別添３

グローバル量子暗号通信網構築のための衛星量子暗号技術の研究開発

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。コンピュータ技術は日進月歩で進展している中、今はまだ解読できない暗号化データを一旦保存しておくことで、将来、量子コンピュータなどの高度なコンピュータが実現した時に全データを一気に解読するような攻撃が懸念されている。将来にわたり、国家間や国内重要機関間で機密情報を安全にやりとりするためには、いかなるコンピュータ技術によっても解読が不可能な、いわゆる情報理論的安全性を有する量子暗号通信技術に基づき、広域的な量子暗号通信ネットワークを構築し、極めて堅牢性の高い安全な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、衛星通信における量子暗号技術の研究開発では、今後の衛星コンステレーションの普及などを見据え、超小型衛星に搭載可能な量子暗号通信技術の研究開発を進めている。

さらに、令和２年度から「グローバル量子暗号通信網構築のための研究開発」として、地上系における量子暗号通信のさらなる高速化・長距離化に資する 4 つの技術

（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

（４）広域ネットワーク構築・運用技術

の研究開発が実施されている。

今後、数百 km～数千 km といった大陸間スケールでの量子暗号通信へのニーズが想定される中、海底光ケーブルを経由する量子暗号通信の実現には未だに時間を要することから、衛星系を用いた量子暗号通信網の長距離化への期待が高まっている。一方、衛星量子暗号では、精密なレーザー捕捉追尾技術等が必要となること、悪天候時には地上局と通信できなくなること、さらには、伝搬距離の増加とともに鍵生成速度が急速に低下し、例えば、高度 3 万 km を超える静止軌道衛星と地上局間では現在の方式による量子鍵配送が困難になること等の課題がある。

したがって、衛星系を用いてグローバル量子暗号通信網を構築するためには、低軌道のみならず中軌道や静止軌道上の衛星と地上局間で情報理論的に安全な暗号通信を実現できる新たな量子暗号技術及び物理レイヤ暗号技術を開発する必要がある。さらに、グローバル量子

暗号通信網の可用性を向上させるためには、衛星とその見通し圏内にある地上局間で量子暗号リンクあるいは物理レイヤ暗号リンクを確立し、地上系量子暗号通信網と統合運用するための衛星系・地上系統合ネットワーク化技術を開発する必要がある。

そこで、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、

（１）衛星量子暗号・物理レイヤ暗号技術

（２）衛星系・地上系統合ネットワーク化技術

の研究開発を実施する。

２．政策的位置付け

『統合イノベーション戦略 2020』（令和 2 年 7 月 17 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 日統合イノベーション戦略推進会議）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。

『成長戦略実行計画』（令和 2 年 7 月 17 日閣議決定）において、いわゆる 6G（ビヨンド 5G）の推進として、量子暗号など、その実現のカギを握る先端技術の研究開発の加速が掲げられ、また、「成長戦略フォローアップ」（令和 2 年 7 月 17 日閣議決定）において、戦略的な研究開発の推進として、2021 年度から量子暗号衛星の試験機の研究開発、宇宙開発利用の拡大に向けた革新的な技術開発等の推進として、省庁横断・産学官連携による開発・実証体制を 2020 年度中に構築し、量子暗号通信等の基盤技術開発が掲げられている。

『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 2 年 7 月 17 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。

『宇宙×ＩＣＴに関する懇談会 報告書』（平成 29 年 8 月 8 日）において、衛星搭載用暗号技術の実用化を目指し、衛星通信用軽量暗号化技術の研究開発を進める。また、次世代光・量子暗号通信技術の実用化を目指し、衛星・地球局間のレーザー捕捉・追尾技術の高精度化、光子検出器の高速・高感度化、衛星用鍵蒸留システム、光伝搬視野特性モニタ・解析技術の研究開発を実施する、とされている。加えて、総務省においては、どれ程の計算力をもってしても解読できない安全性を備えた通信を実現するための暗号技術として、衛星に搭載した物理乱数源から生成された真性乱数を、レーザー光で地上局へ伝送する技術及び衛星・地上

局間で共有した真性乱数データから安全な暗号鍵を蒸留する技術（量子暗号等）の開発を推進するとともに、高秘匿衛星光通信技術の実証を行うことが適当である、とされている。

『宇宙基本計画』（令和 2 年 6 月 30 日閣議決定）において、「産業・科学技術基盤を始めとする宇宙活動を支える総合的な基盤の強化」における「衛星関連の革新的基盤技術開発」として「衛星と地上の間での実用的な量子暗号通信の実現を目指し、2022 年度までにはその基盤技術の確立を図るとともに、衛星ネットワーク等によるグローバルな量子暗号通信網の実現に向けた研究開発等を推進する（総務省）」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、低軌道衛星のみならず中軌道や静止軌道上の衛星と地上局間で情報理論的に安全な暗号通信を実現し、地上系システムと組み合わせてネットワークを構成する必要がある。

そこで、「グローバル量子暗号通信網構築のための研究開発」で実施されている地上系システムの研究開発と連携して（１）衛星量子暗号・物理レイヤ暗号技術、及び（２）衛星系・地上系統合ネットワーク化技術を開発することによって、数百 km～数千 km といった大陸間スケールでの可用性の高い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）

低軌道のみならず中軌道や静止軌道上の衛星と地上局間で情報理論的に安全な暗号通信を実現可能な衛星量子暗号・物理レイヤ暗号技術を搭載した衛星搭載可能な機器を開発し、静止衛星・地上局間の空間光通信路を模擬した環境（80～100dB の減衰）で安全な暗号鍵が生成できる（10bps 以上）ことを実証する。

また、衛星量子暗号・物理レイヤ暗号の実現に必要となる地上局を開発するとともに、衛星系・地上系統合ネットワーク化技術を開発し、様々な軌道上の衛星と地上局間の量子暗号リンク・物理レイヤ暗号リンクを模擬した環境で、軌道上を移動する衛星から複数の地上局へ情報理論的に安全な暗号鍵を配送する機能、及び地上局から地上系量子暗号通信網への安全な相互接続・統合運用動作をシミュレーションや地上検証等により実証し、数百 km～数千 km といった大陸間スケールでの量子暗号通信網を構築できる機能を検証する。

４．研究開発内容

（１）衛星量子暗号・物理レイヤ暗号技術

①　概要

低軌道衛星と地上局間での量子暗号及び物理レイヤ暗号、また、中軌道衛星及び静止衛星と地上局間での量子暗号又は物理レイヤ暗号を実現するために、衛星搭載用量子暗号・物理レイヤ暗号技術及び衛星搭載用光データリンク技術の研究開発を行う。

なお、本研究開発の実施に当たっては、開発する衛星搭載用量子暗号・物理レイヤ暗号装置及び衛星搭載用光データリンク装置の将来的な衛星搭載に向け、総務省の求めに応じて衛星バスの開発主体との搭載要件の検討に参加するなどして、当該要件も踏まえながら開発を進めること。

②　技術課題

ア）衛星搭載用量子暗号・物理レイヤ暗号装置の開発

低軌道衛星と地上局間での量子暗号及び物理レイヤ暗号の高速化、また、中軌道衛星及び静止衛星と地上局間での量子暗号又は物理レイヤ暗号の実現のため、「見通し通信」という空間光通信特有の条件を最大限に生かすことで鍵生成の高速化を図る等により、衛星通信に適した量子暗号及び物理レイヤ暗号のプロトコルを開発するとともに、衛星搭載と宇宙環境動作に適した量子暗号・物理レイヤ暗号装置を開発する。

a）暗号プロトコルの開発及び装置実装技術

衛星通信に適した量子暗号及び物理レイヤ暗号のプロトコルの開発、光・量子通信部の開発、及び衛星搭載用量子暗号・物理レイヤ暗号装置の統合実装を行う。

b）鍵蒸留技術

衛星搭載と宇宙環境動作に適した低電力で小型、かつ耐放射線・恒温機能を持つ鍵蒸留部を開発する。鍵蒸留に必要な公開通信路のための送受信機能も実装する。

イ）衛星搭載用光データリンク技術

衛星量子暗号・物理レイヤ暗号技術の実現のためには、高精度のレーザ捕捉追尾技術、及び衛星・地上局間で高速のデータ伝送を行うための光データリンク技術の開発が必要となる。

a）捕捉追尾技術

衛星から出射されたレーザビームを可能な限り細く絞り地上局の望遠鏡に結合させるための高精度のレーザ捕捉追尾技術、及びジンバルモータ駆動時の揺動抑制等の機能を有する姿勢制御技術を開発する。

b）光データリンク技術

衛星・地上局間で高速の光データリンクを構成するための衛星搭載用光通信技術を開発し、上記課題 a)で開発した技術と統合して衛星搭載用光データリンク装置を開発する。

③　到達目標

ア）衛星搭載用量子暗号・物理レイヤ暗号装置の開発

低軌道衛星・地上局間の空間光通信路を模擬した環境において、軌道条件や大気条件等に応じて設定された種々の盗聴通信路モデルに対して、量子暗号と物理レイヤ暗号を適切に組み合わせることにより、現在開発が進められている衛星量子暗号装置の鍵生成速度（損失 50dB 程度（受信系の損失含む）の空間光通信路において 10kbps 級）の 3 倍程度（30kbps 級）の高速化の実現に必要な機能、及び量子暗号又は物理レイヤ暗号により静止衛星・地上局間の空間光通信路を模擬した環境（光損失 80～100dB 程度）において、情報理論的に安全な暗号鍵を 10bps 以上の速度で生成する機能を地上試験で確認する。さらに、これらの機能を実装した装置について、耐放射線試験や熱真空試験、振動試験等により、衛星搭載に必要な耐環境性を実証する。

イ）衛星搭載用光データリンク技術

広がり角 10 μ rad 程度のレーザビームを衛星・地上局間で安定に捕捉追尾する機能を実装するとともに、量子暗号・物理レイヤ暗号で共有した暗号鍵を用いて暗号化データを伝送するための衛星搭載用光通信技術を実証する。さらにこれらの機能・技術を実装した装置について衛星搭載に必要な耐環境性を実証する。

（２）衛星系・地上系統合ネットワーク化技術

①　概要

衛星量子暗号・物理レイヤ暗号の実現に必要となる地上局を開発するとともに、地上系量子暗号通信網（Tokyo QKD Network など）と相互接続し、統合運用するための衛星系・地上系統合ネットワーク化技術を開発する。

なお、本研究開発の実施に当たっては、「グローバル量子暗号通信網構築のための研究開発」の研究開発成果と組み合わせることが可能となるよう、当該研究開発の受託者と連携して研究開発を進めること。

②　技術課題

ア）衛星量子暗号・物理レイヤ暗号のための地上局の開発

高感度・低損失の光受信アンテナ技術、地上局側での捕捉追尾技術、高感度・低雑音の量子受信技術及び光受信技術、RF 回線通信技術、及びこれらの技術を実装した地上局を製作する。

a）高感度・低損失の光受信アンテナ技術

可能な限り大きな開口径を有し、かつ受信したレーザビームをシングルモードファイバまで低損失で導波するための光受信アンテナ技術を開発する。

b）地上局側での捕捉追尾技術

衛星･地上局間で安定な量子暗号リンク及び物理レイヤ暗号リンクを確立するための地上局側における高精度捕捉追尾技術を開発する。

c）**高感度・低雑音の量子受信技術**及び**光受信技術**

衛星から地上局に届いた極めて微弱な光信号を高感度かつ低雑音で検出し情報理論的に安全な暗号鍵を生成するための量子受信技術を開発する。また、衛星・地上局間での光データリンクの実現に必要な光受信技術を開発する。

d）**RF 回線通信技術**

衛星量子暗号･物理レイヤ暗号における鍵蒸留のための公開通信路や、生成された暗号鍵を用いて秘匿データ通信を実現するための RF 回線通信技術を開発する。

e)**インテグレーション・検証試験**

上記 a)、 b)、 c)、d)の技術を実装した地上局を製作するとともに、課題（1）で開発した衛星搭載用量子暗号・物理レイヤ暗号装置、及び衛星搭載用光データリンク装置とのインテグレーションを進め、検証試験を行う。

イ）衛星系・地上系の統合運用検証

上記の地上局を、地上系量子暗号通信網（Tokyo QKD Network など）と相互接続し、衛星系・地上系にわたり鍵管理やネットワーク制御・管理、セキュリティアプリケーションサービスを行うための統合動作を検証する。

③　到達目標

ア）衛星量子暗号・物理レイヤ暗号のための地上局の開発

低軌道衛星・地上局間の空間光通信路を模擬した環境において、軌道条件や大気条件等に応じて設定された種々の盗聴通信路モデルに対して、量子暗号と物理レイヤ暗号を適切に組み合わせることにより、現在開発が進められている衛星量子暗号装置の鍵生成速度（損失 50dB 程度（受信系の損失含む）の空間光通信路において 10kbps 級）の 3 倍程度(30kbps 級)の高速化を実証する。

静止衛星・地上局間の空間光通信路を模擬した環境（光損失 80～100dB 程度）において、量子暗号又は物理レイヤ暗号により情報理論的に安全な暗号鍵を 10bps 以上の速度で生成できることを実証する。

イ）衛星系・地上系の統合運用

様々な軌道上の衛星と地上局間の衛星量子暗号リンク・物理レイヤ暗号リンクを模擬した環境で、軌道上を移動する衛星から複数の地上局へ情報理論的に安全な暗号鍵を配送する機能、及び地上局から地上系量子暗号通信網への安全な相互接続・統合運用動作をシミュレーションや地上検証等により実証し、既存の量子暗号通信網（例：Tokyo QKD Network）の 10 倍以上の大規模化に相当する数百 km～数千 km といった大陸間スケールでのネットワークを構築できる機能を検証する。

５．研究開発期間

令和３年度から令和７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）及び（２）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い、課題（２）－イ）の受託者は課題（２）及び本研究開発課題全体（課題（１）と（２））のとりまとめを行うものとする。

（１）衛星量子暗号・物理レイヤ暗号技術

ア）衛星搭載用量子暗号・物理レイヤ暗号装置の開発

イ）衛星搭載用光データリンク技術

（２）衛星系・地上系統合ネットワーク化技術

ア）衛星量子暗号・物理レイヤ暗号のための地上局の開発

イ）衛星系・地上系の統合運用

（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、目標を達成するための研究方法、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及び達成度を客観的に評価するための実験方法について、具体的に提案書に記載すること。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。また、本研究開発成果を確実に展開し、アウトカム目標を達成するため、事業化目標年度、事業化に至るまでの実効的な取組計画（事業化及び標準化活動、体制、資金等）についても具体的に提案書に記載すること。

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。

⑤ 本研究開発は総務省施策の一環として取り組むものであることから、総務省が受託者に対して指示する、研究開発に関する情報及び研究開発成果の開示、関係研究開発プロジェクトとのミーティングへの出席、シンポジウム等での研究発表、共同実証実験への参加等に可能な限り応じること。

（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衛星量子暗号技術の研究開発」（令和 3 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。