベルに維持・運用するために以下のような技術の開発を行う。

秘密分散プロトコルを量子鍵配送網における鍵リレーに適用し、ノードの危殆化に対する耐性を強化すると共に、ノードディスジョイントな鍵リレールートの効率的な検索機能を確立する。また、セキュアネットワーク符号化とマルチキャスト分散経路探索法を組み合わせたセキュアマルチキャスト技術を開発する。特に、運用実績から得られたノード危殆化率やリンク誤り率・改竄率に基づき、漏洩情報量とフレーム誤り率を定量的に評価・可視化する手法、ネットワーク状況に応じて機密性・信頼性のトレードオフを自在に制御する技術を確立する。

③ 到達目標

ア）大規模量子鍵配送網における鍵管理の最適制御・高信頼化技術

現在我が国では、20 ノード程度の規模の量子鍵配送網が構築されている。今後さらなるネットワークの大規模化や多数のユーザが接続された場合のことを想定し、20 ノード以上の実ネットワーク環境含む数百ノード程度の規模の量子鍵配送網シミュレーション環境において、ユーザ数 10 以上でのリレーを実施し、オンプレミス型及びクラウド型のサービスにおいて、鍵供給時のコストに対する最適ルート選択を可能とするシステムを実現する。また、異なる量子鍵配送網管理システム（集中管理型及び分散管理型）間の鍵リレー管理手法・プロトコルを確立する。

イ）高秘匿・高信頼鍵リレー技術

情報理論的安全性を有する秘密分散による高信頼鍵リレーにおいて、50 ノード程度の量子鍵配送網に対し、秘密分散の閾値仮定の劣化を最小限とするノードディスジョイントの鍵リレールートの選定を１分以内に完了、鍵リレーを実証する。また、10Mbps 以上のスループットを実現し、ゲノムデータ等を想定した容量がギガバイト相当の秘匿データ伝送を実際の量子鍵配送網を含むシミュレーション環境において実証する。

セキュアネットワーク符号化の処理速度を従来比３倍となる 10 Mbps 以上まで高速化する。

さらに、100 ノード程度のネットワークを想定し、ユーザ数 10 以上、ユーザ毎の分散度５以上で情報理論的機密性及びランク誤り訂正機能を有し、リンク数最小の分散経路からなる多者間秘匿通信のソフトウェアシステムを開発、敷設回線・模擬回線ハイブリッド環境で１対３のマルチキャストを実証するとともに、運用試験、脅威分析を行い分散度・コストのバランス設計法を確立する。

（３）量子暗号通信網の高機能化と統合実証

①　概要

現代暗号技術は認証、完全性保証、秘匿化等の機能を具備しており、量子鍵配送網が暗号インフラとして社会実装するには秘匿化以外の上記機能の具備が必須である。量子鍵配送網に対するこれらの要件を満たすため、情報理論的安全にマルチユーザに対応した相手認証やデータの完全性を担保する機能を実現する。また、量子鍵配送の特徴である情報理論的安全性を具備した形でデータの改竄を検知する技術の研究開発を実施する。

さらに、上記認証・完全性保証技術、課題（１）及び（２）にて開発した技術を適用した量子鍵配送網の機能実証を行うとともに、量子鍵配送網オール光ネットワークで連携によるセキュアオール光ネットワークの構築・実証を行う。

②　技術課題

ア）情報理論的安全な相手認証及びデータ完全性担保技術

量子鍵配送の暗号インフラとしての高機能化を目指し、データの改竄を検知する技術を開発するとともに、量子鍵時配送網の特徴を利用した高効率な相手認証・完全性保証技術を開発する。その際、量子鍵配送の特徴である情報理論的安全性を実現する。

イ）統合実証

オール光ネットワークによる超高速・低遅延を活かした秘匿通信サービスの具体的なユースケースを想定し、オール光ネットワークと量子鍵配送網との統合に必要な要件を明確化する。これらの要件に基づき、両ネットワークの連携により、通信サービスからの鍵需要に応じた効率的な鍵供給機能及び秘匿通信機能を備えた超高速・低遅延セキュアオール光ネットワークの統合運用実証を行う。

また、課題（1）、課題（2）、課題（3）ア）で開発した技術を適用した量子鍵配送網の機能実証を行うことにより、広域網における安定的かつ完全性の担保された鍵供給ができることを確認する。実用的な環境で信頼性試験等を行うことで社会実装に向けたフィージビリティを示す。

③　到達目標

ア）情報理論的安全な相手認証及びデータ完全性担保技術

数十ノード程度の実ネットワークを含む数百程度のノードの量子鍵配送網シミュレーション環境において、任意のノード（２以上）での情報理論的安全な相互認証を１分以内に完了できる機能を実現する。また、同環境において第三者による情報理論的安全な認証や通信の改竄の検知・判断を１分以内に完了できる機能を実現する。

イ）統合実証

量子鍵配送網と将来の普及が期待されるオール光ネットワークとを連携・統合させ、鍵供給に伴う付加遅延を数百マイクロ秒以下とするセキュアオール光ネットワークの統合運用実証、課題（1）、課題（2）、課題（3）ア）で開発した技術を適用した機能実証を行い社会実装に向けたユースケースを創出する。

５．研究開発期間

令和７年度から令和 11 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、課題（1）、（2）、（3）のいずれか又は複数の課題に提案することができる。なお、いずれの研究開発の受託者も相互に連携、協力して研究開発を行うこととする。

課題（1）ア）の受託者は課題（1）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）のとりまとめを行うものとする。また、本研究開発課題全体のとりまとめについては、課題（1）のとりまとめを実施する受託者が行うこととする。但し、課題（1）とは別の課題（(2）もしくは（3)）のとりまとめを実施する受託者が本研究開発課題全体のとりまとめをする提案も可とする。

（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とともに、国内・国外での類似システムの最新のベンチマークを示し、提案の優位性や課題を示すこと。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「量子暗号通信網の早期社会実装に向けた研究開発」による委託を受けて実施した研究開発による成果である」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。