情報理論的暗号を実際に使うとは
宇宙ロケットとの無線通信

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
主任研究員　吉田真紀

NICT第5中長期計画（2021～2025）

- サイバーセキュリティ分野 – 暗号技術
  - **社会の持続的発展**において欠くことの出来ない情報のセキュリティやプライバシーの確保を確かなものとするため、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発を実施するものとする。その安全性評価を行うとともに、安全な情報利活用を推進し、**国民生活を支える様々なシステム**への普及を図るものとする。

安全なデータ利活用技術

データの提供・収集・保管・解析・展開時におけるセキュリティやプライバシーを確保するため、匿名認証や検索可能暗号などのアクセス制御技術、秘匿計算などのプライバシー保護解析技術等の研究開発を行う。これらを用いてデータ利活用や組織横断的な連携を促進するとともに、安全なテレワーク等の社会的な課題解決に貢献する。

暗号技術及び安全性評価

量子コンピュータ時代に安全に利用できる暗号基盤技術の確立を目指し、耐量子計算機暗号を含む新たな暗号技術及び電子政府システムなどで現在使用される暗号技術の研究開発と安全性評価を実施する。具体的には、将来的には耐量子計算機暗号として世界標準となることが予想される格子暗号、多変数公開鍵暗号等や、現在広く使用されているRSA暗号、楕円曲線暗号等について取り組み、国民生活を支える様々なシステムの安全な運用に貢献する。

セキュリティ基盤研究室

- 主に地上システムに着目した研究開発

セキュリティ基盤研究室の最新の主な活動成果

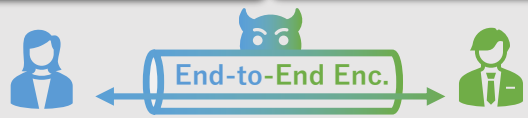
安全なデータ利活用技術

DeepProtect

複数組織による協調学習で元データの秘匿と，得られた学習モデルを使った高精度な解析が可能

プライバシー保護型協調学習

暗号技術及び安全性評価



リアルタイム通信用E2EE技術の具体的な攻撃方法，実行可能性，効果的な対策を設計者に報告（ドラフトに反映された）

E2EEの安全性評価

CRYPTREC
Cryptography Research and Evaluation Committees

電子政府推奨暗号の安全性を評価・監視し暗号技術の適切な実装法・運用法を調査・検討するプロジェクト

安全な暗号技術の普及

- 近い将来，人類の活動領域は宇宙まで進展
  - 今後は地上と宇宙を統合するシステム
  - 宇宙システム固有の理論と技術が必要になる可能性

自己紹介と本講演のテーマ

- 情報理論的暗号に関する研究内容は理論
  - 例えば秘密計算や秘匿計算の最適化
- 理論側へ実用側（NewSpace）から求められたことを紹介

- 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で得た知見の紹介
  - 2018年から開始して現在も継続中
  - 共同研究者は森岡澄夫シニアフェローと尾花賢教授

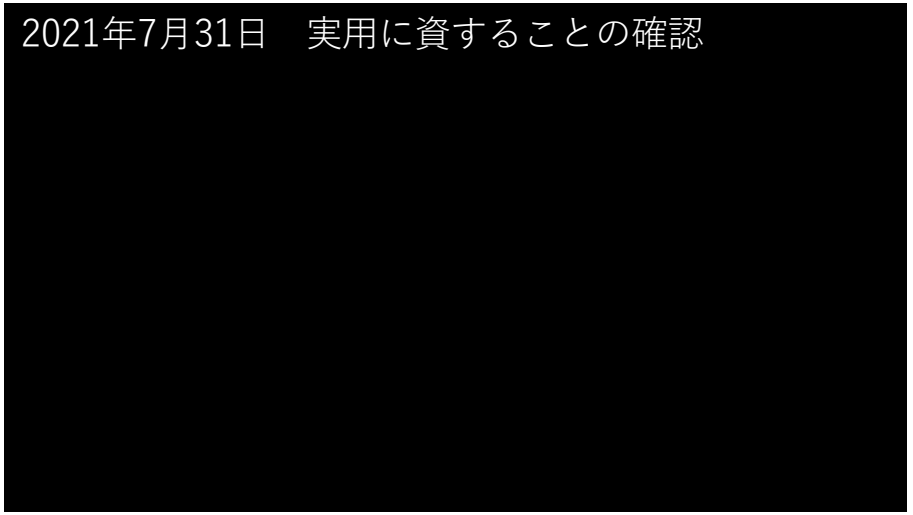
産学連携の共同研究がみせる実験までのスピード感。小型宇宙機の通信を守る

NewSpaceセキュリティプロジェクト
安全なデータ利活用チーム

https://sfl.nict.go.jp/interview/new-space-security.html

本講演の流れ

1. 研究背景
2. 新たな社会ニーズ
3. 研究の概要
4. 基礎研究フェーズ
   - 固有の課題とは
   - 課題解決・基礎実験の概要
5. 実用化フェーズ
   - 固有の課題とは
   - 課題解決
6. まとめ
   - 実際に使うとは



インターステラテクノロジズ株式会社提供

1. 研究背景

NewSpace

OldSpace：国家主導，公益目的

写真出典：www.hq.nasa.gov, https://www.jaxa.jp/projects/rockets/h2b/index_j.html

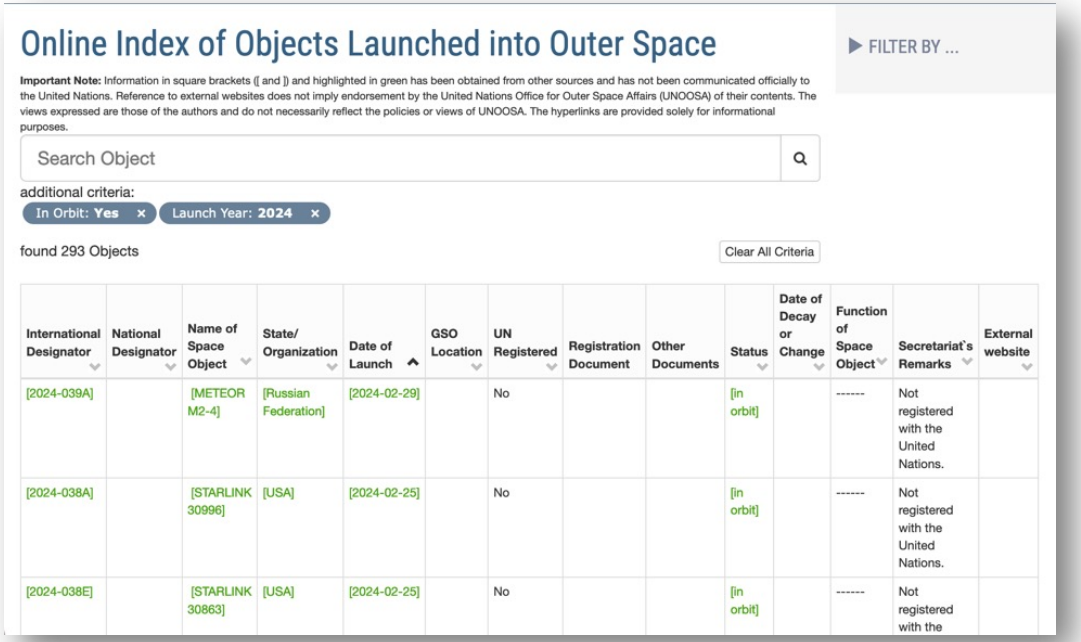
NewSpace：民間主導，民需目的

- 宇宙船，ロケット，人工衛星など全てが対象．開発が速い．

写真出典1：https://www.newsweekjapan.jp/stories/world/2018/04/post-9957.php
写真出典2：https://universemagazine.com/en/spacex-stops-production-of-crew-dragon-spacecraft/
写真出典3：https://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%83%AB%E3%82%B3%E3%83%B3%E3%83%98%E3%83%93%E3%83%BC#/media/File:Falcon_Heavy_Side_Boosters_landing_on_LZ1_and_LZ2_-_2018_(25254688767).jpg

2024年3月7日現在

- 地球軌道上の宇宙機： 12781機
- 2024年に入ってからの打上げ：293機



Online Index of Objects Launched into Outer Space

▶ FILTER BY ...

Important Note: Information in square brackets ([and]) and highlighted in green has been obtained from other sources and has not been communicated officially to the United Nations. Reference to external websites does not imply endorsement by the United Nations Office for Outer Space Affairs (UNOOSA) of their contents. The views expressed are those of the authors and do not necessarily reflect the policies or views of UNOOSA. The hyperlinks are provided solely for informational purposes.

Search Object

additional criteria:

In Orbit: **Yes** × Launch Year: **2024** ×

found 293 Objects

Clear All Criteria

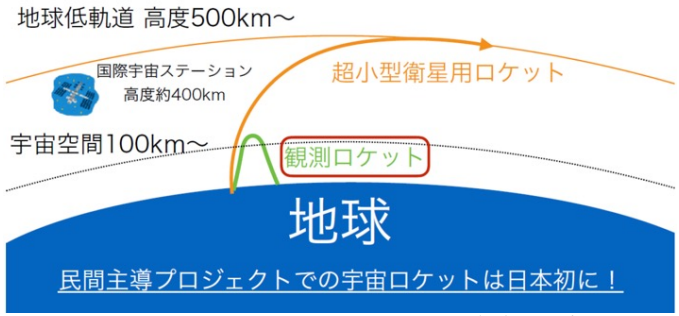
International Designator	National Designator	Name of Space Object	State/ Organization	Date of Launch	GSO Location	UN Registered	Registration Document	Other Documents	Status	Date of Decay or Change	Function of Space Object	Secretariat's Remarks	External website
[2024-039A]		[METEOR M2-4]	[Russian Federation]	[2024-02-29]		No			[in orbit]		------	Not registered with the United Nations.	
[2024-038A]		[STARLINK 30996]	[USA]	[2024-02-25]		No			[in orbit]		------	Not registered with the United Nations.	
[2024-038E]		[STARLINK 30863]	[USA]	[2024-02-25]		No			[in orbit]		------	Not registered with the	

UNOOSA, Online Index of Objects Launched into Outer Space, https://www.unoosa.org/oosa/osoindex/search-ng.jspx

打上げ手段：宇宙ロケット

観測ロケット MOMO
（2019年5月に宇宙到達，7回打ち上げ）

衛星打上げロケット ZERO
（開発中）



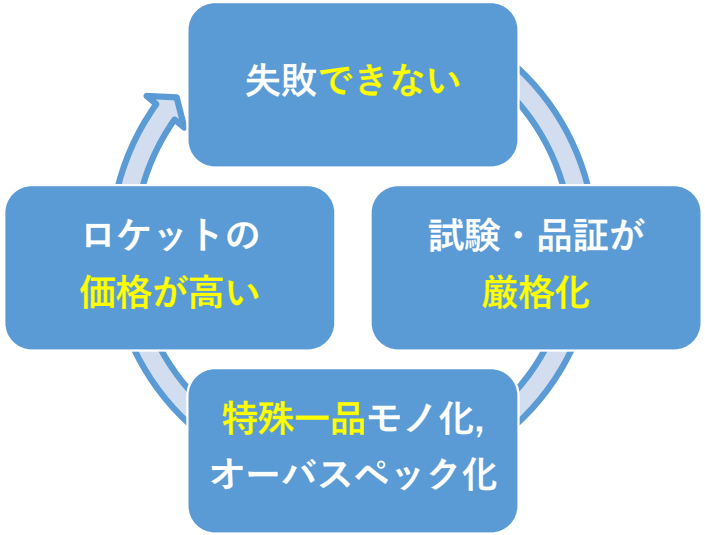
写真提供：インターステラテクノロジズ株式会社

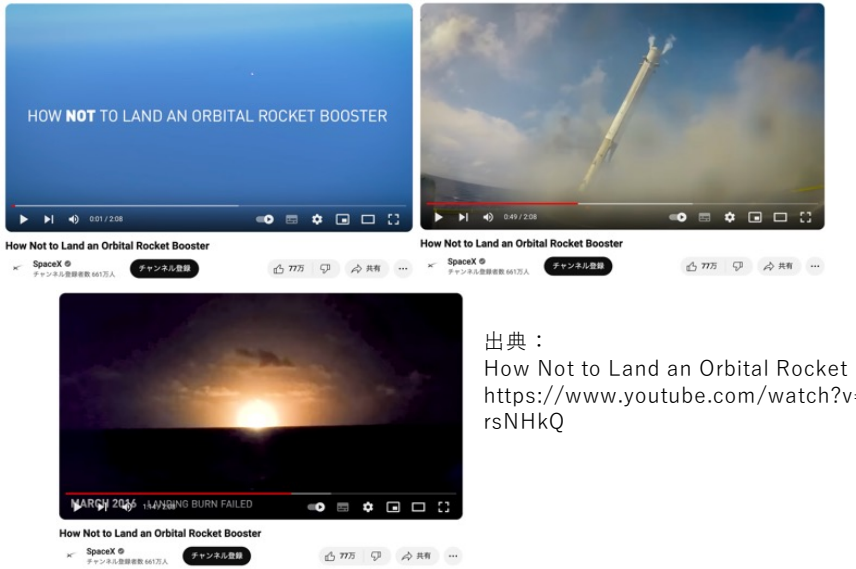
2. 新たなニーズ

OldSpaceからNewSpaceへ

低コスト化への価値転換

- OldSpace：「**絶対に失敗しない**」ことに価値
  - 長い開発期間, コスト上昇の悪循環





出典：
How Not to Land an Orbital Rocket Booster
https://www.youtube.com/watch?v=bvim4rsNHkQ

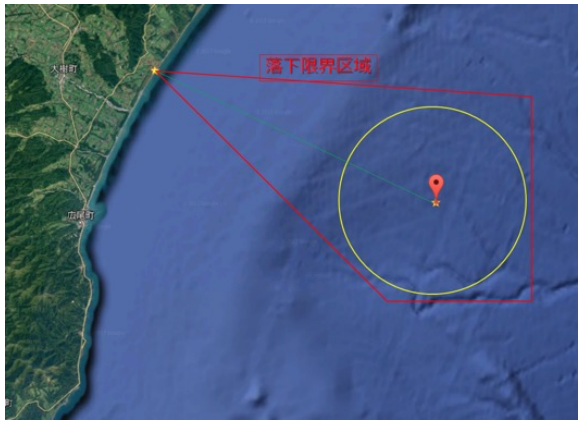
- NewSpace：「多少失敗しても**早く**修正して市場投入」に価値

ただし、公共の安全は低コスト化よりも優先

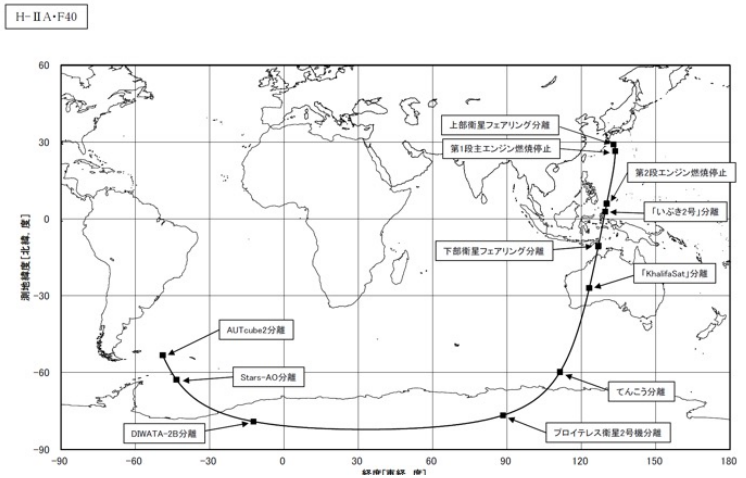
- 価値基準1：公共安全確保（public safety）

超高信頼にすべき
HW,SWを限定

- 価値基準2：主ミッションの達成
- 価値基準3：付随ミッションや広報の達成



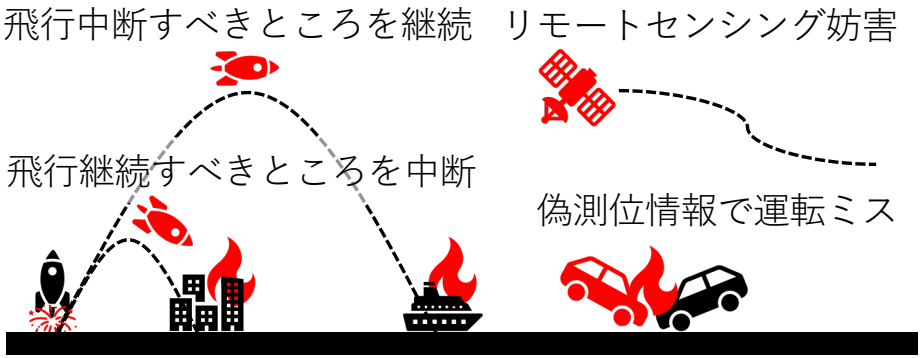
写真提供：インターステラテクノロジズ株式会社



出典：H2Aロケット40号機打ち上げ計画書
https://www.jaxa.jp/press/2018/08/files/20180828_h2af40_j.pdf

回避しなければならない重大トラブル

- 第三者に対する人命・物損被害の発生
- その可能性を予期させる飛行
- 地上局が機体を見失う
- 打上げ中断や飛行中断が不能になる



日本の取り組みと新たなニーズ

- 2018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」（いわゆる宇宙活動法）が施行された

内閣府宇宙開発戦略推進事務局：人工衛星等の打ち上げ用ロケットの**型式認定**に関するガイドライン, p.13

> 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。

- ガイドラインに「適切さ」の具体的な規定はない
- セキュリティとコストはトレードオフ
- 公共の安全のために高セキュリティ，商業利用のために低コストを両立

https://www.space.com/17556-giant-nasa-rocket-space-launch-cost.html

3. 研究の概要

適切なセキュリティを低コストで実用化

研究の目標と最初の一歩

- 目標
  - 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低コストで確立

- 最初の一歩
  - 情報理論的安全性（理論上最高レベルのセキュリティ）を民生電子部品（低コスト）で実現できるか？

多少の政治的意義あり

研究の流れ：実現可能か→実用に資するか

基礎研究フェーズ

2018年：方式の提案と民生電子部品による実装可能性検討

- 観測ロケットMOMOの通信システムを想定した課題を分析し，解決手段の検討
- 最高レベルのセキュリティ（情報理論的安全性）の実現可能性を検討し，方式を提案
- 民生電子部品で速度性能や利用リソースが現実的な範囲に収まるか検討

机上検討

2019年：地上での提案方式の動作実験

- 民生電子部品の正常動作が確認されている地上環境下で提案方式の基本動作を確認

地上試験

2019年～2020年： 飛行環境での民生電子部品の動作確認

- MOMOの飛行環境下で民生電子部品が正常動作することの確認と提案方式の改良

飛行試験

2021年：飛行環境での提案方式の動作実験

- MOMOの実用無線通信における提案方式の動作評価

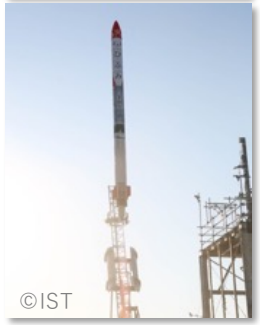
飛行試験

実用化フェーズ

2022年～現在：ZEROでの実用化における課題検討と解決

- 人工衛星打上げ用ロケットZEROのアップリンク通信の課題を分析し，解決手段の提案
- 次にダウンリンク高速大容量通信の課題を分析し解決手段の提案（**SCIS2024**）

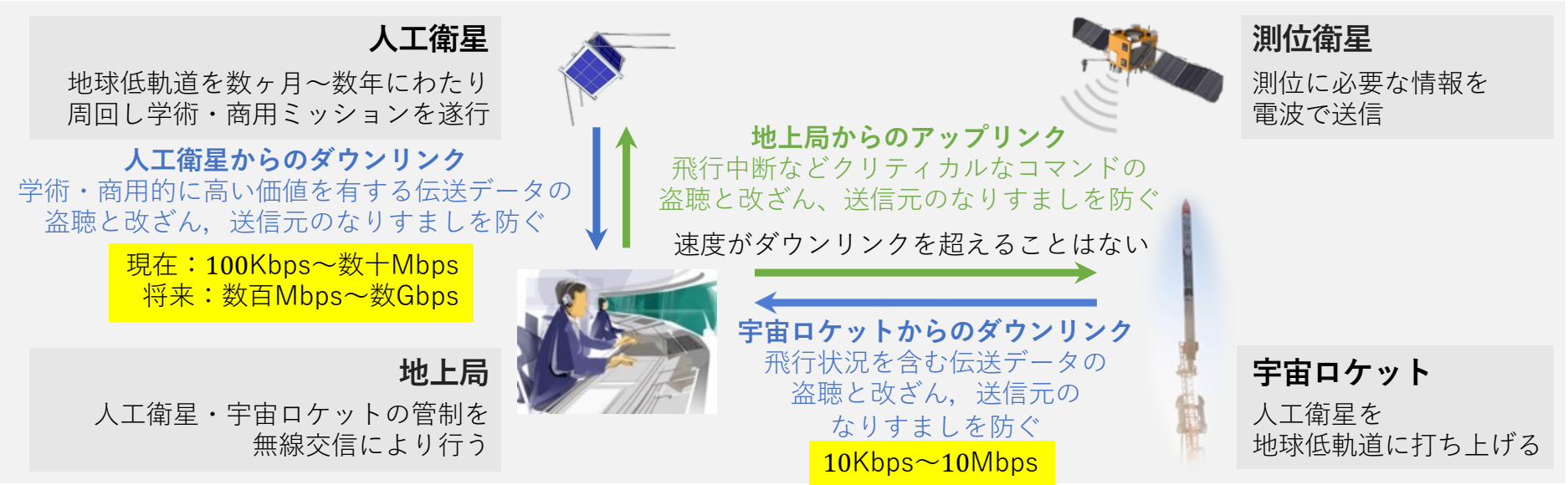
実用化



4. 基礎研究フェーズ

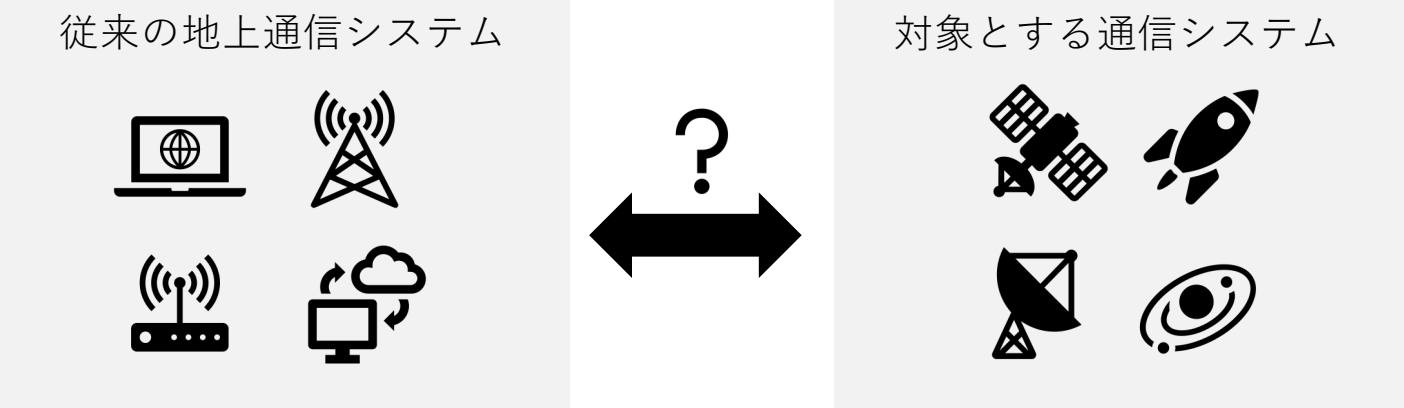
対象通信システムの分析

- エンティティは，地上局，民間宇宙機，測位衛星
- 測位衛星からは受信のみ，主な通信は地上局～宇宙ロケット・人工衛星
- セキュリティ要件は機密性，完全性，可用性

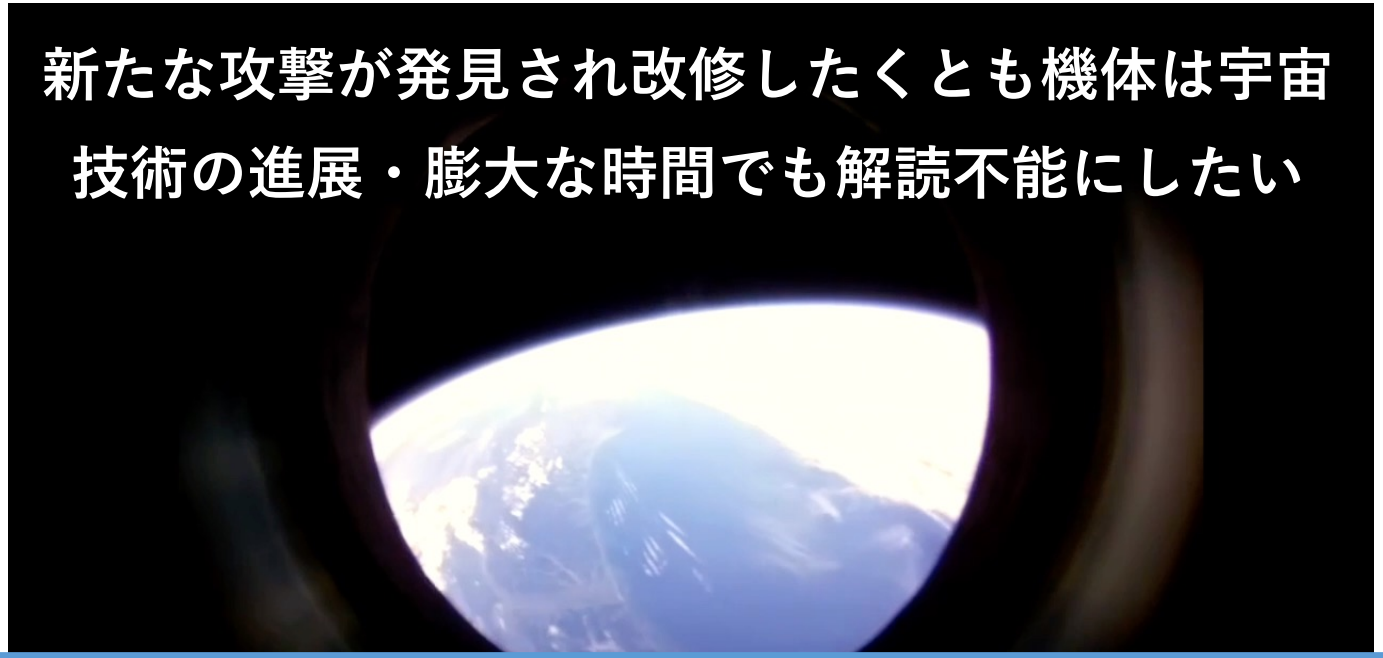


自然な疑問

- 既存の地上通信システム（インターネットや無線LAN）でも，機密性・完全性・可用性は考えられている
- 対象とする通信システムの設計における固有の課題とは？



固有の課題❶ 改修に行けない



要件❶ 高セキュリティ

多様な攻撃に対して継続的に高いセキュリティを確立すべき

固有の課題❷ リアルタイム性への強い要求

出典： Sounding rocket MOMO2 launch 観測ロケットMOMO2号機打上
https://www.youtube.com/watch?v=RJ4LK50TwVs

要件❷ 軽量な設計

簡単な演算からなり，計算効率が良く，スループットも高く，回路規模の小さい暗号を利用すべき

固有の課題❸ 過酷な環境への耐性

要件❸ 高信頼な実装

飛行環境下における演算回路やストレージなどの信頼性を踏まえた，
システムとしての高信頼な実装方式

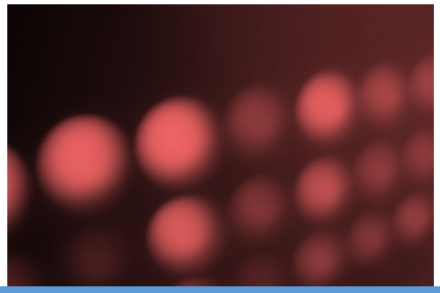
固有の課題❹ 地上の基本対策は利用できない

暗号理論の基本対策1：公開信頼情報の適時利用

- Bulletin board, common reference string
- 地上局と宇宙機との通信周波数は一般に機密情報
- 無線処理系は局外との通信系とは分離
- つまり，使えない

暗号理論の基本対策2：対話して互いの情報を確認

- 通信が不安定な状況ではデッドロックに陥り，管制を喪失する可能性
- つまり，使えない



要件❹ インタラクション排除

外部だけでなく通信相手とのインタラクションを可能な限り避ける

固有の課題をまとめると

- 対象とする通信システムでは，地上局と民間宇宙機との間で無線通信が不安定な状況で，

要件１）高セキュリティ
要件２）軽量な設計
要件３）高信頼な実装

となる非インタラクティブな方式（要件４）を民生電子部品で設計する必要がある

固有の課題をまとめると

- 対象とする通信システムでは，地上局と民間宇宙機との間で無線通信が不安定な状況で，

要件１）高セキュリティ
要件２）軽量な設計
要件３）高信頼な実装

} 机上で設計の工夫と検証
} 飛行試験で検証

となる非インタラクティブな方式（要件４）を民生電子部品で設計する必要がある

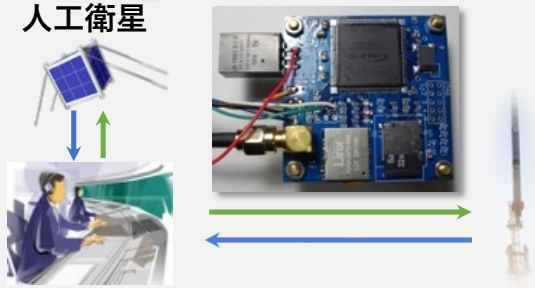
要件1）高セキュリティ

情報理論的暗号の前提

送受信者は通信量に応じた大量の鍵を事前に共有

- 通常の地上通信システム（インターネット等）
  - 鍵の事前共有と総量推定が困難
  - 非現実的コストになり用いられていない
- 民間宇宙機用途
  - 機体～地上局間の1対1通信に制限できる
  - 地上局と機体が打上げ前に物理的に近接するため，**鍵の事前共有が物理的に容易**
  - **鍵消費レートがほぼ一定でライフタイムも短いため**鍵総量の上限を推定できる
  - かつ，現在の民生電子部品で実装可能な範囲にある
- 要件1）高セキュリティを満たす

データ・ダウンリンク例
10Mbps × 1年 / 10 = 4TB 程度 → **SSD**



コマンド・アップリンク例
100Kbps × 10時間 = 450MB 程度→ **SDカード**

要件2）軽量な設計

古典的な情報理論的暗号

機密性の実現にはOne-time pad, 完全性の実現にはA-code

- 有限体上の加算・乗算で実現可能
- 実装可能性も確認
  - ソフトウェア実装：ラズベリーパイ3B (Cortex-A53, 1.2GHz)
  - ハードウェア実装：FPGA Intel Cyclone 10 LP
  - 十分なスループットを小さい回路規模で達成可能で，
    地上通信システムで利用されている「計算量的安全な暗号」より高スループット

$$A\big(\overbrace{(k_0, k_1)}^{\text{鍵}}, \overbrace{(s_1, \ldots, s_\ell)}^{\text{ソース}}\big) = k_0 + \sum_{i=1}^{\ell} s_i \cdot k_1^{\ell-i+1}$$

- 要件2）軽量な設計を満たす

有限体	スループット(Mbps)
$GF(2^{88})$	152.6
$GF(2^{112})$	119.0
$GF(2^{120})$	120.4
$GF(2^{136})$	67.1
$GF(2^{144})$	67.7
$GF(2^{160})$	59.0

有限体	回路サイズ（LE）	動作周波数（MHz）	スループット（Mbps）
$GF(2^{88})$	5650	127.93	11257.84
$GF(2^{112})$	8987	121.94	13657.28
$GF(2^{120})$	10330	118.23	14187.60
$GF(2^{136})$	13137	113.60	15449.60
$GF(2^{144})$	14680	114.60	16502.40
$GF(2^{160})$	18055	104.17	16667.20

もしかしなくとも情報理論的暗号使える？！
→改めて適切なセキュリティの検討

- 要件2）軽量な設計から公開鍵系の暗号は対象外
- 情報理論的暗号，軽量暗号，AESに代表される汎用用途ブロック暗号（general-purpose block ciphers）が候補
- まず，要件1), 2) について，以下の観点で評価
  - 一般的位置付け（時間経過や技術発展に伴い新たな脆弱性が発見される可能性）
  - SW実装・HW実装→ 軽量暗号を使う強い動機はなくなる

評価項目		情報理論的暗号	軽量暗号	汎用用途ブロック暗号
要件1）高セキュリティ		✓		
要件2）軽量な設計		✓	✓	
要件3）高信頼な実装	演算装置			
	ストレージ			

もしかしなくとも情報理論的暗号使える？！
→改めて適切なセキュリティの検討

- 要件3) 高信頼な実装について，以下の影響による信頼性低下リスクで評価
  - ソフトエラー：宇宙線に起因するデータ破損
  - ハードエラー：素子の恒久的な故障
- 演算装置の信頼性
  - 情報理論的安全な暗号の方が回路規模が小さく，リスクが低い
- ストレージの信頼性
  - 汎用用途ブロック暗号の方が鍵サイズが小さく，リスクが低い

評価項目		情報理論的暗号	軽量暗号	汎用用途ブロック暗号
要件1）高セキュリティ		✓		
要件2）軽量な設計		✓	✓	
要件3）高信頼な実装	演算装置	✓		
	ストレージ			✓

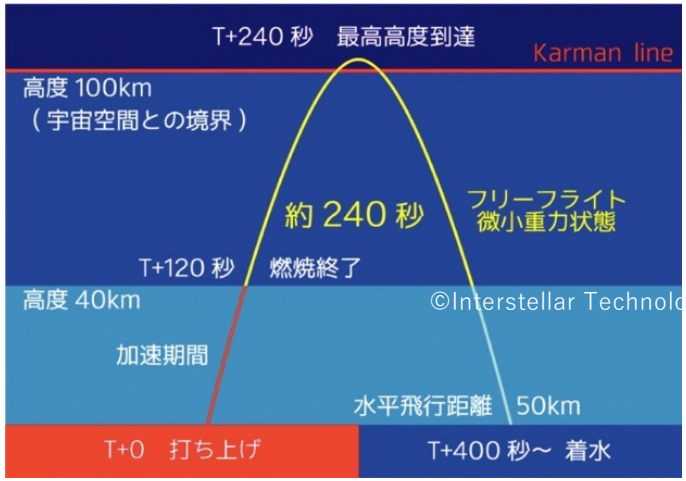
もしかしなくとも情報理論的暗号使える？！
→改めて適切なセキュリティの検討

- ストレージの信頼性が実用上十分であれば，
  情報理論的安全な暗号が最良の選択
  → 飛行実験においてはストレージの信頼性を評価
- もしストレージの信頼性が実用上不十分であれば，汎用用途ブロック暗号も候補となる
  → 演算装置の信頼性も評価

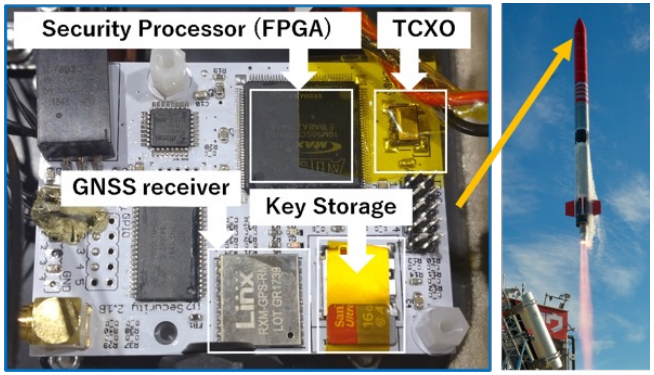
評価項目		情報理論的暗号	軽量暗号	汎用用途ブロック暗号
要件1）高セキュリティ		✓		
要件2）軽量な設計		✓	✓	
要件3）高信頼な実装	演算装置	✓		飛行実験で要検討
	ストレージ	飛行実験で要検討		✓

MOMO3～6号機の実験環境と搭載実験装置

- 宇宙空間に到達する弾道飛行で衛星打ち上げの1段目に相当
  - 飛行中，もっとも振動や温度などの条件が厳しいフェーズ
  - 安全上，もっとも通信の確実性が求められるフェーズ
- 民生電子部品で構成した装置からダウンリンク



最大距離	約120km
最大速度	約4500km/h
最大加速度	4～5g
振動	3～20Grms
機内温度	−20～＋60°C
気圧	ほぼ0～1気圧



MOMO3～6号機での実験結果

- 最終的に，全飛行フェーズにおいて正常通信を実用速度で行えた
- フライト失敗時は異常な機体回転など起こしたが，実験は正常に実施

	フライト成否	総受信パケット数（正常受信パケット）	実効帯域	確認項目
3号機	フルサクセス	1212	8kbps	部品
4号機	失敗（到達高度約10km）	6878	50.1kbps	暗号演算部
5号機	失敗（到達高度約10km）	13239	77kbps	方式全体
6号機	フルサクセス	558313	512kbps	実用速度＋方式全体

要件3）高信頼の実装を満たす

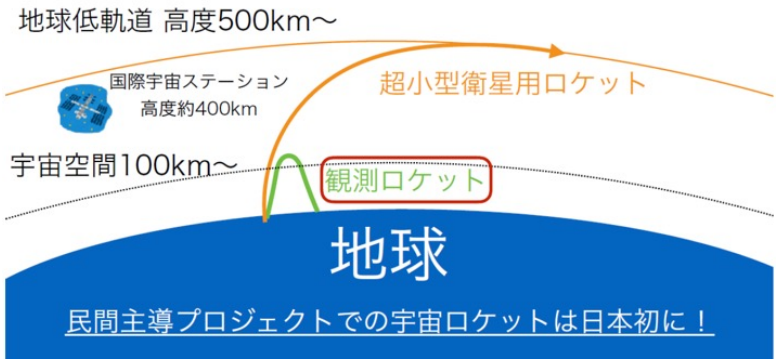
情報理論的に安全な提案方式は宇宙ロケットにおいて実用に資すると判断

6. 実用化フェーズ

人工衛星打上げロケットでの実用化に向けて

- 情報理論的暗号に共通の基本課題として,
  送受信で同じ鍵を使う仕組み（鍵の同期）が必須
- 軌道上運用における固有の課題はあるのか？

衛星打上げロケット ZERO
（開発中）



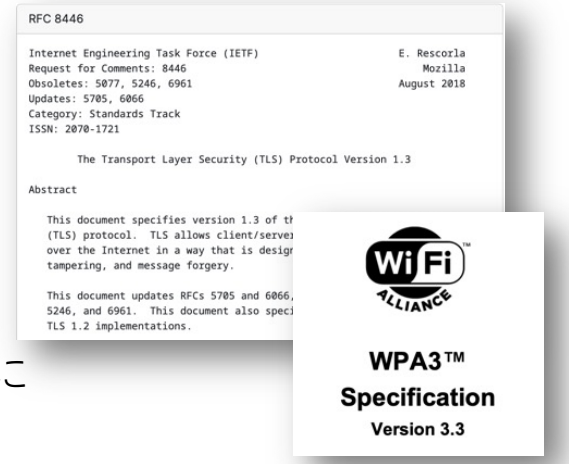
固有の課題：地上の基本対策は利用できない

地上での基本対策1：対話して互いの情報を確認（再）

- 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，管制を喪失する可能性
- つまり，使えない

地上での基本対策2：制御情報を保持して利用

- パケットシーケンス番号や鍵インデックスの前回値
- 放射線などで破損や瞬停による初期化で恒久的な通信不能に
- つまり，使えない



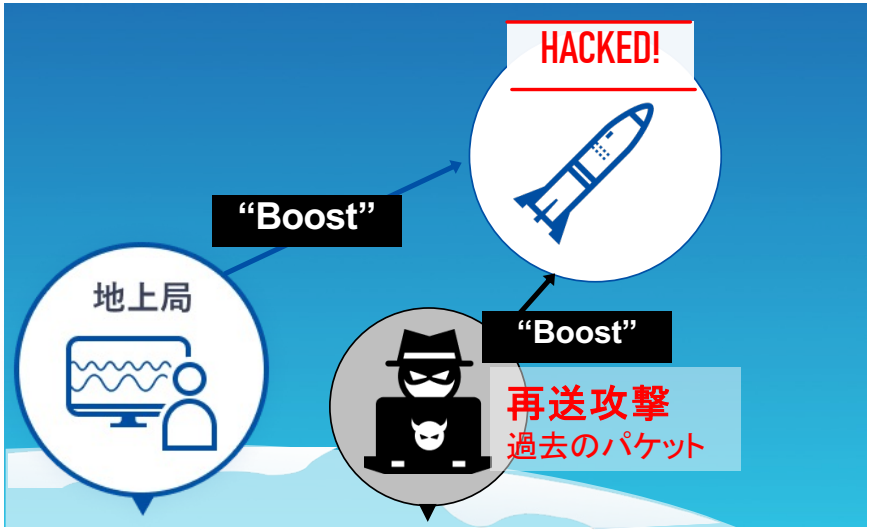
https://datatracker.ietf.org/doc/html/rfc8446
https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.3.pdf

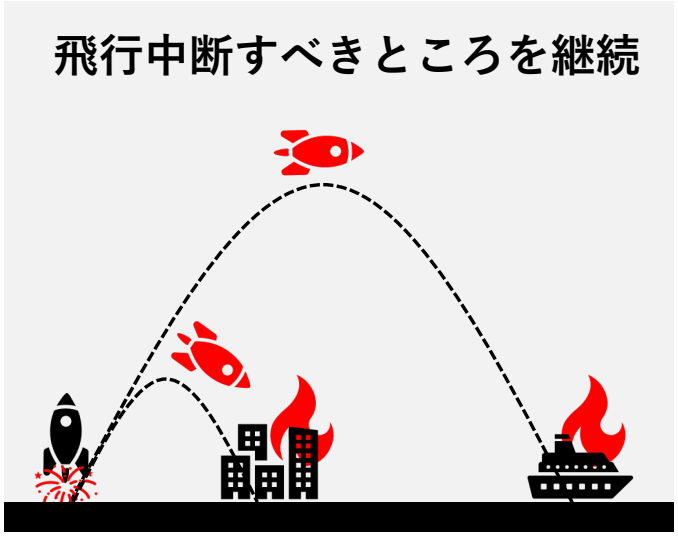
要件：「ひとりぼっちで記憶喪失」に耐える

インタラクションと制御情報の保持を可能な限り避ける

どのような脅威に直結するか

- リプレイ攻撃によって軌道を外れるおそれ
- 暗号学的に安全性を証明できる対策がほしい





ボツになったリプレイ攻撃対策案

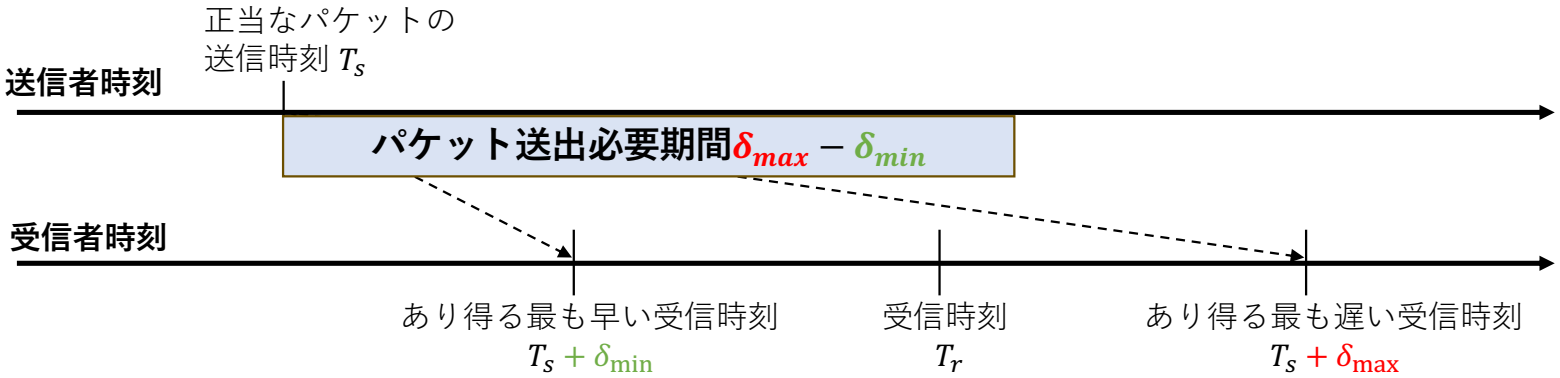
- 対策案：ストレージの使用済み鍵を乱数で上書き
  - リプレイ攻撃されても，鍵が異なるためA-codeの認証をパスしない
- ボツ理由：高速通信のため
  - 高スループット（数十Mbps）
  - 総通信量（≤鍵量）は10Gバイト以上

  - 鍵ストレージのデバイスはNANDフラッシュ
    - 読み出し遅延が長く追い付かない可能性があり先行バースト読み出しが必要
  - 上書きしている場合ではないし誤って上書きすると管制喪失

これこそ机上の空論…

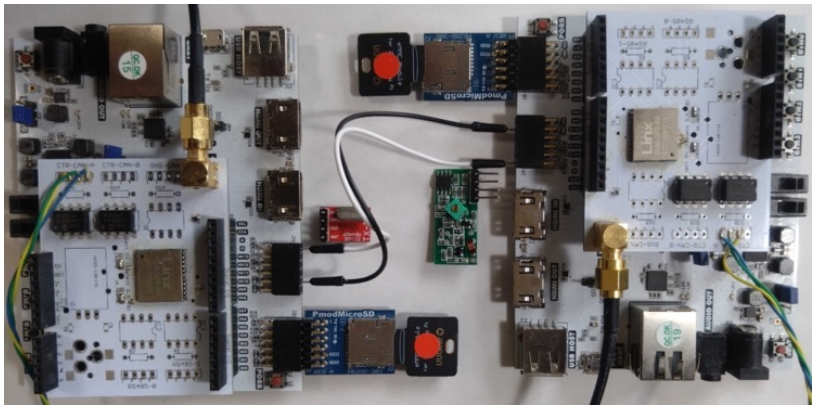
解決手段（安全性証明つき）

- リプレイ攻撃を時刻情報のみで判定し前回値保存を不要にする
  - 送信側は送信パケットに送信時刻T_sを打刻、受信側は受信時に受信時刻T_rを取得
  - 処理遅延や通信遅延の上限$\delta_{\max}$と下限$\delta_{\min}$を推定し、その範囲内なら受理
  - パケット送出はリプレイ攻撃可能な時間帯をなくすため、$\delta_{\max} - \delta_{\min}$の時間をかける
- 実効速度
  - 遅延測定の誤差を飛行前に**静的**推定：100kbps→**コマンド**送信に十分
  - 位置情報を利用して飛行中に**動的**推定：10Mbps→**テレメトリ**送信にも十分



評価・試作実証

- GNSSによる位置測定では遅延測定が0.03ミリ秒程度の精度で可能と推定
  - なお宇宙機は7.8km/秒の速度で移動していることも利用して推定
- 他の処理系遅延などを合わせても $\delta_{\max} - \delta_{\min}$ は0.1ミリ秒程度.
- パケット送信頻度10kHz，実効ビットレート10Mbps程度が実現可能と推定
- 他の処理（認証演算や鍵アクセス）が十分な速度をもつことは試作実証済



6. まとめ

情報理論的暗号を実際に使うとは

まとめ

- 情報理論的暗号を実際に使うには汎用性より特化性
  - 設計段階から実用先における固有の課題を十分に検討する必要あり
- 次々と却下される王道テクニックや砕け散る分野の常識（良い意味です）
- 本気の「実用に資するか」はとても興味深い
  - 理論分野における実証＝実用化における基礎研究
  - 報道発表では「実証実験」ではなく「基礎実験」と表現
- 実際、理論面で課題の新規性や成果の独創性あり
  - 共同研究で得た成果は飛行データを含めて積極的に公開
- 課題解決では基礎に立ちかえることが何より重要だった

本講演で紹介した成果に関係する文献

1. 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，1K19, 2018.
2. 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.
3. 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.
4. 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，3S08, 2019.
5. 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，4I03, 2020.
6. S.~Morioka, S.~Obana, 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 2021).
7. 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).
8. 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, 2M12, 2022.
9. M.~Yoshida, S.~Morioka, S.~Obana: Secure Communication via GNSS-based Key Synchronization. Work-in-Progress in Hardware and Software for Location Computation (WIPHAL 2023).
10. S.~Morioka, S.~Obana, 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).
11. 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, 1R07, 2023.
12. 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).