3-2-2　NewSpace における宇宙機無線通信の暗号技術
3-2-2　Cryptography for Wireless Communication with Spacecraft in NewSpace

吉田 真紀
YOSHIDA Maki

宇宙船やロケット、人工衛星の開発、そして有人飛行といった宇宙開発は、NewSpace と呼ばれる民間主導かつ民需目的で自由な開発の時代に入った。セキュリティ基盤研究室は人工衛星や打上げ用ロケットなどの民間宇宙機の乗っ取り防止による飛行の安全確保と伝送データの保護のため、2018 年からインターステラテクノロジズ株式会社と法政大学との共同研究により、高セキュリティと低コストを両立する無線通信のための暗号技術を研究開発している。本稿では、民間宇宙ロケットとの無線通信において理論上最高レベルのセキュリティである情報理論的安全性を民間電子デバイスで低コストに達成する方式設計及び一連の飛行実験の結果を報告する。

The NewSpace has seen numerous rocket launches for academic and commercial purposes, such as developing satellite constellation networks. Since 2018, we have collaborated with Interstellar Technologies Inc. and Hosei University to enhance the safety and security of data transmission for spacecraft, including satellites and launch vehicles. This paper summarizes our research results on secure, cost-effective radio communication systems and the outcomes of performance evaluation flights.

1　まえがき

宇宙船やロケット、人工衛星の開発、そして有人飛行といった宇宙開発は、国家主導かつ公益目的の時代から、民間主導かつ民需目的で自由な開発（NewSpace と呼ばれる）の時代に入った。

2024 年 8 月 8 日時点で、地球軌道上の人工衛星は 13,438 機あり、そのうち 1,239 機が 2024 年に入ってから打ち上げられている [1]。つまり、一日平均 5 機以上が打ち上げられており、その中でも学術・商用目的で打ち上げられている小型衛星が多数を占める。

それに伴い小型衛星の打上げに特化した低コスト民間ロケットの開発が進展している。日本では 2018 年に「人工衛星等の打上げ及び人工衛星の管理に関する法律」[2]、いわゆる宇宙活動法が施行された。宇宙活動法に関する諸ガイドライン [3] には人工衛星の打上げ用ロケットの型式認定や飛行許可にあたって“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を講ずること”が要求として記載されている。

実際、重要なシステム等に関する信号には飛行中断などクリティカルなコマンドが含まれており、公共の安全を脅かさないためにも、第三者による成りすましや改ざんを受けてはならない。それ以外の信号についても、学術･商業的に高い価値を有する通信データが盗聴されることは好ましくない。また、商業利用では暗号化装置のコストについても意識する必要がある。

セキュリティ基盤研究室では 2018 年からインターステラテクノロジズ株式会社と法政大学との共同研究を実施し、NewSpace において小型衛星や打上げ用ロケットなどの宇宙機の乗っ取り防止による飛行の安全確保と伝送データの保護のため、高セキュリティと低コストを両立する通信セキュリティ技術の研究開発に取り組んでいる。

以降では、**2** で NewSpace の通信セキュリティへの貢献に向けた本研究の目標を述べ、2018 年からどのように段階を踏んで研究を実施しているかを概説する。そして **3** と **4** で前中長期（2018 年度から 2020 年度）と今中長期（2021 年度以降）で得られた成果を紹介し、最後に **5** のむすびで将来の展望を述べる。

2　NewSpace の通信セキュリティへの貢献に向けて

本研究では、公共の安全のために可能な限り高いセキュリティレベルを達成し、商業利用のために装置コストを可能な限り下げることを目標とした。そして

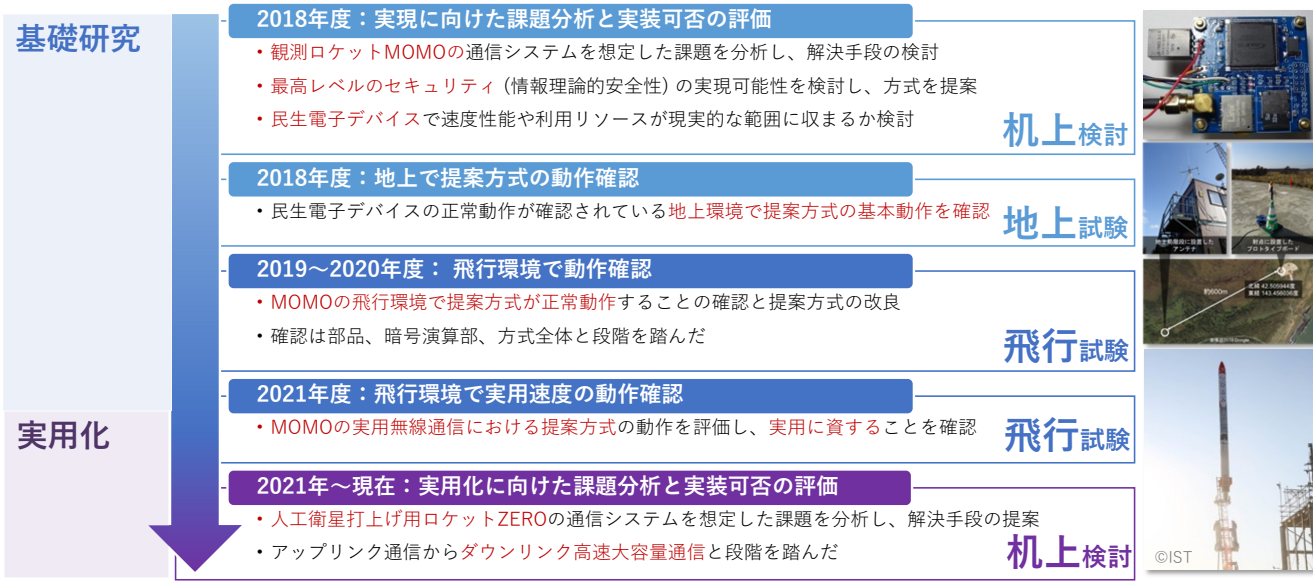

図 1　NewSpace の通信セキュリティへの貢献に向けた研究の流れ

図 1 に示すように、第 4 期中長期（2018 年度から 2020 年度）は基礎研究を実施し、第 5 期中長期（2021 年度から）は実用化研究に取り組んでいる。

基礎研究では、理論上最高レベルのセキュリティである情報理論的安全性[*1]が低価格民生電子デバイスで達成可能であることを見いだし [4]、具体的な方式を提案し安全性を証明した [5]。そして、民生電子デバイスを用いたプロトタイプ通信装置を実装し、観測ロケット MOMO [6] 上で飛行実験を 4 回重ね（3 ～ 6 号機）、情報理論的に安全な提案方式が実用に資することを確認した [7]–[11]。さらに、提案方式では装置コスト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利用可能としている。

実用化研究では、提案方式を小型衛星打上げ用ロケット ZERO [6] で実用化することを目指し、不安定な無線環境による通信パケットの欠落や遅延、宇宙線等による半導体処理装置の一時的故障や瞬停などによる影響（宇宙ロケットとの通信の永続的な喪失、すなわちミッションの失敗）の最小化に取り組んでいる。これまでに、通信パケットの欠落や遅延、半導体処理装置の誤動作から正常動作に自動的に回復するように頑強化した [12]–[15]。そして、プロトタイプ通信装置を実装し、想定する高速大容量通信に十分な通信速度を達成できることを確認した [10][15][16]。

3　第 4 期中長期の基礎研究の成果概要

本章では、図 1 の研究の流れにおける第 4 期中長期（2018 年度から 2020 年度）の基礎研究で得た成果を説明する。

3.1　実現に向けた課題分析と実装可否の評価（2018 年度 [4][5]）

まず、対象となる無線通信システムの課題を分析した。対象システムにおける通信は地上局、宇宙ロケット、人工衛星、全地球航法衛星システム（Global Navigation Satellite System, GNSS）の測位衛星との間で行われる。主な通信は、地上局と宇宙ロケット・人工衛星（宇宙機）との間で行われ、求められるセキュリティの要件は機密性、完全性、可用性である。機密性と完全性は伝送データの保護と乗っ取り防止を意味し、本研究の研究対象である。一方、可用性は再送などの既知手法で対応する。測位衛星から発せられる情報を地上局と宇宙機は利用するが受信のみであり、セキュリティ要件は設けない。

通信の機密性・完全性は非宇宙用通信（代表例としてインターネットと無線 LAN）でも考えられているが、本研究では宇宙用通信で固有の課題があること、非宇宙用通信における基本対策が適用できないことを指摘し、新たな通信方式を提案した。

固有の課題：まず、飛行中の機体に人が直接アクセスすることがほぼできないため（“非修理系”）、新たな攻撃が発見されても事実上改修できない。次に、暗号演算の処理時間増大は状況変化への対応遅れに直結するため、リアルタイム性への強い要求がある。そして、宇宙空間に到達する飛行は最も条件が厳しく、かつ最も通信の確実性が求められる。これらの課題を解決す

*1　インターネット等で広く用いられている共通鍵暗号や公開鍵暗号は、攻撃側が有する計算能力は有限であり攻撃に要する計算量が膨大になるという計算量的安全性に基づいているが、情報理論的に安全な暗号には攻撃側が無制限の計算リソースを有するとしても解読できないという特長がある。

るためには以下の要件を満たすことが重要である。

高セキュリティ：多様な攻撃に対して高いセキュリティ

軽量な設計：簡単な暗号演算から成り、高い計算効率とスループット、小さな回路規模

高信頼な実装：演算回路・ストレージなどの信頼性を踏まえたシステムとしての信頼性

非宇宙用通信における基本対策の適用不能性：インターネットと無線 LAN では、高セキュリティ・低コストを両立するため、

基本対策 1：送信者と受信者で互いの情報を対話して確認

基本対策 2：公開された情報（Bulletin board/common reference string/PKI）を利用

が適用されている。しかし、インタラクションが必要な基本対策 1 は、不安定な通信による予想外の遅延やパケットロスでデッドロックに陥り管制を喪失するため適用できない。また、地上局と宇宙機との通信周波数は一般に機密情報であり、無線処理系は局外との通信系とは分離されるため、基本対策 2 も適用できない。

提案した通信方式のポイント：不安定な通信状況でもデッドロックを防止するために非インタラクティブな一方向の通信とし、その上で十分安全性が検討された秘匿・認証の技法を選定・利用した。理論上最高レベルのセキュリティである情報理論的に安全なワンタイムパッドと A-code、それらの組み合わせに Encrypt-then-MAC と呼ばれる手法を採用した*2。そして小型宇宙機で現在使用されている民生電子デバイスと同水準の実験プラットフォームで速度を評価し、軽量であることを確認した。特に、非宇宙系通信で通常用いる汎用用途暗号（AES 等）よりも演算速度が高く、数十 Gbps の性能を達成した [4]。

なお、情報理論的に安全な方式では送信データごとに異なる鍵を利用する。想定通信システムの分析結果（図 2）より、必要な鍵ストレージは宇宙ロケットで数百 M バイト、小型衛星で数百 G～数百 T バイトと試算された。このサイズであれば、現在入手可能な民生フラッシュメモリ（例えば SD カード）や SSD（ソリッド・ステート・ドライブ）で十分保存できる。

以上より、高セキュリティと軽量な設計の要件を満たすことができた。

3.2　地上・飛行環境での動作確認（2018～2021 年度 [6][7]–[11]）

提案方式が実際の飛行において正常に機能することを、民生電子デバイスの正常動作がメーカ等により保証されている地上環境と、必ずしも保証されていない飛行環境で段階的に実証した。地上環境における基本動作実験と結果については文献 [6] を参照されたい。飛行実験（4 回実施）の目的は、提案方式を介してすべてのデータが正しく伝送され、飛行環境下で装置に重大な問題が発生しないことを確認することであり、表 1 に示すように試験目的は完全に達成された。

*2　一般に、宇宙通信では無通信時のランダムノイズが大きく、受信した信号の変動がノイズによるものか通信データによるものかの識別が困難である。それに対して、提案方式では認証技法を本来の用途（通信内容と通信相手の認証）のみならず通信路から通信データを特定するためにも利用しており、これも方式の特徴である。

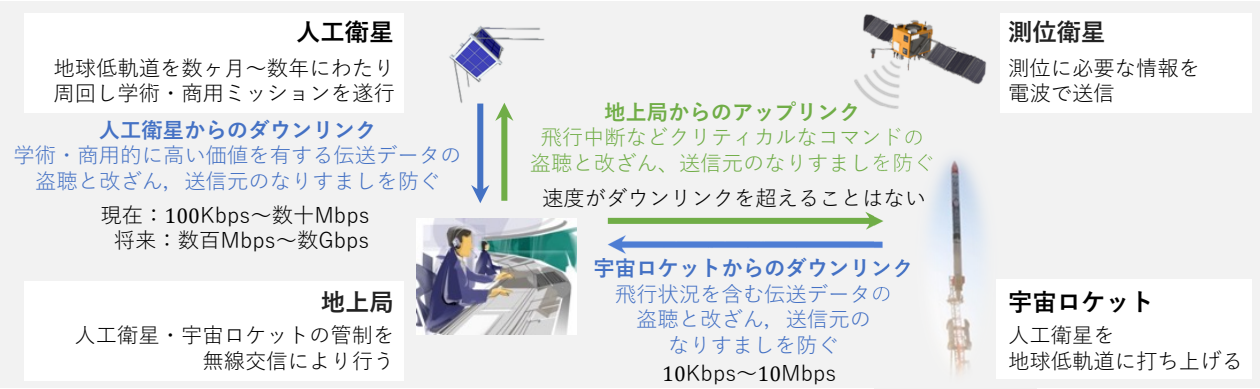

図 2　対象システムの分析

表 1　飛行試験の概要と動作確認の結果

MOMO（打上げ日）	フライト成否（到達高度）	正常受信した総パケット数	実効帯域	確認項目	動作確認成否
3 号機（2019 年 5 月 4 日）	フルサクセス	1212	8 kbps	部品	フルサクセス
4 号機（2019 年 7 月 27 日）	失敗（10 km）	6878	50.1 kbps	暗号演算部	フルサクセス
5 号機（2020 年 6 月 14 日）	失敗（10 km）	13239	77 kbps	方式全体	フルサクセス
6 号機（2021 年 7 月 31 日）	フルサクセス	558313	512 kbps	実用速度＋方式全体	フルサクセス

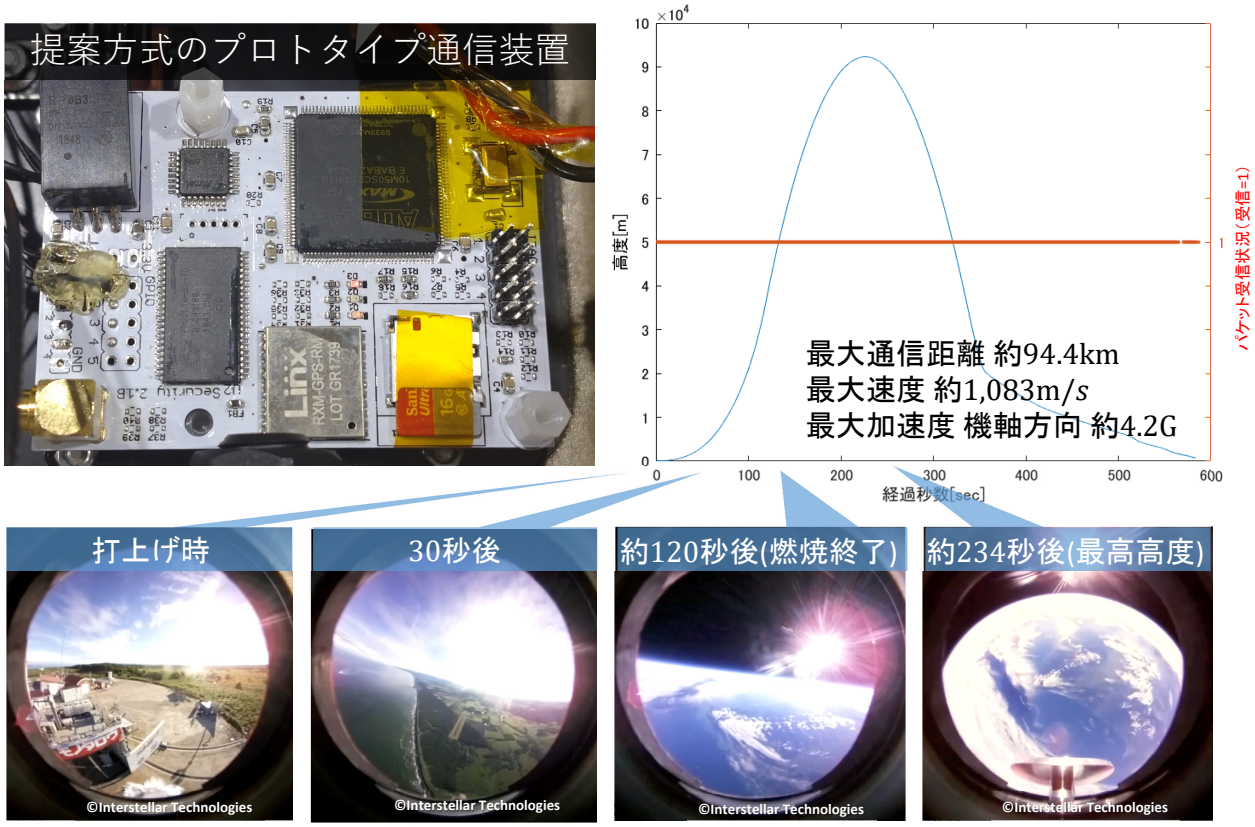

図 3　MOMO6 号機に搭載したプロトタイプ通信装置と飛行試験（2021 年 7 月 31 日）

2021 年 7 月 31 日には実効速度 512 kbps でのダウンリンク伝送に成功している（図 3）。これにより、高信頼な実装の要件を満たすことを確認できた。

4　第 5 期中長期の実用化研究の成果概要

本章では、図 1 の研究の流れにおける第 5 期中長期（2021 年度以降）の実用化研究で得た成果を説明する。

4.1　実用化に向けた課題分析と実装可否の評価（2021 年度 [12][13]）

前中長期に提案した通信方式では、一般的な情報理論的に安全な方式と同様に、送信側と受信側が事前に大量の鍵を共有し、各鍵を一度限り使っていくため、両者が同時に同じ鍵を使うこと（鍵同期）を保証する必要がある。観測ロケット MOMO 上の飛行試験でトラブルは発生しなかったが、人工衛星打上げ用ロケット ZERO での実利用には細心の注意が必要である。飛行中の宇宙機にアクセスする手段は事実上通信系のみであるため、通信系が利用できなくなれば宇宙機全体の損失になる。宇宙機の維持は最も優先度が高く、通信セキュリティのために通信系が利用不能になることは本末転倒である。

本研究では宇宙用通信の鍵同期で固有の課題があること、非宇宙用通信（代表例としてインターネットと無線 LAN）における基本対策が適用できないことを指摘し、新たな鍵同期機構を提案した。

固有の課題：宇宙無線通信では不安定な無線環境による通信パケットの欠落・遅延、宇宙線による半導体処理装置の一時的故障・瞬停等による誤動作のリスクが高いため、このような誤動作の影響を最小化できる高信頼な鍵同期機構の実現が課題となる。

非宇宙用通信システムの基本対策の適用不能性：インターネットの TLS1.3 と無線 LAN の WPA3 では鍵同期の保証のため、

基本対策 1：制御情報として次に使う鍵の指示値（アドレス等）を保持して更新、

基本対策 2：両者で使う鍵の指示値が同じことを対話して相互確認、

が適用されている。しかし、制御情報の保持が必要な基本対策 1 は、宇宙線による値の破損や瞬停による初期化で鍵の同期ずれを引き起こし、恒久的な通信不能になるため適用できない。また、インタラクションが必要な基本対策 2 は、通信が不安定な状況で予想外の遅延やパケットロスでデッドロックに陥り、管制を喪失するため適用できない。

提案した鍵同期機構のポイント：致命的な通信不能・管制喪失の可能性を解消するため、リスク源である制御情報の保持とインタラクティブな通信を不要とし送信時・受信時に衛星を利用した測位である GNSS 時刻

を利用して鍵同期を実現した。そして、通信パケットの欠落・遅延や半導体処理装置の一時的故障・瞬停が発生しても、その影響が該当パケットの棄却のみに限定され、次の通信パケットからは正常に動作すること（通信系回復）を暗号学的に証明した。GNSS 時刻を利用した鍵同期の骨子は図 4 のとおりである。まず、送信側は通信パケットに送信時刻T_sを打刻し、受信側は受信時刻T_rを取得する。ここで、処理遅延・通信遅延の上限δ_{max}と下限δ_{min}は推定しておくとし、受信側は受信時刻が遅延測定の誤差内に収まっていれば（すなわち、$T_s + \delta_{min} \leq T_r \leq T_s + \delta_{max}$が成り立てば）、正当な通信パケットと判定する。そして、この判定を機能させるために、送信側は遅延の変動量$\delta_{max} - \delta_{min}$以上の時間をかけて通信パケットを送出する。これによって、送信側の正当な通信パケットが受信されれば正当と判定される。もし第三者が送出期間中に何らかの信号を意図的に送出すれば、正当な通信パケットの信号が壊れるため受信側の認証機能によって棄却され、正当な通信パケットの送出期間を避けて何らかの信号を送出しても受信側で期間外になるため棄却される。

4.2　実効速度の評価（2022～2023 年度 [14][15]）

提案した鍵同期機構では、通信パケットの送出可能間隔が遅延の変動量$\delta_{max} - \delta_{min}$であり、これにより実効速度の上限が定まる（遅延の大小ではないことに注意）。

遅延測定の誤差量を飛行前に静的に推定する場合、通信パケットの送出可能周期の上限が約 100 Hz になる [14]。これは、宇宙機と地上局の間の通信遅延がほぼ 0 から 10 ミリ秒程度（距離換算で約 3,000 km）まで広範囲に変動するためである。結果として、通信パケットの実効ビットレートは 100 kbps であり、地上局から宇宙機へのアップリンク通信における飛行制御用コマンドなどの通信には十分である。さらに、遅延の値を飛行中に動的に推定することで実効速度を改善した [15]。具体的には、時刻のみならず測位情報（経度・緯度・高度の三つ組から成る位置情報）を GNSS から取得して、通信遅延を動的に測定する。現在の GNSS における測位情報の更新頻度は 0.1 ～ 10 Hz と低いが、高速（秒速約 7.8 km）に飛行する宇宙機であっても位置を数十 km 以下の誤差で測定できる。これにより通信遅延を 100 マイクロ秒未満の精度で推定できるため、通信パケット送出間隔、ひいては実効ビットレートを 2 ～ 3 桁向上した数十 Mbps を達成可能であるとの見通しを得た。これは、宇宙機から地上局へのダウンリンク通信における観測データなどの通信には十分である。なお、他の処理（暗号演算と鍵アクセス）が 10.2 Mbps と十分な速度をもつことは図 5 のプロトタイプ通信装置で実証済みである [10]。

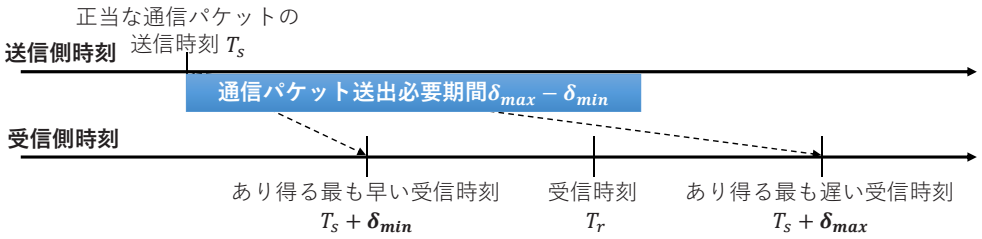

図 4　送信時・受信時の GNSS 時刻を利用した鍵同期の概要

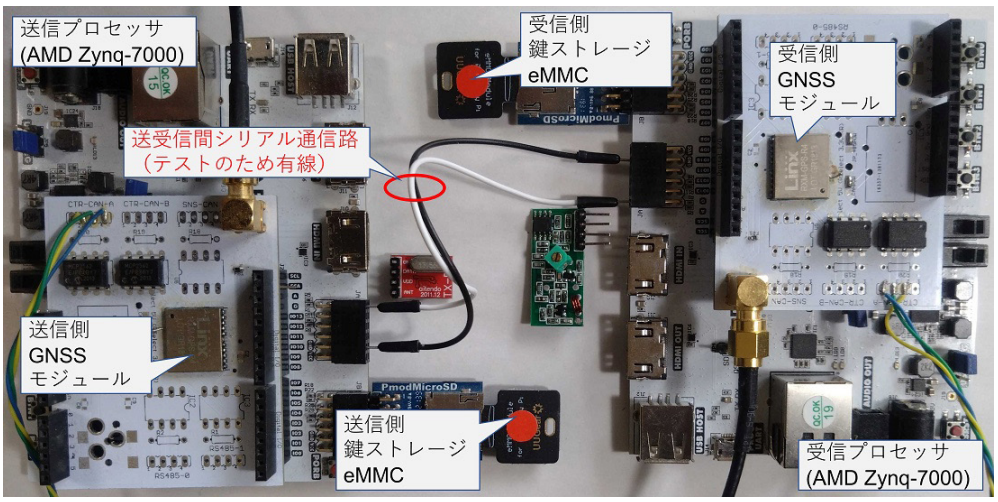

図 5　プロトタイプ通信装置による実効速度評価

5　むすび

宇宙機と地上局との無線通信において、高セキュリティと低コスト、そして高速大容量化の全てを達成する技術の実現可能性を見いだしており、今後は改良と検証を繰り返しながら実用化を進める。

謝辞

本稿の執筆に際してインターステラテクノロジズ株式会社の森岡澄夫シニアフェロー、法政大学の尾花賢教授より有益なコメントをいただいたことに深謝する。

【参考文献】

1　UNOOSA：“Online Index of Objects Launched into Outer Space,” https://www.unoosa.org/oosa/osoindex/search-ng.jspx (参照 2024-08-08).
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（平成二十八年法律第七十六号), https://elaws.e-gov.go.jp/document?lawid=428AC0000000076 (参照 2024-08-08)
3　内閣府宇宙開発戦略推進事務局, 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（改訂第２版), https://www8.cao.go.jp/space/application/space_activity/documents/guideline2.pdf
4　森岡, 尾花, 吉田,“超小型衛星・小型ロケット用セキュア通信のための情報理論的安全性の検討,”第 62 回宇宙科学技術連合講演会, 1 K19, 2018.
5　尾花, 吉田, 森岡,“小型衛星・小型ロケット用通信のセキュリティモデルとプロトタイプ実装,”情報処理学会研究報告, vol.2019-CSEC-84, no.3, 2019.
6　インターステラテクノロジズ株式会社, https://www.istellartech.com (参照 2024-08-08).
7　吉田, 森岡, 尾花,“観測ロケット MOMO3 号機による小型衛星・小型ロケット用セキュア通信方式の基礎実験,”情報処理学会研究報告, vol.2019-CSEC-86, no.10, 2019.
8　森岡, 尾花, 吉田,“情報理論的安全性を有する小型衛星・小型ロケット用セキュア通信方式の基礎実験,”第 63 回宇宙科学技術連合講演会, 3 S08, 2019.
9　森岡, 尾花, 吉田,“小型衛星・小型ロケット用セキュア通信方式の鍵管理における装置故障対策,”第 64 回宇宙科学技術連合講演会, 4 I03, 2020.
10　S. Morioka, S. Obana, and M. Yoshida, “Flight Demonstration Results of Information Theoretically Secure Wireless Communication on a Sounding Rocket MOMO,” 33rd International Symposium on Space Technology and Science (ISTS 2022).
11　森岡, 尾花, 吉田,“情報理論的安全性を有する宇宙ロケット用セキュア通信方式の性能実証飛行,” 2022 年暗号と情報セキュリティシンポジウム (SCIS 2022).
12　森岡, 尾花, 吉田,“小型宇宙機用セキュア通信における GNSS 時刻情報を用いた鍵同期方式,”第 66 回宇宙科学技術連合講演会, 2 M12, 2022.
13　M. Yoshida, S. Morioka, and S. Obana, “Secure Communication via GNSS-based Key Synchronization,” Work-in-Progress in Hardware and Software for Location Computation (WIPHAL 2023).
14　S. Morioka, S. Obana, and M. Yoshida, “A Highly Reliable Key Synchronization Framework in Information Theoretically Secure Wireless Communication for Small Spacecrafts,” 35th International Symposium on Space Technology and Science (ISTS 2023).
15　森岡, 尾花, 吉田,“宇宙ロケット用セキュア通信のための GNSS 測位情報を用いた鍵同期方式,” 2024 年暗号と情報セキュリティシンポジウム (SCIS 2024).
16　森岡, 尾花, 吉田,“GNSS 時刻情報を用いたセキュア通信用鍵同期機構における鍵キャッシュ設計,”第 67 回宇宙科学技術連合講演会, 1 R07, 2023.

吉田 真紀（よしだ まき）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、情報理論、NewSpace セキュリティ
【受賞歴】
2022 年　情報処理学会 IPSJ-ONE2022
2011 年　電子情報通信学会第 67 回（平成 22 年度）論文賞
2009 年　情報理論とその応用学会 2008 年 SITA 奨励賞