情報セキュリティ強化支援業務
仕様書

1　業 務 名　情報セキュリティ強化支援業務

2　目　　的　近年、標的型攻撃等のサイバー攻撃が巧妙化・激化してきている。サイバー攻撃への対策、サイバー攻撃を受けた際の行動指針など、今まで以上に情報セキュリティ対策強化を図っていく必要がある。このような状況を踏まえ、豊橋市民病院（以下「当院」）の情報セキュリティ対策を強化するためには、情報システム及びセキュリティに関する豊富な知識及び経験を有する専門家の支援が必要である。
このため、専門家に委託して情報セキュリティ対策、インシデント対応等に対する提案や助言を求め、当院の情報セキュリティ向上を図るものである。

3　業務期間　契約日　～　令和６年３月 31 日

4　業務場所　豊橋市民病院

5　業務内容

（1）サイバー攻撃へのセキュリティ対策

当院のサイバー攻撃対策として攻撃を受けた際の行動指針を明確にするとともにその教育を実施することに加え、サイバー攻撃の要因となりうる当院のセキュリティ上の脆弱性を把握するため、以下に掲げる業務を実施すること。

ア　サイバー攻撃またはその疑いがある場合のアクシデント等に迅速に対応するための業務継続計画を作成すること。

イ　サイバー攻撃またはその疑いがある場合に備え、豊橋市民病院が設置している CSIRT 要員への研修を企画し、実施すること。

ウ　当院の情報システムのリモートメンテナンスの脆弱性について調査・分析をし、対策を含めた報告書を作成すること。

（2）情報セキュリティ内部監査の実施

ア　各部署に対して、ポリシー等の遵守状況の確認及び手順の確認のための助言型の監査を実施すること。なお、監査の実施にあたっては、当院の実情に合わせて設定した監査項目ごとに具体的な確認事項となる監査要点を列挙した監査チェックシートを作成し、これを基に業務運用実態の訪問調査を行うこと。また、監査は予備調査にて監査対象となる業務や当該業務で取り扱う情報資産や利用する情報システムの基礎情報等を収集したうえで、訪問調査を行うこととする。

イ　監査終了後は報告書を作成し、監査証拠に裏付けられた合理的な根拠に基づく意見、制約または除外事項、その他当該監査の目的に照らして必要と判断した事項を明瞭に記載すること。また、改善指摘事項を記載する場合は、改善すべき理由となる顕在化もしくは残存しているリスク及び具体的な改善提案を記載すること。

（3）情報セキュリティポリシー対策基準及び情報セキュリティ実施手順書の見直し

情報セキュリティポリシー対策基準及び情報セキュリティ実施手順書を精査し、国からの要請事項や新たな脅威及び脆弱性等に対応するために改正すべき、あるいは改正することが望ましい事項を提案し、改正案を作成すること。

改正案の作成にあたっては、以下の法令及びガイドライン等に定められた事項についても反映させること。また、その他にも発出される情報セキュリティに関するガイドラインなどが示される場合は、改正案に含めること。

なお、情報セキュリティポリシー対策基準及び情報セキュリティ実施手順書は本件契約締結後に示すこととする。

・ 地方公共団体における情報セキュリティ監査に関するガイドライン

・ 医療情報システムにおける安全管理に関するガイドライン
・ 個人情報の保護に関する法律
・ 個人情報の保護に関する法律施行規則
・ 臨床研究法
・ 臨床研究法施行規則
・ 人を対象とする生命科学・医学系研究に関する倫理指針
・ その他医療機関等に関係する法令及びガイドライン

（4） 情報セキュリティ対策中期計画の策定

計画的に情報セキュリティ体制を維持・強化するために、情報セキュリティ対策中期計画（令和６年度から８年度まで）を策定する。

ア 過去２ヶ年の当院のアクシデント等の発生傾向を分析し、対策を提案すること。

イ 情報セキュリティ体制を維持・強化するため、自己点検及び内部監査の結果等により確認できた職員のポリシー等の習熟度を分析し、更なる定着を図るために３年間の中期計画（令和６年度から令和８年度まで）案を作成すること。

ウ 中期計画案作成中であっても自己点検及び内部監査の結果分析により令和５年度において即座に対応するべきことについては情報セキュリティ委員会（以下「委員会」）や部会で提案すること。

（5） 職員向け情報セキュリティ研修及び点検の実施

情報セキュリティ委員会の要請に基づいた研修計画を策定、研修教材を作成し、集合研修にて講師業務を実施すること。実施区分・予定受講者数は以下のとおりとする。研修実施後は職員の情報セキュリティに対する知識の定着状況及びポリシー等の遵守状況を把握するために、職員への点検を実施しその報告をすること。

ア 管理者向け（情報セキュリティ責任者・管理者等 20 名～60 名程度）

イ 中堅者向け（新任主査職・新任主任看護師 20 名～30 名程度）

ウ 院内全職員（委託含む）向け

（6） 情報セキュリティ委員会・部会での報告と助言

ア 当院が設置する委員会及び部会の運営支援として、資料説明や質疑応答を行うこと

イ 委員会及び部会において把握した課題から議題を提案すること

ウ 委員会は年３回程度開催を予定（常に１名以上の受託担当者が出席していること）

エ 部会は年４回程度開催を予定（常に１名以上の受託担当者が出席していること）

オ 委員会及び部会の開催にあたっては事前に発注者と打ち合わせするものとする

7 実施体制

（1） 本業務を確実に履行できる体制を設けること

（2） 本業務の管理及び統括を行い、発注者との情報共有や連絡を行う担当者を定めること。

（3） 各業務の実施にあたっては、「6 業務内容」に精通し、当院の情報セキュリティポリシー対策基準及び情報セキュリティ実施手順書を十分に理解できるものを配置すること。

8 成果物

本業務で想定している成果物は以下のとおりである。

成果物	内容
業務完了報告書	各業務の実施結果をまとめたもの
その他	本業務の遂行過程で取得し、又は作成した資料

電子媒体と紙媒体各１部提出すること

成果物の詳細は、業務の仕様に応じて発注者と協議し決定する。

9　その他

（1） 各業務の検討を行うため、月１回程度の打ち合わせを実施するものとする。なお、打ち合わせの出席については、発注者が認めた場合は、Web 会議システムを活用してよいものとする。

（2） 各業務の実施にあたっては、各業務の進捗状況を適時発注者に報告するとともに充分協議したうえで行うこと

（3） 情報セキュリティ対策強化に関する必要な情報を発注者に情報提供のうえ、アドバイス等の支援を行うこと

（4） 打合せ及び協議後は速やかに打合せ・協議記録簿を作成し提出すること

※受託者は、業務の全部又は一部を第三者に委託し、又は請け負わせてはならない。ただし、受託者は、あらかじめ発注者の書面による承諾を得たときは、業務の一部を第三者に委託し、又は請け負わせることができる。