CTG セントラルシステム　１式
仕様書（案）

国立循環器病研究センター

Ⅰ.調達の目的

現在使用中のCTGセントラルシステムについては、購入後、一定年数が経過しており、故障発生時に対応が出来ない可能性があることから調達を行う。

Ⅱ.調達物品・構成内訳

機器名：産婦人科　CTGセントラルシステム　　1式

（内訳）

1．ＣＴＧ セントラルシステム	1 式
2．リモートユニット	6 式
3．ゲートウェイサーバー	1 式
4．患者情報取得ソフト	1 式
5．ＷｅｂＣＴＧ 参照クライアントソフト	1 式
6．無停電電源装置	2 個
7．液晶ディスプレイ　24 型タッチパネル	7 台
8．　外付けハードディスク	1 台
9．ネットワーク分配器	1 台
10．映像分配器　送信用	2 台
11．映像分配器　受信用	3 台
12．DP ケーブル	1 個
13．HDMI ケーブル	5 個
14．システム設置・設定費用	1 式
15．CTG データコンバート費用	1 式

Ⅲ．納入期限

令和8年10月31日

Ⅳ．性能・機能に関する要件

2－1．産婦人科CTGセントラルシステム1式は以下の性能を有すること

2－1－1．胎児集中監視システムは CTG(Cardiotocogram)及び、胎児心拍数、子宮収縮活動を表示でき、胎児心拍数の表示に関しては品胎まで表示できること

2－1－2．母体測定可能な分娩監視装置使用して測定した際にはセントラルシステム上に母体NIBP値、母体SpO2値、SI値が表示できること

2－1－3. 上記各測定項目についての監視情報は、常に把握できるよう全て同一画面上に表示できること
2－1－4. CTG 表示の各波形については、視認性を確保するため線の太さ・色を選択して表示できること
2－1－5. 監視中の CTG データ（以下リアルタイム CTG）及び保存された CTG データ（以下過去 CTG）は、一画面 15～20 分間の範囲でトレンド表示できること
2－1－6. CTG 表示は、胎児心拍数の表示スケールを 30～240bpm と 50～210bpm のどちらかを任意で設定できること
2－1－7. 長時間 CTG 表示は、60 分の CTG 表示と任意の拡大した 20 分を同時に表示できること
2－1－8. リアルタイム CTG 多床表示は、接続数に応じて 1 画面で 1～32 床まで分割数の限定なく自動で分割表示でき、分割表示中は各床の表示サイズは各ベッド同等サイズで表示できること
2－1－9. リアルタイム CTG 多床表示は、分娩監視装置の稼働台数に応じた自動分割表示、または特定ベッド表示を選択、表示でき、特定ベッドの指定は予めグループとして 7 グループ以上登録できること
2－1－10. リアルタイム CTG 多床表示は、患者 ID・患者氏名・警報状態が測定データ毎に表示できること
2－1－11. 過去 CTG データ表示は、CTG 表示画面に同一患者データリストをタブで表示でき、タブをワンクリックすることで該当のデータを表示できること
2－1－12. CTG データの一覧は、ベッド名・患者 ID・氏名・計測日時を表示し、保存済みの CTG を参照できること
2－1－13. 過去 CTG データ表示は、測定時に保存された CTG、リモートマーク表示・各種イベントマーク表示・貼り付けメモ表示の再生できること
2－1－14. 分娩監視装置が母体・胎児心拍一致情報を送信した場合、セントラルモニタ上でで表示し、心拍の入れ変わりを確認できること
2－1－15. 現在参照している特定妊婦の CTG と、現在または過去における同一妊婦の計測 CTG を、一画面に表示、確認できること
2－1－16. 多胎の測定時において、ワンクリックで、胎児 1 のみの波形表示、胎児 2 のみの波形表示に切り替えできること
2－1－17. 測定中に、共有したい内容をメモで貼り付けるイベントボード機能を有し、入力情報は測定中、常に表示できること
2－1－18. 病院現有の分娩監視装置の時刻を測定開始時に自動で同期できること
2－1－19. 警報状態になったベッドの CTG 表示画面枠及びベッド非表示の際には点滅し警報状態を報知できること
2－1－20. 病院保有のセントラルモニタから CTG データならびに付帯する患者属性情報を、

もれなく新システムでも参照できるよう新システムに移行できること
2－1－21. 無停電電源装置は、停電時にそれを検知してシステムを正常に終了させることができること
2－1－22. 無停電装置は、初期性能時においては、15 分以上の電圧供給を行える性能があること
2－1－23. 液晶カラーディスプレイは、対角 23 インチ以上、解像度 1920×1080（フル HD）以上の表示性能であること
2－1－24. 患者データのバックアップ用に外付けハードディスクを付属すること
2－1－25. 外付けハードディスクドライブは、1ｍの落下に耐えうる耐衝撃性能及び耐静電性能・空冷性能を備えるとともに、CTG データをはじめとする各種情報を保持できること
2－1－26. クライアント端末は、胎児集中監視システム（コントロールユニット）と同等に各種情報を参照できること
2－1－27. 電子カルテ連携機能は、産科部門システムから患者基本情報「患者 ID・氏名・フリガナ・生年月日」及び産科部門システム側に「分娩予定日」情報がある場合は「分娩予定日（妊娠週数)」を取得できること
2－1－28. 電子カルテ連携機能は HIS 端末の WEB ブラウザ上で動作し、CTG 情報を参照できること
2－1－29. 電子カルテ連携機能の CTG 表示機能は、胎児集中監視システムと同等の CTG 参照機能を有し、測定中の CTG 波形も電子カルテ端末から時間の制限なく現在及び過去に遡り参照できること
2－1－30. 電子カルテ連携機能は HIS 端末からの参照で、病院現有の産婦人科セントラルモニタで保存されていた CTG データについても参照できること
2－1－31. 院内の電子カルテ端末で CTG 参照でき、かつ複数台の同時接続ができること

Ⅴ. 性能、機能以外に関する要件
1. 搬入・設置条件及び調整等に関すること。
1-1 調達物品の搬入に要する養生及び据え付け、稼動のための調整等を行うこと。
1-2 装置の納入場所については、当院の指定した場所に設置すること。
1-3 機械及び周辺装置の配線等は、当センターの関係者と十分協議したうえで施工すること
1-4 本装置が正常に動作するように、1 年間は無償で定期的に点検、調整を行うこと。
1-5 納入後 1 年間は、通常の使用により故障した場合の無償保証に応じること。
1-6 全工程終了後は、システム全体が正常に作動するよう動作確認した上で引き渡すこと。
1-7 装置に障害が発生した場合は、修理または調整作業を迅速に対応できる体制であること。
1-8 調達物品は、納入後においても稼動に必要な消耗品、及び故障時に対する交換部品の

安定した供給が確保されていること。
1-9 装置の運用を円滑にするための技術的なサポートを適切に行うこと。
1-10 操作マニュアルは、日本語版を 1 部用意すること。
1-11 本仕様に定めのない事項は、必要に応じ発注者と受注者とで協議して定めるものとする。
1-12 導入に伴うネットワーク費用及びその他設置にかかわる施設整備及び金具等、既設の病院情報管理システムへの対応費用も全て費用内に含むこと。
1-13 新規導入、更新に関わらず当センターへの影響は最小限にすること。
1-14 新規導入、更新に関わらず当センター情報セキュリティポリシーおよび情報統括部の指示に従うこと。

VI. 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. 情報セキュリティ水準の維持に関する対応や情報セキュリティインシデントを認知した際の対処など情報セキュリティ対策を実施するために必要な対応を記載した文書を提出すること。
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、排除するための対応(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する)を行うこと。
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。
    制限が出来ない場合は、その旨を記載した資料を提出すること。

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。