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。

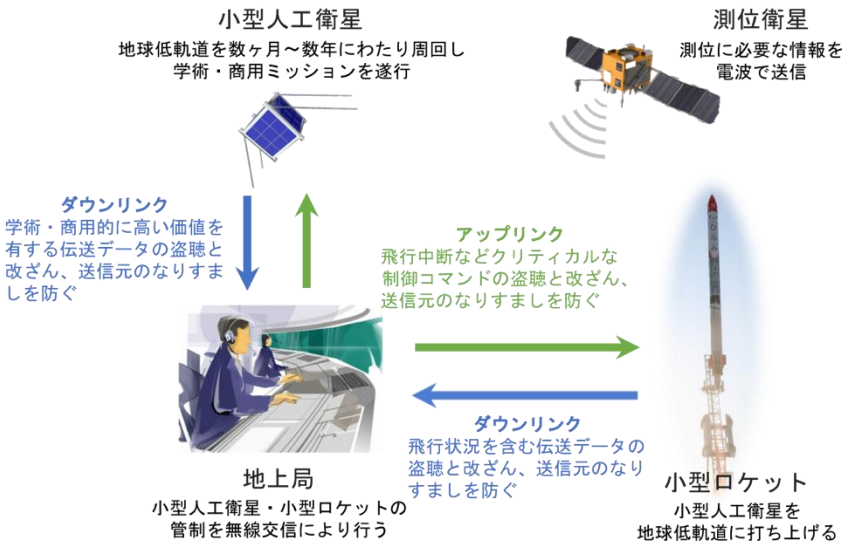

図 3 本開発技術によるアップリンク・ダウンリンクの通信セキュリティ

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。

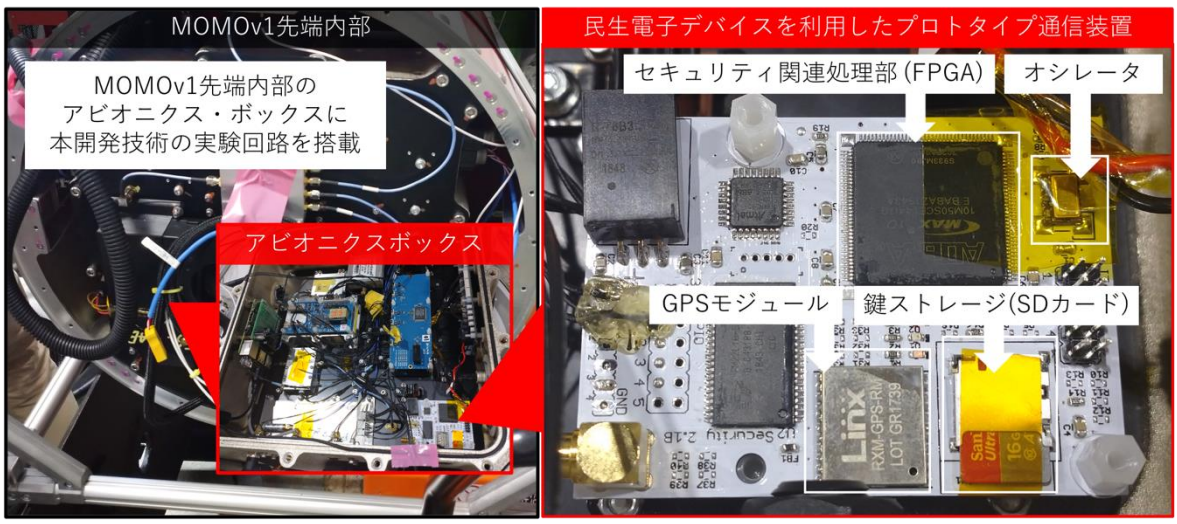

図 4 今回の実験に用いたプロトタイプ実験装置

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。

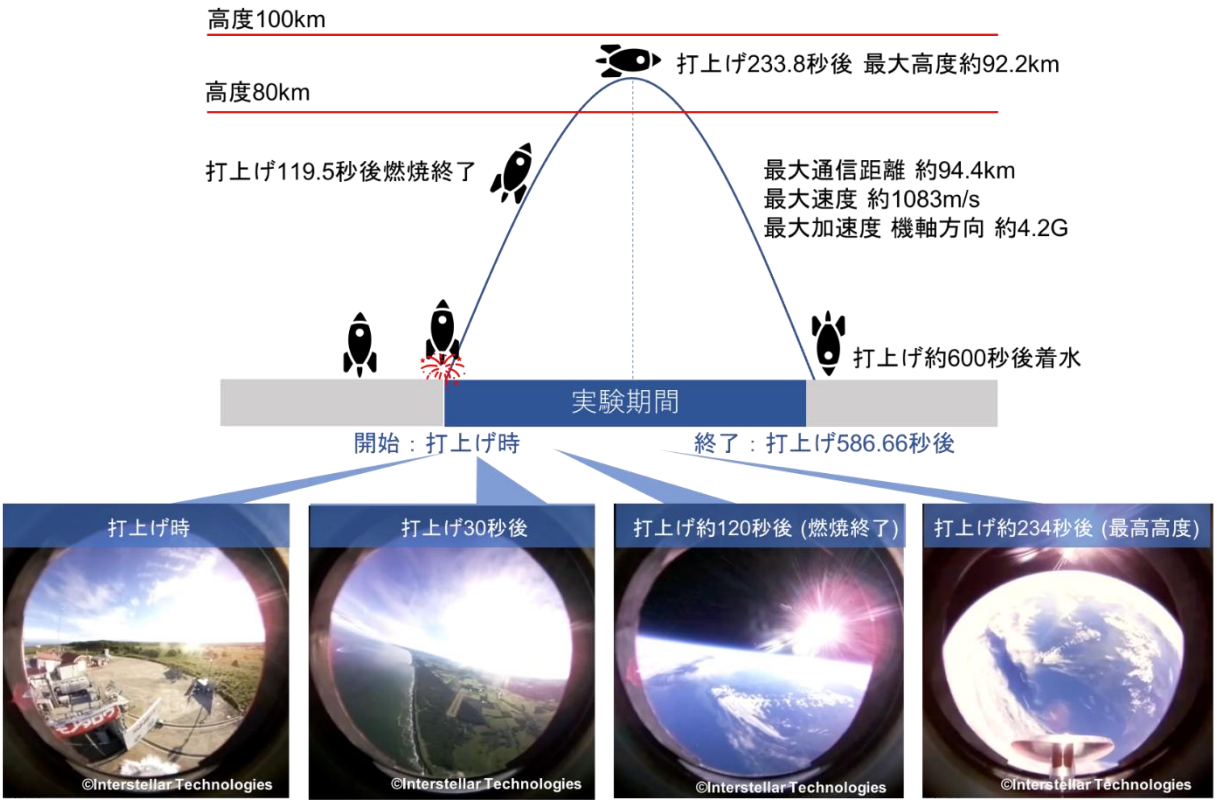

図 5 実験期間と MOMOv1 の位置及び機体からの画像

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