衛星通信における量子暗号技術の研究開発

基本計画書

１．目　的

近年、宇宙分野における人工衛星等の産業利用に向けた官民の活動が国際的に活発化しており、日本経済団体連合会は、今後の我が国の宇宙関連産業の市場規模について、2030 年代には 20 兆円の市場規模を見込んでいる。こうした動きを牽引しているのが、商社や自動車など、これまで宇宙ビジネスに関わったことがない非宇宙系であった業界の企業であり、人工衛星の利用により取得されるデータや衛星測位データ等の収集・活用に着目してビジネス化を図るなど、宇宙の産業利用としての適用分野の裾野を拡げつつある。また、衛星コンステレーションによるグローバルな地球観測や衛星通信網の構築に関する計画が進められており、衛星を利用する通信は、今後一層の需要が見込まれる状況である。さらに、電波帯より格段に大容量の通信を小型装置で省電力に実現できる、レーザー光を用いた衛星光通信技術も急速に進展している。このようなことから衛星による地球観測網や衛星通信網には、ますます多くの重要情報やビジネスチャンスに繋がる価値の高い情報が流れていくと予想される。

こうした中、衛星通信に対する第三者による通信内容の盗聴や改ざん、制御の乗っ取りといったサイバー攻撃が大きな脅威となりつつある。人工衛星へのサイバー攻撃は、軌道変更による衝突や墜落など甚大な物理的被害をもたらす危険性がある。また、測位衛星や通信衛星のサービスがサイバー攻撃により撹乱ないし停止させられた場合、その影響は宇宙インフラのみにとどまらず、様々な地上システムや移動通信システムにも甚大な被害をもたらす。将来の衛星コンステレーション構築においては、攻撃対象となるノードが増加し被害規模も甚大になるため、より一層の衛星通信のセキュリティ強化が求められる。

しかし、人工衛星では実装スペースや消費電力、搭載機器の演算能力に制約があるため、地上系で用いられる様々な情報セキュリティ技術をそのまま実装するのは困難である。回線容量もアクセス環境も限られるため、計算技術の進展により搭載していた暗号方式が危たい化した場合、リモートメンテナンスや鍵長の更新を適時に施すのは極めて困難である。さらに、衛星通信の傍受により盗聴したデータを蓄積しておけば、その時点では解読できなくとも、将来、高度な解読技術や十分な計算資源が利用可能となった時点で過去に遡って解読されるというリスクもある。現行の暗号技術は、暗号文を解読するのに膨大な計算を要するという数学的問題を拠り所としているため（いわゆる計算量的安全性。）、暗号が危たい化する危険性から逃れることはできない。このように、衛星の情報セキュリティ対策は、これまで地上系で使われてきた情報セキュリティ技術の単純な改良のみでは立ち行かないのが実情である。したがって、衛星搭載に適した実装性と安全性とを両立する新しい仕組みの導入が必要である。言い

換えると、人工衛星と地上局とで将来の計算機の発展によっても危たい化しない暗号鍵を配送する技術を極めて限られたリソースで実現する必要がある。

そのような安全な鍵配送技術に関しては、計算技術が進展しても解読の危険性が無い量子暗号技術の開発が地上系で進められており、衛星通信への導入も期待されている。しかしながら、人工衛星にこうした技術を適用するには、宇宙空間という過酷な環境、省スペース・省電力といった制約の多い環境下でも動作可能な高度なシステム構築が必要となる。また、量子暗号技術はレーザー光による通信技術を基礎にしているため、必然的に衛星光通信技術の高度化が必要であり、特に高速移動している人工衛星からの光を地上局で正確に受信できるよう捕捉追尾の精度や受信感度を高める必要がある。さらに、今後、より低コストで衛星通信ネットワークを構築し、かつ情報セキュリティを確保するためには、超小型衛星（100kg 以下の人工衛星：内閣府「宇宙基本計画」（平成 21 年６月２日）による）にも搭載できることが重要になる。

そこで、本研究開発では、超小型衛星に搭載可能な量子暗号通信技術、可搬型光地上局の開発、超小型衛星や航空機などの飛しょう体（以下、「飛しょう体」という）用空間光通信技術、及びインテグレーション・航空機等による実証実験によって、高秘匿な衛星通信の基盤技術を実現する。また、得られた成果について国際標準化活動等を推進することによって、我が国の国際競争力の向上を図る。

２．政策的位置付け

「宇宙産業ビジョン 2030」（平成 29 年５月 29 日）において、技術開発支援策の強化として、「宇宙関連技術は、科学技術と安全保障の両面の特性を有しており、我が国の国民生活を支えるものである。このようなデュアルユース技術については、研究機関・大学においても、研究者の裁量と責任において、積極的に取り組んでいくことが望ましい。また、デブリ除去技術、小型 SAR（合成開口レーダー）やテラヘルツセンサー、測位技術、衛星通信用技術（光・レーザー通信や量子暗号化技術等）、宇宙太陽光発電など、我が国の強みや重要技術を戦略的に強化していくことも重要である。」とされている。

また、「宇宙×ＩＣＴに関する懇談会　報告書」（平成 29 年８月８日）の中では、「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」とあり、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。

さらに、「宇宙基本計画」（平成 28 年４月１日、閣議決定）に基づく「宇宙基本計画

工程表」（平成 29 年 12 月 12 日改訂、宇宙開発戦略本部決定）の「13　技術試験衛星」において、「衛星通信における量子暗号技術の研究開発[総務省]」の実施が盛り込まれている。

３．目　標

（１）政策目標（アウトカム目標）

超小型衛星に搭載可能な量子暗号通信技術を開発することにより、計算技術が進展しても盗聴解読やデータ改ざんの脅威に怯えることのない安全性（以下、「情報理論的安全性」という。）を持った衛星通信網の実現に貢献する。

（２）研究開発目標（アウトプット目標）

超小型衛星に搭載可能な量子暗号通信技術、可搬型光地上局、飛しょう体用空間光通信技術を確立し、インテグレーション及び航空機等による実証実験を行う。特に、低軌道衛星 - 地上局間の典型的な空間光通信路損失に相当する 50dB 程度(すなわち送信信号強度が 10 万分の 1 程度に減衰する）の空間光通信路において、10 kbps を超える速度で情報理論的安全性を持った暗号鍵を配送する技術を実証する。

４．研究開発内容

（１）超小型衛星に搭載可能な量子暗号通信技術

①　概要

情報理論的安全性を持った暗号鍵を衛星・地上局間で配送する量子暗号通信技術の研究開発を行う。特に、低コストの超小型衛星に搭載可能な量子暗号通信技術を開発することで、将来の衛星コンステレーションによるネットワークにも適用可能な情報セキュリティ確保の基盤技術を確立することを目的とする。

②　技術課題

これまでに行われた自由空間における量子暗号通信の代表的な実証実験では、航空機 － 地上間において鍵生成速度 1kbps 程度（通信距離 7km で損失 40dB）[カナダ・ウォータールー大学、2016 年]、低軌道衛星 － 地上局間において鍵生成速度 500bps 程度（通信距離 650km で損失 30dB）[中国科学技術大学、2017 年]の性能が報告されている。これらの装置は大型航空機や重量 600kg を超える大型衛星に対応したものであり、将来的に商用技術へとつなげるためには、新たに超小型衛星に搭載可能な小型装置の開発が必要である。また、利用用途を拡大し広い市場開拓を目指すためには、鍵生成の高速化も重要な課題となる。そこで、以下の研究開発を実施する。

ア）装置の小型化・軽量化技術

飛しょう体に搭載するための量子暗号装置の小型化・軽量化を可能にする実装技術を開発する。

イ）鍵生成の高速化技術

小型・軽量かつ情報理論的安全性を確保したまま、鍵生成の高速化を実現する技術を開発する。従来の量子暗号方式の枠組みのみでは、上記実験例の鍵生成速度を大きく超えることは困難な可能性がある。そこで、「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し、適切な通信路評価技術を導入して通信路への盗聴攻撃リスクをより正確に推定することにより鍵生成の高速化を図るなど、衛星通信に適した新しい量子暗号方式を開発する。その際、大気変動などによる通信環境の変動があった場合でも、適応的な制御によって安定的に鍵生成が行えるような可用性の高い技術を開発する。

③　到達目標

当該暗号装置は超小型衛星に搭載可能なサイズ・重量とすること、及び飛しょう体と地上局からなる損失 50dB 程度（受信系の損失含む）の空間光通信路において、上述した「技術課題」に留意した方式において 10 kbps を超える鍵生成速度の実証を到達目標とする。

（２）可搬型光地上局の開発

①　概要

従来の衛星光通信では、限られた機関が大型の固定光地上局を運用している場合がほとんどであり、そのため、利用者が限定され、かつ、その設置場所における気象条件に通信性能が大きく影響されるという問題があった。そこで、空間光通信の稼働率を向上させ、そのユーザビリティ向上とサービス拡大を図るため、可搬型光地上局及びそのための空間光通信技術を研究開発する。

②　技術課題

可搬型光地上局及びそのための空間光通信技術を実現するため、以下の課題に対する研究開発を実施する。

ア）光地上局用空間光通信機器の小型化・軽量化技術

高精度な捕捉追尾機能を有する光学系について、可搬型光地上局において使用できるレベルの小型化・軽量化を実現する。また低軌道衛星 - 地上局間で想定される大気ゆらぎの影響を低減する機能を有し、小型化・軽量化に適した空間光通信技術を開発する。

イ）光地上局の可搬化技術

上記ア）で開発された空間光通信技術を実装した可搬型光地上局を開発する。その際、可搬型光地上局は、飛しょう体との光通信の稼働率を向上させるため、様々な環境でも容易に移動かつ設置ができ、設置後に空間光通信に必要な精度で光軸校正を行うことができ、通信品質の低下を緩和するための振動防止機能を有

したものとすること。

③ 到達目標

空間光通信路において、飛しょう体に搭載された空間光通信装置と可搬型光地上局との間の総損失が 50dB 以下の結合効率となり、かつ 10kbps を超える鍵生成速度が実現可能な可搬型光地上局の実現を到達目標とする。

（3）飛しょう体用空間光通信技術

① 概要

衛星による量子暗号通信のメリットを最大限に引き出すためには、衛星から出射された光ビームを可能な限り細く絞り光地上局の望遠鏡に結合させる必要がある。一方、超小型衛星では高精度な捕捉追尾技術の実現は依然として挑戦的課題である。そこで、狭ビームでも高精度な捕捉追尾機能を有し、かつ、飛しょう体に搭載可能な空間光通信機器の地上実証モデルを開発する。さらに、当該モデルを可搬型光地上局及び量子暗号通信機と組み合わせて、地上における実証実験を行う。

② 技術課題

過去の超小型衛星で用いられた光通信機器の捕捉追尾よりもすぐれた精度を実現するため、以下の課題に対する研究開発を実施する。

ア）飛しょう体用空間光通信機器の小型化・軽量化技術

飛しょう体に搭載するため、低軌道衛星 - 地上局間を想定した大気ゆらぎの影響を低減する機能を持った光通信装置の小型化・軽量化及び通信品質の向上を可能にする高精度光通信技術を開発する。

イ）飛しょう体用捕捉追尾技術

飛しょう体で生じうるじょう乱（エンジン・機体動揺）の影響を低減可能で、自局の高精度位置情報により捕捉追尾シーケンスを確立し相手局を高精度かつ高安定に捕捉追尾できる飛しょう体搭載用の実装技術を開発する。

③ 到達目標

空間光通信路において、飛しょう体に搭載された空間光通信装置の指向安定性を確保した上で、上記研究開発内容（1）及び（2）の技術課題と合わせて、当該空間光通信装置と可搬型地上局との間の総損失が 50dB 以下の結合効率を維持でき、10 kbps を超える鍵生成速度が実現可能な捕捉追尾性能の実証を到達目標とする。

（4）インテグレーション・航空機等による実証実験

① 概要

量子暗号通信で必要となる公開通信路用の RF 回線を用いた無線局の技術開発を行う。そして、当該無線局及び研究開発内容（1）～（3）で開発した技術をインテグ

レートし航空機等による実証実験を行う。

② 技術課題

ア）RF 回線送受信技術

暗号鍵生成においては、上記研究開発内容（１）～（３）で述べた空間光通信路とは別に、鍵蒸留処理に必要な情報をやり取りし、かつ搭載装置を遠隔制御するための無線公開通信路を利用することが適切である。そこで、鍵生成と遠隔制御のために十分な帯域を有する無線局の開発を行う。

イ）インテグレーション実証実験

上記無線局及び研究開発内容（１）～（３）で開発した技術をインテグレートし、航空機等による実証実験を行う。また、実証実験に適した航空機等の調査も合わせて進める。

③ 到達目標

上記（１）③に挙げた到達目標をフィールド環境において実証する。

５．研究開発期間

平成３０年度から平成３４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Ⅰ、Ⅱ、Ⅲ、Ⅳ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。

また、課題Ⅳの受託者は、本研究開発課題全体の取りまとめを行うものとする。

課題Ⅰ．超小型衛星に搭載可能な量子暗号通信技術

ア）装置の小型化・軽量化技術

イ）鍵生成の高速化技術

課題Ⅱ．可搬型光地上局の開発

ア）光地上局用空間光通信機器の小型化・軽量化技術

イ）光地上局の可搬化技術

課題Ⅲ．飛しょう体用空間光通信技術

ア）飛しょう体用空間光通信機器の小型化・軽量化技術

イ）飛しょう体用捕捉追尾技術

課題Ⅳ．インテグレーション・航空機等による実証実験

ア）RF 回線送受信技術

イ）インテグレーション実証実験

（２）提案及び研究開発にあたっての留意点

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。

② アウトカム目標の達成に向けた適切な研究成果の取扱方策（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。）について提案書に記載すること。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。

③ 複数機関による共同研究を提案する際には、研究開発全体を整合的かつ一体的に行えるよう参加機関の役割分担を明確にし、研究開発期間を通じて継続的に連携するための方法について具体的に提案書に記載すること。

④ 技術課題Ⅳ．ア）の RF 回線送受信技術の開発にあたって必要のある場合には、無線局開設・運用のための免許申請を行うこと。

⑤ 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。

⑥ 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「衛星通信における量子暗号技術の研究開発」（平成 30 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記載すること。