# バイオバンク検体管理、検索システム改修作業契約
# 仕様書

令和８年７月

国立研究開発法人

国立循環器病研究センター

# 仕様書

１．　件名

バイオバンク検体管理システム、検体検索システム改修作業契約

２．　作業内容

・バイオバンク検体管理システムおよび、バイオバンク検体検索システムの OS 最新化

・バイオバンク検体管理システムの HIS 連携機能の改修

・バイオバンク検体検索システムのデータインポート機能の改修

３．　納品期限・作業期間

納品期限　2027 年 3 月 31 日

作業期間　契約締結後速やかに～2027 年 3 月 31 日

４．　場所

国立研究開発法人国立循環器病研究センター　研究棟 3 階バイオバンク

５．　目的

令和元年より、バイオバンク検体管理システム（以下「検体管理システム」という。）およびバイオバンク検体検索システム（以下「検体検索システム」という。）が稼働しています。検体管理システムでは、バイオバンク協力者の試料情報や同意情報、ならびに研究用途への払い出し管理を行っています。協力者数は令和 8 年 4 月時点で 37,000 人を超えています。

また､検体検索システムは院内向けに公開されている WEB アプリケーションです。バイオバンクに保管されている試料等を、病名等を条件に検索できます。両システムとも日本システム開発株式会社（NSK）が設計・構築を実施しています。

これらのシステムが稼働するサーバ OS については、保守期限の到来およびセキュリティ上の懸念があることから、OS を最新化、アプリケーションとデータベースを移行します。加えて、HIS 更改に伴い、検体管理システムの HIS データ連携箇所の改修と、検体検索システムのデータインポート処理箇所の改修を実施します。

仕様詳細

（１）OS の最新化

・現在稼働中の以下のサーバに対して、OS の最新化を実施する。OS は Windows Server 2025 を想定している。

- 検体管理システム AP サーバ
- 検体管理システム DB サーバ
- 検体検索システム AP サーバ
- 検体検索システム DB サーバ

・対象サーバは、当センター情報統括部管轄の仮想基盤上で稼働している。
移行先となる物理端末と OS をセンターが提供する。

・AP サーバの IP アドレス変更が発生した場合、当センターへ DNS レコードの変更を依頼すること。

・移行先のサーバには、当センター指定のソフトウェア(ウイルス対策、資産管理)導入が必須である。インストールは当センターが実施するが、稼働に必要な除外設定等あれば申し出ること。

（２）検体管理システムの改修

・検体管理システムより当センターの統合データベース(以下、「統合 DB」という。)から患者情報、検査情報を参照し本システムに取り込んでいる。次期 HIS 稼働に伴い、統合 DB が更新されるため、新しい統合 DB から患者情報、採血情報を参照、取り込むための改修をすること。

（３）検体検索システムの改修

・HIS の患者情報、検査情報、手術情報、病理情報を検体検索システムに手動で取り込んでいる。現在は、Microsoft Access のファイルを直接取り組んでいるが、これを CSV ファイルで取り込めるように機能改修をすること。

（４）成果物

・受注者は、本業務の完了後、実施した作業内容、改修内容、移行結果及び試験結果等を記載した作業報告書を提出すること。
なお、当センターによる報告書の確認及び成果物の検収をもって業務完了とする。

（５）その他

・作業については、VPN を利用した遠隔操作により実施可能な場合は、遠隔で実施して差し支えないものとする。当センターで作業する場合は、移動費用等を本調

達に含めること。

・サービス停止リスクや作業による不具合を考慮し、現行システムの設計・構築または保守運用に関与した実績、もしくは同等の知見・技術力を有すること。

６．　情報セキュリティ管理

受託者は、以下を含む情報セキュリティ対策を実施すること。

・当センターから提供する情報の目的外利用を禁止すること。

・本業務の実施に当たり、受注者またはその従業員、本調達の役務の内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。

・本改修においては、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

・ソフトウェア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)」

・情報セキュリティ対策の履行が不十分である場合、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。

・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。

・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。

・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。

・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。

７．　その他

その他この仕様書に定めのない事項については、当センターと協議の上、決定すること。

以上