（別紙）

「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β版」に対する意見募集結果の概要

	提出意見	提出意見に対する考え方
1	■対象箇所 表3-18 インシデント等の報告・相談先（62p） 場合　:【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 届出元：脆弱性関連情報の発見者 届出先：IPA セキュリティセンター 根拠となる法令・規程等： 受付機関及び調整機関を定める告示（経済産業省告示） 備考・参考 URL： 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/ ■対象記述箇所 根拠となる法令・規程等： 受付機関及び調整機関を定める告示（経済産業省告示） ■修正案 根拠となる法令・規程等： 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） ■理由・概要 「受付機関及び調整機関を定める告示」は「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」における「受付機関」および「調整機関」として、それぞれ、IPA、JPCERT/CC を指定する告示です。 発見者に届出するよう推奨する規定を含め、各当事者宛の実質的な行動規範を定めている告示は「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」であるため、根拠規程としては「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」を挙げるようお願いいたします。	ご意見の通り修正いたします。
	■対象箇所 ・基本対策事項(1)(c)「衛星実装機能の事前検証」について（73p） ■対象記述箇所 OSS（Open Source Software）の利用に当たっては、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）、『共通脆弱性識別子 CVE 概説』（IPA）等の OSS 検証ツールがある。 ■修正案 OSS（Open Source Software）の利用に当たっては、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）、『共通脆弱性識別子 CVE 概説』（IPA）等の参考資料がある。 ■理由・概要 『共通脆弱性識別子 CVE 概説』は、脆弱性の識別子である CVE について解説した資料です。『共通脆弱性識別子 CVE 概説』は解説文書であってツールではありませんので、「OSS 検証ツールがある」との記述は、「参考資料がある」といった記述に修正いただけますと幸いです。	ご意見の通り修正いたします。
2	本ガイドラインが制定された場合には、このガイドラインに沿って必要なセキュリティ行った上で各団体から民間事業者に発注が行われることになると弊社では認識しております。 セキュリティ対策に関しましては、過剰な対策を行いますと、経済性と利便性の観点において問題が発生する場合がありますので、システムの性質に対して必要十分な対策を選択することが重要と考えております。 セキュリティ対策を検討するシステム担当者としては、セキュリティ対策が不足するというリスクを取ることはしないと考えます。このため、本ガイドラインを参照した場合、適用要否が不明瞭である項目には、「適用しない」という選択を行うことは難しく、迷った場合には「適用」を選択せざるをえなくなると思われます。結果として、本ガイドラインを検討したワーキンググループの委員が想定した以上の過剰なセキュリティ対策が取られることが想定されます。 これは、国内の公共事業関連の場合には、民間事業者から適正な価格で調達を行うことができなくなることに繋がります。また、本ガイドラインの対象となるシステムの調達を行う事業者の立場からすると、設備投資が高額化することによって他の手段との競争力や国際競争力が失われることに繋がることが懸念されます。 このため各項目について、「必須」、もしくは「必須ではない」が明確に判断できる必要があると考えます。 p.26にて規定されています、【高いセキュリティレベルが求められる場合】について、どのようなシステムについて適用する必要があるのかといったことについて、「具体的な判断方法を記述する」、もしくは、「該当するシステムを例示する」ことが望ましいと考えます。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。

		p.7 ・意見内容 「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」とのことですが、今後、チェックリストなど要件の明確化や認定制度の整備を希望致します。 ・理由 事業者が「基本的なサイバーセキュリティ対策を満たす事業者」かどうかを個別に自社で証明することが難しい場合が想定されるため、第三者による確認で適合性を証明できることが望ましいと考えます。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
		p.27-28 ・意見内容 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において、例えば3.1.1などの基本対策事項として複数の基準や枠組みの活用が示唆されておりますが、何を活用すべきか絞り込むための考え方、優先度を明示頂くことを希望致します。 ・理由 複数の基準や枠組みにおいて異なる要求がなされたり、重複する要求内容であっても文章の表現が異なることで適合性の判定が判定者の解釈により差異が生じることを懸念します。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
		p.28 ・意見内容 衛星運用設備や開発・製造設備に属さない、修理・不具合診断や改修用の計算機など事業者が自前で所持する設備についても要件の明確化を希望致します。 ・理由 基本的に契約毎の製品に準じたサイバーセキュリティー対策が事業者が自前で所有する設備についても求められるものと考えますが、これを明確にすることで事業者毎の解釈のブレによる対策レベルの不足が回避されると考えます。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
		p.27-28 ・意見内容 今後、サイバー対策の一環として、関係者の国籍調査や国籍制限が課されることがないことを希望致します。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 個人情報の保護や管理の面で制約があり、実行が厳しいものと考えます。	本ガイドラインには「関係者の国籍調査や国籍制限」に当たる記載はございません。
		p.28 ・意見内容 「セキュアコーディング」が課せられた場合、適用ができないCOTS/OSSが生じることを懸念致します。 ・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。） 実績あるCOTS/OSSを活用できない場合、製造すべきコードの範囲が拡大し、高コスト化してしまう状況を懸念致します。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
3		p.27-28 ・意見内容 今後、このガイドラインを各省庁などが仕様として適用されるケースが生じると思われます。この観点から、各事業内容に対応した要求水準・ランクと、そのランクに応じた要求内容を本ガイドラインまたはその他の手段にて明確化することが必要と思われます。 ・理由 契約毎にお客様の主観で要求水準が変わってしまい、対応が難しくなる、高額化してしまう等を懸念致します。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
		p.28 ・意見内容 表3-1の3.2.2項-3.2.4項　民間衛星本体に高いセキュリティレベルを要求される事は理解致しますが、実施上の観点から、衛星タイプによる必要最低限のセキュリティに関わる検証レベルの規定を要望致します。 ・理由 今後、国産、海外製の超小型衛星、マイクロ衛星が増加する事が予測されます。それらの衛星に必要なセキュリティ対策レベルは従来の衛星とは異なるレベルの要求設定が必要と思われます。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
		p.5 ・意見内容 本ガイドラインの対象範囲の明確化（モデルや例の記載）、特に、通信衛星・放送衛星等のユーザ設備が対象かどうかの明確化を希望します。 ・理由 地上システムの対象が観測衛星の例で記載されており、通信衛星や放送衛星の地上システムと相異が有ると思われます。また、通信衛星・放送衛星のユーザ設備は、宇宙システムとは異なるレベルのセキュリティガイドラインが必要と思われます。	P5に記載の通り、通信衛星や放送衛星は本ガイドラインの対象にはなっていません。
		p.72 ・意見内容 RF通信のジャミング対策の一つとして周波数ホッピング技術が参照されていますが、費用対効果が高いことが見込まれないため、実装されないケースが多くあると思われます。民間宇宙システムにおいては、ホッピングのための周波数帯域確保などを行うためのインセンティブが必要になると考えられます。 ・理由 周波数ホッピング技術でジャミング対策を行う場合、広帯域な周波数範囲が必要になるため、他システムとの干渉回避や帯域確保に想定以上に費用が掛かる場合がございます。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。

	・意見内容 　網羅的に概説を整理頂き、大変分かりやすいガイドラインになっていると考えております。宇宙システムにおけるサイバーセキュリティ対策に関しては、各メーカー共に、各対象に対し採用すべき施策、優先度等に関し経験が不足していることもあり、具体的事例に基づく、検討会、研究会等の実施を希望致します。 ・理由 　上記の活動は、各機関、メーカーが主観的な解釈をするのではなく、ある程度統一的な考え方、レベル感を共有するために必要と思われます。	宇宙産業SWGでは、引き続き、具体的事例に基づく議論に努めてまいります。
4	1.2本ガイドラインの対象範囲（5ページ） 気象衛星・通信衛星・放送衛星、打上設備は本ガイドラインの対象外となっているが、対象外とされた趣旨や今後の策定予定等を公表すべきである。 すでにインシデントの発生している気象衛星を初め、通信衛星、放送衛星、打上設備が現時点で本ガイドラインの対象から外れる意図を明確にされたい。本ガイドラインにおける「随時更新」の対象となり得るのか、今後別途策定予定であるのか、本ガイドライン又は他の規定を参考に対応すべきであるのか等を明確とすることにより、対象外とされた事業を営む民間宇宙システム事業者の便宜にも資するべきである。	本ガイドラインの開発に当たっては、新規参入が活発な超小型観測衛星に係る事業者及びそのサプライチェーンを主な分析対象としたため、気象衛星、通信衛星、放送衛星は対象から外しております。 本ガイドラインの対象の在り方については、今後、宇宙産業SWGの中で検討させていただきます。
	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（26ページ） 「高いセキュリティレベルが求められる場合」がどのような場合を指すのか、具体的な指針が示されるべきである。 「一定の予算や組織体制・人員が整備されてい」る事業者は、どのような事業者を指すのか、事業者の対応の要否が明確となるよう具体的な指針が示されるべきである。	本論点については、今後、宇宙産業SWGの中で検討させていただきます。
5	P80の 「NASA の管轄下にある「EOS-AM 1(Terra)」衛星が他の地球観測衛星と合わせて四機で「朝の星座」“morning constellation”により編成飛行中の 2007 年 と 2008 年において、商用のノルウェーのスバルバード地上局(Svalbard Ground Station)経由で少なくとも 4 回にわたり中国軍からのハッキング攻撃を受け たと報告されている。そのうち Terra 衛星に関しては、2008 年 6 月に 2 分間、同年 10 月には 9 分間攻撃者の完全な制御下に置かれ、衛星を制御するために必 要なすべてのステップを達成することができたと報告されている。」 との記載について、「報告されいている」ことが事実とは限らない。 「報告されている。」には出典を付加するべき。	ご意見を踏まえ、P80は削除することといたします。

その他、意見募集と関係のない意見が6件ありました。