遺伝子検査情報管理システム保守業務仕様書

1. 保守期間

自 令和 9 年 1 月 1 日
至 令和 10 年 12 月 31 日

2. 保守業務を実施する場所

国立循環器病研究センターが認めたリモート作業が可能な場所で実施する。
なお、保守作業内容の重要性や診療への影響度の協議により、相互の合意をもって、当センター敷地内での作業を実施するものとする。

3. 目的

遺伝子検査情報管理システムについて、常に適正な機能を発揮できる状態に保持するための保守業務および、国立循環器病研究センターが行う遺伝子検査を実施するうえで必要な本システムの運用支援業務を実施する。

4. 保守の対象

- システムを構成する遺伝子検査情報管理システムと遺伝子解析システムのソフトウェアを対象とする。対象とするシステム・ソフトウェアは、国立循環器病研究センターで保持される仮想化サーバ上で稼働している本システムを構成するソフトウェア、遺伝子検査室に設置した管理用 PC に導入され本システムとして稼働するソフトウェアである。
- 本システムを稼働させるために同時に導入した管理用 PC、バーコードプリンタ（ラベルプリンタ）については、故障対応はメーカ保守となるが、そのための障害時の一時切り分けの支援および部品交換などを伴わない軽微な障害対応が運用保守業務の対象とする。但し障害の一時切り分け及び障害の復旧対応については、協議のうえ決定する。
- 次世代シーケンサー連携対応後の保守対応も業務内容に含むこと。
- 電子カルテ更新に伴う遺伝子検査情報管理システム移設作業に際し、新たに導入した端末 5 台について、OS の最新バッチ適用に伴うシステム対応作業を最低でも年 1 回現地で実施すること。

5. 業務仕様

(1) システム・ソフトウェアの保守

- システム・ソフトウェアの不具合対応
- 機能維持に必要なシステム・ソフトウェアおよび必要なミドルウェアのバージョンアップ
- 国立循環器病研究センター及び運用保守業者が収集したソフトウェアの脆弱性調査報告への影響度調査および必要な対応
-

(2) 運用支援

- 問合せ対応・セキュリティアップデート・不具合対応

※ 対応範囲については、都度国立循環器病研究センターと協議のうえ決定する。

(3) 対応時間

- 電子メールによる受付の場合は 24 時間 365 日、電話による受付は開院日の 9 時から 17 時半まで対応すること。。
- 対応時間は、操作方法やサービス・機能仕様、契約内容の確認等の緊急性のない内容は行政機関の休日に関する法律第一条にて定められた行政機関の休日以外の日（以下、「平日」という。）の 9:00～17:30（以下、「営業時間」という）とすること。
- セキュリティに係る障害や不具合等、緊急対応が必要な内容は 24 時間 365 日とすること。
-

(4) 作業場所

- 原則として国立循環器病研究センター敷地内で対応すること。
- やむを得ない場合、緊急性が高い場合および軽微な対応については国立循環器病研究センターより御提供頂く VPN 環境を利用したリモートで対応すること。
- リモート対応の場合は、国立循環器病研究センターが業務の遂行に必要であると認めた場所からのみの接続とする。
- 第三者が業務の内容を知りうることが可能な状況下での接続および無償の公衆無線ネットワークなど情報セキュリティ管理が及ばない接続は行わないこと。。
- 情報セキュリティの確保に努め、情報の漏えいがおきない場所で作業をすること。
-

6. 情報セキュリティに関して

業務の実施にあたっては、診療情報を扱うシステムであるため、個人情報保護と情報セキュリティに関して十分に注意すること。具体的には、以下の各項目について遵守すること。

- 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を受託業務を遂行する目的外に利用しないこと。
- 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。
- 受注者の本業務の実施場所について情報提供を行うこと。
- 本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）に関する情報提供を行うこと。
- 情報セキュリティインシデントへの対処方法を整備していること。
- 情報セキュリティ対策に関する履行状況を定期的に確認し、当センターへ報告すること。
- 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。
- 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。
- 本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。
- 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。
- リモートメンテナンス回線は、センターが提供する VPN 環境で接続すること。
- その他、情報セキュリティに関して対応判断が必要な内容については、情報統括部の判断をあおぐこと。

以上