国立研究開発法人
情報通信研究機構

プレスリリース
2026 年 3 月 23 日

国立研究開発法人情報通信研究機構

宇宙放射線に耐える暗号回路の網羅的な動作保証を実現

～民間宇宙開発で高信頼性と低コストを両立する新理論、NASA 国際会議で優秀賞～

【ポイント】

- 宇宙放射線への耐性を上げ、部品点数を抑えた暗号回路の設計と検証を統合する新理論基盤を確立
- 放射線対策等で複雑化した回路でも、入力できる全ての値に対する正しい動作を世界で初めて数学的に保証
- 機器の信頼性向上とコスト削減に直結する本成果は NASA 主催の国際会議 NFM2025 で優秀賞を受賞

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は、宇宙通信の安全性を支える暗号回路について、設計と検証を統合する新たな理論基盤を確立しました。

宇宙機に搭載する暗号回路の設計では、宇宙放射線による誤動作を防止するために放射線耐性を上げ、宇宙機の電力やコストの制限に合わせて部品点数を減らす工夫が求められます。しかし、このような工夫を凝らすほど回路構造は複雑化し、入力できる全ての値（全入力）に対する網羅的な動作保証が困難になるという課題がありました。本理論基盤の適用により、放射線耐性を備え、部品点数を抑えた暗号回路を設計し、全入力２の 256 乗通り[*1]（約 10 の 77 乗通り）に対する正しい動作を世界で初めて数学的に保証しました。動作保証に要した時間は一般的な計算機で約 17 時間です。これにより、機器の信頼性向上と電力とコストの削減が可能になり、NewSpace[*2]と呼ばれる民間主導の宇宙開発の進展に貢献します。

なお、本成果は、NASA 主催の国際会議「NASA Formal Methods[*3] 2025」において Honorable Mention（優秀賞）を受賞しました。

【背景】

人工衛星が学術・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[*4] 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、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が求められています。

図１ 宇宙通信の安全性を支える研究開発

NICT ではこれまでに、宇宙通信の安全性を支える技術として、宇宙機の乗っ取りを防ぎ、伝送データを保護する暗号通信方式を研究開発してきました（図１参照）。宇宙通信では高速・大容量化も求められることから、暗号処理をハードウェアで実装することが重要となります。ハードウェア実装では、宇宙放射線による誤動作を防止するために放射線耐性を上げ、消費電力・デバイスコスト削減のために必要部品点数を抑える設計上の工夫が必要となり、回路構造は複雑化します。同時に、設計された暗号回路は、全入力に対して正しく動作することが求められますが、高いセキュリティ強度では、全入力は 2 の 256 乗通り（約 10 の 77 乗通り）に及び、個別に検証することは現実的ではありません。

【今回の成果】

本研究開発では、暗号回路について設計と検証を統合する新たな理論基盤を確立しました。本理論基盤では、回

路の設計と検証を分離せず、設計における工夫そのものを検証に活用できるようにつなぎ、全入力に対する動作の正しさを数学的な性質として形式検証[*5]することで、その正しさを理論的に保証しました。本理論基盤の適用により、世界で初めて、高いセキュリティ強度のもとで、放射線耐性を備え、国際標準で広く用いられる構成と比べて回路規模を約70%に抑えつつ、全入力2の256 乗通りの動作保証を実現しました。この網羅的な動作保証の形式検証は、一般的な計算機（単一 CPU コア）を用いて約 17 時間で完了しました。

図 2 暗号回路の設計と検証を統合する理論基盤

本成果は、民間宇宙機が担う通信サービスや地球観測、災害監視などの社会基盤サービスにおいて、省電力・低コストの機器でも誤動作や乗っ取りのリスクを抑え、その信頼性向上に貢献します。

なお、本成果は、NASA（アメリカ航空宇宙局）が主催する国際会議 NASA Formal Methods 2025（NFM2025）において、Honorable Mention（優秀賞）として表彰されました。NFM は、宇宙、航空、ロボット工学及びその他の NASA 関連のクリティカルシステムなど、わずかなバグや誤動作が重大な事故やミッション失敗につながる可能性のあるシステムの信頼性を数学的手法で保証する形式手法分野の歴史ある国際会議です。この分野は、宇宙開発をはじめ失敗が許されないシステムの安全性を支える基盤技術として重要視されており、本会議での受賞はその技術的意義が国際的に評価されたことを示しています。

【今後の展望】

本研究で確立した理論基盤は、宇宙が社会インフラとして広く利用される時代において、安全性と信頼性を数学的に保証する基盤技術として、宇宙通信サービスの安定運用に寄与します。また、宇宙分野に限らず、安全性と信頼性が極めて重要となる分野への応用も期待できます。今後も、数学的保証に基づくセキュリティ技術の確立に向けて、更なる研究開発を推進します。

＜論文情報＞

著者: Morioka,S., Obana,S., Yoshida,M.
論文名: Formal Verification of Composite Field Multipliers for Information-Theoretically Secure Radio Communication in Spacecraft Control
掲載誌: NASA Formal Methods (NFM 2025), Lecture Notes in Computer Science, Vol.15682, pp.236-253. Springer, 2025.
DOI: 10.1007/978-3-031-93706-4_14
URL: https://doi.org/10.1007/978-3-031-93706-4_14

＜関連する過去のプレスリリース＞

・2021 年 8 月 17 日 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
https://www.nict.go.jp/press/2021/08/17-1.html
・2019 年 7 月 10 日 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

＜ 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

＜ 広報 （取材受付）＞
広報部 報道室
E-mail: publicity@nict.go.jp

＜用語解説＞

*1 全入力 2 の 256 乗通り

暗号回路には 0 又は 1 の値をとる入力を複数個与える。例えば入力が 4 個ある場合、それぞれの入力は 0 又は 1 の 2 通りの値をとるため、入力できる全ての値（全入力）の総数は 2 の 4 乗通りとなる。同様に、入力が 8 個ある場合、全入力は 2 の 8 乗通りとなる。一般に、入力が n 個ある場合、全入力は 2 の n 乗通りとなる。セキュリティ強度を高くするほど、全入力の数は増える。本研究で設計した暗号回路は高いセキュリティ強度を実現するため、入力は 256 個であり、全入力が 2 の 256 乗通りとなる。2 の 256 乗通り（約 10 の 77 乗通り）は、観測可能な宇宙に存在するとされる原子の数に匹敵する非常に大きな数である。

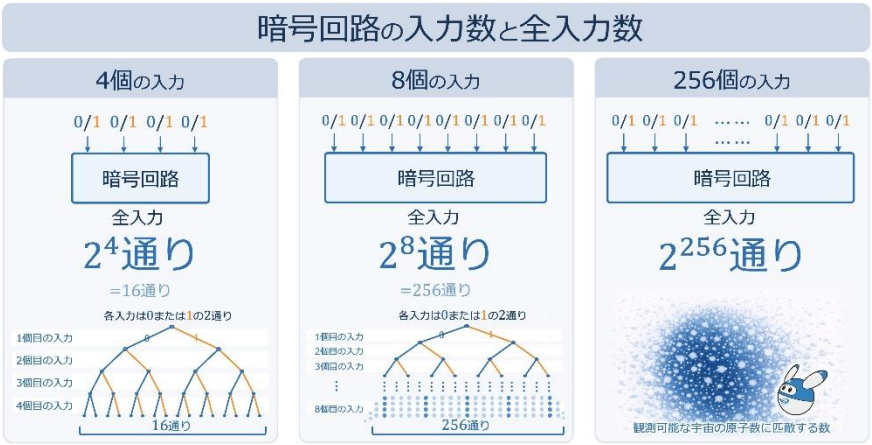

図 3 暗号回路の入力数と全入力数の関係
入力数が増えると全入力数が指数関数的に増加する。

*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 NASA Formal Methods

アメリカ航空宇宙局（NASA）が主催する、システムの信頼性を数学的に保証する形式手法（Formal Methods）分野の歴史ある国際会議である。NASA、他の政府機関、学界、産業界の研究者と技術者が参加し、理論と実務の連携を促進する場となっている。宇宙、航空、ロボット工学及びその他の NASA 関連のクリティカルシステムなど、わずかなバグや誤動作が人命に関わる大事故やミッションの失敗といった甚大な損失に直結するシステムの信頼性保証に関する課題を特定し、解決策を提示することを目的としている。

*4 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。

*5 形式検証（Formal Verification）

ハードウェアやソフトウェアが設計通りに正しく動作するかを、テスト実行だけに頼らず、数学的な理論に基づいて検証する技術であり、形式手法（Formal Methods）と呼ばれる研究分野の代表的な技術である。通常のテストではすべての入力に対する動作を確認することは困難だが、形式検証では数学的な性質を用いて動作の正しさを厳密に保証できる。本成果のように、2 の 256 乗通り（約 10 の 77 乗通り）の入力をもつ暗号回路の動作保証において重要な技術である。