別紙

「診療所における医療情報システムのサイバーセキュリティ対策に係る調査」
回答要領

依頼事項

- 本回答要領に基づき、診療所における医療情報システム（※）のサイバーセキュリティ対策に係る調査（以下「本調査」という。）について回答をお願いします。

- 回答にあたっては、必ず本回答要領を確認してください。

- 本調査は「医療情報システムの安全管理に関するガイドライン」・「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」及び厚生労働省等から発出された通知・事務連絡等の内容を基に調査します。これらの文書について確認の上、回答してください。

  参考：

  「医療情報システムの安全管理に関するガイドライン」および「医療機関・薬局におけるサイバーセキュリティ対策チェックリスト」については、以下のＵＲＬより最新版をご参照ください。調査票回答画面からもアクセスできるようにしておりますのでご活用ください。

  https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

- 技術的な質問・用語等については、院内担当者だけでなくシステム設置事業者や保守ベンダーへ照会等を行い、質問内容を理解した上、回答してください。

- 回答は、令和８年６月末時点の状況についてお答えください。

（※）医療情報システムとは、オーダリングシステム、電子カルテシステム、レセプト電算システム（審査請求受付も含む）、画像・検査等の各部門システム、地域医療ネットワークシステム、PHR 等、診療所における診療を補助するためのシステム全般を指します。

【調査項目について】

Ｑ１　回答者の氏名

回答者の氏名を記載してください。

Ｑ２　医療情報システム安全管理責任者を設置している

医療情報システム安全管理責任者とは情報セキュリティ対策に関する統制の実効性を確保するために、安全管理を直接実行する者を指します。医療情報システム安全管理責任者としての職務は、経営層が担うことを想定していますが、医療機関等の規模・組織等を考慮して、企画管理者が医療情報システム安全管理責任者を兼務することは可能です。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編　3.安全管理全般【遵守事項】
③ 安全管理を直接実行する医療情報システム安全管理責任者及び
企画管理者を設置すること。

Ｑ３－１　サイバー攻撃等によるシステム障害発生時に備え、事業継続計画(BCP)を策定している

「医療情報システムの安全管理に関するガイドライン」では、情報セキュリティインシデントが発生し、医療情報システムの可用性が損なわれる事態に備えて、通常時から、非常時における医療情報システムの運用に関する対応を整理することが重要である、と求めています。自組織において、サイバー攻撃等に備えた事業継続計画（BCP）を策定している場合は「はい」を選択してください。サイバー攻撃等とは、医療情報システムの稼働（可用性）が損なわれる、災害、サイバー攻撃、システム障害等が想定されます。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編 3.安全管理全般【遵守事項】
⑬ 情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の
判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP 等を整備すること。

Ｑ３-２　Ｑ３-１に対して「はい」を選択した方が対象となる質問です。
事業継続計画（BCP)において策定された対処手順が適切に機能するか、訓練等により確認している

「医療情報システムの安全管理に関するガイドライン」では、自組織において定められているサイバー攻撃を想定した事業継続計画（BCP）が適切に機能することを訓練等により確認することが重要であるとされています。自組織の事業継続計画（BCP）において策定された対処手順が適切に機能することを、訓練等により確認している場合は「はい」を選択してください。

参考：「医療情報システムの安全管理に関するガイドライン」
経営管理編 3.安全管理全般【遵守事項】
⑮ 通常時に整備していた BCP が、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。

Ｑ４　サーバ、端末、ネットワーク機器の台帳管理を行っている

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者（医療機関の危機管理を行う責任者のこと）に対して診療所で所有する医療情報を扱うシステムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認可能な状態とすることを求めています。

これを満たしている場合は「行っている」を選択してください。紙媒体であっても電子媒体であっても構いません。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

参考：「医療情報システムの安全管理に関するガイドライン」
企画管理編　9.医療情報システムに用いる情報機器等の資産管理【遵守事項】
① 医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。

Ｑ５　少なくとも年１回程度、職員を対象として、情報セキュリティに関する研修を行っている

「医療情報システムの安全管理責任者が、職員向けに実施する情報セキュリティに関する研修を指します。研修を実施している場合は「はい」を選択してください。

医療機関向けセキュリティ教育支援ポータルサイト：MIST（https://mist.mhlw.go.jp/）で提供される e-learning 研修等も該当します。

参考：「医療情報システムの安全管理に関するガイドライン」

企画管理編　7.安全管理のための人的管理【遵守事項】

② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。

Ｑ６　自組織において、電子カルテシステムを使用している

診療録の記載・保存を電子カルテシステムで行っている場合は「はい」を選択してください。

なお、本問でいう電子カルテシステムとは、以下を指します。

- オーダリング機能、画像管理等の部門システム及び診療録を電子的に記録する機能を備えた統合的な医療情報システム