［リモート保守に関する要件］

No	項目	性能・機能
1.	リモート保守	1. 全般 (1) リモート保守を行う場合、広島市立病院機構が別途定めるリモート保守要件を確認すること。 (2) リモート保守環境構築、運用についての詳細は、本院のシステム担当者と協議のうえ、リモート保守を行うのによりセキュアな方法・環境構築を行うこと。 (3) 詳細・不明な点等については、本院のシステム担当者と協議のうえ、本院の了解を得るものとする。 (4) 本院側にて必要な要件を満たしていないと判断した場合には、実施可否も含めて別途システム担当者と協議のうえ、対応を決定するものとする。 2. ハードウェア (1) リモート保守に使用するルータ・ネットワーク機器群については、以下に留意のうえ、機器を選定すること。 ① 稼働・導入時点で発売から3年以内であること。 ② 稼働・導入時点でメーカーから当該機種のファームウェアサポートが行われていること。 ③ 稼働・導入時点で発見されている脆弱性等に対する対策（ファームウェア提供等）が行われていること。 ④ 通信要件、リモート設定等の要件を満たす最低な機種を選定すること。 (2) 導入するルータ・ネットワーク機器群のファームウェアは、リモート保守稼働開始時点で最新のファームウェアを適用すること。ただし、通信設定や安定動作等の面で適用を見送りたいような場合には、本院のシステム担当者と協議のうえ、対応を決定すること。 (3) ルータ等の通信機器で、脆弱性情報等が公開された場合、速やかにファームウェア更新等の手配を行うこと。 (4) リモート保守に踏台端末ないしサーバ・クライアント等への接続を行う場合、以下に留意のうえ、機器選定・端末設定を行こと。 ① 使用する端末の OS は、メーカーサポート対象期間内のものであること。 ② OS 自体の脆弱性対策の為、パッチ等の更新は適用し、随時更新・最新化しておくこと。 ③ 有効期限の切れていないセキュリティ対策ソフトを導入し、随時更新・監視しておくこと。 ④ リモート保守に必要な最低限のツールソフト以外はインストールしないこと。導入するリモート保守ツールについては、脆弱性等が報告されている場合は、パッチ等を適用し、最新化しておくこと。 ⑤ OS に付随するソフトでリモート保守に必要ないものは全てアンインストールもしくは無効化しておくこと。 ⑥ リモート保守で使用する OS のアカウント権限は、適切に設定すること。 管理者権限ではないリモート保守専用のアカウントを用意し実行すること。 ⑦ OS 上でのドライブ共有設定（管理共有、SMB によるネットワークドライブ設定等）は無効化しておくこと。 ⑧ OS 上で動作している不要な各種サービス群については、リモート保守に関係ないもの、セキュリティ対策上無効にしておくことが推奨されるものについては、無効化しておくこと。 ⑨ 定期的（月一回等）に踏台端末の OS 更新状態、ウィルス感染有無等の確認を行い、本院に報告を行うこと。 ⑩ 踏台端末の設置場所及び診療系 N/W への接続先は、本院側の指定する先に配置・接続すること。 ⑪ 踏台端末は常時起動している状態ではなく、リモート保守が必要となった際に本院側に連絡し起動させたり、作業終了後に端末シャットダウン（手動もしくはタスク等で）を行える運用も考慮すること。 ⑫ 詳細については、本院のシステム担当者と協議のうえ、設定を行うこと。 3. 通信設定 (1) リモート保守拠点との本院側とで安全な通信方法を確立すること。 (2) ルータの通信設定は、以下の内容を満たす設定を行い、通信設定に関して、本院側

		に条件設定内容を開示すること。 ① リモート保守拠点⇔リモート対象端末(サーバ・PC・踏台 PC を含む)間の通信のみ ② (踏台端末を利用する場合)踏台端末の OS の Update を行う為の通信のみ ③ (踏台端末を利用する場合)踏台端末のセキュリティ対策ソフトの定義更新の為の通信のみ ④ ルータ機器等のファームウェア更新の為の通信のみ ⑤ 上記①～④以外の全ての通信を遮断 ⑶ リモート保守に必要な機能以外のルータの不要サービスの停止・無効化を行うこと。 ⑷ 外部(WAN 側)からのルータ設定変更、ping 応答、ポートスキャン等のサービス停止・無効化を行うこと。 ⑸ リモート保守で使用する保守ツール、使用ポート等の情報は開示すること。 ⑹ 通信設定情報は、configファイルを保存し、障害等があった場合に復元可能な状態を維持すること。 ⑺ ルータ上での通信ログを採取できるようにすること。 4. インターネット通信 ⑴ リモート保守で接続する際のインターネット通信の使用は、本院がリモート保守に供する為に敷設している光回線網への接続とすること。 5. 脆弱性対応・定期報告 ⑴ リモート保守に使用するルータ、踏台端末、保守ツール等について、OS や機器本体やツールで脆弱性情報が公開された場合、速やかに影響状況を確認し、必要な措置をとれる体制・対応を取ること。ただし、通信設定や安定動作等の面で適用を見送りたいような場合には、本院のシステム担当者と協議のうえ、対応を決定すること。 ⑵ 脆弱性情報が判明した際に、速やかに調査を行い、結果を本院側に報告すること。 ⑶ リモート保守で使用するルータ、踏台端末、保守ツールの状況、脆弱性対応状況、踏台端末のウィルス感染有無等に関して、定期的に本院に報告を行う体制を取れること。急を要するような場合は、本院の求めに応じて速やかに確認・報告を行えるようにすること。