経済産業省

資料４

産業サイバーセキュリティ研究会WG１
宇宙産業SWG（第６回）

事務局説明資料

令和５年３月１６日

経済産業省 製造産業局 宇宙産業室

１．宇宙分野における海外のサイバーセキュリティ対策等について

２．今年度の作業部会での活動について

３．ガイドラインVer 1.1のアップデート内容について

４．ガイドラインVer 2.0に向けたアップデート方針について

５．今後の予定について

【米国】Aerospace社による宇宙システムのサイバー攻撃フレームワークSPARTAの公開

- 2022年10月、**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**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**ために作成された。
- 本フレームワークは、特に宇宙船を対象としたサイバー脅威に焦点を当てており、宇宙船に対する**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。
- なお本フレームワークは、2021年同社より米国政府機関に提出された「Cybersecurity Protections for Spacecraft: A Threat Based Approach」を参考に整理されている。

SPARTAの概要

対象セグメント	● 地上セグメント、通信リンクセグメント及び宇宙セグメント
目的	● 宇宙システムに関するセキュリティの向上及び独自のサイバー脅威への対抗
背景	● 近年、宇宙船がサイバー攻撃の標的となっている ● 宇宙領域で直面するサイバー脅威に対抗できるようにする必要がある
対象者	● システム開発者・運用者・管理者・セキュリティ担当者 ● セキュリティ研究者
活用方法	● 本フレームワークを活用することで、サイバー攻撃者の戦術、技術、手順、ナレッジ、スキル等を理解し、攻撃の可能性を分析することが可能になる ● 攻撃者の意図を理解した上で必要な防御策を検討することが可能になる ● 攻撃シナリオに基づく実践的な演習に活用することができる
今後の予定	● V1.2のアップデートに向けた検討がなされている

「Cybersecurity Protections for Spacecraft: A Threat Based Approach」とは

- 地上・通信・宇宙の各セグメントで多層の防護策を講じる必要性を提示した文書。
- NIST SP 800-53等の既存のサイバーセキュリティ基準においてカバーされていない観点を整理した上で、脅威分析の結果に基づいた対策要求事項をまとめている。

出所）Aerospace Corporation, “Understanding Space-Cyber Threats with the SPARTA Matrix” 、” Cybersecurity Protections for Spacecraft: A Threat Based Approach”に基づき三菱総合研究所作成
https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix
DistroA-TOR-2021-01333-Cybersecurity Protections for Spacecraft-A Threat Based Approach.docx (aerospace.org)

（参考）SPARTAにおけるサイバー攻撃戦術一覧

戦術 Tactics	概要
偵察 Reconnaissance	攻撃者が攻撃を行うための足がかりを得るための技術で構成される。宇宙船の設計の情報・構成するシステム情報・記述子・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。
資源開発 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、宇宙船のセーフモード時に悪意のあるコマンドを送信し、宇宙船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、ローカルもしく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。
横展開 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。

出所）Aerospace Corporation, “Space Attack Research & Tactic Analysis (SPARTA)” に基づき三菱総合研究所作成
https://sparta.aerospace.org/

（参考）SPARTAにおけるサイバー攻撃技術一覧

戦術

技術

偵察	資源開発	初期アクセス	実行	永続化	防御回避	横展開	データ流出	影響
宇宙船の設計情報の収集	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	ホスト型ペイロード	リプレイ攻撃	詐欺（誤指示）
宇宙船の記述子の収集	インフラストラクチャーへの攻撃	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	バスへの攻撃	サイドチャネル攻撃	妨害
宇宙船の通信情報の収集	攻撃者の能力開発	侵害された近隣の宇宙船を介したクロスリンク	認証プロセスの変更	地上システムへの妨害	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
盗聴	攻撃者の能力向上	セカンダリー/バックアップ通信経路への攻撃	ブートメモリの不正利用	宇宙船の暗号鍵の変更	なりすまし	訪問機インタフェースへの攻撃	アウトオブバンドリンク	劣化
ソフトウェア開発情報の収集		近距離を利用した攻撃	ハードウェア・ファームウェアの破損の悪用		セーフモード時の保護機能低下を悪用した攻撃	仮想化環境への攻撃	プロキシミティ・オペレーション	破壊
セーフモード測定器の監視		なりすまし	暗号化の無効化		ホワイトリストの修正		通信設定の変更	盗聴
サプライチェーン情報の収集		セーフモード時の保護機能低下を悪用した攻撃	シングルイベントアップセット（SEU）の発生		ルートキット		地上システムへの攻撃	
ミッション情報の収集		補助機器・装置の悪用	時間同期実行				開発者・開発環境への攻撃	
		マルウェア	ソフトウェアの欠陥や弱点の悪用				パートナーサイトへの攻撃	
			悪意のあるコードの注入				ペイロードへの攻撃	
			セーフモード時の保護機能低下を悪用した攻撃					
			オンボード値の変更					
			フラッディング攻撃					
			スプーフィング					
			なりすまし					
			サイドチャネル攻撃					

出所）Aerospace Corporation, “Space Attack Research & Tactic Analysis (SPARTA)” に基づき三菱総合研究所作成
https://sparta.aerospace.org/

【EU】NIS2指令の可決

- 欧州議会と欧州理事会は、**デジタル化に伴い増加したサイバー攻撃・サイバーリスクに対するセキュリティ強化を目的**として、現行のNIS指令を改定したNIS2指令を制定することに2022年5月13日に合意した。
- NIS2指令は、**対象セクターにおけるセキュリティリスク管理対策の基準とEU加盟国間の効果的な協力のための仕組みを定めた指令**であり、対象として16セクター（必須分野：10セクター、重要分野：6セクター）を指定し、3つの目標とそれを達成するための具体案を掲げている。
- NIS2指令では、**宇宙セクターを含む複数のセクターを対象範囲に追加**し、宇宙セクターにおける対象事業者として、「**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**（ただし、欧州電気通信法指令の対象となる通信事業者を除く）」が追加された。
- 加えて、**対象セクター・対象事業者に求めるセキュリティリスク管理に関する項目が明記された**ほか、**罰則内容も具体化**された。
- 2022年11月28日に**欧州理事会はNIS2指令を可決**し、**2023年1月16日に施行**された。**EU各国は21か月以内に本指令へ対応した国内法を整備することが求められている**。

NIS2指令で掲げられた3つの目標と具体案

セキュリティリスクの管理	• インシデント対応・危機管理、脆弱性の取扱・開示、セキュリティテスト、暗号化の利用などについてのセキュリティ要求事項の強化 • セキュリティリスク管理措置の遵守について、企業経営者への説明責任の要求　など
協力関係の強化	• EUレベルでの大規模なセキュリティインシデントに対する処置を支援するEUサイバー危機連絡組織ネットワーク（EU-CyCLONe）の創設 • 新たに発見された脆弱性に対して、EU全域で連携した脆弱性情報の共有　など
セキュリティ能力の向上	• 各主体がセキュリティ対策を講じるような、より厳格な監督手段と法執行措置の導入 • セキュリティリスク管理および報告義務の侵害に対する制裁金などの行政処分一覧表の策定　など

出所）European Parliament, The NIS2 Directive: A high common level of cybersecurity in the EU
https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

（参考）NIS2指令に基づき所轄官庁が有する権限

- 本指令は、必須分野・重要分野に属する対象事業者に適用されるが、**所轄官庁が対象事業者に対して有する権限は必須分野・重要分野で異なり**、**必須分野に属する対象事業者に対してより厳格な監査・執行を行う権限を有する**。
- また、本指令では**対象分野の事業者に求めるセキュリティリスク管理の7項目が定義**されているが、これらの項目を満たすための具体的な対策や要件については指令内で定義されず、技術的・非技術的仕様を定めるための実装規則※1を採択しうることが明記されている。
- 罰則について、このセキュリティリスク管理や報告義務※2を侵害した場合は、**1,000万ユーロ又は事業者の前年度世界総売上高の2%のいずれか高い方を課す**と規定している。

※1: 欧州全体での統一的な取組を実施するために、実施権限が欧州委員会に付与される規則のこと。
※2: 対象事業者は、所轄官庁やCSIRTに対して、サービス提供に重大な影響を及ぼすインシデントを不当な遅滞なく報告する義務（24時間以内の通知、所管官庁・CSIRTからの要求があった場合の中間報告、1か月以内の最終報告）が規定されている。

必須分野・重要分野の事業者に対して所轄官庁が有する権限

必須分野の事業者	重要分野の事業者
抜き打ち検査を含む立入検査及びオフサイト監査	立入検査及び**事後の**オフサイト監督
定期的な監査	-
リスク評価又はリスク関連の利用可能な情報に基づく標的型セキュリティ監査	リスク評価又はリスク関連の利用可能な情報に基づく標的型セキュリティ監査
客観的、**無作為的**、公正かつ透明なリスク評価基準に基づくセキュリティ検査	客観的、公正かつ透明なリスク評価基準に基づくセキュリティ検査
文書化されたサイバーセキュリティポリシーを含む、事業者が採用したサイバーセキュリティ対策を評価するために必要な情報、ENISAへの通知義務の遵守要請	文書化されたサイバーセキュリティポリシーを含むサイバーセキュリティ対策を**事後に**評価するために必要なあらゆる情報、ENISAへの通知義務の遵守要請
監督業務の遂行に必要なデータ、文書または**あらゆる情報**へのアクセス要求	監督業務の遂行に必要なデータ、文書または情報へのアクセス要求
有資格監査人により実施されたセキュリティ監査の結果及びその根拠となる証拠など、サイバーセキュリティ対策の実施に関する証拠の要求	-

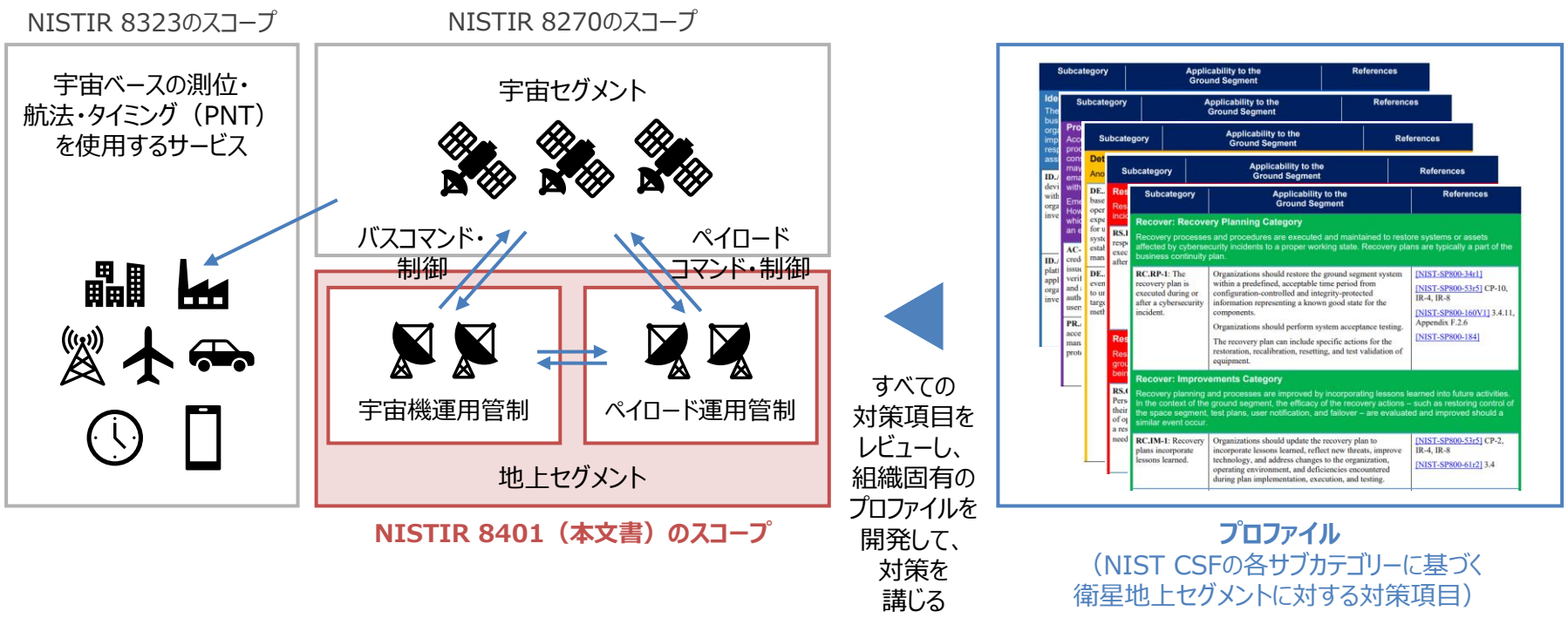
宇宙セクターの対象事業者（地上インフラ事業者）は必須分野の事業者に該当

出所）European Parliament, The NIS2 Directive: A high common level of cybersecurity in the EU
https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

【米国】NISTIR 8401: 衛星地上セグメントに対するCSFプロファイルの発表

- 2022年12月、米国NISTは、**NIST CSFに基づく衛星地上セグメントのためのプロファイルに関する文書であるNISTIR 8401を公開**した。
- 文書では、特に**宇宙機運用管制及びペイロード運用管制の2つに焦点**を当て、NIST CSFで規定されたサブカテゴリー毎に、**衛星地上セグメントに対する対策項目及び対策の参考となる文献が明記**されている。
- NISTは、本プロファイルを活用する組織に対し、**自組織のシステムに対して適用する際に、すべての対策項目をレビューすること**、組織の事業目標に基づくサイバーセキュリティ活動を実践するために、**各組織固有のプロファイルを開発すること**を奨励している。

NISTIR 8401のスコープ及びプロファイルの活用イメージ



出所）NIST, NISTIR 8401 Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Controlに基づき三菱総合研究所作成
https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf

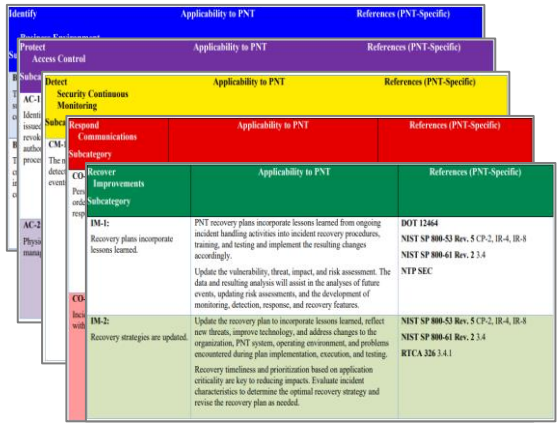
【米国】NISTIR 8323: PNTサービスに対するCSFプロファイルの改訂

- 2023年1月、米国NISTは、**宇宙ベースの測位・航法・タイミング（PNT）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 8323をRevision 1として改訂**した。
- 本プロファイルは、米国大統領令13905で示されたセキュリティ確保に向けた4項目を踏まえ、**NIST CSFの各サブカテゴリーに基づく、PNTサービスに対するセキュリティ対策項目を明記**している。
- Revision 1の改訂では、**リスクマネジメント戦略のサブカテゴリーに関する対策項目が追加**されたほか、付録において、**本プロファイルの想定される活用シナリオを追加している**。
- NISTは、本プロファイルを活用する組織に対して、**包括的に対策項目をレビューすること**や、組織の事業目標に基づくサイバーセキュリティ活動を実践するために**固有のプロファイルを開発すること**を奨励している。

NISTIR 8323r1のスコープ及びプロファイルの概要

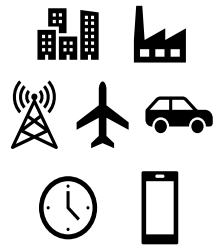
1	**PNTデータを使用又は形成するシステムを特定する**
2	**PNTデータソースを特定する**
3	PNTデータを使用又は形成する**システムの混乱と操作を検出する**
4	システムの責任ある使用に関する**リスクを管理する**

大統領令13905で定められたPNT利用時におけるセキュリティ確保に向けた4項目



セキュリティ対策プロファイル
（NIST CSFの各サブカテゴリーに基づくPNTサービスに対する対策項目）

宇宙ベースの測位・航法・タイミング（PNT）を使用するサービス

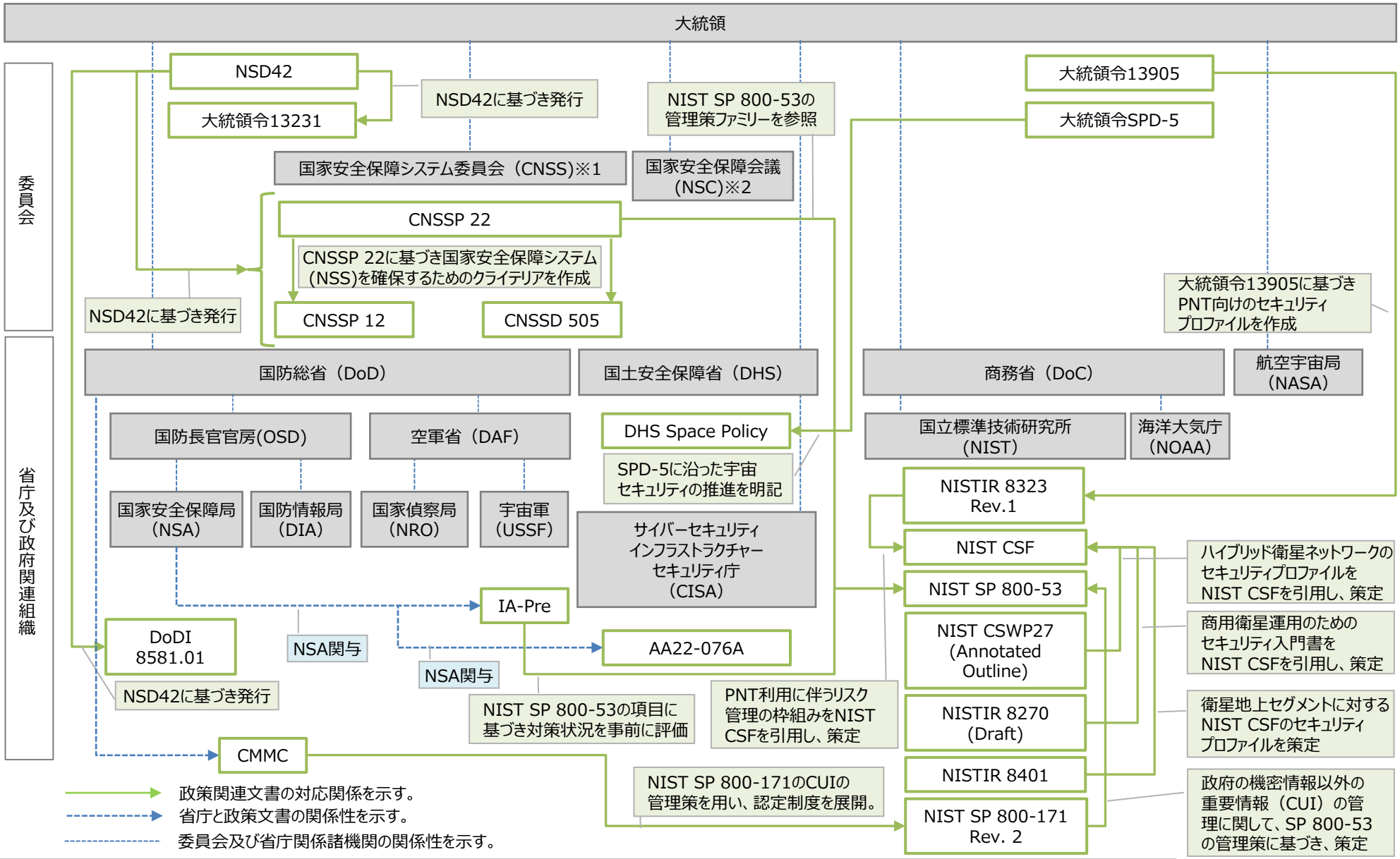


NISTIR 8323のスコープ

出所）NIST, NISTIR 8323r Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Servicesに基づき三菱総合研究所作成 https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8323r1.pdf

【米国】宇宙分野におけるサイバーセキュリティに関する体制・主要政策文書

※ 今後、継続的にアップデートしていく。



※1 CNSSは、国家安全保障システム（NSS）の委員会であり、国防総省の最高情報責任者（CIO）が委員長を務める。構成員は、国務長官等の21の米国政府機関により構成されている。
※2 NSCは、大統領が議長を務め、副大統領、国務長官、国防総省長官、エネルギー省長官が法廷委員として定められており、司法長官等により委員が構成されている。

【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（1/3）

No	発行時期	分類	名称	発行主体	概要
1	1990年7月 発行	大統領令	NSD42 “National Policy for the Security of National Security Telecommunications and Information Systems”	大統領	国家安全保障システムのセキュリティに関する指示、運用手順、指針を提供する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）の設立を指示した大統領令。
2	2001年10月 発行	大統領令	大統領令13231 “Critical Infrastructure Protection in the Information Age”	大統領	NSTISSCを、国家安全保障システム委員会（CNSS)に再指定することを指示した大統領令。
3	2005年6月 発行 2010年1月 改定	省庁訓令	DoDI 8581.01 “Information Assurance (IA) Policy for Space Systems Used by the Department of Defense”	DoD・NSA	米国政府及び国防総省が所有する宇宙システムについて、本方針に定められたIA要件を満たすよう求めた文書。
4	2005年2月 初版発行 2020年9月 第5版発行	ガイドライン	NIST SP 800-53 “Security and Privacy Controls for Information Systems and Organizations”	NIST	政府が調達する機器に関して機密情報を保護するために、セキュリティおよびプライバシーに関して詳細な管理策を規定したガイドライン。
5	2007年3月 発行 2012年1月 改訂 2018年2月 改訂	政策文書・政府調達基準	CNSSP 12 “National Information Assurance Policy for Space Systems Used to Support National Security Missions”	CNSS	NSD42に基づき策定された指針で、国家安全保障任務で用いられる宇宙システムに関する最低限度の指針を示している。
6	2009年2月 発行 2012年1月 改訂 2016年8月 改訂	政策文書・政府調達基準	CNSSP 22 “Policy on Information Assurance Risk Management Policy for National Security Systems”	CNSS	NSD42に基づき策定された指針で、国家安全保障システムのための情報保障リスク管理についての指針を示している。NIST SP 800-53の管理策ファミリーを参照している。

【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（2/3）

No	発行時期	分類	名称	発行主体	概要
7	2014年 初版 2018年4月 更新	ガイドライン	“Framework for Improving Critical Infrastructure Cybersecurity” (NIST CSF)	NIST	業種や企業規模などに依存せず、サイバーセキュリティ対策の効果を数値で評価するための基準など、汎用的かつ体系的なフレームワーク。
8	2017年7月 発行	政策文書・政府調達基準	CNSSD 505 “Supply Chain Risk Management (SCRM)”	CNSS	NSD42に基づき策定された指針で、国家安全保障任務で用いられる宇宙システムにおけるサプライチェーンリスクマネジメントについての最低限の指針を示している。
9	2020年1月 策定 2021年11月 改訂	フレームワーク（調達プログラム）	Cybersecurity Maturity Model Certification（CMMC）	DoD	防衛産業基盤企業のサプライチェーンにおけるFCI（連邦契約情報）とCUI（管理対象非機密情報）の保護を目的としたフレームワーク。DoDが調達する際の要件として、請負業者に対して適合を求めている。
10	2020年2月 発行	大統領令	大統領令13905 “Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services”	大統領	PNTサービスを利用するシステム等におけるセキュリティの確保に向けた取り組みの推進を指示した大統領令。本大統領令を元にPNT向けのセキュリティプロファイル（NISTIR 8323）が作成された。
11	2020年9月 発行	大統領令	大統領令SPD-5 “Cybersecurity Principles for Space Systems”	大統領	国家安全保障上の理由から、宇宙システムにおけるサイバーセキュリティの確保の重要性が強調し、悪意のあるサイバー活動による攻撃を想定して、システムの設計、開発、保護を行う必要がある旨を指示。
12	2020年2月　発行 2021年1月　更新	ガイドライン	NIST SP 800-171 Rev. 2 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”	NIST	非連邦政府の組織及びシステムが扱う「一般情報（Unclassified）」のうち、一部を「保護すべき情報（CUI：Controlled Unclassified Information）」として管理することを目的に、詳細な管理策を規定したガイドライン。
13	2021年2月 発行 2023年1月 改訂	ガイドライン	NISTIR 8323 “Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services”	NIST	大統領令13905に基づき作成されたPNT向けのセキュリティプロファイル。NIST CSFを元に、PNTサービスの利用者がサイバーセキュリティに関するリスクを管理するための枠組みを示している。

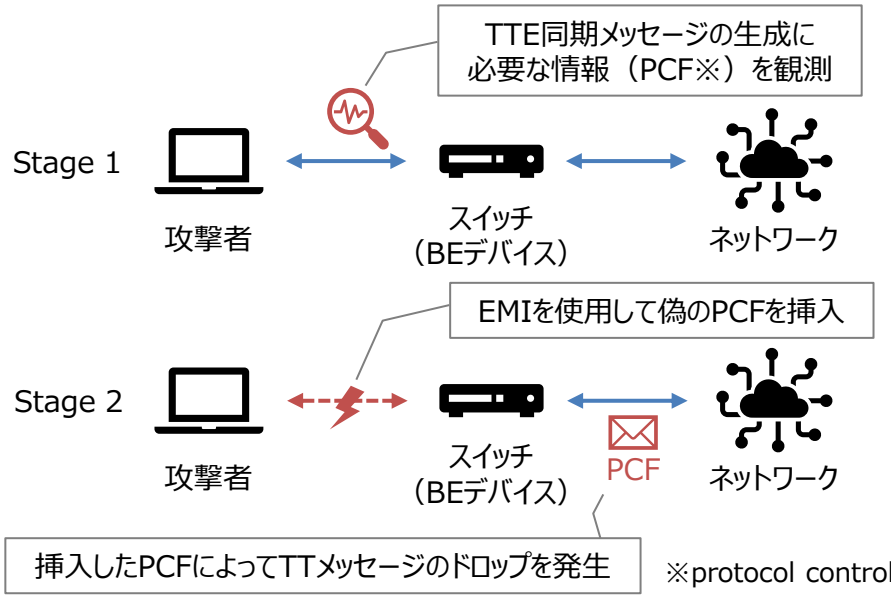
【米国】宇宙分野におけるサイバーセキュリティに関する主要政策文書（3/3）

No	発行時期	分類	名称	発行主体	概要
14	2021年6月 第一草稿発行 2022年2月 第二草稿発行	ガイドライン	NISTIR 8270 (2nd Draft) “Introduction to Cybersecurity for Commercial Satellite Operations”	NIST	商用衛星運用のためのセキュリティ入門書。NIST CSFを実践するための7つのステップに基づき、商用衛星運用におけるサイバーセキュリティリスク管理の基本ステップを示している。
15	2022年3月 発行	セキュリティアドバイザリー	AA22-076A “Strengthening Cybersecurity of SATCOM Network Providers and Customers”	CISA、FBI	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。衛星通信ネットワークのプロバイダー及び顧客に対する緩和策が提案された
16	2022年4月 第一草稿発行 2022年12月 最終発行	ガイドライン	NISTIR 8401 “Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control”	NIST	NIST CSFの各サブカテゴリーに基づき、衛星地上セグメントに対する対策項目を示した文書。
17	2022年4月 発行	政策文書	“DHS Space Policy”	DHS	国土安全保障に係る宇宙政策文書。宇宙システムのサイバーセキュリティの推進に関して、宇宙システム関係企業に対するセキュリティ原則の採用を奨励するとともに、SPD-5に沿ったベストプラクティス、教育教材、標準を開発する旨を明記。
18	2022年5月 発表 2023年1月 最初のサービスを登録予定 2025年9月までに完全移行予定	調達プログラム・政府調達基準	“Infrastructure Asset Pre-Approval” (IA-Pre)	DoD・USSF	米国DoDが調達する商用衛星通信サービスのセキュリティ確保のための取組で、NIST SP 800-53に基づくセキュリティ管理策を用いて、商用衛星通信サービスごとの対策状況が事前に評価するプログラム。
19	2022年7月 第一草稿発行 2022年11月 最終発行	ガイドライン	NIST CSWP 27 “Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity Annotated Outline”	NIST	ハイブリッド衛星ネットワーク（Hybrid Satellite Networks: HSN）に係るサイバーセキュリティプロファイルに関する概要ドラフト。NIST CSFに基づき、セキュリティプロファイルが作成される予定。

PCspooF：ミシガン大学及びNASAがTTEプロトコルに対する攻撃手法を発表

- **Time-Triggered Ethernet（TTE）**は、飛行制御や生命維持装置等のクリティカルな基幹機器と、一般旅客のWi-Fiやデータ収集等のベストエフォート（BE）で十分な機器を**同一のスイッチやネットワーク上で共存させるプロコトル**であり、NASAのOrionやLunar Gateway、ESAのAriane 6等に使用されている。
- ミシガン大学及びNASAは、TTE上に設置したBEデバイスを悪用し電磁干渉（EMI）を発生させ、**クリティカルなTTメッセージをドロップさせる攻撃手法（PCspooF）**を発表した。
- PCspooFによる攻撃は航空機や自動車等のクリティカルなシステムの事故につながる可能性があるとされ、発表では、**宇宙飛行のシミュレーションにおいてミッションの成功や安全性を脅かす制御不能なマニューバ**を引き起こす様子が示された。
- 対策として、**電磁干渉を防ぐフォトカプラーやサージ防護機器をTTEスイッチに導入すること等**が示されている。

PCspooFのイメージ



※protocol control framework

PCspooFに関するNASAのシミュレーション

- 左は通常時（PCspooFなし）、右はPCspooFによる攻撃時
- NASAのOrionのカプセルのドッキングに関するシミュレーションを実施
- PCspooFによってメッセージのドロップと遅延が発生し、ビークルはフライトパスを大幅に逸脱してドッキング機会を喪失

出所）A. Loveless, L. Phan, R. Dreslinski and B. Kasikci, "PCspooF: Compromising the Safety of Time-Triggered Ethernet," in 2023 IEEE Symposium on Security and Privacy (SP) , San Francisco, CA, US, 2023 pp. 572-587. https://web.eecs.umich.edu/~barisk/public/pcspoof.pdf

１．宇宙分野における海外のサイバーセキュリティ対策等について

２．今年度の作業部会での活動について

３．ガイドラインVer 1.1のアップデート内容について

４．ガイドラインVer 2.0に向けたアップデート方針について

５．今後の予定について

今年度の作業部会の活動概要

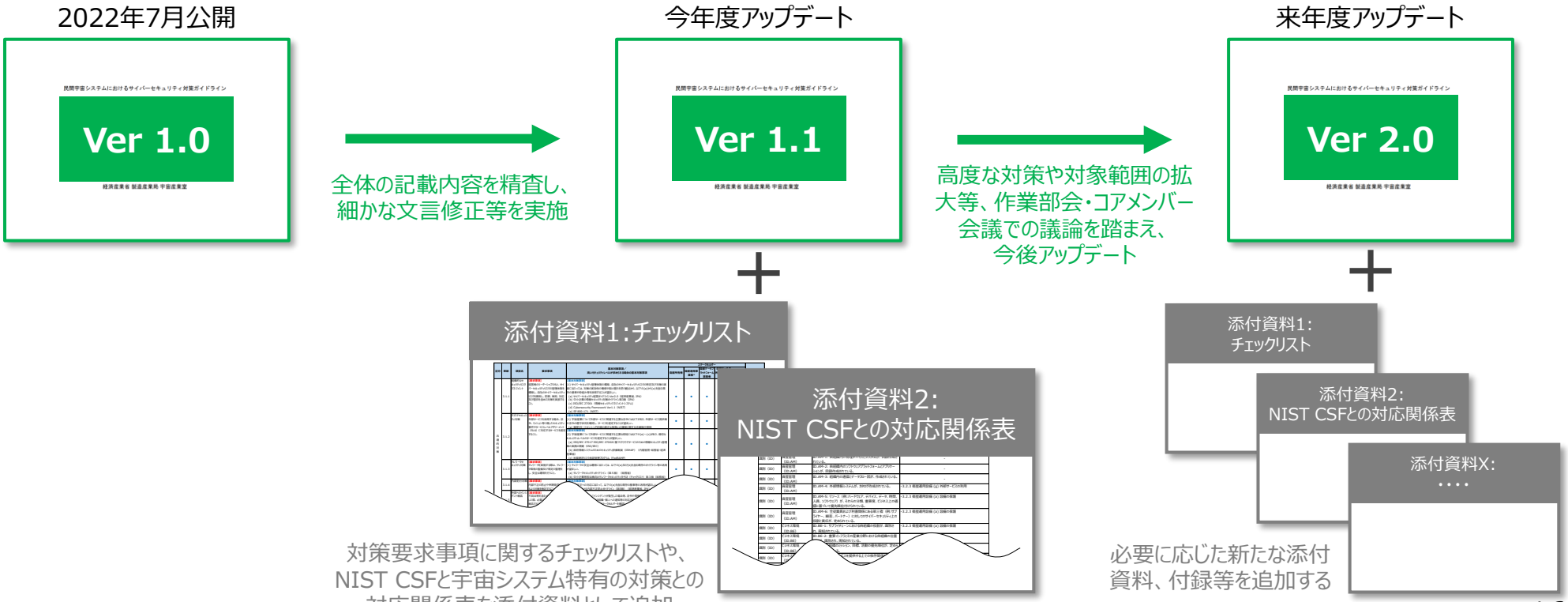
- 前回の宇宙産業SWG（第５回）で御報告したガイドラインVer 1.0について、2022年7月に正式公開した。
- 前回の宇宙産業SWG以降、１回の作業部会と４回のコアメンバー会議を開催し、**ガイドラインのアップデートに向けた議論**を行うとともに、**国内宇宙分野における情報共有体制の構築に関する議論**を行った。
- 本日の宇宙産業SWGでは、**作業部会・コアメンバー会議の議論を通じてアップデートしたガイドラインVer 1.1の案を御報告**するとともに、**今後のVer 2.0へのアップデートに向けた方針について御報告**する。
- ガイドラインのアップデートに関連して、**ガイドラインのVer 1.0の活用に関し、作業部会コアメンバーである粟津様・小出様・國母様よりプレゼンテーション**をいただく。

今年度の作業部会の活動概要

開催日	会議名	主な議題
2022年4月19日	宇宙産業SWG作業部会 コアメンバー会議（第５回）	• パブリックコメントの結果の概要について • ガイドライン公開に向けた今後のスケジュールについて
2022年6月7日	宇宙産業SWG作業部会 コアメンバー会議（第６回）	• パブリックコメントの結果を踏まえたガイドラインVer 1.0の修正内容について • 国内宇宙分野における情報共有体制の構築について
2022年7月21日	宇宙産業SWG（第５回）	• 名和委員及び経済産業省からの情報提供 • ガイドラインVer 1.0（案）について
2022年7月29日	宇宙産業SWG作業部会 コアメンバー会議（第７回）	• 宇宙航空研究開発機構（JAXA）仁尾様からの情報提供 • ガイドラインのアップデート方針について
2022年9月16日	宇宙産業SWG作業部会 コアメンバー会議（第８回）	• JAXA標準に対する質疑応答及び経産省ガイドラインへのフィードバックについて • ガイドラインのアップデート方針について
2022年10月31日	宇宙産業SWG作業部会 （第３回）	• ガイドラインVer 1.0の概要紹介 • ガイドラインのアップデート方針について • コアメンバー粟津様・小出様・國母様からの情報提供
2022年12月22日	宇宙産業SWG作業部会 コアメンバー会議（第９回）	• ガイドラインのアップデート方針について • 国内宇宙分野における情報共有体制の構築について
2023年2月1日	宇宙産業SWG作業部会 コアメンバー会議（第10回）	• ガイドラインVer 1.1のアップデート内容について • ガイドラインVer 2.0に向けたアップデート方針について

ガイドラインのアップデートについて

- ガイドラインのアップデートについて、コアメンバー会議での議論を踏まえ、**現状版のVer 1.0からVer 1.1へのアップデートは今年度**と、**Ver 1.1からVer 2.0へのアップデートは来年度、それぞれ実施**する。
- 今年度、Ver 1.1へのアップデートとして、**対策要求事項に関するチェックリスト**や、**NIST CSFと宇宙システム特有の対策との対応関係表を添付資料として追加**するとともに、**全体の記載内容を精査し、細かな文言修正等を実施**した。
- 来年度、Ver 2.0へのアップデートとして、**次のステップとして実施すべき高度な対策や小型衛星以外の適用範囲の拡大等、より広範な修正対応を作業部会・コアメンバー会議での議論を踏まえて実施**する。
- Ver 1.1におけるアップデート内容及びVer 2.0に向けたアップデート方針の詳細は以降で説明する。



（参考）国内宇宙分野における情報共有体制の構築に関する検討概要

- 2022年6月に開催したコアメンバー会議において、国内宇宙分野の情報共有体制の構築に向けた議論を行った。議論の結果、以下のような意見が挙げられた。
  - ✓ **<u>いきなり情報共有体制の設立を目指すことは敷居が高い</u>**。まずは、定期的な勉強会の開催や対面での打ち合わせ等の取組から始め、**<u>信頼関係を醸成することが重要</u>**である。
- これらの意見を踏まえ、一部のコアメンバー会議は対面を含む会議形式とするなど、**<u>信頼関係の醸成に向けた取組を始めたところ</u>**。
- また、他分野ISACに関する机上調査やヒアリングを通じ、**<u>情報共有体制構築に向けた成熟度モデルを作成</u>**するとともに、本モデルに基づき、**<u>国内宇宙分野の情報共有体制構築に向けたプロセス案を整理</u>**した。
- 2022年12月に開催したコアメンバー会議で挙げられた意見を踏まえつつ、今後、情報共有ニーズの深掘りを行うとともに、情報共有体制のあり方について引き続き議論を行う。

<u>国内宇宙分野における情報共有体制の構築に関するコアメンバー会議での主な意見</u>

- ✓ 情報共有体制の構築を前提とした議論ではなく、必要性の議論も必要であろう。
- ✓ 情報共有体制を構築することで、セキュリティ業界と宇宙業界の両方における情報共有の活性化が期待される。まずは協議会を立ち上げ、定期的に勉強会を開催したり対面での打ち合わせを設けたりといった取組から始めるのが良いと思われる。
- ✓ ベンチャー企業も含めた各民間宇宙企業の情報共有・分析に関するニーズをヒアリングすることから始めても良いのではないか。
- ✓ 信頼関係を醸成する中で、各社のニーズを掘り起こしていく必要がある。信頼関係が構築されれば、情報も出しやすくなる。
- ✓ 情報共有を行う上では、そこに参加している社のニーズが一致していることが重要となる。
- ✓ コアメンバー会議には様々な立場の事業者が参画しているため、まず各社のニーズを整理する必要がある。
- ✓ サイバーセキュリティに関する情報の共有だけではなく、各社が抱えている悩みや課題を共有する役割もあるのではないか。

（参考）情報共有体制の成熟度モデル

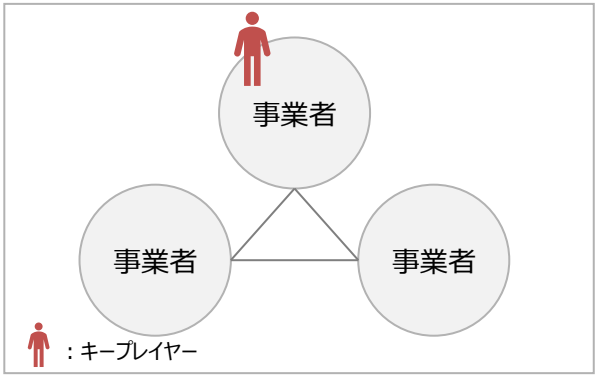
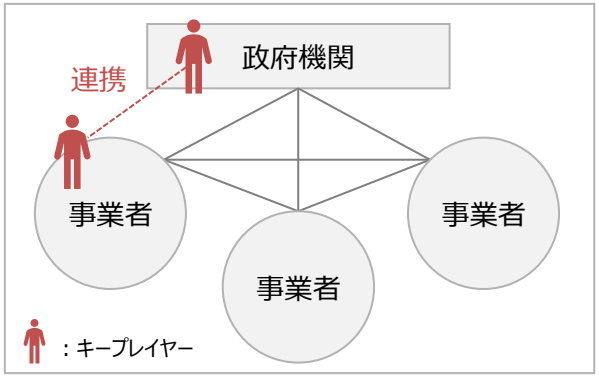
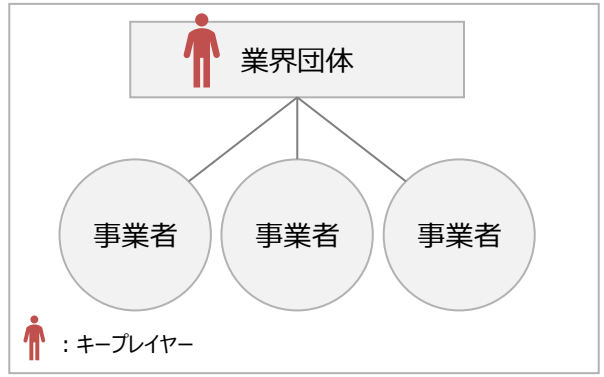
- 国内外のISAC等の取組を踏まえ、情報共有体制の成熟度モデルを4段階で整理。
- 国内宇宙分野においても、フェーズ0として、情報共有体制の組織化に先立ち**限定した関係者間での信頼関係醸成や情報共有の一部実施が必要**である。

	フェーズ0:萌芽期	フェーズ1:設立期	フェーズ2:成長期	フェーズ3:自律期
状態	**限定した関係者間で信頼関係を醸成し、情報共有を一部実施する**	**情報共有体制を組織化し、複数組織間での相互の情報共有を実施する**	**情報共有に加え、情報分析活動を一部実施するとともに、他の組織と連携する**	**会員企業の会費に基づく自律的な組織運営を行う**
詳細	• 限定した関係者間で、情報共有コミュニティの必要性を認識しつつ、信頼関係の醸成を図る。 • 情報共有に積極的なキープレイヤーが小さなコミュニテイを形成し、情報の共有を行う。 (初期はキープレイヤーからの情報提供が中心。)	• 限定した関係者から参加者を広げ情報共有体制を組織化し、ビジョン・ミッション、事業内容、情報共有ルールの策定等を行う。 • 策定したルールに基づき、組織間での相互の情報共有を実施する。	• 加入する組織が増加し、相互の情報共有がより活発化する。 • 情報共有の仕組みを評価・改善する。 • 脅威情報の分析を行い、分析結果を会員企業に共有する。 • 海外の関係組織や他分野ISACとの連携を行う。	• 業界内の多くの事業者が参加し、会員企業の会費に基づき、自律的な組織運営を行う。 • 多数のWG活動やサイバー演習の実施など、情報共有・分析の枠組みにとらわれない活動を実施する。
求められる取組例	• 勉強会や懇親会など顔が見えるネットワークの構築を行う。 • キープレイヤーを中心に、当該分野のセキュリティに関する情報の共有を始める。 • 将来的な情報共有体制構築に向け、必要な事項を整理する。	• 情報共有体制のビジョン・ミッション、事業内容、情報共有ルール等を策定する。 • 情報共有の仕組みを明確化し、相互の情報共有を促す。 • 会員区分や料金体系を整備する。 • 参加者拡大に向けた広報活動を行う。	• 会員数の増加に応じて、情報共有の仕組みを評価・改善する。 • 組織内での脅威情報の分析体制を構築する。 • 組織のセキュリティやコンプライアンスの確保を目的に、ルールの追加整備や見直しを行う。 • 海外の関係組織との連携を図るため、MOUを締結する。	• 会員数や組織規模の拡大に応じて、必要な場合には、資金メカニズムの見直しを行う。 • 会員のニーズを踏まえ、情報共有・分析の枠組みに囚われない活動を行う。（WG活動、サイバー演習、検証環境の整備など）

国内宇宙分野の現状

（参考）フェーズ0における体制の類型

- 情報共有体制構築に向けたフェーズ0における体制は、**①民間企業主導による構築、②政府機関主導による構築、③業界団体主導による構築の3つの類型に分類**される。
- なお、どの類型においても、**積極的な情報発信をするキープレイヤーの存在が重要**となる。
- また、これらの類型はあくまでフェーズ0における類型であり、体制構築後は異なる類型が想定されることに留意。

類型	① 民間企業主導型	② 政府機関主導型	③ 業界団体主導型
例	• 金融ISAC	• 米国Space ISAC • シンガポールOT-ISAC	• 電力ISAC • J-Auto-ISAC • ソフトウェアISAC
イメージ			
構築プロセス概要	• **民間事業者が有志で小規模な情報共有コミュニティを構築**する。 • **事業者におけるキープレイヤーが積極的な情報発信**を行い、キープレイヤー中心に情報共有コミュニティの**活動が活発化**する。 • コミュニティに参加する事業者の拡大やコミュニティの成熟に伴い、最終的にISAC設立（法人化）に至る。	• 政府機関が情報共有体制設立の必要性を認識し、**情報共有コミュニティの設立や運用を支援**する。 • **政府機関は設立を支援する立場で検討をリード**しつつ、**実際の情報共有は民間のキープレイヤーがリード**する。 • コミュニティに参加する事業者の拡大やコミュニティの成熟に伴い、最終的にISAC設立（法人化）に至る。	• **業界団体内で情報共有WGなどを設立**し、当該WGを介して、会員企業間で情報共有を行う。 • 業界団体が運営母体となりつつ、最終的にISAC設立（法人化）に至る。

（参考）国内宇宙分野の情報共有体制構築に向けたプロセス案

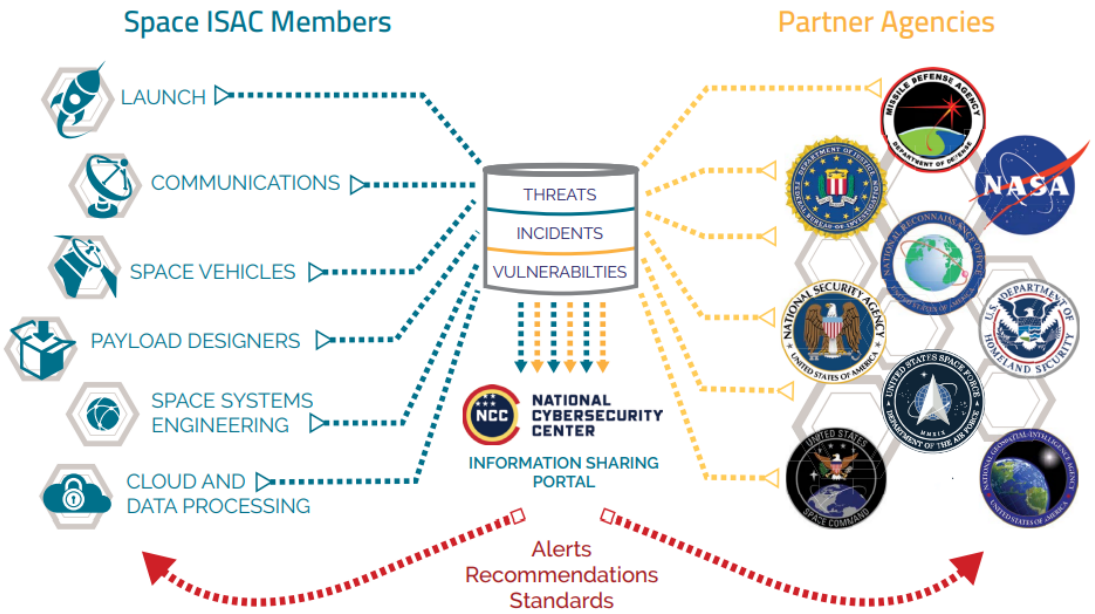
- 国内宇宙分野の情報共有体制構築に向けたプロセス案は以下のとおりであり、**フェーズ0の一年間では、情報共有・信頼関係醸成を進めつつ、体制構築に向けて必要な事項を整理すること**が望まれる。

		フェーズ0:萌芽期	フェーズ1:設立期	フェーズ2:成長期	フェーズ3:自律期
事業運営	情報共有	• キープレイヤーを中心に、宇宙分野のセキュリティに関する情報を共有する。	• 策定した情報共有ルールに基づき、組織間での相互の情報共有を実施する。	• 効率的な情報共有のためにプラットフォームを導入する。 • 必要に応じて、共有された情報のサマリーを作成する。	• フェーズ2から継続した情報共有を行う。
	情報分析			• 宇宙分野に関する脅威情報を分析し、会員企業の分析結果を共有する。	• フェーズ2から継続した情報分析を行う。
	その他	• 勉強会や懇親会など顔が見えるネットワークの構築を行い、信頼関係を醸成する。	• 定例会議、勉強会や懇親会など、顔が見えるネットワークの構築・強化を行う。	• 会員のニーズを踏まえ、WG活動やサイバー演習等の活動を実施する。	• 会員のニーズを踏まえ、複数WG活動、サイバー演習、検証環境の整備等の取組を行う。
組織運営	関係者の拡大	• 関係者間で、将来的な情報共有構築に向けて必要な事項を整理する。	• 初期の関係者以外の組織の参画に向けた広報活動を行う。必要に応じて、経産省から参加を促す。	• Space ISACとMOUを締結し、海外との連携を始める。 • 宇宙SWG関係者以外の組織の参画を促す。	• 宇宙分野への参画に際して、宇宙ISACへの参画を促す。必要に応じて、経産省から参加を促す。
	仕組み構築		• 情報共有のビジョン・ミッション、事業内容、情報共有ルール（TLP）等を策定する。 • 会員区分や料金体系を整備する。	• 組織のセキュリティやコンプライアンスの確保を目的に、ルールの追加整備や見直しを行う。 • 必要に応じて、会員区分や料金体系を見直し、新規参画がしやすい仕組みを構築する。	• 会員数や組織規模の拡大に応じて、必要な場合には、資金メカニズムの見直しを行う。

（参考）米国Space ISACの概要

- Space ISAC（Information Sharing and Analysis Center）は、**脆弱性、インシデント及び脅威に対する準備や対応能力の強化のために世界中の宇宙産業全体の協力を促進**し、さらに、メンバー企業間でのタイムリーかつ実用的な情報の共有等を行うための組織である。
- **2019年4月にコロラド・スプリングスで開催された35th Space Symposiumにおいて、Space ISACの設立が発表**された。その後、2019年11月、**NASAや米宇宙軍（旧空軍宇宙軍団）、米国家偵察局（National Reconnaissance Office）がスポンサー**となり、正式に発足した。
- 特に宇宙分野における**サプライチェーン、ビジネスシステム及びミッション**に対する脅威に焦点を当てている。

Space ISACによる情報共有と分析のエコシステム



Space ISACが注力する宇宙分野における3つの脅威

サプライチェーン

- 宇宙ミッションのサプライチェーンは広大で複雑であり、様々な脅威のベクトルが存在する。
- 設計、製造、配置、維持・管理及び廃棄の一連のサプライチェーンが対象となる。

ビジネスシステム

- ビジネスシステムには広範な対象が含まれる。
- 例えばエンタープライズシステムへの対策、データセキュリティソフトウェアに関する対策、従業員への訓練、外注先の管理等の対応が含まれる。

ミッション

- 宇宙ミッションは、世界中の人々にサービスやサポートを提供し、政府、軍、企業等に必要不可欠である。
- ミッション遂行のためには、安全な通信、暗号、RF監視、SSA等が求められる。

出所）Space ISAC Brochure等の公開情報に基づき三菱総合研究所作成
https://s07f21n96ry3bgacl3z1pdi9-wpengine.netdna-ssl.com/wp-content/uploads/2021/08/SISAC_8x11_Email-rev1.911.pdf

１．宇宙分野における海外のサイバーセキュリティ対策等について

２．今年度の作業部会での活動について

３．ガイドラインVer 1.1のアップデート内容について

４．ガイドラインVer 2.0に向けたアップデート方針について

５．今後の予定について

ガイドラインVer 1.1のアップデート内容について

- ガイドラインのVer 1.1のアップデートとして、**対策要求事項に関するチェックリスト**や、**NIST CSFと宇宙システム特有の対策との対応関係表**を添付資料として追加した。
- また、**ガイドライン全体を再精査した上で、細かな文言修正等を実施**した。

《ガイドラインVer 1.1の主なアップデート内容》

#	作業部会／コアメンバー会議での主な意見	アップデート内容
1	• チェックリストに関する要望があった。ガイドラインで記載している対策要件だけを抜き出してチェックリスト化する方法が想定される。 • チェックリストにおいては、要求事項の達成度をプルダウンで入力できる形式だと使いやすい。	• ガイドラインの要求事項や基本対策事項に関する簡易的なチェックリストを作成し、ガイドラインの添付資料として追加した。
2	• 第3.2節で記載されている宇宙システム特有の対策について、その他のガイドラインとの関係性が示されると事業者にとってはありがたい。整理するガイドラインについて、NIST CSFとのマッピングが取られていると大変ありがたい。 • NISTのガイドラインは広く活用されているため、使う立場としてはNIST CSFを軸に整理していただく方が使いやすい。 • NIST CSFを軸に経産省ガイドラインを整理いただいた方が事業者としては、使いやすい。 • 全社的観点では、CSF全体をみており、その中で宇宙の部分はどこに該当するのかを見ていく必要がある。そのため、NIST CSFを軸に整理していただく方が使いやすい。	• NIST CSFのフレームコアにおける各サブカテゴリーと、経産省ガイドラインにおける宇宙システム特有の対策（3.2.2～3.2.5）との対応関係を整理し、ガイドラインの添付資料として追加した。
3	• チェックリストを使用する際、ガイドラインよりもExcelを見るような形態で使うことが多い。 • NIST CSFとの整理について、Excelでご提供いただければ、自分で使いやすいように整理をすることができる。	• 上記の対策要求事項チェックリスト及びNIST CSF対応関係整理について、Excel形式にて公開する。

１．宇宙分野における海外のサイバーセキュリティ対策等について

２．今年度の作業部会での活動について

３．ガイドラインVer 1.1のアップデート内容について

４．ガイドラインVer 2.0に向けたアップデート方針について

５．今後の予定について

ガイドラインVer 2.0に向けたアップデート方針について

- ガイドラインのVer 2.0に向け、衛星間光通信システムにおける通信方式や暗号の実装方式等、**より高度な対策の実装方法について、その追記の必要性も含めて今後検討**する。
- ガイドラインの適用範囲に関して、**小型衛星以外の適用可能性を議論する**ほか、**宇宙分野特有のサプライチェーン・セキュリティ対策に関する追記を検討**する。
- 加えて、**本ガイドラインに基づく対策事例集やリモセン法ガイドラインとの対応関係整理を追加**する。

《ガイドラインVer 2.0に向けた主なアップデート方針》

#	作業部会／コアメンバー会議での主な意見	アップデート方針
1	• 衛星間や衛星地上間の光通信について、現行のガイドラインではカバーされているわけではなく、一言でも触れられていると良い。 • 光通信では鍵の有効期限が早くなるため、鍵のリニューアルを早く行う必要がある。また、衛星軌道上で鍵の生成をする必要もある。	• 衛星間光通信システムにおける暗号鍵生成や認証に関する対策の具体的な実装手順や留意事項等を整理し、手順書として取りまとめ、ガイドラインの付録や別冊として追加する。
2	• どのような対策を次のステップとして実装すべきかについて、記載がなされると良い。例えば、暗号の実装について、どの実装であれば許容されるか、すぐに読み取ることは難しく、間違った実装をしないための補足説明があると良い。 • 暗号の実装に関する補足説明の要望は理解するが、本ガイドラインのスコープからずれる恐れがあるため、追記するか否か、慎重に議論すべきである。	• 衛星システムにおける暗号実装に関する補足説明について、本ガイドラインのアップデート対象とするか、検討を行う。
3	• 小型衛星以外の衛星に対しても本ガイドラインを適用できるのか、また、衛星ごとに求める対策要求事項が異なるのか、議論できると良い。	• ガイドラインの適用範囲に関して、小型衛星以外の衛星に対する適用可能性を検討するとともに、衛星ごとに求められる対策要求事項を検討する。
4	• サプライチェーンの中で外部委託する場合や購入品に対して、気を付けるべき事項を整理すると良い。 • 衛星運用やアンテナを外部委託するケースがあるため、宇宙特有の議論ができると良い。	• 宇宙特有のシステムやコンポーネントのサプライチェーン対策として留意すべき内容に関して追記を行う。
5	• 対策事例集を追加すると、読み手にわかりやすいガイドラインになるのではないか。	• 本ガイドラインに基づく対策の事例集を取りまとめ、ガイドラインの付録又は別冊として追加する。
6	• 国内事業者においては、NIST CSFだけでなく、リモセン法ガイドラインとの比較ができると分かりやすい。	• リモセン法ガイドと経産省ガイドラインとの対応関係を整理し、ガイドラインの付録として追加する。

１．宇宙分野における海外のサイバーセキュリティ対策等について

２．今年度の作業部会での活動について

３．ガイドラインVer 1.1のアップデート内容について

４．ガイドラインVer 2.0に向けたアップデート方針について

５．今後の予定について

今後の予定について

① ガイドラインについて

- 本日ご紹介したVer 1.1のガイドライン及び概要資料（日本語版・英語版）を正式公開する。
- ガイドライン本文に関して、Ver 1.1の英語版を作成する。
- 英語版資料（本文・概要資料）を用い、国際調和に向けた海外関係機関との議論を行う。
- ガイドライン Ver 2.0のアップデートに向けた議論を行う。

② 宇宙分野におけるサイバーセキュリティに関する情報共有体制について

- 2022年12月に開催したコアメンバー会議で挙げられた意見を踏まえつつ、今後、情報共有ニーズの深掘りを行うとともに、情報共有体制のあり方について引き続き議論を行う。
- また、宇宙産業SWG作業部会の物理開催など、実務者レベルでの信頼関係の醸成に向けた取組を継続する。