プレスリリース
2021 年 8 月 17 日

国立研究開発法人情報通信研究機構
インターステラテクノロジズ株式会社
法　　政　　大　　学

観測ロケット MOMOv1 で情報理論的に安全な実用無線通信に成功

【ポイント】

- 観測ロケット MOMOv1 から地上局に飛行状況を伝送する実用チャネルでセキュア通信の実証実験
- 開発した情報理論的に安全な通信セキュリティ技術の動作確認に実用速度（512 kbps）で成功
- 小型宇宙機の飛行の安全確保に不可欠な伝送データの保護に寄与

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田　英幸）サイバーセキュリティ研究所、インターステラテクノロジズ株式会社（IST、代表取締役: 稲川　貴大）及び法政大学（総長: 廣瀬　克哉）は、共同で開発した小型衛星・小型ロケット用通信セキュリティ技術を観測ロケット MOMOv1[*1] に搭載し、2021 年 7 月 31 日（土）、機体から地上局に飛行状況を伝送する実用チャネルにおいてセキュア通信の実証実験に成功しました。

本研究の目標は、小型宇宙機の乗っ取り防止による飛行の安全確保と、小型宇宙機から伝送される飛行状況や学術的・商業的価値の高いデータの保護のため、第三者によるなりすまし・改ざん・盗聴を防ぐことです。本実験によって、通信の秘匿・認証を最も高いセキュリティである情報理論的安全性で実現できることを実用速度（512 kbps）で確認しました。本成果は、小型宇宙機の飛行の安全確保等に不可欠な伝送データの保護に寄与します。

【背景】

民間事業者による小型衛星が学術・商用目的で多数打ち上げられるようになり、平成 30 年 11 月 15 日に「人工衛星等の打上げ及び人工衛星の管理に関する法律」が施行されました。本法律に基づく基準等に関するガイドライン[*2] において、人工衛星の打上げ用ロケットの型式認定や飛行許可に当たり、重要なシステム等に関する信号の送受信については適切な暗号化等の措置が求められています。NICT、IST 及び法政大学は 2018 年から共同で、NewSpace 時代[*3] に向けた小型宇宙機用通信セキュリティ技術を研究開発しています。

本研究の目標は、小型宇宙機の乗っ取り防止による飛行の安全確保と、小型宇宙機から伝送される飛行状況や学術的・商業的価値の高いデータの保護のため、第三者によるなりすまし・改ざん・盗聴を防ぐことです。これまでに、通信の秘匿・認証を最高レベルのセキュリティである情報理論的安全性で実現する通信セキュリティ技術[*4] を開発し、民生電子デバイスを用いたプロトタイプ通信装置を観測ロケット MOMOv0 に搭載し、実験チャネルで動作確認を実施してきました。[注 1)]

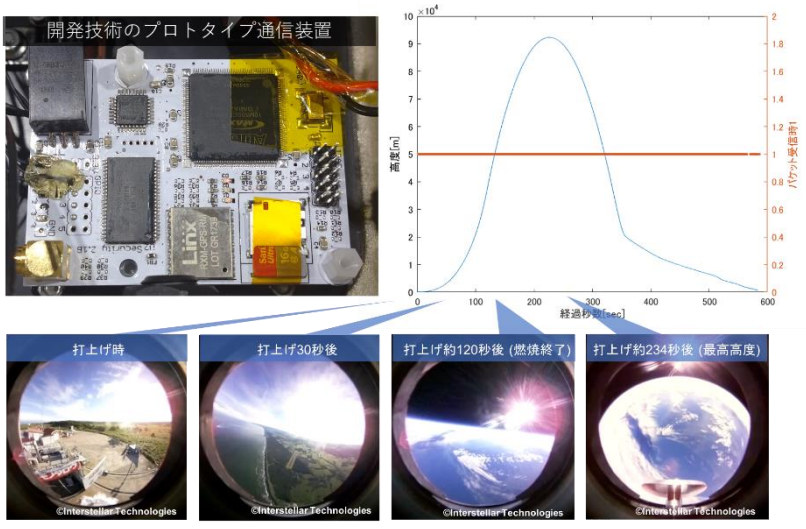

図 1　本実証実験に用いた開発技術のプロトタイプ通信装置と
実験期間中の機体高度とパケット受信状況

【今回の成果】

今回の実験の目的は、我々が開発した情報理論的に安全な通信セキュリティ技術が小型宇宙機から地上局への通信の実用に資することを実証することです。

本年 7 月 31 日（土）の観測ロケット MOMOv1 の打上げ時に、開発技術を民生電子デバイスで実装したプロトタイプ通信装置を搭載し、機体から地上局に情報を伝送する実チャネル（8 Mbps）のうち機体情報分（512 kbps）に開発技術を適用し、動作確認に成功しました。動作環境は、アメリカ連邦航空局の基準 80 km に到達する宇宙空間への弾道飛行として典型的なものであり、軌道投入ロケット初段に類似します。民生電子デバイスを利用して、情報理論的安全性という最高レベルのセキュリティを高速な実用チャネルで達成したことは、世界初の成果になります。なお、本開発技術は軽量なため、実チャネル全体に適用範囲を拡張することは容易にできる見込みです。

本開発技術は、他の情報理論的に安全な技術と同様、送信側と受信側で多量（通信データの総量以上）の鍵を事前共有し使い捨てていきます。開発においては、MOMOv0 の実験結果を踏まえ、高速な実用チャネルにおける潜在的脅威を分析しました。そして、通信遅延が変動しても送信側と受信側が同時に同じ鍵を使い（鍵同期）、同期情報の損壊から復帰する（同期復帰）ように設計し、セキュリティ喪失への対策を施しています。また、装置コストを価格面のみならず装置重量や必要部品点数、消費電力に至るまで削減し、多様な小型宇宙機に適用可能としています。

【今後の展望】

今後も、情報理論的に安全な通信セキュリティ技術の実用化に向けて、更なる技術検証と技術改良を進め、民間事業者による宇宙ビジネスに欠かせない小型宇宙機の飛行の安全確保等に不可欠な伝送データの保護に寄与します。

注 1)　2019 年 7 月 10 日 プレスリリース「NewSpace 時代に向けた通信セキュリティ技術の初期実験に成功」
https://www.nict.go.jp/press/2019/07/10-1.html

＜用語解説＞

***1　観測ロケット MOMO**

観測ロケット（sounding rocket）とは、高空や宇宙空間において科学実験や観測などを行うことを主な目的として弾道飛行するロケットのことである。MOMO は、インターステラテクノロジズ株式会社が開発した観測ロケットであり、ペイロードを宇宙空間へ低コストで打ち上げることができる。その用途は、従来から行われている科学実験や観測、技術試験の範囲にとどまらず、広告やエンターテインメントなどにも広がることが期待されている。2021 年 7 月 31 日（土）時点までに 7 機の打上げが行われている。

***2　人工衛星等の打上げ及び人工衛星の管理に関する法律に基づく基準等に関するガイドライン**

本ガイドラインは、内閣府宇宙開発戦略推進事務局が発行している 4 つのガイドラインを指す。その中の一つ「人工衛星の打上げ用ロケットの型式認定に関するガイドライン」の 6.5.2 節「信頼性及び多重化」に「また、重要なシステム等に関する信号の送受信については、妨害や乗っ取りの被害にあわないよう、適切な暗号化等の措置を講ずること。」と記載されている。

***3　NewSpace**

2000 年頃から始まり最近になって活発化した、従来型の政府主導とは異なった民間主導による（ベンチャー企業や異業種参入を含む）宇宙開発活動を総括的に表した言葉。その活動は、人工衛星やロケットの開発と運用、衛星通信やリモートセンシング等のサービス提供、宇宙探査やスペースデブリ除去、エンターテインメント、有人飛行など多岐にわたる。際立った特徴の一つは、商用ベースに乗せることが求められるためにコストダウンや事業スピード向上への要求が強く、新規技術導入にも柔軟な点である。

図 2　サウンディングロケット「モモ」MOMOv1 内部構造図

***4　情報理論的に安全な通信セキュリティ技術**

通信セキュリティ技術（あるいは暗号）が情報理論的に安全とは、通信の秘匿や認証などのセキュリティを満たすために、送受信者間で通信量に応じた大量の使い捨て鍵を事前に共有することで、攻撃者が無制限の計算リソースを有するとしても、そのセキュリティが破られないことを指す。ここで、無制限の計算リソースとは、スーパーコンピュータなどの現在の計算技術だけでなく、量子コンピュータを含めた将来のあらゆる計算技術を含む。

補足資料

今回の成果のポイント

今回の実験の目的は、NICT、IST 及び法政大学の共同研究で開発した通信セキュリティ技術が、実用チャネルの実用速度で正常に動作することを確認し、小型宇宙機の実用に資することを実証することです。

本開発技術は、図 3 に示すように、地上局と小型衛星・小型ロケットとの通信において、送信元のなりすまし及び制御コマンドの改ざんを防ぎ、飛行の安全を確保します。さらに、地上へ伝送される飛行状況や学術・商用的に高い価値を有するデータの盗聴も防ぎ、伝送データを保護します。

また、本開発技術は、前述のとおり、送信側と受信側で多量（通信データの総量以上）の鍵を事前共有します。打上げ前に地上局と小型衛星・小型ロケットが物理的に近接するため、鍵共有が物理的に容易（鍵ストレージを直接装着等）であり、ライフタイムが比較的短く、通信データの総量（すなわち鍵の総量）が抑えられます。これらにより、情報理論的安全性を低コストで達成できています。

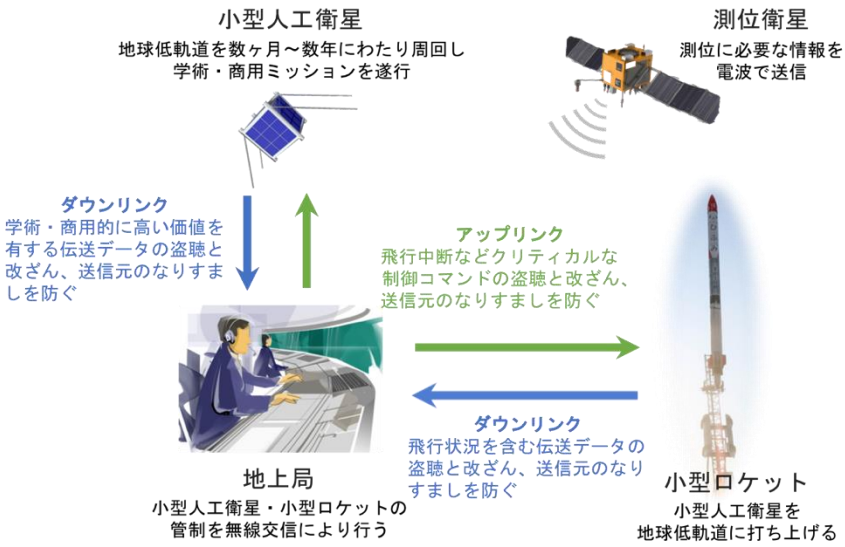

図 3 本開発技術によるアップリンク・ダウンリンクの通信セキュリティ

実験では、開発技術を小型ロケットから地上局へのダウンリンクの実用チャネルに適用し、実用速度（512 kbps）で「鍵スケジューリング」「秘匿」「認証」といったセキュリティ処理が正しく動作することを確認します。

- 「鍵スケジューリング」は、鍵同期と鍵回復、受信者と GNSS 受信機から得た情報を利用
- 「秘匿」は、通信内容の秘匿、加算演算のみ
- 「認証」は、なりすましと改ざんの検知、加算演算と乗算演算のみ

これまでの実験で得られた知見を基に、鍵スケジューリングを改良し、通信遅延が変動しても鍵同期が失敗せず、鍵同期のための情報が破損しても検知し、修復し、鍵回復が可能な方式を開発・装備しています。

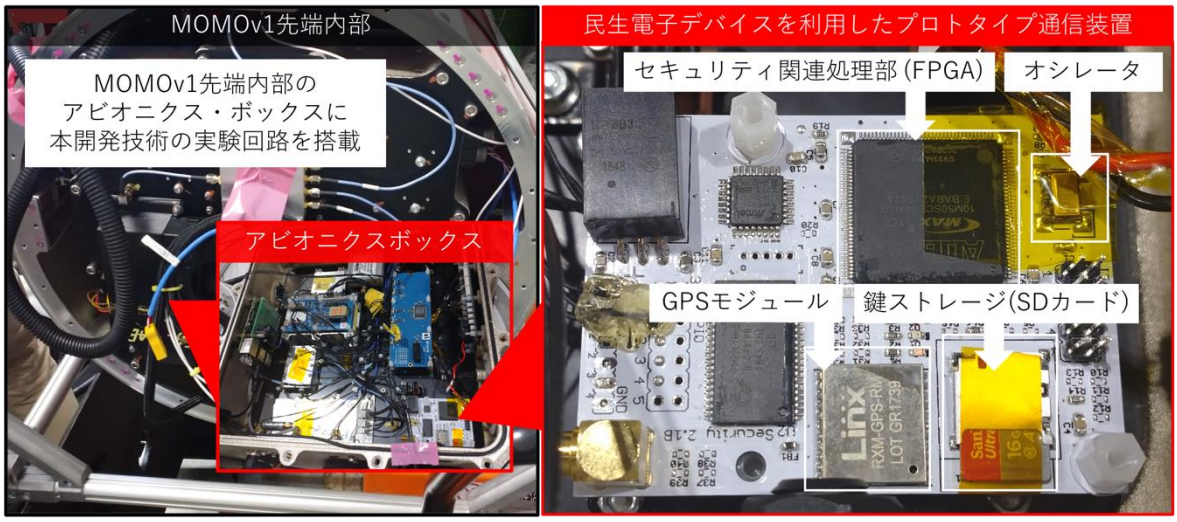

図 4 今回の実験に用いたプロトタイプ実験装置

本開発技術のプロトタイプ通信装置を図 4 に示すように MOMOv1 先端内部のアビオニクス・ボックスに搭載し、打上げ時からパケット受信・セキュリティ処理結果を記録しました。

図 5 に示す実験期間において、表 1 に示すようにパケット欠損時以外は、抽出パケットにおいてセキュリティ処理が完璧に機能しています。

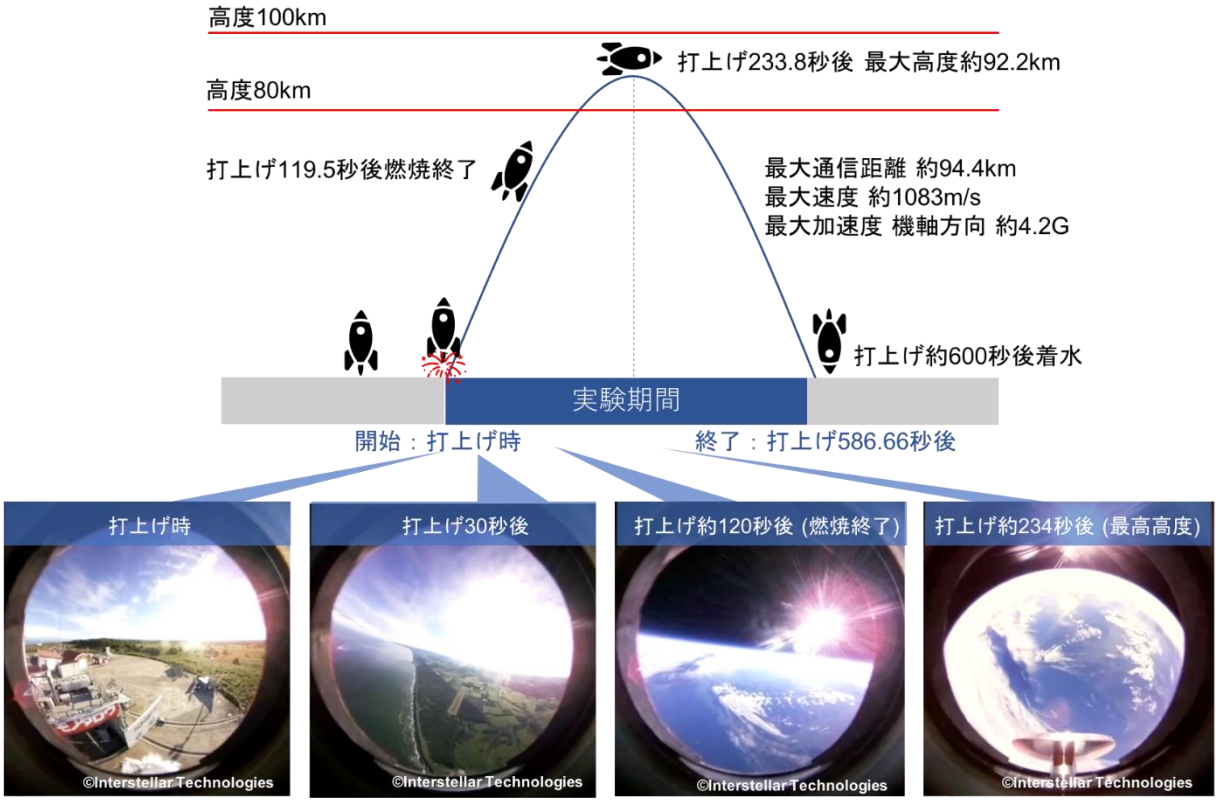

図 5 実験期間と MOMOv1 の位置及び機体からの画像

表 1 打上げから着水直前の 586.66 秒後までのパケット受信・処理結果
（打上げ後 560 秒頃までは、ほぼパケット受信失敗なし）

処理結果		パケット数
パケット受信成功	セキュリティ処理成功	558,313
	セキュリティ処理失敗	無し
パケット受信失敗（誤り・消失による欠損）		28,352
総パケット		586,665

＜ 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
サイバーセキュリティ研究所
セキュリティ基盤研究室
吉田 真紀
E-mail: security@ml.nict.go.jp

インターステラテクノロジズ株式会社
森岡 澄夫
Tel: 01558-7-7330
E-mail: press@istellartech.com

法政大学
尾花 賢
E-mail: pr@sec.cis.k.hosei.ac.jp

＜ 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
Tel: 042-327-6923
E-mail: publicity@nict.go.jp

インターステラテクノロジズ株式会社
広報 小林
Tel: 01558-7-7330
Email: press@istellartech.com

法政大学
総長室広報課（栗山・田村）
Tel: 03-3264-9240
E-mail: koho@hosei.ac.jp