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
【添付資料２】NIST Cybersecurity Framework (NIST CSF) と宇宙システム特有の対策との対応関係

本付録では、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、「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）との対応関係を示します。各文書の記載粒度が異なるため、完全な対応ではありませんが、対策実施時の参考として活用ください。なお、本ガイドラインの3.1節では、「共通的対策」として宇宙システムに関係する全組織に関わる対策を示しており、併せて参照することが望まれます。

※ NIST CSFのフレームコアの日本語文章は、IPAによる日本語翻訳版に基づきます。 https://www.ipa.go.jp/security/publications/nist/

NIST CSFのフレームコア			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）のうち、関連する対策要求事項
機能	カテゴリー	サブカテゴリー	
識別（ID）	資産管理（ID.AM）	ID.AM-1: 自組織内の物理デバイスとシステムが、目録作成されている。	-
識別（ID）	資産管理（ID.AM）	ID.AM-2: 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。	-
識別（ID）	資産管理（ID.AM）	ID.AM-3: 組織内の通信とデータフロー図が、作成されている。	-
識別（ID）	資産管理（ID.AM）	ID.AM-4: 外部情報システムが、カタログ作成されている。	・3.2.3 衛星運用設備 (g) 外部サービスの利用
識別（ID）	資産管理（ID.AM）	ID.AM-5: リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。	・3.2.3 衛星運用設備 (a) 設備の保護
識別（ID）	資産管理（ID.AM）	ID.AM-6: 全従業員および利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。	・3.2.3 衛星運用設備 (a) 設備の保護
識別（ID）	ビジネス環境（ID.BE）	ID.BE-1: サプライチェーンにおける自組織の役割が、識別され、周知されている。	・3.2.3 衛星運用設備 (a) 設備の保護
識別（ID）	ビジネス環境（ID.BE）	ID.BE-2: 重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。	-
識別（ID）	ビジネス環境（ID.BE）	ID.BE-3: 組織のミッション、目標、活動の優先順位が、定められ、周知されている。	-
識別（ID）	ビジネス環境（ID.BE）	ID.BE-4: 重要サービスを提供する上での依存関係と重要な機能が、定められている。	-
識別（ID）	ビジネス環境（ID.BE）	ID.BE-5: 重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。	・3.2.3 衛星運用設備 (a) 設備の保護
識別（ID）	ガバナンス（ID.GV）	ID.GV-1: 組織のサイバーセキュリティポリシーが、定められ、周知されている。	-
識別（ID）	ガバナンス（ID.GV）	ID.GV-2: サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。	-
識別（ID）	ガバナンス（ID.GV）	ID.GV-3: プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。	-
識別（ID）	ガバナンス（ID.GV）	ID.GV-4: ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。	-
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-1: 資産の脆弱性が、識別され、文書化されている。	・3.2.2 衛星本体 (c) 衛星実装機能の事前検証 ・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-2: サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。	-
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-3: 内部および外部からの脅威が、識別され、文書化されている。	・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-4: ビジネスに対する潜在的な影響とその発生可能性が、識別されている。	・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-5: 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。	・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策
識別（ID）	リスクアセスメント（ID.RA）	ID.RA-6: リスク対応が、識別され、優先順位付けされている。	-
識別（ID）	リスク管理戦略（ID.RM）	ID.RM-1: リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。	-
識別（ID）	リスク管理戦略（ID.RM）	ID.RM-2: 組織のリスク許容度が、決定され、明確に表現されている。	-
識別（ID）	リスク管理戦略（ID.RM）	ID.RM-3: 自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。	-
識別（ID）	サプライチェーンリスクマネジメント（ID.SC）	ID.SC-1: サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。	-
識別（ID）	サプライチェーンリスクマネジメント（ID.SC）	ID.SC-2: 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策

NIST CSFのフレームコア			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）のうち、関連する対策要求事項
機能	カテゴリー	サブカテゴリー	
識別（ID）	サプライチェーンリスクマネジメント（ID.SC）	ID.SC-3: サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。	・3.2.2 衛星本体 (c) 衛星実装機能の事前検証 ・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (h) セキュアコーディング
識別（ID）	サプライチェーンリスクマネジメント（ID.SC）	ID.SC-4: サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。	・3.2.3 衛星運用設備 (d) データの保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
識別（ID）	サプライチェーンリスクマネジメント（ID.SC）	ID.SC-5: 対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。	・3.2.3 衛星運用設備 (a) 設備の保護
防御（PR）	アクセス制御（PR.AC）	PR.AC-1: 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されてい	-
防御（PR）	アクセス制御（PR.AC）	PR.AC-2: 資産に対する物理アクセスが、管理され、保護されている。	・3.2.3 衛星運用設備 (a) 設備の保護
防御（PR）	アクセス制御（PR.AC）	PR.AC-3: リモートアクセスが、管理されている。	・3.2.3 衛星運用設備 (b) 通信の保護 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
防御（PR）	アクセス制御（PR.AC）	PR.AC-4: アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。	-
防御（PR）	アクセス制御（PR.AC）	PR.AC-5: ネットワークの完全性が、保護されている（例:ネットワークの分離、ネットワークのセグメント化）。	-
防御（PR）	アクセス制御（PR.AC）	PR.AC-6: IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。	・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (b) 通信の保護
防御（PR）	アクセス制御（PR.AC）	PR.AC-7: ユーザ、デバイス、その他の資産は、トランザクションのリスク（例:個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例:多要素認証など）が行われている。	・3.2.3 衛星運用設備 (b) 通信の保護
防御（PR）	意識向上およびトレーニング（PR.AT）	PR.AT-1: すべてのユーザは、情報が周知され、トレーニングが実施されている。	-
防御（PR）	意識向上およびトレーニング（PR.AT）	PR.AT-2: 権限を持つユーザが、自身の役割と責任を理解している。	-
防御（PR）	意識向上およびトレーニング（PR.AT）	PR.AT-3: 第三者である利害関係者（例:サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。	-
防御（PR）	意識向上およびトレーニング（PR.AT）	PR.AT-4: 上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。	-
防御（PR）	意識向上およびトレーニング（PR.AT）	PR.AT-5: 物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。	-
防御（PR）	データセキュリティ（PR.DS）	PR.DS-1: 保存されているデータが、保護されている。	・3.2.2 衛星本体 (a) RF通信の保護 ・3.2.3 衛星運用設備 (b) 通信の保護 ・3.2.3 衛星運用設備 (d) データの保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
防御（PR）	データセキュリティ（PR.DS）	PR.DS-2: 伝送中のデータが、保護されている。	・3.2.2 衛星本体 (a) RF通信の保護 ・3.2.2 衛星本体 (b) RF通信のジャミング対策 ・3.2.2 衛星本体 (e) 送受信データの完全性 ・3.2.3 衛星運用設備 (b) 通信の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
防御（PR）	データセキュリティ（PR.DS）	PR.DS-3: 資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。	-
防御（PR）	データセキュリティ（PR.DS）	PR.DS-4: 可用性を確保するのに十分な容量が、維持されている。	・3.2.3 衛星運用設備 (a) 設備の保護
防御（PR）	データセキュリティ（PR.DS）	PR.DS-5: データ漏えいに対する防御対策が、実装されている。	・3.2.2 衛星本体 (a) RF通信の保護 ・3.2.2 衛星本体 (e) 送受信データの完全性 ・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (b) 通信の保護 ・3.2.3 衛星運用設備 (d) データの保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
防御（PR）	データセキュリティ（PR.DS）	PR.DS-6: 完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。	・3.2.2 衛星本体 (a) RF通信の保護 ・3.2.2 衛星本体 (e) 送受信データの完全性 ・3.2.3 衛星運用設備 (b) 通信の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
防御（PR）	データセキュリティ（PR.DS）	PR.DS-7: 開発・テスト環境が、実稼働環境から分離されている。	-
防御（PR）	データセキュリティ（PR.DS）	PR.DS-8: 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-1: 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例:最低限の機能性の概念）を組み入れて、定められ、維持されている。	-

NIST CSFのフレームコア			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）のうち、関連する対策要求事項
機能	カテゴリー	サブカテゴリー	
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-2: システムを管理するためのシステム開発ライフサイクルが、実装されている。	・3.2.2 衛星本体 (c) 衛星実装機能の事前検証 ・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (h) セキュアコーディング
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-3: 構成変更管理プロセスは、策定されている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-4: 情報のバックアップが、実施され、維持され、テストされている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-5: 組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-6: データは、ポリシーに従って破壊されている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-7: 防御プロセスは、改善されている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-8: 防御技術の有効性に関する情報が、共有されている。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-9: （インシデント対応および事業継続）対応計画と（インシデントからの復旧および災害復旧）復旧計画が、策定され、管理されている。	・3.2.3 衛星運用設備 (a) 設備の保護
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-10: 対応計画と復旧計画が、テストされている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-11: サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。	-
防御（PR）	情報を保護するためのプロセスおよび手順（PR.IP）	PR.IP-12: 脆弱性管理計画が、作成され、実装されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策
防御（PR）	保守（PR.MA）	PR.MA-1: 組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。	・3.2.3 衛星運用設備 (a) 設備の保護
防御（PR）	保守（PR.MA）	PR.MA-2: 組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。	-
防御（PR）	保護技術（PR.PT）	PR.PT-1: 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。	・3.2.3 衛星運用設備 (d) データの保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
防御（PR）	保護技術（PR.PT）	PR.PT-2: リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。	-
防御（PR）	保護技術（PR.PT）	PR.PT-3: 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。	-
防御（PR）	保護技術（PR.PT）	PR.PT-4: 通信（情報）ネットワークと制御ネットワークが、保護されている。	・3.2.2 衛星本体 (a) RF通信の保護 ・3.2.2 衛星本体 (b) RF通信のジャミング対策 ・3.2.3 衛星運用設備 (b) 通信の保護
防御（PR）	保護技術（PR.PT）	PR.PT-5: メカニズム（例:フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。	・3.2.3 衛星運用設備 (a) 設備の保護
検知（DE）	異常とイベント（DE.AE）	DE.AE-1: ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。	・3.2.3 衛星運用設備 (g) 外部サービスの利用 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	異常とイベント（DE.AE）	DE.AE-2: 検知したイベントは、攻撃の標的と手法を理解するために分析されている。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	異常とイベント（DE.AE）	DE.AE-3: イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	異常とイベント（DE.AE）	DE.AE-4: イベントがもたらす影響が、判断されている。	・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策 ・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	異常とイベント（DE.AE）	DE.AE-5: インシデント警告の閾値が、定められている。	-
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-1: ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保 ・3.2.3 衛星運用設備 (g) 外部サービスの利用
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-2: 物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	・3.2.3 衛星運用設備 (a) 設備の保護
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-3: 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。	-
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-4: 悪質なコードは、検知されている。	-

NIST CSFのフレームコア			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）のうち、関連する対策要求事項
機能	カテゴリー	サブカテゴリー	
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-5: 不正なモバイルコードは、検知されている。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-6: 外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。	-
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-7: 権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。	・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	セキュリティの継続的なモニタリング（DE.CM）	DE.CM-8: 脆弱性スキャンが、実施されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策
検知（DE）	検知プロセス（DE.DP）	DE.DP-1: 検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。	-
検知（DE）	検知プロセス（DE.DP）	DE.DP-2: 検知活動は、該当するすべての要求事項を準拠している。	・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	検知プロセス（DE.DP）	DE.DP-3: 検知プロセスが、テストされている。	・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	検知プロセス（DE.DP）	DE.DP-4: イベント検知情報が、周知されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
検知（DE）	検知プロセス（DE.DP）	DE.DP-5: 検知プロセスが、継続的に改善されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
対応（RS）	対応計画の作成（RS.RP）	RS.RP-1: 対応計画が、インシデントの発生中または発生後に実行されている。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	コミュニケーション（RS.CO）	RS.CO-1: 人員は、対応が必要になった時の自身の役割と行動の順序を認識している。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	コミュニケーション（RS.CO）	RS.CO-2: インシデントが、定められた基準に沿って報告されている。	-
対応（RS）	コミュニケーション（RS.CO）	RS.CO-3: 対応計画に従って、情報が共有されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
対応（RS）	コミュニケーション（RS.CO）	RS.CO-4: 利害関係者との間で調整が、対応計画に従って行なわれている。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	コミュニケーション（RS.CO）	RS.CO-5: サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。	-
対応（RS）	分析（RS.AN）	RS.AN-1: 検知システムからの通知は、調査されている。	・3.2.3 衛星運用設備 (a) 設備の保護 ・3.2.3 衛星運用設備 (f) 送受信データの完全性の確保
対応（RS）	分析（RS.AN）	RS.AN-2: インシデントがもたらす影響は、把握されている。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	分析（RS.AN）	RS.AN-3: フォレンジックが、実施されている。	-
対応（RS）	分析（RS.AN）	RS.AN-4: インシデントは、対応計画に従って分類されている。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	分析（RS.AN）	RS.AN-5: プロセスは、内外のソース（例:内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。	-
対応（RS）	低減（RS.MI）	RS.MI-1: インシデントは、封じ込められている。	-
対応（RS）	低減（RS.MI）	RS.MI-2: インシデントは、緩和されている。	-
対応（RS）	低減（RS.MI）	RS.MI-3: 新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。	・3.2.2 衛星本体 (d) 衛星搭載機器の脆弱性対策 ・3.2.2 衛星本体 (f) サプライチェーンに対するセキュリティ対策
対応（RS）	改善（RS.IM）	RS.IM-1: 対応計画は、学んだ教訓を取り入れられている。	・3.2.3 衛星運用設備 (a) 設備の保護
対応（RS）	改善（RS.IM）	RS.IM-2: 対応戦略は、更新されている。	・3.2.3 衛星運用設備 (a) 設備の保護
復旧（RC）	復旧計画の作成（RC.RP）	RC.RP-1: 復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。	-
復旧（RC）	改善（RC.IM）	RC.IM-1: 復旧計画は、学んだ教訓を取り入れている。	・3.2.3 衛星運用設備 (a) 設備の保護
復旧（RC）	改善（RC.IM）	RC.IM-2: 復旧戦略は、更新されている。	・3.2.3 衛星運用設備 (a) 設備の保護
復旧（RC）	コミュニケーション（RC.CO）	RC.CO-1: 広報活動が、管理されている。	-
復旧（RC）	コミュニケーション（RC.CO）	RC.CO-2: 評判は、インシデント発生後に回復されている。	-
復旧（RC）	コミュニケーション（RC.CO）	RC.CO-3: 復旧活動は役員と経営陣だけでなく、内外の利害関係者にも周知されている。	・3.2.3 衛星運用設備 (a) 設備の保護