資料４－２

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

令和６年３月

経済産業省 製造産業局 宇宙産業室

目　次

本ガイドラインの全体概要

		記載概要	利用方法
本編	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	• 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
本編	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	• 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
本編	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	• 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ー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ーラリングについて検討し、合意・承認することが必要）
本編	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	• 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
添付資料	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	• 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
添付資料	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）のフレームコアにおけるサブカテゴリーとの対応関係を整理	• 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
添付資料	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	• 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ーラリングした上で利用することが必要

1．はじめに

1．1 本ガイドライン作成の背景・目的

（1）背景 1：企業におけるサイバーセキュリティリスクの高まり

近年、AI、IoT、ビッグデータ等のデジタル技術の普及に伴い、「ビジネスに IT を活用する」域を超え、デジタル技術を前提として、顧客価値の実現に向けビジネスモデルや組織、業務、企業文化・風土等を抜本的に変革し、新たな成長・競争力強化に繋げていく「デジタルトランスフォーメーション（DX）」の取り組みが、グローバルレベルで推進されている。こうした中、企業は競争力維持・強化のために、DX をスピーディーに進めていくことが求められている。

一方で、デジタル技術の活用・依存の進展に伴うサイバー空間とフィジカル空間の融合により、サイバー攻撃による被害がフィジカル空間に及ぼす影響が増大している。実際、電力システム、石油化学プラント、自動車工場、ビルシステム等の制御システム（OT）へのサイバー攻撃や、フィジカル空間における脆弱な IoT 機器へのサイバー攻撃が既に数多く確認されている。また、サイバー攻撃の起点（侵入口）も拡大しており、クラウドサービスへの攻撃、企業での利用が拡大しているオープンソースソフトウェア（OSS）を狙った攻撃、グループ会社、海外拠点、取引先を狙った攻撃など、サプライチェーン上の弱点を狙ったサイバー攻撃が数多く確認されている。こうしたサイバー攻撃の中には、国家の関与が疑われる事例のほか、金銭目的の組織・集団・個人による情報・知財窃取、ファイルの暗号化による身代金要求（ランサムウェア）、フィッシングによる情報流出、クリプトジャッキングによる暗号資産の不正なマイニング等のサイバー犯罪も多く、中小企業を含むあらゆる企業がターゲットとなっている。

このように、デジタル技術の活用の進展に伴いサイバー攻撃の対象や起点は拡大しており、またその影響はサイバー空間における個人情報や営業秘密などの情報漏えい・知財窃取のリスクのみならず、フィジカル空間におけるシステムダウンによる事業停止のリスク、人命・安全に関わるリスク、資産の毀損により損害賠償が求められるリスク、レピュテーション（評判）リスクなどの様々な経営リスクと直結している。すなわち、経営層自らがサイバーセキュリティリスクを全社的な課題として捉え、リーダーシップを発揮して対策を実施する必要性が増している。経済産業省でも 2020 年 12 月に「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」を発出してサイバーセキュリティの取組の一層の強化を促している。[1]

[1] 経済産業省 :「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」（2020 年 12 月）
https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf

（２）背景２：宇宙システムにおけるサイバーセキュリティリスクの拡大

宇宙分野においても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。また、米国航空宇宙局（NASA）では、2017 年から 2020 年の 4 年間にフィッシング、マルウェア等のサイバー攻撃が 6,000 件以上検知されたとしている。[2]

宇宙システムのサイバーセキュリティの確保が重要かつ困難となってきている主な要因としては、以下が挙げられる。

- 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（5G 等）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

（３）背景３：宇宙システムのサイバーセキュリティに関する主な海外動向

こうした中、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 1－1 米国等における宇宙システムのサイバーセキュリティ関連施策

年月	主体	関連施策等
1990.7	官	NSD-42「National Policy for the Security of National Security Telecommunications and Information Systems」（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「Critical Infrastructure Protection in the Information Age」（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「Information Assurance (IA) Policy for Space Systems Used by the Department of Defense」（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）

[2] NASA Office of Inspector General/Office of Audits:「NASA'S CYBERSECURITY READINESS」（2021 年 5 月）
https://oig.nasa.gov/docs/IG-21-019.pdf

年月	主体	関連施策等
2007.3	官	NSD-42 を受け、CNSS が CNSSP 12「National Information Assurance Policy for Space Systems Used to Support National Security Missions」（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「Information Assurance Risk Management Policy for National Security Systems」（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「Supply Chain Risk Management (SCRM)」（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 への対応について解説。
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、米国宇宙軍及び米国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「Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services」（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「Commercial Space System Security Guidelines」（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「Cybersecurity Principles for Space Systems」（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。
2022.3	官	CISA 及び FBI が、AA22-076A 「Alert (AA22-076A) Strengthening Cybersecurity of SATCOM Network Providers and Customers」（国際衛星通信のネットワークに対するサイバー攻撃の脅威に関する緩和策や関連情報をまとめたセキュリティアドバイザリー）を発表。
2022.4	官	DHS が、国土安全保障に係る宇宙政策を示す文書である「DHS Space Policy」を更新。
2022.5	官	米国宇宙軍が、IA-Pre「Infrastructure Asset Pre-Approval」（米国 DoD が調達する商用衛星通信サービスの事前セキュリティ評価プログラム）の試行を開始。
2022.6	官	ドイツ情報セキュリティ庁（BSI）が、「IT-Grundschutz-Profil für Weltrauminfrastrukturen (Basic IT Protection Profile for Space Infrastructures)」（衛星システムに対するサイバーセキュリティ対策ベースライン）を発表。
2022.8	官	ドイツ情報セキュリティ庁（BSI）が、「Cybersicherheit für Weltrauminfrastrukturen (Cybersecurity for Space Infrastructures)」（宇宙インフラのサイバーセキュリティ戦略）を発表。

年月	主体	関連施策等
2022.10	民	米 Aerospace Corporation が、MITRE ATT&CK ベースの攻撃フレームワークである「Space Attack Research and Tactic Analysis（SPARTA）」を発表。
2022.11	官	欧州理事会が、「NIS Directive」（ネットワーク・情報セキュリティ指令）を改正した「NIS2 Directive」を可決。対象セクターに、新たに宇宙セクター（加盟国又は民間企業が所有、管理、運営する、宇宙サービスの提供を支援する地上インフラ事業者）を追加。また、Critical Entities Resilience（CER）を採択し、リスク管理やサイバーインシデントが起きた際の報告義務が示されている文書を作成。
2022.12	官	NIST が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文書である NISTIR 8401「Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control」を作成。
2023.3	官	欧州委員会は、宇宙空間の脅威を評価するため、「EU Space Strategy for Security and Defence」を作成。サイバー領域については、NIS2 Directive と連携しつつ、レジリエンスや保護能力を高めることが必要である明記。
2023.4	官民	Aerospace Corporation、米宇宙軍宇宙システムコマンド、米国空軍研究所が共同で、サイバー防御のスキルの向上に向けたトレーニングの提供と研究を目的としたハッキング可能な低軌道衛星「Moonlighter」の打上げ・運用を発表。
2023.5	官	ドイツ情報セキュリティ庁（BSI）が、「TR-03184 Informationssicherheit für Weltraumsysteme（Information security for space systems）」（宇宙インフラのサイバーセキュリティ戦略）を発表。
2023.6	官民	米国電気電子学会（IEEE）は宇宙システムに対するサイバーセキュリティ確保の重要性を受け、宇宙システムのサイバーセキュリティに関する包括的な標準を開発することを目的として、「Space System Cybersecurity Working Group」を設立。
2023.7	官	NIST が商用衛星運用のためのセキュリティ入門書である NISTIR 8270「Introduction to Cybersecurity for Commercial Satellite Operations」を作成。
2023.9	官	NIST がハイブリッド衛星ネットワーク（Hybrid Satellite Networks: HSN）を使用するサービスに関するセキュリティプロファイルである NISTIR 8441「Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)」を作成。
2023.9	官民	欧州委員会は、European Union Agency for the Space Programme（EUSPA）と共同で、新たに EU Space ISAC を設立することを発表。順次参加者の募集を開始。
2024.1	官	NASA が、宇宙セキュリティに関するベストプラクティスを示したガイドである「Space Security : Best Practice Guide」の第 1 版を作成。
2024.2	官	ENISA（欧州ネットワーク情報セキュリティ機関）が低軌道通信衛星（LEO SATCOM）のサイバーセキュリティを調査した「Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment」を作成。

（4）本ガイドライン作成の目的

このように、企業における宇宙システムのサイバーセキュリティリスクが拡大し、海外でも議論や取組が活発化する中、宇宙基本計画工程表（令和 2 年 12 月 15 日閣議決定）では、宇宙システム全体の機能保証強化の一環として、宇宙システムのサイバーセキュリティ対策のための民間企業向けガイドラインを開発することとされた。

我が国の国民生活や安全保障上の重要な宇宙システムの中には、民間事業者が主たる担い手となっているものも多く存在するため、本ガイドラインでは、前述の環境変化や海外動向も踏まえつつ、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している。

（５）本ガイドラインの開発・更新のプロセス

本ガイドラインは、以下のプロセスで開発を行った。

- 産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下に設置した宇宙産業サブワーキンググループ（SWG）において検討。
- 宇宙産業 SWG には、実務者から構成される作業部会を設置し、技術的な論点については作業部会において検討。
- 検討に当たっては、以下を基本的なフレームワークとして活用。
    - ✓「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）
    - ✓「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 情報処理推進機構）
    - ✓JAXA、他産業、海外の取組との調和を念頭に置きつつ開発。

Ver 1.1 では、対策要求事項に関するチェックリストや、NIST Cybersecurity Framework（NIST CSF）と宇宙システム特有の対策との対応関係表をそれぞれ添付資料１、添付資料２として追加するとともに、その他軽微な修正等を行った。Ver 2.0 では、ガイドラインの対象である宇宙システムのスコープを拡大し、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対象とした。スコープの拡大に伴い、想定されるリスクシナリオの追加及び具体的な対策内容に関する改訂を実施した。加えて、NIST CSF のバージョン 2.0（NIST CSF 2.0）が公開されたことを踏まえ、添付資料１の対応を見直したほか、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活用できる情報セキュリティ関連規程の雛形を新たに添付資料３として追加した。

今後も、国内外の最新の知見を取り入れ、1 年に 1 回程度の見直しを図っていくこととする。また、本ガイドラインで引用している参考文献については最新版を確認すること。

１．２ 本ガイドラインの対象範囲

本ガイドラインは、特定の分野（観測衛星、通信衛星、放送衛星等）やシステム規模等に限定せず、民間企業が主体となる衛星システム及び地上システム（衛星運用システム、衛星データ利用システム、衛星通信システム及び開発・製造システム）を対象とする。衛星システムについては、設計・開発・製造、運用・保守及び廃棄フェーズを対象とする。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するものの、システム自体の設計から廃棄までの各フェーズについて特に注意すべき点については対象とする。打上設備については本ガイドラインの対象外とする。

参考のため、衛星システムのライフサイクルとステークホルダーの関係を図 1-1 に整理した。なお、本ガイドラインの対象範囲は随時更新することとする。

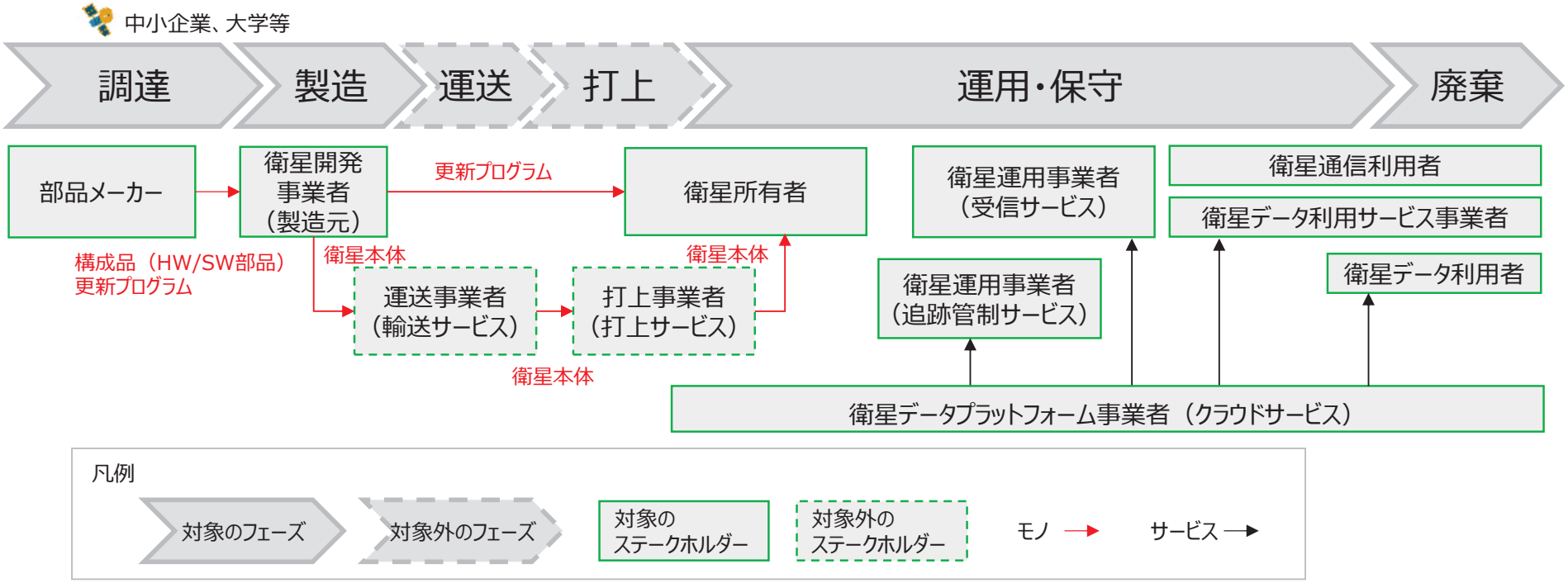

図　1－1　衛星のライフサイクルとステークホルダーの関係の概観

１．３ 本ガイドラインの構成及び想定読者

本ガイドラインの構成及び想定読者を表 1-2に示す。本ガイドラインの各項目のうち、各想定読者に対応する部分を★で示している。

なお、各事業者の経営層は、特に「本ガイドラインの全体概要」、「１．はじめに」及び「２．宇宙システムを取り巻くセキュリティに係る状況」について参照することが望まれる。

表 1-2　本ガイドラインの構成及び想定読者

	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。

「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、宇宙システム関連の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する。

「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、３．１節において一般的な共通的対策、３．２節において宇宙システム特有の対策として各サブシステム（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、開発・製造システム）に求められるセキュリティ対策のポイントを整理する。

１．４ 本ガイドラインの利用方法

本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において、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。

検討対象となる宇宙システムや事業者のビジネス環境は様々であることから、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である。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であるほか、各ステークホルダーのセキュリティ対策上の役割を明確化したうえで、役割を踏まえた責任分界点を明確化することが必要である。

本ガイドラインでは、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に NIST Cybersecurity Framework (NIST CSF) と本ガイドラインの３．２．２～３．２．５に示す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、添付資料３に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整理している。本ガイドライン及び各添付資料について、表 1-3 の利用方法を参照しつつ、対策の検討・実施や情報セキュリティ関連規程の作成・見直しをいただきたい。

表 1-3 各資料の利用方法

区分	項目	概要及び利用方法
本ガイドライン	3.1 共通的対策	「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」（本ガイドライン）における共通的対策（3.1.1 項～3.1.5 項）では、一般的に普及しているセキュリティ対策のうち、事業者が取り組むことが推奨される実践や対策事項が記載されている。自社における一般的なセキュリティ対策の検討・実施時に参照可能である。
	3.2 宇宙システム特有の対策	本ガイドラインにおける宇宙システム特有の対策（3.2.1 項～3.2.5 項）では、宇宙システムを扱う事業者が特に取り組むことが推奨される実践や対策事項が記載されている。宇宙システムに関するセキュリティ対策の検討・実施時に参照可能である。
添付資料	【添付資料 1】対策要求事項チェックリスト	本ガイドラインにおける共通的対策（3.1.1 項～3.1.5 項）及び宇宙システム特有の対策（3.2.2 項～3.2.5 項）の要求事項が表形式で整理されている。自社における対策に関して、要求事項の達成度の確認や、セキュリティ対策の検討・見直し時に利用可能である。
	【添付資料 2】NISTCSF と宇宙システム特有の対策との対応関係	NIST の「Cybersecurity Framework (NIST CSF)」のフレームコアにおける各サブカテゴリーと、本ガイドラインにおける宇宙システム特有の対策（3.2.2 項～3.2.5 項）との対応関係が整理されている。セキュリティ対策の検討・実施時に利用可能である。
	【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「中小企業の情報セキュリティ対策ガイドライン」の「付録 5：情報セキュリティ関連規程（サンプル）」をベースに、本ガイドラインの内容等を踏まえた宇宙事業者特有の内容が追記され、整理されている。自社の情報セキュリティ関連規程の作成・見直し時に利用可能であるほか、規程の上位階層に位置づけられる基本方針や規程の下位階層の細則、実施手順、運用規則等の作成・見直し時にも利用可能である。なお、雛形の項目は必ずしも全ての事業者において十分なものではないため、適宜テーラリングして利用することが求められる。

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

（1）宇宙システムにおけるインシデント事例

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。以下に事例の一部を示す。

表 2-1　宇宙システムにおけるセキュリティインシデント事例（一部抜粋）[3]

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 機全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 のサービスが、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、全ての観測を停止した。

[3] 各種公開情報に基づき作成

年	対象	影響	概要
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 社の下請業者である 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、機密情報の漏えい	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えいしたとしている。

（2）宇宙システムに関連する重要インシデント事例

宇宙分野以外のセキュリティインシデントの中には、宇宙分野にも参考になるものがある。以下に宇宙システムに関連しうる事例を示す。

表 2-2　宇宙システムに関連しうるインシデント事例[4]

年	対象	影響	概要
2019	リアルタイム OS VxWorks	不正アクセス等の可能性	医療、自動車、航空機、防衛等幅広い産業において 20 億個以上のデバイスで採用される WindRiver 社の VxWorks に 11 個の脆弱性があることが発表された。このうち 6 個は致命的な脆弱性とされているが、パッチを当てることが困難な機器も多いとされている。
2020	天然ガス圧縮施設	天然ガス圧縮施設の停止	米国の天然ガス圧縮施設がランサムウェアを使ったサイバー攻撃を受け、2 日間の操業停止に追い込まれた。
2020	NASA を含む最大約 18,000 組織	情報漏えい等	SolarWinds 社は、ネットワーク監視ソフトウェア Orion Platform に正規のアップデートを通じてマルウェアが仕込まれたことを発表。初期段階のマルウェアは、セキュリティサービスの検知を回避しつつ被害組織の情報を C&C サーバーへ送信。攻撃者が関心のある標的に対しては第 2 段階のマルウェアが投入された。
2020	Qualcomm 社 Snapdragon	情報漏えい等の可能性	スマートフォンで使用されているシステムオンチップ（SoC）である Qualcomm 社の Snapdragon に 400 個超の脆弱性が発見された。 （なお、NASA の初期小型衛星でも同 SoC を利用していたケースあり）
2021	Microsoft Exchange Server	バックドア設置等	Microsoft 社は Microsoft Exchange Server の 4 つの重大なゼロデイ脆弱性を悪用した不正アクセス事案の発生を公表。本事案が判明した時点で、全世界で数十万にのぼる組織が攻撃を受けたとされている。
2021	Apache Software Foundation Apache Log4j	情報漏えい等、任意のコマンドの実行の可能性	Apache Software Foundation がオープンソースで提供している 「Apache Log4j」において、リモートコード実行の脆弱性が発表された。遠隔の第三者が細工したデータを送ることで、任意のコマンドを実行される可能性がある。
2023	MOVEit	情報漏えい、不正アクセス等の可能性	米 Progress Software が開発・販売するファイル転送ソフト「MOVEit」において、情報漏えいや不正アクセス等につながるおそれのある複数の脆弱性が発表された。500 以上の組織、3,400 万人以上の個人情報の漏えいに繋がったとも報告されており、影響を受けた組織の中には、米国エネルギー省、英国放送通信庁等の行政機関のほか、米国・英国の大手企業が含まれる。

[4] 各種公開情報に基づき作成

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

（１）全体像の把握のためのフレームワークについて

前述のとおり、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 2 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の整理をすることが推奨される。

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）のように一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事業者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。

CPSF では、図 2-1 のように、産業社会を 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。

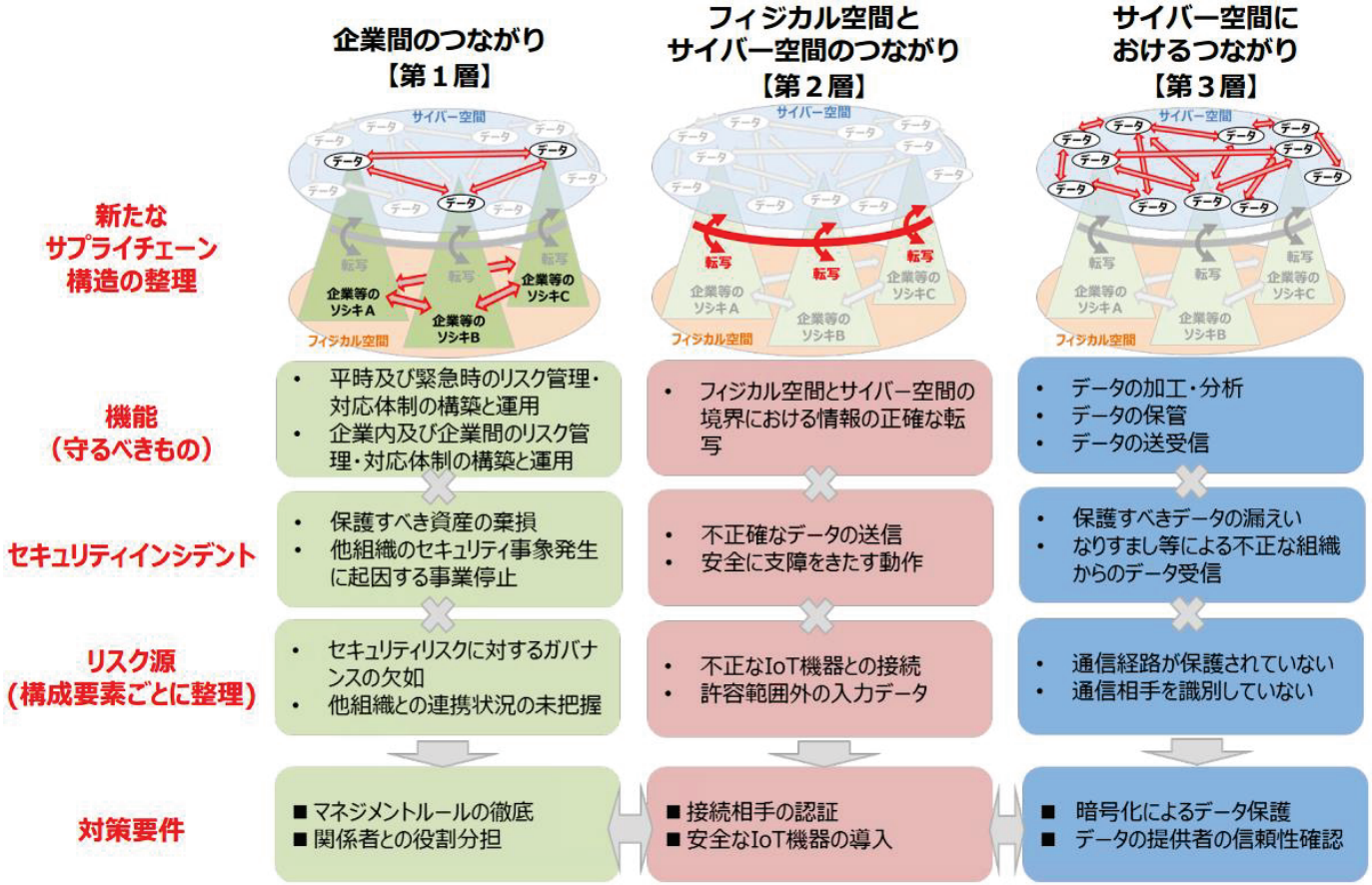

図　2－1　CPSF の全体概要

（２）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 2-2 を提示している。次項では、まず Step 1 の分析対象の明確化を行う。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うるリスクシナリオ」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する。

なお、Step 1～4 の実務的作業レベルでの手順として、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）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、本ガイドの活用を勧める。

図　2-2　CPSF で示されるセキュリティリスクマネジメントの流れ

（３）民間宇宙システムの標準的なモデル

民間宇宙システムの全体像及びステークホルダーの関係性を整理し、以下の標準的なモデルを作成し分析対象を明確化した。各システムやステークホルダーに関する概要は表 2-3及び表 2-4に示すとおりである。

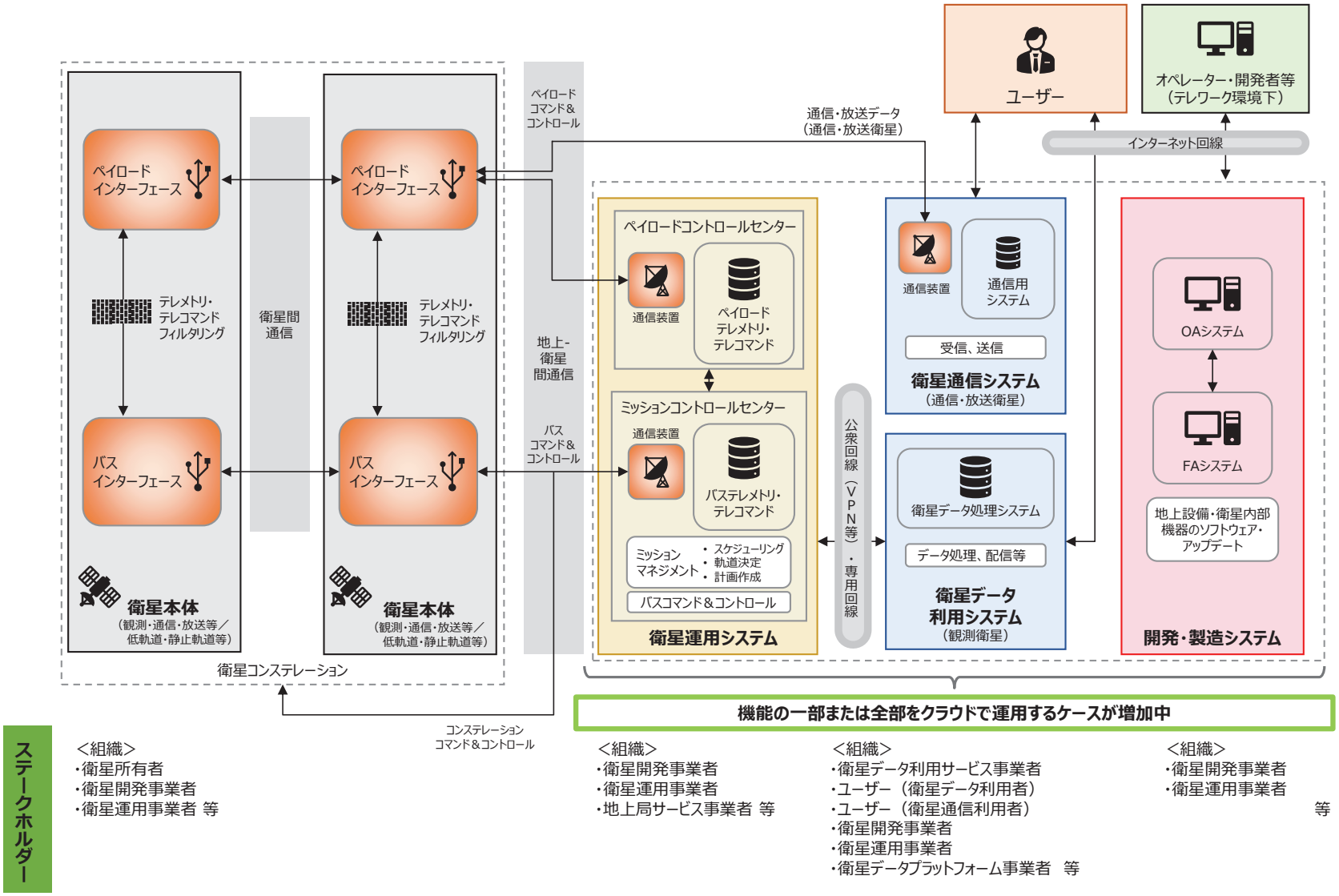

図 2-3　宇宙システムの標準的なモデル

表 2-3　標準モデルにおける各システムの説明

システム名称	説明
衛星本体	衛星システムのうち、測位、通信・放送、気象観測、地球観測を行う個々の衛星をいう。
衛星コンステレーション	同型、異型を問わず複数の衛星が連携・協調して動作することにより共通のミッションを遂行するための衛星運用形態をいう。
衛星運用システム	追跡管制局、受信局等の衛星運用を行う設備及びミッションコントロールシステム等の総称をいう。
ペイロードコントロールセンター	ペイロードをコントロールする機能を持つ衛星運用システムのことをいう。
ミッションコントロールセンター	バス機器をコントロールする機能を持つ衛星運用システムのことをいう。
衛星通信システム	衛星通信あるいは衛星放送において、データの受送信や処理等を行う設備の総称をいう。
衛星データ利用システム	観測衛星データの保存や処理、観測受付、データの配布等を行う設備の総称をいう。
開発・製造システム	衛星開発及び地上システム開発のための施設、設備、システム等の総称で、OT システム（FA システム)、IT システム（OA システム等)、検査設備等を含む。

表 2-4　標準モデルにおける各ステークホルダーの説明

ステークホルダー名称	説明
衛星所有者	衛星を調達し、衛星本体に責任を持つ者をいう。衛星所有者が衛星開発製造、衛星運用、衛星データ利用、廃棄まで全てを実施する場合や衛星運用等を衛星運用事業者等に委託する場合がある。
衛星開発事業者	衛星システムの企画・開発・製造を行う事業者をいう。衛星所有者が兼ねる場合もある。
衛星運用事業者	地上局（追跡管制局、受信局）を整備又は地上局サービス事業者を利用して軌道上の衛星の運用を行う事業者をいう。衛星所有者が兼ねる場合もある。
地上局サービス事業者	衛星運用に必要な追跡管制局、又は受信局を整備し、追跡管制サービス、又は受信サービスを提供する事業者をいう。
衛星データ利用サービス事業者	ミッションデータ処理システム、保存・検索システム、観測受付・データ配布処理システム等を整備し、衛星データ利用者が観測衛星データの利用を容易にするためのサービスを提供する事業者をいう。
ユーザー（衛星データ利用者）	事業あるいは研究の目的を達成するために観測衛星データを活用する企業ユーザー、個人ユーザー等をいう。
ユーザー（衛星通信利用者）	衛星通信あるいは衛星放送を活用する企業ユーザー、個人ユーザー等をいう。
衛星データプラットフォーム事業者	観測衛星データの保存・解析機能等を提供する企業で、データの横断的な連携や解析を可能にする事業者をいう。クラウドの形態でサービスを提供する事業者を含む。
オペレーター・開発者等（テレワーク環境下）	テレワーク環境より、リモートで衛星データ利用システムや開発・製造システムにアクセスする担当者等をいう。

宇宙システムに対するリスク分析を行う場合、図 2-3のモデル図をさらに具体化し、データフローを明確化した詳細なモデル図を作成して、分析を進めることが望まれる。一例として、近年の新規参入が活発な観測衛星システムを分析対象とした場合、以下のような詳細モデル図となる。

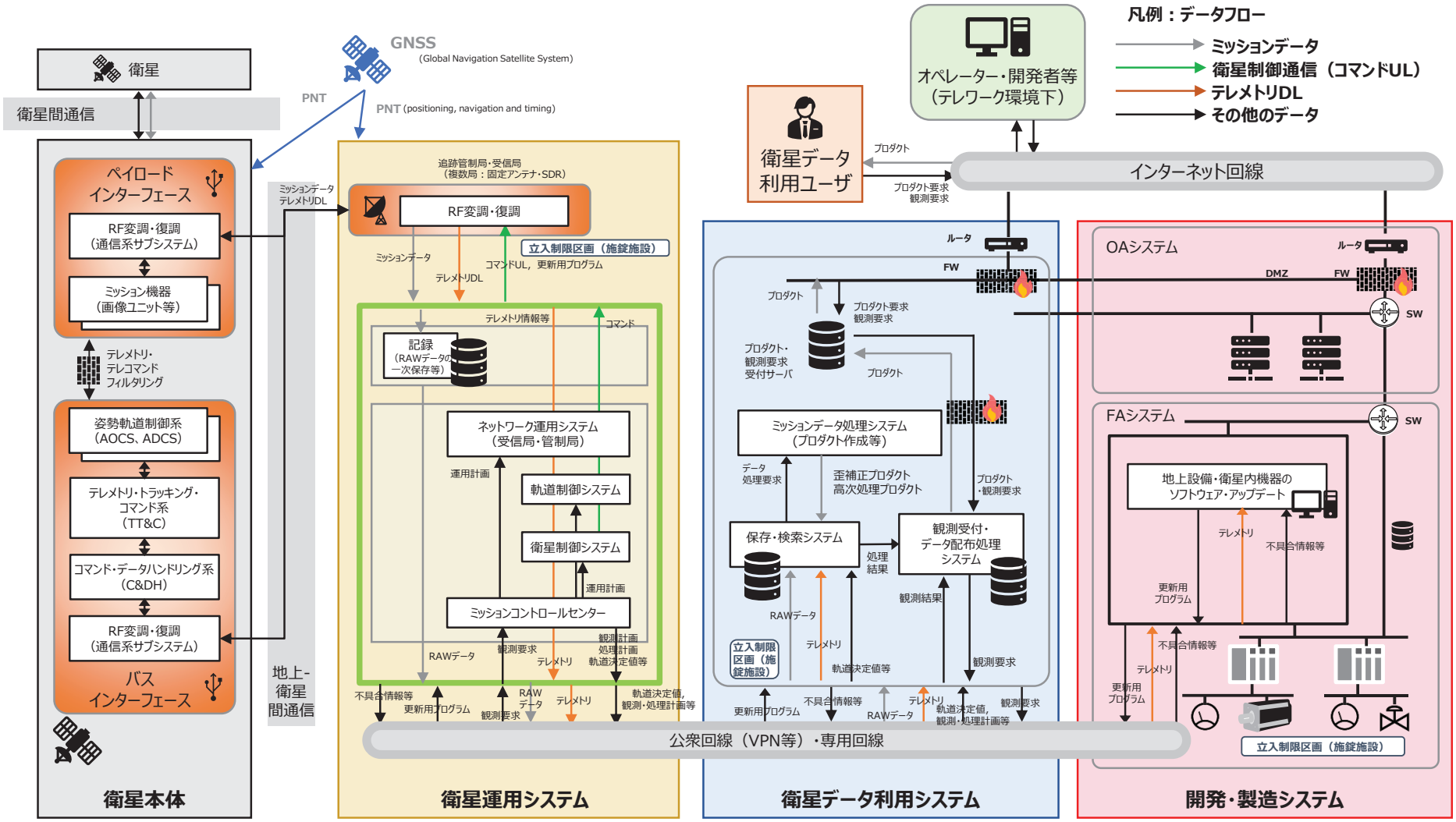

図　2－4　観測衛星を分析対象とした場合の詳細モデル図例

コラム：Consequence-Driven Cyber-informed Engineering (CCE) について

米国のエネルギー省（DOE）傘下のアイダホ国立研究所（INL）において開発された Consequence-Driven Cyber-informed Engineering（CCE）は、電力設備やプラント等の重要インフラシステムの開発・システム更新時に制御システムのエンジニアが活用することを想定して開発されたセキュリティリスクマネジメントの手法である。

CCE は大きく 4 つの検討ステップに分かれている。

- 1st Quad では、対象のシステムにおいて「発生してほしくない事象」を洗い出し、対応の優先順位をつける。ここでは、サイバーセキュリティのことは考えず、単に発生してほしくない事象を検討する。宇宙システムであれば、「衛星の停止」、「機微な衛星データの漏えい」等が挙げられる。
- 2nd Quad では、それらの事象を引き起こす関連システムやサブシステムを洗い出す。
- 3rd Quad は、1st Quad の事象を 2nd Quad のシステムを用いて発生させるには、どのようなサイバー攻撃が考えられるかを検討する。
- 4th Quad では、3rd Quad のサイバー攻撃に対応するセキュリティ対策を検討する。

各 Quad は、前項の CPSF の Step 1～4 の分析に対応する。

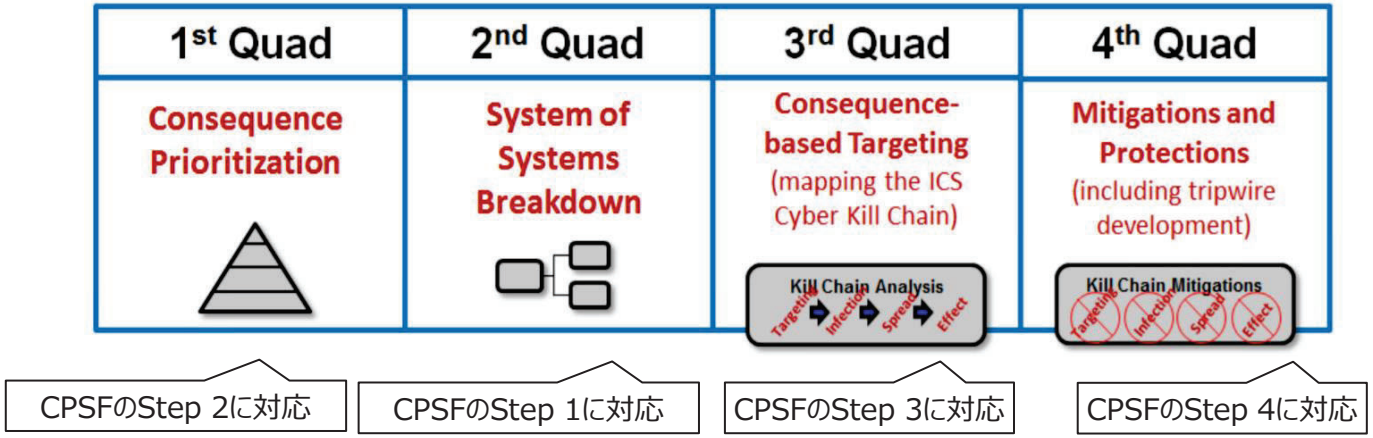

図 2-5 CCE の 4 つの検討ステップ

（４）発生してほしくない事象の例

宇宙システムにおける「発生してほしくない事象」の例を以下の図中に示す。次項ではこれらの事象を及ぼしうるリスクシナリオを複数検討する。

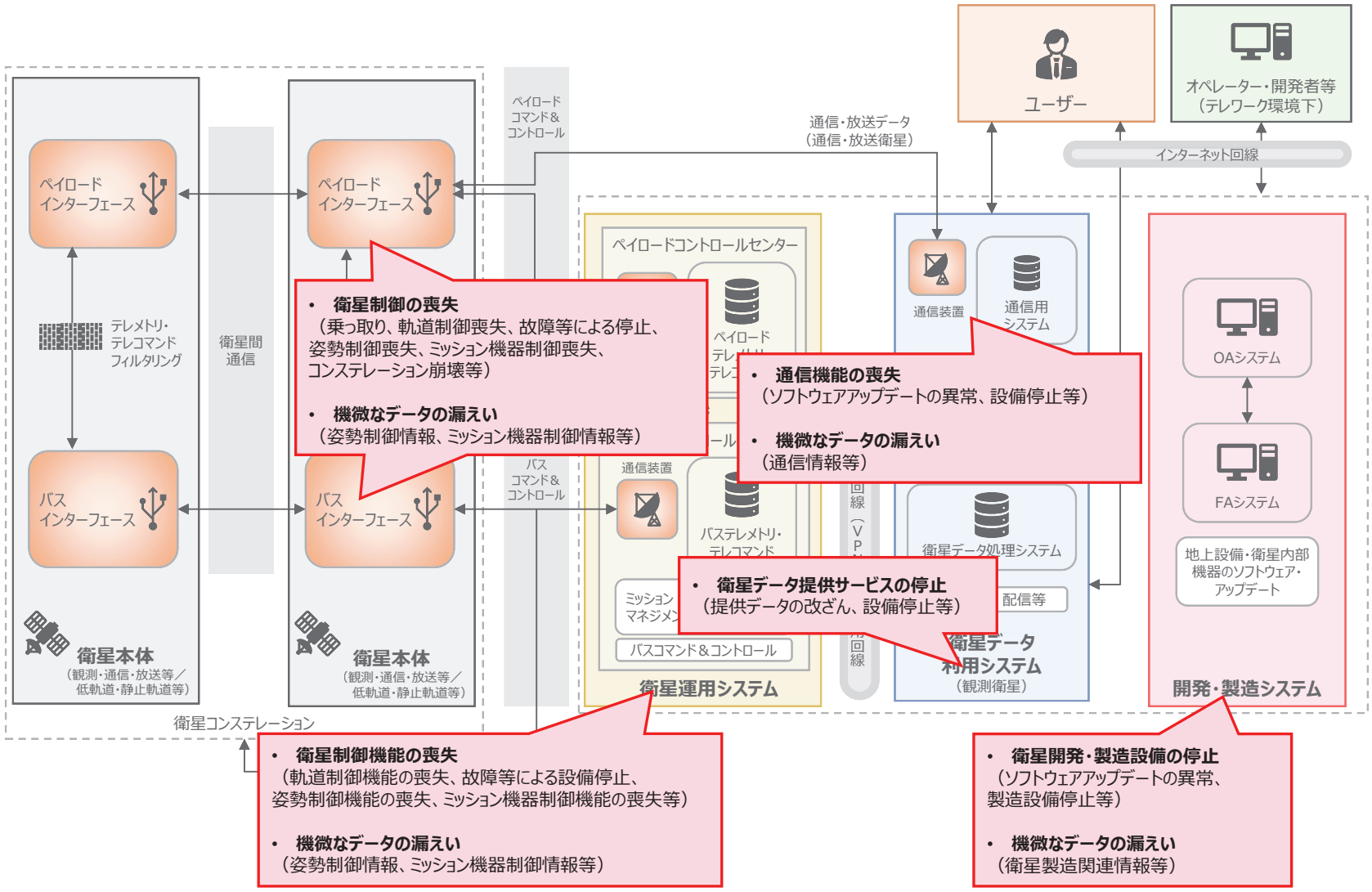

図　2－6　発生してほしくない事象の例

（5）想定されるリスクシナリオの例

本ガイドラインでは、重大な事業被害を及ぼしうるリスクシナリオの例として、以下の 13 の例を示す。これらのリスクシナリオ例では、悪意ある攻撃者が関与することを主に想定しているが、各ステークホルダー内部の関係者による偶発的な操作等、意図しない原因によって引き起こされるリスクも存在することに留意が必要である。

以降では、宇宙システムの標準的なモデルに基づき、各リスクシナリオ例の概要を図示する。

表 2-5　想定されるリスクシナリオの例

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
例 1	標準型メール攻撃による衛星軌道制御の喪失	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。	・ 衛星と地上局の間の通信 ・ インターネット	・ なりすまし・リプレイ攻撃 ・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 機微情報の漏えい ・ 衛星制御の喪失
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	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。	・ 衛星と地上局の間の通信 ・ インターネット	・ 地上からの不正な遠隔操作 ・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動） ・ バックドアプログラム	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ ミッション機器の制御の喪失
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	衛星データ利用システム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、システム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。	・ インターネット	・ 未許可端末の接続に伴う不正侵入 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 衛星制御の喪失

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
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	データ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、サーバー環境の設定不備によりシステム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。	・ インターネット	・ Web アプリケーションに対する攻撃 ・ マルウェア感染（ランサムウェア、ワイパー攻撃等）	・ 諜報機関又は産業スパイ	・ 衛星サービスの提供不能
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	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。	・ インターネット	・ 電子メールを介したマルウェア感染 ・ CNE（諜報・工作活動）	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 企業秘密の漏えい
例６	無許可 USB メモリの利用による操業停止	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。	・ クローズド環境における外部記録媒体	・ USB メモリを使ったことによるマルウェア感染 ・ BadUSB	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 開発・製造システムの操業停止
例７	不正な衛星搭載機器の受入による衛星コンステレーション崩壊の危機	衛星搭載機器調達の際、不正な基板であることに気付かずに受入れて衛星群に搭載。打上げ後の特定条件成立によりロジックボムが起動し、衛星コンステレーションが崩壊の危機に直面する。	・ サプライチェーンにおける不正部品の調達・組込み	・ 受入検査を怠ったことによる不正基板の受入れ ・ 不正改造基板の製作	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 衛星コンステレーション崩壊の危機
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	VPN ルータの設定ミスを足掛かりに、衛星運用システムが不正アクセスを受ける。衛星運用システム内のシステムがマルウェアに感染した後、衛星ブロードバンド通信経由でマルウェアが衛星ユーザーに伝送され、通信衛星のサービスが利用できなくなる。	・ インターネット（VPN）	・ VPN ルータの脆弱性を悪用した攻撃 ・ マルウェア感染	・ 諜報機関又は産業スパイ	・ 衛星通信機能の喪失
例９	ユーザー端末の不正改造による情報の不正送信	攻撃者が用意した通信装置に対して、攻撃者が用意した通信装置に対して不正なチップを取り付けることで、任意コードの実行が可能な状態にする。地上システムから衛星ブロードバンド通信経由で不正情報を伝送する。	・ 衛星と地上局の間の通信	・ ユーザー端末の不正改造 ・ 地上不正端末からの不正操作	・ 諜報機関又は産業スパイ	・ 不正情報の伝送

No.	シナリオ例	概要	侵入経路	攻撃手法	脅威源	影響
例 10	衛星通信の傍受による機微情報の漏えい	ユーザーに向けて平文で送信されている衛星のブロードキャスト通信に対して、公開情報を基に通信衛星の場所を特定し、攻撃者が用意したアンテナを用いて通信傍受する。傍受された機密情報が外部に漏えいする。	・ 衛星と地上局の間の通信	・ 攻撃用アンテナの用意 ・ 衛星ブロードキャスト通信の傍受	・ 諜報機関又は産業スパイ	・ 機微情報の漏えい
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	通信衛星が衛星放送のために送受信している電波に対して、攻撃者の用意した機器が発する妨害電波によるジャミングが行われる。衛星放送通信が妨害され、衛星放送が停止される。	・ 衛星と地上局の間の通信	・ 攻撃用アンテナの用意 ・ 衛星ブロードキャスト通信のジャミング	・ 諜報機関又は産業スパイ	・ 衛星放送サービスの停止
例 12	内部犯による衛星制御のハッキング	衛星運用に関する従業員が、悪意を持ってシステムに管理者アカウントでログインする。ログイン後、不正なミッションを遂行するコマンドや、ミッション機器制御情報を悪用した不正コマンドを衛星に送信する。	・ 内部犯（特別な侵入なし）	・ 管理者アカウントでの不正ログイン ・ テレメトリ・データの傍受・解析 ・ 衛星本体への不正コマンドの送信	・ 内部犯	・ 衛星通信機能の喪失
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	ソフトウェアベンダーが侵害され、宇宙システム開発に利用する SDK のインストーラーにマルウェアが同梱され公開される。ソフトウェア更新を通じて、マルウェアを同梱するインストーラーを実行し、開発環境の端末やサーバーがマルウェアに感染する。	・ サプライチェーンにおける不正部品の調達・組込み ・ インターネット	・ CNE（諜報・工作活動） ・ インストーラーの改ざん ・ マルウェア感染 ・ ソフトウェア更新時のマルウェアチェック不備	・ 諜報機関又は産業スパイ ・ セキュリティ意識の低い従業員	・ 開発・製造システムの操業停止

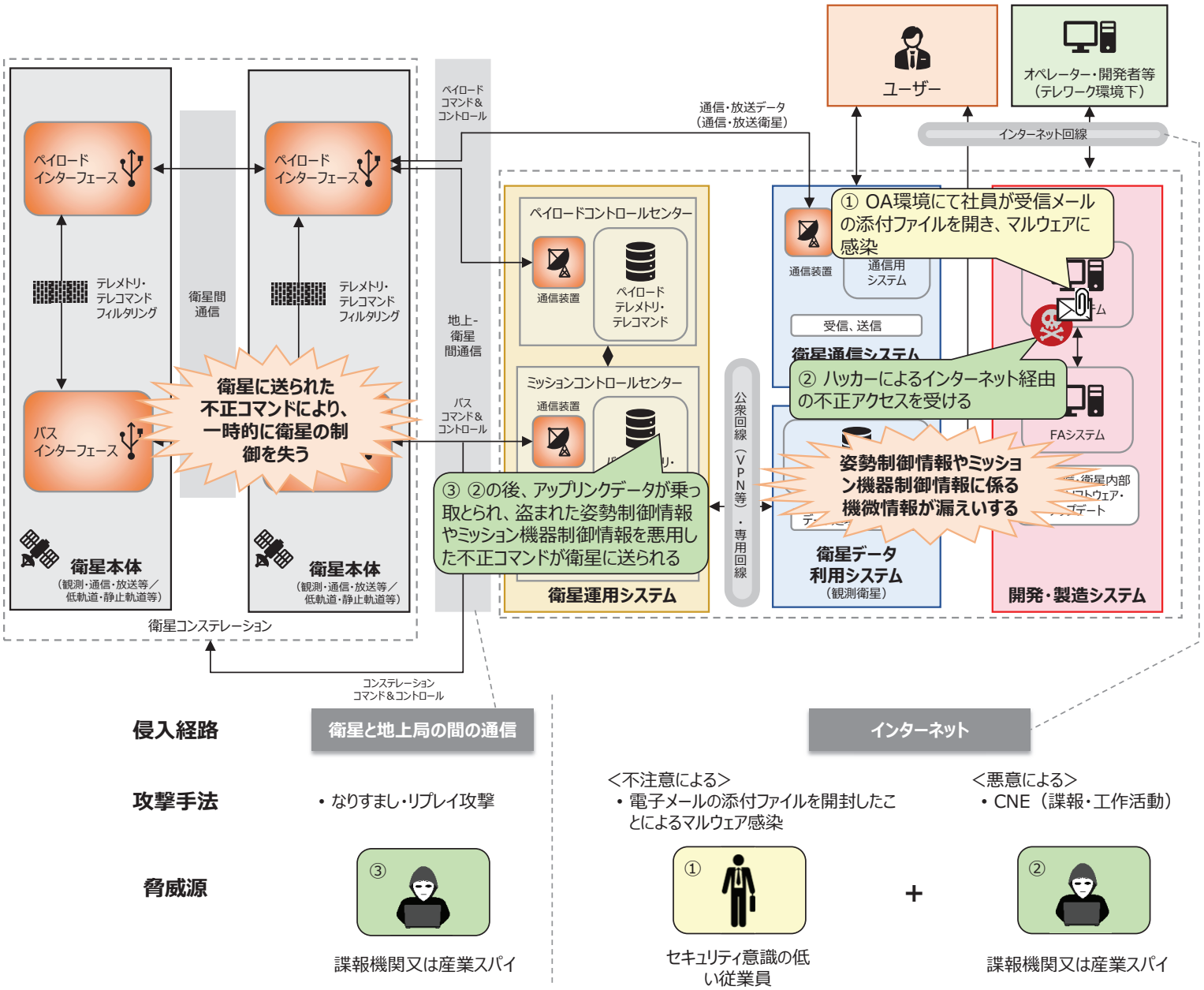

図　2－7　リスクシナリオ例１：標的型メール攻撃による衛星軌道制御の喪失

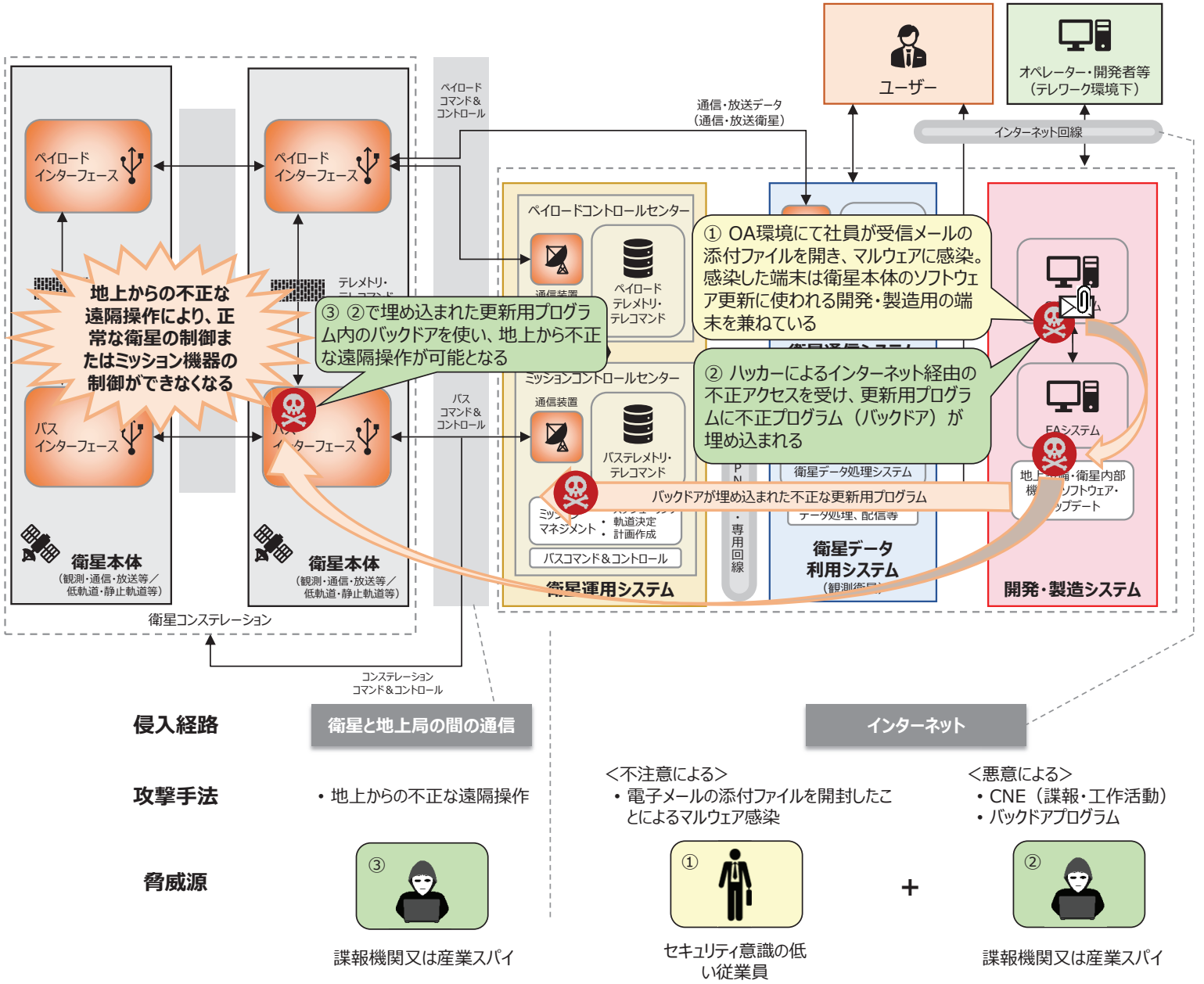

図　2－8　リスクシナリオ例２：開発製造用端末のマルウェア感染による衛星・ミッション機器制御の喪失

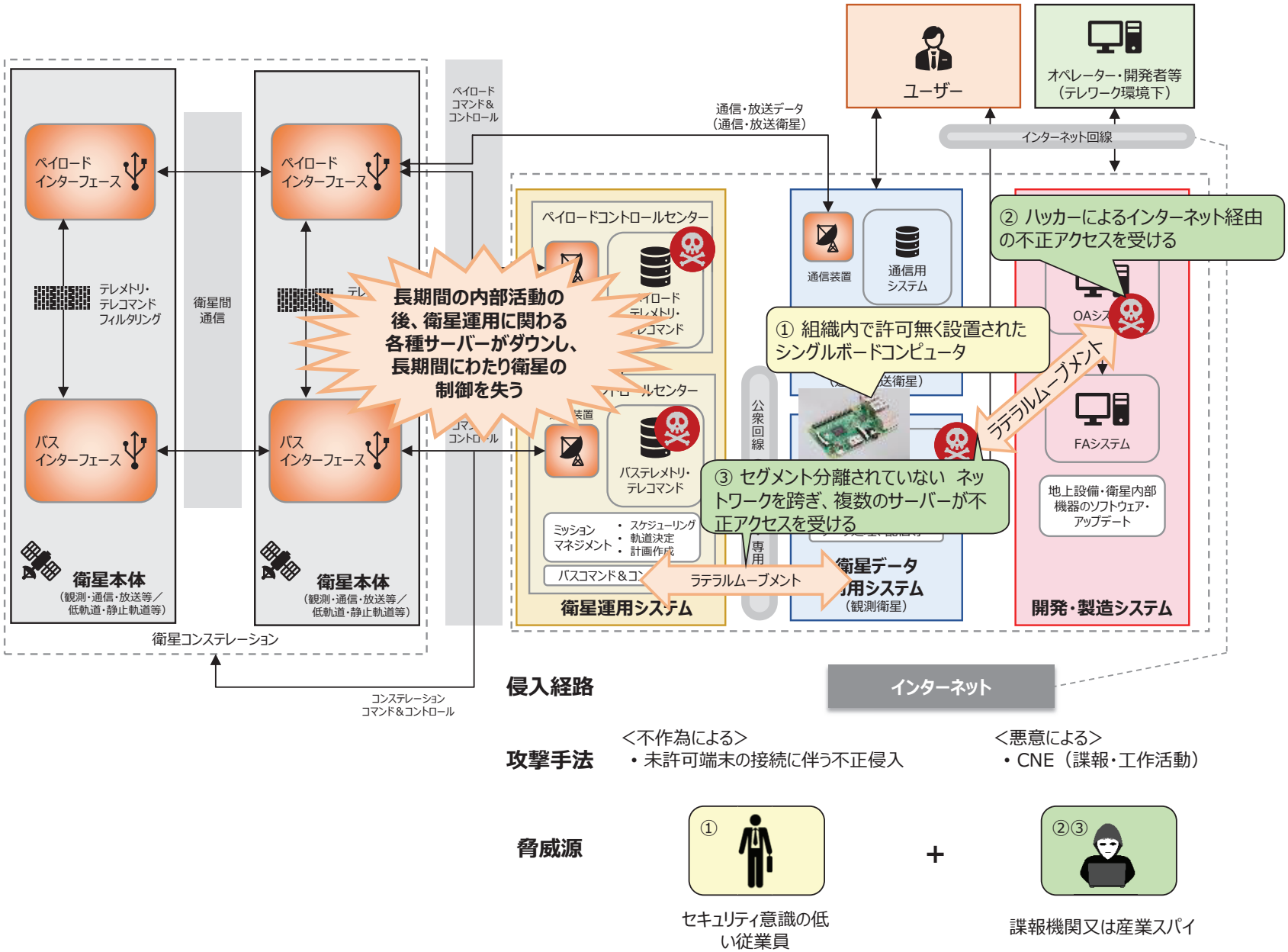

図　2－9　リスクシナリオ例３：衛星データ利用システムへのサイバー攻撃による衛星制御の喪失

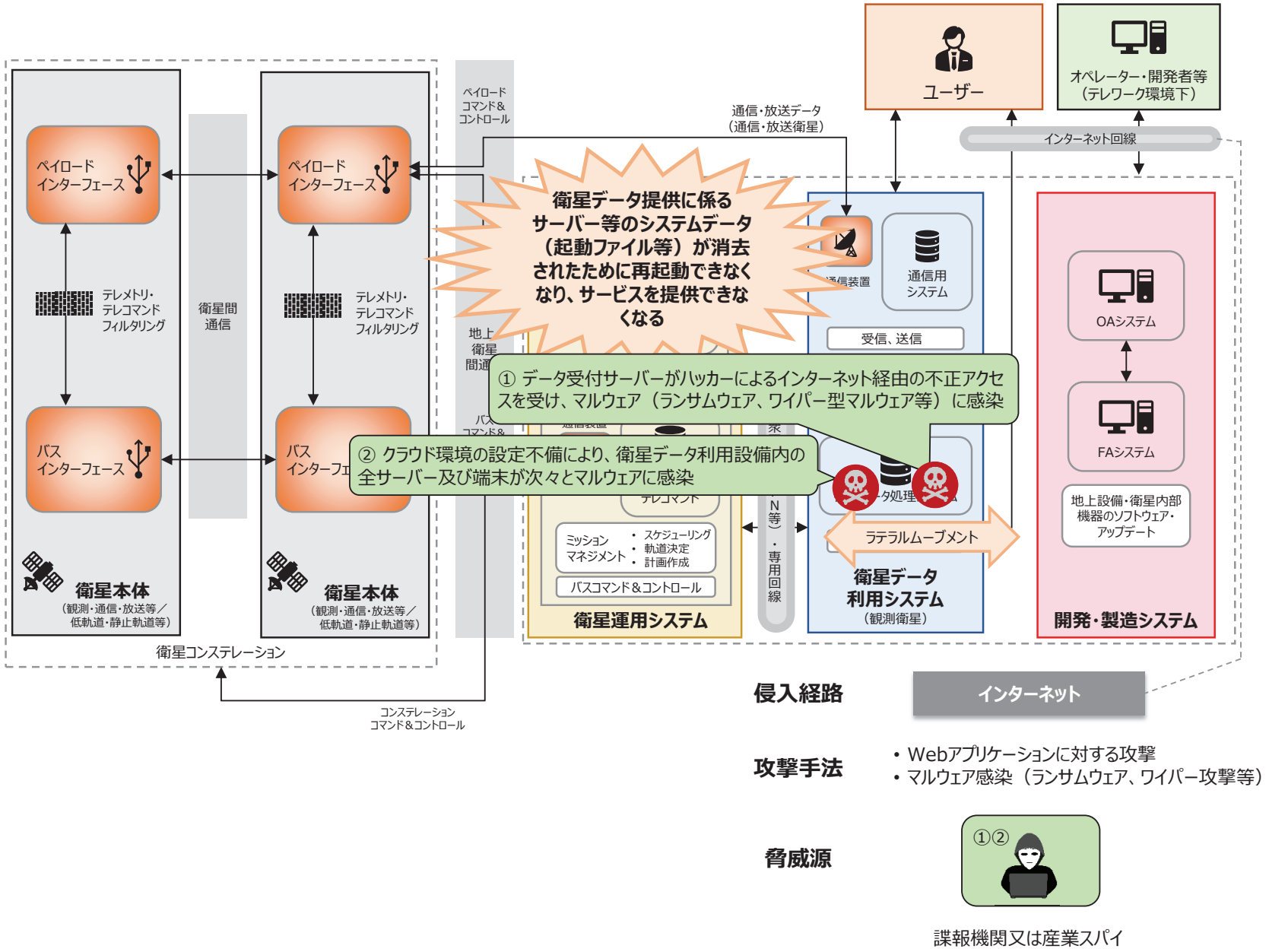

図　2－１０　リスクシナリオ例４：データ受付サーバーへの不正アクセスによるサービス提供不能

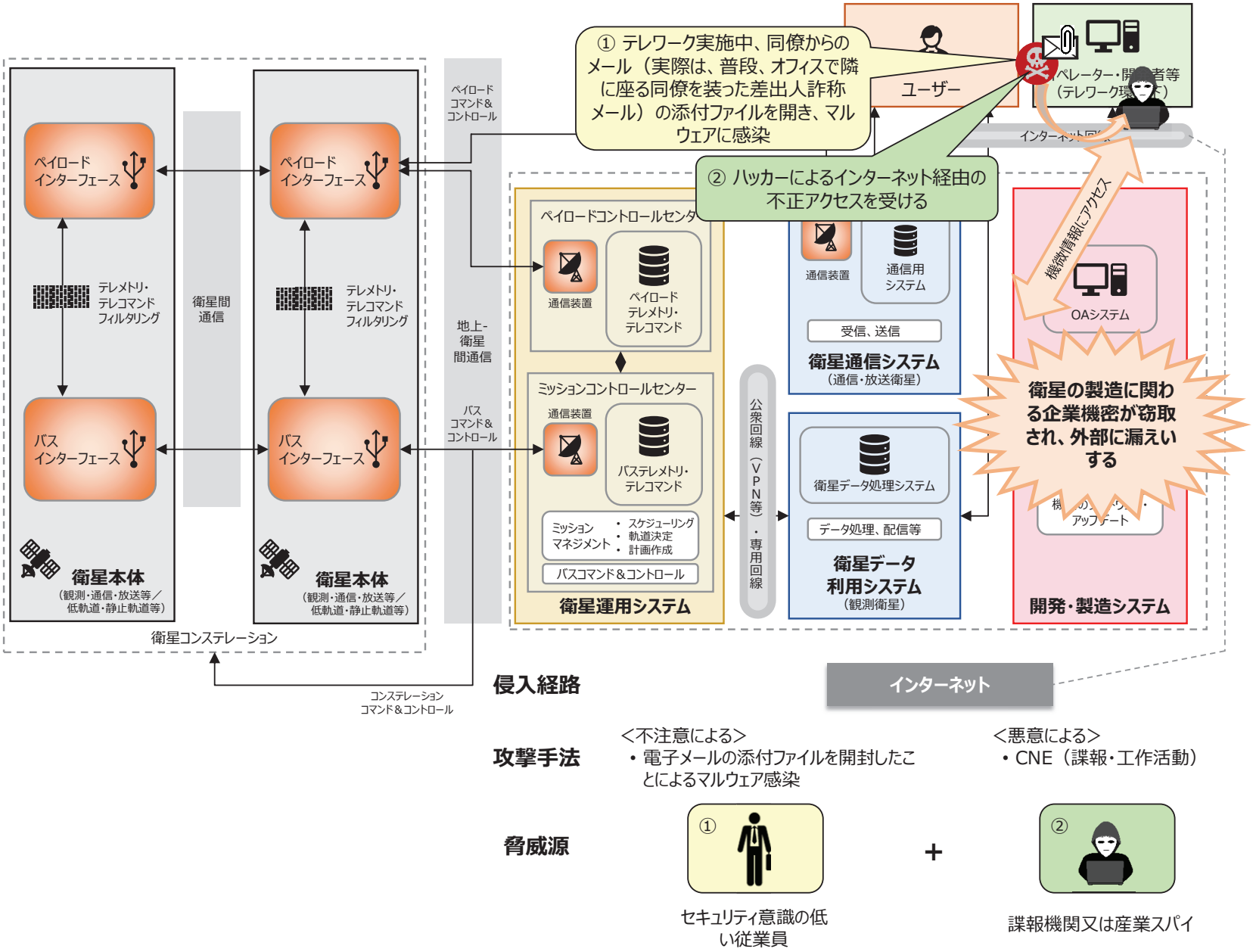

図　2－１１　リスクシナリオ例５：テレワーク環境下でのメール攻撃による企業機密の漏えい

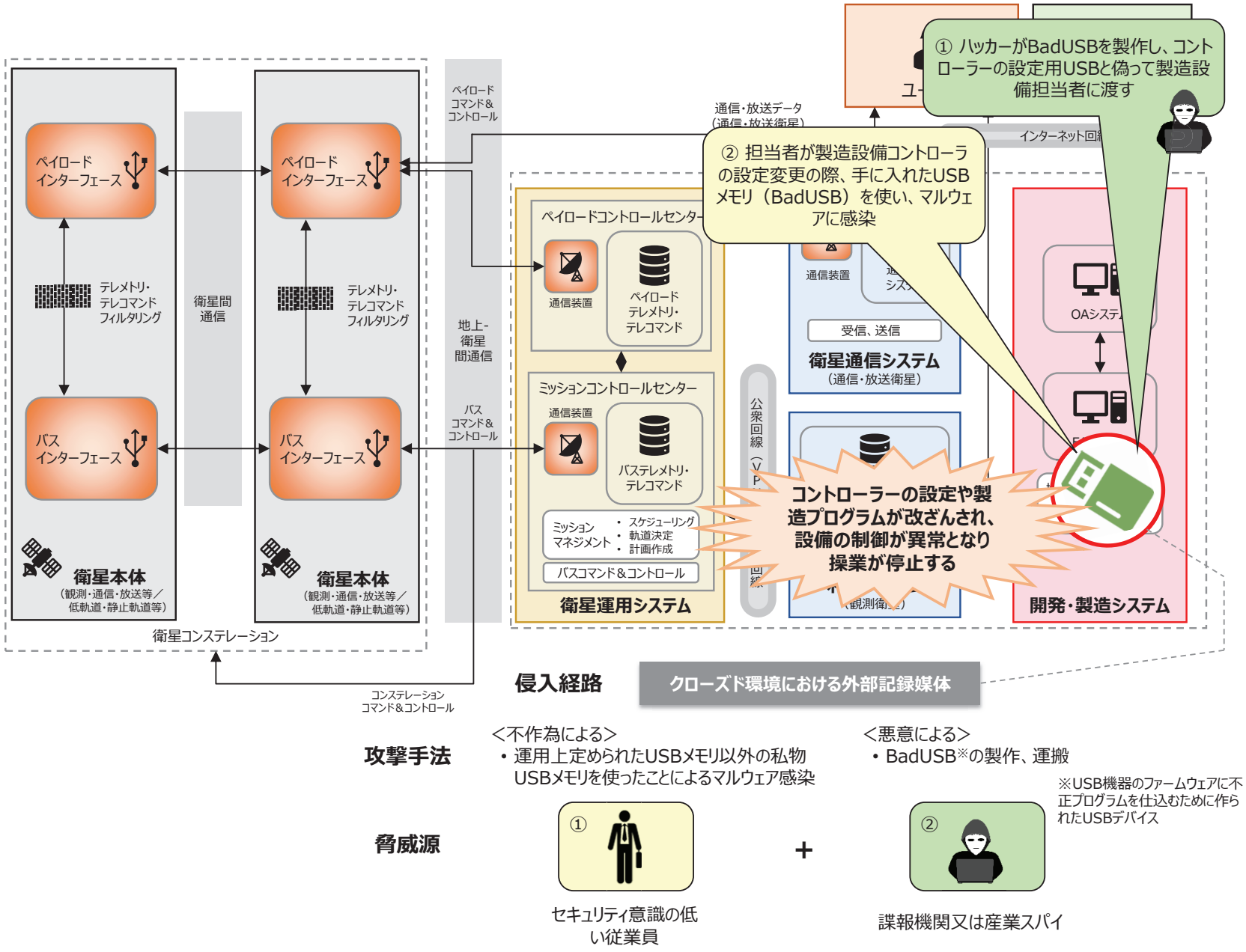

図　2－１２　リスクシナリオ例６：無許可 USB メモリの利用による操業停止

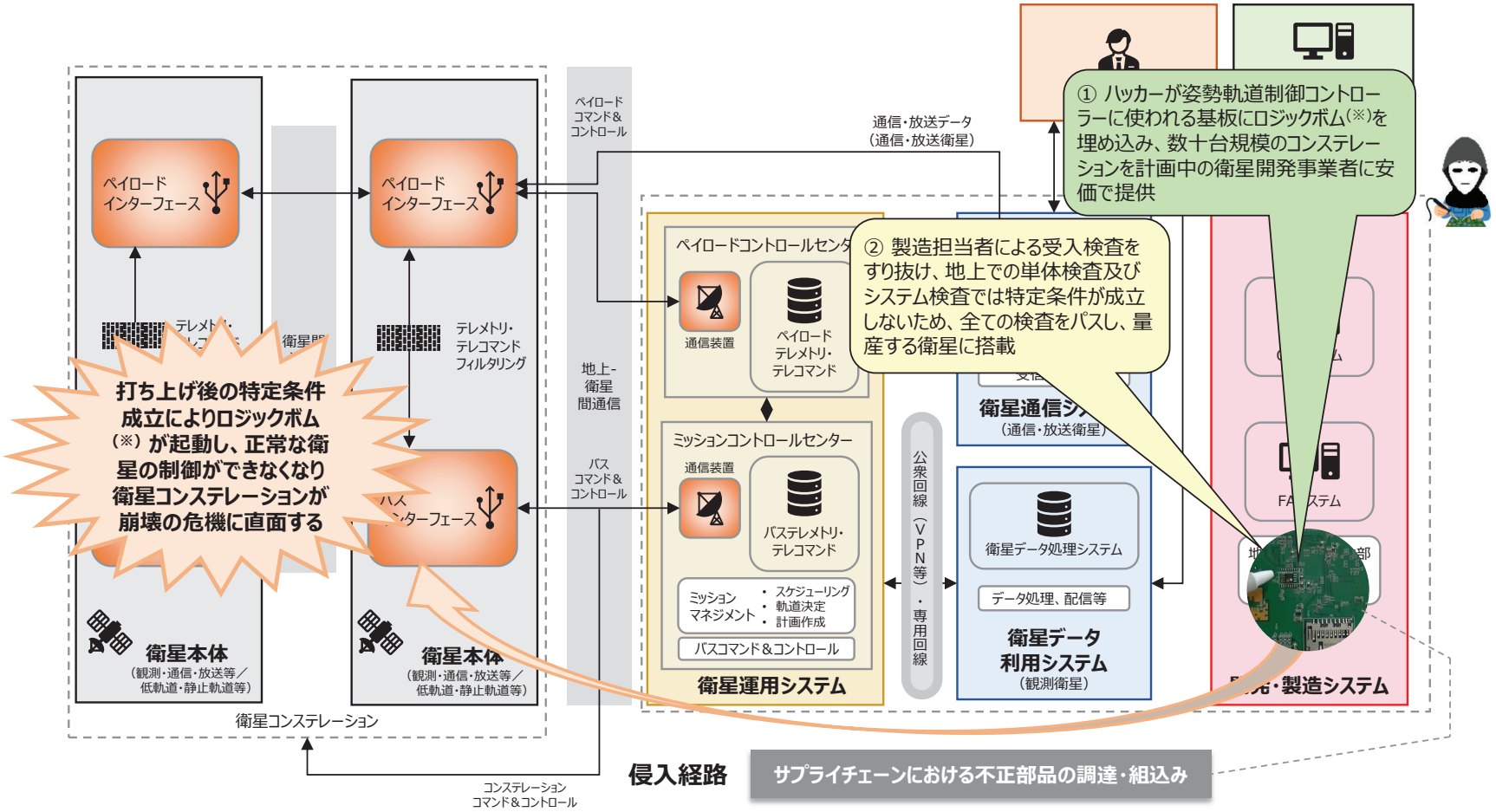

図　2－１３　リスクシナリオ例７：不正な衛星搭載機器の受入による衛星コンステレーション崩壊の危機

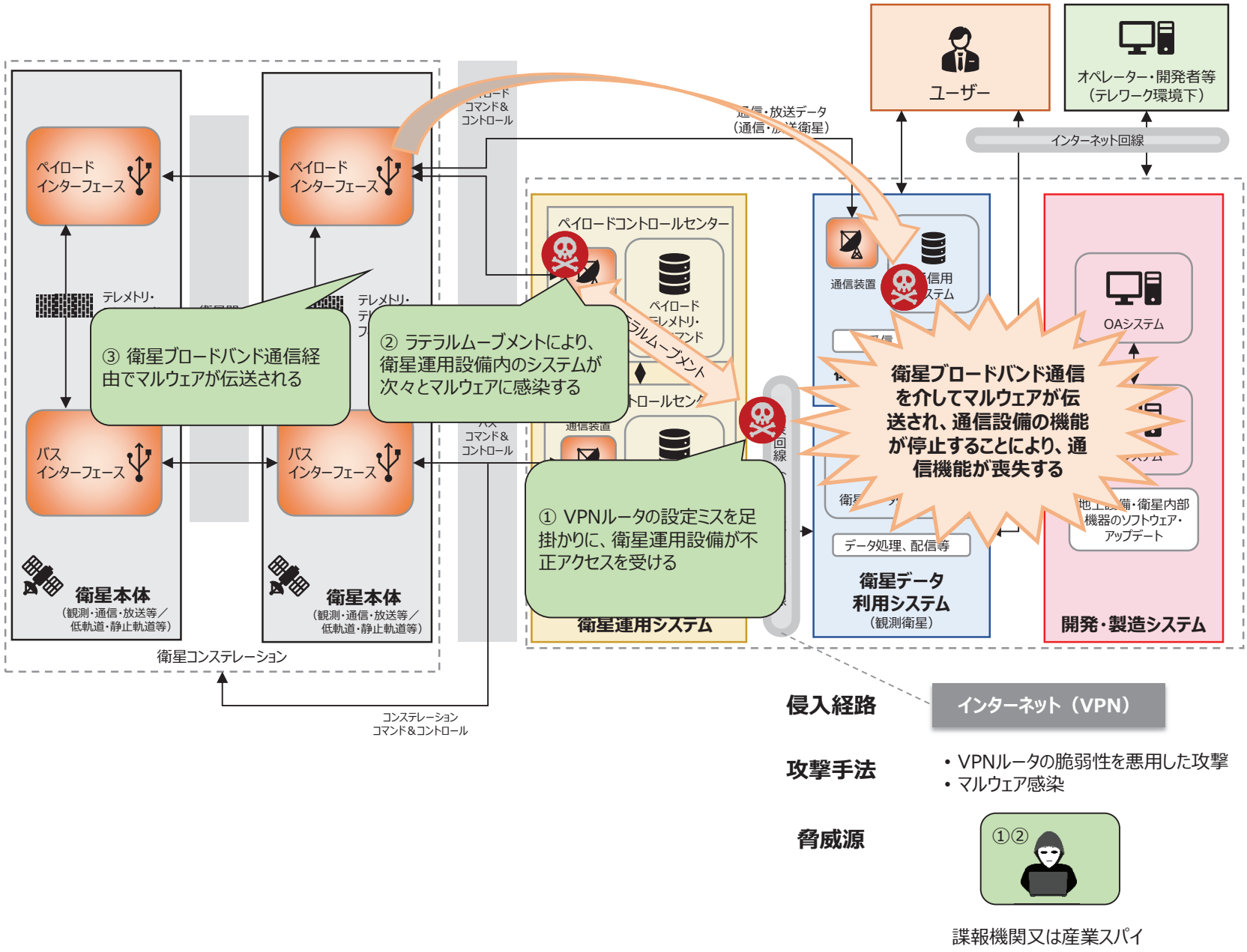

図　2－１４　リスクシナリオ例８：VPN の設定不備を悪用したユーザーの衛星機能の喪失

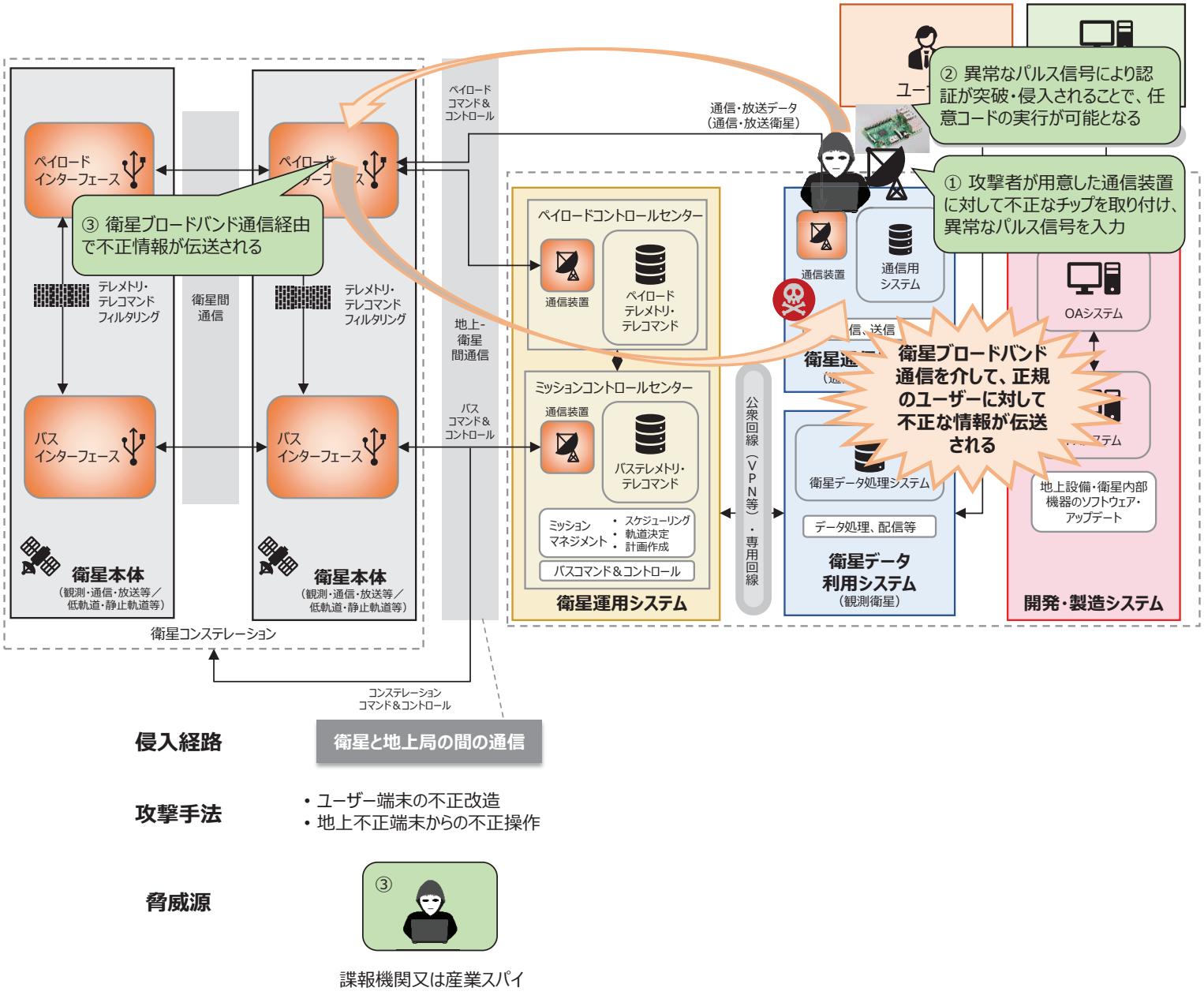

図　2－１５　リスクシナリオ例９：ユーザー端末の不正改造による情報の不正送信

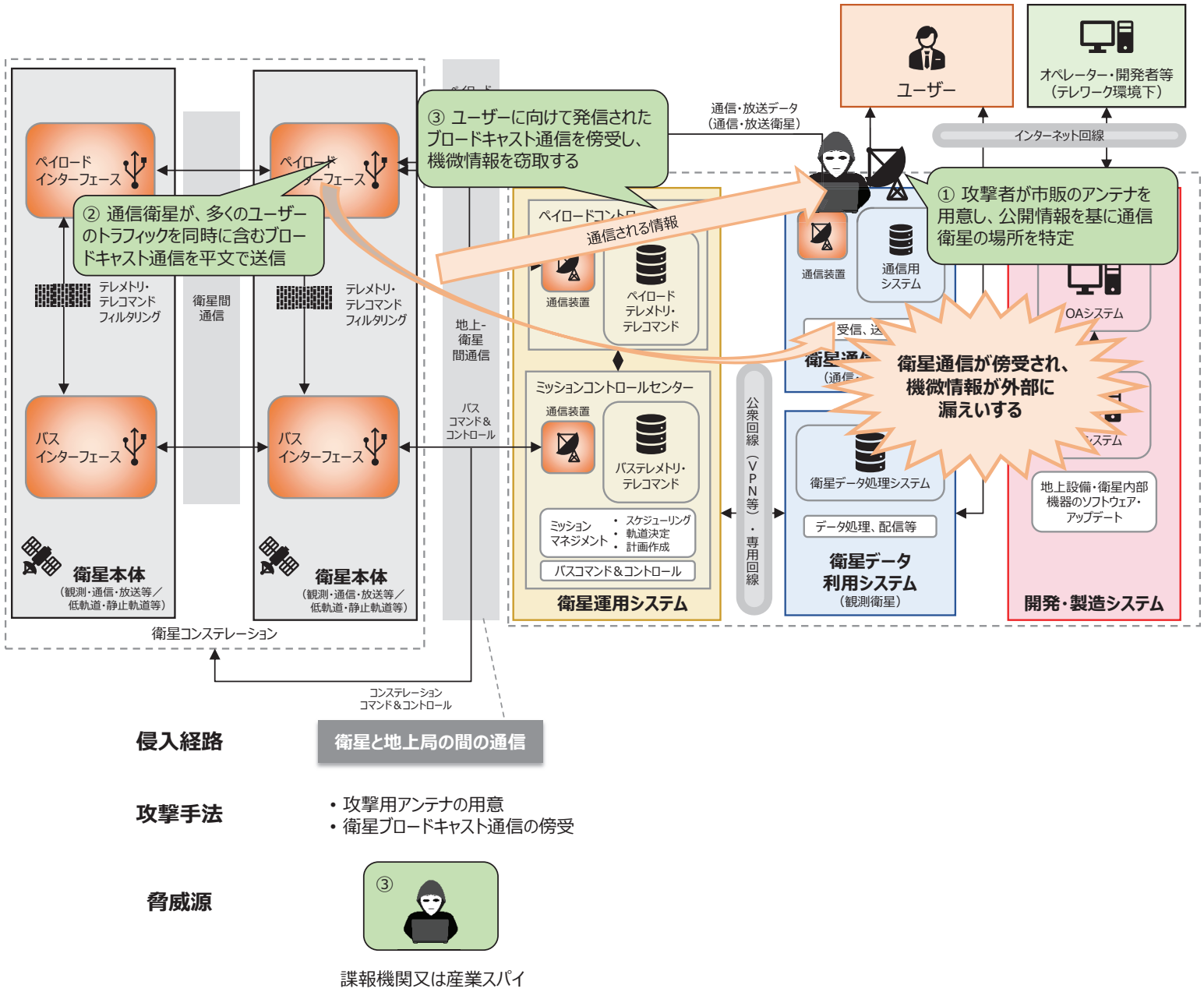

図　2－１６　リスクシナリオ例 10：衛星通信の傍受による機密情報の漏えい

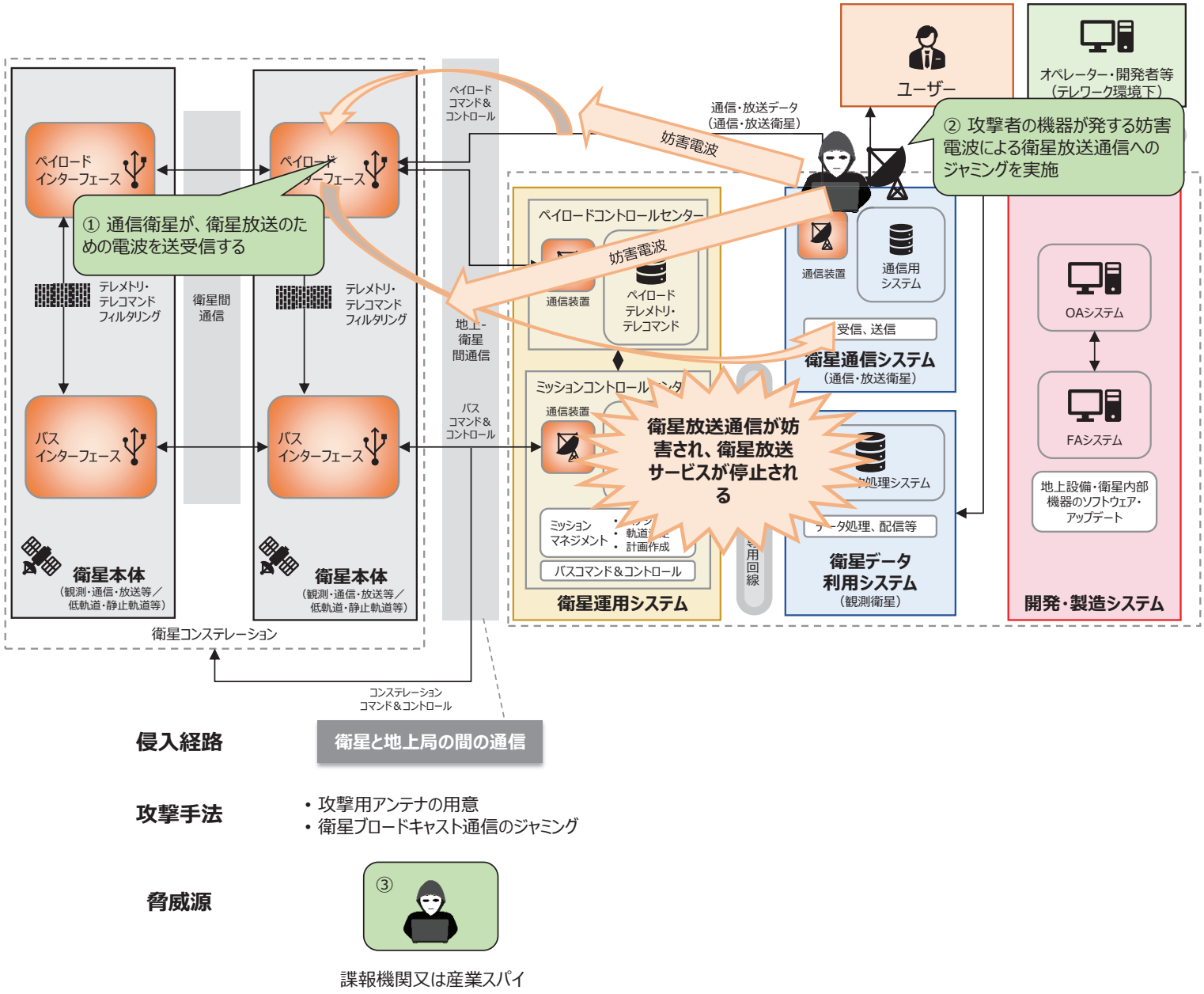

図　2－１７　リスクシナリオ例 11：衛星放送に対するジャミングによるサービスの停止

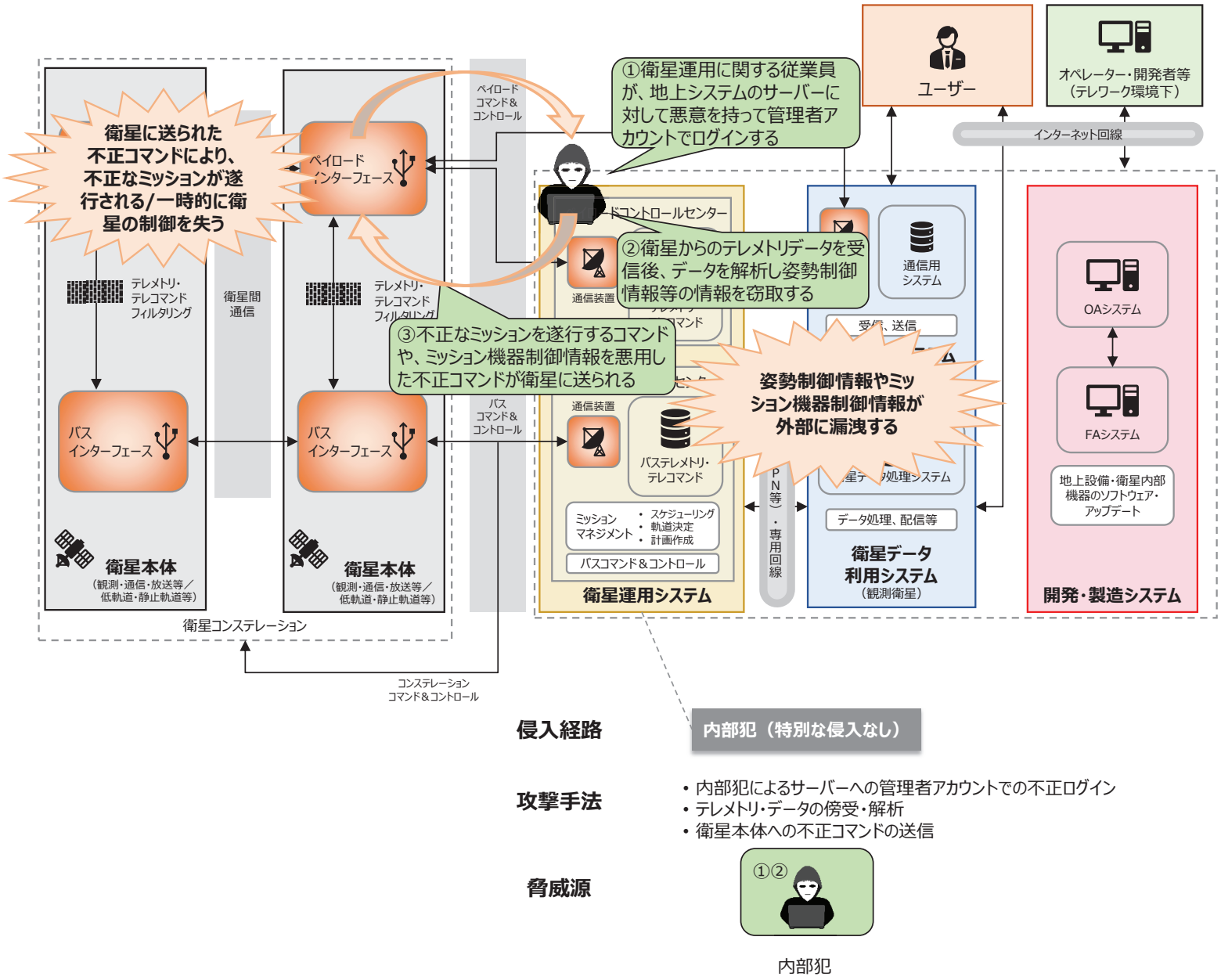

図　2－１８　リスクシナリオ例 12：内部犯による衛星制御のハッキング

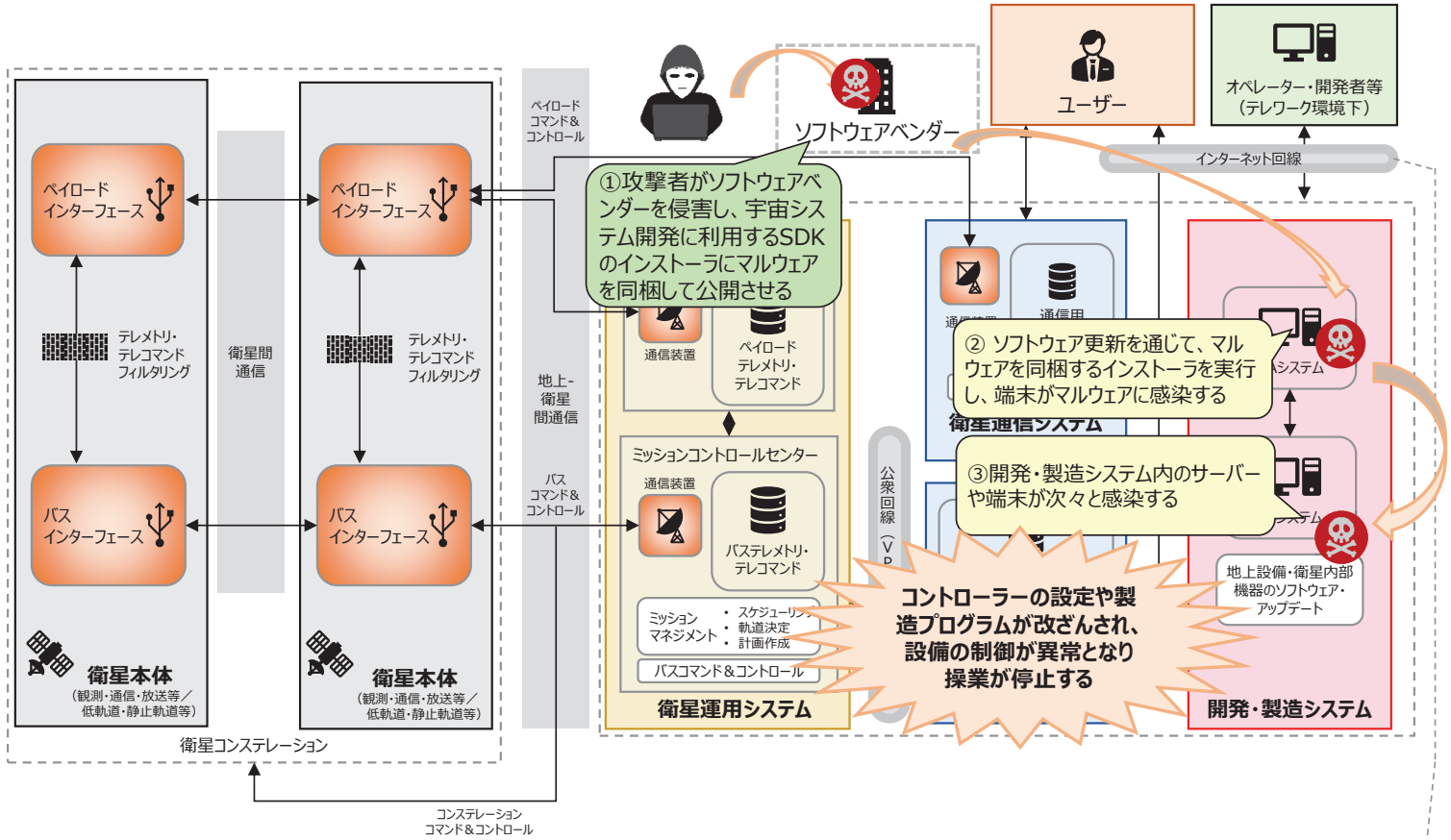

図　2－１９　リスクシナリオ例 13：ソフトウェアサプライチェーン攻撃による操業停止

ここまで述べた 13 のリスクシナリオの例を標準モデル上に整理すると以下のとおりとなる。

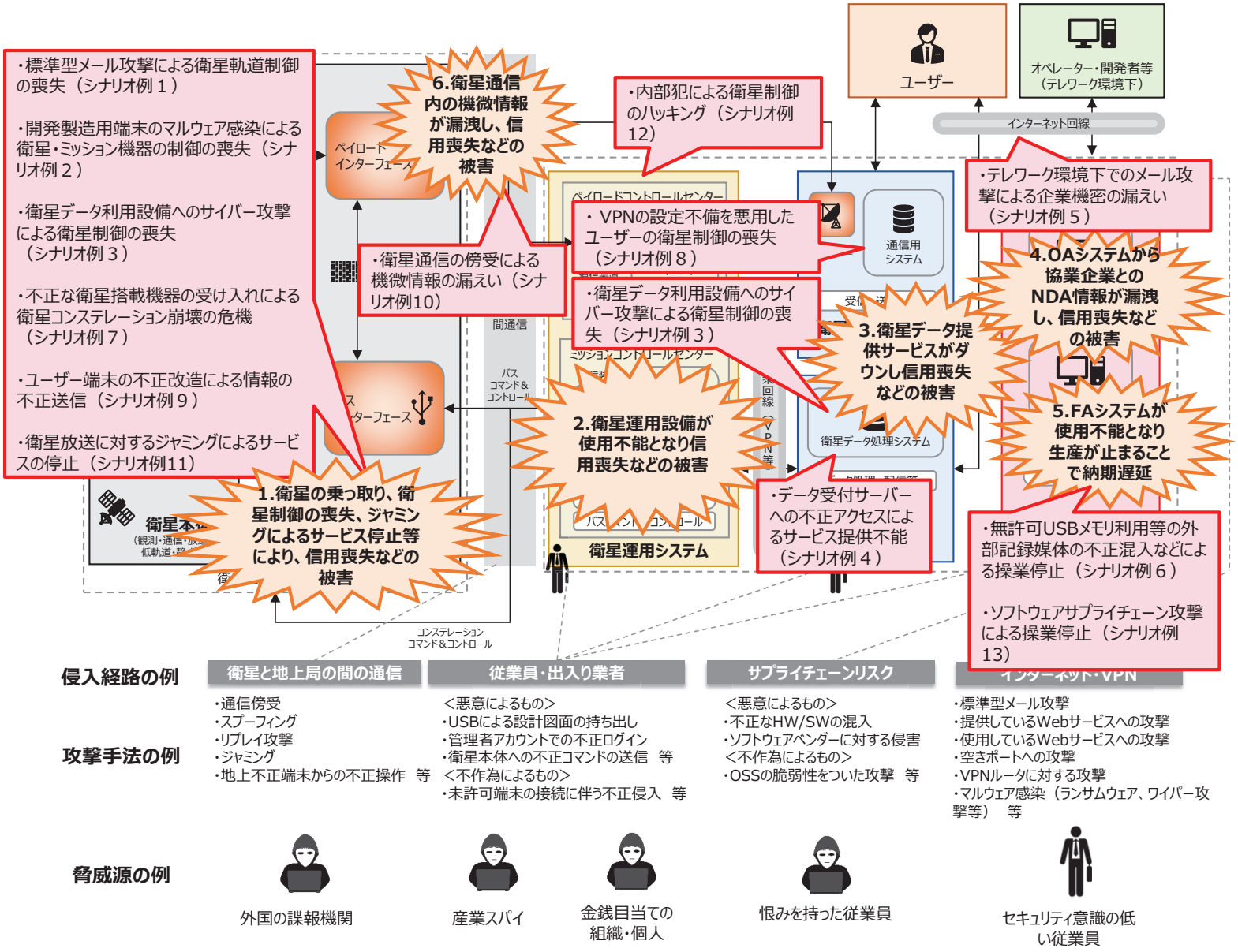

図　2-２０　各ステークホルダーにおける重大な事業被害・攻撃手法等の例

（6）サブシステムごとの主な対策

前述の 13 のリスクシナリオ例について、発生可能性が低いシナリオも存在するものの、仮に発生した場合に大きな事業被害をもたらす可能性があるため、適切な対策を講じる必要がある。それぞれのリスクシナリオ例について、サブシステムごとに求められる主な対策の整理結果を下表に示す。なお、CPSF の第１層に対応する組織マネジメント等に関する対策は３．１節、CPSF の第２層・第３層に対応するサブシステムごとの技術的対策を３．２節に記載している。

表 2-6　想定されるリスクシナリオを踏まえて求められるサブシステムごとの主な対策

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	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。	・ 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	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、システム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	・ 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、サーバー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	－

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付かずに受入れて衛星群に搭載。打上げ後の特定条件成立によりロジックボムが起動し、衛星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
例8	VPN ルータの設定ミスを足掛かりに、衛星運用システムが不正アクセスを受ける。衛星運用システム内のシステムがマルウェアに感染した後、衛星ブロードバンド通信経由でマルウェアが衛星ユーザーに伝送され、通信衛星のサービスが利用できなくなる。	－	・ 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	攻撃者が用意した通信装置に対して、攻撃者が用意した通信装置に対して不正なチップを取り付けることで、任意コードの実行が可能な状態にする。地上システムから衛星ブロードバンド通信経由で不正情報を伝送する。	・ 複数の通信経路等確保 ・ 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	ユーザーに向けて平文で送信されている衛星のブロードキャスト通信に対して、公開情報を基に通信衛星の場所を特定し、攻撃者が用意したアンテナを用いて通信傍受する。傍受された機密情報が外部に漏えいする。	・ 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	通信衛星が衛星放送のために送受信している電波に対して、攻撃者の用意した機器が発する妨害電波によるジャミングが行われる。衛星放送通信が妨害され、衛星放送が停止される。	・ ジャミング対策	・ ジャミング対策	－	－	－

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12	衛星運用に関する従業員が、悪意を持ってシステムに管理者アカウントでログインする。ログイン後、不正なミッションを遂行するコマンドや、ミッション機器制御情報を悪用した不正コマンドを衛星に送信する。	―	―	―	・ 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（内部犯行対策）	―
例13	ソフトウェアベンダーが侵害され、宇宙システム開発に利用する SDK のインストーラーにマルウェアが同梱され公開される。ソフトウェア更新を通じて、マルウェアを同梱するインストーラーを実行し、開発環境の端末やサーバーがマルウェアに感染する。	―	―	―	・ 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)

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

２章で分析を行った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、３章では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示す。宇宙システムに関係する全組織に関わる共通的対策は３．１節に記載し、各サブシステムで特に弱点となる部分の対策については３．２節に記載する。

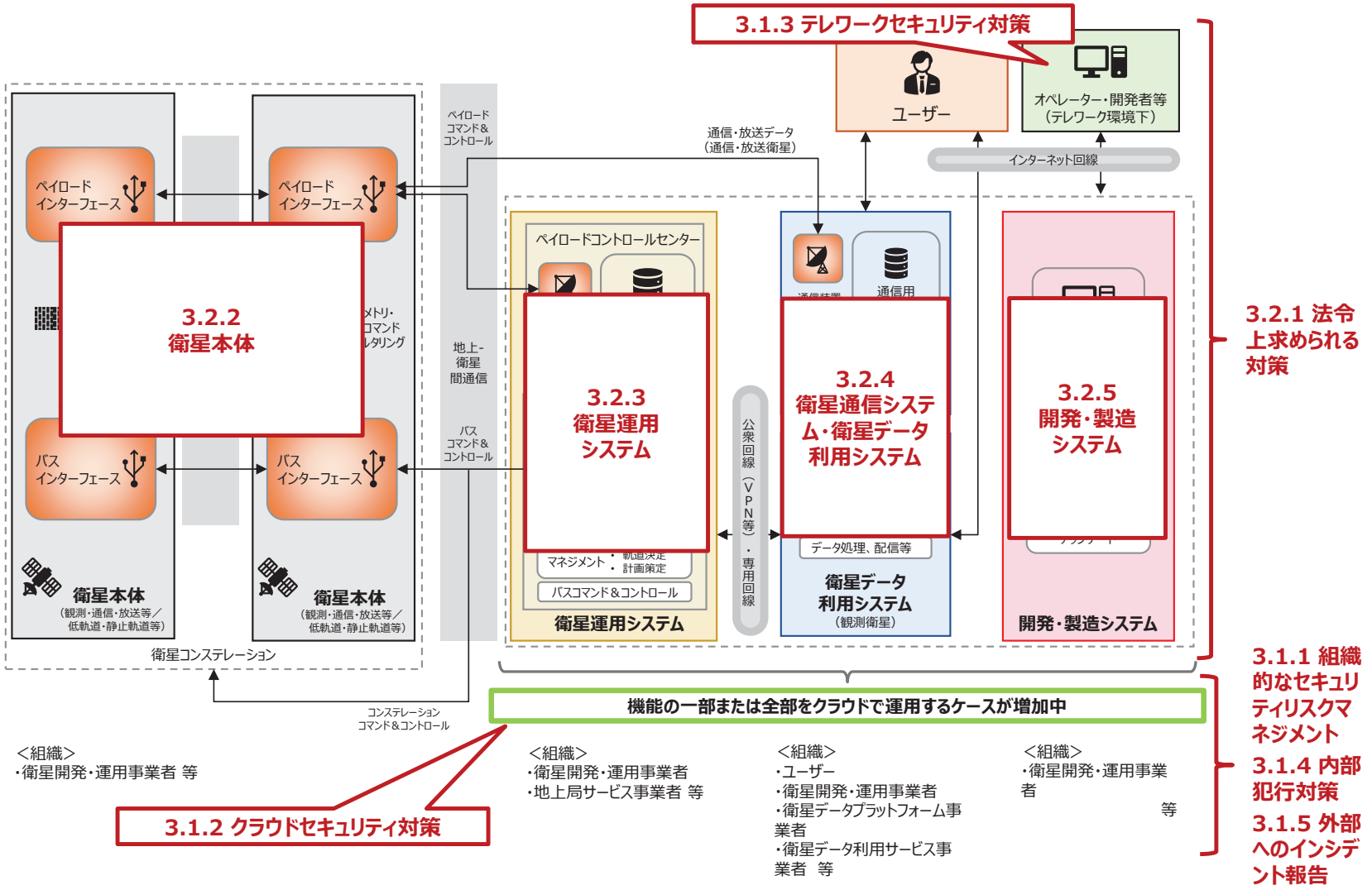

図　３－１　宇宙システムの概観と３章との対応

ここでは、民間宇宙システムに関わる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以下のように、「要求事項」、「基本対策事項」、「解説」の形に分けて整理して示す。

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。

なお、本ガイドラインは民間事業者における自主的な対策を促すことを目的としており、ここで示す「要求事項」は、各サブシステムに何らかの関わりを持つステークホルダーが、共通的に検討すべきサイバーセキュリティ対策の指針として位置付ける。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を踏まえつつ、必要な知識を備えたコンサルタント、システムインテグレータ、ベンダー等と相談することを勧める。サイバー攻撃は常に進化し、これに応じて新たな製品・サービスが出される「いたちごっこ」であることから、常にセキュリティの最前線の情報・知見を保有した組織・専門家に相談することが重要である。

表 3-1及び表 3-2では、ステークホルダーごとに必要とされる対策事項を整理している。また、対策要求事項を整理したチェックリストを添付資料1として掲載している。この対策要求事項チェックリストでは、サイバーセキュリティ一般に関する共通的対策と宇宙システム特有の対策をする上で必要な要求事項・具体的対策事項を示しているため、対策実施時の参考として参照されたい。

表 3-1　各ステークホルダーと3章のセキュリティ対策との対応　1/2

区分	章節	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	3.1.1	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3.1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（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）	●	●	●	●	●	●
	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。

表 3-2　各ステークホルダーと 3 章のセキュリティ対策との対応　2/2

区分	章節	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) 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	●	●	–	–	–	●
	3.2.3	衛星運用システム	【要求事項】 衛星運用システム（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) システムの保護　(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

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（NIST）
(e) SP 800-171（NIST）

（解説）

● 基本対策事項 (1)(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）」について

① 対象

大企業及び中小企業（小規模事業者を除く）

② 概要

サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「３原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめたもの。[5]

ガイドライン中で言及されている経営者が認識すべき３原則は以下のとおりである。

[5] 経済産業省 商務情報政策局 サイバーセキュリティ課：「サイバーセキュリティ経営ガイドライン Ver 3.0」（2023 年 3 月）https://www.meti.go.jp/policy/netsecurity/mng_guide.html

・　経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
・　サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
・　平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

図 3-2 は、経営者が CISO 等に指示すべき「重要 10 項目」の概要である。

サイバーセキュリティリスクの管理体制構築	**指示 1**　サイバーセキュリティリスクの認識、組織全体での対応方針の策定 **指示 2**　サイバーセキュリティリスク管理体制の構築 **指示 3**　サイバーセキュリティ対策のための資源（予算、人材等）確保
サイバーセキュリティリスクの特定と対策の実装	**指示 4**　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 **指示 5**　サイバーセキュリティリスクに効果的に対応する仕組みの構築 **指示 6**　PDCA サイクルによるサイバーセキュリティ対策の継続的改善
インシデント発生に備えた体制構築	**指示 7**　インシデント発生時の緊急対応体制の整備 **指示 8**　インシデントによる被害に備えた事業継続・復旧体制の整備
サプライチェーンセキュリティ対策の推進	**指示 9**　ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
ステークホルダーを含めた関係者とのコミュニケーションの推進	**指示 10**　サイバーセキュリティに関する情報の収集、共有及び開示の促進

図 3-2　経営者が CISO 等に指示すべき「重要 10 項目」の概要

CISO 等は、経営者の指示に基づき、重要 10 項目の各解説ページの「対策例」も参考にしつつ、セキュリティ対策の取組を、セキュリティ担当者に対してより具体的に指示をし、推進することが求められる。組織全体での対応方針の策定に当たっては、企業の経営方針と整合を取ったセキュリティポリシーを策定することが必要であるほか、その策定においては、製造、販売、サービス等、事業が立脚している全ての基盤（設備、システム、情報等の資産、流通プロセス等）に影響を及ぼすと考えられるサイバーセキュリティリスクに応じた対応方針を検討することが重要である。また、デジタル化の進展に伴い、様々な役割においてセキュリティ対策の取組が求められるところ、各役割において適切な取組を講じることができるよう、実効性のある継続的な教育・演習等を各役割に求めていくことが重要となる。さらに、経営者に対して適宜状況報告を行うことを通じて、経営者が適切な判断を行うために必要な情報を提供しなければならない。

「重要 10 項目」については、「サイバーセキュリティ経営ガイドライン実施状況の可視化ツール」（従業員 300 名以上の企業・組織を対象）を用いることで、自社

の取組状況を可視化することが可能である。[6]

可視化ツールを用いて実務者が自社の対策状況を評価するとともに、その回答結果を経営層に報告することで、自社内の対策状況を可視化するほか、取引先等のステークホルダーに対して対策状況を開示することにも活用できる。具体的な質問項目は表 3-3に示す 40 項目であり、各項目について、5 段階で対策状況を選択する。

表 3-3 「サイバーセキュリティ経営ガイドライン実施状況の可視化ツール」の項目

指示	#		項目
指示 1：サイバーセキュリティリスクの認識、組織全体での対応方針の策定	1	1-1	経営者がサイバーセキュリティリスクを経営リスクの 1 つとして認識している
	2	1-2	経営者が、組織全体としてのサイバーセキュリティリスクを考慮した基本方針を策定し、宣言している
	3	1-3	法令・契約やガイドライン等の要求事項を把握し、基本方針等に反映している
指示 2：サイバーセキュリティリスク管理体制の構築	4	2-1	組織の基本方針に基づき、CISO 等からなるサイバーセキュリティリスク管理体制を構築している
	5	2-2	サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にしている
	6	2-3	組織内のガバナンスや内部統制、事業継続に関するリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確にしている
指示 3：サイバーセキュリティ対策のための資源（予算、人材等）確保	7	3-1	経営会議等の議論により、サイバーセキュリティ対策とそれを実施できる資源（予算、人材等）を明確にしている
	8	3-2	サイバーセキュリティ対策に関して、自組織で対応する部分と外部に委託する部分を適切に切り分けている
	9	3-3	自組織に求められるセキュリティ人材の要件を明らかにし、計画的にサイバーセキュリティ人材を確保、育成するとともに、適正な処遇を与えている
	10	3-4	プラス・セキュリティを担う人材を対象に、サイバーセキュリティの知識・スキルの習得を実施している
	11	3-5	外部に委託する部分について、自社の課題、予算、場所等を考慮して適切な外部リソースを選定し、活用している
指示 4：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	12	4-1	守るべきデジタル環境、サービス及び情報を特定し、当該資産の場所やビジネス上の価値等に基づいて対策の優先順位付けを行っている
	13	4-2	守るべきデジタル環境、サービス及び情報に対するサイバー攻撃の脅威、脆弱性を特定し、これらによるサイバーセキュリティリスクが自社の事業にいかなる影響があるかを把握している
	14	4-3	リスクアセスメント結果に基づいてリスク対応計画を策定している
指示 5：サイバーセキュリティリスクに対応する仕組みの構築	15	5-1	重要なシステムの資産管理・構成管理・パッチ管理を行っている
	16	5-2	組織内でシャドーIT を利用させない対策を行っている
	17	5-3	システム設計時にリスクアセスメントを行い、必要なセキュリティ機能を具体化し、開発時に実装している
	18	5-4	重要業務を行う端末・サーバ等には複数の技術的対策を実施している
	19	5-5	重要業務を行うネットワークには複数の技術的対策を実施している

[6] 独立行政法人情報処理推進機構 セキュリティセンター：「サイバーセキュリティ経営可視化ツール」（2023 年 3 月）https://www.ipa.go.jp/security/economics/checktool/index.html

指示	#		項目
	20	5-6	システム等に対する定期的な脆弱性診断や、継続的なパッチ適用、その他の緩和策等の脆弱性対策の計画を立て、実行している
	21	5-7	端末やネットワークからのログを収集・分析している
	22	5-8	サイバー攻撃を検知した際に通信を遮断する等のインシデント対応の仕組みを導入している
	23	5-9	インシデント管理の仕組みを導入している
	24	5-10	従業員に対して、サイバーセキュリティの教育・演習を実施している
指示 6：PDCA サイクルによるサイバーセキュリティ対策の継続的改善	25	6-1	サイバーセキュリティ運用管理に関する KPI を定めている
	26	6-2	経営者が定期的に、サイバーセキュリティ対策実施状況に関する報告を受け、議論・対策指示している
	27	6-3	サイバーセキュリティに関する監査を実施し、その結果を踏まえ、サイバーセキュリティ対策を適時見直している
	28	6-4	サイバーセキュリティリスクへの対策状況についてステークホルダーとコミュニケーションしている
指示 7：インシデント発生時の緊急対応体制の整備	29	7-1	サプライチェーン全体を考慮したインシデント対応計画を策定している
	30	7-2	インシデントに対応可能な専門チーム（CSIRT 等）を設置している
	31	7-3	組織外に共有・報告・公表すべき内容やタイミングを定めている
	32	7-4	インシデント発生時の緊急対応の演習を定期的に行っている
	33	7-5	インシデント発生時のログ分析・調査を速やかに行い、影響範囲を特定できるよう実施計画を策定している
指示 8：インシデントによる被害に備えた事業継続・復旧体制の整備	34	8-1	被害が発生した際の、サプライチェーン全体を考慮した業務の復旧計画を策定している
	35	8-2	定期的に復旧対応演習を行っている
指示 9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策	36	9-1	グループ企業との取引や連携におけるサイバーセキュリティリスクへの対策状況を把握している
	37	9-2	委託先等の取引先との契約で合意したサイバーセキュリティリスクに関する役割と責任範囲に基づいて、適切な方策が講じられていることを確認している
	38	9-3	自社事業に影響を及ぼすサプライチェーン全体にわたって、サイバーセキュリティリスクが許容可能なレベルを超えていないことを確認している
指示 10：サイバーセキュリティに関する情報の収集、共有及び開示の促進	39	10-1	関係団体が提供する注意喚起情報の入手や、業界のセキュリティコミュニティ等への参加を通して情報共有を行い、自社の対策に活かしている
	40	10-2	マルウェア感染、不正アクセス等のインシデントがあった際に、関係団体やコミュニティへの共有・報告や、適切な公表等の情報提供を実施している

なお、このほか、サイバーセキュリティ経営ガイドラインには、以下の付録が用意されている。[7]

- 付録 A サイバーセキュリティ経営チェックシート

[7]経済産業省 商務情報政策局 サイバーセキュリティ課：「サイバーセキュリティ経営ガイドライン Ver 3.0」（2023 年 3 月）https://www.meti.go.jp/policy/netsecurity/mng_guide.html

・　付録 B サイバーセキュリティ対策に関する参考情報
・　付録 C サイバーセキュリティインシデントに備えるための参考情報
・　付録 D 関連する規格・フレームワーク等との関係
・　付録 E 用語の定義
・　付録 F サイバーセキュリティ体制構築・人材確保の手引き 第 2.0 版

● 基本対策事項(1)(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）」について

① 対象

中小企業及び小規模事業者（法人、個人事業主、各種団体も含む）

② 概要

2019 年 3 月に第 3 版が公表されて以降、新型コロナウイルス感染防止策によるテレワークの普及や、DX 推進の両輪としての情報セキュリティ対策といった社会動向が大幅に変化した。そのような情勢の変化を踏まえ、テレワークセキュリティ、セキュリティインシデント対応、サプライチェーンセキュリティに関する具体的な対応策を盛り込むため、第 3.1 版への改訂が実施された。情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめている。表 3-4 に示すとおり、本ガイドラインは経営者編と実践編から構成されている。[8]

表 3-4　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）の構成

構成		概要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明する。
	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明する。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明する。
	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプル。
	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある２５項目のチェックシート。
	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形。
	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプル。

[8] 独立行政法人情報処理推進機構 セキュリティセンター：「中小企業の情報セキュリティ対策ガイドライン」(2023 年 12 月)https://www.ipa.go.jp/security/keihatsu/sme/guideline/

構成		概要
	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引き。１５項目のチェックシートが付いている。
	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の検討を進められる。
	付録８　中小企業のためのセキュリティインシデント対応の手引き	情報漏えいやシステム停止などのインシデント対応のための手引き。

＜第１部　経営者編＞

サイバーセキュリティ経営ガイドラインと整合的な内容となっている。具体的には、表 3-5に示すとおり、経営者が認識すべき「３原則」と、経営者が実施を指示する必要がある「重要７項目の取組」が記載されている。

表 3-5　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）の３原則と重要７項目の取組

経営者が認識すべき「３原則」	実行すべき「重要７項目の取組」
情報セキュリティ対策は経営者のリーダーシップで進める。	情報セキュリティに関する組織全体の対応方針を定める。
	情報セキュリティ対策のための予算や人材などを確保する。
	必要と考えられる対策を検討させて実行を指示する。
	情報セキュリティ対策に関する適宜の見直しを指示する。
	緊急時の対応や復旧のための体制を整備する。
委託先の情報セキュリティ対策まで考慮する。	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする。
関係者とは常に情報セキュリティに関するコミュニケーションをとる。	情報セキュリティに関する最新動向を収集する。

＜第２部　実践編＞

企業のレベルに合わせて段階的にステップアップできるような構成で解説されている。

③ 活用に当たってのポイント

活用に当たっては、「情報セキュリティ自社診断」で満点を取ることが一つの目安となる。

付録の「情報セキュリティ関連規程」（表 3-6参照）を活用すれば、比較的容易に自社のセキュリティ関連規程を策定可能である。

表 3-6　付録 5 セキュリティ規程（サンプル）の構成

	名称	概要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定める。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定める。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定める。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定める。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定める。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定める。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定める。
8	システムの開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定める。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定める。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルを付属する。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定める。
11	テレワークにおける対策	テレワークを実施する際のルールを定める。

● 基本対策事項 (1)(c)「ISO/IEC 27001（情報セキュリティマネジメントシステム）」について

① 対象

適用範囲は組織単位、事業単位、物理単位等、自由に決定できる。

② 概要

ISO/IEC 27001（国内規格は JIS Q 27001）は、ISMS（Information Security Management System：情報セキュリティマネジメントシステム）の要求事項を定めた規格。組織が ISMS を確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されている。2022 年 10 月には改定版の ISO/IEC 27001:2022 が新たに発行され、主に附属書 A（管理目的及び管理策）が変更された。

ISO/IEC 27001 に基づいて適切に情報セキュリティマネジメントシステムが運用管理されているかを第三者である認証機関が審査・証明する「ISMS 認証」を取得するには、ISMS 認証機関に申請し、審査を受ける必要がある。認証を維持するためには、初回審査の後も年に 1 回以上の中間的な審査（サーベイランス審査）と、3 年ごとの全面的な審査（再認証審査）を受ける必要がある。[9]

[9] 一般社団法人情報セキュリティマネジメントシステム認定センター：「ISMS（情報セキュリティマネジメントシステム）とは」https://isms.jp/isms/index.html
一般社団法人情報セキュリティマネジメントシステム認定センター：「ISMS 認証機関一覧」（2021 年 7 月）https://isms.jp/lst/isr/

③ 活用に当たってのポイント

ISO/IEC 27001 の活用に当たっては、必ずしも認証を取る必要があるわけではないが、ISMS 認証は第三者による審査を経ていることから客観的な信頼の証となる。

● 基本対策事項 (1)(d)「Cybersecurity Framework（NIST)」について

① 対象

全産官学、組織規模等を問わずいかなる分野の組織でも利用可能。

② 概要

米国大統領令 13636「Improving Critical Infrastructure Cybersecurity」（重要インフラのサイバーセキュリティの改善」（2013 年 2 月）を受け、2014 年に Ver1.0 が開発され、2018 年に Ver1.1 に更新された[10]。2023 年 8 月には、改訂版である「Cybersecurity Framework 2.0」のドラフト版が公開され、2024 年 2 月にパブリックコメントを踏まえた正式版が公開された[11]。Cybersecurity Framework 2.0 では、重要インフラ事業者に限らず、規模・業種を限定せず、中小企業を含むあらゆる組織でも利用可能となるよう再設計された。

Cybersecurity Framework はフレームワークコア、フレームワークインプリメーションティア及びフレームワークプロファイルの 3 つの要素で構成されている。「フレームワークコア」とは、業種や重要インフラとは関係なく、共通となる具体的なサイバーセキュリティ対策を示したもので、6 つのコア機能と 22 のカテゴリーで構成される。Cybersecurity Framework 2.0 では、従来の「識別（Identify)」、「防御（Protect)」、「検知（Detect)」、「対応（Respond)」及び「復旧（Recover)」という 5 つのコア機能に加え、5 つの機能を実装するための基本的なセキュリティ機能として「Govern（ガバナンス)」が追加される。「Govern（ガバナンス)」の追加に伴い、カテゴリーも見直されており、サプライチェーンリスクセキュリティに焦点を当てたセキュリティ管理策について、加筆された。「フレームワークインプリメーションティア」とは、組織のサイバーセキュリティ対策がどの段階にあるのかを評価する基準を示す段階であり、4 段階のティアが設定されている。そして、「フレームワークプロファイル」とは、組織のサイバーセキュリティ対策の「現状（As-Is)」と「あるべき姿（To-Be)」を記述したものである。

③ 活用に当たってのポイント

商用衛星運用のためのセキュリティ入門書である NISTIR 8270「Introduction to Cybersecurity for Commercial Satellite Operations」では、低軌道小型衛星プラットフォームへの Cybersecurity Framework の実践例が示されている。（表 3 - 7 参照）[12]

---

[10]NIST :「Framework for Improving Critical Infrastructure Cybersecurity Version 1.1」（2018 年 4 月　独立行政法人情報処理推進機構訳）https://www.ipa.go.jp/files/000071204.pdf
[11] NIST :「Cybersecurity Framework（CSF）2.0」https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html
[12]NIST :「Introduction to Cybersecurity for Commercial Satellite Operations」（2023 年 7 月）https://csrc.nist.gov/pubs/ir/8270/final

表 3-7　低軌道小型衛星プラットフォームへの Cybersecurity Framework の実践例

NIST CSF 実践のための 7 ステップ	ケーススタディ（低軌道小型衛星プラットフォーム）
STEP 1：スコープ特定と優先順位づけ	衛星プラットフォームの運用部分のみを所有管理する企業を想定する。最終的に、作成される目標プロファイル（自社の衛星プラットフォームに対するサイバーセキュリティ要件）を利用し、宇宙分野以外でも使われている様々な製品やサービスを比較することになる。
STEP 2：方向づけ	潜在的脅威によるサイバーセキュリティイベントとビジネスへの影響をリスト化（原文 p12 表）する。
STEP 3：現状のプロファイルの作成	NIST CSF のサブカテゴリーを確認し、現在実践されているものを選択する。実践されているサブカテゴリーリスト（現状プロファイル）を作成する。
STEP 4：リスクの評価	DHS や DoD などの機関に相談、業界 ISAC への加入を行い、リスクに関する優先順位の高い情報を共有・受信する場を確保する。NIST SP 800-30 等を参考に、費用対効果の高い方法で対リスク体制確立の準備をする。
STEP 5：目標とするプロファイルの作成	求められる成果、必要とされるサブカテゴリー項目等からなる目標プロファイル（原文 p15 表 1）を作成する。
STEP 6：ギャップ分析の実施	現状プロファイルと目標プロファイル間のギャップを特定し、アクションプランを追加・更新する。
STEP 7：アクションプランの実施	セキュリティ部門責任者は、主要ステークホルダーにアクションプランを提示し承認を得る。幹部にビジネスケースとリソース要求を提示しアクションプランの承認を得る。アクションプランの実施を監視・検討するプロセスにより、アクションが衛星運用におけるリスクに十分に対応していること、現状・目標プロファイルが将来的に更新可能であること、外部サービスプロバイダーに対する監視を維持できることを確認する。

なお、本ガイドラインの添付資料２では、NIST CSF のサブカテゴリーと本ガイドラインにおける３．２．２～３．２．５の宇宙システム特有の対策との対応関係を整理している。対策実施時の参考として活用いただきたい。

● 基本対策事項 (1)(e)「SP 800-171 (NIST)」について

① 対象

米国国防総省（DoD）は、国防総省調達規則 DFARS（252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting）において、管理対象非機密情報（CUI）が含まれる契約には、NIST SP 800-171（Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations）相当のサイバーセキュリティの対応を要求している。また受託者は、下請業者の業務に必要な情報が CUI であるか否かを判断し、該当する場合には DFARS Clause 252.204-7012 に基づく保護を要求している。

② 概要

SP 800-171 は、以下の 14 個のファミリー（カテゴリー）と 110 項目から構成されている。

・　アクセス制御：システムへのアクセスができる人／機能を制限すること

- 意識向上と訓練：セキュリティポリシーを遵守すること
- 監査と責任追跡性：システムの監査を行うとともに責任の追及ができること
- 構成管理：システムを構成する機器に求められるセキュリティ構成設定を確立すること
- 識別と認証：システム利用者、デバイスを識別すること
- インシデント対応：インシデントの追跡、報告ができること
- 保守：組織のシステムのメンテナンスを行うこと
- 媒体保護：CUI をセキュアに格納するとともにアクセスできる者を制限すること
- 人的セキュリティ：システムへのアクセスを行う個人を審査すること
- 物理的保護：組織のシステム、装置等への物理的アクセスを制限すること
- リスクアセスメント：情報資産のリスクを適切に評価すること
- セキュリティアセスメント：セキュリティ管理策を定期的に評価すること
- システムと通信の保護：システムの鍵となる通信を監視し、制御し、保護すること
- システムと情報の完全性：タイムリーに情報及びシステムフローを識別すること

③ 活用に当たってのポイント

DoD との直接契約や、DoD 契約者との契約が発生する場合には、本規則の対象となることの考慮が必要である。

コラム：CMMC（Cybersecurity Maturity Model Certification）について

米国国防総省（DoD）取得・維持担当国防次官室（OUSD）は、中小企業を含む全サプライチェーンに一律に SP 800-171 を要求したことは遵守を非現実的にしていた等との認識のもと、５段階の成熟度モデルを用いた新たな認証制度フレームワークである CMMC を開発した。2020 年 1 月に Ver.1.0 を策定し、2021 年 11 月に Ver.2.0 が公開され、５段階から３段階の成熟度モデルへ修正された。2023 年 12 月に、DoD は CMMC に関する規則案を発表しパブリックコメントを募集した。

CMMC は、サプライチェーンの下請事業者へのフローダウンを考慮し、中小企業を含む各事業者がリスクに見合った各レベル（レベル 1～3）で情報を適切に保護できることについて、第三者評価認定機関（Certified Third-Party Assessment Organizations： C3PAO）から認証を受けられる仕組みになっている。レベル 1（Foundational、基礎）では連邦調達規則 48 CFR 52.204-21 に定められている 15 項目の連邦契約情報（FCI）の保護対策、レベル 2（Advanced、上級）では NIST SP 800-171 Rev.2 に相当する 110 項目の対策、レベル 3（Expert、エキスパート）は SP 800-172（標的型攻撃対策）から選択された 24 項目の対策が要件となっている。なお、CMMC レベル 2 の認証取得は、CMMC レベル 3 の前提条件となっている。

2023 年 12 月に発表された規則案では、請負事業者及び下請事業者に対して、4 ステップ（自己評価で CMMC レベル 1 を達成している請負事業者及び下請事業者、自己評価で CMMC レベル 2 を達成している請負事業者及び下請事業者、CMMC レベル 2 の認定評価を受けている請負事業者及び下請事業者、CMMC レベル 3 の認定評価を受けている請負事業者及び下請事業者）で CMMC の社会実装を図る旨示した。なお、CMMC に関する最新情報は DoD OUSD から提供される[13]。

[13] DoD Office of the Secretary ：「Cybersecurity Maturity Model Certification (CMMC) Program」（2023 年 12 月）
https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program

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

(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）

（解説）

● 基本対策事項 (1)(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」について

「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」における外部サービスに関連する箇所として、表 3-8に示すとおり、記録が保管される国又は地域の制限に留意する必要がある。対象の国又は地域については、国際情勢により変化するため、都度確認する必要がある。また、クラウドに関わらず要求されるセキュリティ要件については、後続の３.２.１法令上求められる対策を参考にすること。

表 3-8　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」の関連条文

第七条 ２　衛星リモートセンシング装置使用者及び衛星リモートセンシング記録保有者は、衛星リモートセンシング記録の取扱い業務の全部又は一部を電気通信回線を通じて外部に保存するサービスを利用して管理する場合は、当該サービスを提供する事業者（以下この項において「サービス事業者」という。）とのサービスの利用に係る契約において、次の各号に掲げる事項を明確に定めるものとする。 二　衛星リモートセンシング記録を次の国又は地域に所在する電子計算機に保存しないこと。 イ　輸出令別表第三の二又は別表第四に掲げる地域 ロ　国際連合の総会又は安全保障理事会の決議において国際社会の平和及び安全を脅かす事態の発生に責任を有するとされた国又は地域

表 3－9　輸出令別表第三の二に掲げる地域

アフガニスタン、中央アフリカ、コンゴ民主共和国、イラク、レバノン、リビア、北朝鮮、ソマリア、南スーダン、スーダン

※2024 年 3 月時点

表 3－10　輸出令別表第四に掲げる地域

イラン、イラク、北朝鮮

※2024 年 3 月時点

● 基本対策事項(2)(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）」について

① 対象

クラウドサービス

② 概要

ISMS クラウドセキュリティ認証は、JIS Q 27001（ISO/IEC 27001）に適合した ISMS（情報セキュリティマネジメントシステム）において、その適用範囲内に含まれるクラウドサービスの提供若しくは利用に関して、クラウドサービス向けの国際規格である ISO/IEC 27017:2015（JIS Q 27017：2016）に規定されるクラウドサービス固有の管理策が実施されていることを認証するものである。図 3-3 に示すとおり、ISMS クラウドセキュリティ認証を取得するためには、前提として ISO/IEC 27001 を取得したうえで、クラウドサービス固有の管理策として、ISO/IEC 27017:2015 が適切に実施されていることが必要となる[14]。

なお、3.1.1(c)ISO/IEC 27001（情報セキュリティマネジメントシステム）を合わせて参照されたい。

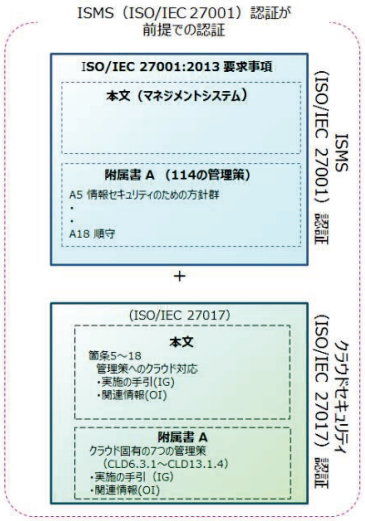

図 3－3　ISMS（ISO/IEC 27001）とクラウドセキュリティ認証（ISO/IEC 27017）の関係[15]

[14] 一般財団法人日本情報経済社会推進協会 情報マネジメントシステム認定センター：「ISMS 適合性評価制度（ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証について）」（2016 年 8 月）https://isms.jp/isms-cls/about-cls.pdf

[15] 図出典：一般財団法人日本情報経済社会推進協会 情報マネジメント推進センター：「ISMS 適合性評価制度 クラウドセキュリティ認証の方針」（2015 年 11 月）https://isms.jp/topics/ISO27017/iso27017_CLS_policy.pdf

● 基本対策事項⑵⑹「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）」について

① 対象

クラウドサービス

② 概要

政府情報システムにおけるクラウドサービスの活用を促進するための認証規格であり、ISO/IEC 27001（国内規格は JIS Q 27001）等をベースに政府機関等の情報セキュリティ対策のための統一基準及び NIST SP 800-53（Moderate）のセキュリティ要件が補足されている。2022 年には、政府情報システムにおけるクラウドサービスの中でもリスクの小さな業務・情報の処理に用いる SaaS を対象とした仕組みとして、ISMAP-LIU（ISMAP for Low-Impact Use）が仕組み化され、運用が始まっている。

● 基本対策事項⑵ ⑹「米国連邦リスク承認管理プログラム（FedRAMP）」について

① 対象

米国のクラウドサービス

② 概要

Federal Risk and Authorization Management Program（FedRAMP）は米国政府全体のプログラムであり、クラウドの製品やサービスに対するセキュリティ評価、認証、継続的監視に関する標準的なアプローチを提供している。NIST SP 800-53 のセキュリティ管理策を基にしており、Low、Moderate、High のベースラインがある。国家安全保障に係る場合は FedRAMP＋という、より厳格なプログラムとなる。

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）

（解説）

● 基本対策事項 (1)(a)「テレワークセキュリティガイドライン（第５版）（総務省）」について

① 対象

テレワークを実施又は検討している事業者（法人、個人事業主及び各種団体を含む）

② 概要

企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示している。表 3-１１にテレワークセキュリティガイドラインの構成を示す。[16]

表 3-１１　テレワークセキュリティガイドライン（第５版）（総務省）の構成

章	概要
第１章　はじめに	本ガイドラインの背景や目的、テレワークの形態、想定読者等を示す。
第２章　テレワークにおいて検討すべきこと	テレワークにおけるセキュリティ対策を進めるに当たり、「ルール」・「人」・「技術」のバランスのとれた対策を行う必要性や、「経営者」・「システムセキュリティ管理者」・「テレワーク勤務者」の適切な役割分担の重要性と、各立場の役割を具体的に示す。 また、近年のテレワークを取り巻く環境やセキュリティ動向の変化を踏まえ、クラウドサービスの活用やゼロトラストセキュリティに関する考え方も示す。

[16] 総務省 サイバーセキュリティ統括官室：「テレワークセキュリティガイドライン（第５版）」（2021 年５月）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

章	概要
第 3 章　テレワーク方式の解説	テレワーク方式を 7 種類に整理した上で、各方式について、基本的構成に加えて派生的な構成を示しているほか、各方式特有のセキュリティ上の留意点等について示す。(各方式共通のセキュリティ対策は第４章・第５章)。また、テレワークによって実現しようとする業務の内容やセキュリティ統制の容易性等を踏まえ、適した方式を選定する際の参考となるよう、フローチャートや、各方式の特性比較表を示す。
第 4 章　テレワークセキュリティ対策一覧	「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の立場ごとに、テレワークにおけるセキュリティ対策として一般的に普及しており、基本的に取り組むことが求められる「基本対策」と、一定の予算や組織体制が整備されていないと実施が困難なセキュリティ対策であるものの、実施により更なるセキュリティの向上が見込める「発展対策」をそれぞれ掲載している。また、各セキュリティ対策は、13 個の対策分類に分け整理している。
第 5 章　テレワークセキュリティ対策の解説	第４章に記載の各セキュリティ対策について、詳細解説を示す。
第 6 章　テレワークにおけるトラブル事例と対策	テレワークセキュリティに関するトラブル事例を具体的に紹介した上で、セキュリティ上の留意点や、本ガイドライン内のどのセキュリティ対策が有効であるかを示す。

③ 活用に当たってのポイント

本ガイドラインでは、セキュリティ対策は表 3-１２に示す 13 個の対策分類で整理されている。さらに、セキュリティ対策は、優先度（実施困難度）の参考として基本対策と発展対策に区分している。加えて、経営者、システム・セキュリティ管理者及びテレワーク勤務者が実施すべき対策を示し、各対策についても解説をしている。そのため、比較的容易に自社のテレワークセキュリティの関連規程を策定可能である。

表 3-１２　セキュリティ対策を整理するための対策分類

	対策分類	説明
A	ガバナンス・リスク管理	テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策。
B	資産・構成管理	テレワークで利用するハードウェアやソフトウェア等の資産の特定や、その管理に関する対策。
C	脆弱性管理	ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策。
D	特権管理	不正アクセス等に備えたシステム管理者権限の保護に関する対策。
E	データ保護	保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策。
F	マルウェア対策	マルウェアの感染防止や検出、エンドポイントセキュリティに関する対策。
G	通信の保護・暗号化	通信中におけるデータの機密性や可用性の確保に関する対策。
H	アカウント・認証管理	情報システムにアクセスするためのアカウント管理や認証手法に関する対策。
I	アクセス制御・認可	データやサービスへのアクセスを、必要最小限かつ正当な権限を有する者のみに制限することに関する対策。

	対策分類	説明
J	インシデント対応・ログ管理	セキュリティインシデントへの迅速な対応と、ログの取得や調査に関する対策。
K	物理的セキュリティ	物理的な手段による情報漏えい等からの保護に関する対策。
L	脅威インテリジェンス	脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策。
M	教育	テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策。

コラム：ゼロトラストセキュリティの考え方について

近年、サイバー攻撃の高度化等に伴い、新たなセキュリティに対する考え方として、「ゼロトラストセキュリティ」というものが注目されている。

テレワークセキュリティガイドライン（第５版）（総務省）では「ゼロトラストセキュリティ」について、以下のように説明されている：

ゼロトラストセキュリティとは、外部ネットワーク（インターネット）と、内部ネットワーク（LAN）との境界による防御（境界型セキュリティ）には限界があり、内部ネットワーク内にも脅威が存在しうるという考えのもと、データや機器等の単位でのセキュリティ強化をうたった考え方を指す。

従来の境界型セキュリティの前提が、「信ぜよ、されど確認せよ」であるとすると、それと対比して、ゼロトラストセキュリティは、「決して信頼せず、必ず確認せよ」であるといえる。

また、ゼロトラストセキュリティを実現するための要件については、参考文献[17]により諸説あるものの、いずれにおいても次のような考え方が特徴的である。

- ネットワークの内部と外部を区別せず、データや機器等の最小単位でセキュリティを考える
- 強固な利用者認証と厳密なアクセス管理を行う
- セキュリティ対策に関しては環境（場所・端末等）の制約を設けない

米国においても、サプライチェーン上の繋がりの深化によるサイバー攻撃の多角化を背景に、「ゼロトラストセキュリティ」は着目されている。米国国防総省（DoD）は、「ゼロトラスト戦略（Zero Trust Strategy）」及び「ゼロトラストケイパビリティ実行ロードマップ（Zero Trust Capability Execution Roadmap）」を発表し、2027 年度までに国防総省内の全ての情報システムについてターゲットレベルを達成するよう取組を進めるとしている[18]。

米国国防総省の取組は宇宙分野も例外ではなく、衛星システムや地上局システムを含むネットワーク全体及びそこに含まれるデータについて、ゼロトラストセキュリティの観点から保護することの必要性が示唆されている。国内の宇宙システムにおいても米国同様、従来の境界防御型アプローチを超える「ゼロトラストセキュリティ」の検討が望まれる。ただし、ネットワークの内部と外部を区別しないその特徴から、攻撃表面が増大化するおそれもあり、より段階的採用の検討が望まれる。

---

[17] ゼロトラストセキュリティの考え方について言及された文献等
1) NIST：「NIST Special Publication 800-27 Zero Trust Architecture」（2020 年 8 月）https://csrc.nist.gov/publications/detail/sp/800-207/final
2) Google：「BeyondCorp」
3) Forrester：「Zero Trust eXtended (ZTX) Ecosystem Providers」
4) 政府 CIO 補佐官等ディスカッションペーパー：「政府情報システムにおけるゼロトラスト適用に向けた考え方」（2020 年 6 月、掲載期間：2022 年 6 月）https://cio.go.jp/dp2020_03

[18] DoD：「Zero Trust Strategy」https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf （2022 年 11 月）、「Zero Trust Capability Execution Roadmap」https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilityExecutionRoadmap.pdf （2023 年 1 月）

● **基本対策事項 (1)(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)」について**

① 対象

予算やセキュリティ体制等が必ずしも十分ではない中小企業等の担当者

② 概要

「テレワークセキュリティガイドライン（第５版）（総務省)」を補うものとして、中小企業等においても実現が容易かつ優先的に実施すべきセキュリティ対策を具体的に示している。 本手引きの構成を表 3-１３に示す。また、テレワークの方式を８つの方式に整理し、対応する対策内容等を示している。[19]

表 3-１３　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）の構成

構成	概要
早引きインデックス	テレワークセキュリティに関する疑問に対する本書の対応ページを示している。
目次	本書の詳細目次を記載する。
はじめに	本書の目的や想定読者像を明らかにした上で、全体構成及び活用方法を説明する。
第１部	
１．テレワークの形態	業務を行う場所に応じた働き方の分類を示す。
２．あなたのテレワーク方式はどれ？	テレワークの利用シーンを想定し、導入（または予定）しているテレワーク方式をフローチャートで確認できる。
３．テレワーク方式の全体概要	本書で取り扱うテレワーク方式の概要を解説する。
４．テレワーク方式の解説	本書で取り扱う各テレワーク方式の詳細を解説する。
第２部	
１．テレワークセキュリティ 対策チェックリスト	テレワーク方式ごとに、実施すべきセキュリティ対策項目を「チェックリスト」の形で示す。
２．対策チェックリストの設定例一覧	テレワークでよく利用される製品の設定・利用方法について解説した「設定解説資料」を紹介する。
３．セキュリティ対策一覧	「チェックリスト」を一覧形式で示すとともに、それぞれのセキュリティ対策項目における想定脅威の詳細 を示す。
参考	
１．テレワーク環境を狙う脅威	テレワーク環境において想定される脅威について解説する。
２．テレワークに有効なセキュリティ対策	テレワーク環境における脅威を回避するための効果的なセキュリティ対策について解説する。
３．知っておきたいキーワード集	テレワークセキュリティ 対策チェックリストに登場するセキュリティ対策の重要なキーワードについて、図解を用いて詳しく解説する。

[19] 総務省 サイバーセキュリティ統括官室：「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第２版）（令和３年５月)」
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

構成	概要
４．用語集	本書で用いている主な用語を解説する。
５．リンク集	対策チェックリストを活用する上で参考となる文献や Web サイト等を示す。
付録（別紙）	
従業員向けハンドブック	テレワークを行う従業員が常に反復して気を付けるべきことやもしもの時の連絡先等を記載している。テレワークを実施する従業員に配布し活用を求める。
緊急時対応カード(シール)	テレワークを行う従業員が困った際にどういった行動を最優先にすべきか記載している。テレワークを実施する従業員に配布し、パソコン等のテレワーク端末に貼付し活用を求める。

③ 活用に当たってのポイント

8 つの方式（方式①会社支給端末・VPN／リモートデスクトップ方式、方式②会社支給端末・クラウドサービス方式、方式③会社支給端末・スタンドアロン方式、方式④ 会社支給端末・セキュアブラウザ方式、方式⑤個人所有端末・VPN／リモートデスクトップ方式、方式⑥個人所有端末・クラウドサービス方式、方式⑦個人所有端末・スタンドアロン方式及び方式⑧個人所有端末・セキュアブラウザ方式）に対応する対策内容について優先度を踏まえて活用すれば、比較的容易に自社のテレワーク対策が実現可能である。

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）

（解説）

● 基本対策事項 (1)(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）」について

① 対象

全組織

② 概要

組織における内部不正の防止を主眼とし、その後の早期発見と拡大防止も視野に入れたガイドラインである。

③ 活用に当たってのポイント

付録 VI：内部不正防止の基本５原則と 25 分類（表 ３-１４参照）を活用すれば、比較的容易に自社の内部不正防止関連規程を策定可能である。また、内部不正チェックシート（表 ３-１５参照）を活用すれば、自組織の内部不正対策の状況を把握することが可能である。

表 3－１４　付録 VI：内部不正防止の基本 5 原則と 25 分類

基本 5 原則と 25 分類		対策例	主な対策項目
犯行を難しくする(やりにくくする)：対策を強化することで犯罪行為を難しくする			
	対象の防御策を強化する	アクセス制御、パスワードポリシーの設定、退職者の ID 削 除、セキュリティワイヤーによる PC 固定	(5)(6)(7)(9)(15)(24)
	施設への出入りを制限する	外部者の立ち入り制限、入退出管理	(8)
	出口で検査する	ノート PC 等の持ち出し検査、メールやネットの監視	(8)(10)(12)(18)(19)
	犯罪者をそらす	物理レベルに応じた入退制限	(8)
	情報機器やネットワークを制限する	未許可の PC/USB メモリの持ち込み禁止、SNS の利用制限、ホテル及び公衆の無線 LAN の利用制限	(11)(13)(16)
捕まるリスクを高める（やると見つかる）：管理や監視を強化することで捕まるリスクを高める			
	監視を強化する	アクセスログの監視、複数人での作業環境、情報機器の棚卸し、モバイル機器の持出管理、入退室記録の監査	(6)(8)(9)(10)(12)(18)(19)(33)
	自然監視を支援する	通報制度の整備	(32)
	匿名性を減らす	ID 管理、共有アカウント廃止、台帳による持出し管理	(7)(9)(10)
	現場管理者を利用する	単独作業の制限	(29)
	監視体制を強化する	監視カメラの設置、機械警備システムの導入	(8)(12)
犯行の見返りを減らす（割に合わない）：標的を隠す/排除する、利益を得にくくすることで犯行を防ぐ			
	標的を隠す （存在がわからない）	アクセス権限の設定、モバイル機器等の施錠保管、覗き見防止フィルムの貼付	(5)(6)(9)(16)(22)
	対象を排除する （存在をなくす）	データの完全消去、記録媒体等の物理的な破壊、関係者に開示した情報の廃棄・消去	(4)(9)(14)(24)
	所有物を特定する	情報機器及び記録媒体の資産管理	(9)

基本 5 原則と 25 分類		対策例	主な対策項目
	市場を阻止する	警察への迅速な届出、(法制度対応)	(30)
	利益を得にくくする	電子ファイル・ハードディスク・通信の暗号化	(13)(14)(15)(16)
犯行の誘因を減らす（その気にさせない）：犯罪を行う気持ちにさせないことで犯行を抑止する			
	欲求不満やストレスを減らす	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(21)(27)(28)
	対立（紛争）を避ける	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(21)(27)(28)(32)
	感情の高ぶりを抑える	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(27)(28)
	仲間からの圧力を緩和する	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(28)
	模倣犯を阻止する	再発防止策、(インシデントの手口の公表を慎重にする)	(31)
犯罪の弁明をさせない（言い訳させない）：犯行者による自らの行為の正当化理由を排除する			
	規則を決める	基本方針の策定、管理・運用策の策定、業務委託契約、就業規則	(1)(2)(17)(21)(22) (23)(25)(30)
	指示を掲示する	基本方針の組織内外への掲示、教育による周知徹底、	(1)(2)(20)(21)(22)
	良心に警告する	管理レベルの表示、誓約書へのサイン、持ち込み禁止のポスター	(3)(4)(11)(20)(21)(22) (23)(26)
	コンプライアンスを支援する	順守事項や関連法などの教育	(20)(21)(22)(25)(26)
	薬物・アルコールを規制する	（職場での飲酒禁止、重要情報所持時の飲酒制限）	-

表 3-15　内部不正チェックシート

No	内容
4.1. 基本方針	
(1)-①	内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか？
(1)-②	「基本方針」に基づき対策を実施するためのリソースが確保されるよう、必要な決定、指示をしていますか？
(2)-①	経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を 行っていますか？（ただし、経営者が組織全体に目が届く 組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はありません。）
(2)-②	総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していますか？
4-2-1. 秘密指定	
(3)	重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか？
(4)-①	重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていますか？
(4)-②	重要情報を含む電子文書には、内部者が分かるように機密マーク等の表示をしていますか？
4-2-2. アクセス権指定	
(5)-①	情報システムを管理・運営する担当者は、利用者 ID 及びアクセス権の登録・変更・削除等の設定手順を定めて運用して いますか？
(5)-②	情報システムを管理・運営する担当者は、異動又は退職により不要となった利用者 ID 及びアクセス権を、ただちに削除 していますか？
(6)	複数のシステム管理者がいる場合は、情報システムの管理者 ID ごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか？ また、システム管理者が一人の場合は、 ログ等により監視していますか？
(7)	情報システムでは、共有 ID や共有のパスワード・IC カード等を使用せず、個々の利用者 ID を個別のパスワード・IC カード 等で認証していますか？
4-3. 物理的管理	
(8)	重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していますか？
(9)-①	PC 等の情報機器や USB メモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理・保護していますか？
(9)-②	情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認していますか？
(10)	モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていますか？
(11)	個人のモバイル機器及び記録媒体の業務利用及び持込を制限していますか？
4-4. 技術・運用管理	
(12)	モニタリングシステムが提供する AI 監視機能等（例： ふるまい解析機能）の有効性を評価していますか？
(13)	組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトや SNS、外部のオンラインストレージ等の 使用を制限していますか？
(14)-①	委託先等の関係者への重要情報の受渡しは、受渡しから廃棄迄を含めて管理していますか？
(14)-②	インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し、暗号化等で保護していますか？
(15)	組織外部で利用・取り扱い可能な重要情報を限定し、重要情報や情報機器を保護していますか？
(16)	組織外で重要情報を用いた業務を行う際に、周囲の環境やネットワーク環境等を考慮して保護していますか？

(17)	委託する業務内容に応じたセキュリティ対策を契約前に確認・合意し、契約期間中にも契約通りにセキュリティ対策が実施されていることを確認していますか？
4-5. 原因究明と証拠確保	
(18)	重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか？（推 奨）
(19)	システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していま すか？
4-6. 人的管理	
(20)-①	すべての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか？
(20)-②	教育を定期的に繰り返して実施し、教育内容を定期的に見直して更新していますか？
(21)	従業員の行動や心身の状態のモニタリングの目的が、従業員の適正かつ健全な就業を支援し、従業員を内部不正から 保護する ためであることを、就業規則で 広く周知していますか？
(22)	派遣労働者による重要情報の漏えい等の不正行為が発生しないように、派遣元と協力して、秘密保持義務を課していますか？
(23)	雇用の終了時に秘密保持義務を課す誓約書の提出を求めていますか？（推奨）
(24)	役職員の雇用終了時および請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却または完全消去し、情報システムの利用者 ID や権限を削除していますか？
4-7. コンプライアンス	
(25)	就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか？
(26)	役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等を要請していますか？
4-8. 職場環境	
(27)	公平で客観的な人事評価を整備するとともに、業績に対する評価を説明する機会を設ける等、人事評価や業績評価の整備を推進していますか？（推奨）
(28)	業務量及び労働時間の適正化等の適切な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していますか？（推奨）
(29)	相互監視ができない環境における単独作業を制限し、単独作業には事前承認、事後確認等の手続きを定めていますか？（推奨）
4-9. 事後対策	
(30)	内部不正の影響範囲を特定するために、 事象の具体的状況を把握するとともに、 被害の最小化策や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保していますか？
(31)	内部不正者に対する処罰を検討し、内部不正の事例を内部に告知することを検討していますか？
4-10. 組織の管理	
(32)	内部不正と思わしき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していますか？
(33)	内部不正対策の項目を抽出し、定期的及び不定期に確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していますか？

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、表 ３-１６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。

（解説）

● **基本対策事項(1)「インシデント時に報告が必要となるステークホルダー」について**

表 ３−１６　インシデント等の報告・相談先の例

場合	届出元	届出先	根拠となる法令・規程等	備考・参考 URL
【必須】 衛星リモートセンシング装置又はこれを搭載する地球周回人工衛星の故障その他の事情により、終了措置を講ずることなく当該衛星リモートセンシング装置の使用を行うことができなくなり、かつ、回復する見込みがない場合	衛星リモートセンシング装置使用者	内閣総理大臣（内閣府）	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 第 11 条（故障時等の措置）	内閣府：「「衛星リモートセンシング装置使用許可」及び「衛星リモートセンシング記録取扱認定」に関する申請受付について」 https://www8.cao.go.jp/space/application/rs/application.html
【必須】 人工衛星の他の物体との衝突その他の事故の発生により、同項の許可に係る終了措置を講ずることなく人工衛星の管理ができなくなり、かつ、回復する見込みがない場合	人工衛星管理者	内閣総理大臣（内閣府）	人工衛星等の打上げ及び人工衛星の管理に関する法律 第 25 条（事故時の措置）	内閣府：「宇宙活動法に関する申請受付について」 https://www8.cao.go.jp/space/application/space_activity/application.html

場合	届出元	届出先	根拠となる法令・規程等	備考・参考 URL
【必須】 電気通信業務の一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他重大な事故が生じた場合	電気通信事業者	総務大臣 （総務省）	電気通信事業法 第 28 条（業務の停止等の報告） 電気通信事業法施行規則 第 58 条（報告を要する重大な事故）	総務省：「重大な事故の報告」 https://www.soumu.go.jp/menu_seisaku/ictseisaku/net_anzen/jiko/judai.html
【必須】 設備に起因する放送の停止、またその他の重大な事故が生じた場合	放送衛星関連事業者	総務大臣 （総務省）	放送法 第 113 条（重大事故の報告） 第 122 条（重大事故の報告） 放送法施行規則 第 125 条（報告を要する重大な事故）	総務省：「放送停止事故に関する報告制度」 https://www.soumu.go.jp/main_content/000496674.pdf
【必須】 宇宙に関連するサービスが起因で重要インフラのサービスに支障が生じる場合	重要インフラ事業者	関係省庁 ※詳細は右記リンク参照	※詳細は右記リンク参照	内閣官房 サイバーセキュリティセンター：「重要インフラのサイバーセキュリティに係る行動計画」（2022 年 6 月） https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf （P48～）
【必須】 契約上の報告義務等がある場合	被害組織	契約相手方	契約	-
【必須】 特定個人情報（マイナンバー等）を漏えい等した場合	個人番号利用事務実施者、個人番号関係事務実施者等	個人情報保護委員会等	事業者における特定個人情報の漏えい事案等が発生した場合の対応について（平成 27 年特定個人情報保護委員会告示第 2 号）	個人情報保護委員会：「特定個人情報の漏えい事案等が発生した場合の対応について」（2021 年 3 月） https://www.ppc.go.jp/legal/rouei/
【努力義務】 個人情報の漏えい等事案が発覚した場合	個人情報取扱事業者	個人情報保護委員会等	個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）	個人情報保護委員会：「漏えい等の対応（個人情報）」 https://www.ppc.go.jp/personalinfo/legal/leakAction/
【任意】 高等教育機関において情報セキュリティインシデントが発生した場合	総務部門等	文部科学省	高等教育機関の情報セキュリティ対策のためのサンプル規程集（2019 年度版増補）	大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 高等教育機関における情報セキュリティポリシー推進部会：「高等教育機関における情報セキュリティポリシー策定について」 https://www.nii.ac.jp/service/sp/
【任意】 サイバー犯罪の被害にあったおそれのある場合	被害組織	各都道府県警察本部のサイバー犯罪相談窓口	-	警察庁 サイバー犯罪対策プロジェクト：「都道府県警察本部のサイバー犯罪相談窓口一覧」 https://www.npa.go.jp/cyber/soudan.html

場合	届出元	届出先	根拠となる法令・規程等	備考・参考 URL
【任意】 機微技術（外国為替及び外国貿易法で輸出管理対象とされている技術等）の情報流出の懸念がある場合	被害組織	経済産業省（サイバーセキュリティ課又は宇宙産業室）	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（経産省）	経済産業省 商務情報政策局サイバーセキュリティ課：「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」（2020 年 12 月） https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf 経済産業省 商務情報政策局サイバーセキュリティ課：「「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバーセキュリティお助け隊」）」の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（2020 年 6 月） https://www.meti.go.jp/press/2020/06/20200612004/20200612004-2.pdf
【任意】 標的型サイバー攻撃を受けたおそれのある場合	被害組織	IPA セキュリティセンター（サイバーレスキュー隊（J-CRAT））	-	独立行政法人情報処理推進機構 セキュリティセンター：「J-CRAT／標的型サイバー攻撃特別相談窓口」（2021 年 8 月） https://www.ipa.go.jp/security/tokubetsu/ 独立行政法人情報処理推進機構：「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）」（2021 年 6 月） https://www.ipa.go.jp/security/J-CRAT/index.html
【任意】 コンピュータウイルス・不正アクセスの被害にあった場合	被害組織	IPA セキュリティセンター	コンピュータウイルス対策基準（経済産業省告示） コンピュータ不正アクセス対策基準（経済産業省告示）	独立行政法人情報処理推進機構 セキュリティセンター：「コンピュータウイルス・不正アクセスに関する届出について」（2021 年 8 月） https://www.ipa.go.jp/security/outline/todokede-j.html 独立行政法人情報処理推進機構 セキュリティセンター：「情報セキュリティ安心相談窓口」 https://www.ipa.go.jp/security/anshin/
【任意】 ソフトウェア製品等の脆弱性関連情報を発見した場合	脆弱性関連情報の発見者	IPA セキュリティセンター	ソフトウエア製品等の脆弱性関連情報に関する取扱規程（経済産業省告示）	独立行政法人情報処理推進機構：「脆弱性関連情報の届出受付」 https://www.ipa.go.jp/security/vuln/report/
【任意】 インシデント対応についての支援・相談を得たい場合	被害組織	JPCERT/CC	-	一般社団法人 JPCERT コーディネーションセンター：「インシデント対応依頼（JPCERT/CC）」（2018 年 11 月） https://www.jpcert.or.jp/form/
【任意】 ベンダーのサービスや保険等が活用できる場合	被害組織	契約相手方	契約	-

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

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

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(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

（解説）

● 要求事項(1)(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」について

① 対象

人工衛星及びその打上げロケットの運用・管理等

② 概要

宇宙諸条約への対応と民間宇宙活動の進展の観点から、図 3-4に示すとおり、人工衛星等の打上げに係る許可、人工衛星の打上げ用ロケットの型式認定、打上げ施設の適合認定、人工衛星の管理に係る許可、損害賠償担保措置の承認等を得る必要があることが本法律で定められている。

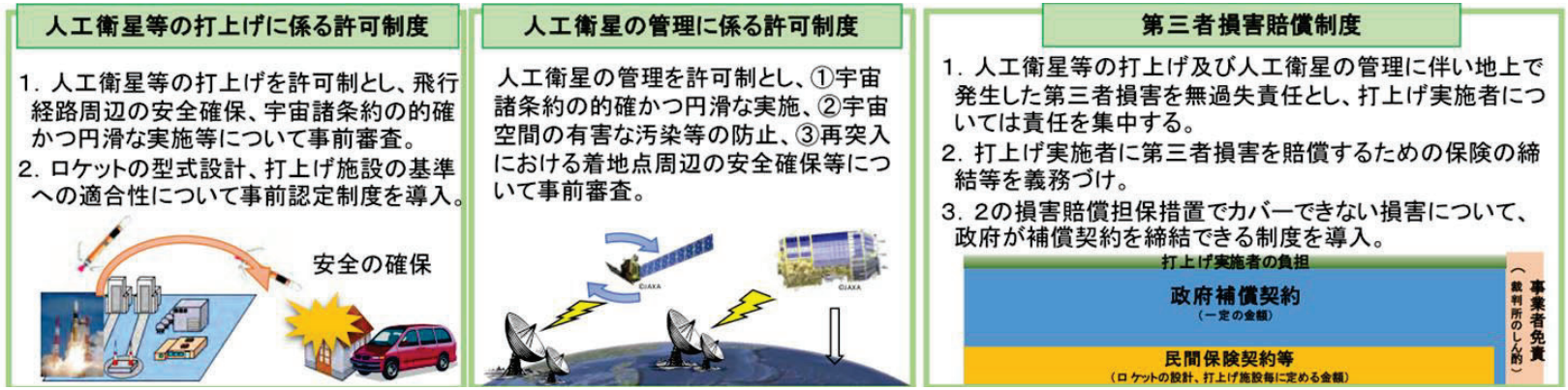

図 3－4　人工衛星等の打上げ及び人工衛星の管理に関する法律の主な内容[20]

なお、審査基準の別表には、法律・施行規則の対応及び具体的な要求事項が記載されている。

● 要求事項(1)(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」について

① 対象

衛星リモートセンシング装置使用者及び衛星リモートセンシング記録保持者

② 概要

衛星リモートセンシング記録の適正な取扱いを確保するため、図 3-5に示すとおり、衛星リモートセンシング装置の使用に係る許可、衛星リモートセンシング記録保有者の義務、衛星リモートセンシング記録を取り扱う者の認定等必要な事項が本法律で定められている。各要求事項の法令体系は図 3-6のように整理される。[21]

[20] 図出典：内閣府 宇宙開発戦略推進事務局：「宇宙政策委員会 第６５回会合 資料１」（2017 年 12 月）https://www8.cao.go.jp/space/comittee/dai65/gijisidai.html
[21] 内閣府 宇宙開発戦略推進事務局：「「衛星リモートセンシング装置使用許可」及び「衛星リモートセンシング記録取扱認定」に関する申請受付について」
https://www8.cao.go.jp/space/application/rs/application.html

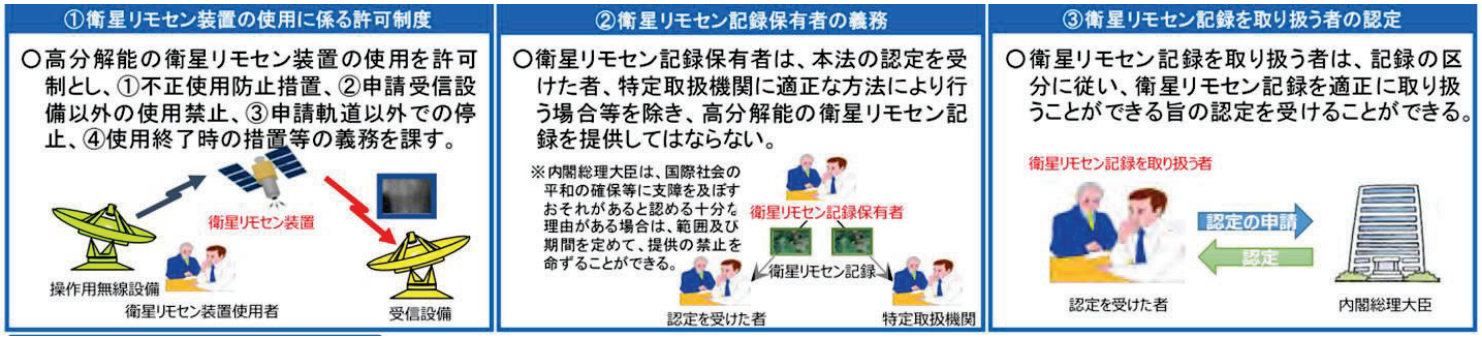

図　3－5　衛星リモートセンシング記録の適正な取扱いの確保に関する法律の主な内容[22]

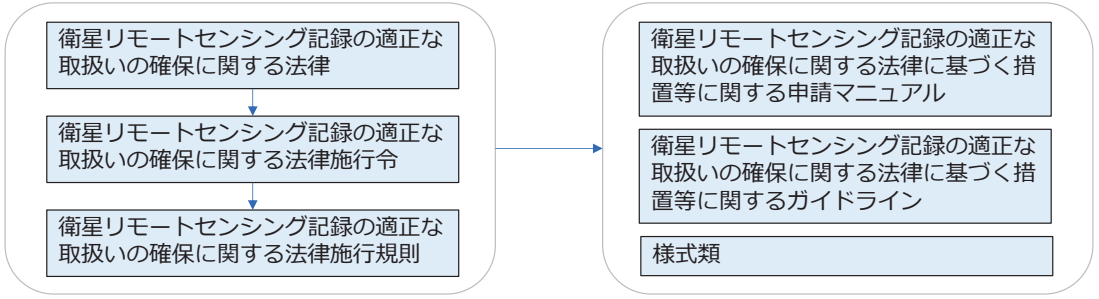

図　3－6　要求事項(1)(b)の法令体系

また、施行規則において、衛星リモートセンシング記録を取り扱う場合は、表 3-１７のセキュリティ要件を満たす必要があることが定められている。

表　3－１７　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の関連条文

第七条　法第六条第二号及び第二十条の内閣府令で定める措置は、次の表の上欄に掲げる衛星リモートセンシング記録の区分に応じ、それぞれ同表の下欄に定めるとおりとする。

センシング記録の区分	措置
一　生データ	イ　組織的安全管理措置 （一）　衛星リモートセンシング記録の安全管理に係る基本方針を定めていること。 （二）　衛星リモートセンシング記録を取り扱う者の責任及び権限並びに業務を明確にしていること。

[22] 図出典：内閣府 宇宙開発戦略推進事務局：「宇宙政策委員会 第６５回会合 資料１」（2017 年 12 月）https://www8.cao.go.jp/space/comittee/dai65/gijisidai.html

	（三）　衛星リモートセンシング記録の漏えい、滅失又は毀損発生時における事務処理体制が整備されていること。 （四）　安全管理措置に関する規程の策定及び実施並びにその運用の評価及び改善を行っていること。 ロ　人的安全管理措置 （一）　衛星リモートセンシング記録を取り扱う者が、法第五条第一号から第四号まで及び法第二十一条第三項第一号イからニまでのいずれにも該当しない者であることを確認していること。 （二）　衛星リモートセンシング記録を取り扱う者が、その業務上取り扱う衛星リモートセンシング記録についての情報その他の特別の非公開情報（その業務上知り得た公表されていない情報をいう。）を、当該業務の適切な運営の確保その他必要と認められる目的以外の目的のために利用しないことを確保するための措置を講じていること。 （三）　衛星リモートセンシング記録を取り扱う者に対する必要な教育及び訓練を行っていること。 ハ　物理的安全管理措置 （一）　衛星リモートセンシング記録を取り扱う施設設備を明確にしていること。 （二）　衛星リモートセンシング記録を取り扱う施設設備への立入り及び機器の持込みを制限する措置を講じていること。 （三）　衛星リモートセンシング記録を取り扱う電子計算機及び可搬記憶媒体（電子計算機又はその周辺機器に挿入し、又は接続して情報を保存することができる媒体又は機器のうち、可搬型のものをいう。以下この項において同じ。）には、その盗難、紛失その他の事故を防止するため、電子計算機の端末をワイヤで固定することその他の必要な物理的措置を講じていること。 ニ　技術的安全管理措置 （一）　衛星リモートセンシング記録を取り扱う施設設備に、不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）を防止するため、適切な措置が講じられていること。 （二）　可搬記憶媒体の電子計算機又はその周辺機器への接続の制限に関する措置を講じていること。 （三）　衛星リモートセンシング記録の取扱いに係る電子計算機及び端末装置の動作を記録していること。 （四）　衛星リモートセンシング記録を移送又は電気通信により送信するときは、暗号化その他の衛星リモートセンシング記録を適切に保護するために必要な措置を講じていること。 （五）　衛星リモートセンシング記録を加工するときは、当該加工を適切に行うために必要な措置を講じていること。
二　標準データ	イ　組織的安全管理措置 生データの項イと同じ。 ロ　人的安全管理措置 生データの項ロと同じ。 ハ　技術的安全管理措置 生データの項ニと同じ。

衛星リモートセンシング記録を取り扱う場合に求められる各安全管理措置への対応に当たって参考となる本ガイドラインの項目は、表 3-１８のように整理される。

表 3-１８　各安全管理措置への対応に当たって参考となる本ガイドラインの項目

安全管理措置	項番	参考となる本ガイドラインの項目
イ　組織的安全管理措置	（一）	３．１．１　組織的なセキュリティリスクマネジメント
	（二）	３．１．１　組織的なセキュリティリスクマネジメント

安全管理措置	項番	参考となる本ガイドラインの項目
	（三）	３．１．１　組織的なセキュリティリスクマネジメント ３．１．４　内部犯行対策 ３．１．５　外部へのインシデント報告
	（四）	３．１．１　組織的なセキュリティリスクマネジメント
ロ　人的安全管理措置	（一）	３．１．１　組織的なセキュリティリスクマネジメント
	（二）	３．１．１　組織的なセキュリティリスクマネジメント
	（三）	３．１．１　組織的なセキュリティリスクマネジメント
ハ　物理的安全管理措置	（一）	３．２．３　衛星運用システム 基本対策事項(1)-(a) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(a)
	（二）	３．２．３　衛星運用システム 基本対策事項(1)-(a) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(a)
	（三）	３．２．３　衛星運用システム 基本対策事項(1)-(a)、(1)-(d) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(a)、(1)-(d)
ニ　技術的安全管理措置	（一）	３．２．３　衛星運用システム 基本対策事項(1)-(b)、(1)-(f) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(b)
	（二）	３．２．３　衛星運用システム 基本対策事項(1)-(f) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(d)
	（三）	３．２．３　衛星運用システム 基本対策事項(1)-(d)、(1)-(f) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(d)
	（四）	３．２．３　衛星運用システム 基本対策事項(1)-(b)、(1)-(f) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(b)
	（五）	３．２．３　衛星運用システム 基本対策事項(1)-(b) ３．２．４　衛星通信システム・衛星データ利用システム 基本対策事項(1)-(b)

衛星リモートセンシング記録を取り扱う場合に求められる各安全管理措置への対応に当たって参考となる添付資料３の項目は、表 3-１９のように整理される。

表 3-１９　各安全管理措置への対応に当たって参考となる添付資料３の項目

安全管理措置	項番	参考となる添付資料３の項目
イ　組織的安全管理措置	（一）	１．組織的対策
	（二）	１．組織的対策 ２．人的対策 ６．IT 機器利用 ７．IT 基盤運用管理

安全管理措置	項番	参考となる添付資料３の項目
	（三）	１．組織的対策 １０．情報セキュリティインシデント対応及び事業継続管理
	（四）	１．組織的対策
ロ　人的安全管理措置	（一）	２．人的対策
	（二）	２．人的対策 ３．情報資産管理
	（三）	２．人的対策
ハ　物理的安全管理措置	（一）	５．物理的対策
	（二）	５．物理的対策
	（三）	５．物理的対策
ニ　技術的安全管理措置	（一）	５．物理的対策
	（二）	６．IT 機器利用
	（三）	７．IT 基盤運用管理
	（四）	３．情報資産管理
	（五）	３．情報資産管理

● 要求事項(1)(c)「電気通信事業法／電気通信事業法施行規則」について

① 対象

電気通信事業者、電気通信設備

② 概要

電気通信事業者は、電気通信役務の確実かつ安定的な提供を確保するために、電気通信事業の開始前に、電気通信設備の管理方針・管理体制・管理方法・設備統括管理者の選任に関する規程を策定し、総務大臣に届け出るよう定められている。また施行規則において、表 3-２０に示すように、管理規程の内容（方針、体制、方法、設備統括管理者の選任）に含むべき事項として、情報セキュリティ確保に関する内容が定められている。

表 3-２０　電気通信事業法施行規則第 29 条第 1 項の関連条文

第二十九条　法第四十四条第二項の総務省令で定める管理規程の内容は、次のとおりとする。

一　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方針に関する事項
　イ　組織の全体的かつ部門横断的な事業用電気通信設備の管理の方針に関すること。
　ロ　関係法令、管理規程その他の規定の遵守に関すること。
　ハ　通信需要、相互接続等を考慮した事業用電気通信設備の管理の方針に関すること。
　ニ　災害を考慮した事業用電気通信設備の管理の方針に関すること。
　ホ　情報セキュリティの確保のための方針に関すること

二　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の体制に関する事項
　イ　経営の責任者の職務に関すること。
　ロ　電気通信設備統括管理者の職務に関すること。
　ハ　電気通信主任技術者の職務及び代行に関すること。
　ニ　各部門の責任者の職務に関すること。
　ホ　各従事者の職務に関すること。
　ヘ　組織内の連携体制の確保に関すること。
　ト　組織外の関係者との連携及び責任分担に関すること。

三　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方法に関する事項
　イ　基本的な取組に関すること。
　ロ　事業用電気通信設備の設計、工事、維持及び運用に従事する者に対する教育及び訓練等の実施に関すること。
　ハ　事業用電気通信設備の設計、工事、維持及び運用に関すること。
　ニ　通信量の変動を踏まえた適切な設備容量の確保に関すること。
　ホ　情報セキュリティ対策に関すること。
　ヘ　ソフトウェアの信頼性の確保に関すること。
　ト　重要通信の確保及びふくそう対策に関すること。
　チ　緊急通報の確保に関すること。
　リ　防犯対策に関すること。
　ヌ　事業用電気通信設備の設計、工事、維持及び運用に従事する者による誤りを防止するための対策に関すること。
　ル　事業用電気通信設備のうち、その損壊又は故障等による利用者の利益に及ぼす影響が大きいものとして総務大臣が別に告示するもののリスクの分析及び評価に関すること。
　ヲ　ルに関する取組を踏まえた事業継続計画又はこれに相当する計画の策定に関すること。
　ワ　ふくそう、事故、災害その他非常の場合の報告、記録、措置及び周知に関すること。
　カ　利用者の利益の保護の観点から行う利用者に対する情報提供に関すること。
　ヨ　事故の再発防止のための対策に関すること。

● 要求事項(1)(d)「放送法／放送法施行規則」について

① 対象

放送事業者、放送設備及び当該放送設備を維持又は運用するために必要な設備

② 概要

放送業務に著しい支障を及ぼすおそれがないよう、サイバーセキュリティの確保のために必要な措置が講じられていなければならない。

● 要求事項(1)(e)「外国為替及び外国貿易法」について

① 対象

外国為替及び外国貿易法第２５条第１項（表 3-２１参照）及び外国為替令第１７条第２項の規定に基づき許可を要する技術を取扱うもの

② 概要

法令等で定める特定技術を海外拠点等で管理する場合、若しくは日本国内で特定国の非居住者に当該技術を提供することを目的とする場合、許可を受ける必要がある旨が定められている。

表 3−２１　外国為替及び外国貿易法の関連条文

第２５条 第１項　国際的な平和及び安全の維持を妨げることとなると認められるものとして政令で定める特定の種類の貨物の設計、製造若しくは使用に係る技術（以下「特定技術」という。）を特定の外国（以下「特定国」という。）において提供することを目的とする取引を行おうとする居住者若しくは非居住者又は特定技術を特定国の非居住者に提供することを目的とする取引を行おうとする居住者は、政令で定めるところにより、当該取引について、経済産業大臣の許可を受けなければならない。

宇宙産業で特定技術に該当する可能性があるものとしては、以下に示すもの等が考えられる。これらの取扱いに際しては、運用設計段階から本法律の内容を十分に考慮の上、必要に応じて手続を行うこと。

- 人工衛星搭載用の姿勢制御装置
- 人工衛星搭載用のコマンド／テレメトリ・データ処理装置
- 人工衛星搭載用の光学センサや SAR
- 上記の使用のために設計したプログラム　等

３．２．２ 衛星本体

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

要求事項

衛星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) 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) 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保護

(f) サプライチェーンに対するセキュリティ対策

（解説）

● 基本対策事項(1)(a)「通信の保護」について

衛星と地上間の衛星通信において RF 通信を用いる場合、RF 通信パラメータを周知していれば誰もが RF 通信情報を傍受可能であるが、暗号化と電子署名等の対策を施していれば情報漏えい、情報の改ざんは防止可能である。加えて、高いセキュリティレベルが求められる場合は、暗号化のみならずスペクトラム拡散技術を組み合わせた情報漏えい防止対策を用いることがある。なお、アマチュア無線帯の利用や衛星本体のリソースの制約等の理由により RF 通信の暗号化が困難な場合には、通信の改ざんを検知する電子署名、メッセージ認証等を組み込む等の対策がある。衛星と地上間の通信環境の可用性を確保するためには、複数のアップリンクパス及びダウンリンクパスを用意する、複数のアクセスポイントを用意する、バックアップ局を用意する、複数のコマンド周波数を使用可能にする等のいずれか又は複数の対策がある。

衛星と地上間の衛星通信において光通信を用いる場合、狭いビームを用いることにより通信の盗聴が困難となる。また、光通信の場合、電波干渉の影響を受けないことも大きな特徴となるが、悪天候の影響を受け通信が実施できない場合があるため、セカンダリーの通信チャネルを用意することが必要となる。システム全体

のリスクを低減するために、セカンダリーの通信チャネルに対しても通信の保護対策を講じることが望まれる。

衛星間通信に対する盗聴やなりすましの攻撃は、攻撃に多大なリソースが必要となるため、衛星と地上間の通信に対する攻撃と比較して脅威は限定的となる。よって、ミッションが侵害された場合の影響度に応じて保護対策を講じることが望まれる。

暗号化技術を用いる場合は鍵管理が重要である。暗号鍵管理に当たっては、IPA の「暗号鍵管理ガイダンス」[23]や NIST の SP 800-57「Recommendation for Key Management」[24]が参考となる。暗号鍵方式の中で、特に共通鍵暗号方式（秘密鍵暗号方式、対称鍵暗号方式ともいう。）では鍵の配送方式が課題となる。例えば、衛星コンステレーション運用時等に、複数の相手と通信を行う際には、共通鍵暗号方式では複数の鍵を管理する点で限界があるため、安全に単一の暗号鍵を共有する方式であるとして公開鍵暗号方式を利用することが想定される。一方で、ポイント・ツー・ポイントの通信であり、相手が限定される宇宙ミッションシナリオでは、処理速度の面から共通鍵暗号方式の使用が推奨されている[25]。特定のミッションに対する暗号方式の具体的な選択は、ミッションに対する脅威を想定し、リスクアセスメントを行った上で決定すべきである。

一般的な暗号についての参考情報として、デジタル庁、総務省及び経済産業省が CRYPTREC の活動を通じて策定している「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」[26]や、本リストに掲載されている暗号技術を利用する際に適切なセキュリティ強度を実現するためのアルゴリズム及び鍵長の選択方法を規定した「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」[27]がある。宇宙分野における暗号についての参照情報として、CCSDS（Consultative Committee for Space Data System：宇宙データシステム諮問委員会）勧告の標準規格「CCSDS CRYPTOGRAPHIC ALGORITHMS」[28,29]がある。また、暗号鍵管理についての参照情報として、CCSDS 勧告の標準規格「SYMMETRIC KEY MANAGEMENT」[30]や「SPACE MISSIONS KEY MANAGEMENT CONCEPT」[31]がある。衛星本体のリソース制約等を踏まえると、軽量かつ高速な暗号アルゴリズムを選択することが望ましい。また、衛星の通信においては、悪天候、宇宙線、ジャミング等によりバースト誤りが発生する可能性を踏まえ、誤り訂正を伴う暗号アルゴリズムを選択することも想定される。

---

[23] IPA：「暗号鍵管理ガイダンス」（2023 年 5 月）https://www.ipa.go.jp/security/crypto/guideline/ckms.html
[24] NIST：SP 800-57「Recommendation for Key Management」https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
[25] CCSDS：「SYMMETRIC KEY MANAGEMENT (RECOMMENDED PRACTICE), CCSDS 354.0-M-1」（2023 年 12 月） https://public.ccsds.org/Pubs/354x0m1.pdf
[26] デジタル庁、総務省、経済産業省：「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」（2023 年 5 月）
https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022.pdf
[27] デジタル庁、総務省、経済産業省：「暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準」（2022 年 3 月）https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf
[28] CCSDS：「CCSDS CRYPTOGRAPHIC ALGORITHMS (INFORMATIONAL REPORT), CCSDS 350.9-G-2」（2023 年 6 月）https://public.ccsds.org/Pubs/350x9g1.pdf
[29] CCSDS：「CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), CCSDS 352.0-B-2」（2019 年 8 月） https://public.ccsds.org/Pubs/352x0b2.pdf
[30] CCSDS：「SYMMETRIC KEY MANAGEMENT (RECOMMENDED PRACTICE), CCSDS 354.0-M-1」（2023 年 12 月） https://public.ccsds.org/Pubs/354x0m1.pdf
[31] CCSDS：「SPACE MISSIONS KEY MANAGEMENT CONCEPT (INFORMATIONAL REPORT), CCSDS 350.6-G-1」（2011 年 11 月）https://public.ccsds.org/Pubs/350x6g1.pdf

【参考】CCSDS 勧告の標準規格について

CCSDS は、1982 年に各国の宇宙機関により設立された宇宙データ通信システムに関わる国際標準化検討委員会で、宇宙データ通信システムの定義・規格化を進めている。CCSDS が作成した文書（推奨規格・推奨実践規範）に拘束力はないが、CCSDS が ISO（国際標準化機構）の宇宙データ通信分野の分科会の役割を担っていることから、それらの文書は発行後、自動的に ISO 文書化の審査・手続へと移行する。

CCSDS が作成する文書は、図 3-7 に示すように文書の種類と検討段階に応じて 9 色のブックカラーで分類されている。

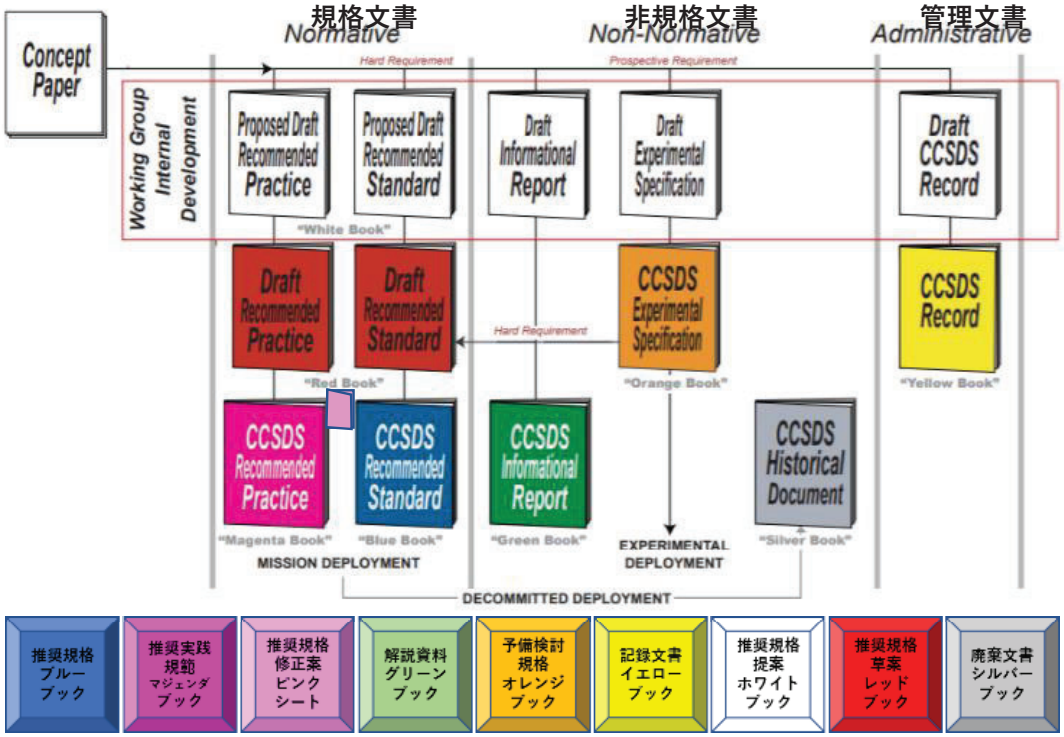

図 3-7　CCSDS の文書の分類[32, 33]

[32] 宇宙航空研究開発機構 JAXA-CCSDS 事務局：「宇宙データシステム諮問員会(CCSDS)「CCSDS 文書について」」 https://stage.tksc.jaxa.jp/ccsds/docs/booktop.html （2021/09/21 参照）
[33] CCSDS：「ORGANIZATION AND PROCESSES FOR THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS RECORD) , CCSDS A02.1-Y-4」(2014 年 4 月) https://public.ccsds.org/Pubs/A02x1y4c2.pdf

暗号アルゴリズムに関する推奨規格を示した「CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), CCSDS 352.0-B-2」[34]では、認証付き暗号化及び認証のための CCSDS 暗号セキュリティアルゴリズムに関する推奨事項を記載しており、適切に実装された標準アルゴリズムを採用することで、安全な相互運用性を実現するとともに、セキュリティサービスを利用するミッションのコストを削減することができるとしている。暗号アルゴリズムについて、機密性を確保するために、単一の共通鍵ブロック暗号である AES（Advanced Encryption Standard）の使用を推奨している。AES は、CCSDS の全てのミッション及び地上システムでの使用が推奨される唯一の対称暗号アルゴリズムで、アルゴリズムの特定の動作モードとして、カウンターモードでの使用を推奨している。鍵長に関して、レガシーシステムでは最小の鍵長である 128bit を使用可能であるとしているものの、CCSDS 352.0-B-2 が発行された 2019 年 8 月以降に計画が開始されるミッションでは 256bit の使用を推奨している。暗号化アルゴリズムと認証アルゴリズムを組み合わせた認証付き暗号アルゴリズム（AEAD）については、GCM（ガロアカウンターモード）での使用を推奨し、タグ長は 128bit を推奨している。さらに、メッセージ認証アルゴリズムとしては、ハッシュベースの HMAC、ブロック暗号ベースの CMAC、電子署名ベースの認証の 3 つの認証方式を推奨している。HMAC に基づく認証においては、SHA-256 以上のハッシュ関数の採用を推奨しているほか、CMAC に基づく認証においては、256bit 以上の鍵長を使用する AES 暗号方式を推奨している。そして、電子署名ベースの認証においては、4096bit 以上の鍵長を使用する RSA 暗号方式（ただし、レガシーシステムでは 2048bit の鍵長も使用可能としている）のほか、DSA や ECDSA 等の暗号方式も使用可能としている。「CCSDS CRYPTOGRAPHIC ALGORITHMS INFORMATIONAL REPORT), CCSDS 350.9-G-2」[35]では、それぞれのアルゴリズム実装に関する解説が示されており、各アルゴリズムの実装に当たっての参考となる。また、「SPACE MISSIONS KEY MANAGEMENT CONCEPT」[36]では、暗号鍵の管理に関する解説が示されており、鍵管理の実装に当たっての参考となる。

CCSDS では OSI（Open Systems Interconnection）モデルのどのレイヤで暗号化アルゴリズムを使用すべきかを規定していない。「THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS (INFORMATIONAL REPORT), CCSDS 350.0-G-3」[37]に示されているように、宇宙通信のレイヤリングモデルの中には、暗号化アルゴリズムを採用できるレイヤが複数あり、ミッション環境に応じて（アルゴリズムをいつ、どこで、どのように実装し、使用すべきかを規定するものではなく、ミッションのセキュリティ要件とリスクアセスメントの結果に基づいて）実施することを個々のミッション計画者に委ねている。また、複数の認証／統合アルゴリズムを用意することを推奨している。

---

[34] CCSDS :「CCSDS CRYPTOGRAPHIC ALGORITHMS (RECOMMENDED STANDARD), CCSDS 352.0-B-2」（2019 年 8 月） https://public.ccsds.org/Pubs/352x0b2.pdf
海外では、ドイツの DLR（ドイツ航空宇宙センター）が CCSDS 暗号アルゴリズムを使用している。国内では、JAXA は 2019 年時点で本推奨規格を使用していない。
https://stage.tksc.jaxa.jp/ccsds/docs/files/bluebook/sea/352_0_b_2.pdf
[35] CCSDS :「CCSDS CRYPTOGRAPHIC ALGORITHMS (INFORMATIONAL REPORT), CCSDS 350.9-G-2」（2023 年 6 月） https://public.ccsds.org/Pubs/350x9g2.pdf
[36] CCSDS :「SPACE MISSIONS KEY MANAGEMENT CONCEPT (INFORMATIONAL REPORT), CCSDS 350.6-G-1」（2011 年 11 月）https://public.ccsds.org/Pubs/350x6g1.pdf
[37] CCSDS :「THE APPLICATION OF SECURITY TO CCSDS PROTOCOLS (INFORMATIONAL REPORT), CCSDS 350.0-G-3」（2019 年 3 月） https://public.ccsds.org/Pubs/350x0g3.pdf

【参考】耐量子計算機暗号（Post-Quantum Cryptography: PQC）について

現在広く使用されている公開鍵暗号方式として RSA 暗号方式や楕円曲線暗号方式が挙げられる。これらの暗号方式が安全である（現実的な時間で解読されない）ためには、素因数分解問題や楕円曲線上の離散対数問題が計算量的に困難であることが必要である。これらの問題は、現在普及しているコンピューターでは効率的に解くことはできない一方で、量子コンピューターの開発が十分に進むと、整数の素因数分解や離散対数を高速に計算できるため、RSA 暗号や楕円曲線暗号の安全性は大きく低下する。そのため、量子コンピューターでも安全性を確保できる耐量子計算機暗号が注目されている。

米国バイデン大統領は 2022 年 5 月、量子コンピューターが米国のサイバーセキュリティに及ぼすリスクに対処するための米国政府の計画を示した国家安全保障覚書[38]に署名した。この覚書では、米国政府の暗号化システムのリスクを可能な限り軽減するために、2035 年までに連邦政府の暗号システムを耐量子計算機暗号に移行する方針を示した。米国 NIST は耐量子計算機暗号に関する標準化活動を 2016 年から実施しており、2022 年 7 月には標準化する方式の一部として 4 つの方式を決定[39]した。2023 年 8 月には、これらの方式に関するパブリックコメントを開始し、2024 年中には正式な標準仕様が発表される見通しである。NIST の動向を踏まえ、各国政府機関は耐量子計算機暗号へ移行する準備を促し始めている。国内では、情報通信研究機構（NICT）と IPA が共同運営する「暗号技術評価委員会」の 2022 年度の活動成果として「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」[40]が公開されているほか、IPA は、暗号技術に関する海外資料の日本語翻訳版を公開[41]している。

今後、宇宙分野においても耐量子計算機暗号への移行準備に動き出すことが想定される。衛星システムは開発・運用ライフサイクルが長いことに加え、内部コンポーネントのアップデートが困難であることを踏まえ、早期の移行が求められる可能性がある。NIST から正式な標準仕様が発表されることが一つの契機となるが、耐量子計算機暗号の動向についても注視することが望まれる。

---

[38] White House：「National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems」https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[39] NIST：「Post-Quantum Cryptography」https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[40] CRYPTREC 暗号技術調査ワーキンググループ（耐量子計算機暗号）：「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf

[41] 独立行政法人情報処理推進機構：「暗号技術に関する海外資料・翻訳」https://www.ipa.go.jp/security/crypto/archive.html

● **基本対策事項(1)(b)「ジャミング対策」について**

衛星と地上との間のRF通信では、有線による通信とは異なり、高い電力レベルで同じ（又は近傍の）周波数を発する機器によって妨害（ジャミング又は干渉）される可能性がある。使用している周波数に対して妨害されると、そのRFリンク上の通信は中断され、衛星と地上局との間のテレメトリやコマンドの送受信ができなくなり、衛星からのデータ収集もできなくなる。その結果、送受信できなかったデータが完全に失われ、回復不能となる可能性がある。また、地上でハウスキーピングデータを受信できないことにより、衛星に対してただちに対処しなければならない緊急事態が発生した場合に対処ができず、衛星を失うことにもなりかねない。同様に、テレメトリを受信できても、コマンドのアップリンクが妨害されていると、衛星が失われることもある。

ジャミングに対抗するための技術にはスペクトラム拡散技術と周波数ホッピング技術があるが、衛星の用途、規模、リソース制限等の理由からジャミングへの対抗技術を搭載できない場合、バックアップ局の用意、バックアップ用通信チャネルの用意（衛星リソース制限の範囲内で実装可能なバックアップ用通信チャネルを用意して適宜切り替えて運用）等の対策が考えられる。併せて、通信が利用できない場合に、未送信のデータを保存し、通信が復旧した後に再送する仕組みを導入することも考えられる。

● **基本対策事項(1)(c)「衛星実装機能の事前検証」について**

衛星に意図しない機能（衛星運用の妨害、ミッションデータの有害な改変、サービス妨害等の形でシステムに損害を与える可能性のあるあらゆる状況又はイベント）が組み込まれていた場合、ミッションの遂行が困難となるばかりか衛星を失う可能性がある。すなわち、組込みシステムのソフトウェア開発プロセス自体が潜在的な脆弱性を含むと言える。例えば、制御システムにバックドアなどの脆弱性を与えるために、開発プロセス中に悪意のあるコードが挿入される可能性がある。また、ソフトウェア開発者はしばしばシステムに再侵入して特定の機能を実行できるように、コードにトラップドアを導入することがある。こうしたソフトウェア開発プロセスにおける潜在的な問題、リスク及び脆弱性については、「SECURITY THREATS AGAINST SPACE MISSIONS」[42]で簡単に取り上げられている。以下にハードウェア及びソフトウェアの観点から事前検証方法について紹介する。

- 汚染されたハードウェア構成品（隠された悪意のある機能、システムの不安定性、システムの損傷、望ましくないシステムへの影響等）の組込み防止に対しては、サプライチェーンの信頼性検証、精査されたハードウェアサプライヤー、点検済みのハードウェア生産、ハードウェアの信頼性検証、ハードウェア機能性の分析等のセキュリティメカニズムにより対応が可能である。
- システムに組み込まれたソフトウェアの脅威（好ましくないイベント、システムへの損傷、他の脅威の有効化等）に対しては、受入テスト、IV&V（Independent Verification & Validation: 独立検証・有効性確認）、コードウォークスルー、自動コード解析、ランタイム・セキュリティ・モニタリング、ソ

[42] CCSDS：「SECURITY THREATS AGAINST SPACE MISSIONS（INFORMATIONAL REPORT）CCSDS 350.1-G-3」（2022年2月） https://public.ccsds.org/Pubs/350x1g3.pdf

フトウェア・パーティショニング（信頼できるコンピューティングベース)、サプライチェーンの信頼性検証等のセキュリティメカニズムがある。なお、IV&V についての参考図書としては、「IV&V ガイドブック【導入編】」（JAXA）[43]が挙げられる。

近年、衛星における OSS（Open Source Software）の活用が増加している。OSS のセキュリティ対策に当たっては、以下に解説する「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」（経済産業省）[44]や「共通脆弱性識別子 CVE 概説」（IPA）[45]等の参考図書がある。

「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」では、多くの企業が OSS を含むソフトウェアの管理手法、脆弱性対応等に課題を抱えている現状を踏まえ、参考になる取組を実施している企業に対するヒアリング等による調査により、選定評価、ライセンス、脆弱性対応、保守・品質保証、サプライチェーン管理、個の能力・教育、組織体制、コミュニティ活動等の観点から OSS 利活用に係る課題が取りまとめられている。衛星システムで利用している OSS に関わる脆弱性が判明した場合、その脆弱性に迅速かつ適切に対応することは、衛星のセキュリティを維持する上で重要となる。IPA（情報処理推進機構）及び JPCERT/CC（JPCERT コーディネーションセンター）によって運営されている「情報セキュリティ早期警戒パートナーシップ」及び「JVN（Japan Vulnerability Notes)」は、これらの一連の対応を行うに当たり必要な情報をユーザーに提供している。 3.1.5 外部へのインシデント報告を合わせて参照のこと。

「共通脆弱性識別子 CVE 概説」で紹介されている共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）は、個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体の MITRE 社が採番している識別子である。脆弱性検査ツールや脆弱性対策情報提供サービスの多くが CVE を利用している。個別製品中の脆弱性に一意の識別番号「CVE-ID（CVE 識別番号)」を付与することにより、組織 A の発行する脆弱性対策情報と、組織 X の発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したりできる。

● 基本対策事項(1)(d)「衛星搭載機器の脆弱性対策」について

サイバー空間とフィジカル空間の高度な融合に伴い、フィジカル空間に点在する機器がサイバー攻撃の新たな対象となるリスクが顕在化している。事実、2016 年には固定された設定のルータやウェブカメラがマルウェア「Mirai」に感染し、感染した機器が発信源となり大規模な DDoS 攻撃が発生した。ほかにも「Bashlite」、「BrickerBot」、「Mirai」の亜種等のマルウェアが IoT 機器のセキュリティを脅かす事例は多く発生しており、IoT 機器の利用者に直接被害を与えるだけでなく、マルウェアに感染した機器を介してネットワークに接続している他の機器に対しても影響が及んでいる。そして、その影響はサイバー空間にとどまらず、フィジカル空間にまで及ぶ可能性がある。

---

[43] 宇宙航空研究開発機構：「IV&V ガイドブック（導入編）Ver2.1」（2018 年 6 月） https://stage.tksc.jaxa.jp/jedi/devel/ivv_project/guidebook/file/ivv_guidebook_1.pdf
[44] 経済産業省 商務情報政策局サイバーセキュリティ課：「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」（2021 年 4 月）
https://www.meti.go.jp/press/2021/04/20210421001/20210421001-1.pdf
[45] 独立行政法人情報処理推進機構 セキュリティセンター：「共通脆弱性識別子 CVE 概説」（2015 年 7 月） https://www.ipa.go.jp/security/vuln/CVE.html

軌道上の衛星搭載機器においても、その脆弱性を確認することが必要である。納入された機器のソースコードがブラックボックスであり、脆弱性が内在しているか確認できない場合、地上においてフライト品と同等の機器に対する脆弱性診断を実施し、その結果、衛星サービスに影響を与える致命的な脆弱性が確認された場合には、衛星通信経由でソフトウェアの更新等、適切な処置を施す必要がある。

セキュリティ脅威に繋がりうる脆弱性の有無やセキュリティ対策の妥当性を確認する方法を、機器に対するセキュリティ検証及び組込ソフトウェアのセキュリティ検証の観点から以下に解説する。

- 機器に対する脆弱性の有無やセキュリティ対策にはセキュリティ検証が有効である。参考図書として、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」（経済産業省）[46]がある。この手引書の本編及び別冊 1・別冊 2 は、機器開発プロセスにおける「検証」のフェーズに焦点を当て、検証において検証サービス事業者が実施すべき事項及び機器メーカが検証依頼のために準備すべき事項等を整理している。加えて、別冊 1 及び別冊 2 では、機器に対する脅威分析手法についても示している[47]。
- 衛星搭載機器の組込ソフトウェアのセキュリティ検証[48]の結果、搭載機器に組み込まれているプログラムに衛星サービスに影響を与える致命的な脆弱性やセキュリティホールが確認された場合、最新のセキュリティパッチ等を適用することが必要となる。脆弱性対策の参考情報として、「脆弱性対策の効果的な進め方 ツール活用編」（IPA）[49] があり、オープンソースソフトウェアの Vuls（Vulnerability Scanner）を活用した脆弱性対策の手順等を解説している。これは、Ubuntu、Debian、CentOS、Amazon Linux、RHEL といった OS を対象としており、約 370 種のソフトウェアスキャンが数分で完了（IPA 検証）する等、日々の脆弱性関連情報の収集時間を短縮できる。

衛星及びミッション機器には様々なソフトウェアがインストールされているため、機器納入時の脆弱性対策に限らず、図 3-8 に示す対策フローを参考に、運用時の脆弱性対策を行うことが必要である。脆弱性対策を適切に行うためには、衛星及びミッション機器内にインストールされているソフトウェアを正確に把握し、最低限、表 3-2 2 に示す項目を一覧で管理することが必要である。そのうえで、定常的に脆弱性情報を収集しつつ、収集した脆弱性情報に基づき適用の判断を行う必要がある。脆弱性や脅威に関する情報の収集においては、IPA の mjcheck[50]等を用いて自動で収集するほか、組織の規模やレベルに応じて、能動的な情報収集を検討することが必要である。能動的な情報収集においては、セキュリティ関係機関（JPCERT/CC、IPA、NISC 等）より最新の情報を収集するほか、関連するセキュリティコミュニテ

---

[46] 経済産業省 商務情報政策局サイバーセキュリティ課：「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」（2021 年 4 月）
https://www.meti.go.jp/press/2021/04/20210419003/20210419003-1.pdf

[47] 引用：46 に同じ

[48] 独立行政法人情報処理推進機構：「脆弱性対策の効果的な進め方 ツール活用編」https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html（2021/09/22 参照）

[49] 独立行政法人情報処理推進機構 セキュリティセンター：「脆弱性対策の効果的な進め方 ツール活用編～脆弱性検知ツール Vuls を利用した脆弱性対策～」
https://www.ipa.go.jp/files/000071584.pdf （2021/9/22 参照）

[50] 独立行政法人情報処理推進機構：「MyJVN 脆弱性対策情報フィルタリング収集ツール (mjcheck4)」https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html

ィ（勉強会、官民協議会等）や ISAC（Information Sharing and Analysis Center）[51]に参画し、情報を収集することが想定される。

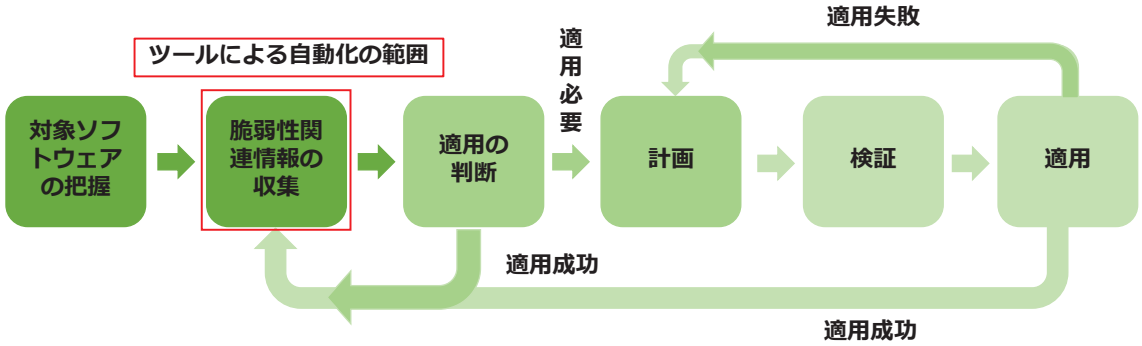

図 3-8 脆弱性対策のフロー（例）[52]

また、ソフトウェアのセキュリティを確保するための管理手法の一つとして、SBOM（Software Bill of Materials）が注目されている。経済産業省は、SBOM を導入するメリットや実際に導入するに当たって認識・実施すべきポイントがまとめた「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」[53]を 2023 年 7 月に発表した。本手引では、SBOM を導入するメリットや SBOM に関する誤解と事実など SBOM に関する基本的な情報が提供されるとともに、SBOM を実際に導入するに当たって認識・実施すべきポイントが、（1）環境構築・体制整備フェーズ、（2）SBOM 作成・共有フェーズ、（3）SBOM 運用・管理フェーズと、フェーズごとに示されている。衛星においても OSS の活用が増加しているところ、SBOM を用いて OSS の情報を管理することで、効果的な脆弱性管理を実施することができる。

[51] 宇宙分野における ISAC としては、米国の Space ISAC（2019 年 4 月設立）や欧州の EU Space ISAC（2024 年初設立）が存在する。EU Space ISAC は EU 域内企業のみを対象としているが、米国 Space ISAC は米国以外の企業も参画可能であり、日本の事業者も複数参画している。https://s-isac.org/

[52] 引用：49 に同じ

[53] 経済産業省 商務情報政策局サイバーセキュリティ課：「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」（2023 年 7 月）
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

表 3-２２　対象ソフトウェアの管理項目[54]

#	項目	備考
1	ソフトウェアの名称	-
2	ソフトウェアのバージョン	-
3	ソフトウェアのインストール方法 ＝最新のバージョンのインストール方法	【Linux サーバーの場合】yum、rpm、ソースコードからコンパイル等 【Windows サーバーの場合】インストーラー、実行ファイルの配置等
4	最新バージョンの提供サイト（URL）	最新バージョンの確認に利用するため#3 のソフトウェアのインストール方法で代替できる場合は確認不要

● 基本対策事項(1)(e)「送受信データの完全性保護」について[55,56]

宇宙ミッションに対する脅威には、能動的なものと受動的なものの 2 種類がある。能動的な脅威とは、脅威の発生源が一連の事象を開始し、積極的にシステムに干渉して脆弱性を利用しようとするものである。能動的な脅威には以下が含まれ、これらによって、衛星、地上システム及び通信システムに対して攻撃されることがある。

- 通信システムを妨害（サービス不能、可用性とデータの完全性の喪失をもたらす妨害）
- アクセス制御されているシステムに無許可のアクセスを試行
- 記録された正規の通信トラフィックを後から再生して、不正データを送信
- アクセス権を得るために、許可されたエンティティへのなりすまし
- ソフトウェアの脆弱性を利用
- データの不正な変更又は破損
- ウイルス、ワーム、分散型サービス拒否（DDoS）エージェント、キーロガー、ルートキット、トロイの木馬などの悪意のあるソフトウェア

一方、受動的な脅威には、脅威源がターゲット・システムを積極的に妨害するのではなく、既に存在し使用しているシステムの悪用等、以下の脅威が考えられる。

- 通信リンク（ワイヤーライン、RF、ネットワーク）の盗聴による機密性の損失

---

[54] 引用：49 に同じ
[55] CCSDS：「SPACE DATA LINK SECURITY PROTOCOL (RECOMMENDED STANDARD), CCSDS 355.0-B-2」（2022 年 7 月）
https://public.ccsds.org/Pubs/355x0b2.pdf
[56] CCSDS：「SECURITY THREATS AGAINST SPACE MISSIONS（INFORMATIONAL REPORT）,CCSDS 350.1-G-3」（2022 年 2 月）
https://public.ccsds.org/Pubs/350x1g3.pdf

・　どのエンティティが相互に通信しているかを判断するためのトラフィック分析

こうした能動的・受動的な脅威に対して、衛星と地上間での送受信データ（テレメトリ・データ、コマンド、更新プログラム、ミッションデータ等）の完全性を確保するためには、以下のセキュリティ対策等が考えられる。

- 不正コマンドからの保護については、地球局（アンテナ設備）からアップリンクされた不正なコマンドや不正な更新プログラムが実行されないよう、識別するための認証機能を施す。
- 攻撃者等、意図しない送信元からの「なりすまし」に対して、正しい相手やコマンドであることを識別するための認証機能を施す。ただし、複雑な識別子を使用した場合であっても、それだけでは通信を傍受され再利用されるリプレイ攻撃には有効でないため、コマンドにタイムスタンプや認証されたメッセージカウンターの付加、送信した時刻を暗号化する等のいずれか又は複数の対策を施す。
- 正規の相手からの送信データが途中で改ざんされたことを検知するため、送信データに自己署名データを含める等の対策を施す。
- 打上げ後の異常対応時や緊急対応時等を除き、定義外のタイムラインではコマンドが実行されないよう、コマンドのタイムライン（予定・前後関係）を定義する等の対策を施す。

● 基本対策事項(1)(f)「サプライチェーンに対するセキュリティ対策」について

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。「情報セキュリティ 10 大脅威 2024」[57]でも、組織向けの脅威の第 2 位としてこうした「サプライチェーンの弱点を悪用した攻撃の高まり」が挙げられている。2019 年に策定された、「IoT・5G セキュリティ総合対策」[58]においても、このようなリスクの例として、ICT の製品やサービスを製造・流通する過程における不正なプログラムやファームウェアの組込み、改ざんなどを挙げているほか、委託等の契約関係がある関係者のうち、サイバーセキュリティ対策が不十分な者が踏み台とされうることについても言及している。

こうした状況を踏まえ、宇宙産業においても衛星の調達から廃棄までのライフサイクルにおけるサプライチェーンリスクについて、自社は勿論のことビジネスパートナーや委託先も含めたライフサイクルの各フェーズにおけるサイバーセキュリティリスクの所在を把握したセキュリティ対策が必要である[59]。サプライチェーン

---

[57] 独立行政法人情報処理推進機構,「情報セキュリティ（情報セキュリティ 10 大脅威 2024）」（2024 年 1 月 25 日）https://www.ipa.go.jp/security/vuln/10threats2023.html
[58] 総務省,サイバーセキュリティタスクフォース「IoT・5G セキュリティ総合対策」（2019 年 8 月）https://www.soumu.go.jp/main_content/000641510.pdf
[59] 経済産業省 商務情報政策局 サイバーセキュリティ課 :「サイバーセキュリティ経営ガイドライン Ver 3.0」（2023 年 3 月）https://www.meti.go.jp/policy/netsecurity/mng_guide.html

全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けては、経済産業省と公正取引委員会より、中小企業等におけるサイバーセキュリティ対策を支援策や、取引先への対策の支援・要請に係る関係法令の適用関係が整理[60]されている。この整理においては、プライチェーン全体のセキュリティ対策強化は重要な取組であり、発注側となる事業者が、取引の相手方に対し、サイバーセキュリティ対策の実施を要請すること自体がただちに独占禁止法上問題となるものではないと整理している。ただし、要請の方法や内容によっては、独占禁止法上の優越的地位の濫用として問題となることもあるとし、そのようなケースが例示されている。

サプライチェーンにおけるサイバーリスクに関するガイドラインには３.１.１で紹介した「サイバーセキュリティ経営ガイドライン v3.0」があり、経営者が認識すべき３原則の一つに「サプライチェーンセキュリティ対策の推進」、サイバーセキュリティ経営の重要 10 項目に「ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策」が盛り込まれている。また、本ガイドラインの添付資料３「セキュリティ管理規程の雛形」における「9-1　委託先情報セキュリティ対策状況確認リスト」は、委託先の情報セキュリティ対策の実施状況を確認する際に活用できる。

衛星のサプライチェーンセキュリティ対策に関して、図 3-9に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。まず、調達フェーズにおいて、構成品（ハードウェア部品及びソフトウェア部品）を調達する場合、以下のセキュリティ対策等が考えられる。

- 構成品のセキュリティに関する脆弱性情報や修正プログラムの提供が、調達元との保守範囲に含まれていることを確認する。
- 構成品においてセキュリティ脅威が発生した場合に、調達元において対応可能な体制ができていることや、依頼時に即応が可能な契約形態であることを確認する。
- 構成品の SBOM 等を確認し、構成品の情報を確認する。
- 調達した構成品に対するセキュリティ検証を実施する。

衛星の製造フェーズにおいては、以下のセキュリティ対策等が考えられる。開発・製造システムに対する対策は３.２.５も参照のこと。

- 開発・製造に関する組織内のセキュリティ管理体制を構築する。
- 開発・製造システムに対するセキュリティ管理を講じる。これには、人的セキュリティ対策（人員に対するセキュリティ要求の明確化、人員に対するセキュリティ教育の実施等）及び物理セキュリティ対策（入退室管理による物理的アクセス制御、機器に対する物理的保護対策、監視カメラの設置等）を含む。

運用・保守フェーズでの対策について、本項(a)、(b)、(e)で記載した通信の保護、ジャミング対策、送受信データの完全性保護のほか、以下のセキュリティ対策等

[60] 経済産業省、公正取引委員会：「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」（2022 年 10 月）
https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

が考えられる。

- 衛星コンポーネントにおける脅威動向・脆弱性情報を収集する。
- SBOM 等の情報を活用し、収集した脅威動向・脆弱性情報を評価・管理する
- 衛星コンポーネントにおいて脆弱性等の問題が明らかとなった場合、ソフトウェアやファームウェアのアップデートによって問題に対応する。
- イベントを検知し、ログに記録する。また、継続的にログをレビューすることで、疑わしいイベントを調査する。

そして、廃棄フェーズに関して、運用が完了した衛星については、IADC（国際機関間スペースデブリ調整委員会）の「スペースデブリ低減ガイドライン」、COPUOS（国連宇宙空間平和利用委員会）の「スペースデブリ低減ガイドライン」及び「宇宙活動に関する長期持続可能性（LTS）ガイドライン」、ISO 24113「Space systems — Space debris mitigation requirements」等の要求事項を参照し、適切に対処する必要がある。また、地上局システムの廃棄については、以下のセキュリティ対策等が考えられる。

- 衛星運用システムや衛星通信システム等の地上局システムの廃棄において、廃棄の手順や基準を定め、システムや機器の内部に保存されているデータを消去（サニタイズ）するなど、データの再利用を防止する。

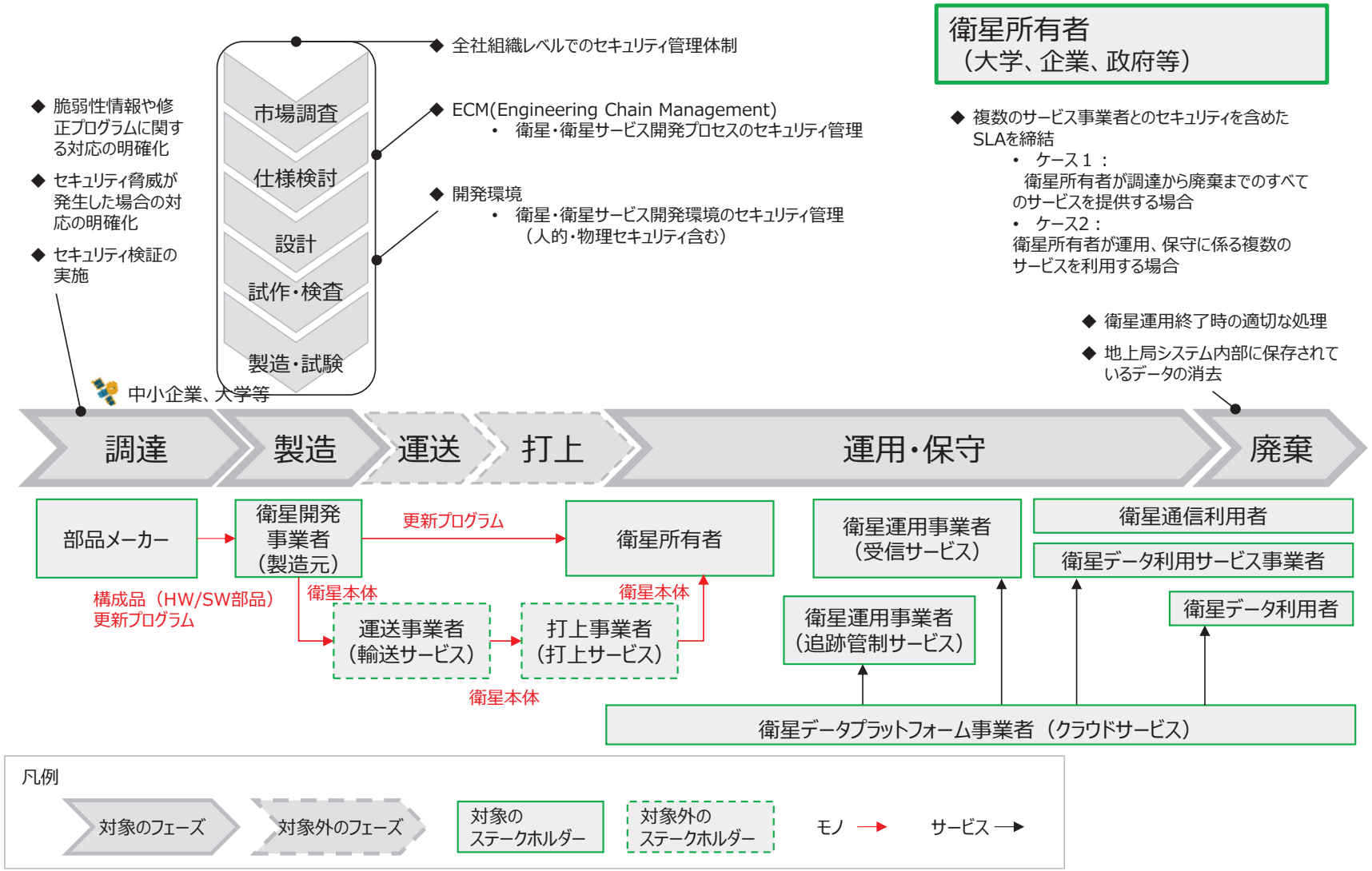

図　3－9　衛星のライフサイクルと調達時のサプライヤーに対するセキュリティ要件マッピング

（備考）本ガイドラインでは衛星の運送・打上フェーズは検討対象の範囲外であるが、衛星輸送中に衛星本体や衛星搭載機器等への改ざん等の攻撃が予想される場合は、改ざん等の攻撃を検知するための耐タンパー性技術等の採用が推奨される。

コラム：SPARTA（Space Attack Research and Tactic Analysis）について

米国 Aerospace Corporation は、MITRE ATT&CK ベースの宇宙システム向け攻撃フレームワークである SPARTA（Space Attack Research and Tactic Analysis）[61]を 2022 年 10 月に公開した。STARTA は、宇宙システムに関するシステムの開発者及び管理者を継続的に教育し、宇宙領域で直面する独自のサイバー脅威に対抗できるようにするために作成され、特に宇宙機を対象としたサイバー脅威に焦点を当てており、宇宙機に対するサイバーキルチェーンを攻撃者の視点から詳細に分析し、サイバー攻撃者の戦術・技術・手順を体系的に整理している。

SPARTA では、表 3-２３に示す 10 の攻撃戦術が設定されており、各戦術に関する複数の攻撃技術（表 3-２４）が整理されている。代表的な攻撃技術として、RF 通信の盗聴、ジャミング、リプレイ攻撃、サプライチェーン攻撃等の本ガイドラインで記載の攻撃技術のほか、対衛星兵器（ASAT）による攻撃技術や電磁パルスの攻撃技術等、高度な攻撃技術も整理されている。また、NIST SP 800-53 や ISO/IEC 27001 をベースに各攻撃技術に対する対策も整理されており、宇宙システムの対策を検討するうえでも参考となる。

表 3-２３　SPARTA における戦術

戦術（Tactics）	説明
偵察（Reconnaissance）	攻撃者が攻撃を行うための足掛かりを得るための技術で構成される。宇宙機の設計の情報・構成するシステム情報・ミッション等の攻撃する対象を選定するために必要な情報を事前に収集する。
攻撃態勢の確立（Resource Development）	攻撃者が、攻撃対象を実際に攻撃するために必要なリソースを作成、購入、窃取する技術で構成される。この戦術では、攻撃する際に必要なインフラの購入やレンタル、ボットネットの作成、侵入技術のアップデートを行うことができる。
初期アクセス（Initial Access）	ネットワーク内に最初の足場を築くために、様々な侵入ベクトルを使用する技術で構成される。主要な通信経路や、ペイロード、地上システムなどの侵害による攻撃経路の確保や、宇宙機のセーフモード時に悪意のあるコマンドを送信し、宇宙機の保護機能を無効にすることができる。
実行（Execution）	攻撃者によって、ローカル又はリモートのシステム、デバイス、その他の資産に対して悪意あるコードが実行される。
永続化（Persistence）	攻撃を半永久的に実施可能とすることを目的とした戦術である。永続化のために、バックドアの挿入、正規のコードの置き換え、乗っ取り、起動コードの追加等、システムへの足場を維持するためのあらゆるアクセス、行動、設定の変更が検討される。
防御回避（Defense Evasion）	攻撃者が被攻撃者に検知されるのを避けようとする技術で構成される。セキュリティソフトウェアのアンインストール・無効化、データやスクリプトの難読化・暗号化などを通じて、攻撃者は、通常では許可されないコマンドを処理させることを可能にする。

[61] Aerospace Corporation：SPARTA: Space Attack Research and Tactic Analysis（2022 年 10 月） https://aerospace.org/sparta

ラテラルムーブメント（Lateral Movement）	攻撃者が、環境内の様々なポイントに攻撃を拡大させる戦術である。
データ流出（Exfiltration）	攻撃者が、ネットワークからデータを盗むために使用する可能性のある技術で構成される。リプレイ攻撃やサイドチャネル攻撃といった技術で、被攻撃者の所有する機密情報をはじめとするデータを流出される。
影響（Impact）	一連の戦術の結果として与えられる攻撃の影響を示す。攻撃によって、被攻撃者のシステムやデータ操作・破壊によるシステムのサービス停止やシステムへのアクセス制限、プロセスやデータの完全性や可用性の破壊が行われる。

表 3-24 SPARTA における技術

偵察	攻撃態勢の確立	初期アクセス	実行	永続化	防御回避	ラテラルムーブメント	データ流出	影響
宇宙機の設計情報の収集	インフラストラクチャーの準備	サプライチェーン攻撃	リプレイ攻撃	メモリ侵害	障害管理メカニズムの無効化	ホストされたペイロード	リプレイ攻撃	詐欺（誤指示）
宇宙機情報の収集	インフラストラクチャーへの攻撃	ソフトウェア無線への攻撃	PNTジオフェンシングへの攻撃	バックドア	ダウンリンクの無効化	パスの分離不足の悪用	サイドチャネル攻撃	妨害
宇宙機の通信情報の収集	サイバー能力の獲得	攻撃された近隣の宇宙機を介したクロスリンク	認証プロセスの変更	地上システムの妨害	オンボード値の変更	クロスリンク経由のコンステレーションホッピング	盗聴	アクセス拒否
宇宙機の打上げ情報の収集	非サイバー能力の獲得	セカンダリー/バックアップ通信路への攻撃	ハードウェア・ファームウェアの破損の悪用	暗号鍵の変更	マスカレード	訪問機インタフェースへの攻撃	アウトオブバンド通信リンク	劣化
盗聴	ステージ能力	ランデブー及び近傍運用	暗号化無効化	有効なクレデンシャル情報	セーフモード時の保護機能低下を悪用した攻撃	仮想環境への攻撃	近傍運用	破壊
ソフトウェア開発情報の収集		ホストされたペイロードへの攻撃	シングルイベントアップセット（SEU）の発生		ホワイトリストの修正	打上げインタフェース	通信設定の変更	盗聴
セーフモード測定器の監視		地上局への攻撃	時間同期攻撃		ルートキット	有効なクレデンシャル情報	地上局への攻撃	
サプライチェーン情報の収集		不正な外部組織	コードの欠点の悪用		ブートキット		開発者・開発環境への攻撃	
ミッション情報の収集		信頼関係	悪意のあるコード		偽装、隠蔽、デコイ（CCD）		パートナー地上局への攻撃	
		セーフモード時の保護機能低下を悪用した攻撃	セーフモード時の保護機能低下を悪用した攻撃		監査ログのオーバーフロー		ペイロード通信チャネル	
		補助機器・装置への攻撃	オンボード値の変更		有効なクレデンシャル情報			
		組み立て、テスト、打上げオペレーションに対する攻撃	フラッディング					
			ジャミング					
			スプーフィング					
			なりすまし					
			サイドチャネル攻撃					
			運動物理的攻撃					
			非運動物理的攻撃					

３．２．３ 衛星運用システム

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

要求事項

衛星運用システム（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。

【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

（解説）

● 基本対策事項(1)(a)「システムの保護」について

衛星のミッションコントロール等を実施する施設に対して、敵対的な組織（テロリスト、犯罪者、外国の諜報機関、破壊活動家、政治活動家、コンピューター・ハッカー、商業的な競争相手等）や悪意あるインサイダー（不満のあるスタッフ、不誠実な保守要員、不誠実なシステム担当者、SNS 等で外部脅威者から影響を受けた内部協力者等）による物理的な攻撃を受けた場合、あるいは技術的にシステムを攻撃することなく、衛星を制御するための施設を制圧された場合、施設を喪失するだけでなく、ミッションの運用や提供するサービスに直接影響を与える可能性がある。

地上システム（特に、衛星のミッションコントロールを実施する施設）の喪失は、データの喪失やタイムリーなデータへのアクセスの喪失だけでなく、ミッション全体の喪失につながる可能性がある。こうした地上施設への物理的攻撃に対しては、以下の対策等がある。[62]

- 警備員の配備
- ゲートの設置
- 施設へのアクセスコントロール（取り扱う情報及び取り扱うエリアの制限）
- 攻撃を受けた場合に備えたバックアップサイトの設置

外部からの不審者や権限のない職員等の侵入に対する備えとして、以下のいずれか、又は複数の対策がある。

- 衛星運用システムのうち、追跡管制・受信を行うシステム又はエリアへの立入りを制限
- 衛星運用システムのうち、ネットワーク運用・ミッションコントロール等の衛星運用業務を行うシステム又はエリアへの立入りを制限
- 衛星運用システムが不正利用されることを防ぐため、施錠、入退室記録又は入室検知といった対策
- 衛星運用システムがほかのシステムの一部に所在する場合には、当該システムの管理者との連絡手段と体制を確認・整備する対策
- 国内外の地上局（追跡管制局及び受信局）ネットワークの運用情報の漏えい・改ざんを防止するため、ネットワーク運用業務を取り扱うエリア及び情報システムを制限
- 国内外の地上局との通信経路・通信情報、格納データの暗号化機能を実装する対策

さらに、環境要因（火災・停電・その他自然災害等）による被害の予防対策（緊急時の衛星運用対応が必要な場合に備えた計画を策定）等がある。

● 基本対策事項(1)(b)「通信の保護」について

３.２.２基本対策事項(1)(a)「通信の保護」において解説したように、衛星の追跡管制・ミッションデータ等の受信・記録に際しては、改ざん・盗聴防止の観点から衛星とのRF通信の暗号化及び暗号化に用いる鍵の暗号化等が行われている。また、衛星の追跡管制を行い、指令を送るミッションコントロールシステムにおいては、暗号化に加えてシステムを利用できる従業員を限定する等の対策がある。加えて、拠点間通信では、改ざん・盗聴防止の観点から、専用回線又は暗号化されたネットワーク利用等の対策が実施されている。

衛星運用システムの「通信の保護」については、以下に示すように衛星と地上局間の「通信の保護」及び衛星運用システムの「拠点間通信の保護」がある。衛星と地上局間の「通信の保護」については、３.２.２基本対策事項(1)(a)「通信の保護」についての解説を参照すること。

---

[62] CCSDS：「SECURITY THREATS AGAINST SPACE MISSIONS（INFORMATIONAL REPORT）CCSDS 350.1-G-3」（2022年2月） https://public.ccsds.org/Pubs/350x1g3.pdf

衛星運用システムの「拠点間通信の保護」においては、以下の対策等がある。

- 改ざん・盗聴防止の観点から、専用回線又は暗号化されたネットワーク（相互認証による VPN（Virtual Private Network）・TLS（Transport Layer Security））等を利用する
- 拠点間通信で不必要・想定外の通信が生じないよう設計する
- ネットワークを分割し、ファイアウォールによって通信を制御する
- 後述の基本対策事項(1)(g)に記載する外部サービス等を利用する場合は、信頼のおけるゾーンとそうではないゾーンの境界を明らかにし、必要最低限の通信のみを外部と接続できる状態にする

また、衛星の追跡管制を行い、指令を送るミッションコントロールシステムにおいては、以下の対策等がある。

- 利用できる従業員を限定するため、ログイン等の認証機構、IP アドレス制限等によりシステムへの接続を制限する
- 操作の記録を保管する
- 関連するシステム、システムとの通信経路・通信情報及び格納データに対する暗号化機能を実装する

● 基本対策事項(1)(c)「ジャミング対策」について

衛星と地上局（追跡管制・受信）との間の RF 通信では、ジャミング、あるいは干渉といった通信妨害を受ける可能性があるため、３.２.２基本対策事項(1)(b)「ジャミング対策」を参照のこと。

● 基本対策事項(1)(d)「データの保護」について

衛星運用及び地上局運用に関る重要なデータが破壊、改ざん又は漏えいした場合、衛星運用に不具合を生じる可能性がある。また、後述の衛星データ利用システムや提供するサービスに影響を与える可能性がある。

衛星運用システム及び受信局の利用記録やハウスキーピングデータ、ミッションデータ、ミッションコントロールシステムのログ等を保護する上で、アクセスを限定すべき情報及び対策の観点から以下に解説する。

- ダウンリンクによって取得される衛星のハウスキーピングデータ、衛星のミッションデータといった情報は、アクセスが限定されるストレージに保管する対策が考えられる。また、衛星運用システムの利用記録、無線局の利用記録、ミッションコントロールシステムのログイン履歴・コマンド送信履歴等、衛星運用に関連する記録は、インシデント対応の観点から保管し、保護する対策がある。
- 必要に応じて、ストレージの暗号化又はファイルの暗号化によるデータの保護を行う対策や分散防護又は秘密クラウド等の保護ソリューションも考えられ

る。

● 基本対策事項(1)(e)「システムの検証とシステムの脆弱性対策」について

衛星運用システム内のシステムに意図しない機能が実装されていた場合、ミッションの遂行が困難となるばかりか衛星を失う可能性がある。

衛星制御に悪影響を及ぼす可能性がある意図しない機能及び情報の漏えい・改ざん等につながる脆弱性やセキュリティホールが確認された場合、最新のセキュリティパッチ等を適用し、衛星運用システム内のシステムの脆弱性を解消する等の対策を実施する必要がある。そのための対策についての参照先は以下のとおりである。

- システムに意図しない機能が実装されていないことを確認する対策については、３.２.２基本対策事項(1)(c)「衛星実装機能の事前検証」を参照のこと。
- 参考図書等については３.２.２基本対事項(1)(d)「衛星搭載機器の脆弱性対策」を参照のこと。

● 基本対策事項(1)(f)「送受信データの完全性の確保」について

衛星運用システム内システムで送受信される情報が漏えいした場合、悪意のある攻撃者に悪用されミッションの遂行が困難になる可能性がある。また、衛星運用システム内システムでミッションデータが改ざんされた場合、後述の衛星データ利用システムの運用に悪影響を与える可能性がある。

送受信データ（テレメトリ・データ、コマンド、更新プログラム等）の完全性の確保や、受信データ（ミッションデータ等）及びネットワークを介した外部記録装置に送信されるミッションデータ等の完全性を確保する対策として、地球局（アンテナ設備）からの不正なコマンド送信や不正な更新プログラムのアップリンクの防止及び受信データ（ミッションデータ等）の漏えい・改ざんの防止等の観点から以下に解説する。

地球局から不正なコマンド送信や不正な更新プログラムのアップリンク防止については、以下の対策等がある。

- 緊急時対応を除き定義外のタイムラインではコマンドが実行されないよう、コマンドのタイムライン（予定・前後関係）の定義、衛星運用システム内のシステムに衛星制御に悪影響を及ぼすような意図しない機能が実装されていないことを確認する等の対策（３.２.２基本対策事項(1)(c)を参照のこと。）
- コマンド送信前にコマンド計画の再評価やチェックツール（シミュレーター等）による確認の実施等の対策
- 過去の教訓事項等を踏まえた誤操作の起きにくいHMI（ヒューマンマシンインターフェース）に対応する等の対策
- 重要操作実行の際は特別な承認フロー（ワークフロー申請、複数承認者、書面を用いた指示等）による承認を必要とする等の対策
- 重要コマンドや更新プログラム等の送信の際の管制操作は２名以上で実施する等の対策

受信データ（ミッションデータ等）の漏えい・改ざん防止については、以下の対策等がある。

- ミッションデータの漏えい・改ざんを防止するため、外部記録装置への送信は専用回線、暗号化されたネットワークを利用する等の対策

・ 受信局設備内に記録されるミッションデータ等の漏えい・改ざんを防止するため、ミッションデータ等を取り扱う情報システムの利用状況（ログイン実績、アクセスログ等）の保管及び定期的な監視、ミッションデータ等へのアクセス状況（操作内容も含む）の監視等を実施する対策

備考：改ざん等への対策の基本は自己署名である。送信データに自己署名データを含める対策等については、３.２.２基本対策事項(1)(e)を参照のこと。

● 基本対策事項(1)(g)「外部サービスの利用」について

３.２.２ 基本対策事項(1)(f)「サプライチェーンに対するセキュリティ対策」で解説したように外部サービス組織を狙ったサイバーセキュリティ事故が報告されている。外部サービスを利用する場合は、サービス提供者が前述の基本対策事項(1)(a)～(f)に相当するセキュリティ対策等を実施しているかの状況を確認する等の対策が必要である。

外部サービスの利用としては、以下に示すように衛星運用システムサービス、パブリッククラウド及び地上局サービスの利用が想定される。

- 衛星運用システムサービスの利用

  衛星運用システムの全部又は一部について、これらを運用するサービスを利用する場合については、当該サービスを提供する事業者とのサービスに係る契約において、「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 第 7 条第 2 項」で定める安全管理措置に相当する措置及び「外国為替及び外国貿易法 25 条」に関連して、衛星運用情報に係る情報を特定国等に所在する電子計算機に保存しないことに関する合意内容を契約相手方との SLA（Service Level Agreement）に含む等の対策がある。参考情報等については、３.２.１法令上求められる対策を参照のこと。

- パブリッククラウドの利用

  衛星運用システムのうち、データの全部又は一部の保存、若しくはソフトウェアシステムの全部又は一部の構築又は運用のためにパブリッククラウド等の外部サービスを利用する場合には、基本対策事項(a)～(f)で解説しているセキュリティ対策等の契約相手方における実施状況、若しくは FedRAMP Moderate レベル又は ISMAP レベル 2 相当の認証状況を確認する等の対策がある。

  - パブリッククラウド利用者側の対策の確認手段としては、SLA 等の契約締結のほか、パブリッククラウド等が提出する SOC レポート等の IT コンプライアンスレポートの参照等の対策がある。
  - ミッションデータの保護に際しては、必要に応じ、パブリッククラウドのストレージの暗号化だけでなく、ファイルの暗号化等の追加の対策を自ら行う等の対策がある。

- 地上局サービスの利用

  衛星運用システムのうち、衛星の追跡管制又はミッションデータ等の受信・記録を行う無線局の全部又は一部について、外部の地上局サービスを利用する場合には、基本対策事項(a)～(f)で解説しているセキュリティ対策等の契約相手方における実施状況を確認する等の対策がある。

- 追加の対策として、RF 通信のための暗号鍵、VPN 等暗号化ネットワークの認証情報といった秘密情報は、これらの地上局サービス内で安全に利用できる保護措置として自ら行うことが考えられる。
- サービス利用に当たり、サーバー、ネットワーク機器、変復調装置等、自らの機器を持ち込む場合には、事前にフロントパネルの施錠、不要ポートの閉鎖、ストレージの暗号化を施してから持ち込む等の対策がある。

● 基本対策事項(1)(h)「セキュアコーディング」について

衛星や地上システム設備等においてはシステムメンテナンスやソフトウェアアップデート時にWEBアプリケーションが多用されており、外部からのリモートアクセスが可能であるため、適切なセキュリティ対策を講じることが求められる。WEB アプリケーションを含む民間宇宙システムの開発に当たってはセキュリティを考慮したセキュアコーディングに配慮し、保証要件に対してはどこまで対応するかを契約時に明確にする等の対策が必要とされる。参考図書として、「情報セキュリティ IPA セキュア・プログラミング講座[63]」、「情報システム開発契約のセキュリティ仕様作成のためのガイドライン[64]」等がある。

● 基本対策事項(1)(i)「サプライチェーンに対するセキュリティ対策」について

衛星運用システムの調達から廃棄までのライフサイクルにおいてサプライチェーンの弱点を悪用した攻撃を受ける可能性があるため、３.２.２基本対策事項(1)(f)「サプライチェーンに対するセキュリティ対策」を参照し、サプライチェーンに対するセキュリティ対策を講じる必要がある。

---

[63] 独立行政法人情報処理推進機構 セキュリティセンター：「情報セキュリティ　IPA セキュア・プログラミング講座」（2017 年 9 月）
https://www.ipa.go.jp/security/awareness/vendor/programming/
[64] 一般社団法人ソフトウェア協会 Software-ISAC：「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」（2020 年 11 月）
https://www.softwareisac.jp/ipa/index.php

３．２．４ 衛星通信システム・衛星データ利用システム

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

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。

【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) システムの保護

(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

（解説）

衛星通信システム・衛星データ利用システムの機密性・完全性・可用性を確保するための参考図書には、品質管理として ISO 9001、ISO/IEC 27001、データ保護として NIST Cybersecurity Framework のサブカテゴリーのデータセキュリティ等がある。なお、衛星通信システム・衛星データ利用システムにおいては、システムの開発・運用において異なるステークホルダーが関与することも想定される。対象とするシステムに応じて、関係するステークホルダーに求めるセキュリティの役割を明確化するとともに、各ステークホルダー間の責任分界点を明確化することが必要である。

● 基本対策事項(1)(a)「システムの保護」について

宇宙システム特有の対策はないが、衛星通信システム・衛星データ利用システムにおける機密性・完全性・可用性を確保するための３．２．３基本対策事項(1)(a)「設備の保護」を参照のこと。

● 基本対策事項(1)(b)「データの保護」について

宇宙システム特有の対策はないが、衛星通信システム・衛星データ利用システムにおける機密性・完全性を確保するための３.２.３基本対策事項(1)(d)「データの保護」を参照のこと。

● 基本対策事項(1)(c)「システムの検証とシステムの脆弱性対策」について

宇宙システム特有の対策はないが、衛星通信システム・衛星データ利用システムにおける機密性・完全性・可用性を確保するための３.２.３基本対策事項(1)(e)「システムの検証とシステムの脆弱性対策」を参照のこと。なお、最新のセキュリティパッチ等の適用に当たってユーザーの対応を求める場合には、システムの開発事業者は、当該対応に関する実行方法をユーザーに適切に周知し、ユーザーにおいて適時にパッチの適用が実行されるようにすること。

● 基本対策事項(1)(d)「受信データの完全性の確保」について

宇宙システム特有の対策はないが、衛星通信システム・衛星データ利用システムにおける機密性・完全性・可用性を確保するための３.２.２基本対策事項(1)(e)「送受信データの完全性」及び３.２.３基本対策事項(1)(f)「送受信データの完全性確保」を参照のこと。

● 基本対策事項(1)(e)「外部サービスの利用」について

衛星通信システム・衛星データ利用システムの開発・運用に当たっては、３.２.３基本対策事項(1)(g)「外部サービスの利用」を参照のこと。

● 基本対策事項(1)(f)「セキュアコーディング」について

衛星通信システム・衛星データ利用システムの開発・運用に当たっては、３.２.３基本対策事項(1)(h)「セキュアコーディング」を参照のこと。

● 基本対策事項(1)(g)「サプライチェーンに対するセキュリティ対策」について

衛星通信システム・衛星データ利用システムのサプライチェーンに対するセキュリティ対策に当たっては、３.２.２基本対策事項(1)(f)「サプライチェーンに対するセキュリティ対策」を参照のこと。

３．２．５ 開発・製造システム

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

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）

（解説）

● 基本対策事項(1)(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）」について

① 対象

工場における産業制御システム

② 概要

「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」[65]では、工場に対する対策を自ら企画・実行するに当たって参照すべき考え方やステップを「手引き」として示し、また、必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策を明記している。具体的には、「情報収集・整理」、「セキュリティ対策の立案」及び「セキュリティ対策の実行・管理体制の構築」の 3 つのステップに基づく、セキュリティ対策の企画・導入のステップが提示されている。なお、工場の規模や機器・システムは千差万別であり、業界・業種ごとに実施すべき事項は異なるため、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である旨も併せて記載されている。また、関連する参考図書として、IPA が提供する「重大な経営課題となる制御システムのセキュリティリスク 第 3 版」[66]、JPCERT/CC が提供する「制御システムセキュリティ自己評価ツール（J-CLICS）」[67]等がある。

---

[65]経済産業省：「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」（2022 年 11 月）
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf

[66] 独立行政法人情報処理推進機構：「重大な経営課題となる制御システムのセキュリティリスク 第 3 版」（2017 年 3 月）
https://www.ipa.go.jp/files/000058489.pdf

[67] 一般社団法人 JPCERT コーディネーションセンター：「制御システムセキュリティ自己評価ツール（J-CLICS）」（2017 年 4 月）
https://www.jpcert.or.jp/ics/jclics.html

コラム：工場一般の製造環境の設備について　　（宇宙産業 SWG 委員　フォーティネットジャパン合同会社 OT ビジネス開発部　佐々木 弘志）

工場一般の製造環境の設備は、その生産に係る役割に応じて概ね３階層に分類される（図 3-１０）。

- 制御情報ネットワーク
  工場の生産管理や状態監視を行うサーバーがある。
- 制御ネットワーク
  PLC（Programmable Logic Controller）、DCS（Distributed Control System）等の制御機器がある。
- フィールドネットワーク
  制御機器によって制御されるモータ、センサ等のフィールド機器がある。

これらの工場設備は、DMZ（Demilitarized Zone）と呼ばれるネットワーク分離のための層を介して、工場建屋内の事務室とつながっていることが多い。ただし、DMZ が存在しない場合もある。また、工場設備内のシステムは一般に次のような特徴がある。

- メーカのサポートが終了した OS を搭載したパソコンがあることが多い。
- 通信に用いられるプロトコルが情報システムとは異なる。制御機器ベンダー固有の制御専用プロトコルも多く、通常の情報システムのネットワークセキュリティ製品の効果が低い。
- 情報システム部門ではなく、生産技術部門の管理下にあり、セキュリティ専任組織や担当者がいないことが多い。

したがって、工場設備のセキュリティ対策は、情報システムに比べると遅れており、十分にリスクが低減されていないことが多い。

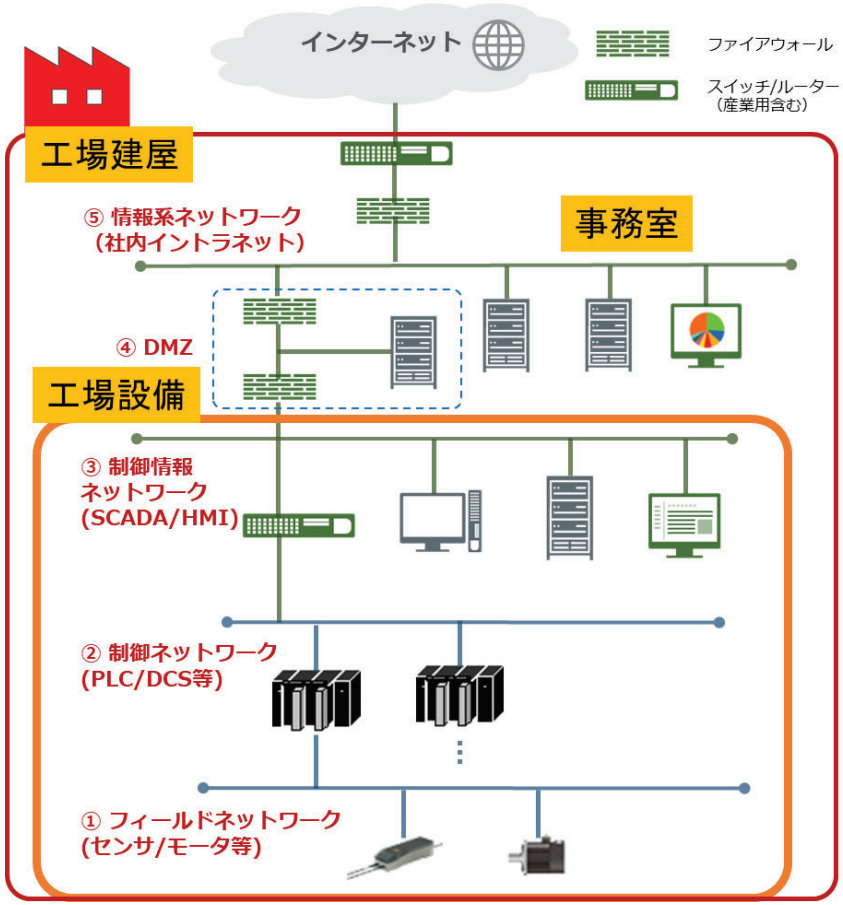

図　3-１０　工場一般の製造設備のネットワーク図例

一方で、DX の進展に伴い、生産の効率化やリモートメンテナンス等の目的で、IT 技術の導入や、外部との接続が増えることでセキュリティリスクが増加している。実際、情報システムを狙ったランサムウェアが工場設備のシステムにまで感染が広がり、生産稼働が停止する等のセキュリティ事故が発生している。

また、海外を中心に、サプライチェーンリスク低減のため、サプライヤーとその調達物のセキュリティ要件を規定する規制やガイドラインが策定されており、工場設備もその対象に含まれている。

このようなビジネス環境の変化により、工場設備へのセキュリティ対策の重要性が高まっており、国内でも多くの製造事業者が、工場設備のセキュリティ対策に

取り組み始めている。

工場設備のセキュリティ対策は、大きく以下の３つに分類される。

- 組織体制の構築
  工場セキュリティ対策の責任組織の構築、情報システム部門との連携、工場セキュリティに関する人材育成、現場担当者の教育等
- 運用手順の策定
  工場設備のサイバー資産管理、工場設備のリスク分析実施、セキュリティポリシーの策定、サイバーセキュリティ要因の BCP 及び事故対応手順書の策定等
- 技術的な対策の導入
  情報システムとのネットワーク境界防護、工場設備ネットワークの監視、端末へのウイルス対策導入等

工場設備では、可用性を理由として、サポート切れや、セキュリティパッチが適用できないような端末を運用する必要があり、技術的な対策の導入が困難なことがあるため、組織体制、運用手順の対策と合わせて、リスクを低減することが肝要である。そのため、自組織の工場設備のリスクを把握した上での、総合的なセキュリティ対策の実施が求められるが、それを推進する人材が不足しているのが実情である。

独立行政法人情報処理推進機構（IPA）の「産業サイバーセキュリティセンター（ICSCoE）」では、制御システムに係るセキュリティ人材を育成するため、「中核人材育成プログラム」、「責任者向けプログラム」、「実務者向けプログラム」、「管理監督者層向けプログラム」等を提供しているため、参考にされたい。

URL：https://www.ipa.go.jp/icscoe/

コラム：開発環境のセキュリティについて　（宇宙産業 SWG 委員　技術研究組合制御システムセキュリティセンター研究開発部　吉松 健三）

製品やシステムの開発プロセスで構築した開発環境は、不具合対応等のため、再構築が必要な場面がある。

開発環境の再構築に当たっては以下の点に留意が必要。

- 開発環境の再構築の可能性が生じる期間は、製品やシステムの耐用年数を超える長い年数にわたる。
- 開発環境のわずかな違いでセキュリティ状態が大きく影響を受けてしまう可能性がある。

これらの点を考慮に入れつつ、開発環境について留意すべき３つの項目を以下に紹介する。

- コンパイラ
  同じソースであってもコンパイラが違う[68]と、生成されるバイナリコードが異なる場合がある。セキュリティ製品やシステムでは、バイナリコードがわずかでも異なると製品のセキュリティ状態への影響の可能性が高くなる。製品の不具合を修正する場合、開発時に利用したコンパイラと同じものを使うことで、デグレードの可能性を減らすことができる。
- 第三者が提供するツール
  固有のハードウェアに固有のソフトウェアをインストールした第三者のツールでは、ソフトウェアのアップグレードは可能だが、ダウングレードができない場合がある。例えば、ファジングなどのアクティブな自動検査ツールは、様々な開発や検査で使いまわされる過程でソフトウェアのバージョンが変わってしまうことがあり、その結果、開発環境の再構築をしようとしたときに、開発時点でのバージョンのソフトウェアがインストールできないという問題が生じる場合がある。
  第三者が提供するツールを利用する場合、開発環境の再構築時にソフトウェアのダウングレードを必要とする可能性の有無、及びダウングレードが必要な場合に利用するツールのダウングレードが可能であるか、注意して確認する必要がある。
- 独自のツール
  開発環境として独自のツールを開発して利用する場合、そのツールの設計資料は構成管理され、ツールそのものも保管されている必要がある。しかし、開発終了後、長い年月を経た後に開発環境の再構築の必要性が生じた場合、独自のツールがうまく動作しなかったり、ツールそのものが見当たらなかったりする場合がある。この場合、ツールの設計資料により再度ツールを作成することになるが、当時の部品が手に入らない場合がある。互換性が保証された部品が手に入らない場合、新たなツールの設計が必要になる。このような状況の発生を考慮し、独自のツールを開発する場合には、製品の設計と同様に、ツールが満たすべき要求仕様を記載した文書を構成資料として管理することが望ましい。

[68] バージョンが異なるコンパイラも含む

4．付録

4．1 用語の定義

用語	本ガイドラインにおける定義
C&C サーバー	外部から侵入して乗っ取ったコンピューターを利用したサイバー攻撃において、踏み台のコンピューターを制御したり命令を出したりする役割を担うサーバーコンピューターのことをいう。
DDoS	インターネット上の多数の機器から特定のネットワークやコンピューターに一斉に過剰な負荷をかけ、機能不全に追い込む攻撃手法をいう。
SQL インジェクション攻撃	インターネットの Web サイトなどの入力画面に対して、直接 SQL 命令文の文字列を入力することで、データベースに不正アクセスを行い、情報の入手や、データベースの破壊、Web ページの改ざんなどを行う攻撃をいう。
衛星運用システム	追跡管制局、受信局等の衛星運用を行う設備及びミッションコントロールシステム等の総称をいう。
衛星運用事業者	地上局（追跡管制局、受信局）を整備又は地上局サービス事業者を利用して軌道上の衛星の運用を行う事業者をいう。衛星所有者が兼ねる場合もある。
衛星開発事業者	衛星システムの企画・開発・製造を行う事業者をいう。衛星所有者が兼ねる場合もある。
衛星システム	科学衛星等の探査機、国際宇宙ステーションへ物資や宇宙飛行士を送る補給機及び測位、通信・放送、気象観測、地球観測を行う人工衛星等の総称をいう。
衛星所有者	衛星を調達し、衛星本体に責任を持つ者をいう。衛星所有者が衛星開発製造、衛星運用、衛星データ利用、廃棄まで全てを実施する場合や衛星運用等を衛星運用事業者等に委託する場合がある。
衛星通信利用者	事業あるいは研究の目的を達成するために観測衛星データを活用する企業ユーザー、個人ユーザー等をいう。
衛星データ利用サービス事業者	ミッションデータ処理システム、保存・検索システム、観測受付・データ配布処理システム等を整備し、衛星データ利用者が観測衛星データの利用を容易にするためのサービスを提供する事業者をいう。
衛星データ利用システム	観測衛星データの保存や処理、観測受付、データの配布等を行う設備の総称をいう。
衛星データ利用者	衛星通信あるいは衛星放送を活用する企業ユーザー、個人ユーザー等をいう。
衛星データプラットフォーム事業者	観測衛星データの保存・解析機能等を提供する企業で、データの横断的な連携や解析を可能にする事業者をいう。クラウドの形態でサービスを提供する事業者を含む。
衛星本体	衛星システムのうち、測位、通信・放送、気象観測、地球観測を行う個々の衛星をいう。
開発・製造システム	衛星開発及び地上システム開発のための施設、設備、システム等の総称で、OT システム（FA システム）、IT システム（OA システム等）、検査設備等を含む。
キーロガー	利用者の意図に関わらず、利用者のキーボードでの操作を記録するソフトウェアをいう。

用語	本ガイドラインにおける定義
脅威インテリジェンス	脅威アクターの意図、機会、能力に関する情報を収集及び分析し、脅威の検知や防御のために利用可能な情報のことをいう。情報そのものを指すほか、情報を収集及び分析し、対策を講じるまでの一連のプロセスを指すこともある。
コマンド	衛星に対する指令のことをいう。
衛星コンステレーション	同型、異型を問わず複数の衛星が連携・協調して動作することにより共通のミッションを遂行するための衛星運用形態をいう。
ジャミング	レーダーや通信のための電波と同一の電波数・周波数帯の電波を送出し電波を混信させる等、正常な通信を妨害することをいう。
受信サービス	受信局を整備し衛星から送られてくるデータの受信等を代行するサービスをいう。
スプーフィング	自分以外のある特定の人物のふりをして、その人に成り代わって活動することをいう。
脆弱性	ソフトウェア等におけるセキュリティ上の弱点をいう。
設備	衛星運用、衛星データ利用、衛星開発・利用のためのファシリティ機能で、各設備にはシステム、サブシステムをいう。設備(Facility)＞システム（System)＞サブシステム（Sub-system)
ゼロデイ脆弱性	脆弱性のうち、ソフトウェアや機器の開発元等によって対策方法や修正プログラム等が提供されていないものをいう。
地上局サービス事業者	衛星運用に必要な追跡管制局、又は受信局を整備し、追跡管制サービス、又は受信サービスを提供する事業者をいう。
地上システム	衛星システムの打上、運用、データ利用、開発・製造を行うために地上に設置された設備及びシステムの総称で、ロケット打上設備、衛星運用設備、衛星データ利用設備、開発・製造設備等をいう。
追跡管制サービス	衛星運用に必要な追跡管制局を整備し衛星の追跡管制を代行するサービスをいう。
テレコマンド	地上から衛星へのコマンドの遠隔通信のことをいう。
テレメトリ	衛星から地上へのメトリ（metry）の遠隔通信のことをいう。メトリとは計測を意味し、ペイロードデータ等のことをいう。
テレメトリ・テレコマンドフィルタリング	テレメトリ及びテレコマンドにおける遠隔通信に対して、一定の基準で選択的に排除する機能のことをいう。
トロイの木馬	何らかの有用なソフトウェアを装って導入や実行を促し、起動すると利用者に気付かれないよう秘密裏にデータ漏えいや遠隔操作等の有害な動作を行うソフトウェアをいう。
ハウスキーピングデータ	軌道上の人工衛星や探査機の電力、温度、姿勢、位置等の衛星自身の状態を表すデータをいう。
バス	宇宙機としての基本的な動作（推進、熱制御、電源、姿勢制御、TT&C 等）のために搭載される機器のことをいう。
バスインターフェース	バス機器が情報の授受を行うために他システムと接続を行う機器をいう。
バスコマンド&コントロール	バス機器へのコマンドによって、バス機器に関するコントロールを行うことをいう。
バステレメトリ・テレコマンド	バス機器に対するテレメトリ及びテレコマンドのことをいう。

用語	本ガイドラインにおける定義
バックドア	ソフトウェアやシステムの一部として管理者や利用者に気付かれないよう秘密裏に仕込まれた、遠隔操作のための接続窓口をいう。
ファジング	ソフトウェア等の製品に問題を引き起こしそうなテストデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する手法をいう。
ペイロード	衛星の特定のミッションのために搭載される機器のことをいう。
ペイロードインターフェース	ペイロードが情報の授受を行うために他システムと接続を行う機器をいう。
ペイロードコマンド&コントロール	ペイロードへのコマンドによって、ペイロードに関するコントロールを行うことをいう。
ペイロードコントロールセンター	ペイロードをコントロールする機能を持つ衛星運用システムのことをいう。
ペイロードテレメトリ・コマンド	バス機器に対するテレメトリ及びテレコマンドのことをいう。
マルウェア	コンピューターの正常な利用を妨げ、利用者やコンピューターに有害な動作を行うソフトウェアをいう。
ミッションコントロールセンター	バス機器をコントロールする機能を持つ衛星運用システムのことをいう。
ラテラルムーブメント	企業や組織のネットワークに侵入したマルウェアが、正規の機能を悪用して、内部の偵察や資格の窃取を行う攻撃手法をいう。
ランサムウェア	パソコン等の端末やサーバー上のデータを暗号化する等して使用不可にし、それらを復旧することと引き換えに身代金を支払うように促す脅迫メッセージを表示するウイルスをいう。
リプレイ攻撃	利用者の確認に用いられる認証データの送受信を盗聴し、得られたデータをそのまま用いてその利用者になりすます攻撃手法をいう。
ルートキット	攻撃ツールや盗聴ツール等の悪質なソフトウェアがパッケージングされたソフトウェアをいう。
ワーム	インターネット等を通じてコンピューターに侵入し、さらに他のコンピューターへの自身の複製を試み、有害な動作を行うソフトウェアをいう。

４．２ 略語集

略語	英文	和文
ADCS	Attitude Determination and Control Subsystem	姿勢決定制御系
AEAD	Authenticated Encryption with Associated Data	認証付き暗号
AES	Advanced Encryption Standard	先進的暗号化標準
AIAA	American Institute of Aeronautics and Astronautics	米国航空宇宙学会
AOCS	Attitude and Orbit Control Subsystem	姿勢軌道制御系
ASAT	Anti-satellite Weapon	対衛星攻撃兵器
C&DH	Command and Data Handling	コマンド及びデータの取扱い
CAN	Controller Area Network	コントローラエリアネットワーク
CCCS	Canadian Center for Cyber Security	カナダサイバーセキュリティセンター
CCSDS	Consultative Committee for Space Data System	宇宙データシステム諮問委員会
CDI	Contexts and Dependency Injection	管理対象防衛情報
CI	Classified Information	機密情報
CIA	Central Intelligence Agency	中央情報局
CISA	Cybersecurity and Infrastructure Security Agency	サイバーセキュリティ・インフラセキュリティ庁
CISO	Chief Information Security Officer	最高情報セキュリティ責任者
CNE	Computer Network Exploitation	コンピューターネットワークによる諜報活動
CMAC	Cipher-based Message Authentication Code	暗号ベースのメッセージ認証符号
CMMC	Cybersecurity Maturity Model Certification	サイバーセキュリティ成熟度モデル認証
CNSS	Committee on National Security Systems	国家安全保障システム委員会
COPUOS	Committee on the Peaceful Uses of Outer Space	国連宇宙空間平和利用委員会
CPSF	Cyber/Physical Security Framework	サイバー・フィジカル・セキュリティ対策フレームワーク
CRYPTREC	Cryptography Research and Evaluation Committees	暗号技術研究・評価委員会
CSEC	Communications Security Establishment	通信セキュリティ協会
CSF	Cybersecurity Framework	サイバーセキュリティフレームワーク
CUI	Controlled Unclassified Information	機密情報ではない重要情報
CVE	Common Vulnerabilities and Exposures	共通脆弱性識別子
DFARS	Defense Federal Acquisition Regulation Supplement	防衛連邦調達規制補足
DHS	Department of Homeland Security	国土安全保障省

略語	英文	和文
DIA	Defense Intelligence Agency	米国国防情報局
DL	Downlink	ダウンリンク（下り通信）
DMZ	Demilitarized Zone	非武装地帯
DoD	Department of Defense	米国国防総省
DoDI	Department of Defense INSTRUCTION	国防総省要領
DOJ	Department of Justice	米国司法省
DSA	Digital Signature Algorithm	デジタル署名アルゴリズム
DSN	Deep Space Network	深宇宙通信情報網
ECDSA	Elliptic Curve Digital Signature Algorithm	楕円曲線デジタル署名アルゴリズム
ECM	Engineering Chain Management	エンジニアリングチェーンマネジメント
ENISA	European Union Agency for Cybersecurity	欧州ネットワーク情報セキュリティ機関
ESA	European Space Agency	欧州宇宙機関
FA	Factory Automation	ファクトリーオートメーション
FBI	Federal Bureau of Investigation	連邦捜査局
FedRAMP	Federal Risk and Authorization Management Program	米国政府機関におけるクラウドセキュリティ認証制度
FIPS	Federal Information Processing Standard	連邦情報処理規格
FISMA	Federal Information Security Management Act Federal Information Security Modernization Act	連邦情報セキュリティマネジメント法（～2014 年） 連邦情報セキュリティ近代化法（2014 年～）
FW	Firewall	ファイアウォール
GCM	Galois/Counter Mode	ガロアカウンターモード
GNSS	Global Navigation Satellite System	全球測位衛星システム
HMAC	Hash-based Message Authentication Code	ハッシュベースのメッセージ認証符号
HW	Hardware	ハードウェア
IaaS	Infrastructure as a Service	インフラストラクチャ・アズ・ア・サービス
IADC	Inter-Agency Space Debris. Coordination Committee	国際機関間スペースデブリ調整委員会
ID	Identification	識別子
IEC	International Electrotechnical Commission	国際電気標準会議
IoT	Internet of Things	モノのインターネット
IPA	Information-technology Promotion Agency, Japan	独立行政法人情報処理推進機構
ISAC	Information Sharing And Analysis Center	情報共有分析センター

略語	英文	和文
ISMAP	Information System Security Management and Assessment Program	政府情報システムのためのセキュリティ評価制度
ISMS	Information Security Management System	情報セキュリティマネジメントシステム
ISO	International Organization for Standardization	国際標準化機構
IT	Information Technology	情報技術
IV&V	Independent Verification & Validation	独立検証及び妥当性確認
JAXA	Japan Aerospace Exploration Agency	国立研究開発法人宇宙航空研究開発機構
J-CRAT	Cyber Rescue and Advice Team against targeted attack of Japan	サイバーレスキュー隊
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center	一般社団法人 JPCERT コーディネーションセンター
NASA	National Aeronautics and Space Administration	米国航空宇宙局
NIST	National Institute of Standards and Technology	米国国立標準技術研究所
NRO	National Reconnaissance Office	国家偵察局
NSA	National Security Agency	米国国家安全保障局
NSC	National Security Council	米国国家安全保障会議
NSD	National Security Directive	国家安全保障指令
NSTISSC	National Security Telecommunications and Information Systems Security Committee	国家安全保障通信及び情報システムセキュリティ委員会
OA	Office Automation	オフィスオートメーション
OS	Operating System	オペレーティングシステム
OSA	Orbital Security Alliance	オービタルセキュリティアライアンス
OSS	Open Source Software	オープンソースソフトウェア
OT	Operational Technology	オペレーショナルテクノロジー
PaaS	Platform as a Service	プラットフォーム・アズ・ア・サービス
PC	Personal Computer	パーソナルコンピューター
PNT	Positioning, Navigation and Timing	測位、航法、時刻
RF	Radio Frequency	無線周波数
SaaS	Software as a Service	ソフトウェア・アズ・ア・サービス
SBOM	Software Bill of Materials	ソフトウェア部品表
SDR	Software-Defined Radio	ソフトウェア無線
SLA	Service Level Agreement	サービス品質保証
SP	Special Publication	特別刊行物

略語	英文	和文
SPD	Space Policy Directive	宇宙政策指令
SW	Switch	スイッチ
SW	Software	ソフトウェア
SWG	Sub Working Group	サブワーキンググループ
TT&C	Telemetry, Tracking and Command	テレメトリ、トラッキング及びコマンド
UL	Uplink	アップリンク（上り通信）
USSF	United States Space Force	米国宇宙軍
VPN	Virtual Private Network	仮想専用線
VSAT	Very Small Aperture Terminal	超小型地球局
WG	Working Group	ワーキンググループ

4.3 本ガイドライン作成について

本ガイドラインは 2020 年度～2023 年度に実施した経済産業省「令和 2 年度サイバー・フィジカル・セキュリティ対策事業（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」、「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)」、「令和 4 年度サプライチェーン・サイバーセキュリティ対策促進事業（産業分野別のセキュリティガイドライン等の整備)」及び「令和５年度産業サイバーセキュリティ強靭化事業（ＩｏＴ機器やソフトウェアのセキュリティ確保等に関する調査)」の各事業成果をもとに、以下に示す有識者会合における議論を通じてとりまとめられたものである。

関連有識者会合

	有識者会合名称	設置期間
イ	産業サイバーセキュリティ研究会ワーキンググループ１（制度・技術・標準化）宇宙産業ＳＷＧ	2021 年 1 月 14 日～
ロ	産業サイバーセキュリティ研究会ワーキンググループ１（制度・技術・標準化）宇宙産業ＳＷＧ作業部会　コアメンバー会議	2021 年 2 月 15 日～
ハ	産業サイバーセキュリティ研究会ワーキンググループ１（制度・技術・標準化）宇宙産業ＳＷＧ作業部会	2021 年 2 月 15 日～

2024 年 3 月時点

有識者会合委員一覧

対象者名 （敬称略）	所属 （2024 年 3 月時点）	参加会合 （上表イからハ）		
		イ	ロ	ハ
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）　常務理事	●		
片岡 晴彦	株式会社 IHI　顧問（元防衛省航空幕僚長）	●		
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 セキュリティ対策推進部脆弱性対策グループ　主任研究員	●	●	●
栄原 聡文	東北大学大学院工学研究科航空宇宙工学専攻宇宙ロボット研究室 准教授 NPO 法人大学宇宙工学コンソーシアム（UNISEC）　理事長	●		
小山 浩	三菱電機株式会社 電子システム事業本部　主席技監	●		
坂下 哲也	一般財団法人 日本情報経済社会推進協会（JIPDEC）　常務理事	●		
佐々木 弘志	フォーティネットジャパン合同会社 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　専務理事・上級分析官	●		
丸山 満彦	PwC コンサルティング合同会社　パートナー	●		
満永 拓邦	東洋大学情報連携学部情報連携学科　准教授 独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター専門委員	●		
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　代表取締役		●	●

対象者名 （敬称略）	所属 （2024 年 3 月時点）	参加会合 （上表イからハ）		
		イ	ロ	ハ
上杉 謙二	PwC コンサルティング合同会社　テクノロジーコンサルティング　ディレクター		●	●
小出 祐輔	株式会社 Synspective　情報セキュリティ管理責任者		●	●
合田 知善	日本電気株式会社　航空宇宙・防衛ソリューション事業部門　宇宙システム統括部　プロフェッショナル		●	●
國母 隆一	株式会社アクセルスペース 執行役員 / Co-CTO（情報技術担当）		●	●
神宮 健	NRI セキュアテクノロジーズ株式会社 DX セキュリティコンサルティング事業本部 IoT セキュリティ事業部		●	●
鈴本 遼	株式会社アークエッジ・スペース　執行役員 / ソフトウェア・基盤システム部長		●	●
多賀 正敏	国立研究開発法人宇宙航空研究開発機構（JAXA） セキュリティ・情報化推進部セキュリティ統括課 課長		●	●
髙橋 康夫	三井物産セキュアディレクション株式会社 コンサルティングサービス事業本部 公共事業部 宇宙防衛グループ プリンシパルアナリスト		●	●
田中 洋吏	三菱電機株式会社電子システム事業本部　鎌倉製作所　宇宙技術部　セキュリティ技術課　課長		●	●
平松 敏史	株式会社パスコ　衛星事業部システム技術部　部長		●	●
ハについては上記メンバー以外に以下の関係者が参加： 一般財団法人リモート・センシング技術センター、宇宙技術開発株式会社、株式会社アストロスケールホールディングス、株式会社 ALE、株式会社日立ソリューションズ、キヤノン電子株式会社、さくらインターネット株式会社、スカパーJSAT 株式会社、日本スペースイメージング株式会社、富士通株式会社、マカフィー株式会社				
オブザーバ	内閣府 宇宙開発戦略推進事務局 内閣官房 内閣サイバーセキュリティセンター 内閣官房 内閣衛星情報センター 総務省 文部科学省 防衛省 独立行政法人宇宙航空研究開発機構			
事務局	経済産業省製造産業局宇宙産業室 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（令和 2 年度、令和 3 年度） 株式会社三菱総合研究所（令和 4 年度、令和 5 年度）			

2024 年 3 月時点