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１】対策要求事項チェックリスト

「要求事項」とは、明示されているステークホルダーが検討し取り組むべき事項を意味します。そして、「基本対策事項」とは、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意味します。
また、更なるセキュリティの向上が見込めますが、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」として示しています。
本チェックリストを用いて、各要求事項の達成度を「1: 未実施」、「2: 一部実施」、「3: 実施済み」、「4: 実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し」、
「5: 実施済みで、管理手順を文書化・自動化し、随時見直し」に応じて評価するなどして、宇宙システムにおけるセキュリティ対策の検討・確認に活用ください。

・項目は例示であり、利用者の状況に応じて、項目の追加・削除や、内容の修正を行っても構いません。
・達成度の基準については、利用者の状況に合わせて簡素化しても構いません。

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					達成度
					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	衛星データ利用サービス事業者	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 Ver1.1（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	●	●	●	●	●	
	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。	●	●	●	●	●	

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					達成度
					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	衛星データ利用サービス事業者	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(c)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) 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（本体及びRF通信）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) RF通信の保護　(b) RF通信のジャミング対策 (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	衛星運用設備	【要求事項】 衛星運用設備（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(h)の対策を実施することが望ましい。 (a) 設備の保護　(b) 通信の保護　(c) ジャミング対策 (d) データの保護　(e) 設備の検証と設備の脆弱性対策 (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	–	●	●	–	●	
	3.2.4	衛星データ利用設備	【要求事項】 衛星データ利用設備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) 設備の保護　(b) データの保護　(c) 設備の検証と設備の脆弱性対策 (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	–	–	●	●	●	
	3.2.5	開発・製造設備	【要求事項】 衛星の開発・製造設備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・製造設備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