プレスリリース
2019 年 7 月 10 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

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

【ポイント】

- 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に適することを宇宙への飛行で実証
- 小型宇宙機の飛行環境下において情報理論的安全性を民生用電子部品で達成
- 小型宇宙機の課題である伝送データの保護と飛行の安全確保に寄与

国立研究開発法人情報通信研究機構（NICT、理事長: 徳田　英幸）セキュリティ基盤研究室、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: 田中　優子）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の実験回路を、観測ロケット「宇宙品質にシフト　MOMO3　号機」[*1]（以下「MOMO3」）に搭載し、2019 年 5 月 4 日（土）、宇宙への飛行環境下における動作確認に成功しました。

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において、適切なセキュリティを確立することです。本実験によって、最高レベルのセキュリティである情報理論的安全性が、民生用電子部品で達成できること、及び小型宇宙機に適していることを実証しました。本成果は、小型宇宙機通信におけるセキュリティ課題の解決に寄与し、NewSpace[*2]と呼ばれる宇宙開発の進展に貢献します。

【背景】

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[*3]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。民間事業者が宇宙ビジネスに参入する　NewSpace　時代に向け、NICT、IST 及び法政大学は 2018 年から共同で、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において、適切なセキュリティを確立することです。これまでに、最高レベルのセキュリティである情報理論的安全性の実現における二大課題（鍵の事前共有と総量）が、地上局と小型衛星・小型ロケットとの通信においては解決し得ることを見いだし、情報理論的に安全な通信セキュリティ技術[*4] の開発と民生用電子部品を用いたプロトタイプ実装、及び地上実験を実施してきました。

図 1: 今回の飛行環境下の実験に用いた MOMO3

【今回の成果】

今回の飛行実験の目的は、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に適していることを実証することです。

NICT セキュリティ基盤研究室の吉田真紀主任研究員、IST の森岡澄夫博士、法政大学の尾花賢教授は、本年 5 月 4 日（土）の観測ロケット MOMO3（機体全長 9.9 m、全備重量 1.1 ton、外径 502 mm）の打上げ

時に、本開発技術を民生用電子部品で実装した実験回路を機体に搭載し、宇宙への飛行環境下における動作確認に成功しました。飛行条件は、液体燃料ロケットの初段として典型的であり、打上げ後 1 分で最大動圧点（Max-Q）[*5]を超え、最大秒速 1.25 km、最大加速度 5G、最大高度 113.4 km に到達しました（いずれも概算値）。実際の飛行環境下で、情報理論的安全性という最高レベルのセキュリティを民生用電子部品で達成したことは、世界初です。

本開発技術は、地上局・小型ロケット・小型衛星の通信におけるセキュリティ関連処理と、通信の同期維持処理から成ります。まず、通信の不安定な状況で通信の齟齬から管制を喪失しないよう、相互確認を最小限にしました。さらに、通信相手が打上げ数分後には音速の数倍以上という速度で移動する状況で、セキュリティ関連処理の遅延によってリアルタイム性が損なわれないように、情報理論的に安全な技術の特長を生かし、計算効率が良く回路規模が小さい方式を設計し、通信の同期維持処理にも応用しました。

また、本開発技術は、回路コストを MOMO3 の機体コストの 0.1%未満に抑え、従来の小型衛星と同グレードの民生用電子部品を利用しているため、多様な小型宇宙機への適用が可能です。

【今後の展望】

今後も、本格的な飛行環境下における、更なる技術検証と技術改良を進め、NewSpace 時代の宇宙ビジネスに欠かせない伝送データの保護と飛行の安全確保に貢献します。本成果について、2019 年 7 月 23 日（火）と 24 日（水）に高知県高知市で開催される「セキュリティサマーサミット 2019」[*6]で発表します。

＜ 本件に関する問い合わせ先 ＞
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
Tel: 042-327-7634
E-mail: newspace_security@ml.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
E-mail: press@istellartech.com

法政大学
尾花 賢
Tel: 042-387-4358
E-mail: obana@hosei.ac.jp

＜ 広報 ＞
国立研究開発法人情報通信研究機構
広報部 報道室
廣田 幸子
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

＜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、約 20kg のペイロードを高度 100km 以上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。2019 年 7 月 10 日時点までに 3 機の打ち上げが行われてきており、本実験で利用された MOMO3 は、日本の民間企業が独自に開発したロケットとしては初めて宇宙空間に到達した機体である。

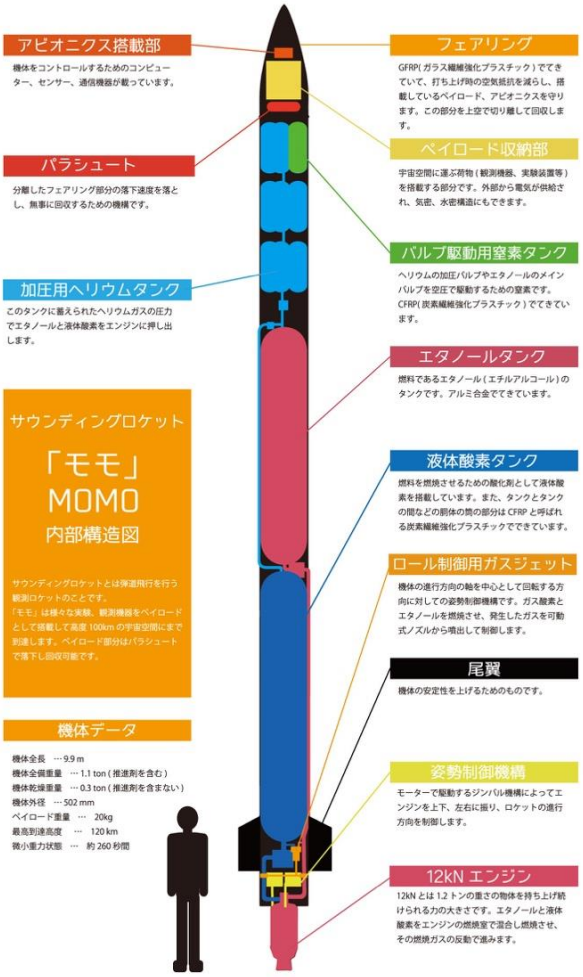

図 2: サウンディングロケット「モモ」MOMO 内部構造図
（http://www.istellartech.com/technology/momo）

***2 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。

***3 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 p.13、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。

***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、スパコン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。

***5 最大動圧点（Max-Q）**

ロケットが地上から大気圏を抜けるまでの間に最も空気抵抗を受ける時点を指す。空気抵抗は、上昇開始直後から増えていき、Max-Q 後には減じていく。典型的なロケットでは、離陸後 1 分前後が Max-Q であり、1 平方メートル当たり 3,000 kg 重（進行方向に向いている面）の力がかかる。機体破壊などが最も起こりやすい時点である。

***6 セキュリティサマーサミット 2019**

正式名称: 電子情報通信学会 ISEC/SITE/ICSS/EMM/HWS/BioX 研究会共催，情報処理学会 CSEC/SPT 合同研究発表会

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、実際の飛行において正常に動作し、小型宇宙機に適してい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。これらの通信セキュリティに加えて、本開発技術は、地上局と小型宇宙機（特に小型ロケット）との通信における強い要求であるリアルタイム性も満たします。

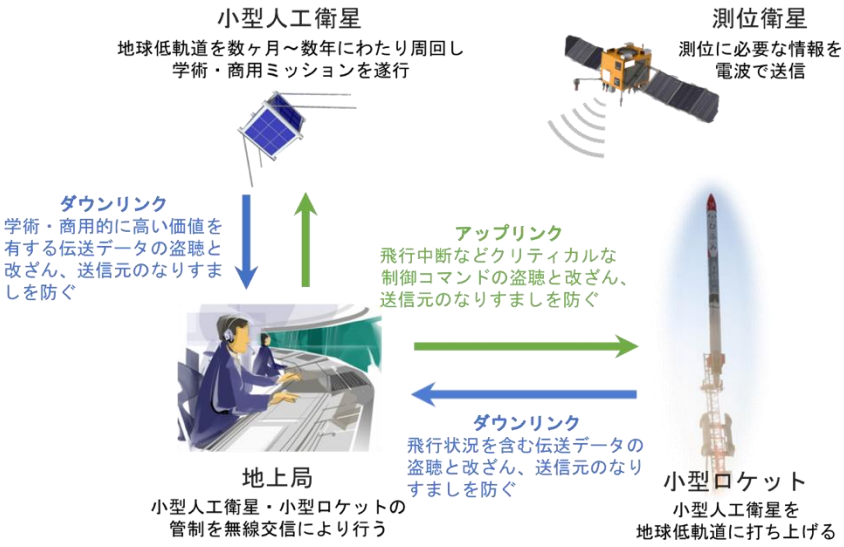

図 3: 本開発技術によるアップリンク・ダウンリンクの通信セキュリティ

本開発技術は、前述のとおり、通信におけるセキュリティ関連処理と通信の同期維持処理から成り、セキュリティ関連処理には、以下の「鍵スケジューリング」「秘匿」「相手認証・改ざん検出」の仕組みがあります。

- 「鍵スケジューリング」には測位衛星から得た情報を利用し、鍵の不一致と再利用を防止
- 「秘匿」の仕組みは加算演算のみ
- 「相手認証・改ざん検出」の仕組みは加算演算と乗算演算のみ、通信の同期維持処理にも活用

なお、想定する通信システムでは、打ち上げ前に地上局と小型ロケット・小型衛星が物理的に近接するため、鍵共有が物理的に容易であり、ライフタイムが比較的短く、総通信量（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。

本実験では、開発技術のソフトウェアやハードウェアの構成要素が個別に正しく動作することを確認するため、図 4 の実験系を構成しました。FPGA 実装部には、情報理論的に安全な秘匿と相手認証・改ざん検出に用いる演算がセキュリティ関連処理部として実装されています。

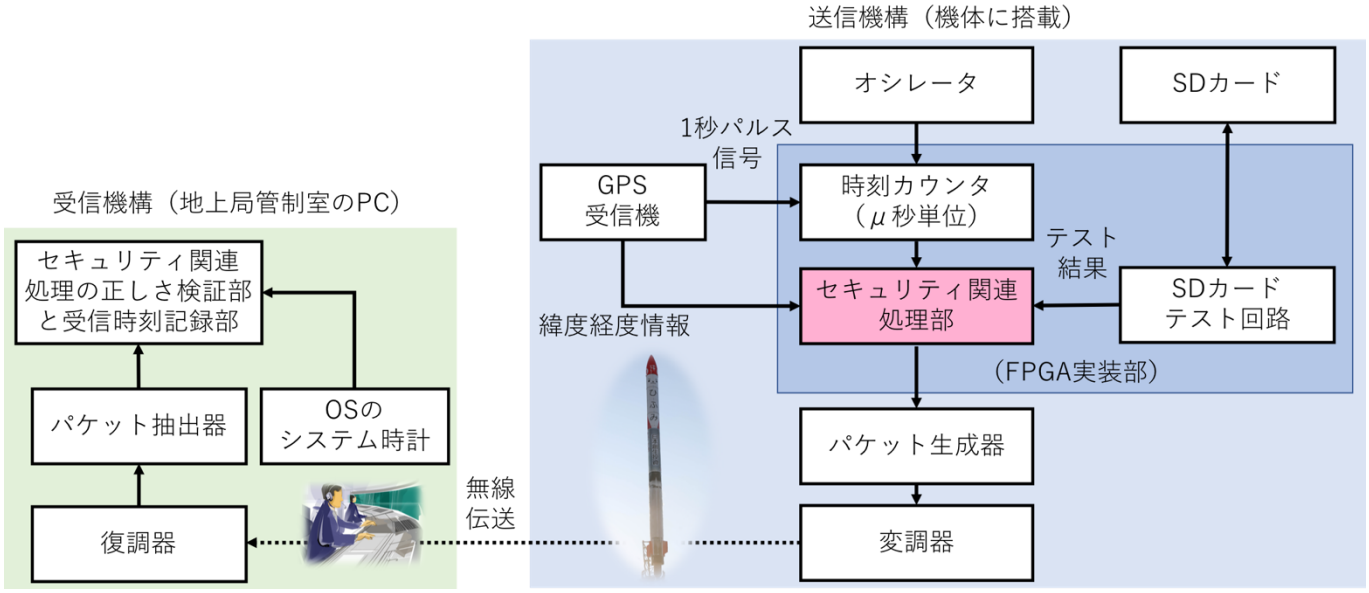

図 4: 実験系における処理構成

本実験回路を、図 5 に示すように MOMO3 先端内部のアビオニクス・ボックスに搭載し、約 600m 離れた地上局に設置した PC に、パケット受信・セキュリティ処理結果を打上げ 20 秒前から記録しました。図 6 に MOMO3 の射点と地上局との位置関係を、図 7 に地上局室内から撮影した MOMO3 打上げ直後の PC に表示されたパケット受信・セキュリティ関連処理結果を示します。

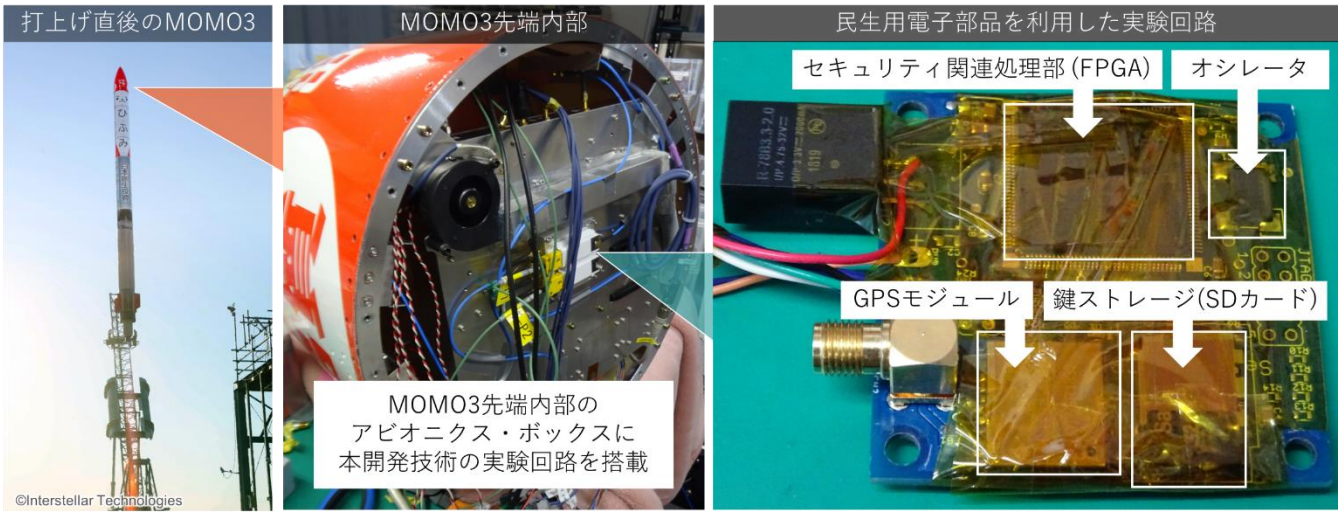

図 5: 今回の飛行環境下の実験に用いた MOMO3 の打上げ及び本開発技術の実験回路

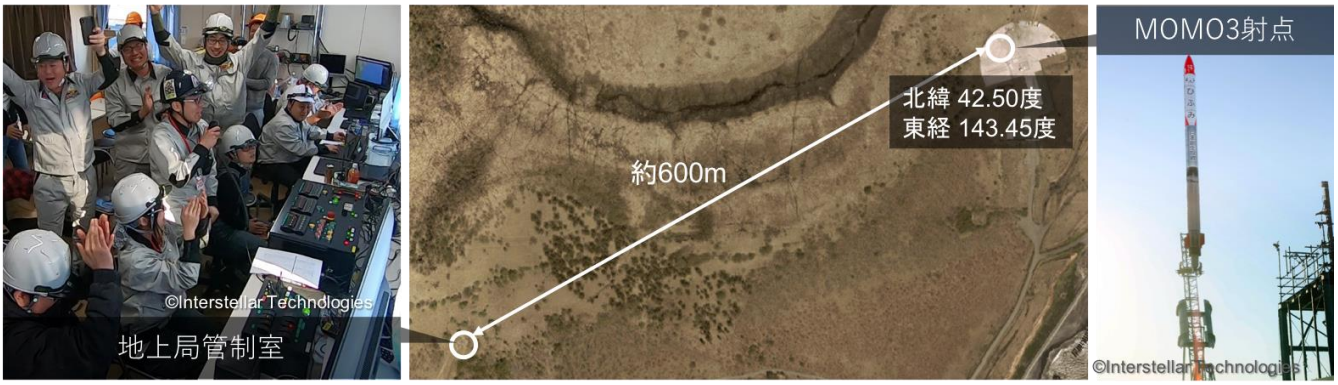

図 6: MOMO3 の射点と地上局の位置
（国土地理院の簡易空中写真（2004 年～撮影）に地上局・射点の位置及び概算距離を追記）

図 7: 打上げ直後の MOMO3 と地上局に設置した PC 画面
（動画: https://youtu.be/UV8lXVtW2nY）

図 8 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。

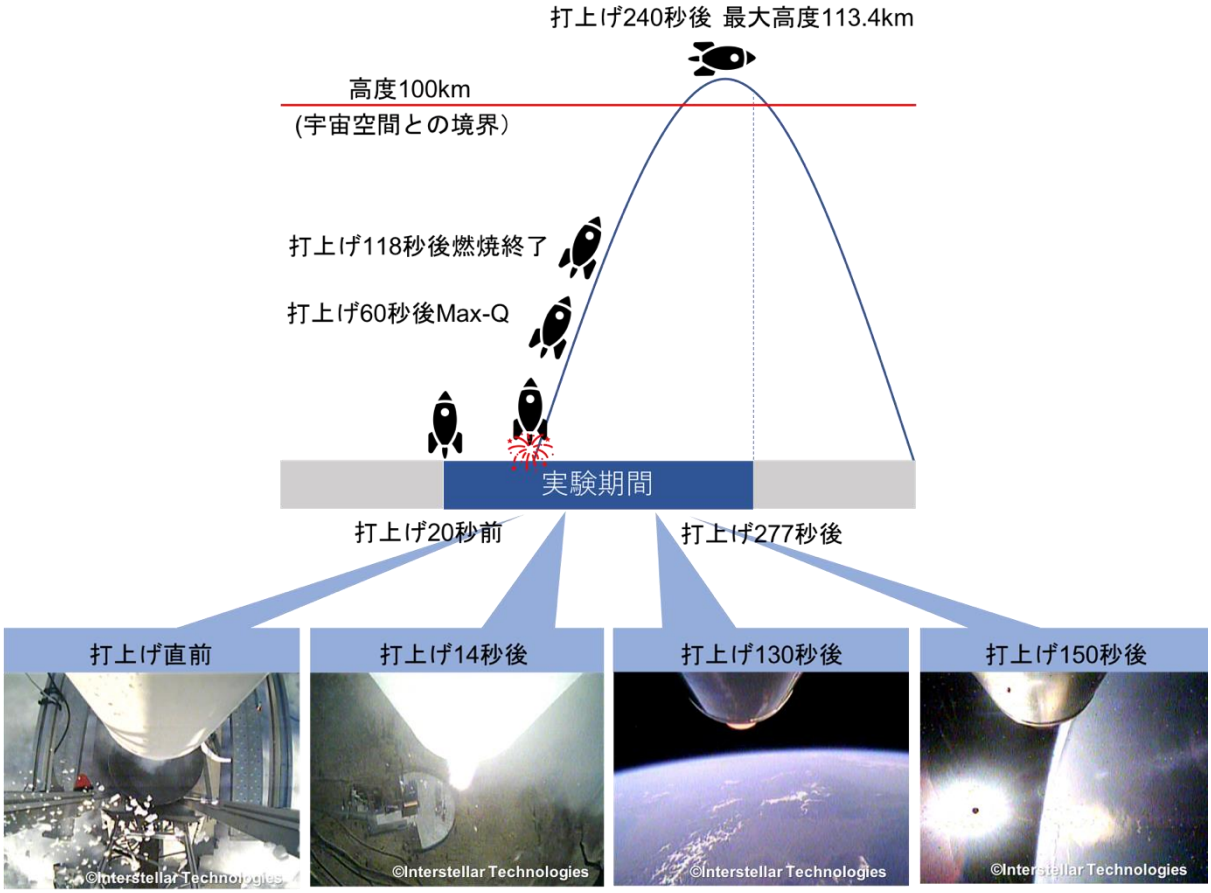

図 8: 実験期間と MOMO3 の位置及び機体からの画像

表 1: 打上げ 20 秒前から全実験終了の 277 秒後までのパケット受信・処理結果
（パケット消失の大部分は主要ミッションが終了した宇宙到達後に起きている）

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	1212
	セキュリティ処理失敗	0
パケット受信失敗（誤り・消失による欠損）		273 (11・262)
総パケット		1485