

「2026年度HPCI共用ストレージ第三世代機保守」
仕様書に対する質問への回答

番号	書類名	対象箇所	質問	回答
1	仕様書	IV.1.(1) 研究所が定める情報セキュリティ対策規程及び情報セキュリティ対策基準を遵守すること。情報セキュリティ実施手順を参照する場合は別途覚書を締結後に開示するものとする。	研究所が定める情報セキュリティ対策規程及び情報セキュリティ対策基準を参照したいのですが、必要であれば、覚書の締結を行い、情報の開示をお願いいたします。	情報セキュリティ対策規程及び情報セキュリティ対策基準は、弊所外に公開しており、以下のURLから確認ができる。なお、特に覚書を締結する必要はない。 https://i.riken.jp/information_security/policy/
2	仕様書	IV.1.(3) 情報管理の体制を定めた情報管理体制図及び情報取扱者名簿、適正な情報管理体制が確保されていることを示す社内規則またはそれに類するものを提出すること。	貴研究所の入札の案件では通常、情報管理の体制を定めた情報管理体制図及び情報取扱者名簿の提出のみの認識ですが、適正な情報管理体制が確保されていることを示す社内規則またはそれに類するものの提示は必須でしょうか。また、情報取扱者名簿につきましては落札後にご提出させていただくのが通例かと存じますので、応札時は情報管理体制図のご提示のみでご理解を賜りたく存じます。	情報管理体制図および情報管理取扱者名簿を提出するのみで問題ない。 また、応札時は情報管理体制図のみの提示で問題ない。
3	仕様書	IV.1.(7) 死活監視や異常検知、アンチウイルスソフト、ファイアウォールなどセキュリティ装置の導入、アクセスログの確認と保存、定期的なアップデートや設定内容の確認などの情報セキュリティ対策を実施すること。具体的にとこまでの対策を実施するかについては、別途研究所と協議の上決定すること。	本調達業務は、貴所設置・稼働機器に関する保守業務であるため、本項要件は該当しないと思われまので、本要件の削除のご検討をお願いいたします。	一部削除する。 一方で、ストレージ装置のファームウェアアップデート情報の提供やログインしての確認などの可能性があるため以下の通り修正する。 システムへのログインなどを行う際は、アクセスログの確認と保存を行うこと。また、ファームウェアアップデート等のセキュリティに関する情報を提供すること。具体的にとこまでの対策を実施するかについては、別途研究所と協議の上決定すること。
4	仕様書	IV.1.(8) 本調達範囲内において暗号を利用する場合は、総務省及び経済産業省が定める「電子政府推奨暗号リスト(CRYPTREC)」に記載された暗号を利用すること。	本調達業務における暗号の利用は、遠隔作業における通信の暗号化であり、通信の暗号化については、IV.2.(2)の要件に定義されているため、本要件の削除のご検討をお願いいたします。	質問3の通り、作業中のログイン等で利用する可能性があるため削除はしない。 一方で、通信の暗号化などは記載通りで構わない。
5	仕様書	IV.1.(10) 情報セキュリティ対策の履行状況を確認するために、研究所が情報セキュリティ監査の実施を必要と判断した場合は、研究所がその実施内容(監査内容、対象範囲、実施等)を受注者と協議の上定めて、情報セキュリティ監査を行う(研究所が選定した事業者による監査を含む)。立ち入りを行なう場合は上記、受注者と協議の上定めた範囲で監査に協力すること。また、受注者は自ら外部監査を実施した場合は、その結果について研究所へ報告すること。	弊社が自ら外部監査を実施した場合、その結果について貴研究所へ報告を行うのは、現実的に難しいと考えますが、こちらについては要件を削除いただけないでしょうか。	削除する。 ただし、IV.1.(10)については、仕様書の以降の通し番号が変更になることもあり、<削除項目>として通し番号は残す。
6	仕様書	IV.1.(16) 研究所が指定する機器等についてリストを提出すること。	本調達は保守業務のみの認識です。機器等のリストの提出は不要と考えますので、本要件の削除のご検討をお願いいたします。	入札時の機器リストの提出は不要である。 一方、本件においては、保守時に交換作業などが発生する際に部材がない場合などに代替品を許可している。このような際にリスト提示などが発生する可能性があるため、本記載は削除しない。
7	仕様書	IV.1.(17) サプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、研究所と迅速かつ密接に連携し導入する機器等の見直しを図ること。	本調達業務は、貴所設置・稼働機器に関する保守業務であり、機器の納入はないため、本項要件は該当しないと思われまます。本要件の削除のご検討をお願いいたします。	質問6と同じとする。
8	仕様書	IV.2.(1) 遠隔作業用コンピュータおよびアカウント ① 遠隔作業用コンピュータに常に最新のセキュリティパッチ、ウイルス定義ファイルを適用すること。 ② 遠隔作業用コンピュータに適宜ウイルス検索を実行すること。 ③ 操作者は本業務用に発行されたアカウントを使用すること。	③については、貴所への接続に使用するアカウントは、貴所にて本業務専用発行頂いたアカウントを利用することで満たす、との理解で良いでしょうか。 尚、弊社セキュリティ規定では、業務に使用する端末は、弊社のセキュリティ規程に基づいて担当者に配布された端末となります。また、端末の利用アカウントは、弊社で管理・配布する業務アカウントを用いる規定となります。	その理解の通りである。 作業端末自体のアカウントへの制限はない。
9	仕様書	IV.7.(1) 受注者は以下の応札条件を満たしていること。なお、第三者機関による認証の有無がわかる資料(認証範囲が業務範囲と一致していること)を研究所に提出すること。	IV.7.(2)の「対象システムと同様規模の運用保守業務の受注経験」については、第三者機関による認証の対象外であると考えますので、こちらについては、「第三者機関による認証の有無がわかる資料」ではなく、弊社の書式でのご提示でよいでしょうか。	問題ない。IV.7.(2)の「対象システムと同様規模の運用保守業務の受注経験」は、受注者のフォーマットで構わない。
10	仕様書	IV.7.(3) ITIL等の標準モデルをベースにした運用作業体系を理解しており、それに基づく運用実績を有すること。	弊社では、本業務にITIL認定を持つ要員の従事をご提案します。但し、ITILは作業個人を認証するものであるため、個人情報の観点から、認証資料の提出については、本業務ご契約の際の提出とさせていただきますでしょうか。	問題ない。

11	仕様書	IV.7.(4)	ISMSあるいはISO/IEC 27001 認証を取得していること。 なお、情報が保存されるデータセンターが別の場合は当該データセンターでもISMSあるいはISO/IEC27001 認証を取得していること。	情報が保存されるデータセンターが別の想定となります。Boxの利用を想定していますが、それについてもISMSあるいはISO/IEC27001 認証の提示が必要でしょうか。	boxサービスは以下の通りISO/IEC27001 認証サポートが明示されているため問題ない。 https://support.box.com/hc/ja/articles/360043691774-ISO-27001%E8%AA%8D%E5%AE%9A%E3%81%AE%E6%A6%82%E8%A6%81%E3%81%A8FAQ
12	仕様書	技術審査項目別紙の提出物について	(2) 未然障害防止対策書	本書式で求める内容についてご教示をいただけないでしょうか。または、ひな形等があればご提供をいただけないでしょうか。	例を提示する。