第1章 非機能要件(基本要件)	
1.1 当院の今回のシステム構築に関する基本的な考え	
1.1.1 今回調達をするシステムの構成	
1.1.1.1 全般	
1	今回導入(更新)するシステムは、「部門システム」及び「オプション」で構成されるものであると考えている。なお、それらを構成する各システム毎の概要については各項を参照すること。
2	今回更新および導入されるシステムは全て納入後7年を稼働期間とし、「基本要件」に記載された要件を遵守すること。
3	本調達には、システム更新に際して、当院は以下の項目について、各部門システムベンダに対して提供するものとする。 ※ただし、当院との協議のうえ、当院が準備することとしたものに限る。 1. 各部門システムベンダの提案内容に基づく仮想環境用のサーバハードウエアおよびOS(WindowsまたはRed Hat) 2. Oracleデータベースの使用を想定する部門システムベンダの提案内容に基づく物理環境用のサーバハードウエアおよびOS(Windows) 3. 仮想環境サーバ群および物理環境サーバ群に対する無停電電源装置および電源管理ソフトウェア 4. 電子カルテシステムと接続するためのネットワーク環境 5. 電子カルテシステムと共用で使用する部門システム用のクライアント端末 6. 部門システム専用のクライアント端末およびOS(Windows) 7. 部門システム専用の周辺備品
4	本調達には、システム更新に際して当院が指定する運用に必要な以下の業務をすべて含むものとする。 ※ただし、当院との協議のうえ、当院が準備することとしたものは除く。 1. ミドルウェア、ソフトウェアおよび備品の調達、設定、設置 2. ネットワーク機器、各種端末、サーバ等の情報機器の調達、設定、設置、接続 3. 既存システムとの接続および設定 4. 医療機器との接続および設定 5. データ移行作業 6. 操作研修の実施 また、上記にかかるすべての費用を本調達に含めること。
5	医療情報システムは長期的な運用を行うことから、現行取り入れることのできるIT新技術を積極的に反映し、コスト効果、耐障害性に優れたものとすること。長期データ運用も想定して、今後柔軟に拡張対応できるシステム構成とすること。
6	既存システムと同等の機能を有すること。更新に対しては基本的にはハードウエア更新とする。ただし、ハードウエア更新がOS及びソフトウェアのサポート終了等の事情により困難な場合は、バージョンアップまたはデビジョンアップを認めるが事前に当院と協議を行うこと。受注者が既存システムベンダではない場合は、提供されるシステムの開発思想・表現方法・プログラム構造等を説明を行い提案を行うこと。
7	本仕様は、当院の医療情報システム構築のための基本的な項目を記述したものである。受注者は実際に詳細打ち合わせ段階では、利用者の要求を満たすために、本仕様に記載されていない項目であっても、パッケージに備わっている機能、または大幅でない変更により対応が可能な場合は、受注者はその機能を紹介し、当院と協議のうえ導入をおこなうこと。
8	受注者は詳細打ち合わせ段階で、本仕様に記載されている項目が実状とそぐわない、または改善をおこなった方が良いと判断をした場合、当院と協議の上、必要であればその内容を変更し導入をおこなうこと。
9	同様に本仕様書に示す機器類の性能について、当院と同規模程度の急性期病院で使用されている機器と比較して性能が劣ると判断される場合は、当院の運用に支障をきたさない性能の機器を提案すること。
10	全てのシステムは、現在販売されているもので最新のバージョンを提供すること。 ※最新リリース直後のもので稼働安定性に課題がある場合は、十分な開発・フォロー体制をとること。
11	入札時点で生産が終了していない現行商品であるシステムおよび機器を選択すること。稼働後7年間は、保守対応が可能な製品であること。 ※流用するシステムおよび機器に関しては、今回保守範囲の対象外とする。 ※保守対象の詳細は、受注者と協議するものとする。
12	納入時期までにコストパフォーマンスの優れた新製品やハードウェアが出荷された場合、協議の上、新製品へ変更できること。その際追加費用は発生しないこと。
1.1.1.2 システムの考え方	
1	インタフェース連携において、ベンダ間にまたがるデータベースの更新処理は、必ずインタフェースプログラムで行うこと。
2	電子カルテ上の利用者マスタは、各部門システムで可能な限り自動連携できるようにシステム構築を行うこと。
1.1.1.3 ネットワークシステムの考え方	
1	当院が要求するシステムを運用するにあたり、基幹から末端に関するネットワーク設備およびそれらに付随するシステムを想定すること。
2	既設のネットワーク機器および電子カルテネットワーク配線を利用し、新規に行う配線を可能な限り少なくして導入コストの削減に努めること。
3	端末管理、ネットワークの障害監視・管理、コンピュータウィルス対策等の、ネットワーク全体のセキュリティ対策も必要に応じて提案すること。
1.1.2 当院に導入されるシステムが満たすべきこと	
1	ヒューマンエラーを防止する機能や、医療法に基づく記載・入力を促す機能、入力漏れ・算定漏れ防止機能、システム自体のクラウド化など、医療の質、病院経営に寄与するような機能や将来性を備えたシステムであること。
2	利用者指向でメンテナンス性の高いシステムであること。
3	サーバおよびクライアントのOSについては、以下の条件を満たす構成を提案すること。 1. サーバは、Windows Server 2022相当の汎用性および安定性を備えたOSを使用すること。 2. クライアントは、Windows 11相当以上の性能を有するOSを使用すること。なお、Windowsに限定せず、他のOSであっても同等以上の性能・信頼性が確認できる場合は可とする。 3. クライアントOSの修正パッチは、原則として稼働後に適用しないものとする。ただし、電子カルテシステムの運用に重大な影響を及ぼす脅威への対応が必要な場合を考慮し、パッチの適用が可能な構成をあらかじめ用意すること。
4	部門システムベンダが準備するサーバおよびクライアントのOSについては、以下のとおり対応すること。 1. OSのサポートについては、部門システムベンダの責任において、継続的かつ適切に実施すること。 2. セキュリティ上の重大な脆弱性または瑕疵が判明した場合は、OSのアップグレード(バージョンアップ)を含む必要な対策を速やかに実施すること。 3. ただし、当該対策によってシステムの安定稼働に支障をきたすおそれがある場合は、事前に当院と協議の上で実施の可否を決定すること。
5	本導入対象である「部門システム」およびその「オプション」については、当院との協議の上、必要と判断された場合、当該機器に対してOSパッチ等を適切に適用すること。
6	毎日のデータバックアップの際にも、利用中のシステムの中断を伴わない運用がとれること。
7	サーバ・クライアント等の統一的な時刻管理が行えるシステムであること。
8	今回導入するすべてのシステムは、利用者側端末であるクライアントと、データ等を集中管理するサーバとの間で、必要に応じて処理を分散する方式(クライアント・サーバ型等)、または中央サーバで処理を行うWeb型のいずれかであること。

9	すべてのシステムにおいて（特にライセンス数が少ない部門システムについては）、通常利用するライセンスとは別に、管理者が機器の変更や設定変更時の動作・連携確認に使用できるライセンスを、1ライセンス以上確保し、指定する端末に導入すること。 ※当該ライセンスは管理者専用とし、通常の医療業務には使用しないことから、無償であること。
10	事業継続管理の観点から、バックアップ装置に自動的にバックアップを実施すること。
11	バックアップは、業務の中断をおこなうことなく実施すること。
12	バックアップのログ(開始・終了日時、対象データ、容量等)を残すこと。
13	バックアップについては、システム全体のバックアップは必要な際に不定期に実施し、データのバックアップは毎日、定期的に実施すること。また、バックアップ、リストアの手順書およびバックアップ状況の確認手順書を提供すること。
1.2 情報システムの安全管理に関する要件	
1.2.1 法的規制、各種ガイドライン等の遵守、電子保存の3原則の遵守、標準化への対応等	
1	電子カルテシステムと連携する部門システムのうち、対応が必要なシステムについては、平成11年4月22日付け旧厚生省三局長連名通知「診療録の電子媒体による保存について」に定められた三原則（真正性・見読性・保存性。以下「診療録等の電子保存に係る三原則」という）に対応可能なシステムであること。 また、医療情報システム全体として、法令により保存義務が規定されている診療録および診療諸記録を電子的に保存する場合には、診療録等の電子保存に係る三原則を満たすシステムであること。
2	法令またはそれに準ずる規定により保存が義務付けられている診療情報の電子保存については、厚生労働省が定める「電子保存に関する三原則」（真正性・見読性・保存性）を満たすシステムであること。 また、提案にあたっては、上記三原則を遵守するために講じられている技術的対応について、説明資料を添付すること。
3	提案するシステムは、令和5年5月に厚生労働省より公表された「医療情報システムの安全管理に関するガイドライン（第6.0版）」に準拠したものであること。
4	提案するシステムは、「個人情報の保護に関する法律」および、平成29年4月に厚生労働省より公表された「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（令和6年12月一部改正）に準拠したものであること。
5	改ざん防止、患者プライバシー保護を十分に配慮した高度なセキュリティ機能を有すること。
6	個人情報保護法に該当する項目については特に細心の注意を払い、不適切な管理、無断での外部持ち出しを行わないこと。
7	過失による虚偽入力、書き換え・消去及び混同の防止が講じられていること。
8	使用する機器あるいはソフトウェアに起因する虚偽入力、書き換え・消去及び混同の防止策が講じられていること。
9	故意による虚偽入力、書き換え・消去及び混同の防止策が講じられていること。
10	電子保存における真正性を担保するため、今回導入する部門システム、関連機器、各クライアント端末等は、当院が指定する時刻源サーバ(NTPサーバ)から、Network Time Protocol(NTP)により自動的かつ定期的に時刻情報を取得し、必要な機器に対して自動的に時刻同期を行う構成とすること。 また、すべての機器における時刻の誤差は、常時1秒以内に保たれること。
11	保存情報を見読するための手段(汎用ツールでの閲覧)が対応づけられて管理できること。
12	不適切なソフトウェアによる情報の破壊・混同をおこさないためにソフトウェア・機器・媒体の管理が適切におこなわれていること。
13	故意又は過失による情報の破壊が起こらないための機能を備えていること。
1.2.2 システムマスタ管理	
1	本システムで新たに必要となるマスタの初期セットアップ作業の経費は、本調達に含むものとし、作業に当たっては当院担当者と協議の上、その指示に従うこと。
2	認証に必要な全ユーザ登録の初期セットアップ作業は、本調達に含むものとし、作業に当たっては当院担当者と協議の上、その指示に従うこと。
3	各種マスタデータの登録に関しては、原則1回の登録で部門システムを含めた複数システムへの登録が自動でなされる仕組みを考慮し実装すること。やむをえず1回で登録不能な場合には、管理者の負担を軽減する仕組みを提案し実装すること。
4	マスタテーブルは、システム毎に分けられたディレクトリ上に配置され一元管理が可能なこと。
5	マスタの各ディレクトリはアクセス制御が可能なこと。
6	受注者が直轄しているシステムの各マスタのメンテナンスには専用ツールを提供すること。
7	マスタメンテナンスの専用ツールを提供できない部分のメンテナンスについては、当院の指示に従い受託者が行うこと。
8	マスタを新バージョンに更新した際に、そのマスタを使用している部門システム端末においても、速やかに新マスタを参照することができ、かつオーダ処理が行えること。
9	マスタを更新した際には、クライアント端末へマスタデータを配信できること。 ※ただし、マスタ配信が不要なWeb型システムについては、この限りではない。
10	新バージョンのマスタおよびコンテンツの初期登録は、受託者が行うこと。また、本稼働前までのマスタメンテナンスに関しても同様に受託者が行うこと。
1.2.3 レスポンス	
1	部門システムベンダが提供するクライアントのシステム起動時間は、通常 1分以内とすること。(資源配布時間は除く)
2	更新対象の全システムにおける応答速度は、入力系については概ね1秒以内、照会系については概ね3秒以内とする。ただし、多項目にわたる検索や、大量のデータを参照する画面等についてはこの限りではない。なお、患者の診療業務に直接関わる場面においては、業務に支障を及ぼさない応答速度を確保すること。
1.2.4 高度なセキュリティを実現	
1	実質的にノンストップ・ノーダウン運用を実現するシステムであること。
2	システム障害対策の為、システム全体として、ハード的対策とソフト的対策をとること。
3	システム主要部分ではないものの、障害発生により中程度の業務影響を及ぼすおそれのある機器(例：クライアント端末、プリンタ等)であって、かつ部門システムベンダが提供するものについては、事前に代替機を確保する等の対策を講じること。なお、該当対策は、保守レベルおよび費用対効果を考慮した内容とすること。
4	自然災害(火災、地震等)、サイバーテロにより、病院施設に影響があった場合についても、バックアップデータ等から、病院の運営に大きな影響の無いレベルにまで、システムの復旧ができること。

5	管理操作上のリスクに対しては、ID番号とパスワード等による二要素認証により、システム利用者の認証を厳密に行えること。 また、誤操作が発生した場合であってもシステム破壊に至らないよう、適切な操作権限（作業レベル）を設定できること。 なお、当該二要素認証を実施済みのシステム（電子カルテシステム）からのシングルサインオンによるアクセスについては、二要素認証が実施されたものとして扱う。
6	コンピュータウィルス、ハッキング等外部からのネットワークを通じた攻撃及び障害に対応するため、ウィルス対応ソフトやファイアウォール等により保護されていること。
7	各部門システムの専用クライアント端末が接続されるネットワークにおいては、情報漏洩対策およびコンピュータウイルス対策の観点から、外部からのデータ持ち込みおよび外部へのデータ持ち出しを防止すること。 このため、外部入力出力装置（USBメモリ、外付けハードディスク等）は、可能な限り使用できない構成とし、データの入出力は、管理部門において許可を受けたもののみが、集中的に実施することを前提とする。 ただし、各部門の業務上の必要性に応じ、正式な手順を経て許可された部門および端末については、例外的にデータの入出力を認める場合がある。 上記を踏まえ、各端末および部門に対して「入出力不可」「入力のみ許可」「出力のみ許可」「入出力許可」などの権限設定を、集中管理により制御できる機能を有すること。
1.2.5 システムの利用権限	
1.2.5.1 権限設定	
1	職員毎に、ゲストユーザを含む利用者権限設定ができるようにすること。ただし、利用者 IDについては、現行の電子カルテシステムおよびグループウェアまたは他の利用者IDからの移行を考慮し、設定すること。
2	提案システム内で利用者IDのマスタを持ち、IDの利用と管理をおこなう場合は、利用者 ID以外に利用権限、氏名、職種、性別、生年月日、有効または無効、有効開始日、有効終了日、最終利用日等のフラグを設定できるようにすること。 なお、他システムで管理された利用者IDを利用する場合は、この機能は不要とする。
3	すべての業務システムは、特別な指定がない限り、「物理認証（ICカード）または知識認証（パスワード）」に、生体認証（顔認証）を組み合わせた二要素認証方式等によりログイン可能であること。 なお、当該要素認証を実施済みのシステム（電子カルテシステム）からのシングルサインオンによるログインも認めるものとする。
4	利用者IDは、数字6桁以上とし、重複がなく、かつ再採番不可の永久番号とすること。 なお、他システムで管理された利用者IDを利用する場合は、この機能は不要とする。
5	利用者IDの有効設定については使用開始日、使用終了日の設定ができること。 なお、他システムで管理された利用者IDを利用する場合は、この機能は不要とする。
6	パスワードは、英数字および記号混在(大文字小文字の区別不要)の8桁以上とすること。 なお、他システムで管理された利用者IDを利用する場合は、この機能は不要とする。
7	連携をしようとする双方のシステムの連携ではシングルサインオンの機能やURL連携機能などで、シームレスな連携をおこなうこと。
8	利用者アカウント情報は既存の情報を移行して使用することが可能なこと。
1.2.5.2 管理者の権限	
1	管理者の権限を持つ者が以下の操作を容易に行えるようにすること。また、その結果については、画面上で分かりやすく表示し、必要に応じて印刷できること。 1. 利用者及びグループの登録、変更、休止、削除等 2. 許可された利用者・グループのシステム利用状況の把握と確認(使用端末、利用時間、操作内容など)
2	システム管理者が、利用者の認証、端末利用状態の確認(最終起動および利用日時、起動時間等)ができること。
3	システム管理者が、利用者アカウント状態(有効・無効)、氏名、IDを条件に検索し、アカウント情報を照会できること。また、検索結果を CSV形式等のテキスト形式で出力できること。
4	システム管理者が、各システムの管理・操作権限の設定、変更等ができること。
5	権限と機能のマトリクスを作成し、権限設定の状況を一覧できるようにすること。
1.2.5.3 利用者の管理機能	
1	管理者により、利用者アカウントの新規発行、再発行、利用停止等の処理が可能なこと。
2	利用者または職種単位で、利用できる機能や資産の参照権限、更新権限を設定できること。
3	システムの利用者の管理を効率化するため、各利用者を職種単位別にグループ化できること。
4	利用者とその利用者の属しているグループの権限が異なった場合は、原則として利用者個人の権限が優先するような仕組みとすること。
1.2.6 セキュリティ監視	
1.2.6.1 セキュリティ監査ログに係る機能要件	
1	不正アクセス防止および情報漏えい防止のため、今回更新対象のすべてのシステムにおいて、利用者ログイン情報のログが取得できること。
2	セキュリティ監査ログとして以下の内容を記録できるようにすること。 (1) 認証に失敗したシステム及び利用者とその端末、日時 (2) 管理権限を持つ者の操作内容
3	セキュリティ監査ログのうち、アクセスログについては、データベースとして保存する等の処理を行い、管理上必要と思われる複数の項目・キーワード等で検索できること。
4	セキュリティ監査ログ情報の管理・参照は、管理権限を持つ者に限定できるようにすること。
5	取得されたログは、改ざん等ができない仕組みで、運用保守期間内保存すること。
1.2.6.2 操作ログ・アクセスログに係る機能要件	
1	構築する各システムにおける操作ログやアクセスログを抽出、管理できること。
2	いつ、誰(ログイン者)が、どこで(端末等)、何を行った(操作内容)のかをアクセスログとして取得できること。
3	日付、時刻、端末名、操作者ID、操作者氏名の情報がアクセスログデータとして記録されること。
4	アクセスログの照会では、操作者ID、検索期間(年月日、時刻を含む)等の指定で絞り込み検索を実施し、検索結果を一覧表示できること。
5	アクセスログへのアクセス権限の設定ができ、権限のないもののアクセスを許可しないこと。
1.2.7 ベンダに求める基本要件	
1	当院との間で「守秘義務契約」を締結し、協力企業も含めて当院の作業をおこなう者に対し、「個人情報保護法」等の法律を遵守することを指示し、監督をおこなうこと。

2	情報保護の観点から、システム構築において携わるSEは全員、院内の出入りに際し、IDの提示もしくは名札の着用をすること。システム構築に携わるSEは全員、提供ベンダの責任において病院内の行動に関する倫理・道徳・社会常識的な指導をすること。指導方法については、マニュアル化し、全員の承諾を得ること。
3	院内で業務を行う場合、入館日時、退館日時、社名、氏名、立ち入りエリア、目的等を管理簿等に都度記載すること。また、サーバ室に入室する場合には別途管理簿等に記載すること。記載がない場合は、院内での業務またはサーバ室での業務は原則認めないこととする。
4	ノートPCやデモPC等、院外から機器を持ち込んで業務を行う場合は、事前に申請を行うものとする。申請がない場合は、院内での利用は原則認めないこととする。
1.3 開発・教育・保守体制要件	
1.3.1 開発体制	
1	システムの導入計画に支障のないよう、以下の開発体制を提供すること。
1.3.1.1 全般事項	
1	今回導入範囲のシステムについてはもちろん、範囲外の医療情報システムについても充分な導入・開発経験を持つ人材でチームを編成すること。構成はプロジェクトマネージャー→ プロジェクトリーダ→プロジェクトサブリーダ→プロジェクトメンバとする。医療情報システムの導入・開発経験が最低3年以上あり、5年以上の者が過半数を占め、プロジェクトリーダ・サブリーダは10年以上であること。ただし、プロジェクトマネージャはこの限りではない。
2	詳細なシステム別開発導入スケジュールを提示し、発注者と協議の上、決定・調整すること。また、経過・進捗状況については、2週に1回以上の頻度で、発注者へ文書にて報告すること。
3	プロジェクトマネージャはプロジェクト全体を統括し、進捗会議には営業と共に必ず出席すること。
4	プロジェクトマネージャ、プロジェクトリーダは、原則稼働時まで同一スタッフであること。ただし、当院の方針に適さない場合、プロジェクト進捗に支障がある場合においては、担当者の変更を行うこと。
5	各システム/WGの担当者は、原則稼働時まで同一スタッフであること。業務区分によって同一担当者が複数兼任することは可とする。ただし、当院の方針に適さない場合、専門知識に劣る場合、プロジェクト進捗に支障がある場合においては、担当者の変更・追加を行うこと。
6	各システム/WGの初回および重要なポイントとなる回の開催時に、該当分野の専門担当者を出席させること。(特に初回において、基本構造の説明・方針を考慮する上で当院からの質問に的確に回答できる担当者を割り当てること。)
7	プロジェクトマネージャは、システム全体(関連事項すべて含む)の導入マネジメントを主体的に行うこと(進捗管理、導入スケジュール提示、打合せ等の準備など)。 WGや各種協議会合の議題、課題については整理した上で、開催する前に当院担当者へ随時確認を必ず行うこと。
8	システム連携と構成、マスタ設定に関する事項は、WG・協議時に他施設事例や各ベンダの集積知識の中で、当院にとって長期的な視野で効果的なプランをWG時に複数提示すること。 ※病院スタッフへの一方的な各種設定作業や検討依頼の丸投げは認めないものとする。
9	受注者は、当院の瑕疵による場合を除き導入スケジュールに遅延が生じた場合、速やかに(概ね2週間以内)人員の増員や変更・技術的サポートの拡大などの対策を行い改善を行うこと。
10	各担当者は、作業に着手する前に必ず病院担当者の許可を得てから行うこと。作業後は書面により報告を行うこと。
11	受注者は、導入に関する問い合わせ、不具合への対応、指示に対する回答等について、原則として1週間以内に回答・対応内容を提示すること。 ※なお、回答に時間を要する場合は、当日中にその経過および今後の対応スケジュールを報告すること。
12	プロジェクトリーダ、サブリーダ及びプロジェクトメンバは、システムが安定稼働するまでの全行程において、極力入れ替えがないよう配慮すること。やむなき理由により、入れ替えが発生する場合は、発注者へ事前報告を行い、充分な引継を行うこと。また、安定稼働後も、発注者からの要請に応じて協力援助ができること。
13	ユーザインタフェース、OSやアプリケーションの設定等は当院担当者と協議を行い、当院の指示に従うこと。
14	当院それぞれの運用に合わせる協議を、当院各部門の担当者と行い、それぞれの指示に従うこと。
15	協議・WGの議事録は受託者が作成し、1週間以内に当院に提出し、その承認を得ること。
16	確定した仕様は、2週間以内に文書で提出し、当院の承認を得ること。
17	当院はパッケージシステムを元に運用していく方針だが、当院が要求する運用機能が適切かつパッケージシステムにない場合、その機能を充足させるために、パッケージシステムの仕様に合わせることに拘らず解決提案と改善作業を行うこと。
18	パッケージシステムの仕様にあわせるための業務内容の変更は必要最小限に止めること。
19	将来の機能拡張に対応するために、パッケージシステムに関する情報をできる限り公開し提供、支援すること。
20	全てのシステムにおいて、構築中もしくは稼働後に修正・追加・新規プログラムの作業を行った場合は、適応後に必ずベンダで動作確認作業を行い、必要に応じて病院担当者へ報告すること。
21	最終的なシステムの動作テスト(接続、機能、プログラム等)は、発注者の立ち会いのもとに行い、その評価(システム検収)を受けること。
22	品質テストとして、システム単体、結合、総合試験をそれぞれ行うこと。
23	納品するすべてのシステムについて、それぞれのシステムごとに品質テストを行うこと。
24	試験を行う前に、詳細の試験手順を記載したテスト計画書を書面で提出し、当院の承認を得ること。
25	試験後は、試験結果を記載したテスト結果報告書を書面で提出し、当院の承認を得ること。
26	テスト結果報告書には、適宜画面のハードコピー等を貼付すること。
27	テスト仕様は、ソフトウエア要件に記載したすべての項目を確認できる内容を網羅すること。
1.3.1.2 開発環境について	
1	開発作業に当たっては、別途当院が指定する病院内の適切な場所を無償で提供する。ネットワークの仮設配線が必要となる場合には，その経費は本調達に含むものとし、作業にあたっては当院担当者と協議の上，その指示に従うこと。
2	開発機器等の準備および環境構築作業は受託者側で行うこと。
3	開発作業場所には、当院職員が随時立ち入り、開発状況の確認を行えること。
4	仮のデモシステム等を常設し、打ちあわせ等で画面を見ながら運用検討を行える環境を整えること。
1.3.1.3 ハードウェアの設置・設定作業要件	

1	機器等の搬入、設置、廃棄等の作業に当たっては、病院業務への妨げや、患者への迷惑とならないよう、かつ、施設を毀損することのないよう十分な注意を払うとともに、受注者が立ち会うこと。
2	受託者は、機器等の設置作業の日程と体制を事前に当院に提示し、当院担当者と協議を行った上、その指示に従うこと。
3	機器管理名称、管理番号、IPアドレス、ドメイン名の付与については、当院との協議の上決定したものを使用すること。
4	端末名称、備品情報を含めた管理シールを作成し、今回更新となる機器等に貼付すること。管理シールに記載する項目は、当院より別途指示する。
5	機器設置後は、サーバ機器、パソコン、プリンタ等の設置図面、配線図面、ラック搭載図等のドキュメントを提出し、当院の承認を得ること。
6	機器等の設置場所については、当院と協議の上調整すること。
7	必要となる電源については、原則として既設の電源を使用すること。ただし、万一電源工事が必要となる場合は、受注者の責任と負担において実施すること。 ※既存のOAタップの流用は可とする。
8	新規のネットワーク配線はタグにより明確に示し、かつ、通行に支障がないように施行すること。
9	今回の調達にて導入するすべての機器について、設定作業後に動作確認を行うこと。 (ハードウェア、ソフトウェア両方)
10	本システムを構成する機器のうち、相互通信が必要である装置間の接続に関しては、通信テストを含む動作確認を行うこと。
11	既設ネットワークとの仮設配線が必要となる場合には、その経費は本調達に含むものとし、作業に当たっては当院担当者と協議の上、その指示に従うこと。
12	仮稼働期間が終了し、本システムの本稼働が確認された後は、保守等の作業に必要となる機器等を除き、速やかに撤収し原状に復すること。
1.3.2 教育体制	
1	システムの導入計画に支障のないよう、教育体制を提供し、利用職員にシステム操作を習熟させること。
2	当院グループウェア上に保管可能な形式で、操作教育に使用可能なコンテンツを提供すること。
1.3.3 保守体制	
1	システムの安定稼働に支障のないよう、保守体制を提供すること。
1.3.3.1 全般事項	
1	年間保守契約とし、次年度以降に関しては請負業者と4月1日付けで契約を締結すること。拘束期間は覚書にて保証すること。なお、当年度に発生するトラブル対応等に係る費用はあらかじめ導入費用に含めておくこと。
2	部門システムと、本システム、ネットワークとの障害切り分けが困難な事象については、各ベンダとともに原因究明を主体的に実施すること。
3	保守に関しては、提案時にSLA(サービス内容と価格)を提出すること。
4	リモート保守の対応時間は、月曜日から金曜日の午前9時から午後5時30分までとし、保守要員による対応が可能であること。 ただし、国民の祝日、国民の休日、年末年始、ならびに部門システムベンダが別途定める日を除くものとする。 なお、緊急障害時については、上記にかかわらず別途対応が可能であること。
5	システム全体を通じて、全ての保守連絡窓口が1本化されていること。また、平日・休日に関わらず、24時間同等の体制が取れること。
6	システムに障害が発生した場合、保守要員(CE及びSE)は即座に問題を切り分け、病院における一次対応の指示をした上で、復旧に必要な措置を取ること。 また、速やかに原因を究明し、再発防止及び対応策を発注者へ文書にて報告すること。
7	致命的ではない障害履歴に関しても別途管理し、運用状況を毎月1回発注者に報告すること。
8	リモート保守システムを構築する際、クローズドネットワーク(専用線・VPN等)に対応できる仕組みを導入すること。また、当院構築予定であるリモートメンテナンス集約システムに接続できること。仕様に対しては別途提示する。
9	リモート保守で利用する端末は特定の端末に限定することとし、リモート保守以外の用途では利用不可とする。なお、その端末にはあらかじめ必要なソフトウェア等をセットアップする必要があるが、ソフトウェアライセンスについては無償で貸与すること。
10	リモート保守を実施する際、事前に作業申請書を提出して作業内容を明確にし、作業完了後には作業報告書を提出して作業実績を明確にすること。なお、ベンダ内にリモート接続管理簿を用意し、リモート接続の実績管理を行うこと。 ※年間保守契約の作業実績として、リモート保守対応の実績が公開可能であること。また、保守費用については、スポット対応に換算した場合の金額を提示できること。
11	現地保守を実施する際、事前に作業申請書を提出して作業内容を明確にし、作業完了後には作業報告書を提出して作業実績を明確にすること。なお、ベンダ内に現地保守管理簿を用意し、現地保守の実績管理を行うこと。 ※年間保守契約における作業実績として、現地保守対応の実績が公開可能であること。また、保守費用については、スポット対応に換算した場合の金額を提示できること。
12	対象機器の各種ログの管理を行い、適時アドバイスを行うこと。
13	部門システムベンダが提供するハードウェアおよびソフトウェアは、7年間の継続使用を前提とし、最低7年間は保守業務を保証すること。 ※ハードウェアについては保守部品等の調達を含み、ソフトウェアについては法令改正等に伴うメンテナンス対応を含むものとする。
14	他病院で起こったトラブル事例が整理されていること。トラブル発生時は全国の各拠点に通知し、同じ原因でトラブルが起こらないよう管理する体制を有するとともに、重大なトラブルについては速やかにユーザが把握できるよう障害情報を公開する仕組みを有すること。
15	リモート保守センター(サポートセンター)内の施設レベル(セキュリティ、環境、拡張性他)として、静脈認証等の生体認証装置によるサポートセンタルームへの入室、退室管理が行えること。
1.3.3.2 ハードウェア保守内容	
1	本項は、当院との協議により、部門システムベンダが準備することと決定したものに限る。
2	定期保守と障害復旧を保守要員(CE)が出張して実施すること。
3	システムの安定稼働を保つために、ハードウェア及びネットワークの定期的な予防保守を行うこと。これらの作業は、原則としてシステム運用時間外に行うこととし、定期的点検時間については、発注者と協議の上、事前に決定すること(24時間/365日稼働のシステムについては、病院業務に極力支障を来さない時間を設定すること)。また、保守点検終了後は、速やかに発注者へ文書にて報告すること。
4	ハードウェアの故障については、主要部品の障害発生を病院スタッフが認識できるサービスを提供すること。(例:パトライトや自動メッセージ、監視ベンダからの電話連絡など)
5	定期点検回数は、サーバは半年に1回程度行うこと。

6	機密保護及びコンピュータウイルス感染に対して充分な対策が講じられていること。また、異常が発生した場合は、保守要員(CE及びSE)と連絡を取り、速やかにシステムの復旧に当たること。
7	不具合が発生した場合は、発注者と協議の上、必要部材・機器の交換・修理を行うこと。また必要に応じて機器の再設定を行うこと。対象機器の復旧の際には、原則として直近のバックアップの状態に復旧すること。(保守対象のものに関しては、請負業者選定後、保証期間を決定する。保守対象外のものに関しては、無償保証期間を1年間とする)
8	サーバに関係ない部分のメンテナンス・バージョンアップ等を行う際、全システムを停止しないように行うこと。
9	ハードウェアに関する障害において即時の修理ができない場合、予備機の提供等による速やかな障害対策ができること。
10	ハードウェアの修理、交換を行った際、必要に応じてサーバおよびクライアントの再設定を行うこと。(原則として、直近のバックアップの状態に復旧すること)
11	ハードウェア障害対応時の作業報告書を作成し、作業実施後3日以内に当院に提出すること。
12	コンピュータ関連の技術、製品等の最新技術情報を定期的に提供すること。
1.3.3.3 ソフトウェア保守内容	
1	ソフトウェア(OS、各種OA機能ソフトを含む)の定期的なバージョンアップ(法令改正対応を含む)情報を遅滞なく提供すること。また、システムの変更に際しては、病院業務に極力支障を来さないよう配慮するとともに、変更内容について充分な説明、支援を行い、文書にて発注者へ報告すること。
2	全てのシステムに関し、サーバソフトウェアについて、管理すべきパラメータの確認およびチューニングを定期的に行うこと。特にデータベース等のファイルの肥大化によるシステムおよびアプリケーションの稼働領域の空き容量枯渇には留意しておくこと。
3	本調達に関する機能に障害が発生した場合は、当院担当者と協義の上、その指示により速やかに障害の回復を行い、対応方法および作業報告を当院担当者へ書面にて提出し、その承認を得ること。なお、障害の内容によっては定例会での報告を行うこと。
4	OSを含むシステムプログラム(プログラム・プロダクト保守)に関して、バグ修正対応を行うこと。
5	医療情報システムパッケージ(医療プログラム・プロダクト保守)に関しては、バグ修正対応および軽微な改善修正(発注者との協議に基づく)を行うこと。また、必要に応じて、発注者と協議の上、本稼働後も安定稼働が確認されるまでSEを常駐させ、バグ対応および改善対応を行うこと。なお、「安定稼働」の定義については、請負業者の選定後、発注社との協議の上で決定するものとする。
6	システムに関わる法令改正(診療報酬改定、薬価改正を含む)が公示された場合は、速やかに対応し、施行前にシステムの変更を完了し、運用に支障を来さないこと。なお、利用開始日等を設定し、自動的に作動する状態にあること。また、抜本的な法令等の改正があった場合、極力費用は発生させないこと。
7	保守の範囲として、医療改定に伴うプログラム変更、薬価・点数マスタを提供することを含むこと。
8	定期的なシステム連絡会を開催し、システムの運用状況、問題点及び改善案の報告を行うこと。開催の頻度は、導入当初は週1～2回程度、3ヶ月後は月2～4回程度、6ヶ月後は月1～2回程度、以降は2ヶ月に1回程度とすること。
9	システム運用・開発・管理に関する質問に対して、適切な回答・助言・改善案を提供すること。
10	代替品からもとの端末に戻した際に再セットアップを行うこと。
1.3.3.4 その他	
1.3.3.4.1 請負期間について	
1	初年度の契約については、契約日と同日を着手日とし、翌年度の3月31日を完了日とすること。(本稼働は、令和8年8月～令和9年1月の間で予定)
1.3.3.4.2 提出見積書への記載事項について	
1	以下の項目について、年度別に費用を算出し記載すること。 1. ハードウェア保守料(7年分) ※部門システムベンダで準備した機器に限る 2. ソフトウェア保守料(7年分) 3. リモート保守・監視費用(7年分)
1.3.3.4.3 仕様書に記載のない事項について	
1	仕様書に記載のない事項については、別途協議の上決定すること。

第2章 機能要件	
1 多要素認証	
1.1 全体事項	
1	更新対象となるシステムは、「1. 基本要件」の仕様各事項を遵守したうえで、本詳細仕様項目を確認・実施すること。データ保存年数やデータ移行に関しては、最低限「1.基本要件」に準ずるものとする。
2	本仕様は、システム構築のための基本的な項目を記述したものである。受注者は実際に詳細打ち合わせ段階では、利用者の要求を満たすために、本仕様に記載されていない項目であっても、パッケージに備わっている機能、または大幅でない変更により対応が可能な場合は、受注者はその機能を紹介し、当院と協議のうえ、導入をおこなうこと。
3	既存システムにおける機能内容は、次期システムにおいても原則としてそのまま継承すること。ただし、受注者より提供されるシステムの開発思想・表現方法・プログラム構造等の根幹に関わる理由により異なる場合には発注者と請負者にて協議の上、変更可能とする。
4	全てのシステムにおいて(特に少数ライセンスの部門システム)、通常利用するライセンスとは別に、管理者が機器変更や設定変更時の動作・連携確認に利用できるライセンスを1ライセンス以上確保し、指定する端末へ導入すること。
5	既存機器で流用可能なものは流用し、調達コストの削減に努めること。流用時、買換時に必要なシステム設定等の対応は、保守契約期間中に随時行うこと。
6	今回調達するシステムのリモート保守を行う場合は、クローズドネットワーク(専用線・IP-VPN等)利用を基本とする。
1.2 基本要件	
1	本システムは、ユーザがクライントPCを利用する際に、認証強度が高い方式を用いて本人認証を行うことを目的とする。なお、ユーザ管理・認証方法等は、運用面も含め，効率的で利便性の高いシステムであること。
2	本件の調達範囲は、多要素認証を使用する上で必要なミドルウェア、ソフトウェアおよび備品の設置、情報機器の設置・設定・接続作業を全て含むこと。
1.3 基本事項	
1.3.1 全般	
1	利用者認証の認証方式は、「物理認証（ICカード）または知識認証（パスワード）＋生体認証（顔）」の二要素認証であること。また、運用を考慮して端末により、「ID＋パスワード」での認証も設定可能であること。また、本認証で使用するIDは電子カルテシステムの利用者IDとし、それに紐づいたICカードが利用可能な機能を有すること。
2	生体認証（顔）については、ノートパソコンは端末搭載カメラを使用し、デスクトップパソコンについては認証用カメラを計530台準備すること。なお、認証用カメラの性能については1.3.5項に記載する。
3	一人の利用者に対して、複数のアカウント情報（異なるIDとパスワード）を登録可能であること。また、電子カルテより起動されたアプリケーションは、シングルサインオンで使用することが可能であること。
4	アカウント情報は、当院でメンテナンス可能であること。
5	利用者の有効期間については終了日を設定できること。
6	認証システムサーバとクライアント端末間の認証情報の通信は暗号化などの方法によりセキュリティの高い方法を利用していること。
1.3.2 顔認証	
1	メガネ及びマスク装着状態でも顔認証が可能であること。
2	顔認証処理は、サーバ側で処理可能な仕組みであること。
3	許容最低照度は、約100Lux程度であること。
4	顔向き角度の最大許容検出範囲は、左右±45°、上下±30°、回転±90°であること。
5	認証用顔テンプレートは、10個保存可能で、認証の都度、スコアの良いテンプレートに置き換えることで、経年対策が可能であること。
6	認証用顔テンプレートの登録ツールを提供可能であること。
7	認証用顔テンプレート登録ツールは、ID＋パスワードで本人確認実施後、顔を撮影して登録可能であること。
8	顔写真から認証用顔テンプレートを登録することも可能であること。また、本機能は、一括登録や差分登録に対応していること。
9	将来的な拡張のため、モバイル端末でも利用できるように組込み用モジュールの提供が可能であること。
1.3.3 パスワード管理機能	
1	一定時間に指定回数のパスワード間違いをした場合は、アカウントロックをし、ログインできないように設定可能であること。また、一定時間及び指定回数は設定・変更可能であること。
2	パスワード間違いによりアカウントロックされた場合は、管理者により解除することも可能であること。
1.3.4 電子カルテシステム連携機能	
1	認証実施後、電子カルテシステムへのシングルサインオンを考慮し、ログイン者情報を電子カルテシステムに通知可能であること。
2	電子カルテシステムからログアウト情報の通知を受信した場合、端末からログアウトし認証システムのログイン画面に遷移可能であること。
3	電子カルテシステムの離席操作後、通知を受信し認証システムのロック画面に遷移可能であること。
4	電子カルテシステムの利用者切替ボタンを押下した場合、認証システムの認証画面に遷移し次の利用者が認証を実施後、次の利用者のログイン済み電子カルテに遷移可能であること。
1.3.5 顔認証用Webカメラ	
1	90万画素以上の有効画素数を備えていること。
2	720p(1,280x720ピクセル)以上の解像度を備えていること。
3	30fps以上のフレームレートを備えていること。
4	USB2.0以上の有線接続に対応すること。
5	プラグアンドプレイにより、一般的なOS(Windows10以降)にて標準ドライバで利用可能であること。
6	USBバスパワーにより動作し、外部電源を必要としないこと。