リモート保守回線に関するセキュリティ仕様書

本書は、外部からの不正アクセスやランサムウェア感染を防止するために、医療機器等に付随してルータ等のネットワーク機器（以下「ルータ」という。）及び回線等を設置する場合に遵守する必要がある事項を記載している。

原則として、リモート保守は必要な場合にのみ行うことし、実施する場合は、当院が別途構築しているリモート保守システムを利用することとする。ただし、真にやむを得ず、受託者が独自に構築する場合は特に責任を持って構築・運用すること。

1. 厚生労働省ガイドライン等の準拠

以下の資料に準拠した形で設置運用を行うこと。

(1) 厚生労働省「医療情報システムの安全管理に関するガイドライン」最新版

(2) 「医療機関におけるサイバーセキュリティ対策チェックリスト」最新版

2. ルータと回線の要件

(1) ルータ

業務上必要のない通信ポートはすべて遮断（ステルス設定等）すること。

利用期間中にメーカーサポートが得られるルータとすること。メーカーサポートが切れた場合は、当院と協議し、リモートの利用を終了するか、ルータを交換すること。

(2) 回線

原則としてインターネットを経由しない閉域網、または IP-VPN 回線を選定すること。

やむを得ずインターネット VPN を利用する場合でも、必要な VPN 設定を実施し、外部の接続元 IP を最小限に限定する等セキュリティを確保すること。

3. ID・パスワードおよび認証管理

(1) パスワードは、初期設定のパスワードから必ず変更し、英大文字・小文字・数字・記号を組み合わせた 12 文字以上の堅牢なものに設定すること。

(2) 別顧客（当院以外の病院等）と同一のパスワードを使い回さないこと。

(3) 可能な限り多要素認証を導入し、なりすましを防止すること。

4. 脆弱性対策とアップデート

(1) ルータ等の通信機器のファームウェアは、受注者側で最新か否かを常に確認すること。

(2) 脆弱性が発見された場合、速やかに（あるいは定期的に）最新バージョンへアップデートすること。

(3) アップデート作業に伴う費用および作業負担は、受注者の責任において行うものとする。

5. 有事の際の対応と責任の所在

(1) 万一、当該リモートの仕組みで不正アクセスやウイルス感染（ランサムウェア等）の疑いが発生した場合は、速やかに当院へ連絡し、被害拡大防止措置を講じること。

(2) 受注者の管理不備（脆弱性の放置、パスワード管理の不備等）に起因して当院に損害が生じた場合、与えた損害（逸失利益、データ破損・復旧費用、情報漏洩による賠償等一切を含む）に対して、損害賠償請求等を行う可能性があるため、十分注意すること。

6. その他特記事項

(1) リモート接続を実施する前に、当院の承認を得てから接続を開始すること。

(2) リモート接続の開始・終了日時、作業内容の記録を最低 5 年間保管し、当院の求めに応じて直ちに開示すること。

(3) リモート回線を廃止する場合は、設定情報を含むルータ等のデータ消去を行うこと。

7. 各種提出書類

(1)構築時に以下の「リモート保守構築資料」を提出すること。

【1】操作対象機器、設置場所

【2】リモート接続のネットワーク構成図(IP アドレスを含む)

【3】ルータの機種情報

【4】回線の種類

【5】認証方式

【6】運用時・緊急時の連絡先

(2)年に 1 回、以下の内容を含む「リモート保守運用報告書」を提出すること。

【1】操作対象機器、設置場所

【2】ルータのファームウェアバージョン（それが対応可能な新しいものであることの証明を含む）

【3】脆弱性情報の確認結果（確認日、確認方法を含む）

【4】ファームウェアのバージョンアップ実績、パスワードを変更した場合はその実績

【5】操作実績、アクセスログの異常の有無

【6】運用時・緊急時の連絡先