

研究用仮想化基盤システム 一式
仕様書

国立研究開発法人
国立循環器病研究センター
令和6年11月

項番	機能要件
A	研究用仮想化基盤システム 一式
A.1	調達背景・目的
A.1.1	<p>国立研究開発法人 国立循環器病研究センター(以下、「NCVC」又は「当センター」という)では、当センターが主体となるレジストリ研究を多数実施している。それら研究では、電子的データ収集システム(EDC)を活用している。</p> <p>EDCやこれをメンテナンスする情報システムは、当センターのVMware仮想化基盤上で動作している。このVMware仮想化基盤では、他に「病院情報管理システム(電子カルテや診療部門システム)」、「ネットワーク・セキュリティ」、「財務会計・人事給与」等の当センターにとりミッションクリティカルな情報システムが稼働しているため、高い可用性が確保されている。</p> <p>一方で、EDC等の研究利用の情報システムは病院情報システムほどの高い可用性は求めていないことから、本調達では管理負担や運用コストを削減することを目的としている。このため、提案に当たっては、機器や構成が過度とならないよう留意すること。</p>
A.2	調達概要
A.2.1	本調達の範囲は、以下のとおりとする。
A.2.1.1	研究用仮想化基盤 一式
A.2.1.1.1	仮想化基盤(Hyper-V) 一式
A.2.1.1.1.1	<ul style="list-style-type: none"> サーバ NAS 無停電電源装置(UPS)
A.2.1.1.2	その他部品等 一式
A.2.1.1.2.1	<ul style="list-style-type: none"> サーバラック(設置作業含む)
A.2.1.1.2.2	<ul style="list-style-type: none"> 電源工事
A.3	納入期限・スケジュール
A.3.1	2025年3月24日までに、納入すること。
A.3.2	導入スケジュールは、当センターと協議の上、決定すること。
A.4	納入場所
A.4.1	納入場所は、大阪府吹田市岸部新町6-1 当センター内とすること。
A.5	仕様
A.5.1	受託者は、以下の仕様を満たす機器一式を納品、設置、導入すること。
A.5.2	仮想化基盤(Hyper-V) 一式
A.5.2.1	OSは、Microsoft Windows Server 2022 Datacenter Edition(又は2025)を用い、Hyper-V環境を構築すること。当該環境には、当センター既設のVLAN(10程度)を通信できること。なお、本基盤を接続する上位スイッチ側のtrunk設定は、当センターが行うものとする。
A.5.2.2	CPUは、第4世代インテルXeon (2.1GHz, 32コア)以上を2基以上搭載すること。
A.5.2.3	主記憶(メモリ)は、512GB以上搭載すること。
A.5.2.4	ディスク装置は、SSDを複数搭載し、冗長構成を取ること。
A.5.2.5	実効容量として、Windows OS用に100GB、仮想ゲストイメージ用に10TB割り当てられること。
A.5.2.6	ネットワークポートは、10GbEを1ポート以上、1GbEを1ポート以上有すること。
A.5.2.7	ディスプレイ出力用に、VGAポートを1つ以上搭載すること。
A.5.2.8	USBポートは、Type-Aを2つ以上搭載し、必ずUSB3.0以上のポートを含めること。
A.5.2.9	サーバの電源は、冗長構成・ホットプラグ仕様とすること。
A.5.2.10	サーバやストレージ装置等の電源について、提案機器に合わせたコンセント形状の変更や切替え工事が必要な場合は、本調達の電源工事に含めること。なお、現状敷設済みで未使用の電源ケーブルは、負荷容量：100V-20A/回路で、形状NEMA15-5Rの4個口タップが4本(1本/回路)である。
A.5.2.11	IPMIに対応したBMCを搭載し、OSの挙動に影響を受けずハードウェアの性能・障害監視が行えること。
A.5.2.12	当センターが指定するSNMPマネージャーからのポーリングを受け入れ、又、障害時にSNMPトラップを送出できること。なお、監視ツールとしてZabbixを想定している。
A.5.2.13	シャーシは1~4U程度のラックマウントサーバであること。
A.5.2.14	仮想ゲストOSのバックアップ用に、NASを用意すること。実効容量は20TB程度で、ディスクは冗長構成とすること。Hyper-Vサーバからの仮想ゲストOSバックアップができること。
A.5.2.15	Hyper-Vサーバ、NASを接続するUPSを用意すること。UPSは瞬間停電対策を目的とし、5分程度稼働維持できること。

項番	機能要件
A. 5. 2. 16	UPSは以下機能を有することが望ましい。ただし、有償オプションとなる場合は不要である。 <ul style="list-style-type: none"> 指定時間UPS稼働後にサーバ、及びNASを安全にOSシャットダウンする機能 UPSをLAN接続してリモートで管理する機能
A. 5. 2. 17	納入から1年分のライセンス・保守費用は本調達に含めること。又、次年度から6年目までの5年分の保守費用を別途提示すること。次年度以降の保守について、サーバの利用状況によっては、途中で稼働を打ち切る場合もあるので注意すること。なお、当センターはMicrosoft 365 Enterprise E3を契約しており、ここに含まれないライセンス(CAL)のみ本調達に含めること。
A. 5. 3	その他部品等 一式
A. 5. 3. 1	サーバ ラック
A. 5. 3. 1. 1	本研究用仮想化基盤一式を収容するサーバラック一式を納入すること。
A. 5. 3. 1. 2	ラックは、当センター既設の「日東工業 FSS110-722EKNヘンケイ」と同等以上とすること。
A. 5. 3. 1. 3	ラック搭載位置は、当センターと協議の上決定すること。
A. 5. 3. 1. 4	階下への調整が必要なことから、設置工事は30日前を目安にセンターの承認を得ること。
A. 5. 3. 2	その他
A. 5. 3. 2. 1	有償オプションとなる場合は、ディスプレイ・マウス・キーボードは含める必要はない。当センターサーバ室において設置・構築に必要となる場合は、当センターが貸与するものを接続して利用すること。
A. 5. 3. 2. 2	本調達機器一式の設置に当たり、A. 5. 3. 2. 1を除いて必要な物品(電源ケーブル、LANケーブル、ケーブルガイド、ケーブルタグ、電源タップ、ラックマウントキット・レール等)は全て、本調達に含めること。
A. 5. 3. 2. 3	ケーブルにはタグを付け、対向機器・ポート番号等を明記すること。ケーブル類は、サーバラックの両サイドやケーブルガイドに丁寧且つ視認しやすいよう配線すること。俗に言うスパゲティ状態や、将来のハードウェア保守やラック内作業の支障になる配線は絶対に行わないこと。配線後にはセンター職員の日視確認を受け、承認を得ること。
A. 5. 4	納品文書
A. 5. 4. 1	以下の文書を納品すること。なお、当センター指定様式はないため、受託者の様式でよい。 <ul style="list-style-type: none"> 設計書(構成図、パラメーターシート、認証情報)
A. 5. 5	動作試験・引き渡し
A. 5. 5. 1	OS・ドライバ・ファームウェア等は、構築時における最新安定バージョンとすること。
A. 5. 5. 2	メーカーから脆弱性や不具合にかかる情報公開、ならびに最新のドライバ・ファームウェア等の提供を受けられること。
A. 5. 5. 3	実機の設定が、設計書(パラメーターシート)に相違ないことを確認すること。
A. 5. 5. 4	動作試験結果を文書にて報告し、当センターの承認を得ること。
A. 5. 6	動作試験・引き渡し
A. 5. 6. 1	本調達機器一式の輸送・設置・養生にかかる費用も全て含めること。
A. 5. 6. 2	本調達機器一式の設置場所は、当センター敷地内のサーバ室である。
A. 5. 6. 3	搬入や設置については、当センター情報統括部の指示に従うこと。
A. 5. 6. 4	受託者は、不要となった梱包物を回収し適切に廃棄すること。
A. 5. 6. 5	受託者は、保守・障害の連絡は日本語で対応し、電子メール又は電話で受付すること。
A. 5. 6. 6	受託者は、オンサイト保守対応を含めること。オンサイト対応は日本語で行い、時間は平日(月～金)の9時から17時とする。
A. 5. 6. 7	設置・搬入経路については、受託者が希望する場合、入札前に申し出ることにより、事前確認を認める。
A. 6	情報セキュリティ管理
A. 6. 1	受注者は、本調達にかかる業務について、以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を契約締結後2週間以内に作成し、当センターの承認を受けること。 なお作成にあたっては、以下の文書類を参考にすること。 <ul style="list-style-type: none"> 「政府機関の情報セキュリティ対策のための統一基準」の最新版 「国立循環器病研究センター 情報セキュリティポリシー」の最新版 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」(SBD(Security by Design))

項番	機能要件
A. 6. 2	サプライチェーン・リスクに十分配慮し、情報セキュリティ対策に支障のない機器およびソフトウェア等を提案すること。 なお機器の選定にあたっては、以下の文書類を参照・分析し、支障のない製品を選択すること。 ・「IT製品の調達におけるセキュリティ要件リスト」 ・「ITセキュリティ評価及び認証制度（JISEC）」
A. 6. 3	新たなサプライチェーン上の脅威が発見された場合に、受注者は当センターに対しかかる脅威についての情報提供を行うこと。
A. 6. 4	受注者の本業務の実施場所について情報提供を行うこと。
A. 6. 5	本業務従事者の所属、専門性(情報セキュリティに係る資格・研修実績等)、国籍に関する情報提供を行うこと。
A. 6. 6	当センターの許可なく、作業の一部又は全部を第三者(再委託先)に請け負わせないこと。
A. 6. 7	本業務の実施に当たり、受注者又はその従業員、本調達の役務の内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。
A. 6. 8	本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。
A. 6. 9	情報セキュリティインシデントへの対処方法を整備していること。
A. 6. 10	本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに当センターに報告すること。
A. 6. 11	情報セキュリティ対策に関する履行状況を再委託先まで含めて定期的に確認し、当センターへ報告すること。
A. 6. 12	情報セキュリティ対策の履行が不十分であると認められた場合、速やかに改善策を提出し、当センターの承認を受けた上で実施すること。
A. 6. 13	本システムに格納されている情報を受託者にて取り扱う場合には、受託者の責により情報セキュリティインシデントが発生した際に、受託者への立入検査又は情報セキュリティに関する監査の受入れについて、対象範囲、実施者、実施方法等を当センターと協議した上で、契約等に含めること。なお、本項は政府統一基準群R5年度版4.1.1に従うものである。
A. 6. 14	当センターから提供する情報を受託業務を遂行する目的外に利用しないこと。
A. 6. 15	当センターから要保護情報を受領する場合は、情報セキュリティに配慮した受領方法にて行うこと。
A. 6. 16	当センターが提供する情報(資料等)は、原則として貸出しによるものとし、本契約終了時まで担当職員の指示に従い、当センターに返却し、当該資料の複写はしないこと。
A. 6. 17	当センターから受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。
A. 6. 18	当センターが提供する情報(資料等)は、情報セキュリティ管理体制の下、第三者への漏えいや目的外利用が行われないよう、適切に管理すること。
A. 6. 19	委託業務において取り扱う情報について、再委託先が閲覧することがないように、受注者は情報を厳重に管理すること。
A. 6. 20	やむを得ず、再委託先において委託業務に係る情報を閲覧する必要がある場合には、受注者は、事前に当センターの担当者と調整し、その指示に従うこと(再委託先における情報の取扱いを含む包括的な秘密保持契約を締結する、作業の都度情報の取扱いについて調整する等)。
A. 6. 21	納入時の確認・検査手続きには情報セキュリティ対策の実装状況を含め、事前に当センターの承認を得て検査を行い、結果を報告すること。
A. 6. 22	情報セキュリティ管理計画書には、情報セキュリティ水準の維持に関する手順や情報セキュリティインシデントを認知した際の対処手順等、情報セキュリティ対策を実施するために必要な手順を含むこと。
A. 6. 23	本基盤にかかる主体認証のパスワードは、複雑かつ推測不可能な文字列を設定すること。具体的には以下の強度を想定しているが、実現が不可能な項目はその内容を明確にし、代わりとなるリスク低減策を提案すること。 ・文字種：英大・小文字(52種類)＋数字(10種類)＋記号(26種類)の計88種類程度 ・規則性：ランダム文字列(前項文字種を混在させ、規則性はなし)を採用 ・文字数：医療情報システムは13桁以上、医療情報以外の情報システムのは10桁以上
A. 6. 24	アカウントロックの機能を実装すること。 不可能な場合はその理由を明確にし、代わりとなる不正な主体認証の試行に対抗するための措置をリスク低減策として提案すること。
A. 6. 25	運用段階へ移行する際に、利用可能なアカウント情報を整理し、それぞれがアクセス可能な範囲を明確にすること。開発・構築時に使用したアカウントを放置しないこと。
A. 6. 26	OSのファイアウォール機能等を使って使用する通信を明確にし、それ以外を使用できないように設定すること。

項番	機能要件
A. 6. 27	導入するハードウェア・ソフトウェアは、本稼動時点で最新のファームウェアや修正プログラム、及びセキュリティパッチを適用の上でシステム動作試験を行い、正常に動作することを検証すること。
A. 6. 28	機器納入時に情報セキュリティ要件を実装していること及び不正プログラムが混入していないことを確認するためのチェックリストを用意し、各項目に対する確認結果を報告すること。
A. 7	提供を求める資料
A. 7. 1	提供可能な範囲で、以下に掲げる一般的な参考資料その他の資料等の提供を求める。なお、全ての項目に回答する必要はないが、電源諸元については必ず資料提供すること。
A. 7. 1. 1	◦ 提供者に関する情報(会社案内 等)
A. 7. 1. 2	◦ 技術提案に関する参考資料(定価・導入実績等を含む)
A. 7. 1. 3	◦ 提案を実現するために必要な費用に関する資料
A. 7. 1. 4	◦ カタログ等
A. 7. 1. 5	◦ 設置条件(電源諸元)に関する資料
A. 7. 1. 6	◦ 納入に要する期間に関する資料
A. 7. 1. 7	◦ 消耗品、光熱水量に関する資料
A. 7. 1. 8	◦ 保守・障害支援体制に関する資料
A. 7. 1. 9	◦ その他必要と思われる資料
A. 8	その他
A. 8. 1	提供された資料等が不明確な場合、技術的要件を満たしていないとみなす。
A. 8. 2	提出資料等に関する照会先を明記すること。
A. 8. 3	本仕様書に定め無き事項又は疑義を生じた場合は、事前に協議の上、その指示に従うこと。