別紙

「病院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、病院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（6.0 版）」・「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」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するため、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（第 6.0 版）
  （添付ファイル 002～005）

  ・医療機関のサイバーセキュリティ対策チェックリスト
  （添付ファイル 006～007）

- 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３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、病院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】

Ｑ１−１　回答者の氏名

回答者の氏名を記載してください。

Ｑ１−２　回答者の所属（病院名）

回答者の所属（法人名および病院名）を記載してください。

Ｑ１−３　電子カルテ等の情報システム担当者の所属部署名

電子カルテ等の情報システム担当者の所属部署名を記載して下さい。
（例：情報システム部、医療情報部、総務課、医事課）

Ｑ１−４　回答者の連絡先（メールアドレス）

記入いただいたメールアドレスには、厚生労働省から、事業に関するお知らせや、注意喚起等を送付するためにのみ利用します。
その他の用途に用いることはありません。

Ｑ１−５　回答者の所属部署の責任者の連絡先（メールアドレス）

回答者様の上司に当たる、課長、部長職の方のメールアドレスの入力をお願いいたします。記入いただいたメールアドレスには、厚生労働省から、事業に関するお知らせや、注意喚起等を送付するためにのみ利用します。
その他の用途に用いることはありません。

Ｑ２−１　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 6.0 版」
経営管理編　3.1.2 医療情報システムにおける統制上の留意点
② 医療機関等において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。

Ｑ２-２　Ｑ２－１に対して「はい」を選択した方が対象となる質問です。医療情報システム安全管理責任者は情報処理に関連した資格を保持している

情報処理推進機構(IPA)の資格に限らず、民間資格についても「はい」を回答いただけます。

Ｑ２-３　Ｑ２-２に対して「はい」を選択した方が対象となる質問です。医療情報システム安全管理責任者が情報処理推進機構(IPA)の情報処理実理技術者資格または試験で合格しているものはいずれか（複数選択可）

所持している資格をすべて選択してください。民間資格については「その他」を選択してください。

Ｑ３　情報システム部門の所属人数は何人か

情報システム部門の所属人数を選択肢から選択してください。所属人数とは常勤で専任（就業時間の 5 割以上、当該業務に従事している）職員の人数とします。部門を設置していない場合は０人を選択してください。

Ｑ４　調達権限を持つ各部門（診療部門、薬剤部門、看護部門、放射線部門、事務部門等）に情報セキュリティ担当者を設置している

調達権限を持つすべての部門に情報セキュリティ担当者を設置している場合に「はい」を選択してください。

情報セキュリティ担当者とは、その部門において情報セキュリティインシデント等が発生した場合に、インシデントのとりまとめを行う責任者を指します。情報セキュリティ担当者には、医療情報システムの調達への関与、インシデントの院内全体への共有や、サイバーセキュリティに関する情報の部門内普及啓発をすることが期待されます。 すべての調達部門に配置で「はい」としてください。

Ｑ５　インシデント発生時の対策チーム（組織内 CSIRT）を設置している

院内で何らかの情報セキュリティインシデントが発生した場合に対応をする、特定のインシデント対策チーム（CSIRT: Computer Security Incident Response Team）を設置している場合に「はい」を選択してください。

CSIRT はコンピュータセキュリティにかかるインシデントに対処するための組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をします。

Ｑ６　JAHIS および JIRA が策定した MDS/SDS（医療情報セキュリティ開示書）を用いて点検している

「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」では、事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらうこととしています。当該文書を活用し、自組織が保有している情報機器・システムが「医療情報システムの安全管理に関するガイドライン」への準拠性を確認している場合は、「はい」を選択してください。Ver5.0 以上であることとします。

参考：「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド Ver.5.0
<https://www.jahis.jp/standard/detail/id=1119>

MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security)）：医療情報セキュリティ開示書（製造業者/サービス事業者による医療情報セキュリティ 開示書の略称です。各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明 の標準的記載方法（書式）を JIRA(一般社団法人日本画像医療システム工業会)/JAHIS で定めた物 で、製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジ メントを実施する医療機関等を支援するため、医療機関等側において必要な対策の理解を容易にすることなどの用途に用いられることが想定されています。

Ｑ７－１　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、「不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、事業継続計画（BCP）として定めておくことが重要である」としています。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 6.0 版」
経営管理編 3.4.1 事業継続計画（BCP：Business Continuity Plan）の整備と訓練
①　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。

Ｑ７－２　Ｑ７－１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 6.0 版」
経営管理編 3.4.1 事業継続計画（BCP：Business Continuity Plan）の整備と訓練
③ 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。

Ｑ８　サーバ、端末 PC、ネットワーク機器（医療機器を除く）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、厚生労働省としては企画管理者に対して医療機関で所有する医療情報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「院内全体の台帳管理を行っている部門」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。

Ｑ９　ネットワークに接続される医療機器の一元的な台帳管理を行っている

医療機関で所有する医療情報システムとして用いる医療機器等について機器台帳を作成して管理を行い、医療機器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が重要です。

これを満たしている場合は「院内全体の台帳管理を行っている部門」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医療機器の設置部署、MAC アドレス、ソフトウェアのバー

ジョンなどが想定されます。

Q10　ネットワーク構成図を定期的に更新しており、各部門でいくつの外部接続点が存在するか把握できている

「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、医療情報システムに関する全体構成図（ネットワーク構成図等）を作成し、常に最新の状態を維持することとしています。また、医療情報システムを、外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、監視を行うこととしています。各部門の外部接続点数を含むネットワーク構成を俯瞰的に把握できている場合は「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 6.0 版」
システム運用編　2. システム設計・運用に必要な規程類と文書体系
② 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態を維持すること。
システム運用編　13. ネットワークに関する安全管理措置
⑪ 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。

Q11　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。

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：疑義解釈資料の送付について（その 30）
【診療録管理体制加算】
問２　「Ａ２０７」診療録管理体制加算の施設基準において、「専任の医療情報システム安全管理責任者を配置すること。また、当該責任者は、職員を対象として、少なくと も年１回程度、定期的に必要な情報セキュリティに関する研修を行っていること。」 とあるが、厚生労働省委託事業として運営される「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/）」上で提供される研修に職員を 参加させた場合は、ここでいう「情報セキュリティに関する研修を行っていること」 に該当すると考えてよいか。

（答）該当する。MIST で提供される研修には、一般職員向けの「初学者等向け研修」、経営 層向けの「経営者向け研修」、システム担当者向けの「システム・セキュリティ管理者向け研修」等があり、対象者に応じて適切に活用すること。

Q12　ネットワーク機器に対して定期的にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが必要となります。ルータ等のネットワーク機器に対してこの対応ができている場合には「はい」を選択してください。

（用語の解説）

パターンファイル：ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。

（補足）

古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム

全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

Q13　サーバ、端末 PC に対して、定期的にセキュリティパッチ（最新ファームウェアや更新プログラム）を適用している

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に

運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが必要となります。すべてのサーバ、端末 PC に対してこの対応ができている場合には「はい」を選択してください。

Q14―１　医療情報システムに二要素認証を導入している

「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「利用者認証にパスワードを用いる場合には、令和９年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。」としています。

自施設の医療情報システムすべてに対して二要素認証を導入している場合は、「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 6.0 版」

システム運用編　１４．１．１ 利用者の識別・認証

また医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬 局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末 が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証 が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体の いずれか 2 つ以上）の認証がなされている場合には、二要素認証に相当すると考えてよい。

Q14―２　Q14－１に対して「はい」を選択した方が対象となる質問です。
二要素認証の導入に要した金額規模はいずれか

二要素認証を導入した際に要した実際の費用の概算を選択してください。

法人グループなどで、複数施設同時に導入した場合は１施設あたりの費用を概算して回答してください。

Q14―３　Q14－１に対して「いいえ」を選択した方が対象となる質問です。
二要素認証が導入できない理由はいずれか

二要素認証を導入していない理由にもっとも近いものをひとつ選択してください。

Q15　医療情報システムのパフォーマンス管理と死活監視を行っている

医療情報システムが正常に稼働しているか、継続的にパフォーマンス管理や、

死活監視を行うことが必要です。異常が検知された場合に、速やかにその状況が把握できるようにする体制を設けている場合は「はい」を選択してください。事業者に委託している場合も「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 6.0 版」
システム運用編　11. システム運用管理（通常時・非常時等）
② 医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。

Q16　令和６年６月に総務省、厚生労働省、経済産業省においてとりまとめた「医療情報システムの契約における当事者間の役割分担等に関する確認表」を知っている、または事業者との契約の際に利用している。

「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、「運用管理においては、医療機関等とシステム関連事業者との間で決定された責任分界を、契約書や SLA（Service Level Agreement：サービス品質保証、サービス・レベル合意書）などの形で双方の拘束力ある合意文書として明らかにした上で、具体的に責任分界を踏まえた運用を行うことが求められる。」としています。

事前に医療機関と事業者双方の役割分担等について取り決め、有事の際に即座に対応できるよう、契約の段階で合意形成文書（契約書やサービス・レベル合意書（SLA）等）に落とし込むことが重要です。「医療情報システムの契約における当事者間の役割分担等に関する確認表」では契約において、医療機関と事業者が役割分担等を協議する上で必要な項目について、具体化を図っています。

「医療情報システムの契約における当事者間の役割分担等に関する確認表」を知っている、もしくは事業者との契約の際に利用している場合は「はい」を選択してください。

参考：医療情報システムの契約における当事者間の役割分担等に関する確認
https://www.meti.go.jp/shingikai/mono_info_service/medical_information_system/checklist.html

Q17―１　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。

- オーダリングシステム
- 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

Q17―２　Q17―１に対して「はい」を選択した方が対象となる質問です。
オフラインバックアップを確保している

「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、「電子カルテシステムなど重要なファイルは、端末及びサーバ装置やネットワークから切り離したバックアップデータを保管すること」が重要であるとされています。

オフラインでバックアップデータを保管している場合は「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 6.0 版」
システム運用編　18. 外部からの攻撃に対する安全管理措置
① 医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。

- バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）