契約管理システム構築

業務請負契約　仕様書

令和７年３月

国立循環器病研究センター

１．概要

国立循環器病研究センター（以下「当センター」とする）で実施する研究契約(治験・特定臨床研究等含む)については、産学連携本部と臨床研究管理部、臨床研究監査室が、それぞれ研究内容に応じて管理している。この両者を相互に紐づけて閲覧可能となることで複数部署が契約の進捗を確認出来て利便性が高まるので、契約情報を一元管理するシステムを調達する。なお、産学連携本部と臨床研究管理部、臨床研究監査室において、それぞれの契約管理進捗データは個別（部署単位、担当者単位など）にアクセス制限を付与できることに加え、特定個人に限定した部署を超えて相互閲覧も可能となるアクセス権限設定を柔軟に行えるシステムが、本業務では必要である。

２．契約期間

構築期間：契約締結日～最大９ヶ月

稼働期間：構築後１年間

※構築後１年間の維持管理費用を含むこと

３．納入場所

当センター研究棟２階２０１０５室産学連携本部、臨床研究管理部、臨床研究監査室、財務経理課外部資金係

４．システム構築に必要な要件

(1)　サーバにかかる要件

・当センターの NCVC ネットワークからのインターネット接続により利用できること。

・OS は Windows Server 2019 以降であること。
　サポートが切れる前に更新等は必ず行うこと。

・Web サーバとして IIS（Internet Information Service）をインストールすること。

・リレーショナルデータベースとして SQL Server Express をインストールすること。

・通信の暗号化のため SSL 証明書(https 通信)を取得すること。

・登録済みユーザのみがアクセスできるものとすること。

(2)　入力にかかる要件

・新規登録申請(変更申請含む)に必要な条件を全てカバーした入力フォームを作成すること。

・過去登録データは Excel もしくは csv 形式で取り込めること。

・指定した入力全データ(アルファベットごと)を Excel もしくは csv 形式で取

り出せること。
・入力項目にフリー記載（治験薬の登録を想定）項目(10,000 字まで)含めること。
・入力フォーム登録後は管理者以外で上書きできないようにすること。
・登録完了時に契約締結案内(メール文案)を自動作成する要件を選択できること

(3)　検索にかかる要件
・受付番号から検索すると契約の進捗を確認できること。
・入力項目のうち少なくとも 1 種類を指定して検索すると、該当する契約名を一覧表示させること。
・検索時に複数条件を指定すると、そのすべての条件を満たす契約名のみ一覧表示させること。
・キーワード検索ができること。
・検索結果は Excel もしくは csv 形式で出力可能なこと。

(4)　ユーザ管理にかかる要件
＜システム管理者に付与する権限＞
・システム利用者の登録
・当センター職員以外のユーザのアクセス承認
・申請内容の確認、承認および登録
・申請件数、ディスク使用量、ユーザログイン履歴、メール送受信履歴の確認
＜システム利用者に付与する権限＞
・契約書登録にかかるフォーム入力
・契約申請の進捗確認

(5)　採番にかかる要件
・採番した番号を各自入力できること。
・フォームに入力した財源種別によって、桁数は、アルファベット+数字(①(まるいち等含む)+記号(#、アンダーバー(_)、ハイフン(-)等)+特定の文言(発明、意匠等)で構成された最大１５字まで、各自入力できること

(6) アクセス管理
・産学連携本部、臨床研究管理部、臨床研究監査室において相互閲覧する場合は、メンバーを限定するアクセス制限を設けること。

５.情報セキュリティ管理

1. 「政府機関の情報セキュリティ対策のための統一基準」の最新版及び当センターの情報セキュリティポリシーに準拠していること。なお、当センターの情報セキュリティポ

リシーが原則的に優先するが、統一基準にある記載内容を考慮したものであることが必要である。

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)」

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)」

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。
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。
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。
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。
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また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。
9. 情報セキュリティ対策に関する履行状況を再委託先含めて定期的に確認し、当センターへ報告すること。
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。

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。
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。
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。
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、または抹消し、書面にて報告すること。
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。
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など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。
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。
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。
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。
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長の判断をあおぐこと。
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すること。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、提案の見直しを図ること。
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。
23. データベース内に格納するデータは暗号化することが望ましい。
24. データベースの管理者アカウントは、情報システム管理者との区別、データへのアクセス要否、委託先を含む管理者権限付与の適切性等を勘案した上で、適正に設定管理すること
25. データベースの操作ログには操作対象データや操作内容を含むこと。
26. 主体認証のパスワードは英大文字（26 種類）小文字（26 種類）＋数字（10 種類）＋記

号（26 種類）の計 88 種類の文字をランダムに使って、医療情報システムの場合は 13 桁以上、医療情報以外の情報システムの場合は 10 桁以上とすること。また、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やアクセス可能な範囲の見直しを行うこと。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。

27. 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。
28. 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。
29. 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。
30. 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。
31. 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。
32. 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。
33. 保守においては、必要に応じて経路制御及びアクセス制御の設定の見直しを行い報告すること。
34. クラウドサービスを利用する場合は、当該の情報システムにおける情報セキュリティ対策の実施状況を、定期的に確認・記録し、報告すること。
35. クラウドサービス（EDC を含む）の利用がある場合は、導入するクラウドサービスが政府情報システムのためのセキュリティ評価制度（ISMAP）クラウドサービスリスト、または、ISMAP-LIU クラウドサービスリストに登録されていること。又は、その取得が進められていること。どちらにも該当しない場合は、ISMAP 管理基準についての自己評価を提出するか、提案者における情報セキュリティに関する体制や取り組みなどの資料を提出し、情報統括部の判断をあおぐこと。

５．費用請求に関する事務手続き

受託者は業務終了後に作業完了報告書を発行して、その内容をもとに当センター職員

の検認を受けること。
検認の結果合格となった場合に、当センター検収日付の翌月 10 日までに請求書に検収印押印済みの作業完了報告書を添付して、当センター担当者に提出すること。
上記期限内に適正な請求書が提出された場合、請負費用は検収日の翌々月末営業日に銀行振り込みにて支払うこととする。
検認の結果不合格となった場合には、契約期間内に不備を是正して再度当センターの検認を受けること。不備是正のために要した費用は受託者が負担するものとする。

6．秘密保持
受託者が本業務の実施に当たり得た情報については他者に漏洩してはならない。また、当該情報を他業務に用いることもできない。
この条項は本契約終了後も存続するものとする。

7．その他
この仕様書に定めのない事項については、双方協議のうえ決定すること。

以上