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。

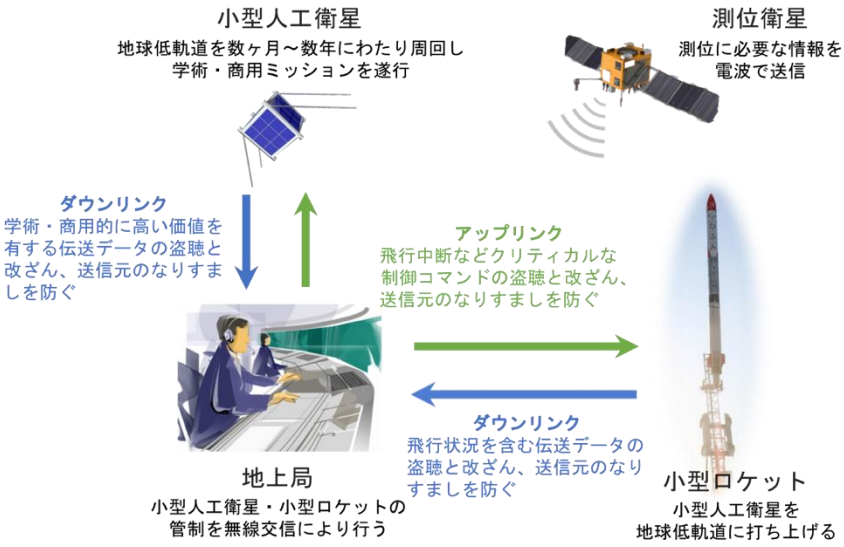

図 3: 本開発技術によるアップリンク・ダウンリンクの通信セキュリティ

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。

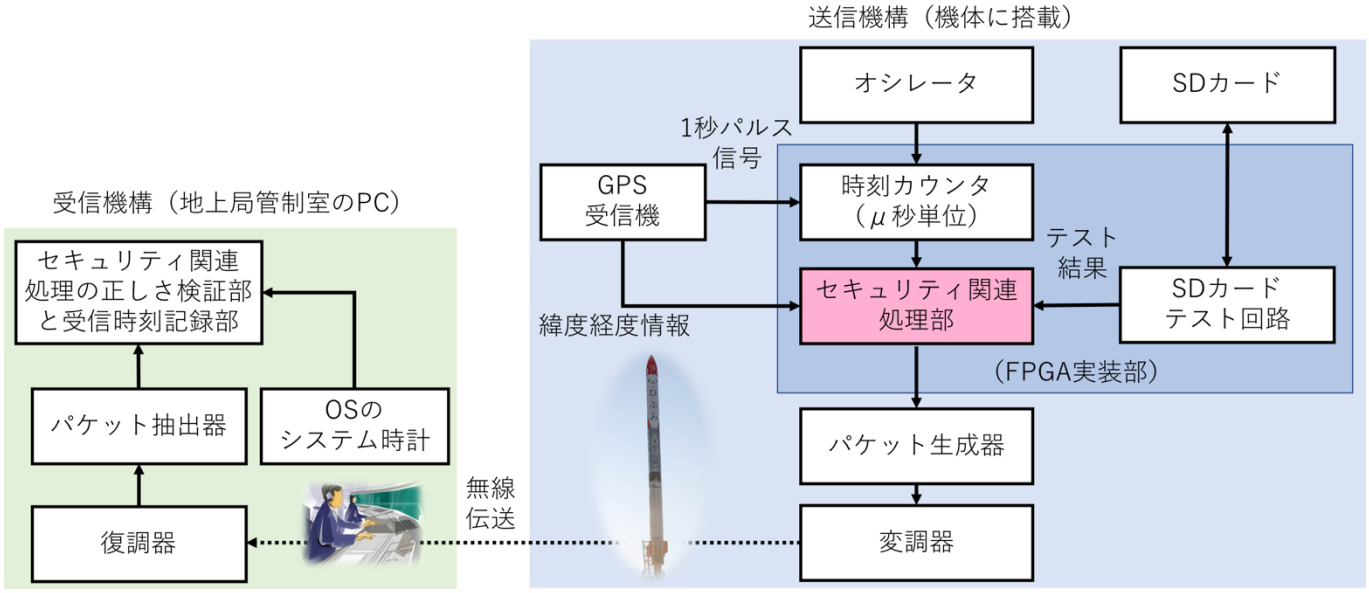

図 4: 実験系における処理構成

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。

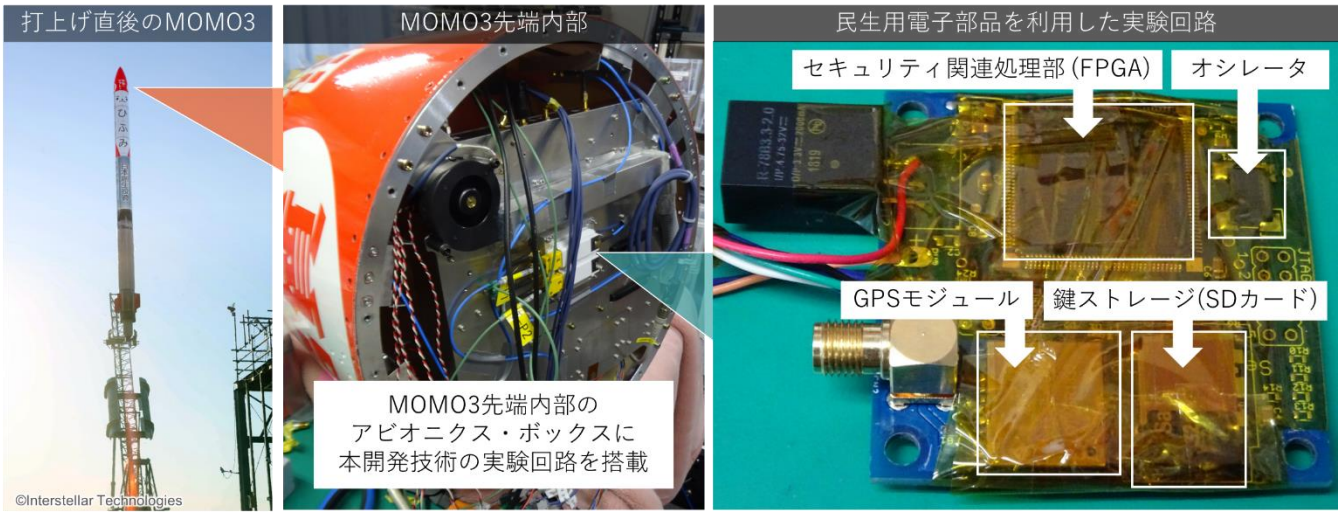

図 5: 今回の飛行環境下の実験に用いた MOMO3 の打上げ及び本開発技術の実験回路

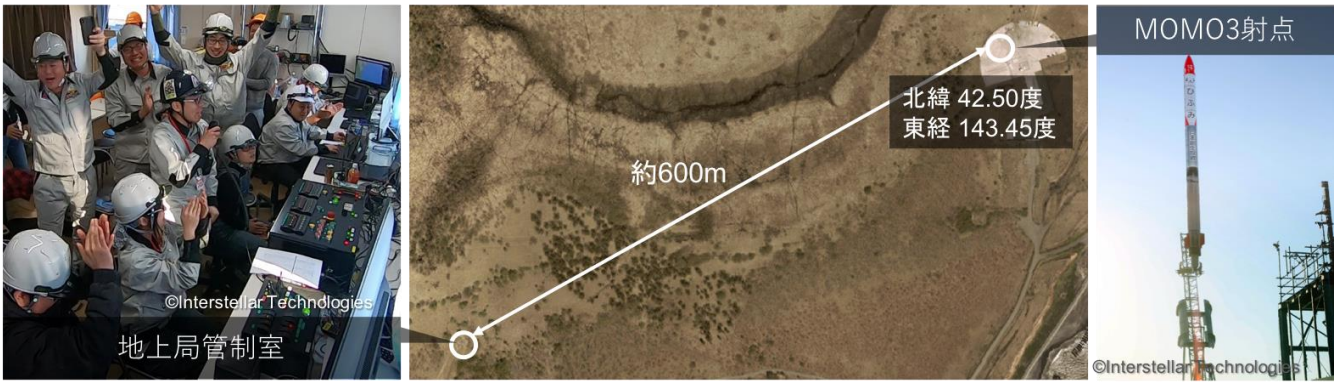

図 6: MOMO3 の射点と地上局の位置
（国土地理院の簡易空中写真（2004 年～撮影）に地上局・射点の位置及び概算距離を追記）

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。

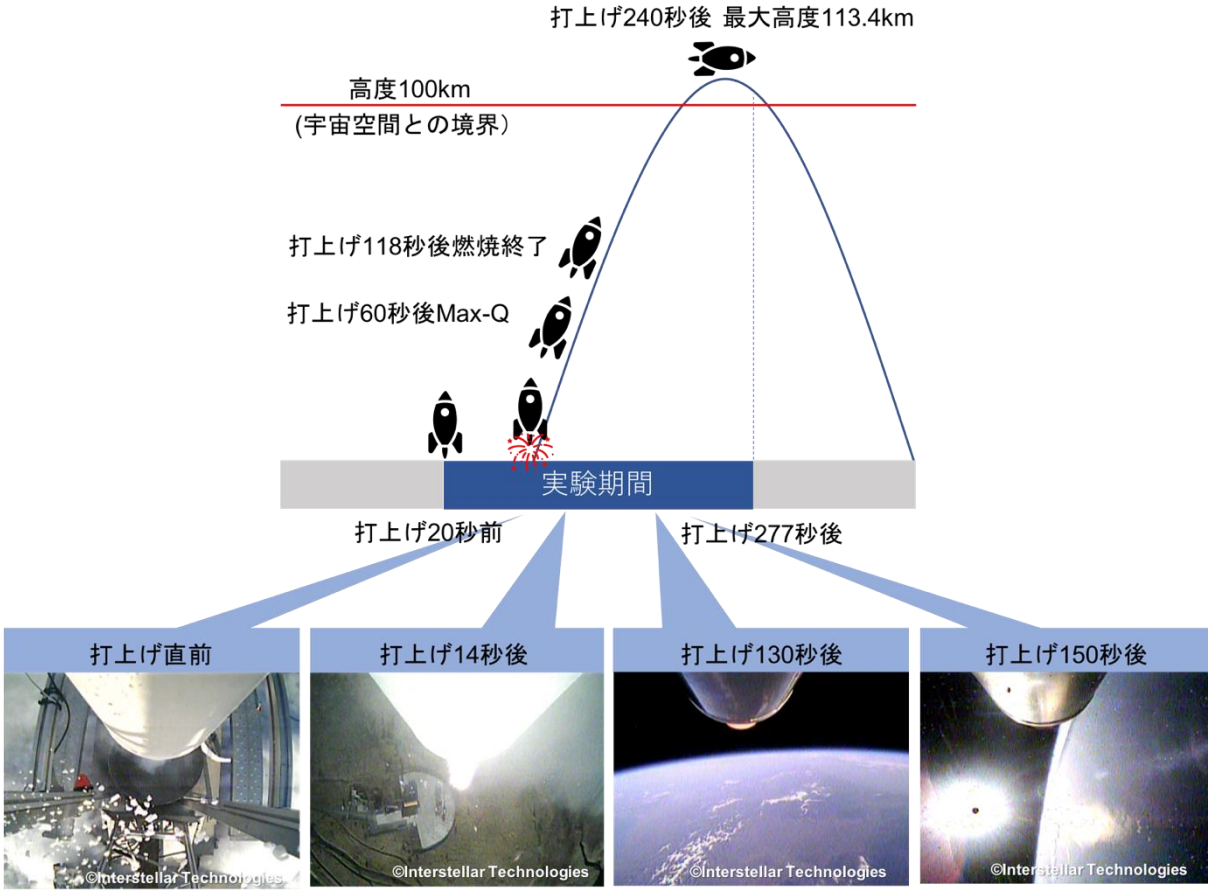

図 8: 実験期間と MOMO3 の位置及び機体からの画像

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