診療現場用インターネット環境

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8年1月

国立研究開発法人　国立循環器病研究センター

診療現場用インターネット環境

仕様書　目次

【重要】仕様書で求める機能要件について

・全てが必須要件であり、開札後の実現不可の申入れには応じない。

・前提や制約がある場合はD列にコメントとして追記すること。

ただし当センターが認めない場合は失格となるので留意すること。

項番	機能要件
A	基本要件
A.1	現行課題と基本方針
A.1.1	国立研究開発法人　国立循環器病研究センター(以下「当センター」という。)は、脳卒中と心臓病の患者様の専門的治療と研究を行っている世界でも有数の施設である。1977年に設置され、2019年7月に吹田市民病院や高齢者向け複合居住施設、健康増進広場、さらにはイノベーションパーク等を擁する面積30ヘクタールの医療クラスターである北大阪健康医療都市(通称健都)に全面移転した。 基本理念は次の三つである。第一は「循環器病の予防と制圧」の国際拠点を目指すこと。第二はOICやイノベーションパークを中心としたオープンイノベーションにより最先端医療・医療技術の開発で世界をリードすること。第三はオープンイノベーションに連動した周辺エリアの産業活性化を起こすこと。これらの基本理念を実現するためのシステム面からのサポートとして各種機能を提案すること。
A.1.2	当センターの情報システムは、その運用目的から2つの情報システムに大別できる。 ・「HIS」…診療を目的とした情報システム群で、インターネットに接続できない環境。 ・「NCVC」…HISを除く業務・研究を目的とした情報システム群で、インターネットに接続できる環境。
A.1.3	2019年7月の移転時に新規構築したHISは約7年の運用期間を経て、2026年9月に新システムに更新予定であり、現在導入作業中である。
A.1.4	本仕様書は、「HIS」というクローズドなネットワークで、インターネット上の脅威から診療情報等を保護しつつ、安全にインターネット利用が可能となるインターネット分離環境を構築することを求めている。
A.1.5	本調達の範囲(前項までの課題と方針を踏まえて、本調達の範囲は以下とする。)
A.1.5.1	ネットワーク設定によりインターネットにアクセスできないHIS用ネットワーク配下の端末(以下、HIS端末という。)から、インターネットアクセスできる環境の構築、および2026年9月から2032年8月までの6年間の保守サービス一式。
A.2	共通要件
A.2.1	全体
A.2.1.1	納入場所は、大阪府吹田市岸部新町の国立研究開発法人　国立循環器病研究センターとするこ
A.2.1.2	良質な医療を効率的に運営するために、より低価格で、より良い医療ICTを調達するという目的に沿った提案を行うこと。
A.2.1.3	同時接続ライセンスの場合は150同時接続、ユーザーライセンスの場合は1300ユーザで使用できるシステムであり、コストの最適化を図った提案であること。
A.2.1.4	本調達は仕様書だけではなく、別表等の他資料の要件も含めて応札すること。
A.2.1.5	本仕様書は全て必須要件であり、機能要件を満たすための費用は、全て本調達に含めること。なお設置にあたって当センター既存ネットワークの変更が必要となる場合は、その内容がわかる資料を提示すること。
A.2.1.6	仕様書の必須項目は、完全に実現できなければならない要件であるが、部分的にできない内容やシステム上の機能が異なる場合は、その旨を記載してシステム上又は運用上での回避方法を明記すること。
A.2.1.7	その提案が合理的であると当センターが判断すれば、仕様を満たしていると判断することもある。ただし、提案内容が不十分であれば、失格となる場合があるので十分に注意すること。
A.2.1.8	デファクトスタンダードを追求したシステム構築を基本とし、システムのOS・通信プロトコル等は国際標準・業界標準を積極的に採用すること。
A.2.1.9	汎用性とシステムの安定性を考慮し、サーバのOSは最新又は同等以上の性能・機能を有すること。最新でない場合は妥当性について当センターと協議の上指示に従うこと。
A.2.1.10	デスクトップ仮想化基盤システムまたはブラウザ仮想化システムとしての稼動実績を有する製品で提案を行うこと。
A.2.1.11	仕様書に記載されていない機能を最新標準機能として搭載している場合は、その利用を前提として機能を提供すること。
A.2.1.12	500床程度の医療機関でHIS端末からインターネット接続環境の導入実績をメーカーとして複数有すること。ただし、提案製品やシステムが最新のソリューションであり稼動実績が要件に満たない場合は、従来の同等製品での導入実績とする。
A.2.1.13	医療情報に関する3省2ガイドラインの最新版に準拠していること。
A.2.1.14	受注者は、本調達提案費用の明細書(ハードウェア・ソフトウェア・導入作業費用・保守費用等の品名、数量、標準価格、提供価格が記載された明細書)を提示すること。
A.2.1.15	本調達システムは、2026年8月末までに確実に納入すること。ただし、動作確認やユーザーへの告知など円滑な展開ができるように導入スケジュールは当センターと十分協議すること。
A.2.1.16	稼動スケジュールは、落札後、当センターと協議の上で決定すること。
A.2.1.17	開札後2週間以内に、詳細なスケジュールとシステム概要説明のためのキックオフ会議を行うこと。

A.2.1.18	キックオフ当日は事前に選定した当センターのWGと運用担当者のメンバーと、受注者の担当者が初回の打合せを行い、次回の打合せ日程を決めること。
A.2.1.19	導入スケジュールは、当センターと十分協議し、導入に当たっては通常業務への影響を最小限にとどめ、病院業務に混乱を起こさず、且つ、当センター職員の負荷が増大しないこと。
A.2.1.20	受注者又は実作業者の責めに帰すべき理由により、当センターと協議により決定した稼動期日に対して遅延が発生した場合は、契約書に規定する条項に沿った損害負担をすること。
A.2.1.21	受注者の自社製品だけで仕様を満たさない場合は、他社製品を使って仕様を満たしてもよい。ただし、受注者は、他社製品を用いて満たす要件も含めて、本仕様書の全要件の内容を把握し、各章にまたがる要件を整理の上、他社製品導入者との役割・業務分担や機能範囲を明確にするこ
A.2.1.22	本調達システムに接続が必要な既存システム及び機器は全て接続すること。
A.2.1.23	既存システムや機器側の接続費用は、本調達に含めること。
A.2.1.24	疑義がある場合には、入札前に質問事項として当センターに提出し、その回答に従うこと。
A.2.1.25	提案するシステムに関し、ハード・ソフトを納入でき、責任を持って構築できる体制を整えること。
A.2.1.26	円滑なシステム本稼動を実現するために、提案システムの構築経験のあるSEによる体制を整備すること。
A.2.1.27	一施設で生じたシステムトラブルの事例を全国の各システムサポートの拠点に通知し、同原因によるトラブルの再発を防止する体制を有すること。
A.2.1.28	仕様書に記載のない機能要件で、標準機能で有する有用で革新的な機能がある場合は、その機能を資料で提示すること。
A.2.1.29	本システムの構成が理解できるように、ハードウェア・ソフトウェア等の構成図を提出するこ
A.2.2	情報セキュリティ
A.2.2.1	情報セキュリティ対策の立案・実施に当たっては、以下の文書への準拠性を考慮すること。なお、文書間に齟齬がある場合、原則として当センターの情報セキュリティポリシーを優先するが、統一基準にある記載内容を考慮することが必要である。 ◦ 「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
A.2.2.2	受託者は、導入及び保守の期間を通じて、受託業務の実施にあたって計画している情報セキュリティ対策を「情報セキュリティ管理計画書」としてまとめること。 本書は契約締結後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、プロジェクト実施計画書・体制図等の一部としても差し支えない。 情報セキュリティ管理計画書には、以下の内容を記載すること。 （必須項目） ・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)、国籍等 ・従事者が利用するPCの管理方法 ・授受した情報・電子ファイルの管理・廃棄ルール、目的外利用の禁止 ・本受託業務の実施場所 ・インシデント発生時の対応フロー・連絡先 （参考文献） ・「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)) ・「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.2.2.3	機器の選定に当たっては、サプライチェーン・リスクに配慮すること。調達後新たなサプライチェーン上の脅威が発見された場合には、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。 （参考文献） ◦ 「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.2.2.4	受注者の資本関係・役員等の情報について情報提供を行うこと。
A.2.2.5	作業の一部又は全部を再委託する場合は、契約前に当センターに許可を求めること。
A.2.2.6	本業務の実施に当たり、成果物に対して意図しない変更が加えられないための管理、および機密情報の窃取等が行われないための管理がされていること。
A.2.2.7	本調達の役務内容を一部再委託する場合は、再委託先に対しても情報セキュリティ管理計画書に準拠した情報セキュリティ対策を実施すること。また再委託先と秘密保持契約を締結すること。
A.2.2.8	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.2.2.9	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.2.2.10	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.2.2.11	当センターが求めた場合に、速やかに情報セキュリティ監査を受け入れること。

A.2.2.12	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.2.2.13	当センターから受領する要保護情報、又は当センターのデータが国内法以外の法令及び規制が適用される環境に保存される場合は当センターの承認を受けること。
A.2.2.14	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.2.2.15	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.2.2.16	納品物に含む運用手順書には、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.2.2.17	納品物には、システム構成情報、取り扱う情報の内容、接続するセンター外通信回線の種別、委託先情報を含めること。
A.2.2.18	リモートメンテナンスが必要となる場合は、原則として当センターが提供するVPN環境で接続すること。当センターVPN環境が利用できない場合は、接続方法について当センター情報統括部と協議の上、決定すること。
A.2.2.19	独自のネットワーク(無線LANも含む)を構築しないこと。その必要がある場合は、理由など必要な資料を提示し、当センター情報統括部長の判断を求めること。
A.2.2.20	ネットワークカードの2枚挿しやルータの導入によるネットワーク分離が必須である場合は、その理由や構成図を示して情報統括部の判断をあおぐこと。
A.2.2.21	納入候補となる機器等については予め当センターに機器等リストを提出し、当センターがサプライチェーン・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、当センターと迅速且つ密接に連携し提案の見直しを図ること。
A.2.2.22	情報システムに当センターの意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、当センターと連携して原因を調査し、排除するための手順及び体制(例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、要求された場合には提出できるなど)を整備していること。これらの手順書、体制について資料を提出すること。
A.2.2.23	仮想化基盤管理ソフトの主体認証のパスワード強度は、本仕様書記載の要件を満たすこと。又、運用保守段階へ移行するに当たっては利用可能なアカウント情報やアクセス可能な範囲のルールを講じること。不可能な場合はその理由を明確にし、代わりとなる措置をリスク低減策として提案すること。
A.2.2.24	アカウントロックの機能を実装すること。アカウントロックされた場合、管理者へ通知ができ、システム管理者によるロック解除か、一定時間経過でのロック解除を設定可能なこと。不可能な場合はその理由を明確にし、不正な主体認証の試行に対抗するための代替措置をリスク低減策として提案すること。
A.2.2.25	一定回数以上のログイン試行を管理者に通知する仕組みを実装すること。不可能な場合はその理由を明確にし、不正な主体認証の試行に対抗するための代替措置をリスク低減策として提案すること。
A.2.2.26	通信要件を明確にし、OSのファイアウォール機能等を使って、それ以外を使用できないように設定すること。具体的には、通信目的（アプリケーション名）、送信元、送信先、通信プロトコル（ポート番号）を文書で示すこと。
A.2.2.27	情報システムのサーバや端末のOS、その他の端末上で稼動させるソフトウェアは、本稼動時点で最新の修正プログラムや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.2.2.28	情報セキュリティ上の問題が発生した際に確認するため、導入するサーバOS及びアプリケーションについてのログを取得すること。
A.2.2.29	システムや機器の納入時に、情報セキュリティ対策の実装状況について確認し、確認結果について情報統括部長への承認を求めること。チェック項目については仕様書にもとづき、構築開始時点で協議により決定する。
A.2.2.30	障害や被災からの復旧後に、その間の利用が適切であったか情報セキュリティの観点でログを監査する必要があるため、受託者はチェックに必要なログの一覧、及びチェック項目手順を提供すること。
A.2.2.31	障害や被災時等、通常と異なる情報システムの利用が想定される。情報セキュリティインシデントの発生リスクを常に低くする対策を講じ、発生時は被害が最小限になるように、手順を作成すること。又、変遷する攻撃手段にも速やかな対策が行えるように情報収集及び事前対策を継続して実施すること。
A.2.2.32	ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とするため、SBOM(Software Bill of Materials：ソフトウェア部品表)を提出すること。または、構成するソフトウェアに関する脆弱性、サプライチェーン・リスクについて確認したSBOMと同程度の効果が発揮できる資料の提示でもよい。実現できない場合は明示し、センターと対応を協議すること。
A.2.3	高可用性

A.2.3.1	本調達システムは、24時間・365日稼動可能であること。ただし、システムのメンテナンス時は除く。
A.2.3.2	メンテナンス等の必要時を除き、再起動の必要がないこと。必要な場合は、その頻度を提案書に記載すること。
A.2.3.7	バックアップからのリカバリ試験を計画し、実施すること。本試験は稼働前に必ず実施し、当センターに稼働判定の条件として結果を示すこと。試験の結果、手順等に問題があった場合には、改善した手順を作成し、成功するまで再試験を行うこと。試験の手順及び結果は記録し、納品すること。
A.2.4	障害対策
A.2.4.1	障害復旧時の保守管理操作をマニュアルにまとめること。
A.2.4.3	停電の回復後には、ハードウェア障害等が発生した場合を除き、通常の電源投入操作のみで全機能が利用できるようにすること。SE等が介在しなければ平常時の状況とできないハードウェア構成、ソフトウェア構成とはしないこと。
A.2.5	ソフトウェア
A.2.5.1	当センターの仮想化基盤(Hyper-V)上に仮想ゲストOSとしてWindows Server 2022/2025を構築する場合のみ、当該ライセンスは当センターが提供するため、本調達に含めないこと。物理サーバで構築する場合や他の有償OS、ミドルウェアについては本調達に含めること。
A.2.5.2	インターネット分離環境を実行するホスト端末（HIS端末）は当センターが別に調達済みであり、そのOSはWindows11 Enterprise IoTである。納品時にはこの環境で動作すること。 導入後の課題発生の際、できるかぎり協力すること。
A.2.5.3	当センターではMicrosoft 365 E3(以下「M365 E3」という。)を契約している。本提案においては、M365 E3のライセンスを活用して重複購入しないこと。（例：CALの購入は不要）
A.2.5.4	ホスト端末（HIS端末）には、EPPが導入済みであるので留意すること。
A.2.5.5	M365 E3に含まれないライセンスが構築に必要な場合は、本調達に含めること。
A.2.6	サーバ・ストレージ
A.2.6.1	当センターの仮想化基盤(Hyper-V)上に仮想ゲストOSを構築する場合は、必要なリソース(CPU,メモリ、ディスク)を提示すること。
	アプライアンス製品の場合は、当センター既設のラック(日東工業FSS110-722EKNヘンケイ)に設置すること。設置に必要な器具は本調達に含めること、また、ユニット数、電源を示すこと。
A.2.7	院内ネットワーク
A.2.7.1	当センターの既設ネットワークに接続すること。
A.2.7.2	当センターの指定したIPアドレス体系を利用すること。
A.3	共通機能
A.3.1	マスタ・コンフィグ管理
A.3.1.1	各マスタやコンフィグ情報のメンテナンスは、当センター職員ができること。
A.3.1.2	各マスタやコンフィグ情報は、権限を与えられた管理者のみが修正、登録できること。
A.3.2	本仮想化基盤やバックアップ等の管理ツールのログイン・認証は、以下のとおりとすること。
A.3.2.1	ログインパスワードの文字種に、以下の条件を満たしたパスワード文字列を設定できること。 "12文字以上かつ文字列中に「英大文字・英小文字・数字・記号」の4種類を含む"(例) ABcd1234!#$%
A.3.2.2	一定時間システムを使用しなかった場合は、自動的にログオフされること。制限時間については、システム管理者で設定できること。
A.3.3	運用管理機能
A.3.3.1	障害発生後の復旧作業に必要となるバックアップ（設定ファイル、データベースのダンプ等）は、自動的に取得すること。その対象と頻度については、当センターと協議の上、了承を得るこ
A.3.3.3	当センターが指定するタイムサーバによる時刻同期ができること。
A.3.3.4	レスポンスタイム(処理応答時間)は、ピーク時においても支障がない構成であること。
A.3.3.5	データ容量が増えても、継続して初期のレスポンスタイムを維持できる構成であること。
A.4	サービスレベル
A.4.1	導入後に大幅な性能不足(速度低下)やリソース不足が発生した場合は、その原因や対応策について当センターとの協議に誠意を持って応じること。

項番	機能要件
B	役務・保守他
B.1	役務
B.1.1	プロジェクト管理
B.1.1.1	管理手法
B.1.1.1.1	管理業務の遂行に当たり、PMBOK(Project Management Body Of Knowledge)又はこれに類するプロジェクト管理体系に準拠したプロジェクト管理を行うこと。
B.1.1.1.2	プロジェクト計画書を策定し、当センターに説明すること。
B.1.1.2	進捗管理
B.1.1.2.1	作業計画に基づき、各タスクの状況把握及びスケジュール管理を行うこと。
B.1.1.2.2	各タスクの進捗状況に関するプロジェクト会議を開催し、当センターに作業状況を報告するこ
B.1.1.2.3	プロジェクト会議では、対象とする作業期間に予定していた全タスクについて作業進捗を報告すること。
B.1.1.2.4	計画から遅れが生じた場合は、原因を調査し、要員の追加及び担当者の変更等の体制の見直しを含む改善策を提示し、当センターの承認を得た上でこれを実施すること。
B.1.1.3	品質管理
B.1.1.3.1	プロジェクト計画書に基づき、設計工程完了時の品質指標を測定した上で、プロジェクト内で評価し、評価結果を当センターに報告すること。
B.1.1.3.2	プロジェクト内に、品質管理を担当する担当者が存在すること。
B.1.1.3.3	上記、品質管理担当者による品質レビューを定期的に実施すること。
B.1.1.4	コミュニケーション管理
B.1.1.4.1	作業工程毎にコミュニケーション計画を策定し、当センターの承認を受けること。なお、コミュニケーション計画では、会議体の目的、開催頻度及び対象者等を明確にすること。
B.1.1.4.2	策定したコミュニケーション計画に基づき、設計工程における各種作業に関する打合せ、成果物等のレビュー、進捗確認及び課題共有等を行うために、当センター職員が出席するプロジェクト会議を開催すること。
B.1.1.4.3	各会議が開催される都度、受注者にて議事録を提示し、原則3営業日以内に提示の上で当センターの承認を受けること。
B.1.1.4.4	議事録にはワーキングで意思決定を行った当センター担当者を明記し、システム稼動後に仕様の検討経緯や決定者の遡及確認が行えるように留意すること。
B.1.1.5	課題管理
B.1.1.5.1	プロジェクト遂行上様々な局面で発生する各種課題について、課題の認識、対応案の検討、解決及び報告のプロセスを明確にすること。
B.1.1.5.2	積極的に課題の早期発見に努め、迅速にその解決に取り組むこと。
B.1.1.5.3	本業務の推進に影響を与えるような重大な課題が発生した場合は、速やかに当センターに報告し、対応策について協議すること。
B.1.1.5.4	課題は表等で一元管理し、当センターと受注者との間で共有すること。課題の内容、影響（重要度）、優先度（緊急度）、発生日、担当者、対応状況、対応策、対応結果、解決日などの他、受注者が必要と考える項目を記載すること。なお、上記の内容で目的とする事を充足するならば、独自の課題管理表を用いて構わない。
B.1.1.6	構成・変更管理
B.1.1.6.1	本システムの整合性を維持し、プロジェクト環境の変更に対するトレーサビリティを確保すること。
B.1.1.6.2	構成管理対象(仕様書及び設計書等)を特定し、管理レベル(参照・更新権限及び保存方法・期間等)を定めること。
B.1.1.6.3	要件と構成管理対象の変更について、双方向に追跡可能な仕組みを確立すること。
B.1.1.7	リスク管理
B.1.1.7.1	技術的観点、進捗的観点、人員的観点や、本システムと類似する案件で発生した問題等から、プロジェクトの遂行に影響を与えるリスクを識別し、その発生要因、発生確率及び影響度等を整理すること。
B.1.1.7.2	発生確率及び影響度に基づき、リスクの優先度を決定し、それに応じた対策を行うこと。
B.1.1.7.3	上記で整理したリスク及び各内容について定期的に監視・評価し、その結果を反映・報告すること。
B.1.1.7.4	リスクを顕在化させないための対応策(対応手順、体制等)を策定すること。
B.1.2	体制・導入
B.1.2.1	体制
B.1.2.1.1	受注者決定後、1ヶ月以内には構築作業を開始できる体制とすること。
B.1.2.1.2	構築時のシステムベンダーの人員体制は、当センターの稼動を十分にサポートできるものであること。
B.1.2.1.3	仮に、当センターがサポートが不十分と判断した場合は、相談により人員体制を強化すること。
B.1.2.1.4	作業開始から稼動までのマスタスケジュール表を当センター役割とベンダー側役割に分けて、詳細な作業分担表を提示すること。
B.1.2.2	従事者

B.1.2.2.1	提案システムのプロジェクトマネージャーは当センター又は当センターと同規模以上(500床以上)の医療機関等において、提案システムの構築経験を有すること。
B.1.2.2.2	プロジェクトマネージャーのこれまでの経歴、及び実績医療機関名や同等規模の機関名を記載して提出すること。
B.1.2.2.3	必要に応じて、実績医療機関に問合せができるように協力すること。
B.1.2.2.4	主担当SEは、当センター又は当センターと同規模以上(500床規模)の医療機関・大学・研究機関等のネットワークにおいて、主担当SEとして5年以上の経験を有すること。
B.1.2.2.5	主担当SEの担当経歴を記載すること。
B.1.2.2.6	体制図の中には、バックグラウンド部分で支援する組織も記載すること。
B.1.2.2.7	担当者に異動・退職等の事案が発生した場合は、当センターにその旨を遅滞なく届け出ること。
B.1.3	導入作業
B.1.3.1	受注者は構築に当たり、当センターの現状の運用を調査し、その結果を基に構築・設計するシステムの説明を行うこと。
B.1.3.2	提案システム導入後の運用においては、当センターの運用担当者目線に沿い、効率性・経済性に優れた提案を行い、当センターと協議の上で決定すること。
B.1.3.3	提案システムの構築に当たっては、当センターと協議・承認の上行うこと。
B.1.3.4	導入時や機能追加・変更時の設計書等のドキュメントを提出すること。
B.1.3.5	セキュリティ・情報保護の観点から、システム構築に携わるSEは全員、当センターの出入りに際し、IDの提示又は名札を着用すること。
B.1.3.6	システム構築に携わるSE全員に対し、提供ベンダーの責任でセンター内の行動に関する倫理・道徳・社会常識的な指導を行うこと。
B.1.3.7	当センターのシステム管理者への引継ぎのためマニュアルを提供し、協議の上、当センターの承諾を得ること。
B.1.3.8	受注者は、プロジェクト会議を必要に応じて開催し、導入の過程・進捗状況・課題対応状況を当センターに報告すること。開催頻度は、当センターと協議の上、決定するものとする。
B.1.3.9	プロジェクト会議には当センター職員を参加させ、その意見の中で適切なものは採用すること。
B.1.3.10	システム導入における設計・構築・テスト等の各工程の完了は、当センター職員も参加するレビュー会議を開催して当センターの承認を得ること。
B.1.3.11	レビュー会議で指摘された内容を真摯に受け止めて迅速に対応すること。
B.1.3.12	システムの稼動は、当センターの確認及び許可によって行うこと。
B.1.3.13	本システムの稼動が確認された後は、保守等の作業に必要となる機器等を除き、速やかに撤収して原状に復すること。
B.1.3.14	導入作業をする場合は、作業日程と体制を事前に当センターに提示し、当センター担当者と協議を行いその指示に従うこと。
B.1.3.15	受注者がサーバ室等の管理区域内へ入退室する際は、当センター所定の手続きを経ること。
B.1.3.16	担当のSEは、システム構築期間中は当センターにて用意するリモート環境を用いて構築を行うことができるが当センターの定める利用規定を順守すること。
B.1.3.17	作業に伴う各室への立入り時には、当センター担当者経由で各部署の責任者に確認を取り、その許可を受け、当センターの業務に支障を来さないように、且つ、患者への迷惑とならないように配慮すること。
B.1.3.19	当センターにて用意するOSを使用する場合、当センターがサーバーに当センターポリシーに基づくIPアドレスを設定するので、設定したIPアドレスに従い構築すること。受注者にてOSを用意する場合、IPアドレスについては、当センターが全体管理しているIPアドレス体系に基づくIPアドレスを受注者で設定し、当センターに申請後、払出しを受けたものを利用すること。
B.1.4	ソフトウェアインストール作業(ソフトウェアは本調達で導入するものとする。)
B.1.4.1	ソフトウェアインストール作業共通要件
B.1.4.1.1	サーバOS等、当センターの事前導入したソフトウェアやドライバは当センターで、本稼動時点で最新の修正プログラムを適用するが、動作確認に協力すること。受注者が導入したソフトウェアは最新の修正プログラムを適用すること。
B.1.4.1.2	ソフトウェア資産管理台帳の作成のために必要な情報を提供すること。
B.1.4.2	サーバソフトウェアのインストール作業
B.1.4.2.1	当センターが管理上必要なソフトウェア・アプリケーションは当センターにてインストールするが、提案システムの稼働に必要なソフトウェア・アプリケーションソフトウェアは受注者にてインストールし、動作確認を行うこと。
B.1.4.2.2	サーバソフトウェアのバックアップの作成及び復旧手順書を納めること。
B.1.4.2.3	サーバ毎に設定した設定情報等の詳細内容を当センターと協議の上、指定の電子媒体で提出すること。
B.1.4.2.4	協議内容・作業内容・動作確認の結果をそれぞれ書面で報告し、当センターの承認を受けるこ
B.1.4.3	クライアントソフトウェアのインストール作業
B.1.4.3.1	提案システムで展開するクライアントソフトは、別途調達するHIS用端末に導入すること。
B.1.4.3.2	HIS端末へのインストールは原則としてマスター端末への導入となる予定であるが、その方法についてはHIS端末を導入展開するベンダーと十分協議し、効率的で確実な方法を取ること。
B.1.5	システム切替計画

B.1.5.1	2026年8月末納品に向けて、HIS端末はリハーサルや事前展開など複数のステップを踏んだ展開になる予定なので、当センターやHISベンダーと協議の上、スケジュールを立てること。
B.1.5.2	システム切替えまでに当センターで事前に検討や準備をすべき重要ポイントを資料に記載し、提出すること。
B.1.6	当センターへの引継ぎ
B.1.6.1	導入前に作成した情報セキュリティ管理計画書に対する履行状況をまとめて書面にて提出すること。
B.1.6.2	最終納品物にウィルススキャンを行い、問題ないことを報告すること。
B.1.6.3	稼動開始前に、当センターのシステム管理者に対し、システム構成、操作・設定方法を含むシステム管理の教育を行うこと。
B.1.6.4	バックアップデータからのシステム回復手順を文書化すること。導入時に最低一度は回復手順の確認テストを当センターにて行うので、協力すること。又、定期的な回復訓練ができるよう書面により適切な方法手順について記載すること。
B.1.6.5	システムを運用する当センター職員又はそれに準ずるオペレータ要員等に対し、システムの運用管理方法等を指導すること。
B.1.6.6	日常的な操作問合せ対応(ヘルプデスク)や、障害発生時におけるセンター内からの問合せ対応、及び障害切り分け等の初動対応の方法に関して教育を行うこと。
B.1.6.7	管理者に対して障害発生時の初動対応の方法に関し、書面により適切な方法手順等についての教育を行うこと。
B.1.6.8	本項各項目の引継ぎ完了の同意が確認できる書面を取り交わすこと。
B.1.7	稼動後の体制
B.1.7.1	切替え直後は、各種の不具合や課題が発生することが想定される。稼動後1週間は不具合や課題を早急に改善できる体制を設けておくこと。必要に応じてメール、電話、Web会議等の対応をおこなうこと。
B.1.8	その他・納品物
B.1.8.1	本件に関わるシステムの試験結果報告書を提出すること。
B.1.8.2	各システムには、システム構成・技術要件の確認、システムメンテナンスを容易に行うために、設計ドキュメントを添付すること。
B.1.8.3	完成図書はシステム稼動開始までに、電子データ(1式とし当センターで編集可能なデータ形式)を提出すること。
B.1.8.4	完成図書は、以下を含めること。なお、本調達で該当しないものについては対象外とするが、その旨を当センターに説明の上、承認を得ること。
B.1.8.4.1	◦ システム全体関連図(クライアント群、サーバ、通信、保存されるデータが分かる関連図)
B.1.8.4.2	◦ 機能仕様書
B.1.8.4.3	◦ 全会議体の議事録
B.1.8.4.4	◦ テスト仕様書兼成績書
B.1.8.4.5	◦ 要件定義書
B.1.8.4.6	◦ 設計書
B.1.8.4.7	◦ システム導入計画書
B.1.8.4.8	◦ 調達ソフトウェア、ライセンス類一覧
B.1.8.4.9	◦ 検証作業計画書及び検証作業結果報告書
B.1.8.4.10	◦ マニュアル・運用手順書類
B.1.8.4.11	◦ 情報セキュリティに関する文書・手順書
B.1.9	用語定義(納品物)
B.1.9.1	◦ 要件定義書：本調達のシステム一式の設計を行うに当たっての機能、非機能要求事項を記載したもの。
B.1.9.2	◦ 設計書：本調達のIT資産管理システム一式のソフトウェア及びサーバについて設計を記したもの。なお、パラメータシートのみの提出は認めない。
B.1.9.3	◦ システム導入計画書：本調達のIT資産管理システム一式について、実施計画を策定して実施方法と手順を明確化すること。
B.1.9.4	◦ 調達ソフトウェア、ライセンス類一覧：提案システムの構築に必要なライセンス及びソフトウェアを記載したもの。　※ただし、当センターが用意するライセンス及びソフトウェアは対象外とする。
B.1.9.5	◦ 検証作業計画書及び検証作業結果報告書：受注者が行う検証作業と、当センター職員が行う検証作業を整理した上で、検証作業計画を策定し、当センターの承認を得ること。
B.1.9.6	◦ マニュアル・運用手順書類：「B.3.1」記載のもの。
B.1.9.7	◦ 議事録：当センターとの会議においては議事録を作成し、3営業日以内に当センターに提出し、内容について承認を得ること。
B.1.10	納品物に対するセキュリティチェックの実施
B.1.10.1	納品時には必ずマルウェアに対するセキュリティチェックを行い、クリーニングした上でその証左と共に納品すること。
B.2	保守
B.2.1	全般

B.2.1.1	2032年8月末までの稼動後6年間の全ての保守費用を本調達に含めること。なお、本調達範囲内での稼動後6年間の追加費用の発生は認めない。
B.2.1.2	本調達に含まれる納品物は、平日時間内（9:00～17:30）6年間の保守対応が取れること。
B.2.1.3	本調達システムの7年目以降の保守費用について、具体的に記載して提出すること。
B.2.1.4	本調達システムの運用を円滑に実現するため、技術的サポートを行える体制を有することを、具体的に書面で証明すること。
B.2.1.5	当センター側の誤操作による障害時の回復作業及び原因不明時の回復作業を支援すること。
B.2.2	保守体制
B.2.2.1	本調達システムに精通した保守体制を整備すること。
B.2.2.2	障害時には必要なログ取得、復旧作業は当センターにて実施するが、発生した障害に対する調査、ログ解析、復旧の手順提示などにより支援を行うこと。
B.2.2.3	保守担当者は、センター担当者または運用支援業者と協力・協調して、復旧操作を支援するこ
B.2.3	ソフトウェア保守
B.2.3.1	本稼動後1年以内に発見されたソフトウェアの瑕疵対応の費用は本調達に含めること。
B.2.3.2	瑕疵対応は当センター担当者と協議の上、その指示により修正すること。
B.2.4	バージョンアップ
B.2.4.1	契約期間中のバージョンアップを行い、プログラムおよび必要な付帯情報を提供すること。バージョンアップ作業は当センターにて実施する。
B.2.4.2	バージョンアップは保守の範囲内で実施できることを前提とし、追加費用が発生しないこと。
B.2.5	運用
B.2.5.1	運用手順に従い、センター担当者が運用を行うが、運用に関する問い合わせについて、保守サポート窓口等を通じて対応すること。
B.2.5.2	本調達システムの障害に対する復旧支援を行うこと。
B.2.5.3	ユーザーからの問合せや、要望、問題点及びそれに対する対応方法に関し、蓄積情報をシステム管理者用に整理、閲覧可能にして運用効率向上を図ること。
B.2.5.4	製品の不具合や障害、セキュリティ上の問題が発生した場合は、情報提供および製品の問題解決に向けて当センターに協力すること。
B.3	手順書・マニュアル
B.3.1	各機能の稼動開始までに、以下の手順書を電子媒体の形式で提供すること。
B.3.1.1	◦ 設定手順書(各種設定パラメータ)
B.3.1.2	◦ システム運用手順書
B.3.1.3	◦ バージョンアップ手順書
B.3.1.4	◦ バックアップ/リカバリ手順書
B.3.1.5	◦ 障害対応手順
B.3.1.6	◦ 正常動作確認手順書(運用手順書に含めてもよい)
B.3.1.7	◦ 製品マニュアル
B.3.2	製品マニュアルについては、以下の要件を満たすこと。
B.3.2.1	本調達で導入する全てのソフトウェアに関するマニュアルを提供すること。
B.3.3	その他
B.3.3.2	上記の手順書・マニュアルは、日本語版で提供すること。

項番	機能要件
C	診療現場用インターネット環境
C.1	機能概要
C.1.1	HIS端末内に隔離されたインターネット接続環境を構築することにより、通常はインターネットへの接続を許されないHIS端末からインターネットにアクセスできる環境を構築すること。（以下、WindowsPCのデスクトップ内に作成する本環境を隔離領域という。）
C.1.2	隔離領域内でインターネットから入手したOffice文書ファイルは、隔離領域内で編集・保存できること。なお、HIS端末にはMicrosoft Officeアプリがインストール済みである。
C.1.3	上記ファイルの保管は、NCVCネットワークのファイルサーバにも安全な状態で保存できること。
C.1.4	HIS端末と隔離領域間のクリップボード共有やファイルのやり取りを禁止できること。
C.1.5	インターネット上の脅威（マルウェア等）が隔離環境からHIS端末に及ばない環境であること
C.1.6	隔離領域を生成するためのソフトウエアは、サイレントインストールコマンドの実行を行うことで資産管理ツールやグループポリシーで展開・削除ができること。
C.2	個別機能
C.2.1	認証機能
C.2.1.2	隔離領域を利用する際の主体認証(ID、パスワード)は、当センターが指定するActive Directory(Windows Server 2025)を用いること。
C.2.1.5	ファイル共有サーバー接続時の認証は隔離領域起動時に認証したID、Password情報を自動で用いること。
C.2.2	基本操作
C.2.2.1	隔離領域内での作業と隔離領域外での作業がユーザーの操作によって切り替え可能であること。
C.2.2.2	隔離領域内と隔離領域外でそれぞれ実行中のアプリケーションをAlt+Tab等のキーボード操作もしくはタスクバーのアイコンクリック等で瞬時にウィンドウを切り替え可能なこと。
C.2.2.3	隔離領域内で実行されたアプリケーションからの印刷処理を制御可能なこと。
C.2.2.4	隔離領域内で実行したアプリケーションは、HIS端末で実行したアプリケーションと視覚的区別が容易であること。一例として、隔離領域側のウィンドウを色で縁取る等を想定している。
C.2.2.5	画面上のアイコンをクリックすると、隔離領域内のアプリケーションを一時的に非表示とする機能を有すること。
C.2.3	インターネットブラウザ
C.2.3.1	隔離領域内でWeb参照を可能とする専用のブラウザを提供すること。（以下、専用ブラウザ、という。）
C.2.3.2	専用ブラウザを利用してWebサイトへアクセスする際は、アクセス先Webサーバーとコンピュータとで直接通信させることなく、専用のゲートウェイを経由した通信経路に限定するなどしてHISネットワークとNCVCネットワークの独立した運用を維持できること。
C.2.3.3	専用ブラウザダウンロードしたOfficeファイルやPDFファイルを開くことができること。
C.2.3.4	専用ブラウザによりダウンロードしたファイルの、隔離領域外への保存を制限できること。また、当該ファイルを編集可能なアプリケーションが隔離領域内において実行可能な場合は、編集後のファイルの隔離領域外への保存を制限できること。
C.2.4	ファイル操作
C.2.4.1	隔離領域内でユーザーがダウンロードした実行形式のファイルは、セキュリティ対策として実行を禁止すること。
C.2.4.2	隔離領域内のファイルを、zip形式（パスワード付き含む）で解凍および圧縮できること。
C.2.4.3	隔離領域外のファイルを、隔離領域内から参照することを制御できること。
C.2.4.4	隔離領域内からファイル共有サーバー内のファイルを編集、保存できること。
C.2.4.5	隔離領域内とファイル共有サーバ間でファイルの移動やコピーができること。
C.2.5	セキュリティ
C.2.5.1	隔離領域内で実行されたアプリケーションが行うファイルの書き換え（保存）やレジストリ値の変更が、隔離領域外の環境には影響を与えないように制御し、コンピュータの環境を保護できること。
C.2.5.2	隔離領域内のプロセスはローカルのプロセスと分離されており、ローカル環境と隔離環境間の意図しない通信を防ぐことができること。
C.2.5.3	隔離領域内で実行されたアプリケーションと、OSや隔離領域外で実行された他のアプリケーション間とのデータ通信（COM 経由によるデータ通信）を禁止できること。
C.2.5.4	隔離領域外のアプリケーションから隔離領域内のデータへのアクセスを禁止できること。
C.2.5.5	隔離領域内のダウンロードファイルや編集済みファイルをセキュアコンテナ型セキュリティソフトウェア終了時に自動的に削除する機能を有すること。
C.2.6	通信制御（ゲートウェイ機能）
C.2.6.1	本調達機能実現のために通信を制御するゲートウェイ機能は以下の要件を満たすこと。
C.2.6.2	ゲートウェイ機能に脆弱性が発見された場合は適宜修正パッチが提供されること。
C.2.6.3	提案システムとゲートウェイ間の通信は全て暗号化通信とすること。
C.2.6.4	提案システムとゲートウェイ間の暗号化通信の強度はTLS1.2/1.3のみ使用可能とし、TLS1.0/1.1による接続を禁止できること

C.2.6.5	ゲートウェイへの接続は、予期しないソフトウェアからの接続を排除できること。
C.2.6.6	ゲートウェイへの接続時に利用する認証システムはActive Directory、LDAPサーバーが選択できること。
C.2.6.7	ゲートウェイはWebベースの GUIで管理できること。Web管理画面へのアクセスは暗号化通信を利用していること
C.2.6.8	ゲートウェイの管理画面へのアクセスには認証（ID/Password）を必要とすること。
C.2.6.9	Web管理画面は日本語で提供されていること。
C.2.7	ログ収集機能
C.2.7.1	提案システムのシステムログ、アラートログ、ステータスログ及びイベント情報、アプリケーションログ等を収集・保管できること。
C.2.7.2	隔離領域内部のファイル操作、アプリケーション起動、印刷、Webアクセス等のクライアント操作ログを取得できること。
C.2.7.3	各ログ情報は、当センターの指定するSyslogサーバに送出できること。
C.2.8	運用保守
C.2.8.1	提案システムは脆弱性対応を含むアップデートプログラムが適宜ベンダーより提供されること。
C.2.8.2	提案システムのアップデートプログラムは資産管理ソフトウェア等を用いての配布、サイレントインストールが可能であること。