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
Research and development of satellite quantum cryptography technology for building a global quantum cryptography communications network

代表研究責任者　間宮　敦　スカパーJSAT 株式会社

研究開発期間　　令和３年度～令和５年度

【Abstract】

This paper describes the "Research and development of satellite quantum cryptography technology for building a global quantum cryptography communications network" implementation structure, objectives, research and development results, implementation status of efforts toward achieving policy goals (outcome goals), and plans and efforts results for achieving policy goals (outcome goals) in this R&D.

This R&D was scheduled to last five years from FY2021 to FY2025, but it was finished in three years until FY2023. Therefore, this paper will show the results on the three years from FY2021 to FY2023.

1　研究開発体制

○ **代表研究責任者**　　間宮　敦（スカパーJSAT(株)　技術推進部・マネージャー）

○ **研究分担者**　　藤原 幹生（情報通信研究機構　量子 ICT 協創センター・研究センター長）

田中 正樹（日本電気(株)　スペースプロダクト統括部・プロフェッショナル）

佐藤 英昭（(株)東芝　コンピュータ＆ネットワークシステムラボラトリー・フェロー）

○ **総合ビジネスプロデューサ**　三森　丞（スカパーJSAT(株)　宇宙・防衛事業部　部長）

○ **ビジネスプロデューサ**　　久保田 実（情報通信研究機構　ソーシャルイノベーションユニットユニット長）

星野 裕毅（日本電気(株)　スペースプロダクト統括部　部長）

神田　　充（(株)東芝　研究開発センター情報通信プラットフォーム研究所　コンピュータ＆ネットワークシステムラボラトリー室長）

○ **研究開発期間**　令和３年度～令和５年度

○ **研究開発予算**　総額　4,500 百万円

（内訳）

令和３年度	令和４年度	令和５年度	令和６年度	令和７年度
1,500 百万円	1,500 百万円	1,500 百万円	1,500 百万円	1,500 百万円

２　研究開発課題の目的および意義

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・長距離化に資する以下の４つの技術の研究開発が実施されている。

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

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、以下の研究開発を実施する。

３　研究開発成果（アウトプット）

３．１　（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

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。

各課題の研究開発成果について、下記の通り示す。

a）暗号プロトコルの開発および装置実装技術

a)-1 暗号プロトコルの開発と検証

見通し通信 QKD と物理レイヤ暗号という２つの暗号プロトコルを設計し、装置構成の要件を明確化した。プロトコルに要求される、ダイナミックレンジの広い送信パワーの変調（ブライト変調）、衛星と地上局間での鍵配送に必要な正確な時刻同期信号の重畳、ドップラーシフトを地上局側で補正するためのデバイス制御機能などを搭載した原理実証機（送受信とも）を作成し、プロトコルの実動作を確認できた。さらに、他の課題で開発している送受信機の試作機と原理実証機を相互接続して、各課題で進めている装置設計の妥当性を確認できた。

a)-2 光・量子送信部の実装

課題 a)-1 にて設計された見通し通信 QKD と物理レイヤ暗号の暗号プロトコルを実現するための光・量子送信部に係る機能仕様要件を取り纏め、搭載化に向けたフライト部品選定・評価及び、各部品を組み合わせた DPS 変調器、光強度制御器、同期光送信器に相当する部分試作器の性能検証を完了し光・量子送信部の電気 EM の製造を完了した。課題 a)-1 で開発された原理実証機の鍵蒸留部からの実信号による動作検証により原理実証機と同等の性能を得られたことでインターフェースを含む機能仕様の妥当性を確認した。

高強度な同期光と微弱な鍵配送用の信号光を合波しかつ同期光用の光増幅器からのノイズを低減し光送信アンテナから出力させる機能を有する光合波器の製造を完了した。

b）鍵蒸留技術

b)-1 耐宇宙環境用鍵蒸留基板の開発

鍵蒸留基板評価系開発として、搭載用鍵蒸留基板と地上用鍵蒸留基板との間を接続し、衛星から地上へ届く光への影響を加味して両基板間のデータ通信を電気的にエミュレートする、機能検証用エミュレータの試作を完了。さらに、当該エミュレータの完成度を高めることを目的に、鍵蒸留基板の鍵蒸留機能に影響を与える要素について、関連論文や過去の光衛星通信実験結果を調査し、具体的なパラメータの検討を完了。また、衛星搭載用鍵蒸留基板向けの一部の部品についての調査や評価を完了。

なお、上記の鍵蒸留基板については、先行する総務省委託課題「衛星通信における量子暗号技術の研究開発」で製作を行った国際宇宙ステーション搭載用の鍵蒸留基板に用いている、耐放射線環境技術の開発の際に得られた知見を活かし、より過酷な放射線環境である静止軌道においても放射線耐性を有する基板の開発を実施した。また、同基板にインストールする鍵蒸留ソフトウェアの開発においても、同先行課題での開発結果を受けて実装条件や運用条件に合わせた修正を

施している。

b)-2 耐宇宙環境用鍵蒸留部の実装

見通し通信 QKD・物理レイヤ暗号装置について、鍵蒸留基板として開発を行い、CPU、RAM といった高性能かつ主要である部品に関しての耐放射線試験の実施や、熱対策部材の選定・試作、それらを使用した BBM の製作と BBM を用いた熱真空試験の実施により、衛星搭載に必要な耐環境性を検証し、低電力で小型、かつ耐放射線・恒温機能を持つ鍵蒸留部として実装可能な衛星搭載用暗号装置の鍵蒸留部の基本的設計を完了した。

イ）衛星搭載用光データリンク技術

広がり角 10μrad 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。

各課題の研究開発成果について、下記の通り示す。

a）捕捉追尾技術

実績のある衛星光空間通信で用いられている技術をベースに可搬型地上局からのアップリンクビーコン光を捕捉追尾するための捕捉追尾アルゴリズムを検討しシミュレーション解析により妥当性を検証した。検証したアルゴリズムの実現と課題（２）ア）e)-1 の機能実証に必要な機能要求を分析しソフトウェア機能仕様を規定しソフトウェア製作並びに改修を行うとともに試験を完了した。

b）光データリンク技術

b)-1 衛星搭載用光データリンク装置の開発

見通し通信 QKD および物理レイヤ暗号で共有した「暗号鍵」で暗号化したデータを伝送する光通信技術を実証することを目的とし、誤り訂正・フレーミングを行う古典通信部と光データリンク送信部、さらに捕捉追尾機能を有する光送信アンテナの開発を実施した。

古典通信部（送信部）は実装する物理レイヤフレームにユーザー伝送容量 1 GbE を格納することを想定し、DVB-S2 規格に基づいた符号化率 1/2 の誤り訂正(LDPC/BCH)をベースとした構成とし、FPGA に実装する RTL 設計のシミュレーションによる検証を行い FPGA のピン配置や CLK 周波数指定を含む仮の合成と配置配線を実施し問題なく実装できることを確認し設計検証を完了した。光データリンク送信部は NEC の既存設備を活用し変調器の性能確認等の整備を行い整備後の送受信部を用いた評価により目標を上回る受信感度を確認した。光送信アンテナは実績のある衛星光空間通信で用いられている技術をベースに下位構成部品の製造を完了した。

b)-2 暗号装置とのインターフェース技術

暗号装置とのインターフェース技術として、RF 回線を経由する公開通信路を安全な経路とするために、地上ネットワークと VPN（IPSec）接続可能なネットワークルータの開発を行った。これにより、ミッションに関わる装置をトラステッドノード内に収めることが可能となった。トラステッドノード内の機器の制御及びアプリケーション等の実行のため、OBC（オンボードコンピュータ）の開発も行った。これらに用いた CPU、記憶装置、パワー半導体等の主要部品の選定は、

宇宙機搭載を考慮して行われ、それらの互換品を用いて構成した試作品を用いて、放射線試験、振動試験などを行い、宇宙環境で使用可能であることを検証し、基本設計を完了した。

３．２　（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

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。

各課題の研究開発成果について、下記の通り示す。

a）高感度・低損失の光受信アンテナ技術

受信光学系の各要素の可搬型光地上局への搭載を進め、先行する総務省委託課題「衛星通信における量子暗号技術の研究開発」における可搬型光地上局の機能検証の際に得られた知見を活かしつつ、令和４年度までに実施した試作等の結果も踏まえ、それらの光学的損失を統括し、回線計算結果の保守・更新を完了した。この損失に対してさらなる改善を検討し、光受信アンテナに用いる反射鏡の更新、合波器の改良、指向精度向上のための再較正および制御ソフトウェアの改良等を完了した。追尾システムの要となるビーコン光学系については、大気擾乱の影響を受けにくいとされる多数の射出光学系を用いたシステムとし、専用のレーザーシステムの製作を行った。その他、可搬局としての可用性を向上させるため、GPS システムの導入や、可搬局内で完結する光学系較正システムの組みこみを実施し、光受信アンテナ性能向上のための機能実装を完了した。

b）地上局側での捕捉追尾技術

b)-1 地上局用捕捉追尾システム

受信アンテナの後段となる精追尾光学系の製造および可搬局への搭載を完了した。先行する総務省委託課題「衛星通信における量子暗号技術の研究開発」における可搬型光地上局の機能検証の際に得られた知見を活かし、光路長の設定を最適化するなど光学系の設計を実施した。また、光受信アンテナと精追尾光学系の架台の防振性を向上させるべく、構造計算および加振試験を実施し、フレームの固有振動による共振についての対策を完了した。

b)-2 衛星から地上局捕捉追尾システムへのインターフェース

衛星−地上局間での捕捉追尾を実現するため、捕捉追尾手順及びビーコン光/同期光/データリンク光の波長や偏光などを規定する捕捉追尾インターフェース管理仕様書を取り纏め、衛星/地上局間の光回線計算の更新状況、及び地上局の捕捉追尾システム開発の進捗状況により維持管理を行い衛星−地上局間のインターフェースの調整を完了した。

c）高感度・低雑音の量子受信技術および光受信技術

c)-1 APD 型量子受信機

可搬型地上局に搭載可能な APD 型量子受信機の一次試作として、APD 検出器・時刻同期基板・

光学システムのハードおよびソフトの部品試作ならびに量子受信機としての組み立てを完了。さらに、実験室環境で APD 検出器・時刻同期基板・光学システムの検証・評価・改良を完了。そして課題(2)ア)c)-2 の担当チームが開発する NICT 作成の原理実証機との結合試験を完了。

c)-2 APD-SSPD 統合型量子受信機システム

NICT の超伝導 ICT 研究室が令和４年度に設計・製造した SSPD 素子を導入した SSPD 評価系を可搬型光地上局上に展開し、望遠鏡駆動用モーターなどから発生するノイズによる影響の測定を実施する予定であったが、装置の故障により未実施となっている。また、課題(2)イ)c)-1 の担当チームが開発した光・量子受信部 BBM との結合試験は、同 BBM と NICT 原理実証機との結合試験を優先したため未実施である。

c)-3 光データリンク用受信器

「暗号鍵」で暗号化したデータを伝送する光通信技術を実証することを目的とし、誤り訂正・フレーミングを行う古典通信部と光データリンク受信部の開発を実施した。古典通信部（受信部）は実装する物理レイヤフレームにユーザー伝送容量１GbE を格納することを想定し、DVB-S2 規格に基づいた符号化率 1/2 の誤り訂正(LDPC/BCH)をベースとした構成とし、FPGA に実装する RTL 設計のシミュレーションによる検証を行い FPGA のピン配置や CLK 周波数指定を含む仮の合成と配置配線を実施し問題なく実装できることを確認し設計検証を完了した。光データリンク受信部はNECの既存設備を活用し変調器の性能確認等の整備を行い整備後の送受信部を用いた評価により目標を上回る受信感度を確認した。

d）RF 回線通信技術

d)-1 RF 回線送受信機システム

衛星で変復調する衛星−地上間の一定以上のデータ通信用途での誤り訂正方式においても、調査の結果、汎用的な衛星通信として使用される DVB-S2 や LDPC が今後利用の普及が進んでいくこと確認した。

モデム同士を有線で繋ぎ、TCP/IP ベースで鍵蒸留を実施した結果、500kbps 程度に情報レートを下げると鍵生成時間に影響が出ることが判明。そのため、現状のソフトウェアの範囲では鍵蒸留、鍵管理用途の RF 回線は１Mbps 以上の回線が望ましいことが分かった。

また、RF 回線には鍵管理に必要な通信も通すため、それを考慮した検討を行った。

d)-2 RF 回線送受信機インターフェース

可搬型光地上局に RF 通信装置を組み込むために、スカパーJSAT が調達したモデムを可搬型光地上局への積み込み、動作確認を完了した。

e）インテグレーション・検証試験

e)-1 衛星・地上局インテグレーション・検証試験とりまとめ

【試験環境の手配を含む統合運用試験の準備】

令和４年度に各検証試験の試験計画書（初版）を策定以降も各受託機関と連携して、各機能・装置の単体試験も含めた検証項目・実施時期・課題の共有を目的としたシートを作成。実証実施に向けて調整を継続するもプロジェクトの終了に伴いスケジュールなど計画書への反映には至らなかった。

令和５年度に実証実施場所の絞り込みを完了した。候補場所での今後の交渉や実証に向けた、各種詳細要件の具体化及び課題の検討を継続するもプロジェクトの終了に伴い実施場所の絞り

込みまでとなった。

【可搬型光地上局の製造】

車両の調達、望遠鏡の設計・調達並びに精追尾光学系の設計・製造を行った。望遠鏡及び精追尾光学系の性能向上に向けた対応を実施した。具体的には、光軸調整機構について、先行する総務省委託課題「衛星通信における量子暗号技術の研究開発」における機能検証などの知見を取り入れ、可視天体指示による捕捉追尾較正機構や、End-to-End の光軸較正システムを導入し、よりフィールドにおける実用性を考慮した機能実装とした。

e)-2 可搬型光地上局の統合実装

可搬型光地上局車両への各構成要素の搭載は順調に進み、光受信アンテナと広視野ガイド鏡、ビーコンシステム等の補助光学系、精追尾光学系の搭載まで完了した。また、性能向上及び安定した可用性を維持するための除振台の再設計、光学系構成システム等の組み込みも含め、統合実装を完了した。これらの動作・性能検証のための調整、試験、統合実証についてはプロジェクトの終了に伴い、未実施である。

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。

各課題の研究開発成果について、下記の通り示す。

a)-1 衛星系・地上系の統合運用検証とりまとめ

衛星系・地上系統合 QKD ネットワークの構想を通じて、本研究開発における統合運用実証の試験構成を決定した。併せて実証に必要な環境、設備を整理した。また、QKD ネットワークにおいて各ノード間でやり取りされる情報回線種別ごとに整理した。

a)-2 衛星系・地上系相互接続・鍵管理・運用

衛星 QKD ネットワークを地上系 QKD ネットワークと統合するために必須となる相互接続インターフェースの実装・検証を完了した。 QKD ネットワークの操作性・運用性向上のための鍵管理ソフトウェアの環境構築自動化システム、マネージャ機能を及び管理ログ収集機能管理システムの実装・検証を完了した。さらに、分散型 QKD ネットワーク管理のためのコントローラ機能の基本仕様策定と試作を完了した。

a)-3 衛星系・地上系コンポーネント組み込み

放射線耐性をもつ衛星搭載用ハードウェアに対し、地上系の量子鍵配送網で開発したものと同等の鍵管理用ライブラリをインストール、鍵管理機能のビルトインに成功し、鍵管理機能の基本動作の確認を完了した。また当該鍵管理システムは集中管理型の２つの量子鍵配送ネットワーク間での鍵リレーを可能とする機能も有しており、原理的に地上系の量子鍵配送網との鍵リレーを可能とするシステムの原理検証に成功した。

4　政策目標（アウトカム目標）の達成に向けた取組みの実施状況

グローバルスケールの量子暗号通信ネットワークで想定される潜在ユーザー等に対して、ビジネスモデルに関する市場動向調査を行った。また、海外を含む関連機関・企業の動向調査を実施し、事業化検討に資する情報の収集を行った。

衛星量子鍵配送の各国の取り組みと今後の予定等につき、米、中、欧州、カナダ、シンガポール、英国、イスラエル等）の QKD 先進国の最新動向につき情報収集を行い、各国の動向調査を行った（図 1 ご参照）。基本計画書「6. その他」の特記事項については、提案書に反映をし、提案書に従い計画通りに実施した。

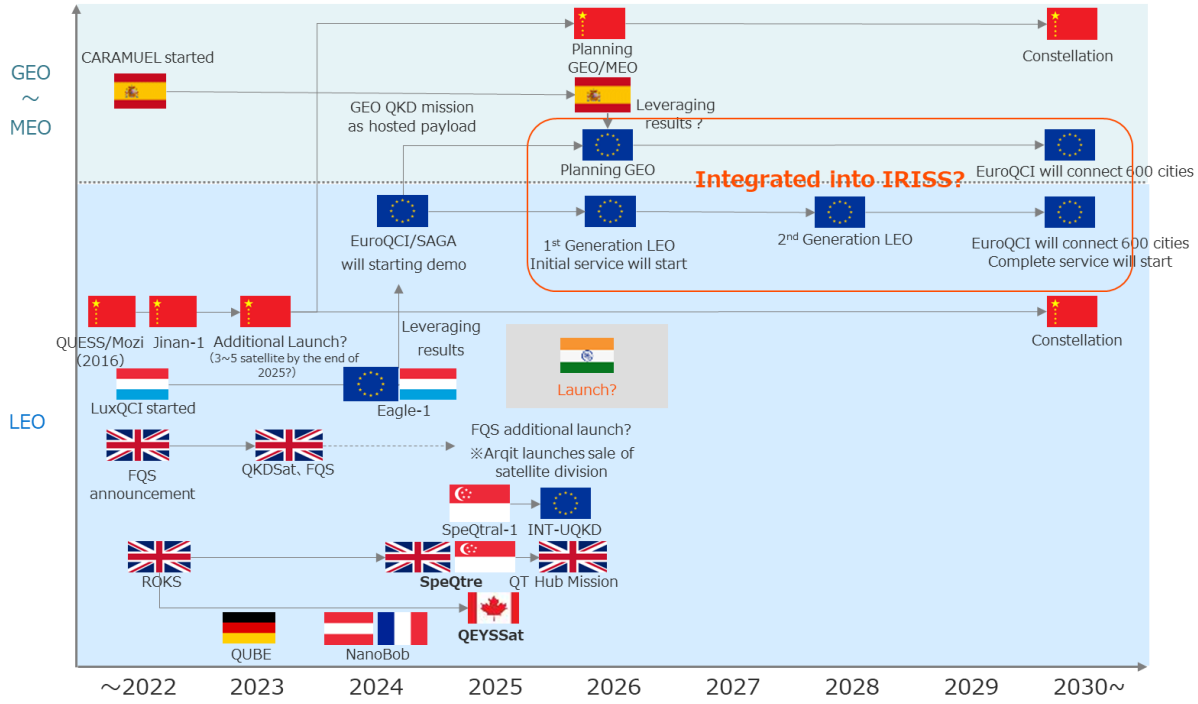

図 1　各国の衛星量子鍵配送に関する開発・事業化スケジュール

（株式会社日本総合研究所作成）

また、グローバル量子暗号通信の将来的なユーザー発掘、想定される利用シーンやビジネスモデルの検討に向けて、海外等動向ならびに潜在顧客と想定されるユーザー等へヒアリングを行った実績を表 1 に示す。

表１　ヒアリング調査実施状況（令和３年度～令和５年度）

日付	対象	場所
2021 年 6 月	関連団体セミナー	オンライン
2021 年 10 月	関連団体セミナー	オンライン
2021 年 10 月	潜在ユーザー（安全保障）	対面
2021 年 11 月	潜在ユーザー（安全保障）	対面
2021 年 12 月	国内企業（メーカー）	対面
2022 年 1 月	海外動向調査（英国）	対面
2022 年 1 月	潜在ユーザー（安全保障）	対面
2022 年 2 月	潜在ユーザー（安全保障）	対面
2022 年 3 月	潜在ユーザー（安全保障）	対面
2022 年 7 月	国内企業（商社）	対面
2022 年 8 月	国内機器メーカ	オンライン
2022 年 9 月	海外企業（イスラエル）	都内（来日時）
2022 年 10 月	海外企業（米国）	都内（来日時）
2022 年 11 月	国内企業（商社）/海外企業（英国）	都内
2023 年 1 月	国内企業（メーカ）	オンライン
2023 年 1 月	国内企業（メーカ）	対面
2023 年 7 月	潜在ユーザー（安全保障）	対面
2023 年 8 月	潜在ユーザー（安全保障）	対面
2023 年 8 月	潜在ユーザー（安全保障）	対面
2023 年 9 月	海外動向調査	オンライン
2023 年 10 月	潜在ユーザー（安全保障）	対面
2023 年 10 月	潜在ユーザー等（安全保障等）	展示会・対面
2023 年 11 月	潜在ユーザー（安全保障）	対面
2023 年 11 月	潜在ユーザー（安全保障）	対面
2024 年 1 月	国内企業（メーカ）	オンライン
2024 年 1 月	潜在ユーザー（安全保障）	対面
2024 年 2 月	潜在ユーザー（安全保障）	対面
2024 年 2 月	海外動向調査	対面
2024 年 2 月	国内企業（メーカ）	対面
2024 年 3 月	国内企業（メーカ）	対面

上記市場・技術動向調査によって、シンガポール、欧州、カナダの 2020 年代半ばに QKD 実証を予定する各国は、まずは低軌道（LEO）衛星での実機実証を予定していることがあらためて確認できた。一方、より長期的将来において、今後は中軌道（MEO）、静止軌道（GEO）といった多様な軌道での実証も行われることが想定されるため、本研究開発案件で実施した LEO のみならず多様な軌道からの鍵配送を見据え、高い耐宇宙環境性を備えた衛星搭載用機器の開発を世界に先駆けて実施し知見を集積したことは将来

の製品化の観点から重要であったと考える。

また、衛星実証を令和７年度に控えているシンガポールへのヒアリングからは、同国の企業が地上量子鍵配送に取り組む事業者・機関等と連携し、統合的な QKD ネットワークを目指す動きが始まっていることがうかがえた。引き続き社会実装に向けてはこれら諸外国の事例も収集しながら社会実装当初のふさわしいビジネスモデルを検討していくことが肝要であると考える。

以上より、本研究開発では、地上量子暗号網を交えた鍵管理も含めた鍵配送サービスの事業化の可能性、また、LEO のみならず、MEO、GEO までを視野に入れた高い耐宇宙環境性を備えた衛星搭載用機器の将来的な製品化に向けて取り組みを進めてきたが、これら情報・知見を集積し、情報取集ならびに実証の機会を重ねて、社会実装へつなげていくことが肝要であると思料する。

【特許戦略について】

特許に関しては、機微情報についてはクローズとする当初からの情報公開戦略にしたがって、公開可能な技術については出願している（本書 12 項、14 項参照）。一方、安全保障に影響を与えかねない情報を含む機微情報については公開しない方針を貫いており、本年 5 月施行の特許出願非公開制度を活用することで機微情報の保護を図ることも検討している。とりわけ、潜在ユーザーへのヒアリングを通じて暗号システムの運用に関する情報などもまとめているが、これについても原則非公開としつつ、上述の特許出願非公開制度の活用なども視野に入れつつ関係者と検討を継続している。

５　政策目標（アウトカム目標）の達成に向けた計画

潜在ユーザーならびに海外動向に関するヒアリングと並行して、想定される利用シーンやビジネスモデル、市場投入スケジュール等につき、令和３年度から引き続き基礎調査を実施のうえ、事業モデル変遷シナリオ並びに衛星＋地上連接でのサービス提供モデル及びビジネスモデルについて検討した事業モデルについては政府向け利用並びに一部商用利用向け実証を経てからの実導入～普及が予想される。なお、コロナウイルス感染拡大やロシアによるウクライナへの軍事侵攻などの影響により各国のプロジェクトはスケジュールの遅滞が発生しており、市場の形成までは当初の想定より５年程度遅延することが想定される。

アウトカム目標達成に向けて、サイバー攻撃の巧妙化、量子コンピュータの登場等様々なことを要因に情報セキュリティの高度化が求められる。情報セキュリティの高度化を実現させる手法の一つである量子暗号、その構成要素である量子暗号通信技術は諸外国においても国家プロジェクトとして実装に向けた研究開発が進められている。

衛星量子鍵配送については、中国が先行しており、既に小型衛星の開発・打上のうえ、衛星－地上間の実証を進めている。中国に続いて、欧州では欧州各国が連携した QKD ネットワークの構築を目指す EuroQCI の宇宙セグメントである SAGA において開発されているプロトタイプ衛星の Eagle-1 が令和６年の打ち上げを予定している。その他のプロジェクトについても小型実証衛星の開発が進められている状況にあり、2024 年～2026 年頃の打上が予定されている状況にある。さらに、中国や欧州においては低軌道小型衛星に加えて、中軌道、静止軌道衛星の開発も並行して進められており、複数軌道の衛星が連携したコンステレーションの構築が目指されている状況にある。

以上のことから、我が国においても、宇宙活動の自立性や国際競争力を支える基盤技術として、国際連

携も踏まえた出口戦略を明確化のうえ、机上検証、地上検証段階から研究開発衛星実機の開発へ移行し、試行運用を経た社会実装に向けてスピード感をもって進めていくことが求められる。
なお、その際には、エンドユーザーへのサービス提供モデルを念頭に置いた検討を進めることが重要となる。量子鍵配送のうち、地上量子鍵配送は衛星量子鍵配送に先行して事業化に向けた検討が進められており、政府機関や金融などの一部民間向けにトライアルサービスの提供が開始されている状況にある。これらのサービスでは量子鍵配送で共有化した暗号鍵による通信の暗号化をサービスとして提供するものであり、エンドユーザーにおいては鍵配送、暗号化・復号化といったオペレーションを意識することなく、量子暗号の恩恵を享受できるサービス提供内容となっている。中国や欧州においては地上量子鍵配送と衛星量子鍵配送の連接が視野に入れられていることからも、現状先行する地上量子鍵配送のサービス提供モデルを意識して、衛星量子鍵配送の事業化検討を行うことが求められると考えられる。

６　査読付き誌上発表論文リスト

無し

７　査読付き口頭発表論文（印刷物を含む）リスト

無し

８　その他の誌上発表リスト

[1]スカパーJSAT 株式会社　長谷川　広大、“宇宙通信ビジネスの動向と今後の展望に関して”、通信ソサイエティマガジン B-Plus 68 号（令和 6 年 3 月 1 日）:

９　口頭発表リスト

[1]情報通信研究機構　佐々木 雅英、“量子技術分野の動向と今後の課題”、総務省 情報通信審議会 情報通信技術分科会 技術戦略委員会（令和 4 年 1 月 28 日）

[2]スカパーJSAT 株式会社　間宮　敦、“Satellite-based Quantum Key Distribution and Cryptographic Technology for Global Quantum Cryptographic Network Construction”、IEEE ICSOS2022（令和 4 年 3 月 29 日）:

[3]スカパーJSAT 株式会社　横手　紗織、“Satellite-based QKD for Global Quantum Cryptographic Network Construction”、Quantum Innovation2022（令和 4 年 11 月 29 日）:

[4]スカパーJSAT 株式会社　田中　賢太郎、“スカパーJSAT 新規事業への取り組みのご紹介”、スペース ICT 推進フォーラム光通信技術分科会令和５年度第１回分科会（令和 5 年 8 月 31 日）:

[5]スカパーJSAT 株式会社　秋山　貴宏、“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”、一般社団法人電子情報通信学会（令和 5 年 9 月 1 日）:

[6]スカパーJSAT 株式会社　根本　和哉、“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”、一般社団法人電子情報通信学会（令和 6 年 3 月 6 日）:

１０　出願特許リスト

[1] 佐々木 雅英、遠藤 寛之、藤原 幹生、暗号鍵共有システム、日本、令和 4 年 3 月 30 日

[2] 佐々木 雅英、遠藤 寛之、藤原 幹生、暗号鍵共有システム、PCT 出願、令和 5 年 2 月 9 日

[3] 藤原 幹生、小澤 俊介、北村 光雄、西澤 亮二、光空間通信における効率的 Vernam’s one time pad 暗号化方式、日本、令和 5 年 10 月 25 日

１１　取得特許リスト

無し

１２　国際標準提案・獲得リスト

無し

１３　参加国際標準会議リスト

無し

１４　受賞リスト

無し

１５　報道発表リスト

（１）報道発表実績

無し

（２）報道掲載実績

無し

研究開発による成果数

	令和３年度	令和４年度	令和５年度
査読付き誌上発表論文数	０件（　０件）	０件（　０件）	０件（　０件）
査読付き口頭発表論文数（印刷物を含む）	０件（　０件）	０件（　０件）	０件（　０件）
その他の誌上発表数	０件（　０件）	０件（　０件）	１件（　１件）
口頭発表数	２件（　１件）	１件（　１件）	３件（　０件）
特許出願数	０件（　０件）	１件（　０件）	２件（　１件）
特許取得数	０件（　０件）	０件（　０件）	０件（　０件）
国際標準提案数	０件（　０件）	０件（　０件）	０件（　０件）
国際標準獲得数	０件（　０件）	０件（　０件）	０件（　０件）
受賞数	０件（　０件）	０件（　０件）	０件（　０件）
報道発表数	０件（　０件）	０件（　０件）	０件（　０件）
報道掲載数	０件（　０件）	０件（　０件）	０件（　０件）

	令和６年度	令和７年度	合計
査読付き誌上発表論文数	０件（　０件）	０件（　０件）	０件（　０件）
査読付き口頭発表論文数（印刷物を含む）	０件（　０件）	０件（　０件）	０件（　０件）
その他の誌上発表数	０件（　０件）	０件（　０件）	１件（　０件）
口頭発表数	０件（　０件）	０件（　０件）	６件（　２件）
特許出願数	０件（　０件）	０件（　０件）	３件（　１件）
特許取得数	０件（　０件）	０件（　０件）	０件（　０件）
国際標準提案数	０件（　０件）	０件（　０件）	０件（　０件）
国際標準獲得数	０件（　０件）	０件（　０件）	０件（　０件）
受賞数	０件（　０件）	０件（　０件）	０件（　０件）
報道発表数	０件（　０件）	０件（　０件）	０件（　０件）
報道掲載数	０件（　０件）	０件（　０件）	０件（　０件）

注１：各々の件数は国内分と海外分の合計値を記入。（括弧）内は、その内海外分のみを再掲。

注２：「査読付き誌上発表論文数」には、定期的に刊行される論文誌や学会誌等、査読（peer-review（論文投稿先の学会等で選出された当該分野の専門家である査読員により、当該論文の採録又は入選等の可否が新規性、信頼性、論理性等の観点より判定されたもの））のある出版物に掲載された論文等（Nature、Science、IEEE Transactions、電子情報通信学会論文誌等および査読のある小論文、研究速報、レター等を含む）を計上する。

注３：「査読付き口頭発表論文数（印刷物を含む）」には、学会の大会や研究会、国際会議等における口頭発表あるいはポスター発表のための査読のある資料集（電子媒体含む）に掲載された論文等（ICC、ECOC、OFC など、Conference、Workshop、Symposium 等での proceedings に掲載された論文形式のものなどとする。ただし、発表用のスライドなどは含まない。）を計上する。なお、口頭発表あるいはポスター発表のための査読のない資料集に掲載された論文等（電子情報通信学会技術研究報告など）は、「口頭発表数」に分類する。

注４：「その他の誌上発表数」には、専門誌、業界誌、機関誌等、査読のない出版物に掲載された記事等（査読の有無に関わらず企業、公的研究機関及び大学等における紀要論文や技報を含む）を計上する。

注５：PCT 国際出願については出願を行った時点で、海外分１件として記入。（何カ国への出願でも１件として計上）。また、国内段階に移行した時点で、移行した国数分を計上。

注６：同一の論文等は複数項目に計上しないこと。例えば、同一の論文等を「査読付き口頭発表論文数（印刷物を含む）」および「口頭発表数」のそれぞれに計上しないこと。ただし、学会の大会や研究会、国際会議等で口頭発表を行ったのち、当該学会より推奨を受ける等により、改めて査読が行われて論文等に掲載された場合は除く。