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。

（※）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。

Ｑ２－１　医療情報システム安全管理責任者（CISO）を設置している

「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、医療情報システム安全管理責任者を設置することとしています。自組織において、医療情報システム安全管理責任者（システム管理者）が設置されているか、回答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　3.1.2 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。 CISO は医療情報に関連した資格を保持している

情報処理推進機構の資格に限らず、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。 CISO が情報処理推進機構の実施する情報処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）

CISO の保持している資格を選択してください。民間資格については「その他」を選択してください。

Ｑ２－３　その他の資格または試験を記入してください。

CISO の保持している民間資格等を自由記載してください。必須記載ではありません。

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。

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。

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。

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。

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。

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「はい」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。

Ｑ10　厚生労働省や関係団体などから発出されるサイバー攻撃に係る注意喚起や脆弱性情報を日頃から収集・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、「自組織において日頃から脆弱性情報を収集し、速やかに対策を行える体制を整えておくことが必要である」としています。自組織において、厚生労働省および関係省庁等から発出されるサイバー攻撃に係る注意喚起通知や脆弱性情報を日頃から収集し、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 3.4.2　情報共有・支援、情報収集

② 情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策やEOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示すること。

Q11　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。

Q12　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。

Q13　医療情報システムのログインパスワード規程は最低何桁か（半角数字で入力）

「医療情報システムの安全管理に関するガイドライン」の Q&A では「医療情報を取り扱う医療情報システムの性格や構成を鑑みると、原則として、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが求められる。ただし、利用するパスワードが 13 文字以上のランダムな設定がなされており、パスワード管理の安全性などが担保されているシステムを用いている場合には、パスワードの定期的変更は必ずしも求められない。
また、医療情報システムのシステム上の制約等で 13 文字以上の文字列を設定できない又は適切な管理を行うことができない環境においては、推定困難なパスワードを、脆弱にならない形で定期的に変更させることにより、安全性を担保することができると考えられます。この場合、英数字、記号を混在させた８文字以上の推定困難な文字列のパスワードでもよい」としている。
　自施設の医療情報システムにおけるパスワードの最低桁数を記載してください。

Q14　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。」としている。
　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。

Q15　USB メモリ等の外部接続媒体の使用を運用管理規程やシステムで制限している

「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「システム運用担当者は、医療機関等の外部への医療情報の持出しに関する具体的な手順を、企画管理者が策定する規程を踏まえて作成する。手順は、持ち出す医療情報や記録媒体、持出し方法の種類や特性に応じて策定する。また手順における策定対象は、持出し前の手続から、外部からの持ち帰り等に至るまでを想定する。」としている。

外部接続媒体の使用を運用管理規定またはシステムで制限している場合は「はい」を選択してください。

Q16　医療機関とシステム事業者等の役割分担を契約書やサービスレベル合意書に落とし込んでいる

「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。

契約書やサービスレベル合意書に落とし込んで事業者との役割分担を決定している場合は「はい」を選択してください。

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。 電子カルテシステムのバックアップデータを作成しているか

「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、非常時には医療情報システムが完全に停止してしまうおそれがあることから、定期的なバックアップを実施することが望ましいとされています。自組織において、バックアップデータを作成しているか、回答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）

① 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。

- 重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

Q17-３　Q17-２に対して「はい」を選択した方が対象となる質問です。
電子カルテシステムのバックアップデータ作成個数は何個か

「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、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップデータの保存する電磁的記録媒体等の種類や世代管理の方法等を考慮して保管することが求められています。何個のバックアップデータを作成しているか、回答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）
①　非常時の医療情報システムの運用について、次に掲げる対策を実施すること。
- 重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。
-

Q17-４　Q17-２に対して「はい」を選択した方が対象となる質問です。
バックアップを何種類の方式で取得しているか

「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、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップデータの保存する電磁的記録媒体等の種類や世代管理の方法等を考慮して保管することが求められています。バックアップデータを何種類の電磁的記録媒体で保管しているか、回答を選択してください。

例えば、NAS（Network Attached Storage）とクラウドストレージへの保存の組み合わせで 2 種類と考えられます。

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」
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）

Q17-５　Q17-２に対して「はい」を選択した方が対象となる質問です。
バックアップを何世代で管理しているか

「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、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップデータの保存する電磁的記録媒体等の種類や世代管理の方法等を考慮して保管することが求められています。バックアップデータにおいて管理している世代数を回答してください。

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 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）
① 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。
- 重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

Q17-６　Q17-２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か

「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）