トレーサビリティ情報管理システム

要求仕様書

令和６年７月

京都大学 ｉＰＳ細胞研究財団

Ⅰ．仕様書概要説明

1. 調達の背景及び目的

公益財団法人京都大学 iPS 細胞研究財団(以下、CiRA_F)では、自家 iPS 細胞由来の移植治療を普及させるべく、myiPS プロジェクトを推進している。この取組みでは、患者自身の細胞から製造を行うため、患者自身の細胞を使用して加工物が製造されたことを、サプライチェーン全体を通して担保する必要がある。そこで下記の項目を目的にトレーサビリティ情報管理システムを調達する。

- 患者検体と生産した自家 iPS 細胞及びその由来物の取り間違いを防止し、確実に患者に受渡しできること。
- 取り間違えが発生した時に患者への間違った細胞の受け渡しがないように未然に防止できること。
- 患者細胞の採取～製造～医療機関への加工物受渡に至るサプライチェーン全体のトレーサビリティを担保すること。
- ステークホルダ間(CiRA_F-医療機関-輸送企業)の情報共有を効率化すること。
- ステークホルダ間(CiRA_F-医療機関-輸送企業)の調整業務(日程調整など)を効率化すること。
- ER/ES、Part11、Data Integrity などの規制に対応した適切なデータ管理を行うこと。

2. 納品物名及び内訳

トレーサビリティ情報管理システム　一式

（内訳）

(1)	設計図書	1 式
(2)	テスト仕様書/報告書	1 式
(3)	トレーサビリティ情報管理システム	1 式
(4)	操作教育資料	1 式
(5)	操作マニュアル	1 式

3. 技術的要件の概要

(1) 本調達物品に係る機能及び技術等（以下「性能等」という。）の要件 （以下「技術的要件」という。）は、Ⅱ．調達物品に備えるべき技術的要件に示すとおりである。

(2) 技術的要件は、すべて必須の要件である。

(3) 必須の要件は、当財団が必要とする最低限の要件を示しており、本調達物品の性能等がこれを満たしていないとの判定がなされた場合には不合格となり、落札決

定の対象から除外する。

(4) 本調達物品の性能等が技術的要件を満たしているか否かの判定は、本調達物品に係る技術仕様書その他の入札説明書で求める提出資料の内容を審査して行う。

4. その他

(1) 技術仕様書等 提案するシステムは原則として入札時点で製品化され、再生医療薬製造企業に対し、国内導入実績を有していること。

(2) 提案に関する留意事項

① 再生医療薬製造企業に対し、システム導入した経験のあるメンバーをアサインすること。

② 2025 年 3 月末までにシステムの導入が完了すること。

③ 初期費用だけでなく、ランニング費用(保守費・利用料等)を、提案書に明記すること。

④ 保守の内容について具体的に記載すること。

⑤ 当該システムに対する操作教育を見積に含めること。

⑥ 提出資料等に関する照会先を明記すること。

⑦ 提案された内容等に対する問い合わせやヒアリング対応すること。

Ⅱ．調達物品に備えるべき技術的要件

1. 機能・非機能要件

分類	番号	項目	内容
機能要件	001	サプライチェーンモデル設定	ある患者への加工物の提供(以下､案件)における検体採取～製造～加工物の受渡までのサプライチェーン全体の業務モデル(以下、サプライチェーンモデル)を設定にて定義できること。
	002	サプライチェーンモデル参照	サプライチェーンモデルを参照できること。
	003	案件番号管理	案件に対して、ユニークな ID(案件番号)を自動発番できること。 ※案件番号は検体に対して発番し､CIRA_F が管理する番号を指す。
	004	ラベル印刷	案件番号を識別するバーコードラベルをラベルプリンタから複数枚発行できること。
	005	業務画面設定	サプライチェーンモデル内の各業務に対して、データの登録・参照が可能な業務画面を有すること。

分類	番号	項目	内容
	006	トレジャーマップ管理	サプライチェーンモデルに業務の進捗をマップ表示できること。
	007	テナント管理	医療機関、製造業者、輸送業者等のテナントを管理できること。
	008	ユーザ管理	医療機関、製造業者、輸送業者等に属するユーザを管理できること。
	009	ロール管理	ロール(役割)を定義し、当該ロールが実行可能な業務を管理できること。
	010	サプライチェーンテナント管理	ユーザ・ロール・テナントを組合わせたアクセス制御ができること。
	011	スケジュール管理	案件に対して、各ユーザが入力した予定日程をガントチャート形式で表示できること。
	012	バーコード照合	案件番号でのバーコード照合機能を有すること。なお、照合結果が NG の場合、NG であることを画面上に明示できること。
	013		各プロセスにて案件番号によるバーコード照合が行えること。
	014	CSV 出力	業務画面に表示している項目を CSV ファイル出力できること。
	015	ファイルアップロード	案件に紐づく関連ファイルをアップロードできること。
	016	電子署名	ID/PW による電子署名機能を有すること。
	017	メール通知	指定されたロールに対してメール通知する機能を有すること。
	018	監査証跡	監査証跡機能を有すること。
非機能要件-性能・スペック	019	性能・スペック	システムの画面切り替えのレスポンスが 3 秒以内であること。 ※ネットワークを除くリクエスト～レスポンスまでの時間。ただし、表示項目数や登録項目が多数(約 20 項目)の画面、月次処理や一括処理等は除く。
	020	性能・スペック	バッチ処理・バックグラウンド処理が適切な時間内に終了する性能を有すること。

分類	番号	項目	内容
	021	性能・スペック	想定する同時接続数を定義し、最大数接続時にも適切なレスポンスが得られること。
	022	性能・スペック	必要なデータ量を定義し、保存することが出来るデータ容量を有すること。
-セキュリティ	023	セキュリティ	セッションタイムアウト及びレスポンスタイムアウトまでの時間を設定出来ること。
	024	セキュリティ	システム設定を変更出来る許可された特定のユーザのみに付与するため、システム管理者ロールがあること。
	025	セキュリティ	障害発生時の原因解析のために、システムログやアプリケーションログ等が取得できること。
	026	セキュリティ	ログの重要性や、ログの容量に応じてログの保管期間を明確にすること。
	027	セキュリティ	ログのアーカイブ方法を定義し、実装できること。
	028	セキュリティ	ウィルス対策ソフトのパターンファイルが、常に最新版になるように管理されていること。
	029	セキュリティ	ウィルス対策ソフトは常駐し、常にウィルスの侵入対策を行うこと。
	030	セキュリティ	ウィルスを検知した場合、適切に通知が行われること。
	031	セキュリティ	ソフトウェア障害による下記事象に対策がなされていること。 ・データ消失／改竄／窃取
	031	セキュリティ	サービス不能攻撃(Dos,Spam 等)によるサービス停止に対策がなされていること(目標項目)。
	032	セキュリティ	脆弱性攻撃による情報漏洩／サービス停止／不正アクセスに対策がなされていること(目標項目)。
	033	セキュリティ	他社サーバ攻撃の踏み台にされることに対して対策がなされていること。
	034	セキュリティ	公衆網／インターネット(有線／無線)データ盗聴による情報漏洩に対して対策がなされていること。 ・ID／パスワード不正取得 ・送受信メール／ファイル転送データの不正取得

分類	番号	項目	内容
	035	セキュリティ	モバイル通信データの不正取得による情報漏洩に対策がなされていること。
	036	セキュリティ	タイムスタンプの時刻を正確にするために、ネットワーク上の時刻サーバに同期すること。
-監視	037	監視	監視時間／間隔を定義し、実装すること。
	038	監視	ログを監視することで、アプリケーションやミドルウェアの障害を検知し、アラートメールを配信すること。
	039	監視	サーバの CPU、メモリの利用量が定められた閾値を超えた場合は、システム管理者へメールで通知されること。
	040	監視	ハードウェアやネットワークの障害を検知し、アラートメールを配信すること。
	041	監視	ディスク容量の監視を行い、ディスクの空き容量が定められた閾値を超えた場合は、システム管理者へメールで通知されること。
-可用性	042	可用性	プログラムやデータのバックアップを行うことが出来、障害時には、リストア出来る機能を有すること。
	043	可用性	バックアップの領域及び、復旧できる範囲（領域、領域日時）が明確になっていること。
	044	可用性	バックアップのスケジュールが明確になっていること。(定期バックアップ、システムバックアップ)
	045	可用性	バックアップ先が遠隔地保管になっていること。
	046	可用性	アプリケーションサーバおよびデータベースは冗長構成とし、可用性を向上すること。
-電子記録・電子署名要件	047	電子記録・電子署名	セッションタイムアウト及びレスポンスタイムアウトまでの時間を設定出来ること。
	048	電子記録・電子署名	利用者(ユーザ ID)とパスワード及びパスコードによる二段階認証を実装すること。
	049	電子記録・電子署名	数度に及ぶ認証の失敗に対しては、アカウントロックをかけること。ロックがかかるまでの回数は可変であること。
	050	電子記録・電子署名	アカウントロックは、適切な時間維持されること。ロック解除までの時間は可変であること。

分類	番号	項目	内容
	051	電子記録・電子署名	アカウントロックの解除が可能なこと。
	052	電子記録・電子署名	過去使用したパスワードが利用出来ないこと。利用出来ない過去パスワードの回数は可変であること。
	053	電子記録・電子署名	ID／パスワードへの攻撃（総当たり攻撃等）への対策として、アカウントロックが実装されていること。
	054	電子記録・電子署名	パスワードの文字列構成（半角の英字、数字、特殊文字の組み合わせ、文字数）について具体的に定め、それを許容できる機能を有すること。
	055	電子記録・電子署名	予め定められた周期で、パスワードの変更をシステムの利用者に求める機能を有すること。
	056	電子記録・電子署名	システム管理者が仮パスワードを設定出来る機能を用意すること。
	057	電子記録・電子署名	電子署名された電子記録は以下の情報を含むこと。 ・署名者の署名時点のフルネーム ・署名者を識別できるコード ・署名された日時 ・署名された意味
	058	電子記録・電子署名	電子署名者の表示／印字形態について、以下を考慮した対応方針を定め、システムに実装すること。 ・同姓同名の署名者への対応(例:氏名＋社員番号)

2. その他

(1) 当該システムには個人情報の登録は行わない。

(2) MES、LIMS の範囲となる機能は本要求仕様書の対象外とするが、将来導入時に連携可能な仕組みを有すること。

(3) CSV(Computerized System Validation)は対象外とする。

(4) PJ 期間中に「1.機能・非機能要件」以外の要件が発生した場合は、契約金額を変更する場合がある。

(5) 納品後に不具合(「1.機能・非機能要件」を満たせていないなど)が発生した場合は、瑕疵の範囲として対応すること。

(6) 納品後にシステム改修が対応可能なシステムであること。

(7) 納品後にシステムの標準機能エンハンスがあった場合は、当該システムにも更新可能であること。

以上