国立研究開発法人情報通信研究機構
国立大学法人東京大学大学院工学系研究科
株式会社ソニーコンピュータサイエンス研究所
次世代宇宙システム技術研究組合
スカパーJSAT株式会社

国際宇宙ステーションと地上間での秘密鍵共有と高秘匿通信に成功

～衛星量子暗号通信の実用化に期待～

【ポイント】

- 国際宇宙ステーションから可搬型光地上局への光通信で安全な鍵を共有、高秘匿通信可能なシステムを開発
- 1 回の上空通過で 100 万ビット以上の安全な秘匿鍵共有が可能
- 国家安全保障や外交などの高秘匿通信で用いることができる衛星量子暗号通信システムの社会実装に期待

国立研究開発法人情報通信研究機構（ＮＩＣＴ（エヌアイシーティー）、理事長: 徳田　英幸）、国立大学法人東京大学大学院工学系研究科（研究科長: 加藤　泰浩）、株式会社ソニーコンピュータサイエンス研究所（代表取締役社長: 北野　宏明）、次世代宇宙システム技術研究組合（理事長: 山口　耕司）及びスカパーJSAT株式会社（代表取締役　執行役員社長: 米倉　英一）は、低軌道上の国際宇宙ステーション[*1]（ISS）から地上の可搬型光地上局への光通信により、1 回の上空通過で 100 万ビット以上の秘密鍵を共有し、ISS と地上局とでの情報理論的に安全な通信の実証に成功しました。

本通信実証の成功により、低軌道衛星からの光通信による高速かつ高い安全性を持つ暗号鍵を任意の地上局と共有する技術的な見通しが立ちました。

本技術が実用化されれば、原理的に地球上のどこでも安全な暗号鍵の共有ができ、通信で漏えいを防ぐことができるため、国家安全保障や外交の分野において不可欠な重要情報の高秘匿通信が可能になります。今後、本技術の開発を更に進め、機密情報を扱うユーザ向けの衛星量子暗号システムの社会実装を目指します。

【背景】

近年、量子コンピュータ研究が急速に進展し、この実現により従来の暗号技術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ます。また、今は解読できない暗号データでも、一旦保存しておいて将来高度なコンピュータで全データを解読するタイプの攻撃がされるおそれは現に高まっています。個人・国家レベルの重要な機密情報を将来にわたって安全にやり取りするためには、いかなる計算機によっても解読が不可能な、情報理論的安全性を有する暗号技術の導入が喫緊の課題となっています。

この課題に応えるべく、NICT では、情報理論的に安全な鍵共有・秘匿通信を可能とする技術として量子鍵配送[*2]・量子暗号[*3] 通信の開発を進めてきました。現在、地上光ファイバー網における量子暗号通信の更なる高速化・長距離化に資する研究開発（量子鍵配送ネットワークとして 100 km 圏内を対象とした地上 2 地点間の量子鍵配送装置や、トラステッドノードをベースとした量子鍵配送ネットワークの研究開発など）に取り組んでいますが、量子鍵配送をグローバル規模に拡大するには、数千 km にわたる量子暗号通信を行う必要があり、地上光ファイバー網では通信路の途中で中継する量子中継技術の発展を待たねばならない状況です。

一方、地上での中継が不要な、衛星を用いた量子鍵配送の可能性も模索され、2017 年に中国で衛星量子鍵配送の実験が成功しました。これを機に世界各国で衛星量子暗号技術の開発が進めら

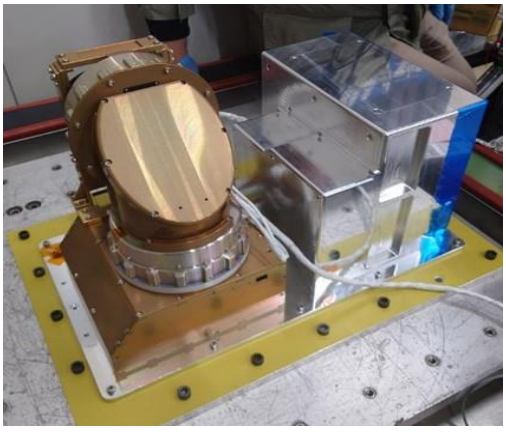

図 2 今回開発した SeCRETS のフライトモデル外観

れましたが、共有される鍵の量が限られ、また大型の地上局が必要など、その実用には課題が残っていました。

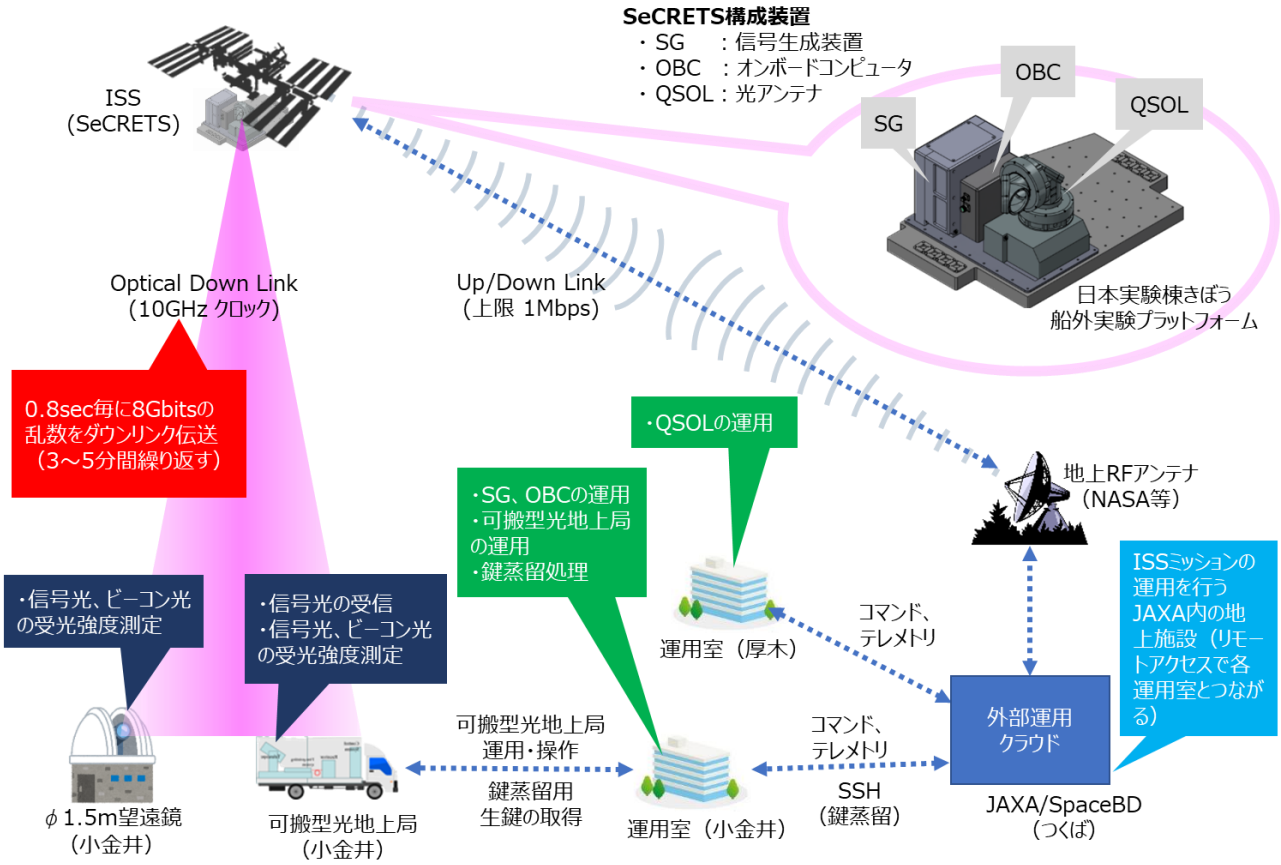

図 1　ISS-可搬型光地上局間の物理レイヤ暗号通信実験の全体構成図

【今回の成果】

今回、NICT を始めとした 5 機関の研究開発チームは、衛星―地上局間の見通し通信路の性質を利用し、より高効率で鍵共有を可能とする物理レイヤ暗号[*4] の研究開発を進め、その宇宙実証を行いました。

今回の実験（図 1 参照）で我々研究開発チームは、低軌道高秘匿光通信装置（SeCRETS[*5]）を開発し、ISS の日本実験棟きぼう船外実験プラットフォームに搭載しました（図 2 参照）。この SeCRETS から 10 GHz クロックで乱数データ（鍵データ）を変調した信号光を地上に向けて発射し、NICT 本部（東京都小金井市）に設置した可搬型光地上局の直径 35 cm 反射型望遠鏡（図 3 参照）で信号光を受信することができました（なお、可搬型光地上局及びそこから 25 m 離れた直径 1.5 m 地上固定局望遠鏡で光信号とビーコン光の光強度を測定し、地上での光ビームの広がり具合を推定しています。）。そして、信号の盗聴者への情報漏えい量を無限小とするため、この受信した乱数データを ISS と地上局の間で鍵蒸留処理[*6] をすることで、1 回の上空通過で 100 万ビット以上の安全な暗号鍵の生成に成功しました。

さらに、この蒸留処理した暗号鍵を用いて軌道上にある写真データをワンタイムパッド暗号[*7] 化して ISS からの電波による通信を通じて地上に送信し、復号することでこの写真データを取得することにも成功しました（図 4 参照）。

今回開発した SeCRETS は、そのほとんどの部分を民生

図 3　今回開発した可搬型光地上局と直径 35 cm 望遠鏡の外観

図 4　今回開発した SeCRETS（写真中央）と同装置を船外実験プラットフォームに取り付けた古川宇宙飛行士。
この写真を軌道上でワンタイムパッド暗号化して地上に送信後、復号により取得に成功した。

部品で構成していますが、低軌道衛星を想定した環境での使用を想定した耐真空環境、耐放射線被曝に関する試験を行い、低軌道のような過酷環境下でも問題なく動作することを確認しています。また、光学系望遠鏡をトラックに搭載することで可搬型の光地上局を構成し、かつ、高速変調した信号の受信のための極めて微細な調整が可能な追尾システムを導入しています。

これらの開発により、衛星搭載用暗号装置の低コスト化及び開発期間短縮の可能性を高め、可用性の高い可搬型光地上局を用いた高速光通信を実証することができ、衛星量子暗号通信の社会実装に向けて大きな一歩を踏み出しました。

【今後の展望】

本プロジェクトで行った実証研究では、光送信を行う範囲をセキュリティの確保された受信局周辺の区域に限る方式（物理レイヤ暗号）を用いて行いました。今後はここで得られた結果の検証を進めることで、暗号装置に組み込む機器等の開発を更に進め、衛星搭載用の量子鍵配送装置の製作を加速させます。

また、量子鍵配送実証に好適な電力系や姿勢制御系を備えた衛星バスシステムの開発を視野に入れた研究・開発を加速させ、実用化への足掛かりとします。

さらに、ISS-可搬型光地上局での実験デモを更に進め、我が国独自の衛星量子暗号を実現するための基本データ収集を実施する予定です。

＜用語解説＞

***1 国際宇宙ステーション**

国際宇宙ステーション（International Space Station, ISS）は、NASA（米国）、ロスコスモス（ロシア）、JAXA（日本）、ESA（ヨーロッパ）、CSA（カナダ）の 5 つの宇宙機関が参加する多国籍共同プロジェクトによる低軌道にあるモジュール式の宇宙ステーション（居住可能な人工衛星）。
日本は実験棟（きぼう）を運用しており、ロボットアーム、電源供給ポートなどを備えた船外実験モジュールが用意されている。

***2 量子鍵配送**

量子鍵配送（Quantum Key Distribution, QKD）は、通信を行う二者間でのセキュア通信を保証するために、量子力学を用いてランダムな暗号鍵を共有する手法であり、現在、東芝が製品化を行っている。
（参考）https://www.global.toshiba/jp/products-solutions/security-ict/qkd.html

***3 量子暗号**

量子暗号は、光子を使って暗号鍵共有を行う量子鍵配送（QKD）装置、及びその暗号鍵を使い、ワンタイムパッド（OTP）方式により、情報の暗号化・復号を行う暗号技術のこと。量子コンピュータを含むあらゆる計算機で原理的に解読できない極めて安全な通信を実現できる（図 5 参照）。

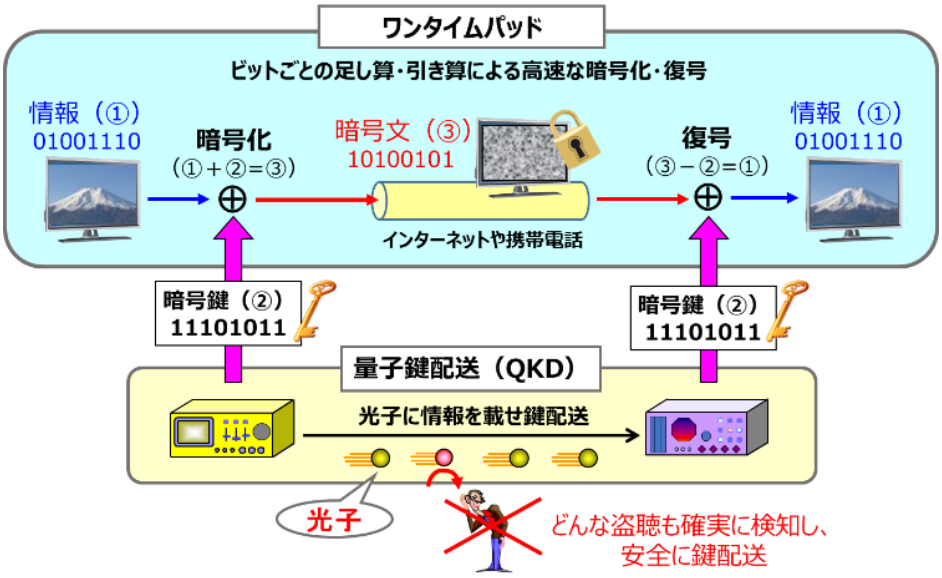

図 5 量子暗号模式図
下部の QKD レイヤで暗号鍵共有を行い、その暗号鍵を使い、上部のアプリケーションレイヤで暗号通信を行う。

***4 物理レイヤ暗号**

物理レイヤ暗号は、狭い広がりのレーザによる見通し通信であるという光空間通信の特長を活用し、受信局の周辺の限られた領域のセキュリティを確保することで、いかなる計算能力を持つ盗聴者に対しても安全に情報を送ることができる技術。

***5 低軌道高秘匿光通信装置**

低軌道高秘匿光通信装置（SeCuRe lasEr communicaTionS terminal for LEO, SeCRETS）は、信号生成器（Signal Generator, SG）、内部電源制御用オンボードコンピュータ（On Board Computer, OBC）及び光アンテナ（Quantum-Small Optical Link, QSOL）によって構成され、SG 内で生成した乱数データを信号化し QSOL から光信号を地上局に向けて射出する装置（SG には鍵蒸留処理ソフトウェアも搭載）。

***6 鍵蒸留処理**

鍵蒸留処理は、送信側と受信側で共有した鍵データの誤りを訂正する機能及び盗聴者に漏れた情報量を除去する秘匿性増強処理を合わせたプロセス。

***7 ワンタイムパッド暗号**

ワンタイムパッド（One Time Pad, OTP）暗号とは、暗号化対象のデータと同じ長さの乱数を暗号鍵として暗号化し、さらに、一度使用した乱数は二度と使わないようにする暗号方式。

＜各機関の役割分担＞

・情報通信研究機構: 暗号技術及び ISS 搭載用の暗号装置の開発・運用、可搬型光地上局の開発・運用
・東京大学大学院工学系研究科: 量子鍵配送、物理レイヤ暗号通信に関する安全性の検討
・ソニーコンピュータサイエンス研究所: ISS 搭載用の光アンテナの開発・運用
・次世代宇宙システム技術研究組合: ISS 搭載装置のインテグレーション、実証実験のコーディネート
・スカパーJSAT: 可搬型光地上局の運用、実証実験環境の整備、衛星量子鍵配送の事業化に向けた市場・技術動向調査等

＜関連する過去の報道発表＞

・2023 年 3 月 16 日付け
スカイツリー-地上可搬局での盗聴解読の脅威のない暗号鍵共有に向けた光伝送実証に成功
-衛星と地上間での量子暗号を見据えた原理実証実験-
https://www.nict.go.jp/press/2023/03/16-1.html

本研究開発は、総務省「ICT 重点技術の研究開発プロジェクト（JPMI00316）」のうち「衛星通信における量子暗号技術の研究開発（JPJ007462）」の一環として実施されました。

（参考）総務省報道発表
2018 年 6 月 14 日付け
平成 30 年度 情報通信技術の研究開発に係る提案の公募の結果
http://www.soumu.go.jp/menu_news/s-news/01tsushin03_02000247.html

＜ 本件に関する問合せ先 ＞
国立研究開発法人情報通信研究機構
量子 ICT 協創センター
藤原　幹生

国立大学法人東京大学工学系研究科
光量子科学研究センター
小芦　雅斗

株式会社ソニーコンピュータサイエンス研究所
広報窓口

次世代宇宙システム技術研究組合
森田　皓子

＜ 広報 （取材受付）＞
国立研究開発法人情報通信研究機構
広報部 報道室

国立大学法人東京大学大学院工学系研究科
広報室

株式会社ソニーコンピュータサイエンス研究所
広報窓口

次世代宇宙システム技術研究組合
森田　皓子

スカパーJSAT株式会社
広報・IR部