第406回　NRIメディアフォーラム

ITロードマップ【Day 1】

宇宙空間におけるIoTセキュリティの再定義

～地上の無線機器向け規格をベースとした セキュリティ評価要件の検討～

NRIセキュアテクノロジーズ株式会社
オフェンシブセキュリティ事業本部
IoTセキュリティ事業部

シニアセキュリティコンサルタント　江藤 修

株式会社NDIAS出向

セキュリティコンサルタント　橘 和樹

2026年3月23日

NRIセキュアテクノロジーズ
NRI SecureTechnologies

Envision the value, Empower the change

目次

1． 背景と課題～宇宙IoTで何が変わり、何が危ういのか～

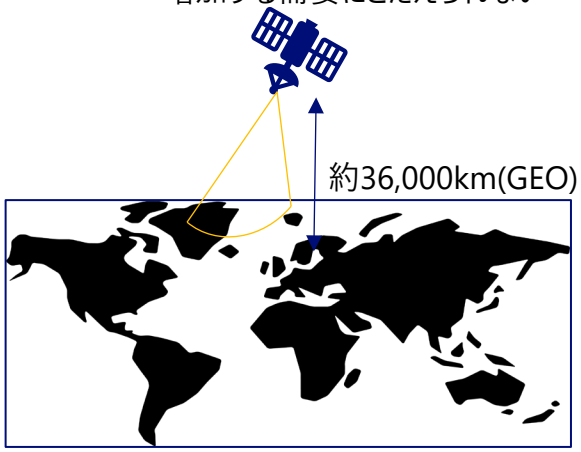
2030年代の宇宙利用は地球低軌道（LEO）上の衛星コンステレーション※を基盤に拡大する

（※協調して特定の目的を果たす複数個の人工衛星のまとまり）

- 地上では、遠隔監視・制御・災害時通信などを支えるIoT利用が拡大し、通信圏外を含む広域エリアで機器をネットワークに接続したいという需要が高まってきている。
- 近年は打ち上げコストの低下、小型衛星の実用化、衛星間通信の進展により、低軌道上に複数の機器を大量に打ち上げたうえで相互リレーすることで広域通信可能な構成が実現。宇宙空間もIoT基盤として活用され始めている。【01-02-04,p.22】

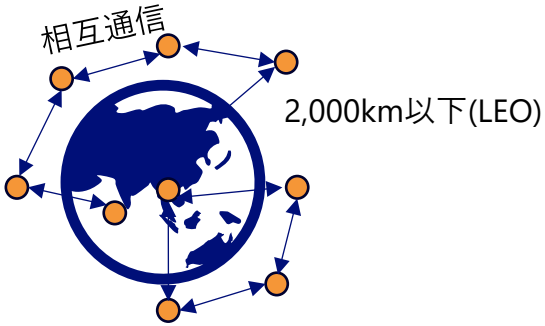
Before（従来の宇宙通信）

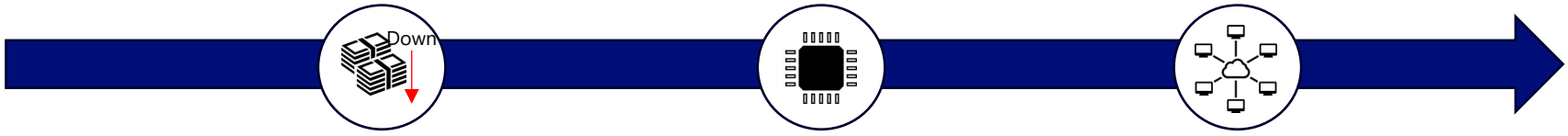
静止衛星（GEO）を用いた広域中継ネットワークを用いた宇宙利用
1機で多くをカバーできるが、打ち上げコストや運用の壁があり、
増加する需要にこたえられない



After（今後の宇宙通信）

通信モジュールを備えた小型のデバイスを相互通信させることで
広域中継ネットワークを実現し、農業分野での遠隔センサ監視、
災害時・僻地での通信インフラ、海洋・物流での資産追跡の
サービスを実現【03,p.22】

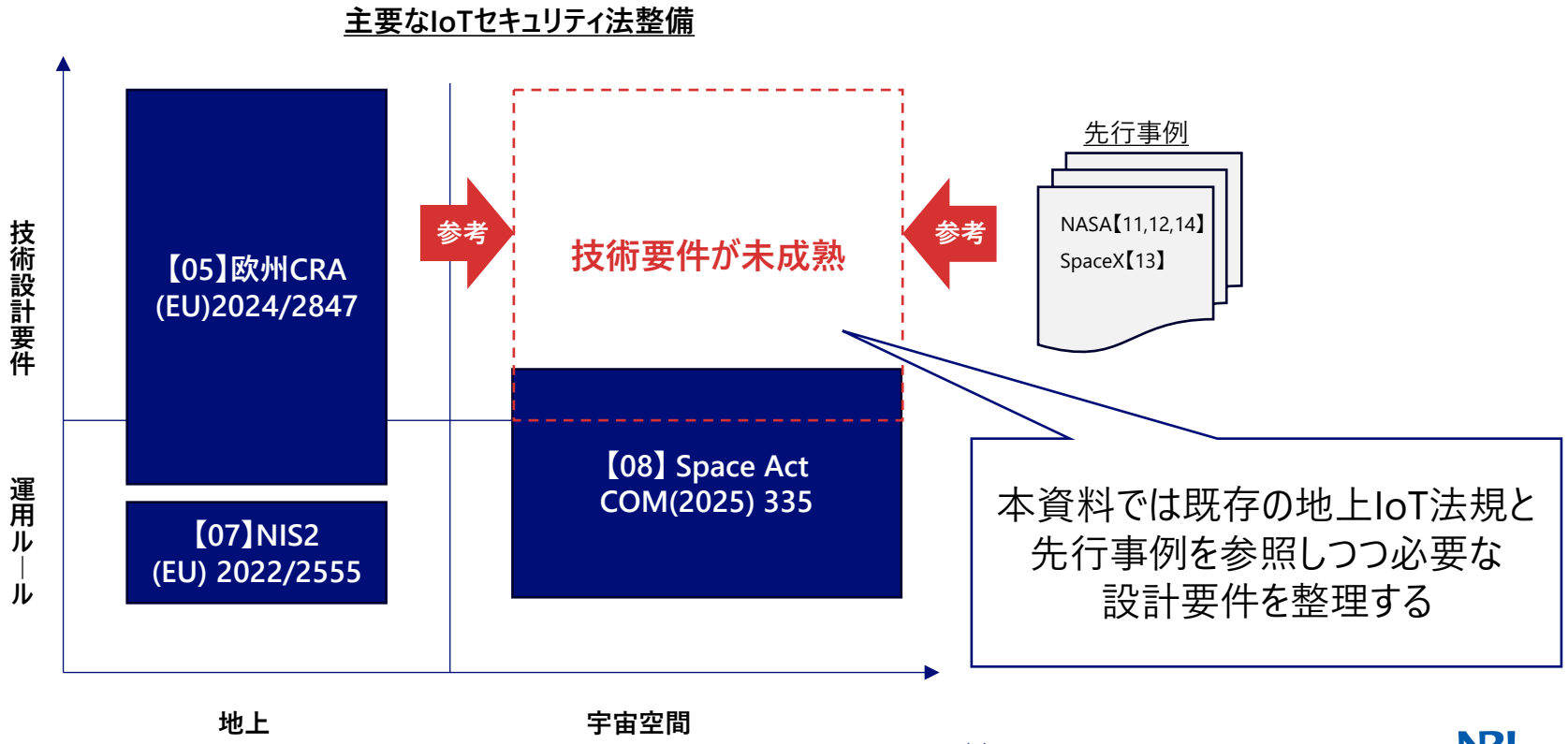




打ち上げコストの低減　電子部品の小型化　IoT技術の普及

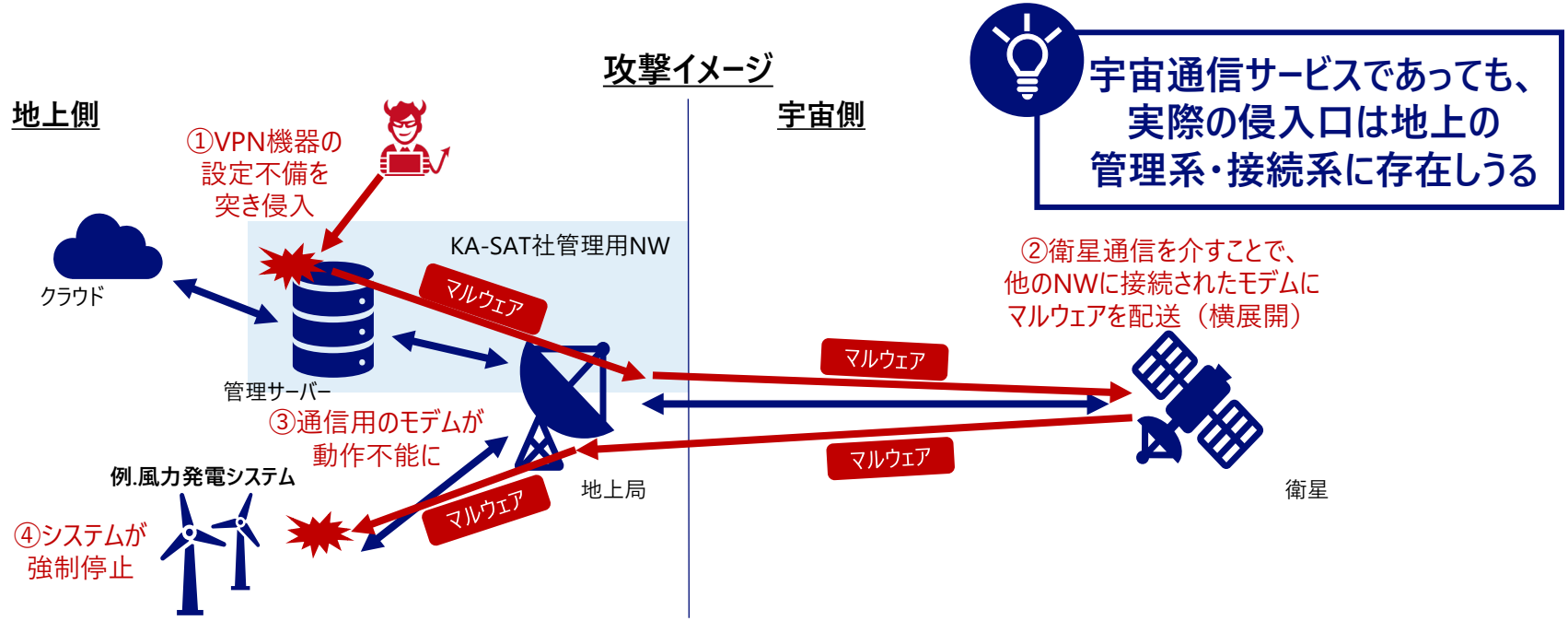
2026年現在、宇宙IoTを直接対象とする包括的な規制は未成熟

- 宇宙IoT市場が拡大していく一方、機器を直接対象とした包括的なセキュリティ法規は現時点では十分に整備されていない。現状ではNASAやSpaceX社等の先行事例も参照しつつ、各社が独自に設計・運用上の対応を行っている。
- 欧州では無線機器、IoT機器を対象とする大規模なセキュリティ法規CRA（Cyber Resilience Act ）が整備されつつあり、付随する技術規格を含めて実務上の参照軸になりつつある。（例.EN18031）【05-06,p.22】



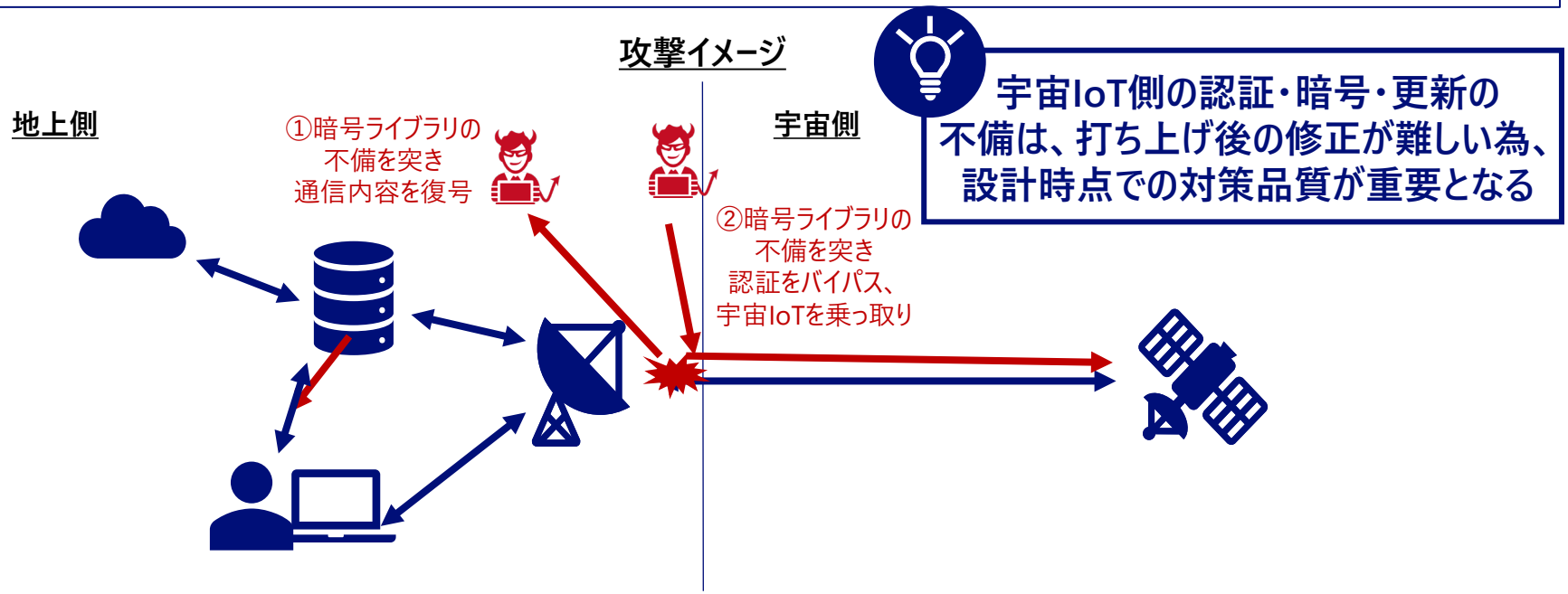
【脅威の事例1（地上側）】：米Viasat社の衛星通信サービスへのサイバー攻撃【09,p.22】

- **日時**： 2022年2月24日
- **対象**： 仏Eutelsat S.A.保有の通信衛星 KA-SAT を利用した衛星通信サービス
  （例.風力発電システムの監視制御）
- **内容**： 攻撃者がVPN機器の設定不備により管理セグメントのサーバに侵入、管理用コマンドを利用して多数の利用者モデム（衛星と通信する端末）に不正な操作（例.マルウェア「AcidRain」）を適用。
  結果、複数のモデムが感染して動作不能な状態に陥らせた。
- **影響**： 約4万台のモデムが機能停止し、独Enercon社の**約0.6万台の風力タービン遠隔監視/制御通信が停止**



【脅威の事例2（宇宙側）】：NASA深宇宙通信ソフトウェアの深刻な脆弱性【10,p.22】

- **日時**： 2025年12月18日
- **対象**： NASAの宇宙船ー地上間通信を保護する暗号ライブラリ「CryptoLib」
- **報告者**：米カリフォルニアのスタートアップ企業AISLE（自社開発したセキュリティ診断ツールで発見）
- **内容**： 詳細は不明だが重大な脆弱性が存在
  - 予見される影響内容の記載から推測するに、認証アルゴリズムの不備による認証バイパスや、暗号化アルゴリズムの不備による通信内容の復号などが行える状態であった
- **影響**： 攻撃の観測はされていないが、悪用されていた場合、**NASAの火星探査車などの遠隔操作が可能に**



凡例： 本資料の主題

脅威の事例から見える設計上の論点

地上側

- 地上側のシステムは**攻撃の対象となる面**（アタックサーフェス）**が多数存在**
- 一方で地上に設置しているため、更新・監視・物理対処が比較的容易
- 一般的な**ITシステム/IoT機器におけるサイバーセキュリティ対策や物理セキュリティ対策が適用可能**

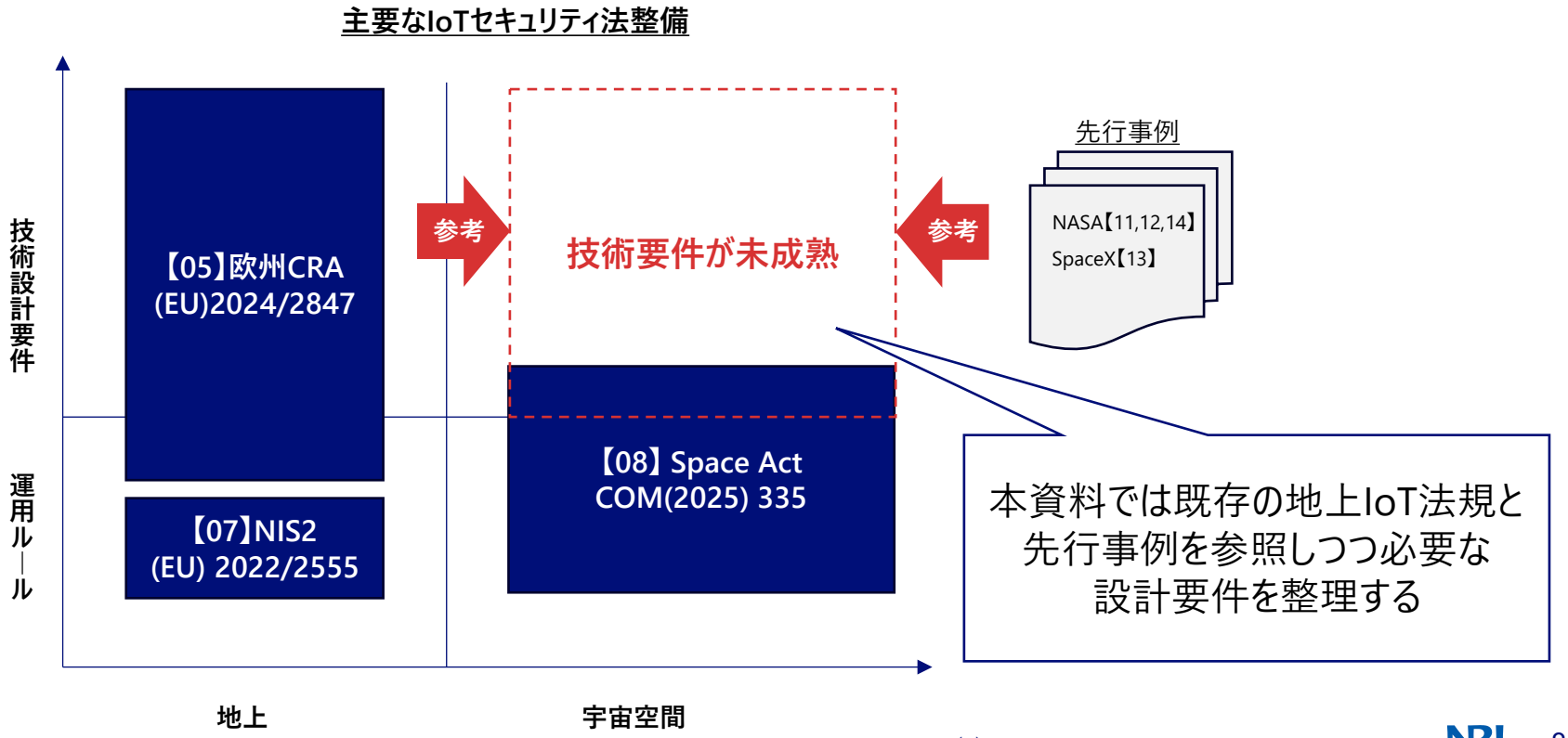
宇宙側

- 宇宙空間に存在するという制約上、**打ち上げ後の修正や物理対処が難しく、後付けの補強に限界がある**
- 宇宙IoT**単体として打ち上げ前に十分な対策を織り込んだ設計が必要**

再掲

2026年現在、宇宙IoTを直接対象とする包括的な規制は未成熟

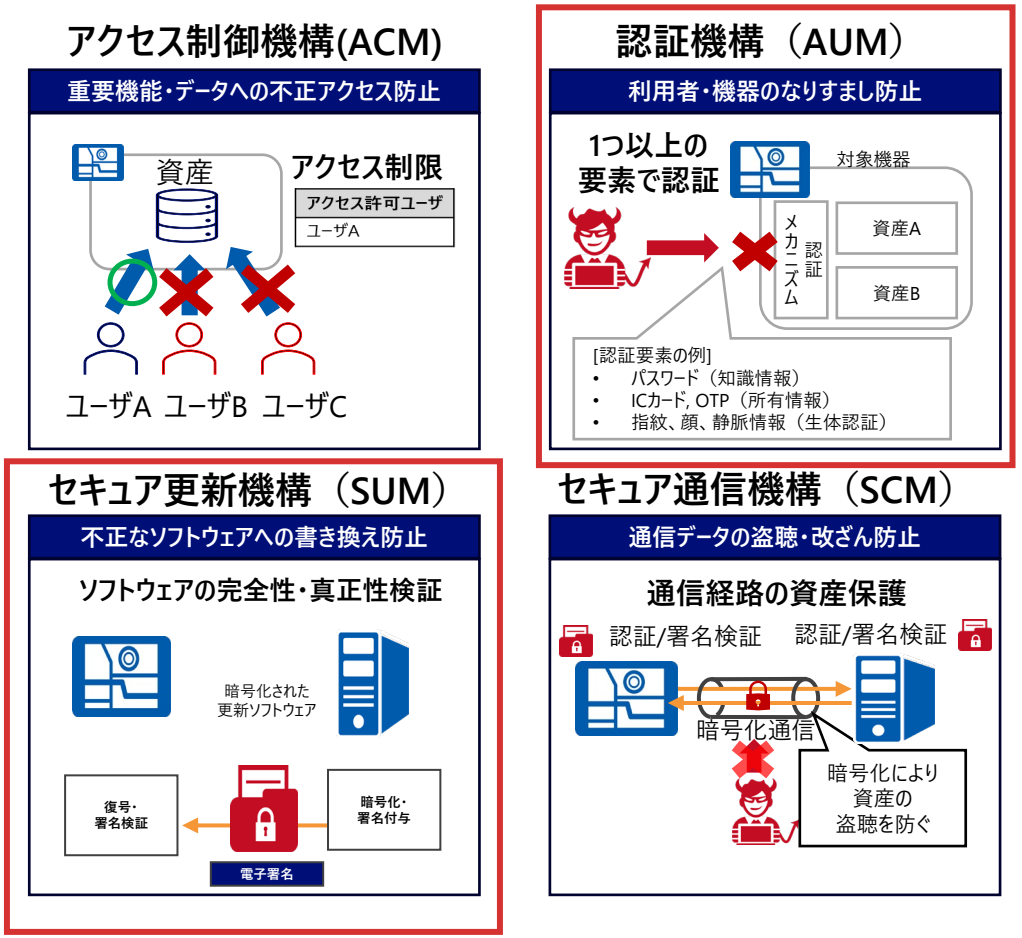
- 宇宙IoT市場が拡大していく一方、機器を直接対象とした包括的なセキュリティ法規は現時点では十分に整備されていない。現状ではNASAやSpaceX社等の先行事例も参照しつつ、各社が独自に設計・運用上の対応を行っている。
- 欧州では無線機器、IoT機器を対象とする大規模なセキュリティ法規CRA（Cyber Resilience Act ）が整備されつつあり、付随する技術規格を含めて実務上の参照軸になりつつある。（例.EN18031）【05-06,p.22】



2．先行事例から学ぶ設計方針

宇宙IoTの設計要件整理に用いる4つのセキュリティ機能群

- 欧州法規で参照される技術規格EN18031では主要なサイバーセキュリティ対策を複数の機能群に分けて整理している。【06,p.22】
- 本資料では、宇宙IoTの設計検討に特に重要な4つの機能群を参照軸として用いる。



凡例：

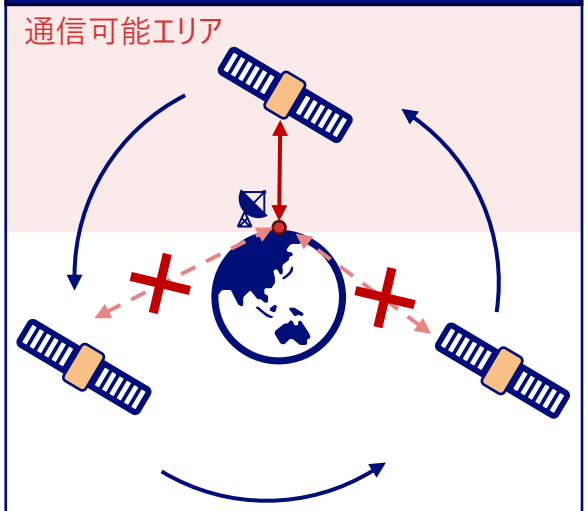
本資料の3章で説明

宇宙IoT(LEO)は “つながらない・時刻がずれる・直しに行けない” 前提で設計する

宇宙の「通信の断続性」・「時刻同期の不確実性」・「物理アクセスの困難性」それぞれを考慮する必要がある。

通信の断続性

要点：通信可能時間が短い

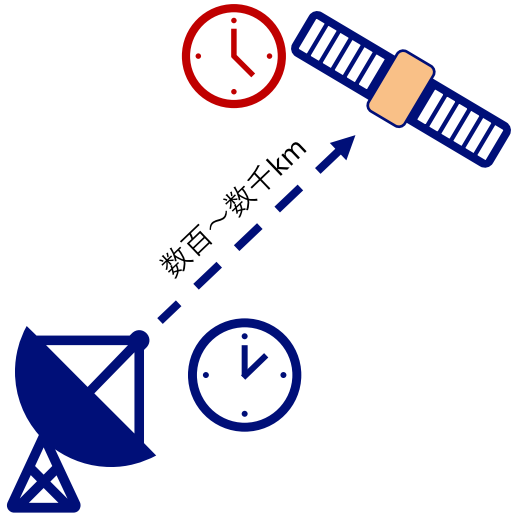


LEOで飛んでいるため、単一の衛星とは1日数回・各回10分程度しか通信ができない

毎回の通信で認証、制御が確実に完了できる設計が必要

時刻同期の不確実性

要点：時刻がずれやすい

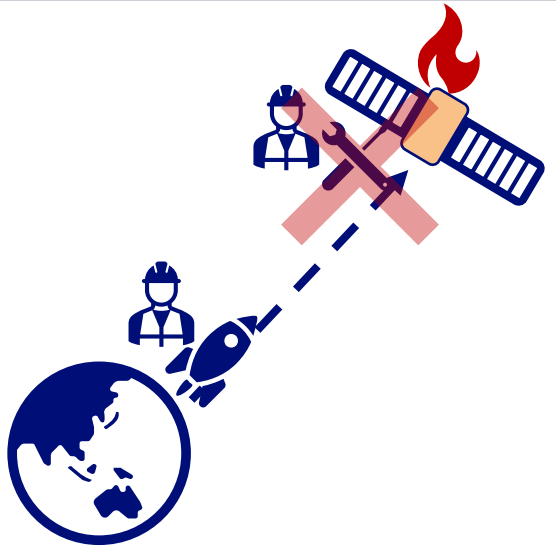


距離差があることから、伝搬遅延、往復遅延により時刻のずれが地上よりも大きくなる

時刻カウンターに依存しすぎない設計が必要

物理アクセスの困難性

要点：異常動作時に修正が難しい



一度打ち上げると、宇宙空間かつ高速で動く衛星に保守等の目的で物理的にアクセスすることは困難

遠隔更新・安全停止・復旧手順まで最初から考慮した設計が必要

先行事例から学ぶ設計方針

- 紹介した4機能（ACM/AUM/SCM/SUM）を、宇宙環境でどのように成立させるか検討する。
- 先行事例を参照すると、宇宙特有の制約（通信の断続性・時刻同期の不確実性・物理アクセスの困難性）により**時間に依存した設計を避け、機器の状態・カウンタ・署名で成立させるのが共通の留意項目**として認識される。

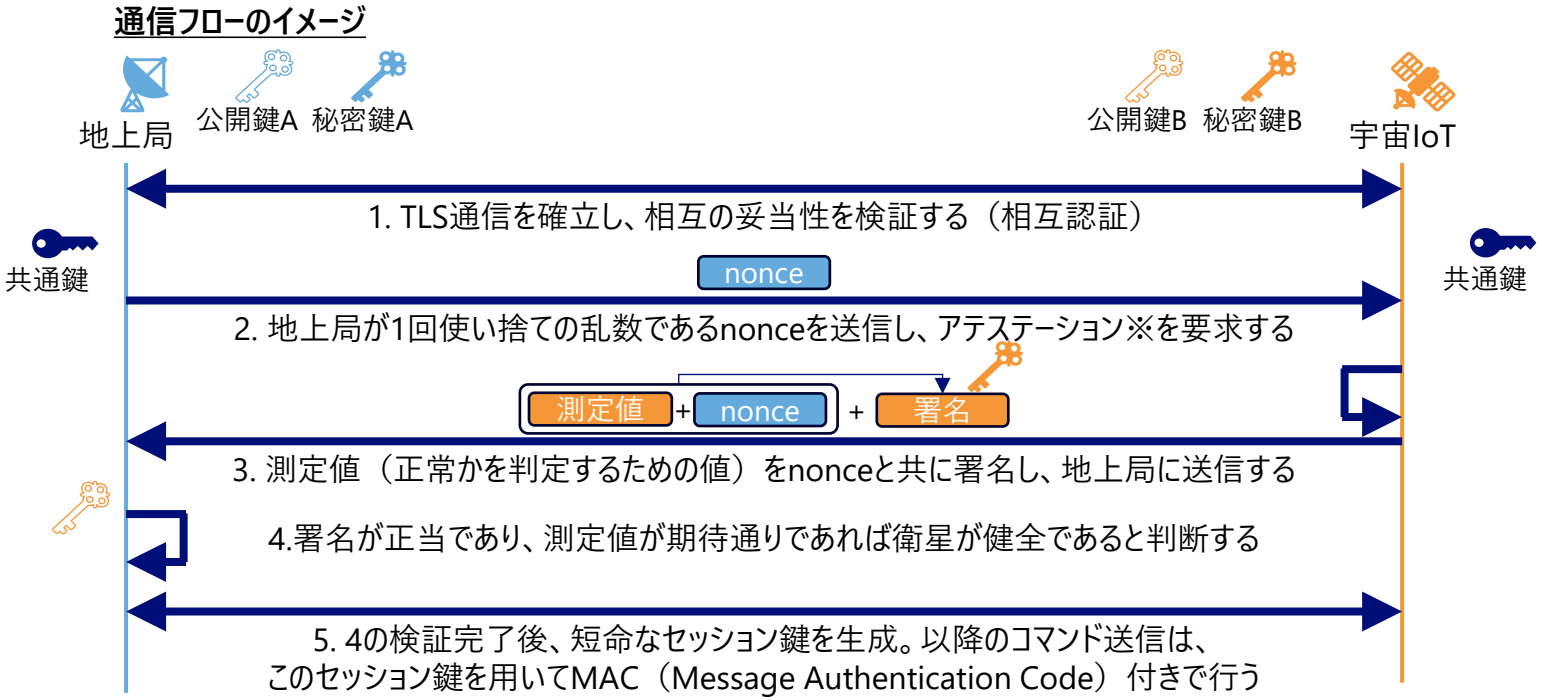
先行事例	概要	宇宙での教訓	関係するセキュリティ機能
【11-12,p.22】宇宙機―地上局間通信のセキュリティ（SDLS等の実装・ガイド）	通信フレームを単位として、認証（真正性）と守秘（暗号化）を成立させる枠組み	宇宙は通信が途切れるので、「一度つながったから安心」が通用しない。だから、送るたびに「相手確認」と「中身の保護」をセットで行う。	SCM（主） AUM（従：相互認証）
【13,p.22】鍵運用の実装・運用（OTAR※1等）	長期運用・断続通信でも鍵を更新し続けるための鍵配布・更新方式（運用込み）	宇宙は長期運用なので、暗号の鍵は「途中で入れ替え（更新）」できないと困る。 ただ宇宙は時計がズレたり通信が途切れるので、更新の順番は「連番（カウンタ）」で管理する。	SCM（主：鍵運用） AUM（従：鍵の信頼性） ACM（従：鍵更新の権限）
【14,p.22】構成信頼と更新・復旧（Secure Boot※2／復元性を含む）	更新の途中失敗や改ざんに備え、機器側で自律判定し安全に復帰できる設計（長期運用前提）	宇宙では頻繁に通信が途切れるため、ソフト更新（アップデート）が「途中で止まる」事象が発生する。 更新に失敗することを予め想定し、機器側が自動で「前の正常版に戻る」仕組み（復旧）を組み込む。	SUM（主） AUM（従：アテステーション） ACM（従：更新権限）

※1: OTAR：軌道上で暗号鍵を更新する運用（Over-The-Air Rekeying）
※2: Secure Boot：起動時に改ざんを検知し、不正なソフトウェアの実行を防ぐ仕組み

3．宇宙空間におけるあるべき設計例（認証機能/更新機能）

認証機構（AUM: Authentication Mechanism）の実装例

■ 技術的なポイント：初回接続時の相互認証(1)→アテステーション※(2,3,4)→軽量な認証付き通信(5)



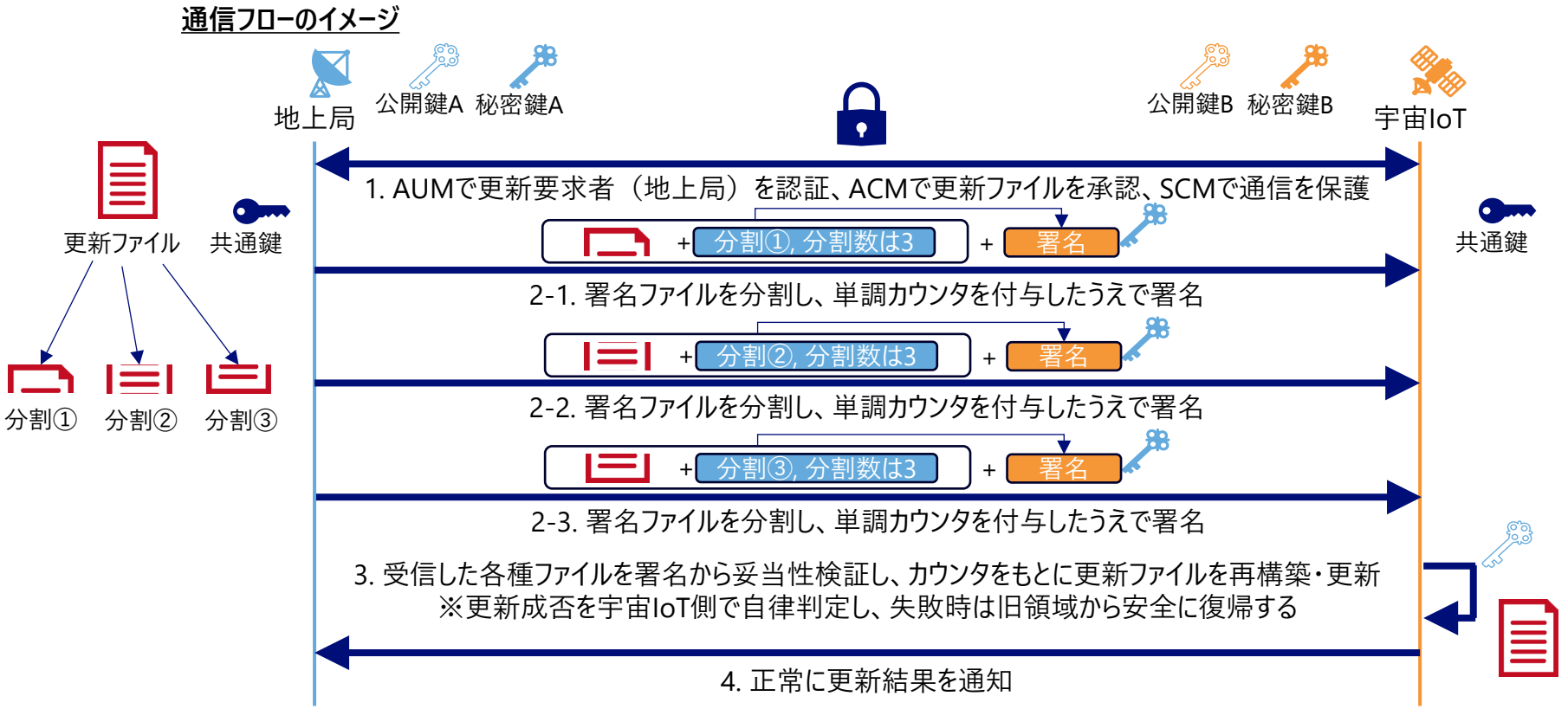
宇宙IoTでは、短い通信機会の中で通信相手の正当性と機器状態の健全性を確認する必要がある。そのため、初回接続時に「相互認証」と「アテステーション」を実施し、その後は軽量な認証付き通信へ移行する設計が重要である

※FWのハッシュ値や重要設定のダイジェストなどに乱数をつけた値に署名して送信することを実施することで、衛星側が健全であることを確認する仕組み

3．宇宙空間におけるあるべき設計例（認証機能/更新機能）

セキュア更新機構（SUM: Secure Update Mechanism）の実装例

■ 技術的なポイント：更新要求者の認証(1) →署名付き分割更新(2) →検証・安全復旧(3,4)



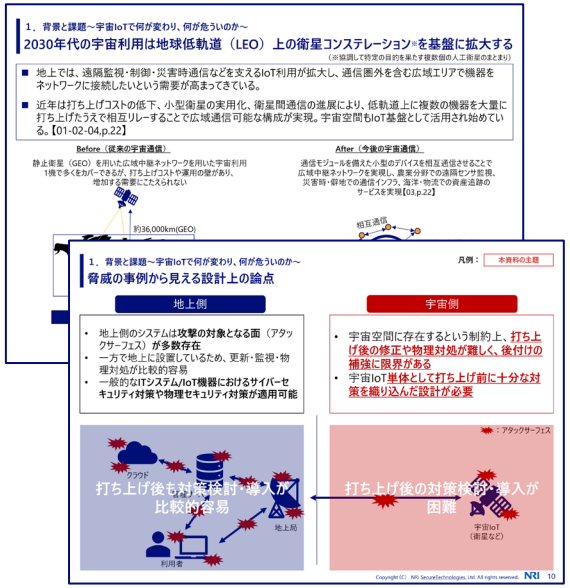
宇宙IoTでは、通信断や短い通信機会のため、更新データを一括で安全に送り切れるとは限らない。そのため、「分割配信できること」だけではなく「各断片の真正性を検証できること」と「途中で更新が失敗した時に元の状態に安全に復帰できること」が設計において重要である。

4．本日の振り返り

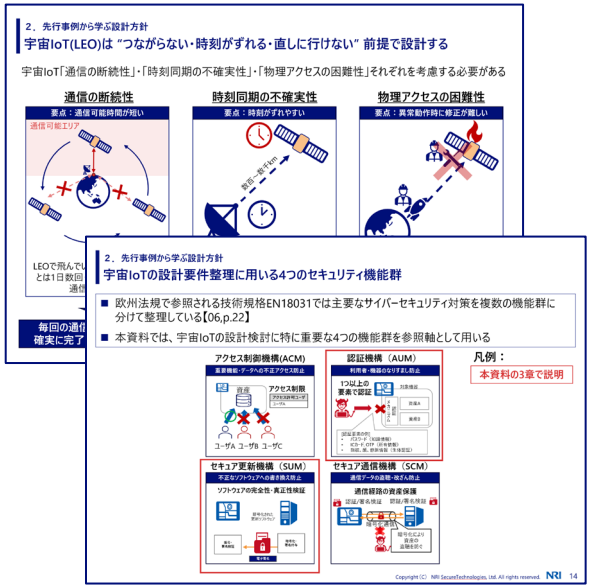
まとめ：宇宙IoTセキュリティ設計の要点

■ ①②③の観点で紹介した通り、宇宙IoTでは、通信断・高遅延・長期運用を前提に、認証・更新・通信保護を一体で設計することが重要である

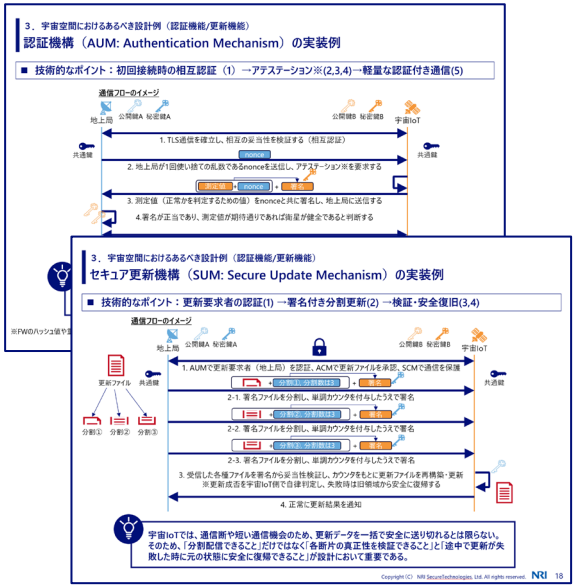
①なぜ必要か？



②何が難しいか？



③どう実装するか？



今後も宇宙IoTの利用は拡大していくことから、地上のIoT製品向け設計・実装概念を、宇宙特有の環境に最適化してセキュリティ対策を検討していく必要がある

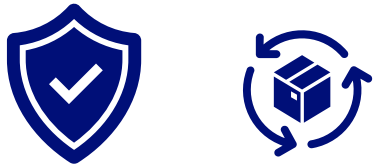
2030年代までの技術的な展望と課題

事業環境の変化

- 世界の宇宙市場規模が1兆ドルを超えて拡大、打ち上げ市場規模：400億ドル超（年平均成長率15%程度）【01,02】
- 低軌道(LEO)衛星ネットワークが拡大し、**地上のIoT機器が宇宙空間のIoT機器に直接接続しての通信**も一般的に

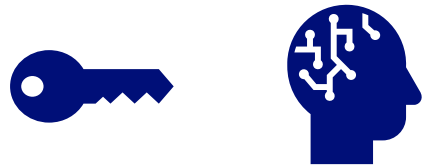
製造業者に求められる実装要求

- **Security by Design**に基づく開発・保守プロセスの組込み
- **脆弱性監視、パッチ供給、インシデント報告**を含む運用体制の整備
- SBOM、設定管理、鍵管理を含む**構成管理の継続運用**
- 規制・標準適合を支える**証跡管理と説明可能性の確保**



中長期の技術課題

- **通信断・高遅延・長寿命運用を前提**とした認証・更新・復旧設計
- 放射線影響や計算資源制約を踏まえた**暗号・鍵管理方式の最適化**
- **宇宙環境を模擬したセキュリティ試験・評価基盤**の整備
- **PQC、AI活用、自律的監視**の導入可能性評価



参考文献

【01】"Space: The $1.8 trillion opportunity for global economic growth", McKinsey&Company, 2024

【02】"Space Launch Services Market Forecasts to 2030 - Global Analysis By Service Type (Pre-launch and Post launch), Payload, Orbit, Launch Vehicle Type, End User and By Geography", Stratistics Market Research Consulting, 2024

【03】"Satellite IoT Market Size & Share 2026 – 2034", Global Market Insight, 2025

【04】"Satellite IoT market growth and outlook: 5 drivers propelling the market to $4.7 billion by 2030", Kalpesh Baviskar, IoT Analytics, 2025

【05】"Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," European Union, 2024

【06】"Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," European Union, 2022

【07】"Proposal for a Regulation of the European Parliament and of the Council on the safety, resilience and sustainability of space activities in the Union (EU Space Act)," European Commission,

【08】"Common security requirements for radio equipments - Part 1-3 (EN 18031series)," CENELEC, 2024

【09】"NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation," Jonathan Greig, 2022

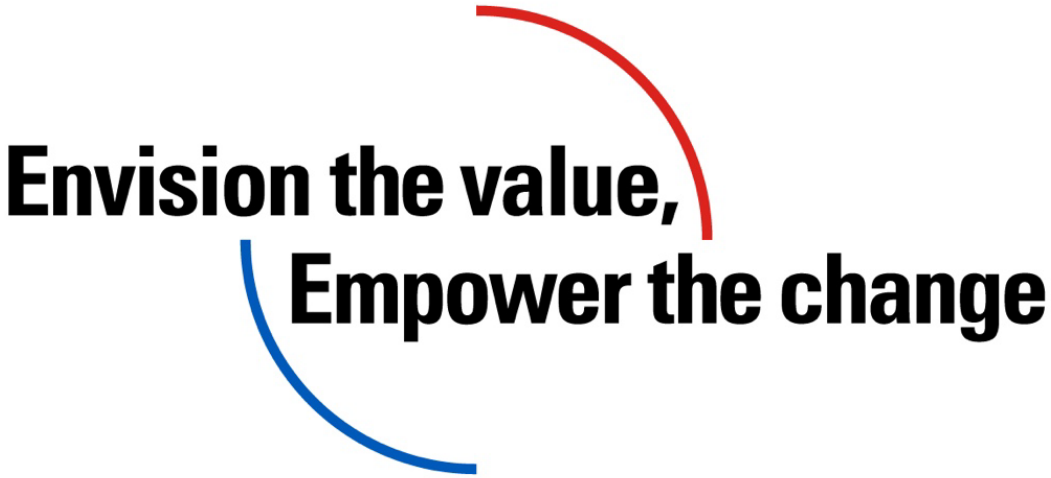
【10】"NASA spacecraft were vulnerable to hacking for 3 years and nobody knew. AI found and fixed the flaw in 4 days," Tereza Pultarova, 2025

【11】"Recommendation for Space Data System Standards - Space Data Link Security Protocol - Recommended Standard - CCSDS 355.0-B-2 - Blue book," CCSDS, 2022

【12】"Draft Report Concerning Space Data System Standards - Space Data Link Security Protocol – Summary of Concept and Rationale - Informational Standard - CCSDS 350.5-G-2 - Green book," CCSDS, 2024

【13】"STARLINK WELCOMES SECURITY RESEARCHERS (BRING ON THE BUGS)," SpaceX, 2022

【14】"7.22 – Space Security: Best Practices Guide(BPG)," NASA, 2023


Envision the value,
Empower the change