経済産業省 商務情報政策局　御中

令和２年度

サイバー・フィジカル・セキュリティ対策促進事業

（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）

2021 年（令和 3 年）3 月 26 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、５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の結果を報告した。

具体的には、各国の宇宙システムにおけるセキュリティに関する施策及び宇宙システムに係るサイバーセキュリティのインシデント事例を中心に国内外動向等の調査を実施した。また、国内事業者等へのインタビューを通じて実態の調査を実施した。これらを踏まえ、脅威・リスクの抽出、宇宙産業サブワーキンググループ（以下、「SWG」という。）及び作業部会での検討結果を反映することで対象となる宇宙資産を明確化することにより、国内宇宙産業の課題分析を実施した。

第 3 章では、宇宙産業 SWG 及び技術面での精緻化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、本事業の方向性、ゴール、対象とする衛星についての各委員からのコメントや意見を整理した。

第 4 章では、本事業で整備する施策について『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 v1.0』の構成・内容についての検討結果を取りまとめた。

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。

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」（以下、「研究会」という。）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、サプライチェーンの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 において、「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を明確化した。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 SWG（ビル SWG やスマートホーム SWG 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として新たに「宇宙産業ＳＷＧ」を立ち上げ、宇宙関連産業の事業者において必要なサイバーセキュリティ対策について、関係府省庁と連携しつつ、検討を行うもので、本年度は以下の３項目について実施するものである。

- 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
  - ✧ 海外動向調査及び国内調査
- 検討会の運営
  - ✧ 宇宙産業ＳＷＧ及び作業部会の運営
- 施策のとりまとめ
  - ✧ ガイドライン作成に関する検討

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

2.1.1. 各国の宇宙システムにおけるセキュリティに関する施策

a) 全世界における宇宙産業に係るセキュリティ動向

宇宙産業においては、国際連合を中心に原則等の整備を進めてきた。表 2-1 に全世界における宇宙産業に係るセキュリティ動向の年表を示す。国際的には安全性（フィジカル・セキュリティ）に重点を置いたセキュリティの推進を先ず進めている段階である。

表 2-1　全世界における宇宙産業に係るセキュリティ動向の年表

年代	官民	主な事項
1959	官	国際連合宇宙空間平和利用委員会（United Nations Committee on the Peaceful Uses of Outer Space : COPUOS）設立
1964	官	国際電気通信衛星機構（International Telecommunications Satellite Organization : ITSO）設立
1967	官	「月その他の天体を含む宇宙空間の探査及び利用における国家活動を律する原則に関する条約（宇宙条約）」が国連採択。
1971	官	「宇宙物体により引き起こされる損害についての国際的責任に関する条約（宇宙損害責任条約）」が国連採択。
1974	官	「宇宙空間に打ち上げられた物体の登録に関する条約（宇宙物体登録条約）」が国連採択。
1982	官	「国際的な直接テレビ放送のための人工地球衛星の国家による使用を律する原則　（放送衛星法原則）」が国連採択。
1986	官	「宇宙空間からの地球のリモートセンシングに関する原則（リモートセンシング法原則）」が国連採択。
2007	官	「デブリ低減ガイドライン」が国連採択
2019	官	「宇宙活動の長期持続可能性ガイドライン」が国連採択

MBSD 作成

b） 米国における宇宙システムのセキュリティに係る施策等の概要

米国では国家安全保障上の理由により、関連する宇宙産業を中心にセキュリティの方針を定めてきた。民間事業者等の宇宙進出が進むにつれ、民間レベルでのセキュリティに対する活動も増えてきた。表 2-2 に米国における宇宙産業に係るセキュリティ動向の年表を示す。

表 2-2　米国における宇宙産業に係るセキュリティ動向の年表

年代	官民	主な事項
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。 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）に再指定。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（NSA）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”で衛星オーナーの 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	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”(rev1.0.1)を発行。
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）作成中。
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。

MBSD 作成

c） 欧州における宇宙産業に係るセキュリティ動向

欧州では、欧州宇宙機関（ESA）等の宇宙関連の組織はあるものの、欧州を横断して取り組まれている施策等はまだ少ないようである。

表 2-3　欧州における宇宙産業に係るセキュリティ動向の年表

年代	官民	主な事項
2010.	官	[英] 英国宇宙革新成長戦略 2010～2030 で、宇宙を今後の成長産業／市場とし、国家宇宙指針及びその実行機関の必要性を掲げる。
2012.	官	[ECSS]ISO 24113:宇宙システム - スペース・デブリ低減要件と整合を図った ECSS-U-AS-10C を策定。
2012.	官	[英]民間宇宙戦略（Civil Space Strategy）で民間の成長支援を掲げる。
2014.	官	[英]英国宇宙革新成長戦略への政府の対応 2014-2030 で先の戦略を深化。
2014.	官	[英]国家宇宙セキュリティ政策（National Space Security Policy）で、国としての整備方針を示す。
2018.	官	[英]宇宙産業法 2018（Space Industry Act 2018）の制定。
2019.6.4	官	[英]首相が国家宇宙会議（National Space Council）の設立を発表。
2020.	官	[独]中国の国有軍需企業による衛星技術会社の買収をドイツ政府が阻止。
2020.11.	官	[ESA] 民間事業者によるスペース・デブリ除去任務を開始。

MBSD 作成

2.1.2. 宇宙システムに係るインシデント事例

次の文献ならびにホームページを対象として、宇宙システムに係るインシデント事例を抽出した。なお元資料に挙げられていても宇宙システムに係るとは確定できない事例は抽出対象から省いた。

- Manulis M: Cyber Security in New Space,2020/5
- PwC 社 HP: https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/space-cybersecurity-service.html
- NHK オンライン:衛星通じたネット通信 “漏えいの危険性” 英の研究者が指摘, 2020/8/6, https://threatpost.com/black-hat-satellite-comms-eavesdropping-hack/158146/ https://www3.nhk.or.jp/news/html/20200806/k10012554731000.html
- 内閣府宇宙開発戦略推進事務局 :『宇宙システムの機能保証強化に関する調査』,2019/3
- IPA:制御システムのセキュリティリスク分析ガイド第二版, 2020/3
- Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, Tyler Way, Makena Young: Space Threat Assessment 2020
- 佐々木雅英(NICT):宇宙×ICT の安心、安全対策,2017/2
- Ruben Santamarta: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

抽出されたインシデント 92 事例のうち、宇宙システムにおいて特徴的であると判断した 5 事例についてはさらに詳細に調査を実施した。

これら 92 事例を各カテゴリ（セグメント/セクター/テクニック/サブシステム）ごとに年代別に集計した結果を表 2-4 に、また各カテゴリ別の推移を図 2-1 に示す。

表 2-4　宇宙システムに係るインシデント数の年代別集計

カテゴリー	サブカテゴリー	発生年						合計
		1986-2000	2001-2005	2006-2010	2011-2015	2016-2020	NA[*1)]	
セグメント	データ通信	4	8	8	13	9	2	44
	地上セグメント	4	4	9	14	7	0	38
	宇宙セグメント	2	0	8	1	3	0	14
	不明	0	0	0	0	0	0	0
セクター	政府系	5	5	14	14	6	0	44
	商用	4	3	6	13	8	1	35
	軍事	2	3	4	2	3	0	14
	民間	0	3	2	4	4	0	13
	NA[*2)]	0	0	0	0	0	1	1
テクニック	CNE[*3)]	3	4	8	12	7	0	34
	ジャミング[*4)]	3	5	4	9	2	2	25
	乗っ取り[*5)]	2	2	4	1	2	0	11
	スプーフィング[*6)]	0	0	0	3	4	0	7
	サービス拒否	1	0	2	2	0	0	5
	事故	1	0	3	0	1	0	5
	盗聴	0	1	1	1	1	0	4
	ASAT	0	0	2	0	1	0	3
	コントロール	1	0	2	0	0	0	3
	ミーコニング[*7)]	0	0	0	1	0	0	1
	盗難・紛失	0	0	0	1	0	0	1
サブシステム	衛星本体	7	8	10	13	13	2	53
	衛星データ利用	0	1	6	11	2	0	20
	衛星運用	3	1	6	1	3	0	14
	開発・製造	0	2	1	3	2	0	8
	インシデント数	10	12	22	27	19	2	92

MBSD作成　複合的インシデントを複数分類で重複カウントしたため、縦計はインシデント数と一致しない

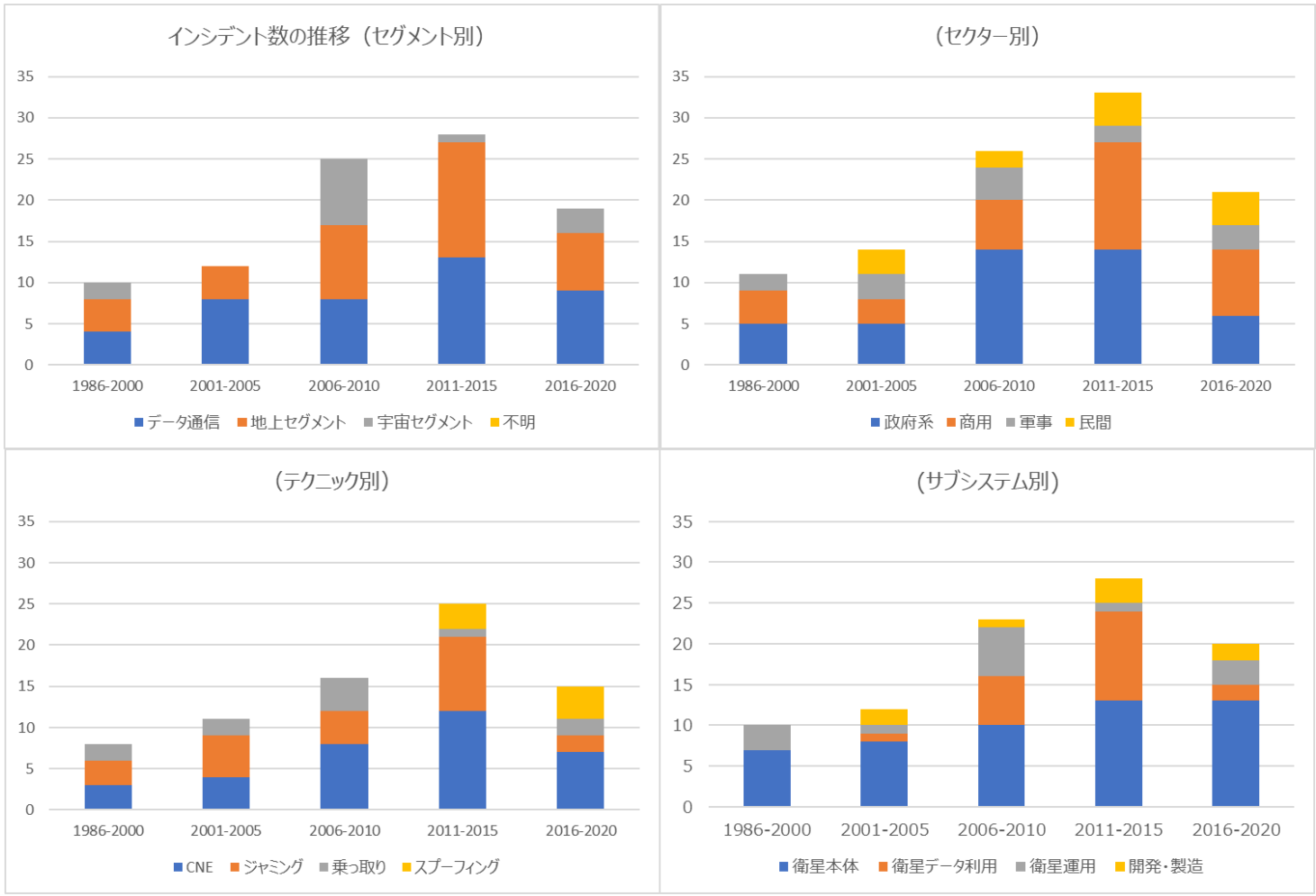
[*1)] 実インシデントは未発生であるが、インシデント発生の危険性が指摘(年度不明)されたもの

[*2)] 実インシデントは未発生であるが、インシデント発生の危険性が指摘されたもの

[*3)]Computer Network Exploitation, 諜報活動 [*4)]通信妨害

[*5)]CNE活動の延長で諜報活動に含まれる場合もあるが、電波ジャック(放送波の不正使用)や衛星ジャック(衛星の制御を不能にする)などを含む

[*6)]なりすまし[*7)]誤差混入させ再送信



複合的インシデントを複数分類で重複カウント等したため、各カテゴリ別総計は一致しない
MBSD作成

図 2-1　宇宙システムに係るインシデント数の推移（セグメント/セクター/テクニック/サブシステム別）

2.1.3. 国内事業者等へのヒアリング

表 2-5 に整理した国内における宇宙関連産業事業者（サプライチェーンを含む）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調査を行った。

表 2-5 ヒアリング先

ヒアリング先	日時	備考
A 社	2020.11.16	訪問、リモート会議併設
B 社	2020.11.18	リモート会議
C 社	2020.11.17	リモート会議
D 社	2020.12.02	訪問、リモート会議併設
E 社	2020.12.04	リモート会議
F 社	2020.12.07	訪問、リモート会議併設
G 社	2020.12.09	リモート会議
A 協議会	2020.12.09	リモート会議

ヒアリング内容から本事業の施策に対する主な意見を以下の 4 項目について整理した。

- コンセプトに対するコメント
- チェックリスト等へ組み込んで欲しいセキュリティ事項に対するコメント
- 参考にすべき海外の取り組み等に対するコメント
- 宇宙特有の考慮すべき事項に対するコメント

2.2. 課題等の分析

2.2.1. 脅威・リスクの抽出

2.1.2 で調査した結果をベースに、後述の対象システム（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・攻撃手法の例をサブシステム・想定される主な事業被害・リスクシナリオ例・侵入経路と攻撃手法について 5 つの例を示すとともに本調査で検討・明確化した対象システム上へのマッピングを試みた。

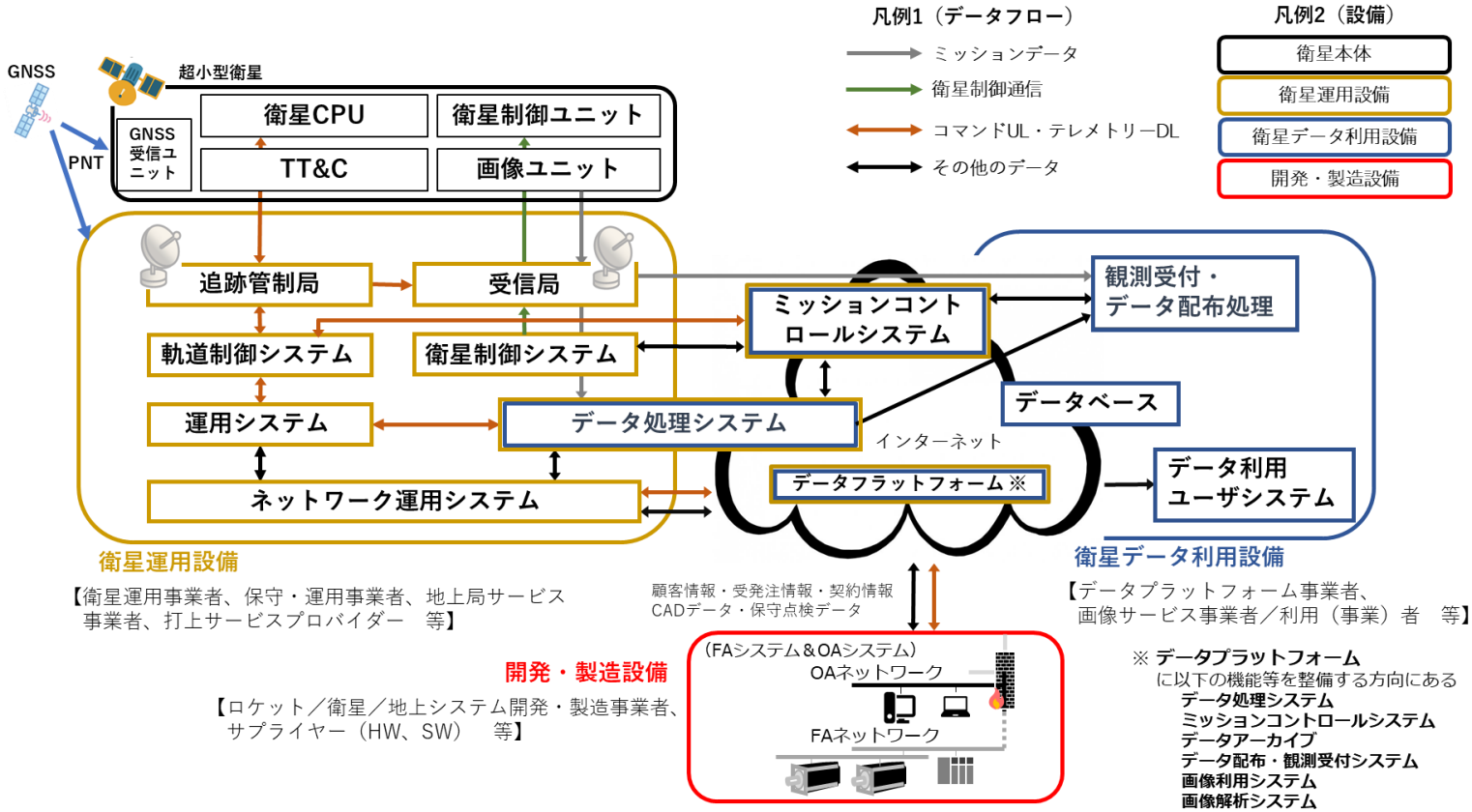
表 2-6　想定される主な事業被害とリスクシナリオの例

No.	サブシステム	想定される主な事業被害	リスクシナリオの例	侵入経路・攻撃手法の例
1	衛星本体	違約金が発生。	一時的に衛星の軌道制御を喪失する。	衛星と地上局の間の通信に対する攻撃
			衛星本体に対して地上からの遠隔操作により、正常な姿勢制御またはミッションができなくなる（機能不全）。	マルウェア感染及び不正操作
2	衛星運用設備	違約金が発生。 修復のための費用が発生。	衛星運用を行う地上のインフラシステムがサイバー攻撃を受け、長期間にわたり衛星の制御を失う。	悪意を持った内部犯行
3	衛星データ利用設備	違約金が発生。	不正アクセスを受けてランサムウェアに感染。その後、設備内の全サーバ及び端末に感染し、サービスを提供できなくなる。	OSコマンドインジェクション攻撃
4	OAシステム	違約金が発生。	インターネット経由のリモートアクセスにより施一計情報等が外部に漏えいする。	PC感染
5	FAシステム	違約金が発生。	マルウェアによって設備の制御が異常となり操業が停止する。	内部関係者の過失

インシデント事例等を参考に MBSD 作成

2.2.2.　主要なシステム構成（モデルケース）の作成

先ず、分析対象とする全体像として、データフローに着目した以下の図を全体イメージとした。



MBSD 作成

図 2-2　分析対象とする全体像のイメージ

次に、データフローに加え、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）における三層構造の第一層（フィジカル空間）に対応した企業間のつながりに着目し、宇宙システムにおける「組織間のつながり」を検討した。

さらに、分析対象とする全体像として、各システムの内部構造およびシステム間のつながりに着目した以下の図を全体イメージとし、作業部会におけるコメント等を踏まえ、システムの内部構造を簡略した上でシステム間のつながり及びデータフローに着目した民間宇宙システムの全体像（システム構成）を標準モデルとして作成した。

3. 検討会（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について検討を行った。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。

宇宙産業 SWG 構成員及び作業部会構成員を**エラー! 参照元が見つかりません。**に整理した。

検討会においては、本事業のゴール設定及び対象とする宇宙システム及び資産についての検討を実施した。

表 3-1　検討会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 1 回宇宙産業 SWG	2021.01.14 13:00～15:00	● 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起の公表について ● 宇宙産業と宇宙安全保障の連携の動向について ● ビル分野におけるサイバーセキュリティガイドライン開発 ● 近年の宇宙産業の動向 ● 近年のサイバー攻撃の動向 ● 宇宙分野におけるセキュリティインシデント事例 ● 海外における宇宙分野のセキュリティ対策 ● 検討体制・検討方針 ● ガイドライン開発について	座長、事務局出席のもとリモート会議併設
第 1 回宇宙産業 SWG 作業部会	2021.02.15 15:30～17:30	● 宇宙分野におけるセキュリティインシデント事例 ● 米国における宇宙分野のセキュリティ対策 ● 検討体制・検討方針 ● ガイドライン開発について	リモート会議
第 2 回宇宙産業 SWG	2021.03.03 15:30～17:30	● 宇宙システムのデータ構成 ● 制御システムのセキュリティリスク分析とインシデント事例 ● 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 v1.0 についての検討	座長、事務局出席のもとリモート会議併設

4. 施策のとりまとめ

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、民間宇宙事業者のビジネスを振興する観点から、宇宙システムに係るセキュリティ上のビジネスリスクや、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整備が急務と考える。

本事業においては、以下に示す内容のガイドラインの開発を目指すものである。

ガイドラインの概要：

2 章では宇宙システムにおけるインシデント事例を中心に整理するとともに、宇宙システムに将来的に影響を与えると考えられる一般的なインシデントについても整理する予定である。また、海外（主に米国）民間宇宙システムにおける施策等を参考に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について整理する予定である。

3 章では、民間宇宙事業者が宇宙システムのセキュリティ対策を検討する上で参考になるポイント、プラクティス、参考文献、活用可能な既存施策（例えば、IPA（独立行政法人情報処理推進機構）の「中小企業の情報セキュリティ対策ガイドライン」や、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録する制度である ISMAP など）をサブシステムごとに整理する予定である。

5. 今後の展開

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実施すべき 10 項目の検討・開発・整備内容を整理した。

検討・開発・整備内容例：

- 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（案）の開発・拡張・運用等についての検討
- 宇宙国内外における施策調査、インシデント事例の収集・整理・分析の継続　検討会・作業部会の運営

令和 2 年度　サイバー・フィジカル・セキュリティ対策促進事業
（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）

2021 年（令和 3 年）3 月 26 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・防衛グループ

二次利用未承諾リスト（公表用）

報告書の題名
令和２年度サイバー・フィジカル・セキュリティ対策促進事業（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）

委託事業名
令和２年度サイバー・フィジカル・セキュリティ対策促進事業（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
10	図2-2	分析対象とする全体像のイメージ
2	表2-1	全世界における宇宙産業に係るセキュリティ動向の年表
3	表2-2	米国における宇宙産業に係るセキュリティ動向の年表
4	表2-3	欧州における宇宙産業に係るセキュリティ動向の年表
6	表2-4	宇宙システムに係るインシデント数の年代別集計