MBSD21PWD-CPS-A-004

経済産業省 製造産業局 御中

令和３年度

産業経済研究委託事業

（宇宙産業におけるサイバーセキュリティ対策に関する調査）

調査報告書（公表用）

2022 年（令和 4 年）2 月 28 日

三井物産セキュアディレクション株式会社

（空白ページ）

目次

図目次

表目次

要約

本報告書は、６章で構成している。

第 1 章では、本事業の背景および目的について述べている。

第 2 章では、宇宙分野におけるサイバーセキュリティ対策についての調査を参考に『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』開発のため課題分析の結果を報告した。

具体的には、令和 2 年度に引き続き、米国、欧州等における宇宙産業のサイバーセキュリティ対策に関する政策動向や、宇宙産業に関するセキュリティインシデント事例等について調査を実施し、国内外における宇宙産業に関わる組織や有識者へのヒアリング等を通じ、サイバーセキュリティ対策の現状・課題や求められる施策等について意見交換を実施し、令和 2 年度の検討結果を評価し、ガイドライン開発に反映した。また、動向調査に加え、CPSF によるセキュリティマネージメントフローに沿った分析対象の明確化（標準モデル、サプライチェーン及び分析対象の具体化による資産の明確化）、想定されるセキュリティインシデント及び事業被害、リスク分析、リスク対応について課題分析を実施した。

第 3 章では、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ためのガイドライン開発に関して、宇宙産業 SWG 及び技術面での妥当性評価を実施するための作業部会の運営について整理するとともに、次年度に向けた各委員からのコメントや意見を整理した。

第 4 章では、本事業で開発した『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』の構成・内容について概要を取りまとめた。

第 5 章では、今後の展開について、令和 3 年度以降に実施すべき検討項目・ガイドライン開発・体制構築等について整理した。

第 6 章には、宇宙産業 SWG 及び作業部会おいて使用した資料及び議事概要を添付した。

1. はじめに

1.1. 背景

経済産業省では、平成２９年１２月に、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される「産業サイバーセキュリティ研究会」を立ち上げ、同研究会の下に専門的な議論を行う３つのワーキンググループ（以下、「WG」という。）を設置し、「制度・技術・標準化」、「経営・人材・国際」及び「サイバーセキュリティビジネス化」のテーマ毎に議論を行っている。特に、サプライチェーンにおけるサイバーセキュリティ強化に向けては、「制度・技術・標準化」WGにて、「Ｓｏｃｉｅｔｙ５．０」における新たな形のサプライチェーンに求められるセキュリティ対策の全体像を整理した「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「ＣＰＳＦ」という。）を平成３１年４月に策定した。ＣＰＳＦでは、「Ｓｏｃｉｅｔｙ５．０」における産業社会を３つの層（企業間のつながり（第１層)、フィジカル空間とサイバー空間のつながり（第２層)、サイバー空間におけるつながり（第３層））に整理し、セキュリティ確保のための信頼性の基点の明確化を行った。加えて、ＣＰＳＦの考え方を産業活動に実装するために、産業活動の実態に応じて、必要な対策要件や対策水準について検討を行う産業分野別のサブワーキンググループ（ビルサブワーキンググループ、スマートホームサブワーキンググループ等。以下、まとめて「産業分野別ＳWG」という。）を立ち上げ、それぞれの課題に応じた検討を並行して進めている。

1.2. 目的

本事業では、産業分野別ＳWGとして令和３年１月に新たに立ち上げた「宇宙産業ＳWG」及び当該ＳWGの下に設置をした「宇宙産業ＳWG作業部会」の事務局として会議開催や資料案作成を行うとともに、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を令和３年度中に開発する。

- 国内外の宇宙分野におけるサイバーセキュリティ対策等についての調査
- 検討会の運営
- 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の開発
- 情報共有・教育訓練のあり方などの検討

2. 宇宙分野におけるサイバーセキュリティ対策についての調査

2.1. 動向等の調査

米国、欧州等における宇宙産業のサイバーセキュリティ対策に関する政策動向や、宇宙産業に関するセキュリティインシデント事例等について調査を実施した。

a) 各国の宇宙システムにおけるサイバーセキュリティに係る施策

米国等の海外では、宇宙システムのサイバーセキュリティ対策について、官及び民での議論や取組が活発化している。

表 2-1　米国等におけるサイバーセキュリティにかかる施策

年月	主体	関連施策等
1990.7	官	NSD-42（国家安全保障電気通信及び情報システムのセキュリティに係る国家方針）を発行。
1990.7	官	NSD-42 に基づき、国家安全保障電気通信及び情報システムセキュリティ委員会（NSTISSC）を設立。
2001.10	官	大統領令 13231“情報時代における重要インフラの保護”において、NSTISSC を国家安全保障システム委員会（CNSS）に指定。CNSS は国防総省（DoD）、中央情報局（CIA）、国防情報局（DIA）、司法省（DOJ）、連邦捜査局（FBI）、国家安全保障局（NSA）、国家安全保障会議（NSC）等から構成される。
2005.6	官	国防総省が DoDI 8581.01“国防総省が使用する宇宙システムにおける情報保証方針”を発行。（2010.6 改訂）
2007.3	官	NSD-42 を受け、CNSS が CNSSP 12“安全保障任務に用いられる宇宙システムのための国家情報保証方針”を発行。（2012.1 改訂、2018.2 改訂）
2009.2	官	NSD-42 を受け、CNSS が CNSSP 22“国家安全保障システムのための情報保証リスク管理”を発行。 （2012.1.改訂、2016.8.サイバーセキュリティリスク管理方針に改訂）
2012.3	官	NSD-42 を受け、CNSS が CNSSD 505“サプライチェーンリスク管理”を発行。（2017.7.26 改訂）

2017.1	民	エアロスペースコーポレーションが“NAVIGATING THE POLICY COMPLIANCE ROADMAP FOR SMALL SATELLITE”で衛星所有者の DoDI 8581.01 及び CNSSP 12 への対応ついて解説。
2018.8	民	米国航空宇宙学会（AIAA）小型衛星カンファレンスで“No Encryption, No Fly”のルールが提案される。
2019.4	官民	宇宙情報共有分析センター（Space ISAC）の設立。（NASA、米国宇宙軍、国家偵察局が立ち上げ。）
2019.4	民	Orbital Security Alliance（OSA）が“Big Risk in Small Satellites”を発表。
2020.2	官	大統領令 13905 ”測位・航法・時刻 サービスの責任ある使用による国家のレジリエンスの強化”発行。 PNT サービスに関連したセキュリティプロファイルに関する文書（NISTIR 8323）を 2021.2 に発行。
2020.5	官	UKSA(英宇宙局)が宇宙資産所有者、宇宙業界製品サプライヤー向けに“Cyber Security Toolkit ver2”を発行。
2020.5	民	OSA が民主導による“商用宇宙システムセキュリティガイドライン”を発行。
2020.9	官	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”（宇宙システムは悪意のあるサイバー活動による攻撃を考慮して設計・開発されるべきこと、地上システム・運用技術・情報処理システムの保護等が盛り込まれた）を発行。
2021.5	官	重要インフラ 16 セクターに宇宙システムを追加の要否の検討のための審理プロセスとして、国土安全保障省（DHS）が WG を設立。
2021.6	官	NIST が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 NISTIR 8279(Draft) ”Introduction to Cybersecurity for Commercial Satellite Operation”を作成。

MBSD 作成

b） 宇宙システムに係るインシデント事例

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している（参考：添付資料『宇宙システムにおけるインシデント事例.xlsx』）。以下に代表的な事例の一部を示す。

表 2-2　宇宙システムに係るインシデント事例（一部抜粋）

年	対象	影響	概要
2008	NASA　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　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。

MBSD 作成

2.2. 国内外の公的機関・有識者・組織との意見交換

2.2.1. 意見交換先

表 2-3 に整理した国内外における宇宙産業に関わる組織や有識者へのヒアリング等を通じ、サイバーセキュリティ対策の現状・課題や求められる施策等について意見交換を実施し、令和 2 年度の検討結果を評価し、ガイドライン開発に反映した。

表 2-3　ヒアリング先

ヒアリング先	日時	備考
国立研究開発法人情報通信研究機構法（NICT）	2021.11.05	リモート会議
制御システムセキュリティセンター（CSSC）元専務理事	2021.11.16	リモート会議
SpaceISAC-JAXA-METI 会合	2021.8.11	リモート会議
宇宙システム開発推進機構	2021.10.22	リモート会議
宇宙産業 SWG 委員（個別）	2021.11.19～29	リモート会議

MBSD 作成

2.2.2. 課題の分析

宇宙システムでは様々なセキュリティインシデントが発生しており、宇宙システムに係るセキュリティリスクや対策の全体像を把握するのは容易ではない。このため、『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver1.0』（2019 年 4 月 経済産業省サイバーセキュリティ課）を活用し、民間宇宙システムにおけるセキュリティリスクや対策の考え方を整理した。

CPSF は、サイバー空間とフィジカル空間が高度に融合する「Society5.0」という新たな産業社会におけるサプライチェーン全体のセキュリティ確保を目的としており、大きな特徴として、情報セキュリティマネジメントシステム（ISMS）の様に 1 組織を対象にしたフレームワークとは異なり、関連企業、取引先等を含めたサプライチェーン全体としてセキュリティ対策に取り組むマルチステークホルダーによるアプローチをとっていることが挙げられる。宇宙システムも、衛星開発事業者、衛星運用事業者、地上局運用事業者、衛星データプラットフォーム等の様々なステークホルダーがサプライチェーンを構成していることから、CPSF のアプローチが有効であると考えられる。

国内外の公的機関・有識者・組織意見交換を通じて、本調査において開発した標準モデルとサプライチェーン及び分析対象にについて民間宇宙システムにおけるセキュリティリスクを検討・整理した。

CPSF では、図 2-1 に示すように、産業社会を企業間のつながり、フィジカル空間とサイバー空間のつながり、サイバー空間における繋がりの３つの層で捉え、各層におけるリスク源や対策要件等を整理している。

宇宙システムについてもこの３層モデルを活用することで、セキュリティリスクや対策の全体像を洗い出すことが可能であると考えられる。

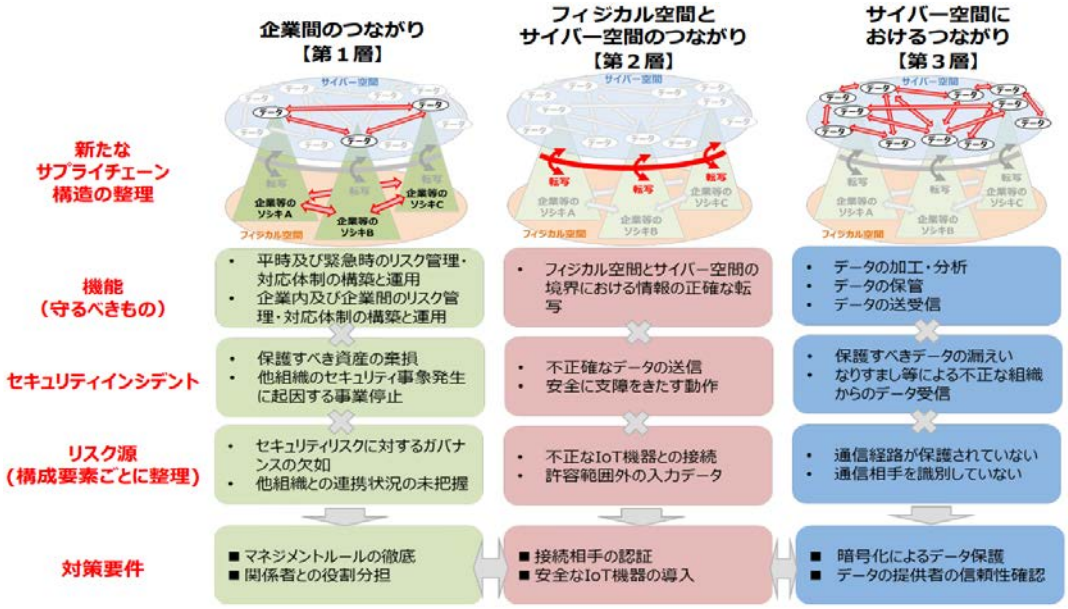


図 2-1 CPSF の全体概要 [1]

[1] 経済産業省商務情報政策局サイバーセキュリティ課：『サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.0』（2019 年 4 月）

a） 標準モデルとサプライチェーン及び分析対象

1） 標準モデル

CPSF の３層構造を活用しつつ、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、表 2-2 の標準的なモデルを作成した。

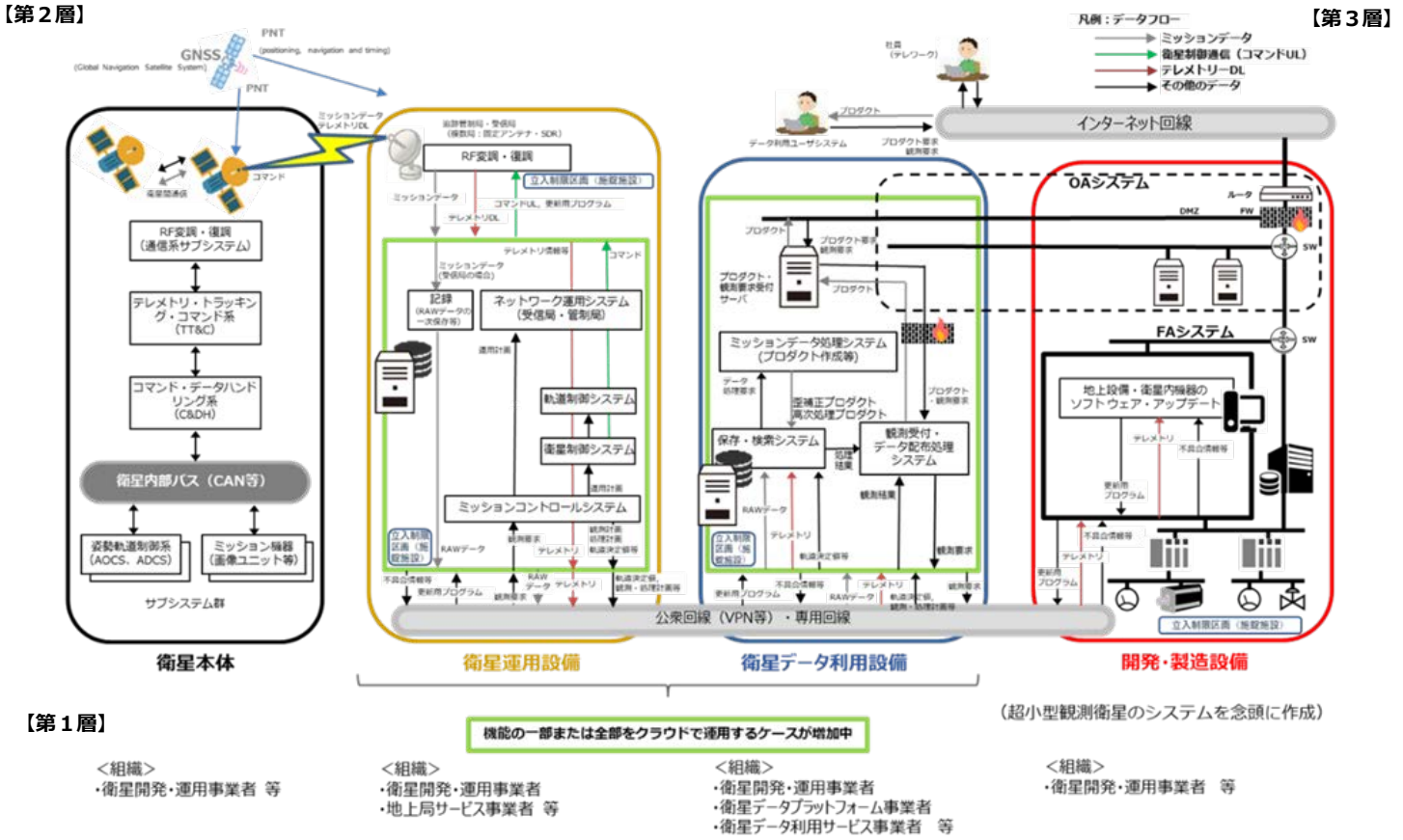


図 2-2 民間宇宙システムの標準的なモデル

MBSD 作成

2)　サプライチェーン

近年では、新たなセキュリティリスクとして、サプライチェーンリスクへの懸念も出てきている。現在ではグローバルバリューチェーンと呼ばれる世界規模での分業体制が多くの分野で見られる。この分業体制により、様々な製品が安く生産できるというメリットがあるが、一方で、様々な地域の多くの企業が生産等に関与することから、新たなリスクの要因ともなり得る。本調査では衛星の調達から廃棄までのライフサイクルと調達時のサプライヤーに対するセキュリティ要件を整理した。

3)　ガイドラインβ版の分析対象

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。

図 2-3　宇宙システム全体と本ガイドラインβ版の分析対象

MBSD 作成

b） セキュリティリスクマネジメントの流れ

CPSF ではセキュリティリスクマネジメントの流れとして図 2-4 を提示している。

前項では Step 1 の分析対象の明確化を行った。

次項以降では Step 2～3 に対応する分析として「重大な事業被害を及ぼし得るリスクシナリオ」を複数検討し、これらに対応できるような形で、Step 4 のリスク対応の考え方を整理した。

なお、Step 1～4 の実務的作業レベルでの手順としては、IPA『制御システムのセキュリティリスク分析ガイド第 2 版』(2020 年 3 月)[2]がある。各社において個別かつ詳細なリスク分析を行う際には、本ガイドの活用が考えられる。

c） 脅威・リスクの抽出

令和 2 年度及び令和 3 年度の調査・検討結果をベースに、宇宙システムにおける「発生してほしくない事象」について整理し、これらの事象を及ぼし得るリスクシナリオを複数検討・整理した。また、対象システム（サブシステム）に対して想定できる事業被害とその侵入経路・攻撃手法の例を整理した。また、各ステークホルダーにおける重大な事業被害・攻撃手法等の分析例を対象システム（サブシステム）毎に示した。

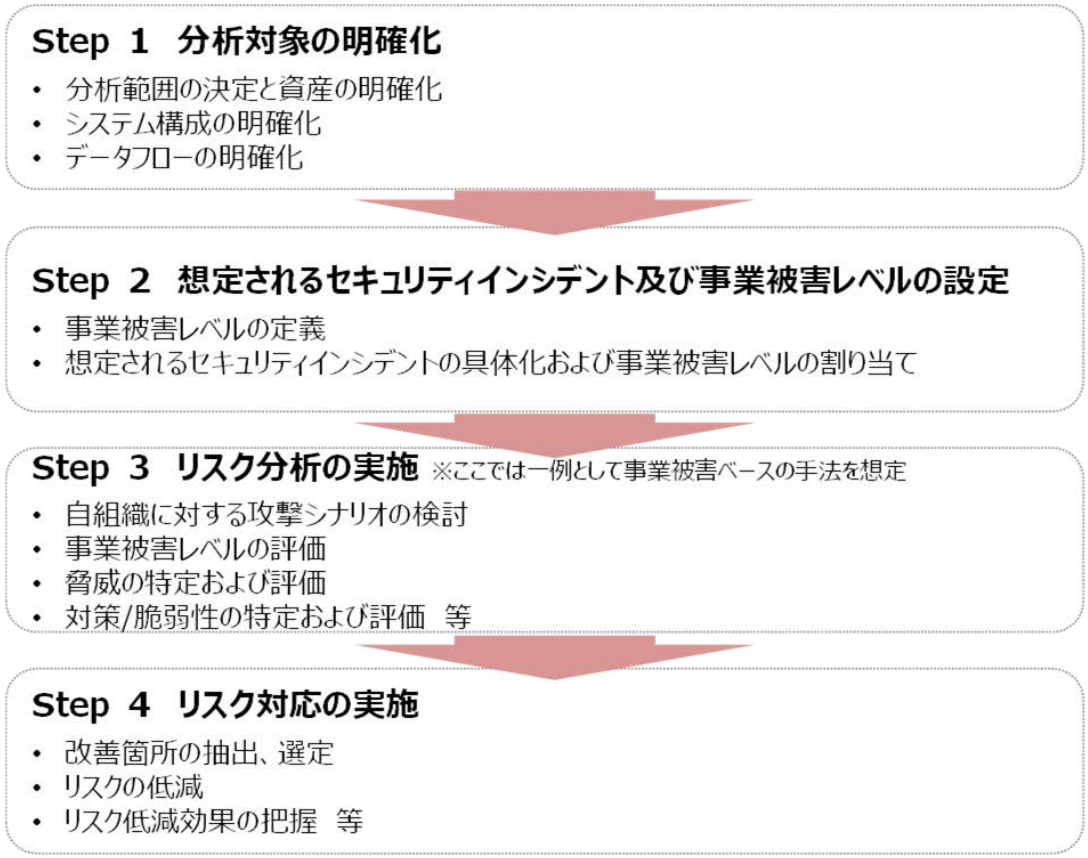


図 2-4 CPSF で示されるセキュリティリスクマネジメントの流れ[2]

[2] 独立行政法人情報処理推進機構 セキュリティセンター :『制御システムのセキュリティリスク分析ガイド第 2 版』(2020 年 3 月)
https://www.ipa.go.jp/files/000080712.pdf

3. 検討会（宇宙産業 SWG）

3.1. 宇宙産業 SWG の運営

宇宙分野におけるサイバーセキュリティ対策についての調査と並行して、専門的な視点からの検討、分析及び助言を得るために、宇宙産業 SWG を運営し、宇宙産業において必要なサイバーセキュリティ対策ガイドラインについての検討を行った。また、宇宙分野特有の課題を解決する上で必要と考える事業者、有識者による作業部会を運営し、技術的な立場からの検討・分析・助言を得た。

3.2. 開催実績

検討会及び作業部会の開催実績と主な検討内容を表 3-1 に整理した。

表 3-1　宇宙産業 SWG 及び作業部会の開催実績

会議名	開催日時	主要テーマ	備考
第 2 回 宇宙産業 SWG 作業部会	2021.07.06 15:00~16:30	● 最近の海外の動向 ● 宇宙産業ＳＷＧ 作業部会 コアメンバー会議 について ● 第 1 回作業部会及び第 2 回検討会でのご指摘事項 ● 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 v0.1 （執筆中）について	・ コアメンバーによるリモート会議 ・ 資料１議事次第・配付資料一覧 ・ 資料２事務局説明資料
第 3 回 宇宙産業 SWG 作業部会	2021.07.26 15:00~16:30	● 最近の海外の動向 ● 第 1 回作業部会及び第 2 回検討会でのご指摘事項 ● 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 v0.1 （執筆中）について	・ コアメンバーによるリモート会議 ・ 資料１議事次第・配付資料一覧 ・ 資料２事務局説明資料

第 4 回 宇宙産業 SWG 作業部会	2021.09.03 13:00~14:30	● 宇宙産業ＳＷＧ 作業部会 名簿の更新について ● 今後の想定 スケジュールについて ● 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.0.1 について	・ 拡大メンバーを含むリモート会議 ・ 資料１議事次第・配付資料一覧 ・ 資料２作業部会名簿（更新版） ・ 資料３今後の想定 スケジュール ・ 資料４民間宇宙システムセキュリティガイドライン作業中ファイル Ver.0.1
第 3 回 宇宙産業 SWG	2021.11.04 15:00~17:00	● 最近の産業サイバーセキュリティに関する動向について ● 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.0.2	・ 座長、事務局出席のもとリモート会議併設 ・ 資料１議事次第・配付資料一覧 ・ 資料２委員等名簿 ・ 資料３サイバーセキュリティ課からの情報提供 最近の産業サイバーセキュリティに関する動向について ・ 資料４事務局説明資料 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.0.2
第 5 回 宇宙産業 SWG 作業部会	2021.12.21 15:00~16:00	● 今後のスケジュールについて ● 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.0.2 について ● ガイドライン概要版（案）について	・ コアメンバーによるリモート会議 ・ 資料１議事次第・配付資料一覧 ・ 資料２作業部会名簿（コアメンバー） ・ 資料３今後の想定スケジュール ・ 資料４民間宇宙システムセキュリティガイドライン（Ver.0.2） ・ 資料５概要版（案）

第 4 回 宇宙産業 SWG	2022.02.07 13:30~14:00	● 最近の海外動向 ● 前回 SWG で頂いたご意見への対応状況（Ver.0.2 からβ版（案）への修正） ● ガイドラインβ版案の概要資料（案） ● 今後の予定	・ 座長、事務局出席のもとリモート会議併設 ・ 資料１議事次第・配付資料一覧 ・ 資料２委員等名簿 ・ 資料３第 3 回宇宙産業 SWG 議事概要 ・ 資料４最近の産業サイバーセキュリティの動向 ・ 資料５事務局説明資料（非公表） ・ 資料６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（案）（非公表）
第 6 回 宇宙産業 SWG 作業部会	2022.02.22 15:00~16:30	● 今後の予定 ● 民間宇宙産業事業者が抱えるサイバーセキュリティ課題等についての情報交換	・ コアメンバーによるリモート会議

MBSD 作成

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の開発

民間事業者が構築する宇宙システムの安全保障や経済社会における役割が大きくなっているが、こうした宇宙システムは様々な形でネットワークに接続しており、高度化するサイバー攻撃への対応が必要となってきている。実際、宇宙システムにおけるセキュリティインシデントは多数確認されている。こうした中、令和 2 年度から民間宇宙事業者のビジネスを振興する観点で、宇宙システムに係るセキュリティに起因するビジネスリスクや、リスクに適切に対応するための対策のポイントについて分かり易く示したガイドラインの検討・開発を進め、令和 3 年度においては、図 4-1 に示す構成のガイドライン β 版の開発を実施した。

4.1. 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ている。図 4-2 に産業サイバーセキュリティ研究会の体制を示した。

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

MBSD 作成

図 4-1 ガイドライン β 版の構成

図 4-2　産業サイバーセキュリティ研究会の推進体制

MBSD 作成

4.2.　民間宇宙システムのセキュリティ対策ガイドライン開発の背景・目的

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。

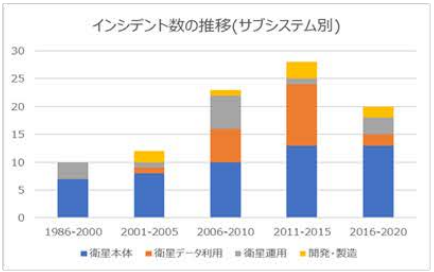
欧米では宇宙システムのセキュリティ対策が進められており、我が国においても対応が必要になってきた。

●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

図 4-3　ガイドライン開発の背景と目的

4.3. ガイドラインの対象範囲

図 2-3 に示したように、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、調達、製造（設計・開発を含む)、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。
なお、ガイドラインの対象範囲は、随時更新することとした。

4.4. 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

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。

4.5. リスクシナリオの検討

図 2-2 に示した標準モデルを踏まえて、各サブシステム（衛星本体および各地上設備）に対して 7 種類のリスクシナリオを検討し、各サブシステムごとの主な対策を検討・整理した。

4.6. ガイドラインの構成と想定読者

表 4-1 に示すようにガイドライン β 版では各章ごとに読者を想定し、各読者がガイドラインを次のように利用することを想定している。

- 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

表 4-1　ガイドラインの構成と想定読者

	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		★	★			★
3．2．3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。

MBSD 作成

4.7.　セキュリティ対策のポイント

前項（4.5）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、示した。

また、セキュリティ対策のポイントを共通的対策事項及び宇宙システム特有の対策事項について、各事業者が実施すべき要求事項をよりわかりやすくするため、表に一括整理した。

表中、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要求事項として明示した。

また、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基本対策事項として明示した。

さらに、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」との条件付きで明示した。

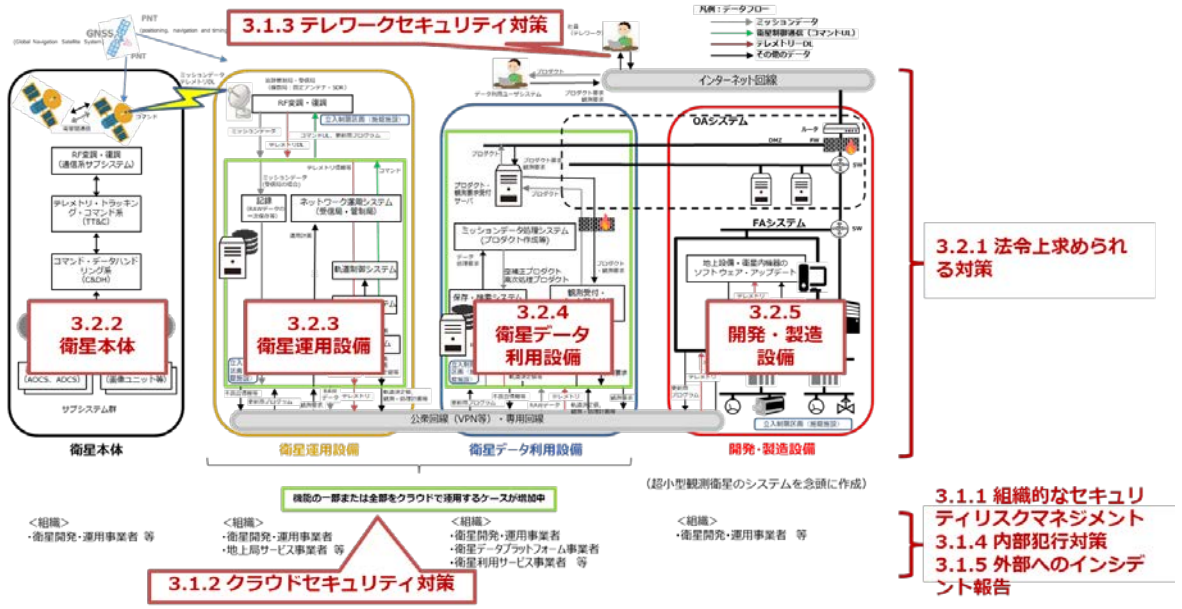


図 4-4　民間宇宙システムにおけるセキュリティ対策のポイント

MBSD 作成

5.　情報共有・教育訓練のあり方などの検討

a） ISAC（情報共有分析センター）[3]

1998 年 5 月、米国において、ISAC（Information Sharing and Analysis Center: 情報共有分析センター）のコンセプトが PDD-63（Presidential Decision Directive-63：大統領令 63）で示された。PDD-63 では、重要インフラ分野が攻撃される可能性を懸念して、所管組織の決定と情報共有の専門組織の設立が推奨された。また、情報共有の専門組織の機能として、分野における脅威や脆弱性に関する情報を分野内で共有することを求めた。これに対応する形で設立されたのが現在の ISAC の枠組みである。その後、官民の対話を経て、NASA、米国宇宙軍（旧空軍宇宙司令部）、国家偵察局が初の宇宙専用 ISAC(Space ISAC)を後援することになり、2019 年 4 月に Space ISAC が設立された。2021 年末時点の Space ISAC の Founding Member は図 5-1 に示すとおりである。

（出典:Space ISAC HP）

図 5-1　Space ISAC の Founding Member

[3] 政府 CIO ポータル：『米国のセキュリティ情報共有組織（ISAC）の状況と運用実態に関する調査』
https://cio.go.jp/node/1962

b） 教育訓練

コミュニティ形成について

・ ガイドライン運用によるサイバーセキュリティ対策については、実施しているところと実施してないところが混在することが懸念される。社会実装するにあたっては、そういった不合理な状況が生じないようにすることが重要である。それを具体化するには米国の Space ISAC のような日本版 Space ISAC 組織の下、サイバーセキュリティ対策を共同で進めて行くという土俵を作って、その中で、ステークホルダー間の協調（監視・情報共有、責任分解の明確化・不足への対応・・）を図り、ガイドラインの普及促進、メンテナンス方針、教育・訓練等について議論することが重要である。

c） 教育訓練について

・ 大学、教育関係者がサイバーセキュリティの重要性の理解を深めるために、ガイドラインをそのようなはたらきかけにつなげていくことが重要で、ベンチャーや大学で宇宙開発が進んでいるが、本ガイドラインを活用することで教育分野であるからサイバーセキュリティを意識しなくて良いということではないという意識づけをする活動を展開し、フィードバックすることが重要と考える。日本版 Space ISAC はそのための機能も必要と考える。
・ 情報提供に対して、スルーされることが多い。そうした事態を防ぐためには、訓練を通して経験していくということが重要で、日本版 Space ISAC 等が中心になった民間主体のワークショップ、演習の役割が大きくなる。
・ ガイドラインを定着させるための施策として、どういった形で普及・教育していくかについて、次年度以降、訓練・机上演習等のやり方を含めて検討していくことも重要である。

6. 添付資料

第 3 回、第 4 回宇宙 SWG 検討会資料及び議事概要、第 2 回から第 6 回宇宙 SWG・作業部会資料及び議事メモおよび宇宙システムにおけるインシデント事例を報告書（詳細版）に添付した。

令和 3 年度 産業経済研究委託事業
（宇宙産業におけるサイバーセキュリティ対策に関する調査）
2022 年（令和4年）2 月 28 日

三井物産セキュアディレクション株式会社
公共事業部 宇宙・防衛第 2 グループ

二次利用未承諾リスト

報告書の題名
令和3年度産業経済研究委託事業（宇宙産業におけるサイバーセキュリティ対策に関する調査）調査報告書（公表用）

委託事業名
令和3年度産業経済研究委託事業（宇宙産業におけるサイバーセキュリティ対策に関する調査）

受注事業者名
三井物産セキュアディレクション株式会社

頁	図表番号	タイトル
9	図 2-1	CPSFの全体概要
10	図 2-2	民間宇宙システムの標準的なモデル
11	図 2-3	宇宙システム全体と本ガイドラインβ版の分析対象
12	図 2-4	CPSFで示されるセキュリティリスクマネジメントの流れ
16	図 4-1	ガイドラインβ版の構成
17	図 4-2	産業サイバーセキュリティ研究会の推進体制
18	図 4-3	ガイドライン開発の背景と目的
21	図 4-4	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
22	図 5-1	Space ISACのFounding Member
5	表 2-1	米国等におけるサイバーセキュリティにかかる施策
7	表 2-2	宇宙システムに係るインシデント事例（一部抜粋 ）
8	表 2-3	ヒアリング先
13	表 3-1	宇宙産業SWG及び作業部会の開催実績
20	表 4-1	ガイドラインの構成と想定読者