経済産業省

資料5-4

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 1.1

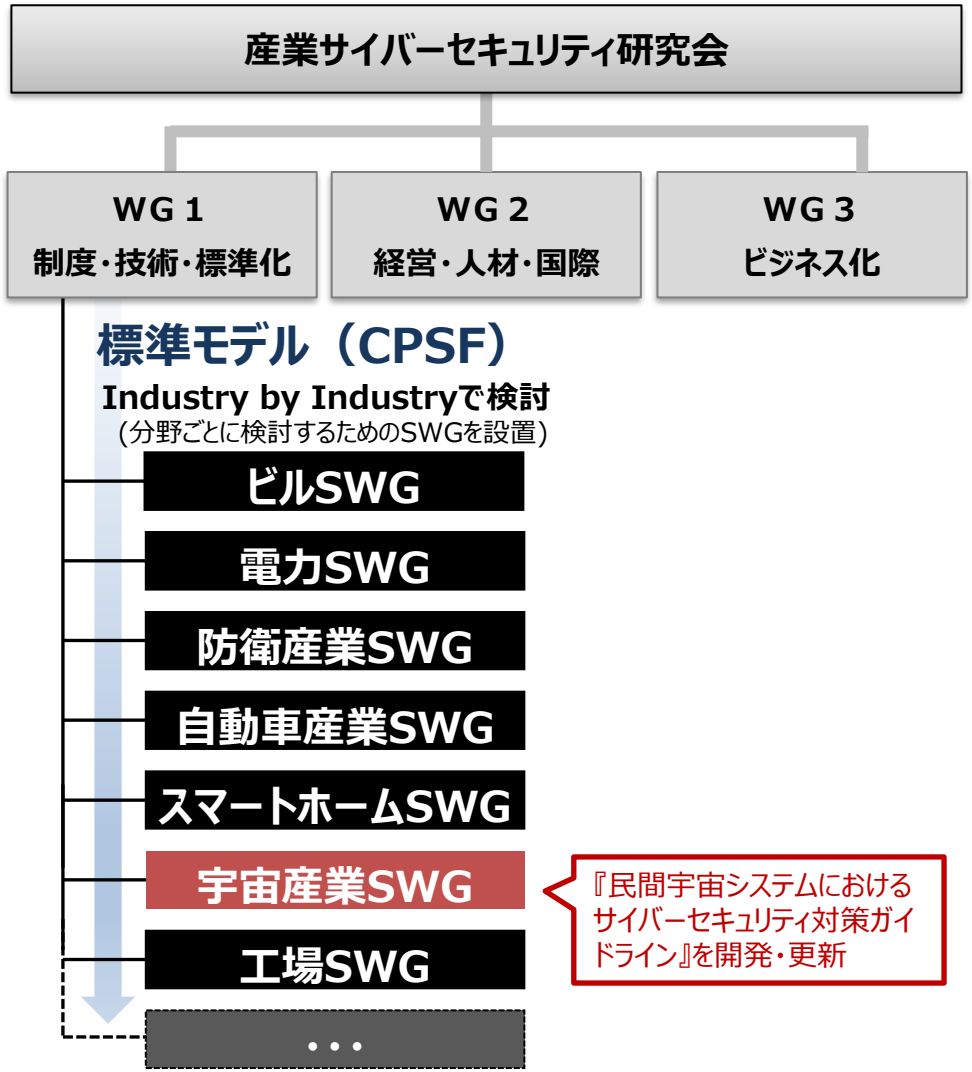
概要資料（案）

令和５年●月●日

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した。



有識者	所属（2023年1月時点）	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（JSS）	●	
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（IPA）セキュリティセンター	●	●
来原 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（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		●
國母 隆一	株式会社アクセルスペース		●
小出 祐輔	株式会社Synspective		●
鈴本 遼	株式会社アークエッジ・スペース		
髙橋 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		●
仁尾 友美	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		●
合田 知善	日本電気株式会社		●

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

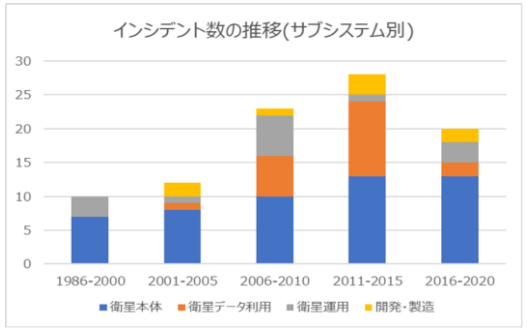
- 我が国の安全保障や経済社会における民間宇宙システムの役割が増大する一方で、宇宙システムにおけるデジタル技術の浸透、ネットワークの複雑化等から、セキュリティ上の懸念も増大している。
- 欧米では宇宙システムのセキュリティ対策が進められており、我が国においても対応が必要である。

●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】**
- 2022.2 米国：**商用衛星運用のためのセキュリティ入門書のドラフト版発行 【NIST】**
- 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】**

●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

- 本ガイドラインでは、民間企業が主体となる衛星システム（観測衛星）及び地上システム（衛星運用設備、衛星データ利用設備、開発・製造設備）を対象とした。
- 衛星システムについては、設計・開発・製造、運用・保守、廃棄フェーズを対象とした。
- 地上システムについては、運用・保守フェーズを主な対象としつつ、システムの設計から廃棄までの各フェーズで特に注意すべき点は対象とした。

宇宙システム全体と本ガイドラインの対象

宇宙システムの全体

宇宙システム			運用主体
輸送システム	輸送機	ロケット	国
有人システム	宇宙ステーション	実験棟等	国
衛星システム	探査機	月探査機、惑星探査機等	国
	補給機	物資補給機	国
	人工衛星	測位衛星	国
		気象衛星	国・民間
		通信衛星	国・民間
		放送衛星	民間
		観測衛星	国・民間
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	国・民間
	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	国・民間
	打上設備	射場、打上管制設備等	国・民間
	開発・製造設備	OTシステム（FAシステム 等）	国・民間
		ITシステム（OAシステム 等）	国・民間

本ガイドラインの対象

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、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1.3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。

	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					
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。

本ガイドラインの想定利用方法

本文の1.4節

【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、対象システムの特性・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ラ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ラ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。

宇宙システムにおけるインシデント事例

本文の2.1節

- 宇宙分野では、1986～2022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。

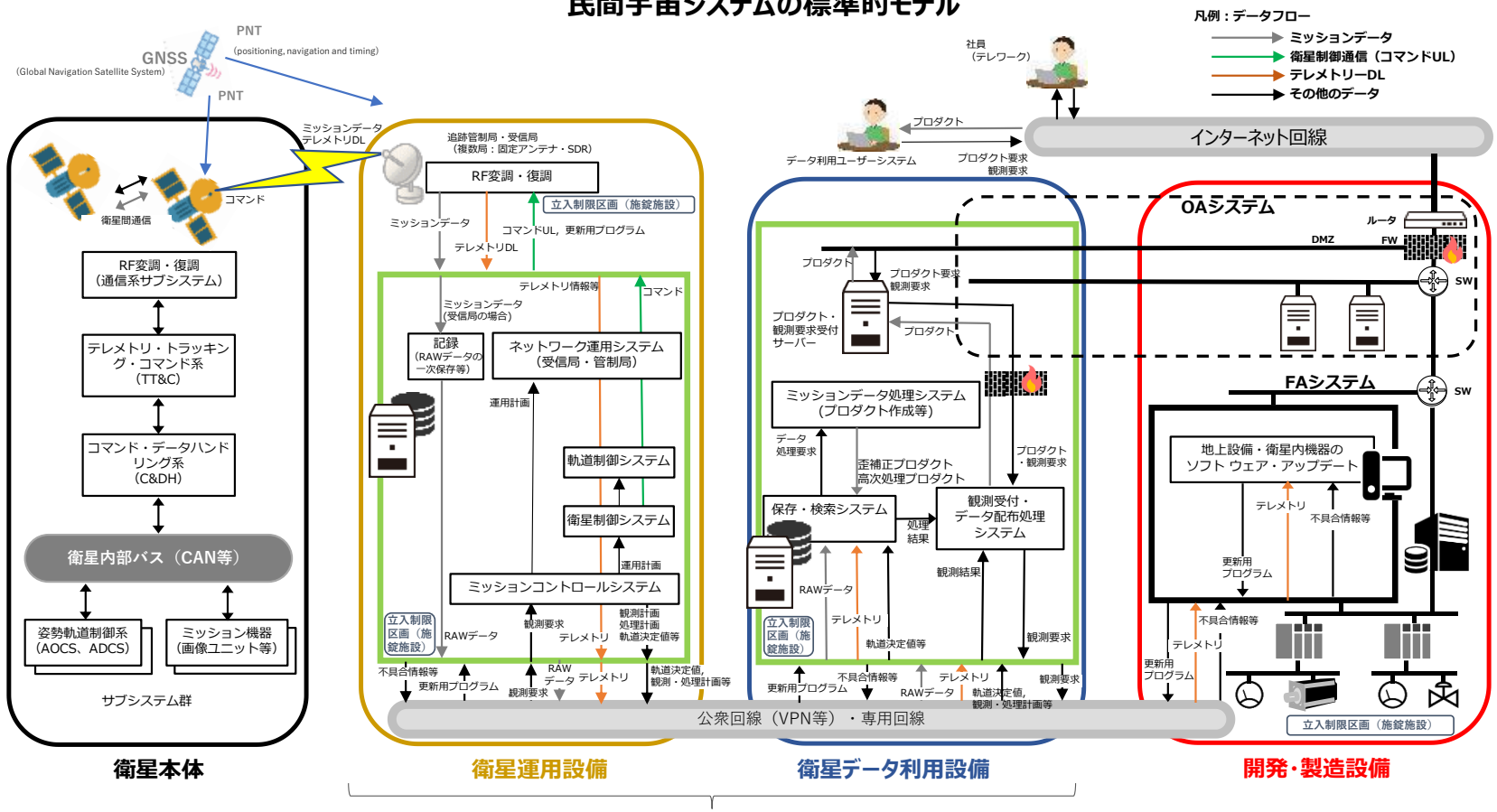
年	対象	影響	概要
2014	NOAA 気象観測NW	衛星データが閲覧不能に	海洋大気庁（NOAA）の気象観測衛星ネットワークがインターネット経由でサイバー攻撃を受けた。
2015	イリジウム 通信衛星	通信内容が見られる状態に	イリジウム通信衛星のページャ通信データが暗号化されていないという脆弱性が指摘された。 国際会議Chaos Communication Camp 2015では実際に、市販（計€50程度）のアンテナ等でイリジウム通信衛星のページャ通信データを解析・解読し、クリアテキスト情報（平文）に変換する操作のプレゼンがあった。
2018	NASA ジェット推進研究所 （JPL）	ミ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が影響を受けたため、すべての観測を停止した。

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。

民間宇宙システムの標準的モデル



（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

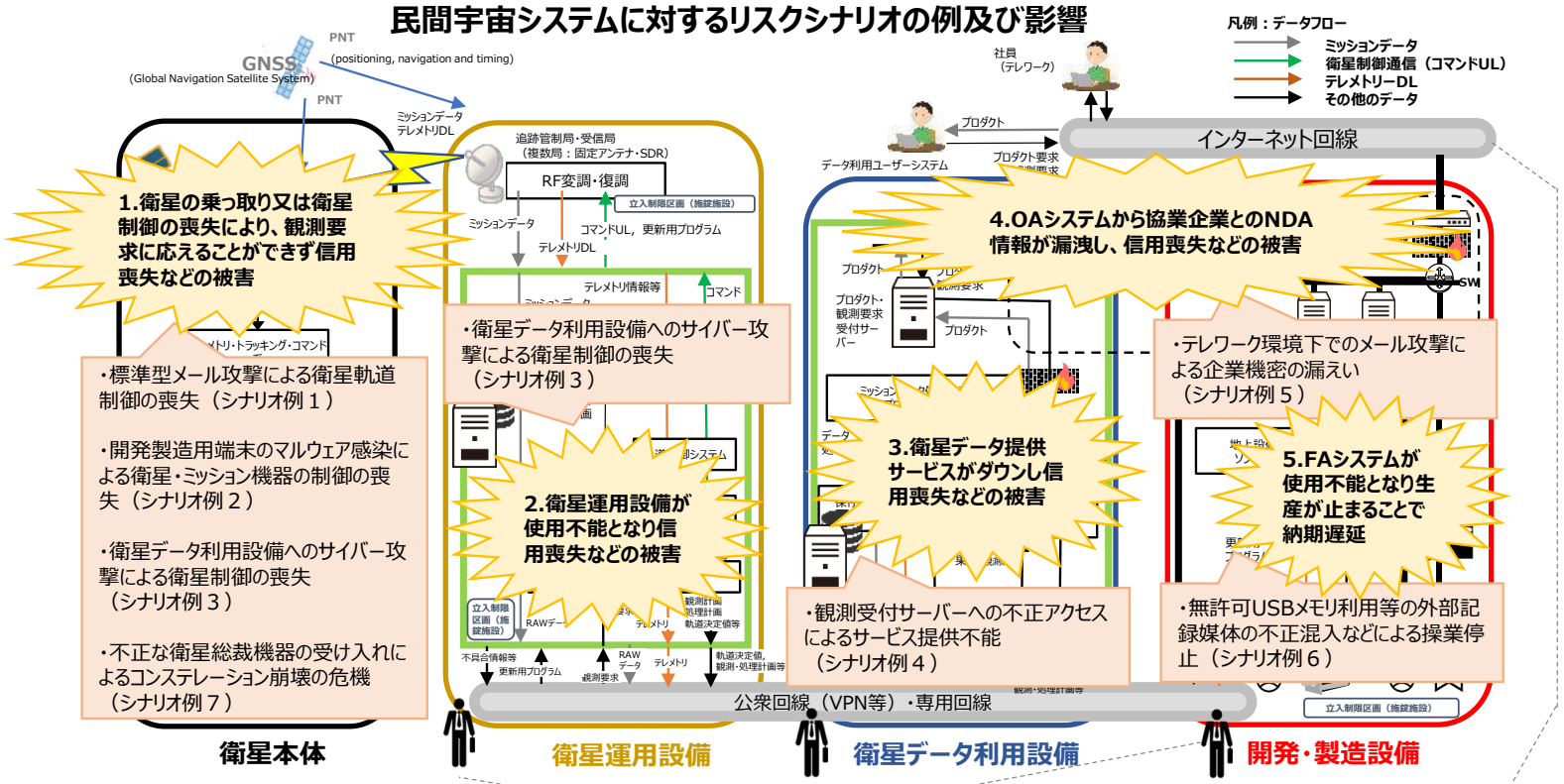
<組織>
・衛星開発・運用事業者 等

リスクシナリオの検討

図中の表記ゆれを修正

本文の2.2節

- 民間宇宙システムの標準モデルを踏まえ、重大な事業被害を及ぼしうるシナリオ例を7つ整理した。



	衛星と地上局の間の通信	従業員・出入り業者	サプライチェーンリスク	インターネット
侵入経路の例				
攻撃手法の例	・通信傍受 ・スプーフィング ・リプレイ攻撃 ・ジャミング　等	＜悪意によるもの＞ ・USBによる設計図面の持ち出し　等 ＜不作為によるもの＞ ・未許可端末の接続に伴う不正侵入　等	＜悪意によるもの＞ ・不正なHW/SWの混入 ＜不作為によるもの＞ ・OSSの脆弱性をついた攻撃　等	・標準型メール攻撃 ・提供しているWebサービスへの攻撃 ・使用しているWebサービスへの攻撃 ・空きポートへの攻撃　等
脅威源の例	外国の諜報機関	産業スパイ 金銭目当ての組織・個人	恨みを持った従業員	セキュリティ意識の低い従業員

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。

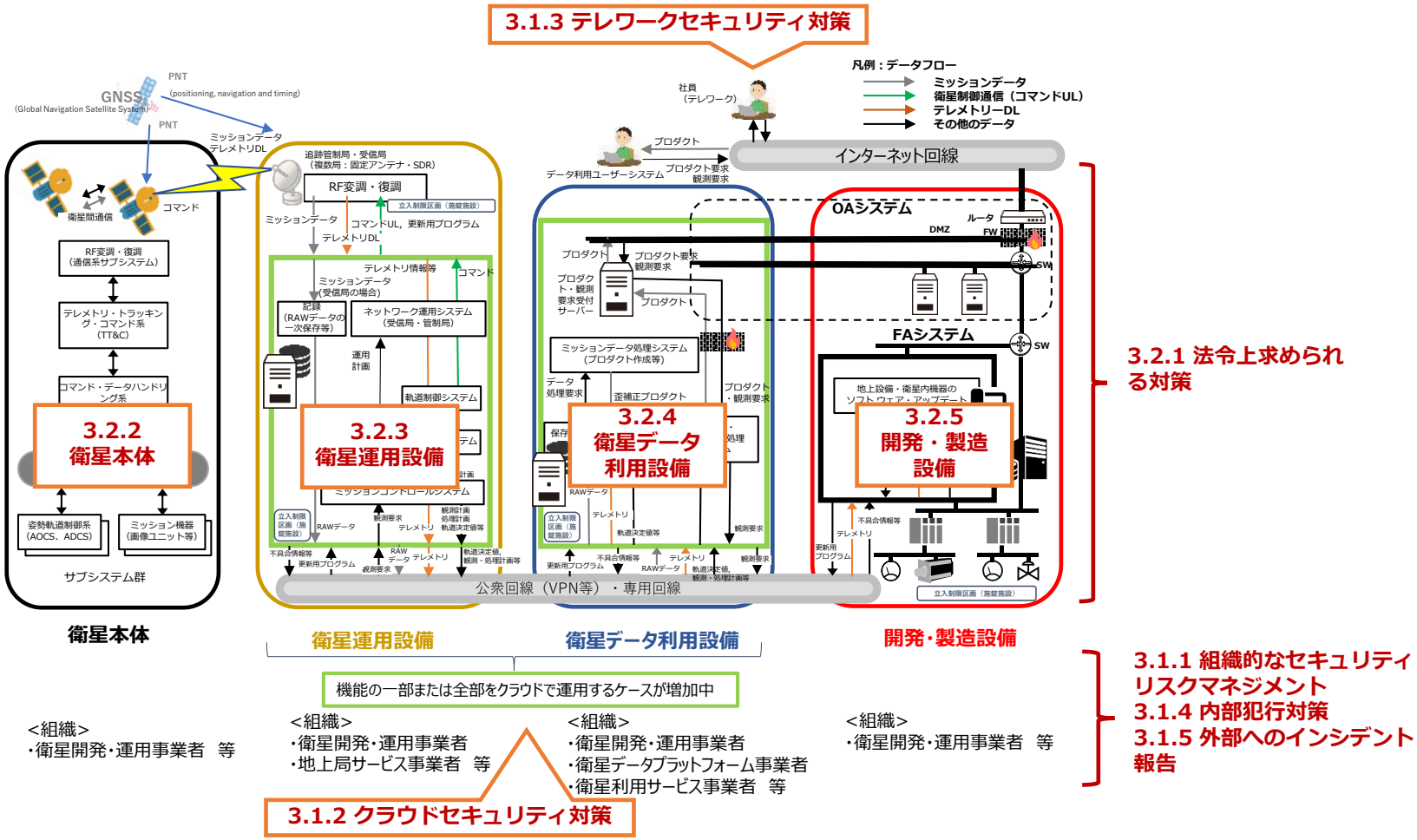
No.	大きな事業被害をもたらす リスクシナリオの例	主な対策 衛星本体	衛星運用設備	衛星データ利用設備	システム	開発・製造設備
例 1	OA環境の社員端末が標的型メール攻撃を受けてマルウェアに感染。インターネット経由のリモートアクセスにより姿勢制御やミッション機器制御に係る機密情報が窃取される。その後、衛星本体のアップリンクデータが乗っ取られ、窃取情報を使った不正コマンドが衛星に送られ、一時的に衛星の軌道制御を喪失する。	• RF通信における送受信データの完全性・暗号化	• RF通信における送受信データの完全性・暗号化	–	• 従業員に対するサイバーセキュリティの教育・演習の実施	–
例 2	衛星本体のソフトウェア更新に使われる開発・製造用の端末（OAと兼用）がマルウェア感染したため、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、正常な衛星の制御又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※ （※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ーがダウンし、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 • 情報システムのIT資産管理・構成管理・パッチ管理	–
例 4	観測受付サーバーがインターネット経由で不正アセスを受けてランサムウェアに感染。その後、サーバード環境の設定不備により設備内の全サーバー及び端末に感染し、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 • 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、マルウェアに感染。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 • 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 • ホワイトリスト型マルウェア対策
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) • 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)	• RF通信における送受信データの完全性・暗号化 (3.2.3) • 設備の脆弱性対策 (3.2.3)	• 設備の脆弱性対策 (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) • 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全体像

本文の3章

- 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を踏まえ、対策のポイントを整理した。
- 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



本ガイドラインにおけるセキュリティ対策に関する記載事項

本文の3章

- 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	衛星開発事業者
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Ver2.0（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

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

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(c)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) 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) RF通信の保護 (b) RF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	衛星開発事業者
宇宙システム特有の対策	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(h)の対策を実施することが望ましい。 (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　(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 (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。	【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) 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 (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】 (1) 衛星の開発・製造設備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