市立四日市病院医療情報システムにおけるリスクアセスメント及びサイバー攻撃に係る事業継続計画策定業務委託仕様書

近年、サイバー攻撃による医療情報システムへの侵害により診療の継続が困難となる事例が報告されており、医療情報システムの安全管理ガイドラインにおいて情報セキュリティインシデントに対する事業継続計画の整備が求められている。当院でも医療情報システムにおけるリスクアセスメントを実施し、その結果からサイバー攻撃に係る事業継続計画策定を行ない、情報セキュリティインシデント発生時の医療提供体制の維持強化を図る。

１．委託場所

市立四日市病院

２．委託期間

契約の日　から　令和７年３月３１日まで

３．業務内容

（ア）本業務には、『医療情報システムの安全管理に関するガイドライン第6.0 版』（厚生労働省）（以下、「安全管理GL」という）を基準として用いること。本業務に関連する安全管理GLの「遵守事項」に対して、該当する納品物の条項及び対応事項を示すこと。

（イ）本業務実施のための、実施方針、検討条件・方法、工程、実施体制等を検討し、実施計画書を作成し提出すること。本業務の遂行途中において計画に修正が必要と判断する場合は、情報処理係の承認のもと、速やかに変更を加えること。

（ウ）医療情報システムにおけるリスクアセスメントの実施・報告

当院における医療情報システムの現状の調査を実施し、リスクの見積り、優先度の設定、リスク対応措置をまとめた、報告書を作成すること。（本報告書には（エ）（オ）を実施するための内容を含めること）

（エ）情報セキュリティ対策ロードマップ（計画概要）の作成

リスクアセスメント結果から、優先度に応じた年次の情報セキュリティ対策のロードマップを作成すること。ロードマップは５年計画とする。

（オ）サイバー攻撃に係る事業継続計画（IT-BCP）の策定

・リスクアセスメント結果をふまえ、サイバー攻撃に係る事業継続計画を策定すること。

・当院の災害時対応マニュアル業務継続計画（BCP）との整合性を図ること。
・情報セキュリティインシデント発生時における対応計画には、具体的な復旧手順、紙媒体での運用、代替システム使用を含め、全体の流れ（全体フロー）を策定すること。
・IT-BCPの教育訓練の計画と、IT-BCPの各項目における維持改善計画を含めること。

（カ）各打ち合わせに関する会議等の議事録を作成すること。

（キ）本業務の実施にあたり、情報処理係以外の部門やシステムベンダーへのヒアリングが必要な場合は、実施すること。その際は、情報処理係の許可を得てから行うこと。

（ク）サイバー攻撃に係る事業継続計画の策定後に、当院経営層向けに説明を行なうこと。

（ケ）各打ち合わせは、定期的なリモート会議と月次１回の訪問にて開催する。

4. 作業要員に求める資格等の要件

本業務を円滑に推進し、かつ品質を確保するため、受託者は、次の資格及び業務経験を有するプロジェクトチームを編成すること。

（ア）資格要件

システムの評価に関する知識・技能、情報セキュリティ技術に関する知識・技能に有する専門家資格（次のいずれか）を保有する者が含まれていること

a. 情報処理安全確保支援士
b. CISSP（情報システムセキュリティプロフェッショナル）
c. システム監査技術者
d. CISA（公認情報システム監査人）

（イ）業務経験

業務の効率と品質の保持のため、次の実績（実務経験）を有する専門家が、１人以上含まれていること。

a. 医療情報システム安全管理ガイドラインに基づくアセスメント
b. 医療情報システム安全管理ガイドラインに基づくIT-BCPに関するコンサルティング

5．納品物

・情報セキュリティに係るリスクアセスメント結果報告書
・情報セキュリティ対策ロードマップ
・情報セキュリティに係る事業継続計画書
・各打ち合わせ、会議等の議事録