

医療情報共有プラットフォーム構築Ⅰ期 要求仕様書

平成 30 年 7 月 4 日

大阪府立病院機構 本部事務局

目 次

第1章 調達件名	4
第2章 作業の概要	4
1. 開発作業のタイプ分類	4
2. 背景と目的	4
3. 用語の定義	4
4. 業務の概要	4
5. 現行システムの概要	5
6. 調達の範囲及び情報システム化の範囲	5
7. 作業内容・納入成果物	7
第3章 開発するシステムの要件	10
1. 業務機能要件	10
2. 画面要件	12
3. 帳票要件	12
4. 情報・データ要件	12
5. 外部インタフェース要件	13
6. 規模要件	13
7. 性能要件	13
8. 信頼性要件	13
9. 拡張性・柔軟性要件	14
10. システム中立性要件	14
11. 事業継続性要件	14
12. 運用性要件	14
13. 保守性要件	14
14. 情報セキュリティ要件	15
第4章 開発するシステムの稼動環境要件	17
1. 全体構成	17
2. データセンター構成	17
3. ハードウェア構成	17
4. ソフトウェア構成	18
5. ネットワーク構成	18
第5章 テスト作業要件	19
1. テスト計画書の作成	19
2. テスト実施要件	19
第6章 開発作業体制及び作業方法	21

1. 作業体制	2 1
2. 開発方法	2 1
3. 実装	2 2
4. 教育と引継ぎ	2 2

第1章 調達件名

医療情報共有プラットフォーム構築 I 期

第2章 作業の概要

1. 開発作業のタイプ分類

- ア) 開発の形態：新規、再構築；大規模追加修正；中小規模追加修正；リファクタリング
- イ) システム化対象範囲：新規、拡げる；変わらない
- ウ) 事務フロー：新規、大幅な改善；若干の改善；変わらない
- エ) 開発方式：ウォーターフォール；スパイラル；パッケージ；ストレートコンバージョン

2. 背景と目的

近年の ICT の急速な進展を踏まえ、システム化による生産性向上と患者様の利便性向上を目指した取組みをすすめ、生体認証を用いた患者認証を行い、受付から会計に至るまでの各所で患者さまの手間や時間の短縮化、また患者さまの医療情報は患者さまのものという基本理念のもと医療情報共有化を図り、構築は段階的（I 期・II 期以降）に進める。

他にも患者さまと医師、看護師をはじめとした医療従事者、そして医療と関連する企業さまとの円滑なコミュニケーションを可能にするプラットフォーム化をすすめ、さまざまな医療サービスを必要とする患者さまと、そのサービス提供によって自らの事業価値を高めたいと考える民間事業者さまとを結びつける基盤となり、新たな事業機会を創出することも目的としている。

< I 期 >

患者さま固有の ID とクレジットカード情報を医療情報共有プラットフォームで管理し、会計での待ち時間の短縮を目指す。

- ①クレジットカード決済サービス利用
- ②患者さまサービスの向上（会計待ち時間短縮）

< II 期以降 将来構想 >

下記項目の中から優先順位を付け、順次実現していく。

- ①生体認証
- ②コミュニケーションツール（SNS ツール）利用
患者さまサービスの向上（コミュニケーションサイトでの交流）
- ③治療・検査予約の事前通知
患者さまサービスの向上（リマインド）
- ④調剤薬局との処方連携
患者さまサービスの向上（電子処方箋対応、持参薬連携）
- ⑤在宅見守りサービス
患者さまサービスの向上（遠方からの生存確認）
- ⑥医療情報共有化（災害やセカンドオピニオンを求める時など、
患者さまが必要とする時に利用できる仕組み作り）、
- ⑦国で検討している医療等 ID との連携、⑧ 5 センターへの展開

3. 用語の定義

- (1) 「パーソナル ID」とは、各医療機関や診療所、調剤薬局や一般企業とで保有している患者 ID を名寄せし、一元管理されたプラットフォーム基盤上の固有の ID を示す。
- (1) 「当センター」とは、大阪国際がんセンターを示す。

4. 業務の概要

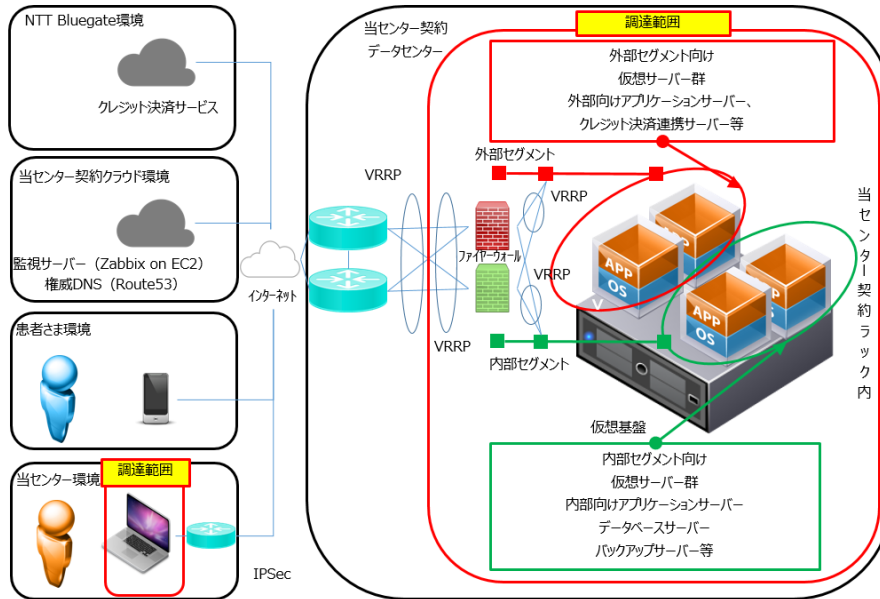
当センターでは、患者さまの会計に関連する主な業務として、以下の(1)～(4)を行っている。今回のシステム化により、前述の目的に沿った業務の流れに変更することを想定している。

- (1) 患者登録業務
新患登録を行う。
- (2) 会計業務
外来、入院における会計計算を行い、請求金額を確定する。
- (3) 収納業務
患者さまから、現金、クレジットによる収納を行う。
- (4) 未収金管理業務
患者さまへの請求で、未収金が発生した場合、未収金を管理する。

5. 現行システムの概要

現在のネットワーク構成を含めたシステム概念図を下記に示す。

図1 現行システム概念図



6. 調達の範囲及び情報システム化の範囲

(1) 調達の範囲

- ① アプリケーション開発を含めた情報システムの構築・テスト
- ② 当該アプリケーション稼動のためのシステム設計
- ③ 上記システム設計を実現するためのハードソフト等調達
- ④ クレジット決済機能 (NTT データが運営母体となっている『CAFIS BlueGate サービス』) 調達 (初期費用のみ)
- ⑤ 上記の関連作業
- ⑥ アプリケーション、ハードウェアについては、5年分の保守費用も含む

注意：データセンターについては、当センターでハウジングサービスを調達し用意する。
本調達にはデータセンターに設置するサーバーハードウェアやラック内で必要なスイッチ類は含まれるが、それ以外のラック自体やUPS（無停電装置）については、本調達には含まない。

(2) システム化対象範囲

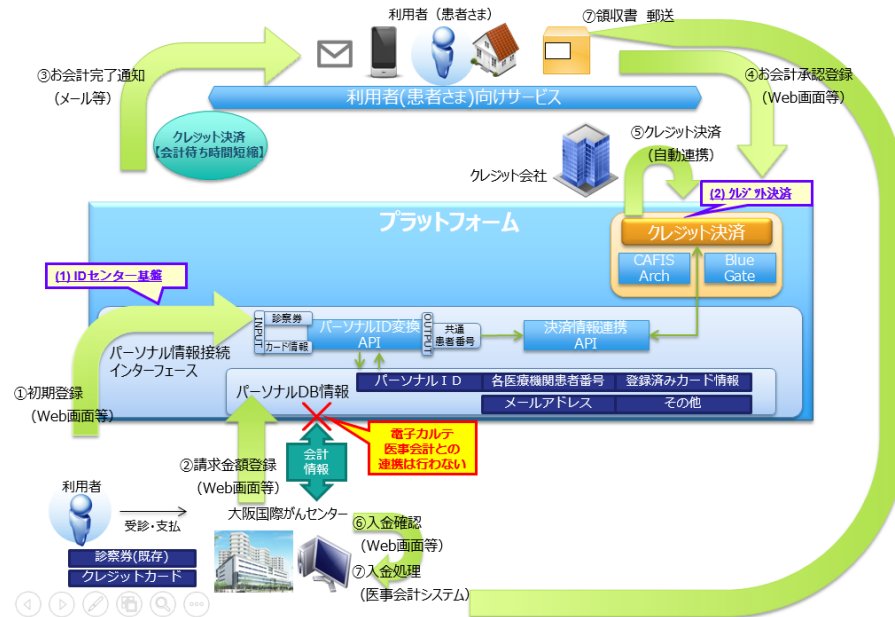
今回のシステム構築は、将来のⅡ期構想、Ⅲ期構想を踏まえ、Ⅰ期構想におけるID基盤の構築と、クレジット決済機能（NTT データが運営母体となっている『CAFIS BlueGate サービス』）を利用したシステム構築を目的としている。将来構想を踏まえた、システム概念図を下記に示す。

図2 システム概念図（将来構想）



上記の内、今回の調達範囲となるⅠ期構想を踏まえた、システム概念図を下記に示す。

図3 システム概念図（Ⅰ期構想）



7. 作業内容・納入成果物

(1) 作業内容

本調達では、平成 31 年（2019 年）3 月の医療情報共有プラットフォームの本稼働に向け、要求分析確認、基本設計、詳細設計、プログラム製造・単体テスト、結合テスト、総合テスト、運用テスト、インフラ構築に係る各作業を行う。

以上を行うに当たり、良いと思われる具体的な方策があれば、提案すること。以下の個々の仕様箇所に分散して記述しても構わない。

図 4 開発スケジュール予定

年	2018年			2019年			
月	10月	11月	12月	1月	2月	3月	4月
要求分析確認							
基本設計							
詳細設計							
プログラム製造・ 単体テスト							
結合テスト							
総合テスト							
運用テスト							
仮稼働							
本稼働							
インフラ構築							

(2) 納入成果物及び期限

ア) 納入成果物一覧と期限

本調達で想定される納入成果物と納入期限は下表のとおりとするが、応札希望者がパッケージ等を用いることで作成できない成果物がある場合、提案書において、その旨理由を記載すること。また下表以外にも運用・保守上、必要な成果物がある場合は、提案書において記載すること。応札希望者がパッケージ等を用いる場合でもアドオンする機能部分は、ソースコードや設計書等を提出すること。

また納入成果物は書面・電子媒体とする。

書面での提出書類は、原則として A4 判とし、日本語で記載すること。部数は、正 1 部及び副 3 部とし、電子媒体 3 部を併せて提出すること。原則として、媒体の種類は、CD-R とし、ファイル形式は、「ワード」、「エクセル」、「パワーポイント」（ともにバージョン 2013）を基本とすること。これ以外の形式を利用する場合は、当センターと相談すること。

なお、専門用語には必ず説明を付すこと。

表1 納入成果物及び納入期限

開発作業 範疇 ^{はんちゆう}	成果物 範疇 ^{はんちゆう}	成果物名・内容説明	納入期限
計画	プロジェクト計画書	プロジェクト計画書（各工程の作業内容と手順、管理手順・方法（決定ルール、連絡、会議体等）、スケジュール、体制図、役割分担等を記載）	平成30年10月26日
業務・機能設計 システム方式設計 情報・データベース設計 ユーザインタフェース設計 外部インタフェース設計 ネットワーク設計 画面・帳票設計 性能・規模設計	基本設計書	要件定義確認書（確定版） 業務フロー（確定版） システム方式・構造設計書 データ項目辞書 論理データモデル又はER図 画面遷移図 画面・帳票一覧 外部インタフェース仕様書 機器類調達要件定義書	平成30年11月16日
	詳細設計書	データベース設計書 トランザクション定義書 データフロー定義書 画面・帳票設計書 各種環境設定定義書 プログラム構造図 運用設計書	平成30年12月7日
開発	開発標準	コーディング標準 共通部品	平成30年12月21日
	プログラム設計書	プログラム仕様書 仕様変更管理表	
	ソースコード		
	実行プログラム一式		
情報セキュリティ	情報セキュリティ設計書	情報セキュリティ設計書 セキュリティ確認テスト報告書 セキュリティ作業環境管理表	平成30年12月21日
テスト	テスト計画書	各テスト毎計画（合否判定基準付） テスト実施報告書 品質報告書（バグ・テスト消化曲線） テスト管理ツール テストデータ、テストスクリプト	平成31年2月8日
	テスト実施管理 品質評価		
	テスト作業		
運用・保守	運用設計書	運用設計書	平成30年12月7日
	操作マニュアル 教育教材	システム管理者、利用者向けマニュアル（運用引継ぎの文書含む） 運用操作研修実施計画書	平成31年1月18日
	システム運用手順書	運用マニュアル（通常時（稼働・停止手順）、障害時（ログ取得、障害時の再起動手順等））	平成31年1月18日

開発作業 はんちゅう 範 疇	成果物 はんちゅう 範 疇	成果物名・内容説明	納入期限
	システム構築手順書（開発環境・本番環境）	サーバー構築手順書（OS 設定、ミドルウェア設定等） アプリケーション構築手順書（アプリインストール等） ※開発環境用と本番環境用	平成 31 年 1 月 18 日
インフラ関連資料	インフラ運用手順書	インフラの運用担当者が運用保守を行うためのサーバー・ネットワークの監視サービス（死活監視、リソース監視等）の運用手順と障害発生時の対応手順をまとめたもの。	平成 31 年 1 月 18 日
	ネットワーク機器設定仕様書	ネットワーク機器のインターフェース設定、VLAN 設定、その他設定情報の仕様書。	平成 31 年 1 月 18 日
作業体制、プロジェクト管理及び会議等の資料	担当者名簿	担当者名簿（WBS に対応付け）	プロジェクト開始後 1 週間以内
	体制図	作業、機密保持、品質管理など	プロジェクト開始後 1 週間以内
	管理表	WBS の作業工数予実績管理表 文書管理、ガントチャート進捗管理、品質管理、課題・問題管理、変更管理及び構成管理等（定例会議毎に提出・報告）	随時
	報告書	・進捗報告（定例会議毎に提出） ・作業報告、臨時・緊急報告等	随時
	打合せ議事録等	議事録 ・その他会議資料	随時（会議等の打合せ終了後 3 営業日以内）

注 1 プログラムには、ソースプログラム、実行形式プログラム、利用環境等を定義するファイル、コンテンツを含めること。また当センターが別途調達するハードディスク及び CD-ROM 等に格納すること。

注 2 データには、テストデータ及び現行システムからの移行データを含むものとし、別途調達するサーバ上のハードディスクに格納すること。

注 3 担当者・体制表等、変更があれば都度提出すること。

イ) 納入場所、納入条件

大阪国際がんセンター 医療情報部（大阪府大阪市中央区大手前 3-1-69）

なお、詳細については、別途当センター担当職員の指示に従うこと。

ウ) 検収方法

①運用テスト

i) 第 5 章テスト作業要件に従い運用テストの合格をもってプログラム等についての検収とする。

ii) テスト時に使用した一時ファイル等の不要なファイル等は、運用テスト終了後、受託者において削除すること。

②書類の検収

i) 設計書等、開発の各段階でレビューを行う。納品時に検収会議を行って、ドキュメント品質も検収する。

第3章 開発するシステムの要件

各要件については、各省庁から策定されている各ガイドライン（厚生労働省「医療情報システムの安全管理に関するガイドライン」、「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」、経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン」、総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン（第1版）（策定中）」等）について、内容を理解し、最低限のガイドラインを守ること。

1. 業務機能要件

対象システムは対象業務を適正、確実かつ効率的に行うシステムとして構築する。以下に、対象システムの機能について必要と考える主な機能を示す。

なお、各機能の具体的な仕様については、設計時において受託者と当センターの協議により決定するが、応札希望者は、提案書において、各機能の具体的な実現方法、実装方法についての考え方を記載すること。

(1) 患者情報管理業務

患者管理業務は、対象システムの利用同意を得た患者さまの基本情報（氏名、性別、生年月日、住所等）やクレジット決済情報の管理を行うものである。

ア) 患者情報管理業務

本業務では、参加施設・事業者（以下「各施設」という）の患者情報を ID 基盤に集約し、パーソナル ID に紐付けて管理する。

① 患者情報登録機能

本機能は、各施設の患者情報を ID 基盤に登録するものである。

機能要件としては

- ・ 各施設の患者情報を ID 基盤に登録できること。
- ・ 医療等 ID など、患者情報に付随する複数の種類の ID を管理できること。
- ・ 登録インタフェースは、画面またはバックグラウンドでの実行、いずれも可とする。ただし、各施設の患者情報を間違いなく登録できる仕組みを提供すること。
- ・ 登録している全患者の一覧について、画面と帳票で確認できること。

② 名寄せ機能

本機能は、参加施設・事業者で患者登録されたタイミングで名寄せを行うものである。

機能要件としては

- ・ ID 基盤と連携し、名前、住所、生年月日、性別等から、名寄せ対象の絞り込みができること。
- ・ 名寄せ対象の絞り込み方法は、容易にカスタマイズを行えること。
- ・ パーソナル ID に紐付けて、名寄せの登録・編集・解除ができること。
- ・ パーソナル ID には、利用者向けサービスのログインアカウントも紐付けて管理できること。なお、ログインアカウントの紐付けについては、セキュアで、かつ、患者さまに負担のかからない方法を具体的に提案すること。
- ・ パーソナル ID 自体の名寄せもできること。

③ 決済情報管理機能

本機能は、患者さまのクレジット決済を行うものである。

機能要件としては

- ・ クレジット決済機能には、NTT データのクレジット決済サービスを利用すること。

(2) 参加施設・事業者管理業務

本業務は、ID センター基盤に参加する施設・事業者の管理を行うものである。

ア) 参加施設・事業者管理業務

ID センター基盤に参加する施設・事業者の基本情報を管理する。

① 施設管理機能

本機能は、施設・事業者の基本情報の管理を行うものである。

機能要件としては

- ・ 施設の移転時にも変更されない一意の施設コードを付与して施設・事業者を管理できること。
- ・ 管理する項目には、名称、住所、電話番号、代表者名、医療機関コードなどが含ま

れること。

- ・ 将来的には最大 1 万施設の登録を見込んでおり、管理事務負担の少ない方法を提案すること。

イ) 職員情報管理業務

ID センター基盤を利用する職員情報を管理する。

機能要件としては、

- ・ 施設に属する職員情報を管理できること。
- ・ 管理する項目には、職員 ID、職員氏名、職種、資格などが含まれること。
- ・ 職員の異動時期には、職員情報の大量更新が発生する可能性がある。事務作業の一極集中を防ぐため、施設の管理者が自施設の職員管理を行える仕組みを提案すること。
- ・ 本プラットフォームの管理者が全職員情報を管理ができる仕組みを提案すること。

(3) 会計・収納／未入金管理業務

本業務は、各施設で発生した会計データを登録し、患者さまからのクレジットによる収納管理を行うものである。また、未入金が発生した場合の管理も行う。

ア) 会計データ登録機能

本機能は、施設の職員が患者 ID に紐付けて会計データの登録を行うものである。

機能要件としては、

- ・ ID センター基盤に対して、施設患者 ID で患者を検索できること。
- ・ 検索した患者に対して、会計データを登録できること。
- ・ 会計データが登録された旨を利用者のメールアドレスに通知できること。

イ) 収納、未入金管理機能

本機能は、患者さまからのクレジットによる収納、未入金の管理を行うものである。

- ・ ID センター基盤に登録された会計に対する収納／未入金情報を一覧で閲覧できること。過去の情報も検索でき、期間指定等も行えること。
- ・ 一覧から当該会計情報を選択した際に、患者情報および会計情報、収納があった場合は、決済日が閲覧できること。未入金の場合には、未入金の旨がわかること。

(4) 利用者（患者さま）向けサービス

利用者がインターネットを使ってスマートフォンまたは PC により利用する機能。I 期では、クレジット機能のみとするが、将来構想を踏まえた拡張性のある提案をすること。

ア) ログイン機能

本機能は、利用者の認証を行うものである。

機能要件としては、

- ・ 利用者が登録したログインアカウント、パスワードでログインできること。
- ・ ログイン後、利用者自身で、ログインアカウント、パスワードを変更できること。
- ・ パスワードを忘れた場合に、安全に再設定できる仕組みを提供すること。

イ) 会計一覧機能

本機能は、利用者が自身の会計情報を参照するものである。

機能要件としては、

- ・ 期間を指定して、会計情報を検索できること。
- ・ 検索結果を一覧で表示できること。一覧では、決済状況を確認できること。
- ・ 一覧から選択した会計の詳細情報を参照できること。

ウ) クレジット決済承認機能

本機能は、患者さまがクレジット決済を行うものである。

機能要件としては、

- ・ 一覧から選択した会計が未決済の場合に、『CAFIS BlueGate サービス』と連携してクレジット決済が行えること。
- ・ 決済情報は、(3)の収納／未入金管理機能と連動すること。
- ・ ある一定期間を過ぎた場合に自動決済できる設定ができること。
- ・ 患者さまにメールを送り、クレジットの決済内容（金額、決済日等）を確認し、

承認行為を記録できるような画面へ遷移できること。

- ・センターで保有している窓付封筒へ格納する送り先が分かるもの（住所、氏名）を印刷できること。※同封する明細書等は医事会計システムより出力する。

(5) 各種システム管理機能

システム管理者が本システムを管理できる機能。

ア) マスタ管理機能

本機能は、マスタメンテナンスを行うものである。

機能要件としては、

- ・各種マスタを画面上で新規作成、修正、削除、複写ができること。

イ) システム設定管理機能

本機能は、システム設定の変更を行うものである。

機能要件としては、

- ・バックグラウンドで処理される機能の実行時間設定等ができること。
- ・将来の新年号にも対応できる拡張性を持たせること。
- ・将来の消費税率改定にも対応できる拡張性を持たせること。

2. 画面要件

具体的な画面デザイン及び遷移等の決定は、設計時において受託者と当センターの協議により行うので、受託者は、効率化・合理化の方策がある場合には提案すること。

3. 帳票要件

具体的な帳票デザインの決定は、設計時において受託者と当センターの協議により行うので、受託者は、効率化・合理化の方策がある場合には提案すること。（特に今回、センター内の医事会計システムとは直接連携を行わないため、本システムへの2重入力の簡略化、誤入力防止の観点で、より良い効率化・合理化の方策がある場合には提案すること。）

また扱う文字種は Shift_JIS (CP932)、ISO/IEC 2022 (SS-MIX2)、UTF-8 (IHE ITI) とすること。

4. 情報・データ要件

- (1) 効率的なアクセス処理を可能とし、かつデータベース維持管理のためのプログラムコードの開発の必要性を極小化できるようにするため、正規化等を十分に考慮の上、冗長なデータの発生を抑制する設計とすること。
- (2) また本システム内で共通データを扱う共通部品等を使用する場合は、その提案をすること。
- (3) 将来、DBMS 製品を変えても対応できるよう、製品に依存するような SQL 等は使わないこと。

5. 外部インターフェース要件

対象システムが行う業務のうち、他システムのインターフェースを適用する機能は、以下のとおりであり、それぞれ、各システムが定めるインターフェース仕様に従うこと。(閲覧可能)
また国で検討している医療等IDにも将来的には対応できること。

表2 インターフェース要件

機能名	インターフェース
決済連携機能	CAFIS BlueGateサービス
診療情報連携機能 (将来構想)	PIX/PDQ, XDS.b, XCA
診療情報ストレージ機能 (将来構想)	SS-MIX2

6. 規模要件

(1) 利用者数

対象システムの利用者は、患者さまをはじめ、当センター職員、他施設・事業会社の職員等であり、将来構想を踏まえた最大規模要件は以下のとおりである。

ア) 最大患者登録数

1000万人

イ) 最大参加施設・事業者登録数

1万施設

ウ) 最大利用職員登録数

2000人／参加施設・事業者当たり

7. 性能要件

端末利用者にとって快適な作業を実現でき、かつシステムの日常運用を円滑に進めることができるために下記の処理速度を実現すること。

- ・ クレジット処理時間の目標値は、1件当たりオーソリ12秒、売り上げ7秒以内とする。
- ・ オンライン処理のレスポンス時間の目標値は、平常時5秒以内とする。
- ・ データ量の多い日でもバッチ処理の全体処理時間は4時間以内とすること
またバッチ処理は基本夜間時間帯とし、業務時間帯はさけること。

8. 信頼性要件

以下を実現するための構成や方式の考え方について提案すること。その際の条件等も含めて、複数案の提示があっても良い。

- (1) 障害に伴うシステム停止は、年2回以内、年間の合計停止時間は、基本48時間以内とすること。
- (2) 障害発生から対応着手時間を基本2時間以内として、復旧を行う手順又は機能を設計すること。
- (3) データベースのバックアップについては、週1回フルバックアップを取り、3世代分のバックアップデータを保管すること。
- (4) データベースはログファイルを保管し、障害発生時の直前までロールフォワードできること。
- (5) システムのイメージバックを週に1回は取得し、3世代保管すること。
- (6) 各バックアップは別筐体で保管を行うこと。

9. 拡張性・柔軟性要件

- (1) 将来構想では、様々な医療情報を扱うことが想定されるため、将来構想時の調達で外部ストレージの追加が容易な構成であること。
- (2) 歴年で保有するデータベースやファイルについては、将来、調達において指定した量の3倍になっても、プログラムやファイル等を改修することなく対応できるようにすること。
- (3) 業務アプリケーションの構成は、データ管理部分、業務ロジック、ユーザインタフェースを分離・分割し、相互の独立性を高めることにより、機能追加や保守作業に対する影響範囲を局所化でき、システムの改変に対する柔軟性が確保できるように配慮すること。
- (4) 将来的にはクラウドサービスにも移植できる柔軟性が確保できるように配慮すること。

10. システム中立性要件

対象システムは特定製品・技術に依存せず、可能な限り標準インタフェースを採用すること。また、将来のシステム更新時に、他事業者のシステムへの切り替えが発生した際には、データ可搬性が考慮された、構造化された状態を保持したデータとして、施設情報、職員情報、患者情報（名寄せ情報含む）、会計情報、収納情報等の移行ができること。当該移行作業も本調達の見積もりに含めること。

11. 事業継続性要件

応札希望者の過去の経験に基づき、コストパフォーマンスに優れる BCP 対策がある場合、提案書に含めること。

12. 運用性要件

下記の仕組みを提案すること。運用監視ツール等を開発する場合は、その見積も含めること。

- (1) システム操作・監視等要件
 - ア) 本システムの運用時間は、原則として 24 時間運用が行えること。
 - イ) システム障害の予防と早期発見を行うため、運用監視ツールを使用し、当センター内においてサーバーやネットワークの集中管理ができること。
 - ウ) ネットワークの帯域不足等、キャパシティ管理ができること。
- (2) データ管理要件
 - ア) 可能な限り 24 時間 365 日無停止での運転を行うため、システムを停止しないオンラインバックアップができること。
 - イ) プログラム、データ、各種ログ等の特性に応じ、日次又は定期的にバックアップができること。

13. 保守性要件

- (1) ソフトウェア保守要件
 - ア) 不具合発生時に早急な修正対象の特定と修正計画が可能な仕組みを用意すること。
 - イ) ソフトウェアのバージョン管理を適切に行える仕組みを提供すること。
 - ウ) ソフトウェア構造を明確にし、仕様変更時や障害対応時の妥当性検証を省力化するための工夫をすること。
 - エ) セキュリティホールが発見された場合の設定の変更やセキュリティアップデートの適用等の対策、その実施に先立つ調査・検証を適宜行うことを想定した仕組み又は手順を提供すること。
- (2) ハードウェア保守要件
 - ア) 可能な限り、オンライン中にも保守対応ができること。

14. 情報セキュリティ要件

- (1) 下記の各セキュリティ要件は当センターが求める必須要件であるが、すべてに具体的な実現方法を提案すること。また更に良い機能等があれば提案すること。

ア) 主体認証

- ① システムにアクセスする施設、システム利用者、システム管理者、システム運用要員及びシステム保守要員の一人一人を識別・認証する機能を有すること。
- ② 当該ログイン手段について、長さ又は複雑さの要件を満たさないパスワードの設定を制限する機能を備えること。また、これらの他に適切な認証方法があれば、提案すること。

イ) 権限管理

- ① システムにアクセスするシステム利用者、システム管理者、システム運用要員及びシステム保守要員が用いるアカウントの管理（登録、更新、停止、削除等）を行うための機能を有すること。
- ② アカウント管理者による不正を防止するため、アカウントの管理を行う権限を制御する機能を備えること。

ウ) アクセス制御

- ① システムにおけるそれぞれの職務・役割（システム利用者、システム管理者、システム運用要員及びシステム保守要員）に応じて、利用可能なシステムの機能、アクセス可能なデータ、実施できるデータの操作等を制限する機能を有すること。

エ) ログの取得・管理

- ① システムの利用記録、例外事象の発生に関するログを取得すること。また、十分なストレージ容量を確保し、取得したログは最低1年間保管すること。
- ② ログの不当な消去や改ざんを防ぐため、アクセス制御機能を備えること。
- ③ ログに記録される時刻にずれが生じないように、システム内の機器の時刻を同期する機能を備えること。
- ④ 容量の不足や障害の発生等により、ログが取得できなくなるおそれのある事象が発生した場合、又はログが取得できなくなった場合、速やかにシステム管理者及びシステム運用担当者へ通知する機能を備えること。
- ⑤ 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施できる機能を備えること。

オ) データの暗号化

- ① 個人情報に該当するようなデータについて、不正なアクセス及び閲覧を防ぐためにアクセス制御機能に加えて暗号化が必要な場合、暗号化して保存すること。
- ② 暗号化に使用するアルゴリズムは、原則として「電子政府推奨暗号リスト」に記載されているものの中から選択すること。

カ) 不正プログラム対策

- ① 不正プログラム（ウィルス、ワーム、ボット等）の感染を防止する機能について、すべてのサーバ及び端末に導入すること。
- ② ①に示す機能は、新たに発見される不正プログラムに対応するための更新を行い、効果を維持することが可能であること。
- ③ システム全体としてマルウェアの感染防止機能を確実に動作させるため、(1)に示す機能の動作状況及び(2)に示す更新の状況を一元管理する機能を備えること。

キ) 標的型攻撃対策

- ① システムに対する想定しない通信プロトコルによる通信や許可されていないコマンドやデータの入力を拒否する機能を備えること。
- ② 認証を行うサーバ及び個人情報に該当するようなデータを取り扱うサーバと他のサーバ及び端末との間の通信を最小限に限定し、その内容を監視する機能を設けること。
- ③ 不正侵入検知 (IDS) の機能を持った装置、システムを配置し、異常を検知した場合、即時にシステムの管理者等に電子メールで異常の検知を通知する機能を備えること。

ク) セキュリティ管理のための機能

- ① システムに導入・開発するセキュリティ機能(本節ア)～キ)に記載したものを含む。)に関する統合的な管理、異常及び故障の発生に関する通知等の管理機能を備えること。

- (2) 当センター以外を対象システム利用者の情報セキュリティ水準低下を防ぐため、受託者はアプリケーションの開発において以下の点のそれぞれについて、具体的な措置を提案し、当センターと協議の上で実施すること。

ア) アプリケーションに不正プログラムが含まれないこと

イ) アプリケーションに脆弱性^{ぜいじやく}を含まないこと

ウ) 他に手段がない場合を除き、実行形式プログラムの形式でコンテンツを提供しないこと

エ) コンテンツの改ざん等がなく真正なものであることを確認できる手段(電子証明書等)がある場合は、利用者にそれを提供すること

オ) 脆弱性^{ぜいじやく}が存在するバージョンの OS やソフトウェア等の利用やセキュリティ水準を低下させる設定変更を利用者に要求しないこと

カ) サービス利用に当たって必須ではない、利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能を組み込まないこと

第4章 開発するシステムの稼動環境要件

1. 全体構成

受託者は、システム構築に当たって必要となるソフトウェア及びハードウェアの構成を提案し、調達を行うと共に、ソフトウェアを含めたシステム全体の構築を実施すること。また開発に関わる機器・設備（通信回線、作業室等）および作業人員の管理等に対し、十分なセキュリティ対策を実施すること。

以下の事項及び全体の構成について、第1章の現行システムを吟味し現時点で想定する新システムの構成等における考え方を記述すること。

(1) データーセンター構成

ア) 当該システムを設置するデーターセンター内ハウジングラックについて、設置する機器に関する資料、電力設計に関する資料、並びに最終的なラックマウント構成図を示すこと。

(2) ハードウェア構成

ア) サーバ、端末機器等のハードウェア構成等について、開発対象システムに係る稼動環境を明記し主要なコンポーネントについては、全体システム構成図の中でそれを示すこと。

(3) ソフトウェア構成

- ア) サーバ、端末機器等の基本ソフトウェア構成、ミドルウェア環境等について、開発対象システムに係る稼動環境を明記し主要なコンポーネントについては、構成図を示すこと。
- イ) ソフトウェアの脆弱性が発見された場合、どのようにソフトウェアの修正または回避策の提示が行われるかを示すこと。

(4) ネットワーク構成

ア) 当該システムが利用するネットワーク環境及びそのコンポーネント構成を示すこと。

2. データーセンター構成

- (1) 本システムを構成するハードウェアは、当センターにて用意するデーターセンター内ハウジングラックへ構築すること。サーバ、スイッチを始めとするハードウェアは、原則として全てラックマウント型とし、マウント金具にてラックへ固定をおこなうこと。
- (2) 当センターが用意するハウジングラックのサイズは 19 インチ・フルラック (42U) とする。将来的な拡張性の観点から、本システムのフットプリントは 19U 以下に収まるよう、構成を決めることが望ましい。
- (3) 電源の仕様は AC100V 単相、2KVA×2 系統とし、プラグ形状は NEMA 5-15 とする。
- (4) データーセンターの電源は CVCF からの配電であるため、ラック内 UPS は必須としない。
- (5) KVM スイッチを構成に含めること。

3. ハードウェア構成

- (1) 本システムを構成する主要なハードウェア構成要素（物理サーバ、スイッチ）は、原則として冗長構成を取ること。
- (2) 物理サーバは IPMI 等によりリモート保守が可能であること。具体的には、物理サーバの BIOS 設定・更新、およびリモートのインストールメディアを用いた OS の再インストールがリモートからおこなえること。これら機能を有効にするにあたり、追加ライセンスが別途必要になる場合は、その費用も含めること。
- (3) スイッチは SSH 等によりリモート保守が可能であること。
- (4) 本システムを構成する主要なハードウェア構成要素（物理サーバ、スイッチ）は、IPMI・SNMP・Zabbix 等のプロトコル・ソフトウェアを通じ、当センターが別途運用する外部の監視サーバから一元監視できること。
- (5) 物理サーバのストレージは RAID 構成を取ること。ホットスワップ対応とし、一台以上のホットスタンバイディスクを用意すること。但し技術的な観点から、本要件を満たさない構成にて提案をおこなう場合には、その理由を併記せよ。

- (6) ノート端末は下記要件を満たすものを4台調達すること。
- ア) 端末 OS は WindowsOS ロードマップを考慮し、最適な OS を搭載し、最新のサービスパックを適用すること。
 - イ) CPU は、上記最適な OS を快適稼働できる性能を有すること。
 - ウ) メモリは、4Gbyte 以上とする。
 - エ) ディスクは、320Gbyte 以上の容量であること。
 - オ) 有線ネットワーク I/F は、1000BASE-TX/100BASE-TX/10BASE-T に準拠し、Wake up On LAN 対応であること。
 - カ) 無線ネットワーク I/F は、将来的な拡張性を持ち、ネットワーク要件に最適な性能を有すること。
 - キ) 光学ドライブは、DVD マルチドライブを1ドライブ以上搭載すること。
 - ク) 画面解像度は、最大解像度 1366×768 (1,677 万色)以上とする。但し、システム稼働環境における解像度については、検証を行い可能な限り文字が大きく表示されるように留意すること。ディスプレイサイズは 15.6 インチワイドとする。
 - ケ) USB3.0×3 ポート以上を有すること。
 - コ) 有線 USB レーザー式マウスを同梱していること。また、USB マウスで操作する際にノート PC 本体のタッチパッドデバイスなどが自動的に停止する機能があること。
 - サ) バッテリーについては、可能な限り標準バッテリーではなく、容量の大きい拡張バッテリーを搭載すること。
 - シ) ウィルス対策ソフトをインストールされていること。またウィルス対策サーバにより、クライアント PC のウィルス対策ソフトの定義ファイル更新状況を把握できるようにすること。

4. ソフトウェア構成

- (1) 本システムを構成するサーバは、仮想基盤サーバ自身を除き、原則として仮想基盤上の仮想サーバとして構築すること。
- (2) 本システムを構成する主要なソフトウェア構成要素(仮想サーバ等)は、SNMP・Zabbix 等のプロトコル・ソフトウェアを通じ、当センターが別途運用する外部の監視サーバから一元監視できること。

5. ネットワーク構成

- (1) 本システムの構築にあたり、/26 までの IPv4 グローバルネットワークアドレスを上限に用いてよい。ネットワークセグメントが複数個必要となる場合は、アドレスを CIDR で自由に分割し用いること。
- (2) 使用する IP アドレス毎に、対応する DNS ホスト名を定めること。本システムのドメイン名は当センターの(サブ)ドメインとし、権威 DNS は当センターが用意する。
- (3) スイッチ等ネットワーク機器は IEEE802.1Q VLAN 対応とし、ネットワークセグメント毎に異なる VLAN ID を割り当てて用いること。仮想基盤サーバのネットワーク・インターフェースはタグ付き VLAN とし、仮想サーバの所属先 VLAN について、自由な設定を可能とすること。
- (4) L2 ネットワークの冗長化プロトコルとして、LACP、MSTP を用いてよい。
- (5) 本システムのファイアウォールは、仮想基盤上に構築してよい。
- (6) 使用するネットワーク機器は IPv6 に対応したものであること。
- (7) 当センターと本システムが通信する上で、特に機密性が求められる箇所については、IPsec VPN とすること。ブロック暗号のアルゴリズムは AES、鍵長は 256bit 以上であること。鍵交換プロトコルとして IKE に対応すること。(当センター側の IPsecVPN ルーター機器及び設定作業は本調達に含めない。)
- (8) ネットワーク・インターフェースの冗長化プロトコルとして、VRRP を用いてよい。
- (9) ルーティングプロトコルとして、スタティックのほか OSPF を用いてよい。

第5章 テスト作業要件

1. テスト計画書の作成

実施する単体テスト、結合テスト、総合テスト、運用テストについて、テスト方針、実施内容及び実施理由を記載し、テスト工程毎にテスト計画書として提出すること。また、当センターが主体となって実施する運用テストについては支援すること。

テスト計画書に記載すべき事項を以下に示す。

- (1) 受託者のテスト実施体制と役割
- (2) テストに係る詳細な作業及びスケジュール
- (3) テスト環境（テストにおける回線及び機器構成、テスト範囲）
- (4) テストに関するツール類（開発するプログラムの概略仕様も含め）
- (5) テストデータ
- (6) 評価指標

2. テスト実施要件

(1) テスト工程共通要件

単体テスト、結合テスト及び総合テストの各テスト工程において共通する要件を以下に示す。

ア) 受託者はテストの管理主体としてテストの管理を実施すると共に、その結果と品質に責任を負い適切な対応を行うこと。

イ) 受託者は当センター及び関連する他システムに係る業者等との作業調整を行うこと。

ウ) 当センターに対し定期進ちょく報告及び問題発生時の随時報告を行うこと。

エ) 各テストを行うため、一連のテストケース（入力、出力及びテスト基準）、テストシナリオ（例外処理を含む。）、テストデータ、テスト評価項目及びテスト手順を各テスト実施前に作成の上、提出すること。

オ) 各テスト終了時に、実施内容、品質評価結果及び次工程への申し送り事項等について、当センターと協議の上、テスト実施報告書を作成すること。

カ) 他システムとの接続試験を実施する際には、当センター職員、当該システム開発及び保守業者と十分な調整を図り、受託者の負担と責任において実施すること。

キ) テストに必要なプログラム類の開発ないし用意を行い、進捗を報告すること。

(2) テストデータ要件

テストにおいて使用するテストデータに係る要件を以下に示す。

ア) 運用テスト以外のテストデータは、原則として受託者において用意すること。

イ) テストデータの管理は、受託者が責任を持って行うこと。なお、テスト工程毎のテスト計画書にテストデータの種類等を記載し、使用したテストデータは、テスト結果と共に媒体で納入すること。

(3) テスト環境要件

テスト環境に係る要件を以下に示す。

ア) 単体テスト及び結合テストに必要な機器等は、受託者の負担と責任において準備すること。

イ) 総合テスト及び運用テストに必要な機器等は、ハードウェア納入業者が導入するため、テストを実施するために必要な各種設定を受託者の責任において実施し、本番環境と同等の環境を準備すること。

(4) 結合テスト要件

プログラム及びモジュールが、本システム全体において、正しく機能することを確認するため、段階的に結合した状態でテストを行い、結果を報告すること。

(5) 総合テスト要件

総合テストに係る要件を以下に示す。

- ア) ソフトウェアが仕様に適合し、かつ本番環境で利用可能であることを確認できる評価指標を設定した上で、テストを実施すること。
- イ) 性能及び負荷のテストにおいては、本番環境と同様の環境により相応の負荷等をかけ、問題が発生しないことを確認すること。
- ウ) 総合テストでは、以下の項目について確認を行うこと。

① 機能性

- ・ システム機能が、正常系、異常系共に仕様書どおりに動作すること。
- ・ 他システムとの業務連携処理が正常に機能すること。
- ・ 情報セキュリティ要件を満たしていること。

② 信頼性

- ・ 信頼性要件を満たしていること。
- ・ 障害が発生した際の回復処理が適切であること。

③ 操作性

- ・ 要件及び説明書どおりに動作し、利用者が利用しやすいこと。

④ 性能

- ・ オンライン処理、バッチ処理の応答時間、スループットが適切であること。
- ・ システムの限界条件（データ量、処理量）下で、正常に動作すること。

(6) セキュリティテスト要件

セキュリティテストに係る要件を以下に示す。

- ア) 開発したソフトウェアについて、想定範囲外の入力を拒否できない脆弱性を狙った攻撃等の既知の手法による攻撃（バッファオーバーフロー、SQL インジェクション、コマンドインジェクション、セッションハイジャック、クロスサイトリクエストフォージェリ、クロスサイトスクリプティング等）が試みられた場合にシステムのセキュリティに影響を及ぼさないことを確認すること。

- イ) システムの動作環境又は動作前提であるハードウェア及びソフトウェアについて、既知の脆弱性が存在しないこと、及び既知の攻撃手法に対して脆弱な設定が行われていないことを確認すること。

- ウ) ア及びイの確認は、適切なテストツールを選択して想定されるパターンを網羅的に行うこと。

- エ) セキュリティテストにおいて発見された脆弱性及び当該脆弱性に関して実施した対処について、(1)オのテスト実施報告書に記載すること。

(7) 運用テスト支援要件

当センターが主体となって実施する運用テストに係る要件を以下に示す。

- ア) 運用テストにおける具体的な手順及び結果を記入するための運用テスト手順書（案）を作成すること。なお、システム操作に精通していない職員でも分かりやすいテストとなるように工夫すること。

- イ) 運用テストは当センターが主体となって行うが、当センターの求めに応じて運用テストを支援するための要員を確保すること。

- ウ) 運用テストで必要となるテストデータについて準備するのを支援すること。

- エ) 運用テストで確認された障害について対応方針を提示し当センターの承認を得ること。

- オ) 当センターに承認された対応方針に従い、プログラム及びドキュメント等を修正すること。

第6章 開発作業体制及び作業方法

1. 作業体制

(1) 受託者体制

受託者は、本作業を履行できる体制案を提出し、当センターの了承を得ること。なお、原則として体制の変更は認めず、やむを得ず変更する場合は事前に当センターの了承を得ること。

また、受託者は、本作業の履行が確実に行われるよう、本作業の全期間に渡って、必要となるスキル、経験を有した要員の確保を保証すること。また受託者は「業務・システム最適化指針（ガイドライン）」について十分な知見を有すること。

ア) 受託者側の体制（責任者・実施責任者を含む実行部隊）

イ) 受託者側の実施責任担当者

責任担当者に求める要件は、次のとおりとする。プロジェクト管理担当責任者と設計開発担当責任者は兼任して差し支えないものとする。

① プロジェクト管理担当責任者

進捗管理手法に精通し、経験を有すること。

② 設計開発担当責任者

データベース・システムの企画・設計に関する知見や技術を有すること。

ウ) 連絡体制（受託者側の対応窓口）

(3) 当センター職員が受託者に対し、常時契約履行状況に関する確認を行える体制とすること。なお、受託者は作業体制図を作成・提出すること。

2. 開発方法

(1) 開発計画

ア) 計画スケジュールに基づき、各作業別に各関係者の各責任範囲が分かるような責任範囲表を作成すること。

イ) 開発を行うに当たり、良いと思われる具体的な方策があれば、提案すること。以下の個々の仕様箇所に分散して記述しても構わない。

ウ) 本作業を実施するため、開発計画書及び計画表（日程表、成果物と対応した WBS を含む。以下「開発計画書等」という。）、並びにソフトウェアの作成に適用する情報セキュリティの観点も含めたコーディング規約を作成・提出し、当センターの承認を得て決定すること。

エ) 開発計画書については、「業務・システム最適化指針（ガイドライン）」に記載された設計・開発段階における標準管理要領に準じた管理要領及び以下の事項について定めること。そのための種々管理表は当センターと相談し合意を得ること。但し、各社において確立されたプロジェクト管理手法が当センターの求める管理表と異なる場合には、予め提案書にて提案し、受注後に相談調整するものとする。

① ソフトウェア開発プロセス

(i) 成果物

(ii) 成果物と関連づけられた作業スケジュール

(iii) チェックポイント

(v) 主要マイルストーン

② ソフトウェア変更管理

(i) ソフトウェア構成管理計画と手順

(ii) ソフトウェアの仕様に関する変更の定義と手順

(iii) 仕様変更の影響を最小にする対処の考え方

③ ソフトウェア評価

(i) ソフトウェア評価基準とフィードバックに関する手順

④ 標準と手順

(i) 技術的成果物に関する標準と手順

オ) WBS については、「業務・システム最適化指針（ガイドライン）」の設計・開発段階における標準 WBS の項目を含め、成果物と対応させ作成すること。また、同 WBS に基づき、ガントチャート形式の開発計画表を併せて作成・提出すること。なお WBS の内容（詳細度や項目・実績の表示等）については当センターの承認を得ること。

カ) 開発計画書等は、作業の進捗状況に合わせ随時内容の更新及び詳細化を図ることとし、更新後の計画書等は、定例会等の機会を利用して、当センターに報告・提出すること。

(2) 開発工程

ア) 本作業の遂行に当たっては、本作業の開発計画書等に定めた事項を遵守し、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。

イ) ソフトウェアの設計工程において、情報セキュリティに関する妥当性を確認するための設計レビューを含め、レビューを行うこと。また、製造工程において、ソースコードレビューを行うこと。設計レビュー及びソースコードレビューの範囲及び方法は事前に定め、当センターの承認を得ること。

ウ) 作成したソースコードについて、不必要なアクセスから保護すると共に流出を防ぐこと。

(3) 進捗管理方法

ア) 各作業に関する打合せ、納品物等のレビュー及び作業進捗確認のため、作業期間中、原則として月2回、定例会議を行うこと。

イ) 毎回の定例会を含めた各会議の議事録を、遅くとも会議日を除き、3営業日以内に作成し提出すること。

ウ) 定例会議では、開発スケジュールと実際の進捗状況の差を明らかにし、その原因と対策を明らかにすること。そのための課題管理表などは開発計画で定めたドキュメント類を用いること。なお、進捗管理に当たってはWBS・ガントチャートによるものとし、作業計画書の各管理要領については一覧形式の管理表を作成し報告を行うこと。

エ) 当センター内での作業に当たっては、当センターの指示に従い作業終了後は報告書を提出すること。

オ) 開発工程中における仕様変更については、変更を少なくするための方策を提案すると共に、各フェーズにおける変更不可となる時点についての考え方を示すこと。

(4) ドキュメント基準

ア) ドキュメントについては、作成に先立ちその構成や記載項目、記載内容及び記載水準等を規定した作成要領を提出し、これに従うこと。

(5) 開発環境

本調達における開発環境は、ネットワーク環境含め、受託者の負担と責任において確保すること。また本システム稼働後もテスト環境として利用できることとし、各種改修作業時、本番環境適用前の動作確認環境として、利用できること。

3. 実装

(1) 別途調達を実施するハードウェア等の納入業者との連携・協力を図り、ハードウェア等の設置作業終了後、本システムの導入作業及び試験・調整を実施すること。

(2) 本システムの導入作業及び試験・調整は当センターが指定する日時及び設置場所で行うこと。

(3) 試験・調整に当たっては、予め計画書を提出し、これに従うこと。

4. 教育と引継ぎ

(1) 運用業者への引継ぎ

ア) 別途調達する本システムの運用業者に対し、納入するドキュメント類を用いて、作成した運用設計の説明を行い、当該業者への引継ぎをすること。

イ) この引継ぎの計画を立て当センターの了承を得ること。

ウ) 引継ぎ結果を報告書にまとめ納入すること

(2) 教育に係る要件

システム利用者が、本システムの操作を習得するために必要な教育を当センター内で実施すること。