資料２

経済産業省

# 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版

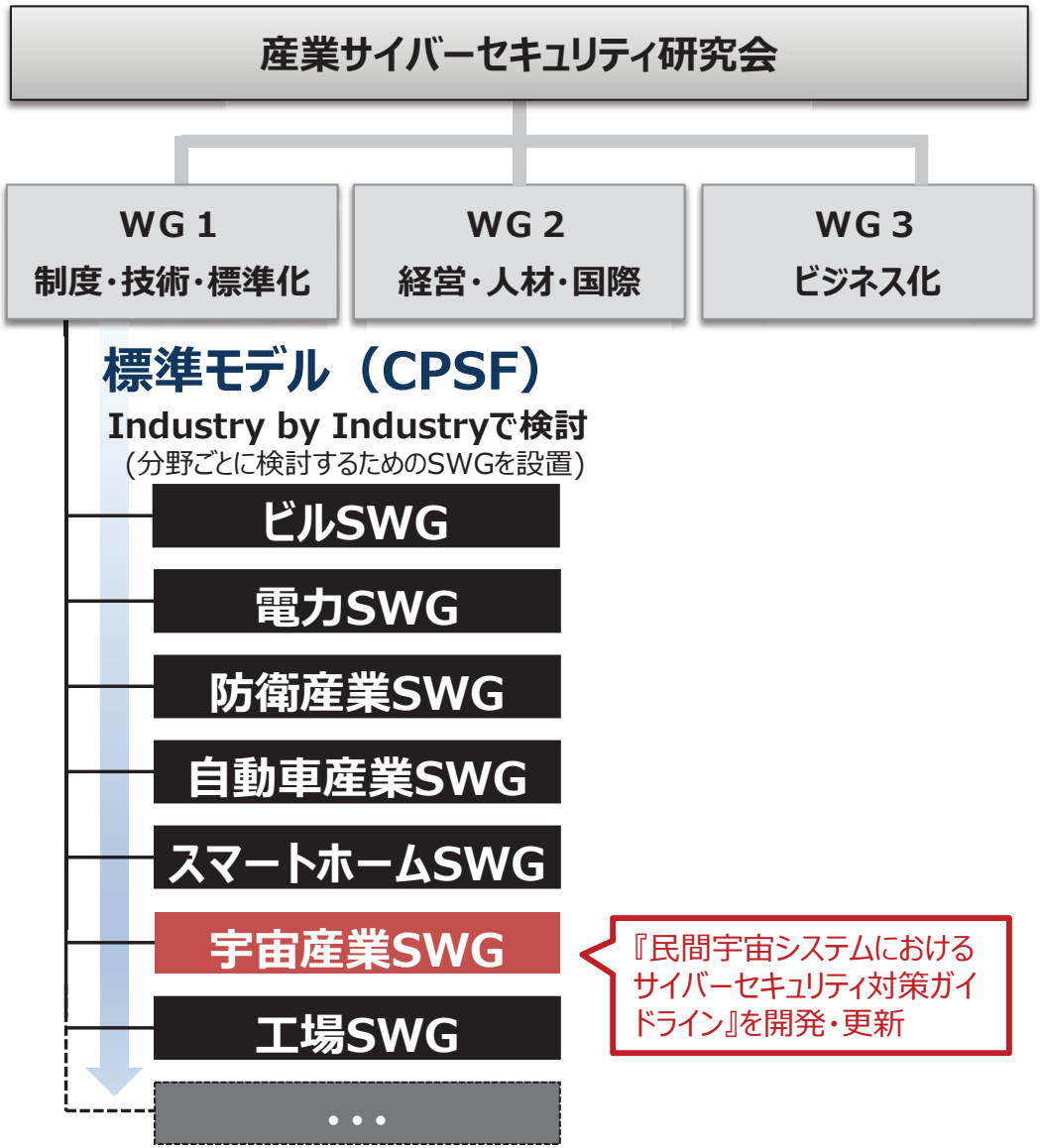
## 概要資料

令和４年４月

経済産業省 製造産業局 宇宙産業室

# 民間宇宙システムにおけるサイバーセキュリティ対策の推進体制

- 経済産業省では、産業サイバーセキュリティ研究会の下、産業分野別のセキュリティ対策の具体化・実装を推進中。**2021年1月、新たに「宇宙産業SWG」を新設し、ガイドラインを開発中。**




| 有識者 | 所属（2022年2月現在） | 宇宙産業SWG | 宇宙産業SWG作業部会 |
|---|---|---|---|
| 鹿志村 修 | 一般財団法人宇宙システム開発利用推進機構 | ● | |
| 小山 浩 | 三菱電機株式会社 電子システム事業本部 | ● | |
| 片岡 晴彦 | 株式会社IHI | ● | |
| 木下 仁 | 独立行政法人情報処理推進機構セキュリティセンター | ● | ● |
| 菜原 聡文 | 東北大学大学院工学研究科航空宇宙工学専攻 | ● | |
| 坂下 哲也 | 一般財団法人 日本情報経済社会推進協会 常務理事 | ● | |
| 佐々木 弘志 | フォーティネットジャパン株式会社OTビジネス開発部部長 | ● | ● |
| 名和 利男 | 株式会社サイバーディフェンス研究所 | ● | |
| 丸山 満彦 | PwCコンサルティング合同会社 | ● | |
| 満永 拓邦 | 東洋大学情報連携学部情報連携学科 | ● | |
| 吉松 健三 | 技術研究組合制御システムセキュリティセンター | ● | ● |
| 栗津 昂規 | スカイゲートテクノロジズ株式会社 | | ● |
| 上杉 謙二 | PwCコンサルティング合同会社 | | ● |
| 永島 隆 | 株式会社アクセルスペース | | ● |
| 小出 祐輔 | 株式会社Synspective | | ● |
| 田中 洋吏 | 三菱電機株式会社電子システム事業本部 | | ● |
| 濱田 剛 | 株式会社スペースエッジラボ | | ● |
| 平松 敏史 | 株式会社パスコ衛星事業部 | | ● |
| 三好 弘晃 | 日本電気株式会社社会基盤ビジネスユニット | | ● |

# 民間宇宙システムにおけるサイバーセキュリティ対策ガイドラインβ版　目次

# 本ガイドライン開発の背景・目的

本文の1.1節

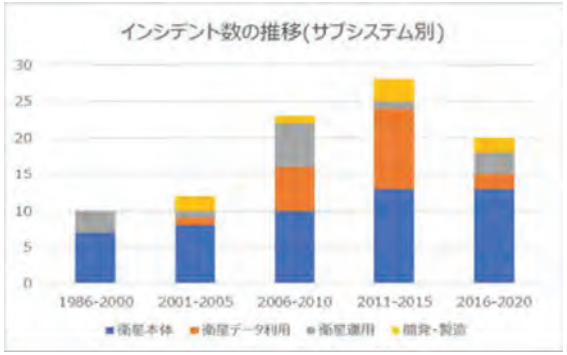
- 我が国の安全保障や経済社会における民間宇宙システムの役割が増大する一方で、宇宙システムにおけるデジタル技術の浸透、ネットワークの複雑化等から、セキュリティ上の脆弱性も増大。
- 欧米では宇宙システムのセキュリティ対策が進められており、我が国においても対応が必要。

## ●宇宙システムのセキュリティ確保が重要かつ困難となってきている要因

- 我が国の安全保障や経済社会における**宇宙システムの役割の増大**
- 宇宙システムの省人化・自動化・クラウド利用の増加等、**デジタル技術の浸透**
- 衛星間通信の増加、衛星と地上通信網との接続等、**ネットワークの複雑化**
- 衛星のコンステレーション化等による、衛星数・地上局数・データ**量の増大**
- 宇宙システムに関する技術の民間開放・民生技術の取り込みに伴う**ステークホルダーの多様化・サプライチェーンの複雑化**

## ●宇宙システムにおけるインシデントの増加

- 1986年～2020年：**国内外で90件以上のセキュリティインシデントが発生**
- 2017年から2020年：米国航空宇宙局では、フィッシング、マルウェア等のサイバー攻撃を6,000件以上検知




## ●欧米における宇宙システムのセキュリティ対策の取組

- 2019.4 米国：官民によるSpace ISAC設立 【民間、NASA、米国宇宙軍、国家偵察局】
- 2020.5 英国：宇宙業界製品サプライヤー向けに“Cyber Security Toolkit ver2” 発行 【英国宇宙局】
- 2020.9 米国：**大統領令SPD-5“宇宙システムにおけるサイバーセキュリティ原則”発行**
- 2021.6 米国：**民間衛星向けのサイバーセキュリティ対策のガイドラインのドラフト版発行 【NIST】**

## ●ガイドライン開発の目的

**民間宇宙事業者のビジネス振興及びサイバー攻撃による倒産等の経営リスク軽減の観点**から、

- 宇宙システムに係るセキュリティ上のリスク
- 宇宙システムに関わる各ステークホルダーが検討すべき基本的セキュリティ対策
- 対策の検討に当たり参考になる参考文献、活用可能な既存施策 等

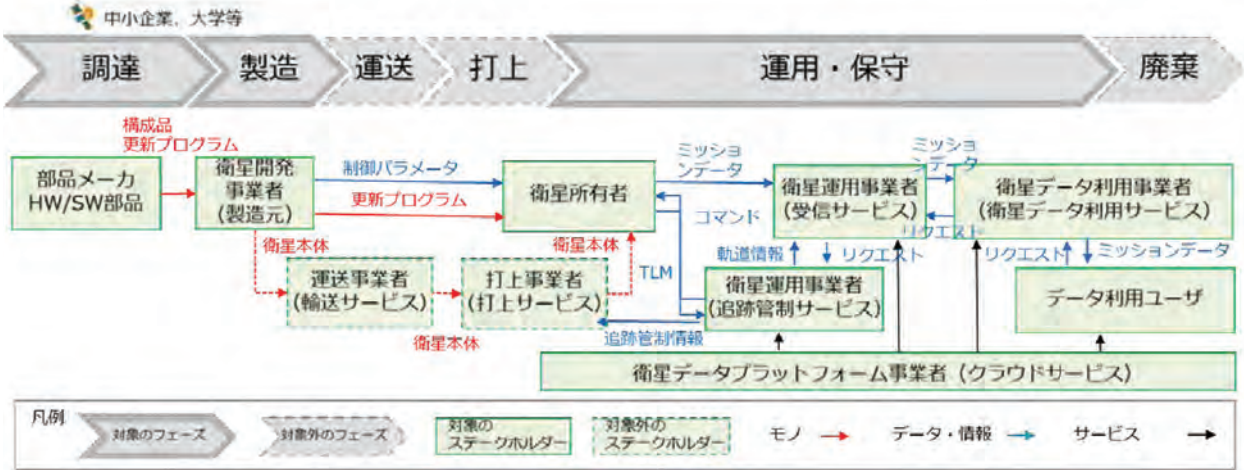
について分かりやすく整理して示し、**民間事業者における自主的な対策を促すことを目的**とする

# 本ガイドラインの対象範囲

本文の1.2節

- 民間企業が主体となる衛星システム及び地上システムを分析対象としている。
- 衛星システムは設計・開発・製造、運用・保守、廃棄フェーズを対象とし、地上システムは運用・保守フェーズを主な対象としている。
- ガイドラインの対象範囲は、随時更新することとする。

**衛星のライフサイクルとステークホルダーの関係の概観**




宇宙システムの全体

| 宇宙システム | | | 国主体 | 民間主体 |
|---|---|---|---|---|
| 輸送システム | 輸送機 | ロケット | ○ | — |
| 有人システム | 宇宙ステーション | 実験棟等 | ○ | — |
| 衛星システム | 探査機 | 月探査機、惑星探査機等 | ○ | — |
| | 補給機 | 物資補給機 | ○ | — |
| | 人工衛星 | 測位衛星 | ○ | — |
| | | 気象衛星 | ○ | ○ |
| | | 通信衛星 | ○ | ○ |
| | | 放送衛星 | — | ○ |
| | | 観測衛星 | ○ | ○ |
| 地上システム | 衛星運用設備 | 追跡管制局、受信局、ミッションコントロールシステム等 | ○ | ○ |
| | 衛星データ利用設備 | データ処理システム、観測受付・データ配布処理等 | ○ | ○ |
| | 打上設備 | 射場、打上管制設備等 | ○ | ○ |
| | 開発・製造設備 | OTシステム（FAシステム等） | ○ | ○ |
| | | ITシステム（OAシステム等） | ○ | ○ |

本ガイドラインの分析対象

| 民間宇宙システム | | ライフサイクルにおける対象とするフェーズ | | | |
|---|---|---|---|---|---|
| | | 設計・開発・製造 | 打上 | 運用・保守 | 廃棄 |
| 人工衛星 | 観測衛星 | ○ | — | ○ | ○ |
| 衛星運用設備 | 追跡管制局、受信局、ミッションコントロールシステム等 | — | — | ○ | ○ |
| 衛星データ利用設備 | データ処理システム、観測受付・データ配布処理等 | — | — | ○ | ○ |
| 打上設備 | 射場、打上管制設備等 | — | — | — | — |
| 開発・製造設備 | OTシステム（FAシステム等） | ○ | — | ○ | ○ |
| | ITシステム（OAシステム等） | ○ | — | ○ | ○ |

※設計・開発・製造フェーズには運送・据付調整・試験を含むが分析対象外とする。

# 本ガイドラインの構成及び想定読者

本文の1.2節

- ガイドラインは以下のような利用を想定している。
  - 宇宙産業に関わる事業者：自社のサイバーセキュリティ対策の参考として利用
  - 調達者（政府・自治体・企業等）：宇宙システムを調達する際に、基本的なサイバーセキュリティ対策を満たす事業者であるかどうかの確認等に利用

| | 経営層 | 衛星所有者 | 衛星運用事業者* | 衛星データプラットフォーム事業者 | 衛星データ利用サービス事業者 | 衛星開発事業者 |
|---|---|---|---|---|---|---|
| 1．はじめに | | | | | | |
| 1．1本ガイドライン作成の背景・目的 | ★ | ★ | ★ | ★ | ★ | ★ |
| 1．2本ガイドラインの対象範囲 | | | | | | |
| 1．3本ガイドラインの構成及び想定読者 | | | | | | |
| 2．宇宙システムを取り巻くセキュリティに係る状況 | | | | | | |
| 2．1インシデント事例 | ★ | ★ | ★ | ★ | ★ | ★ |
| 2．2民間宇宙システムにおけるセキュリティリスクの考え方 | | | | | | |
| 3．民間宇宙システムにおけるセキュリティ対策のポイント | | | | | | |
| 3．1共通的対策 | | ★ | ★ | ★ | ★ | ★ |
| 3．2宇宙システム特有の対策 | | | | | | |
| 3．2．1法令上求められる対策 | | ★ | ★ | ★ | ★ | ★ |
| 3．2．2衛星本体 | | ★ | ★ | | | ★ |
| 3．2．4衛星データ利用設備 | | | ★ | ★ | | ★ |
| 3．2．4衛星データ利用設備 | | | ★ | ★ | ★ | |
| 3．2．5開発・製造設備 | | | ★ | | | ★ |

＊：追跡管制局サービス又は受信局サービスを提供する地上局サービス事業者を含む。

# インシデント事例

本文の1.2節

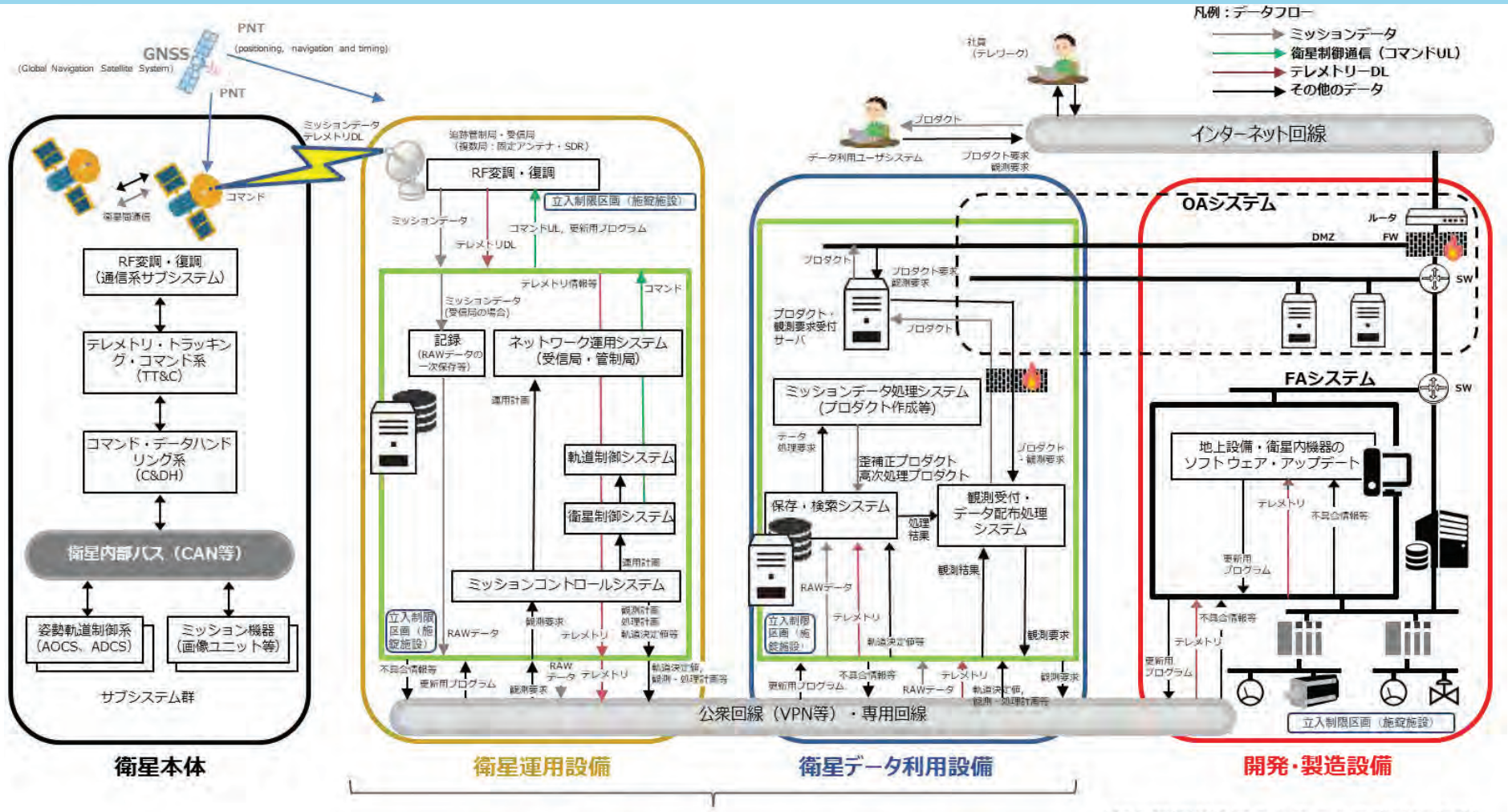
- 宇宙分野では1986～2021年に国内外で90件以上のセキュリティインシデントが発生。
- 以下は事例の一部。

| 年 | 対象 | 影響 | 概要 |
|---|---|---|---|
| 2008 | NASA<br>Terra 衛星 | 衛星が制御不能に | NASAの地球観測衛星Terraに対して干渉があり、数分間制御不能に。2008年の6月と10月に２回発生。米議会への報告書では商用の地上局が侵入口であった可能性が示された。（ノルウェーのKSAT社はこれを否定） |
| 2014 | NOAA<br>気象観測NW | 衛星データが閲覧不能に | 海洋大気庁（NOAA）の気象観測衛星ネットワークがインターネット経由でサイバー攻撃を受けた。 |
| 2015 | イリジウム<br>通信衛星 | 通信内容が見られる状態に | イリジウム通信衛星のページャ通信データが暗号化されていないという脆弱性が指摘された。<br>国際会議Chaos Communication Camp 2015では実際に、市販（計€50程度）のアンテナ等でイリジウム通信衛星のページャ通信データを解析・解読し、クリアテキスト情報（平文）に変換する操作のプレゼンがあった。 |
| 2018 | NASA<br>ジェット推進研究所（JPL） | ミッションデータの漏えい | 職員が無許可設置したRaspberry Piを侵入口としてJPLのネットワークに不正侵入し、複数システム間を横移動。およそ10か月に渡って内部活動があり、合計23ファイル、500MBの情報が抜き取られた。 |
| 2020 | 静止軌道上の<br>18機の通信衛星 | インターネット通信の盗聴 | 国際会議BlackHatで、静止軌道上の通信用衛星18機からの電波を市販（計$300程度）のアンテナ等で受信し、通信データを分析したところ、18機すべてで暗号がかけられずに通信が行われ、機密情報が見られる状態になっていたとのプレゼンがあった。危険物に関する情報、風力発電所の管理者権限情報、機微な個人情報（パスポート番号やクレジットカードデータ等）等が見られる状態になっていた。 |

# ガイドラインにおける民間宇宙システムの標準的なモデル

本文の2.2節

- 超小型観測衛星を分析対象として民間宇宙システムの全体像を整理し、以下の標準的なモデルを作成した。




（超小型観測衛星のシステムを念頭に作成）

**機能の一部または全部をクラウドで運用するケースが増加中**

<組織>
・衛星開発・運用事業者 等

<組織>
・衛星開発・運用事業者
・地上局サービス事業者 等

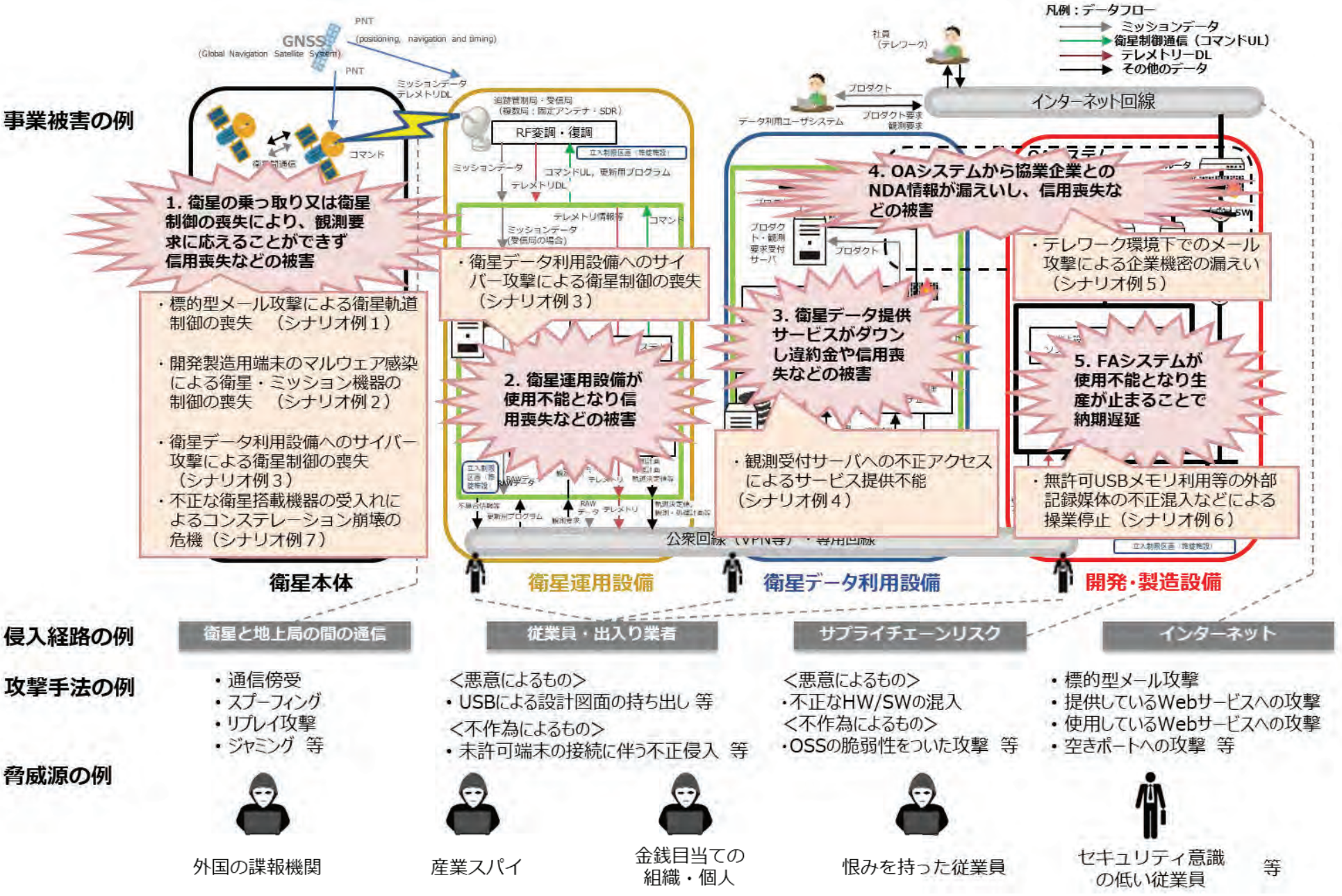
<組織>
・衛星開発・運用事業者
・衛星データプラットフォーム事業者
・衛星データ利用サービス事業者 等

<組織>
・衛星開発・運用事業者 等

# リスクシナリオの検討

本文の2.2節

- 前項の標準モデルを踏まえて、7種類のリスクシナリオを検討した。



# サブシステムごとの主な対策

本文の2.2節

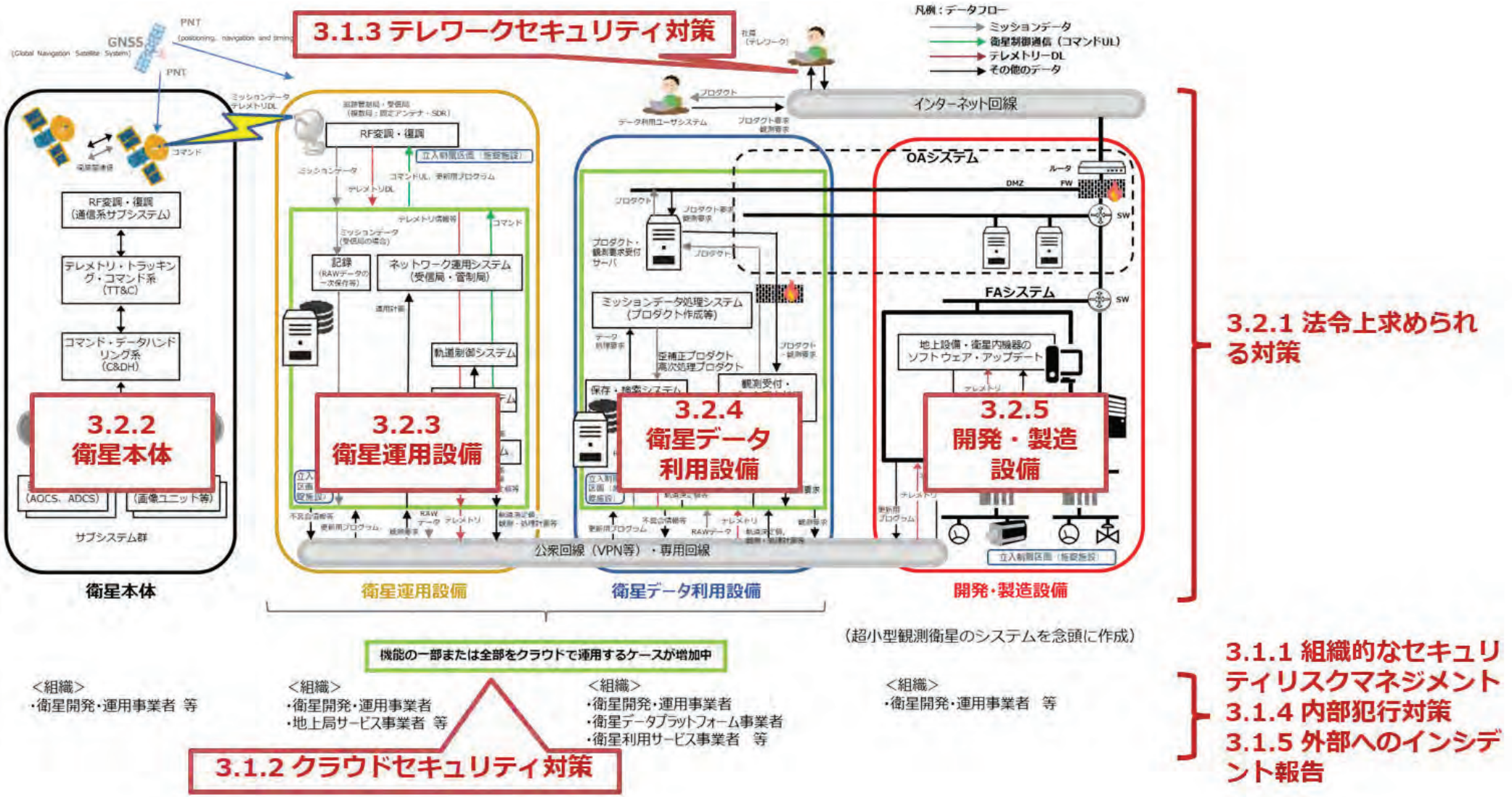
- 前項のリスクシナリオを踏まえて、サブシステムごとの主な対策を検討した。

| No. | 大きな事業被害をもたらすリスクシナリオの例 | 主な対策 | | | | |
|---|---|---|---|---|---|---|
| | | 衛星本体 | 衛星運用設備 | 衛星データ利用設備 | ＯＡシステム | 開発・製造設備 |
| 例１ | OA環境の社員端末が標的型メール攻撃を受けてマルウエアに感染。インターネット経由のリモートアクセスにより姿勢制御やミッション機器制御に係る機密情報が窃取される。その後、衛星本体のアップリンクデータが乗っ取られ、窃取情報を使った不正コマンドが衛星に送られ、一時的に衛星の軌道制御を喪失する。 | RF通信における送受信データの完全性・暗号化 | RF通信における送受信データの完全性・暗号化 | － | 従業員に対するサイバーセキュリティの教育・演習の実施 | － |
| 例２ | 衛星本体のソフトウエア更新に使われる開発・製造用の端末（OAと兼用）がマルウエア感染したため、更新用プログラムに不正プログラム（バックドア）が埋め込まれ、地上からの遠隔操作により、正常な衛星の制御またはミッション機器の制御ができなくなる。 | 更新プログラム等の事前検証・脆弱性対策※<br>（※打上げ後のため、実際には開発・製造設備にて実施） | － | － | 従業員に対するサイバーセキュリティの教育・演習の実施 | ・情報システムと制御システムの分離 |
| 例３ | 衛星データ利用設備に設置された無許可端末がインターネット経由でサイバー攻撃を受け、設備内部へのインターネット側からの攻撃の起点となった結果、衛星運用を行う地上のインフラシステムを含めた各種サーバがダウンし、長期間にわたり衛星の制御を失う。 | 複数の通信経路等確保 | 設備の脆弱性対策 | 設備の脆弱性対策 | ・シャドーITを利用させない対策<br>・情報システムのIT資産管理・構成管理・パッチ管理 | － |
| 例４ | 観測受付サーバがインターネット経由で不正アクセスを受けてランサムウェアに感染。その後、クラウド環境の設定不備により設備内の全サーバ及び端末に感染し、起動に必要なシステムデータが消去されたために再起動できなくなり、サービスを提供できなくなる。 | － | － | ・セキュア開発の実施<br>・クラウド等外部サービス利用 | ・重要業務を行うサーバ等の技術的防御<br>・サイバー攻撃を検知した際のインシデント対応 | － |
| 例５ | テレワーク実施中、同僚からのメール（実際は、普段、オフィスで隣に座る同僚を装った差出人詐称メール）の添付ファイルを開き、マルウエアに感染。インターネット経由のリモートアクセスにより衛星製造に関わる企業機密が窃取され、外部に漏えいする。 | － | － | － | ・従業員に対するサイバーセキュリティの教育・演習の実施<br>・端末やネットワークのログの収集・分析 | － |
| 例６ | 製造設備コントローラに対し、許可されていない私物のUSBメモリを使って設定変更を行ったため、USBメモリ内のマルウェアによって設定やプログラムが改ざんされ、設備の制御が異常となり操業が停止する。 | － | － | － | － | ・無許可USBメモリの使用禁止<br>・ホワイトリスト型マルウエア対策 |
| 例７ | 衛星搭載機器調達の際、不正な基板であることに気づかずに受入れて衛星群に搭載。打ち上げ後の特定条件成立によりロジックボムが起動し、コンステレーションが崩壊の危機に直面する。 | － | － | － | － | ・部品受入検査の徹底・精度向上 |
| サブシステムごとの主な対策のまとめ | | ・RF通信における送受信データの完全性・暗号化（3.2.2）<br>・更新プログラム等の事前検証・脆弱性対策（3.2.2）<br>・複数の通信経路等確保（3.2.2） | ・RF通信における送受信データの完全性・暗号化（3.2.3）<br>・設備の脆弱性対策（3.2.3） | ・設備の脆弱性対策（3.2.4）<br>・セキュア開発の実施（3.2.4）<br>・外部サービス利用（3.1.2、3.2.1） | ・一般的なセキュリティ対策（3.1）<br>・インシデント報告（3.1.5） | ・サプライチェーンに対するセキュリティ対策　（3.2.2）<br>・一般的な制御システムセキュリティ対策（3.2.5） |

# 民間宇宙システムにおけるセキュリティ対策のポイント①

本文の3章

- 前項の主な対策を踏まえて、民間宇宙システムにおけるセキュリティ対策のポイントを整理した。



# 民間宇宙システムにおけるセキュリティ対策のポイント②

本文の3章

・要求事項は、明示されている各ステークホルダーが検討し取り組むべき事項を示す。
・基本対策事項は、要求事項を満たすため、一般的に普及しており、取り組むことが推奨される実践や対策の例を示す。
・更なるセキュリティの向上が見込めるが、一定の予算や組織体制・人員が整備されていないと実施が困難な、高度な実践や対策の例については、「高いセキュリティレベルが求められる場合」との条件付きで示す。

| 章節 | 項目名 | 取り組むべき事項、または取り組むことが推奨されるレベルの区分け | 内容 | 衛星所有者 | 衛星運用事業者* | 衛星データプラットフォーム事業者 | 衛星データ利用サービス事業者 | 衛星開発事業者 |
|---|---|---|---|---|---|---|---|---|
| 3.1 | 共通的対策 | | | | | | | |
| 3.1.1 | 組織的なセキュリティリスクマネジメント | 要求事項 | 経営者のリーダーシップのもと、サイバーセキュリティリスクの管理体制を構築し、自社のサイバーセキュリティリスクの特定、防御、検知、対応及び復旧を含めた対策を実装すること。 | ● | ● | ● | ● | ● |
| | | 基本対策事項 | (1)サイバーセキュリティ管理体制の構築、自社のサイバーセキュリティリスクの特定、対策の実装に当たっては、対策の実効性の確保や抜け漏れを防ぐ観点から、以下の(a)から(e)を含む既存の基準や枠組み等の活用が望ましい。<br>(a)中小企業の情報セキュリティ対策ガイドライン第3版（IPA）<br>(b)サイバーセキュリティ経営ガイドラインVer2.0（経済産業省、IPA）<br>(c)ISO/IEC 27001（情報セキュリティマネジメントシステム）<br>(d)Cybersecurity Framework Ver1.1（NIST）<br>(e)SP 800-171（NIST） | ● | ● | ● | ● | ● |
| 3.1.2 | クラウドセキュリティ対策 | 要求事項 | 外部サービスを活用する場合、法令、ミッション等に適したセキュリティ要件やサービスレベルアグリーメント（SLA）に対応するサービスを選定すること。 | ● | ● | ● | ● | ● |
| | | 基本対策事項 | (1)宇宙産業について外部サービスに関連する主要な法令には以下があり、法令の遵守状況を確認し、サービスを選定すること。<br>(a)衛星リモートセンシング記録の適正な取扱いの確保に関する法律施行規則<br>(2)宇宙産業について外部サービスに関連する主要な認証には以下の(a)～(c)があり、適切なセキュリティレベルのサービスを選定すること。<br>(a)ISO/IEC 27017 ISO/IEC 27002に基づくクラウドサービスサービスのための情報セキュリティ管理策の実践の規範（ISO/IEC）<br>(b)政府情報システムのためのセキュリティ評価制度（ISMAP）（内閣官房・総務省・経済産業省）<br>(c)米国連邦リスク承認管理プログラム（FedRAMP） | ● | ● | ● | ● | ● |
| 3.1.3 | テレワークセキュリティ対策 | 要求事項 | テレワークを実施する際は、テレワーク環境の整備及び規定の整理をし、安全な運用を行うこと。 | ● | ● | ● | ● | ● |
| | | 基本対策事項 | (1)テレワークの安全な運用に当たっては、以下の(a)及び(b)を含む既存のガイドライン等の活用が望ましい。<br>(a)テレワークセキュリティガイドライン（第５版）（総務省）<br>(b)中小企業等担当者向けテレワークセキュリティ手引き（チェックリスト）第２版（総務省） | ● | ● | ● | ● | ● |
| 3.1.4 | 内部犯行対策 | 要求事項 | 内部不正の防止や早期発見ができるよう対策を検討すること。 | ● | ● | ● | ● | ● |
| | | 基本対策事項 | (1)内部不正への対応に当たって、以下の(a)を含む既存の基準等の活用が望ましい。<br>(a)組織における内部不正防止ガイドライン（第4版）（経済産業省、IPA） | ● | ● | ● | ● | ● |
| 3.1.5 | 外部へのインシデント報告 | 要求事項 | 不具合等を含むインシデントが発生した際、必要に応じ、外部の組織に報告すること。 | ● | ● | ● | ● | ● |
| | | 基本対策事項 | (1)宇宙システムにおいてインシデントが発生した場合等、管轄省庁等への届出、影響が出る組織・個人への通知等の対応が求められることがある。このため、表を参考に、インシデント時に報告が必要となるステークホルダーを確認し、連絡フローを整理しておくことが望ましい。 | ● | ● | ● | ● | ● |

＊：追跡管制局サービス又は受信局サービスを提供する地上局サービス事業者を含む。

# 民間宇宙システムにおけるセキュリティ対策のポイント③

本文の3章

・要求事項は、明示されている各ステークホルダーが検討し取り組むべき事項を示す。
・基本対策事項は、要求事項を満たすため、一般的に普及しており、取り組むことが推奨される実践や対策の例を示す。
・更なるセキュリティの向上が見込めるが、一定の予算や組織体制・人員が整備されていないと実施が困難な、高度な実践や対策の例については、「高いセキュリティレベルが求められる場合」との条件付きで示す。

| 章節 | 項目名 | 取り組むべき事項、または取り組むことが推奨されるレベルの区分け | 内容 | 衛星所有者 | 衛星運用事業者* | 衛星データプラットフォーム事業者 | 衛星データ利用サービス事業者 | 衛星開発事業者 |
|---|---|---|---|---|---|---|---|---|
| 3.2 | 宇宙システム特有の対策 | | | | | | | |
| 3.2.1 | 法令上求められる対策 | 要求事項 | (1)関連する法令を遵守し、ライフサイクル全体を通して、適切な対応を行うこと。安全な宇宙の利活用を促進するため、宇宙産業に関連する以下の(a)から(c)の主要な法令に準拠することが求められる。<br>(a)人工衛星等の打上げ及び人工衛星の管理に関する法律<br>(b)衛星リモートセンシング記録の適正な取扱いの確保に関する法律<br>(c)外国為替及び外国貿易法 | ● | ● | ● | ● | ● |
| 3.2.2 | 衛星本体 | 要求事項 | 衛星システム（本体及びRF通信）に対するサイバーセキュリティ対策を講じること。 | ● | ● | ― | ― | ● |
| | | 基本対策事項 | ― | ― | ― | ― | ― | ― |
| | | 高いセキュリティレベルが求められる場合の基本対策事項 | (1)高いセキュリティレベルが求められる場合、以下の(a)から(f)の対策を実施することが望ましい。<br>(a) RF通信の保護　(b) RF通信のジャミング対策<br>(c) 衛星実装機能の事前検証(d) 衛星搭載機器の脆弱性対策<br>(e) 送受信データの完全性　(f) サプライチェーンに対するセキュリティ対策 | ● | ● | ― | ― | ● |
| 3.2.3 | 衛星運用設備 | 要求事項 | 衛星運用設備（追跡管制局、受信局、ネットワーク運用システム、ミッションコントロールシステム（衛星制御システム、軌道制御システムを含む））に対するサイバーセキュリティ対策を講じること。 | ― | ● | ● | ― | ● |
| | | 基本対策事項 | ― | ― | ― | ― | ― | ― |
| | | 高いセキュリティレベルが求められる場合の基本対策事項 | (1)高いセキュリティレベルが求められる場合、以下の(a)から(h)の対策を実施することが望ましい。<br>(a) 設備の保護　(b) 通信の保護　(c) ジャミング対策　(d) データの保護<br>(e) 設備の検証と設備の脆弱性対策(f) 送受信データの完全性の確保<br>(g) 外部サービスの利用　(h) セキュアコーディング | ― | ● | ● | ― | ● |
| 3.2.4 | 衛星データ利用設備 | 要求事項 | 衛星データ利用設備に対するサイバーセキュリティ対策を講じること。 | ― | ― | ● | ● | ― |
| | | 基本対策事項 | ― | ― | ― | ― | ― | ― |
| | | 高いセキュリティレベルが求められる場合の基本対策事項 | (1)高いセキュリティレベルが求められる場合、以下の(a)から(f)の対策を実施することが望ましい。<br>(a) 設備の保護 (b) データの保護 (c) 設備の検証と設備の脆弱性対策<br>(d) 受信データの完全性の確保　(e) 外部サービスの利用　(f) セキュアコーディング | ― | ― | ● | ● | ― |
| 3.2.5 | 開発・製造設備 | 要求事項 | 衛星の開発・製造設備に対するサイバーセキュリティ対策を講じること。 | ― | ●** | ― | ― | ● |
| | | 基本対策事項 | ― | ― | ― | ― | ― | ― |
| | | 高いセキュリティレベルが求められる場合の基本対策事項 | ― | ― | ― | ― | ― | ― |

＊：追跡管制局サービス又は受信局サービスを提供する地上局サービス事業者を含む。

**：地上局サービス事業者は対象外