

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 Ver 2.0

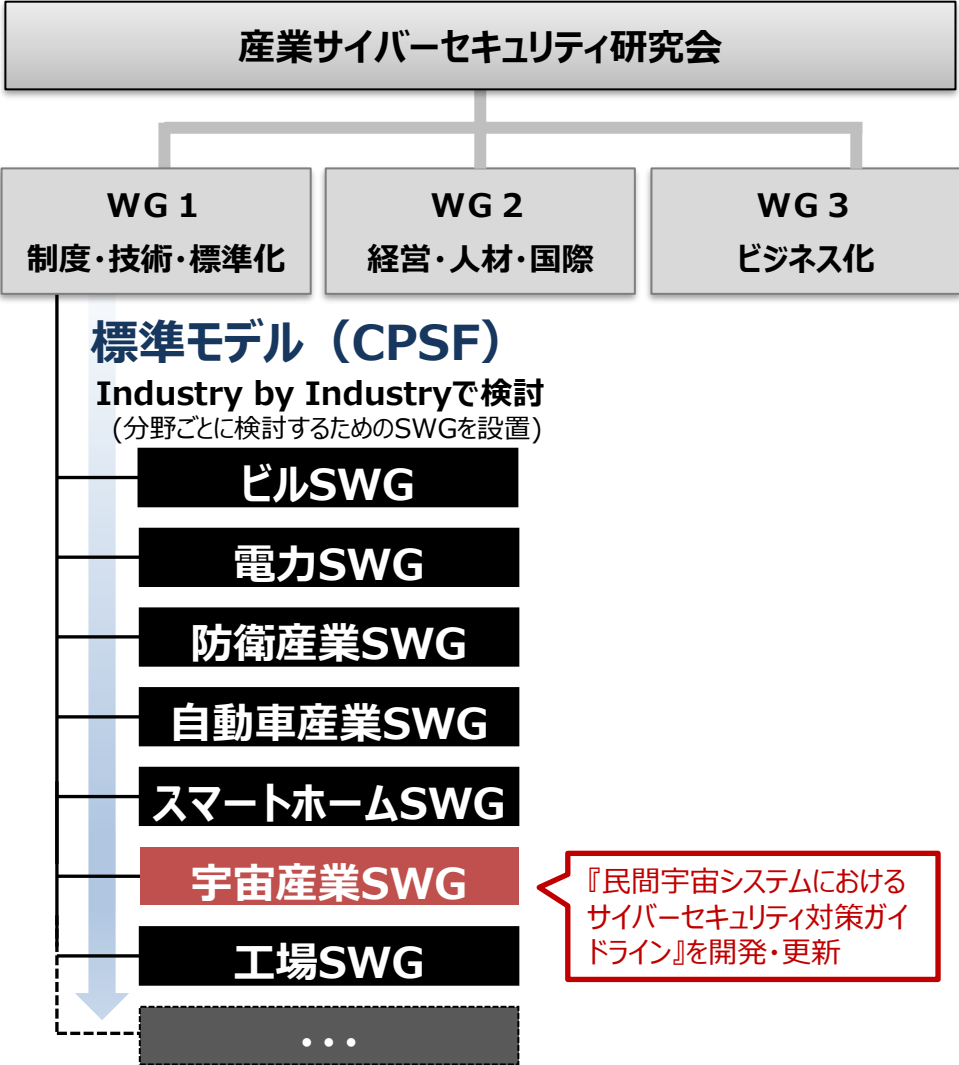
概要資料

令和6年3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、「宇宙産業SWG」を新設し、ガイドラインを開発。



有識者	所属（2024年3月時点）	宇宙産業SWG	宇宙産業SWG作業部会
安達 昌紀	一般財団法人宇宙システム開発利用推進機構（JSS）	●	
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（IPA）セキュリティセンター	●	●
栗原 聡文	東北大学大学院工学研究科航空宇宙工学専攻	●	
小山 浩	三菱電機株式会社 電子システム事業本部	●	
坂下 哲也	一般財団法人 日本情報経済社会推進協会（JIPDEC）	●	
佐々木 弘志	フォーティネットジャパン合同会社	●	●
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（CSSC）	●	●
粟津 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		●
合田 知善	日本電気株式会社		●
小出 祐輔	株式会社Synspective		●
國母 隆一	株式会社アクセルスペース		●
神宮 健	NRIセキュアテクノロジーズ株式会社		●
鈴木 遼	株式会社アークエッジ・スペース		●
高橋 康夫	三井物産セキュアディレクション株式会社		●
田中 洋吏	三菱電機株式会社		●
多賀 正敏	国立研究開発法人宇宙航空研究開発機構（JAXA）		●
平松 敏史	株式会社パスコ		●

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 目次

本ガイドラインの全体概要.....	1
1. はじめに.....	2
1.1 本ガイドライン作成の背景・目的.....	2
1.2 本ガイドラインの対象範囲.....	7
1.3 本ガイドラインの構成及び想定読者.....	8
1.4 本ガイドラインの利用方法.....	9
2. 宇宙システムを取り巻くセキュリティに係る状況.....	11
2.1 インシデント事例.....	11
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.....	14
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.....	42
3.1 共通的対策.....	46
3.1.1 組織的なセキュリティリスクマネジメント.....	46
3.1.2 クラウドセキュリティ対策.....	57
3.1.3 テレワークセキュリティ対策.....	60
3.1.4 内部犯行対策.....	66
3.1.5 外部へのインシデント報告.....	71
3.2 宇宙システム特有の対策.....	74
3.2.1 法令上求められる対策.....	74
3.2.2 衛星本体.....	82
3.2.3 衛星運用システム.....	99
3.2.4 衛星通信システム・衛星データ利用システム.....	105
3.2.5 開発・製造システム.....	107
4. 付録.....	111
4.1 用語の定義.....	111
4.2 略語集.....	114
4.3 本ガイドライン作成について.....	118

添付資料 1 対策要求事項チェックリスト

添付資料 2 NIST CSFと宇宙システム特有の対策との対応関係

添付資料 3 情報セキュリティ関連規程（サンプル）

本ガイドラインの全体概要

本編

添付資料

記載概要

1. はじめに

- ・ 諸外国における関連施策等に基づき、本ガイドライン作成の背景・目的について記載、
- ・ 本ガイドラインの対象範囲、構成及び想定読者、利用方法について記載

2. 宇宙システムを取り巻くセキュリティに係る状況

- ・ 宇宙システムに関するインシデント事例を記載
- ・ 本ガイドラインで扱う民間宇宙システムの標準モデルを示すとともに、当該モデルに基づき、民間宇宙システムに想定される13のリスクシナリオを例示

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

- ・ 宇宙システムに関係する全組織に関わる「共通的対策」と、各サブシステムで求められる「宇宙システム特有の対策」に分け、各ステークホルダーが検討し取り組むべきセキュリティ対策を記載
- ・ 各対策について、取り組むべき事項を示した「要求事項」、要求事項を満たすために推奨される実践や対策例を示した「基本対策事項」、これらに関する補足説明や参考情報を示した「解説」に分けて整理

4. 付録

- ・ 本ガイドラインで使用する用語の定義や略語集を記載

添付資料1 対策要求事項チェックリスト

- ・ 3.で示した対策要求事項に関するチェックリスト

添付資料2 NIST CSFと宇宙システム特有の対策との対応関係

- ・ 3.で示した「宇宙システム特有の対策」と、NISTのCybersecurity Framework（NIST CSF）のフレームワークにおけるサブカテゴリーとの対応関係を整理

添付資料3 情報セキュリティ関連規程（サンプル）

- ・ 民間宇宙事業者の情報セキュリティに関する社内関連規程の雛形であり、IPAの既存雛形に対して、宇宙事業者特有の内容を追記し、整理

利用方法

- ・ 諸外国における関連施策等を確認可能
- ・ 本ガイドラインの対象範囲、構成、利用方法等を確認することで、効果的なガイドラインの利用が可能
- ・ 宇宙システムに関わる近年のインシデント事例を確認可能
- ・ 宇宙システムにおいて重大な事業被害を及ぼし得るリスクシナリオについて、その侵入経路、攻撃手法、脅威源、影響等を確認可能
- ・ 全組織に「共通的対策」や各サブシステムで求められる「宇宙システム特有の対策」の検討・実施時に参照可能
- ・ なお、対策の検討に当たっては、本ガイドラインに記載している対策事項をテラリングすることも可能（複数のステークホルダーで共通的に対策を検討する場合には、当該ステークホルダー間で対策のテラリングについて検討し、合意・承認することが必要）
- ・ 本ガイドラインに記載の用語や略語の意味を確認する際に利用可能
- ・ 要求事項に対する達成度の確認や、セキュリティ対策の検討・見直し時に利用可能
- ・ NIST CSFに対応したセキュリティ対策の検討・実施時の参考情報として利用可能
- ・ 情報セキュリティ関連規程の作成・見直し時に利用可能
- ・ なお、雛形の項目を適宜テラリングした上で利用することが必要

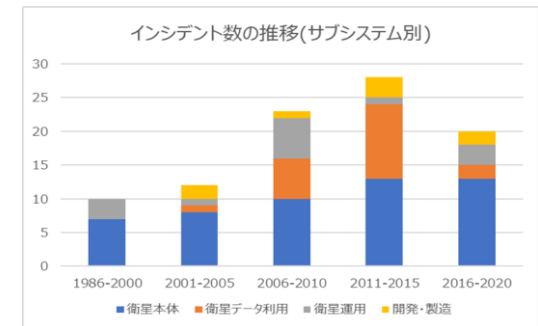
- 我が国の安全保障や経済社会における民間宇宙システムの役割が増大する一方で、宇宙システムにおけるデジタル技術の浸透、ネットワークの複雑化等から、セキュリティ上の懸念も増大している。
- 欧米では宇宙システムのセキュリティ対策が進められており、我が国においても対応が必要である。

● 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た要因

- ・ 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～：
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】
- ・ 2020.9 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
- ・ 2022.12 米国：衛星地上セグメントのためのセキュリティプロファイルに関するガイドラインの発行【NIST】
- ・ 2023.7 米国：商用衛星運用のためのセキュリティ入門書の発行【NIST】
- ・ 2023.9 EU：官民によるEU Space ISACの設立を発表
【民間、研究機関、政府機関、ナショナルCERT等】
- ・ 2024.2 EU：低軌道通信衛星に関するサイバーセキュリティ調査文書の発行【ENISA】

● 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。**

- ## 衛星のライフサイクル・ステークホルダーと本ガイドラインの対象フェーズ



本ガイドラインの構成及び想定読者

本文の1.3節

- 「2. 宇宙システムを取り巻くセキュリティに係る状況」では、宇宙システムを取り巻く過去のインシデント事例や、宇宙システムにおいて想定される主なセキュリティリスクについて整理した。
- 「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」では、宇宙システムに関係する全組織に共通的な対策や、宇宙システム特有の対策を整理した。

目次構成	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	衛星データ利用者／衛星通信利用者	衛星開発事業者
本ガイドラインの全体概要	★	★	★	★	★	★
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						
1.4 本ガイドラインの活用方法						
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 共通的な対策	★	★	★	★	★	★
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	★	★				★
3.2.3 衛星運用システム		★	★			★
3.2.4 衛星通信システム・衛星データ利用システム		★	★	★	★	★
3.2.5 開発・製造システム		★				★

*：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。

【利用者】

- 民間宇宙システムに関わる事業者が、自社のサイバーセキュリティ対策の参考として利用する。
- 政府・自治体・企業等が、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する。

【利用に当たっての留意事項】

- 対策の検討に当たっては、対象システムの特長・重要度、リスク評価結果、事業者のビジネス環境等を踏まえ、本ガイドラインに記載している対策事項をテーリングすることが可能。
- 複数のステークホルダーで共通的に対策を検討する場合には、当該ステークホルダー間で対策のテーリングについて検討し、合意・承認することが必要。
- また、添付資料 1 として対策要求事項を整理したチェックリストを添付しているほか、添付資料 2 としてNIST Cybersecurity Framework (NIST CSF) と宇宙システム特有の対策との対応関係を整理した対照表を掲載しており、対策実施時の参考資料として活用可能。
- 加えて、添付資料 3 として、民間宇宙事業者が社内の情報セキュリティ管理に当たって利用できる情報セキュリティ関連規程の雛形を添付しており、情報セキュリティ関連規程の作成・見直しに当たっての参考資料として活用可能。

宇宙システムにおけるインシデント事例

本文の2.1節

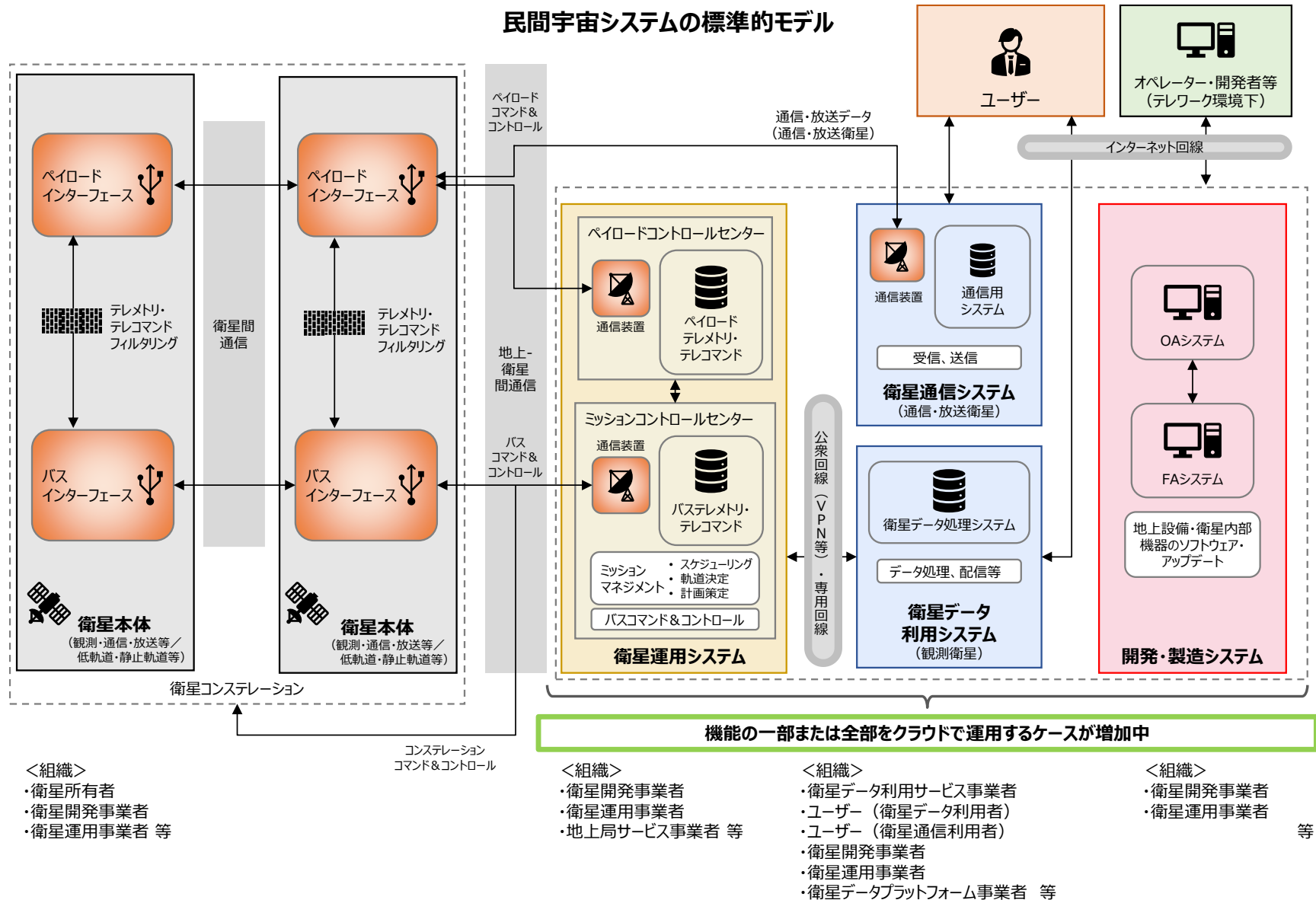
- 宇宙分野においてサイバーセキュリティリスクは増加傾向にあり、国内外で多数のセキュリティインシデントが発生している。
- 海外で明らかとなった近年の代表的なインシデント事例は以下のとおりである。

年	対象	影響	概要
2018	NASA 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 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。
2022	Viasat社 通信衛星KA-SAT	衛星ブロードバンドへの 接続が不能に	Viasat社の通信衛星「KA-SAT」サービスに利用する数万の通信モデムが標的型DoS攻撃を受け、当該サービスを利用するウクライナや欧州の組織からの衛星ブロードバンドへの接続が一時的に不能となった。この攻撃により、ウクライナ軍の指揮系統に対して混乱を巻き起こしたほか、ドイツでは、当該モデムを使用する複数の風力タービンが影響を受け、複数の発電事業者が管理する7,800基を超える風力タービンのリモート制御が不能となった。
2022	Space X社 衛星地上設備	インターネット接続 サービスの停止	米SpaceX社がウクライナ政府に提供する衛星コンステレーションを用いたインターネット接続サービスであるStarlinkのサービスに対し、衛星信号を探知することでStarlinkの地上設備の位置を特定できるため、ロシアによる攻撃対象となりうる可能性が示された。
2022	電子望遠鏡アルマ 計算機システム	観測停止	アルマ望遠鏡のチリにある計算機システムが、サイバー攻撃を受け、科学観測とチリ合同アルマ観測所のウェブサイトが停止した。通信やその他の運用に用いる計算機クラスターが影響を受けたため、すべての観測を停止した。
2023	SpaceX社、 Maximum Industries社	設計情報の流出	LockBitと呼ばれる国際的な攻撃グループが、SpaceX社の下請けであるMaximum Industries社に対してランサムウェア攻撃をしかけ、SpaceX社のロケットに関する約3,000の設計文書を窃取した。また、攻撃グループは、SpaceX社のイーロン・マスクCEOに対して、身代金を支払わない場合に設計文書を公開すると脅迫した。
2023	ロシアの国防省と治安 当局が利用するロシア の衛星通信プロバイ ダーDozor-Teleport	サービスの停止、機密 情報の漏洩	ロシアの国防省と治安当局が利用するロシアの衛星通信プロバイダーであるDozor-Teleportに対し、攻撃を行ったと犯行声明が出された。犯行声明は、民間軍事会社のワグネルグループと関係があるとされるハッカーによるものであるとされており、Dozor社の地上局側の端末に悪意のあるソフトウェアを送ることでオフラインにしてサービスを停止し、また同社のサーバーに保管されていた機密情報を漏洩したとしている。

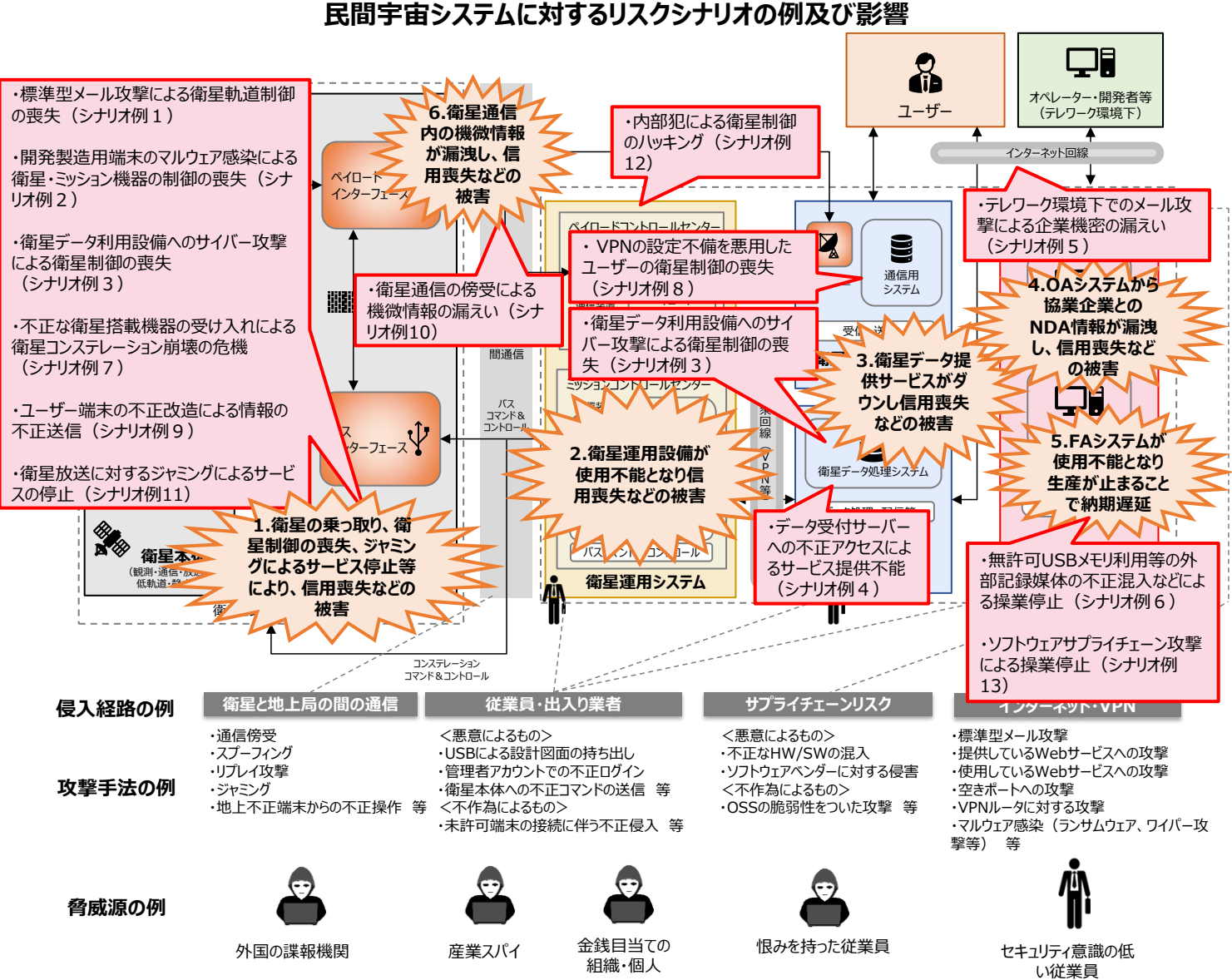
ガイドラインにおける民間宇宙システムの標準的なモデル

本文の2.2節

- 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。



● 実際のインシデント事例等を踏まえ、重大な事業被害を及ぼしうる13のシナリオ例を整理した。



サブシステムごとに求められる主な対策

本文の2.2節

- 前項のリスクシナリオを踏まえて、サブシステムごとに求められる主な対策を整理した。

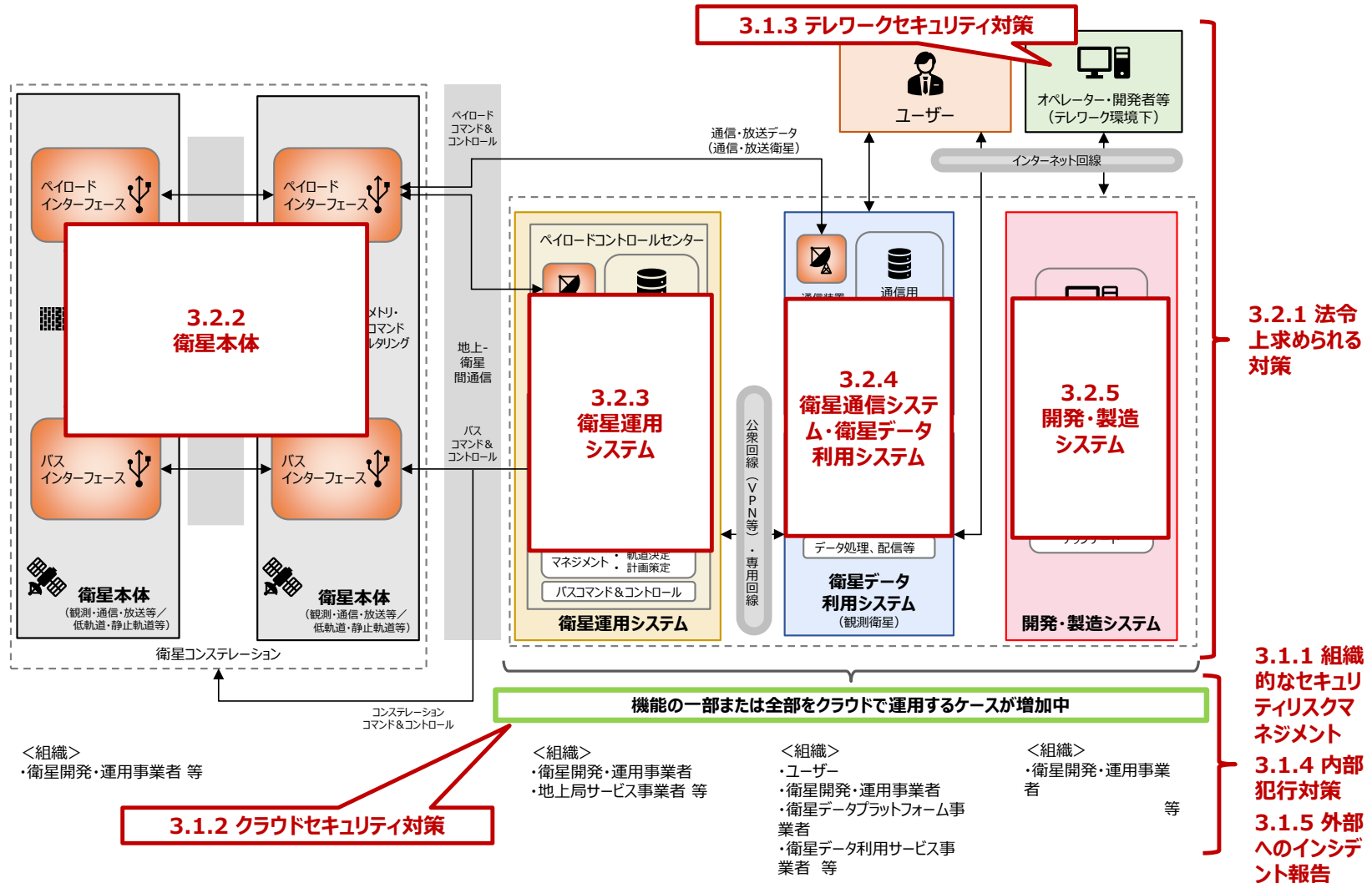
No.	大きな事業被害をもたらすリスクシナリオの例	主な対策				
		衛星本体	衛星運用システム	衛星通信システム・衛星データ利用システム	ITシステム	開発・製造システム
例 1	標準型メール攻撃による衛星軌道制御の喪失	・ 送受信データの完全性・暗号化	・ 送受信データの完全性・暗号化	－	・ 従業員に対するサイバーセキュリティの教育・演習の実施	－
例 2	開発製造用端末のマルウェア感染による衛星・ミッション機器制御の喪失	・ 更新プログラム等の事前検証・脆弱性対策※ （※ 打上げ後のため、実際には開発・製造システムにて実施）	－	－	・ 従業員に対するサイバーセキュリティの教育・演習の実施	・ 情報システムと制御システムの分離
例 3	衛星データ利用システムへのサイバー攻撃による衛星制御の喪失	・ 複数の通信経路等確保	・ システムの脆弱性対策	・ システムの脆弱性対策	・ シャドーITを利用させない対策 ・ 情報システムのIT資産管理・構成管理・パッチ管理	－
例 4	データ受付サーバーへの不正アクセスによるサービス提供不能	－	－	・ セキュア開発の実施 ・ クラウド等外部サービス利用	・ 重要業務を行うサーバー等の技術的防御 ・ サイバー攻撃を検知した際のインシデント対応	－
例 5	テレワーク環境下でのメール攻撃による企業機密の漏えい	－	－	－	・ 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 ・ 端末やネットワークのログの収集・分析	－
例 6	無許可USBメモリの利用による操業停止	－	－	－	－	・ 無許可USBメモリの使用禁止 ・ ホワイトリスト型マルウェア対策
例 7	不正な衛星搭載機器の受入れによる衛星コンステレーション崩壊の危機	－	－	－	－	・ 部品受入検査の徹底・精度向上
例 8	VPNの設定不備を悪用したユーザーの衛星機能の喪失	－	・ システムの脆弱性対策	・ システムの脆弱性対策	・ 情報システムのIT資産管理・構成管理・パッチ管理	－
例 9	ユーザー端末の不正改造による情報の不正送信	・ 複数の通信経路等の確保 ・ 更新プログラム等の事前検証・脆弱性対策※ （※ 打上げ後のため、実際には開発・製造システムにて実施）	－	－	－	－
例10	衛星通信の傍受による機微情報の漏えい	・ 送受信データの完全性・暗号化	・ 送受信データの完全性・暗号化	－	－	－
例11	衛星放送に対するジャミングによるサービスの停止	・ ジャミング対策	・ ジャミング対策	－	－	－
例12	内部犯による衛星制御のハッキング	－	－	－	・ 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（内部犯行対策）	－
例13	ソフトウェアサプライチェーン攻撃による操業停止	－	－	－	・ 情報システムのIT資産管理・構成管理・パッチ管理	・ 情報システムのIT資産管理・構成管理・パッチ管理 ・ 情報システムと制御システムの分離
サブシステムごとの主な対策のまとめ		・ 送受信データの完全性・暗号化（3.2.2） ・ ジャミング対策（3.2.2） ・ 更新プログラム等の事前検証・脆弱性対策（3.2.2） ・ 複数の通信経路等確保（3.2.2）	・ 送受信データの完全性・暗号化（3.2.3） ・ ジャミング対策（3.2.3） ・ システムの脆弱性対策（3.2.3）	・ システムの脆弱性対策（3.2.4） ・ セキュア開発の実施（3.2.4） ・ 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） ・ 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等） ・ 開発・製造システムにおけるセキュリティ対策（3.2.5）

民間宇宙システムにおけるセキュリティ対策の全体像

本文の3章

- ガイドライン3.1節では全組織に関わる共通的な対策を示し、3.2節では、宇宙システム特有の対策として、各サブシステム固有の対策を記載した。

民間宇宙システムに対する共通的対策・各サブシステム固有の対策の概観



- 各ステークホルダーが検討し取り組むべきセキュリティ対策や、対策の検討に当たり参考になる情報を「要求事項」、「基本対策事項」、「解説」の3つの項目に分けて整理した。
- 具体的なセキュリティ対策の検討に当たっては、「基本対策事項」に記載されている対策事項や、参照しているガイドライン等の内容及び「解説」を踏まえた検討を行うことが重要である。

セキュリティ対策に関する3つの記載事項

要求事項

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。

【基本対策事項】

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。

また、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かつ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。

(解説)

要求事項及び対応する基本対策事項に関する補足説明や参考情報を示す。

各ステークホルダーと本ガイドラインのセキュリティ対策との対応①

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。

区分	節番号・項目名	要求事項	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	ステークホルダー					
				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	衛星データ利用者／衛星通信利用者	衛星開発事業者
共通の対策	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を識別し、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及び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を活用することが望ましい。 (a) サイバーセキュリティ経営ガイドラインVer3.0（経済産業省、IPA） (b) 中小企業の情報セキュリティ対策ガイドライン第3.1版（IPA） (c) ISO/IEC 27001（情報セキュリティマネジメントシステム） (d) Cybersecurity Framework Ver1.1（NIST） (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、外部サービス提供者の法令の遵守状況を確認し、サービスを選定することが望ましい。 (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	●	●	●	●	●	●
			【基本対策事項】 (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が望ましい。 (a) ISO/IEC 27017 ISO/IEC 27002に基づくクラウド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） (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） (c) 米国連邦リスク承認管理プログラム（FedRAMP）	●	●	●	●	●	●

*：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。

各ステークホルダーと本ガイドラインのセキュリティ対策との対応②

- ・**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。

区分	節番号・項目名	要求事項	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	ステークホルダー					
				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	衛星データ利用者／衛星通信利用者	衛星開発事業者
共通的対策	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。 (a) テレワークセキュリティガイドライン（第5版）（総務省） (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3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。 (a) 組織における内部不正防止ガイドライン（第5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、法令や規程の定めるところにより、所管省庁等への届出、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、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。

各ステークホルダーと本ガイドラインのセキュリティ対策との対応③

- ・**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。

区分	節番号・項目名	要求事項	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	ステークホルダー					
				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	衛星データ利用者／衛星通信利用者	衛星開発事業者
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】 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(e)の主要な法令に準拠することが求められる。 (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 (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 (c) 電気通信事業法／電気通信事業法施行規則 (d) 放送法／放送法施行規則 (e) 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。	【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。 (a) 通信の保護 (b) 通信のジャミング対策 (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 (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	●	●	—	—	—	●

*：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。

各ステークホルダーと本ガイドラインのセキュリティ対策との対応④

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。

区分	節番号・項目名	要求事項	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	ステークホルダー					
				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	衛星データ利用者／衛星通信利用者	衛星開発事業者
宇宙システム特有の対策	3.2.3 衛星運用システム	【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及びミッションコントロールシステム（衛星制御システム及び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。	【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(i)の対策を実施することが望ましい。 (a) システムの保護 (b) 通信の保護 (c) ジャミング対策 (d) データの保護 (e) システムの検証とシステムの脆弱性対策 (f) 送受信データの完全性の確保 (g) 外部サービスの利用 (h) セキュアコーディング (i) サプライチェーンに対するセキュリティ対策	—	●	●	—	—	●
	3.2.4 衛星通信システム・衛星データ利用システム	【要求事項】 衛星通信システム・衛星データ利用システムに対するサイバーセキュリティ対策を講じること。	【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(g)の対策を実施することが望ましい。 (a) 設備の保護 (b) データの保護 (c) システムの検証とシステムの脆弱性対策 (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 (g) サプライチェーンに対するセキュリティ対策	—	—	●	●	●	●
	3.2.5 開発・製造システム	【要求事項】 衛星の開発・製造システム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】 (1) 衛星の開発・製造システムに対する対応に当たって、以下の(a)を含む既存の基準等の活用が望ましい。 (a) 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（経済産業省）	—	● **	—	—	—	●

*：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