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　回答者の情報（氏名、所属、連絡先）

回答者の氏名、所属（法人名および病院名）、連絡先を記載してください。回答内容によっては、後日、確認のため厚生労働省より回答者に対し連絡をさせていただく場合がございます。

Ｑ２　医療情報システム安全管理責任者（システム管理者）を設置していますか。

「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、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。

Ｑ３　医療情報の管理、医療機関等外への持ち出し、破棄等の方針等を含む情報管理に関する規程を定めていますか。

「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、医療情報の管理、医療機関外への持ち出し、破棄等の方針と手順を含む情報管理に関する規程等を定めることとしています。

医療情報の持ち出しについては、適切に行わなければ、漏洩のリスクを伴います。組織として情報又は情報機器の持ち出しを どのように取り扱うかを整理した方針・手順を策定しているか、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」
企画管理編　8. 情報管理（管理、持ち出し、破棄等）
① 医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。

Ｑ４　医療情報システムの契約締結、契約更新やシステムの追加構築等の際に、医療機関とシステム関連事業者等の責任分界を考慮して協議していますか。

「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、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、契約書等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としています。医療情報システムの契約締結時等に、責任分界を協議しているか、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」
企画管理編　2. 責任分界
① 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。

Ｑ５　自組織の医療情報システムに接続する、外部接続等を含むネットワーク構成を把握していますか。

「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、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。医療機関内の医療情報システムに接続する、外部接続を含むネットワーク構成を俯瞰的に把握しているか、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　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。

Ｑ６　サイバーセキュリティに係る相談先として、当てはまるものを選択してください。
① 自医療機関
② 事業者
③ 他医療機関
④ その他
⑤ 相談先がない(相談先を求めている)
⑥ 相談先がない（相談先を求めていない）

「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の発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取り決めや体制を整備することとしています。平時の医療機関内のサイバーセキュリティに係る相談先について、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 3.4.2 情報共有・支援、情報収集
① 情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を 想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。

Ｑ７　サイバー攻撃またはサイバー攻撃の兆候を認めた際に連絡するべき医療情報システムの保守ベンダー・所管官庁等の連絡先を把握していますか。

「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、不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合は、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備することとされています。自組織において、サイバー攻撃等により医療情報システムに障害が発生した際、所管官庁や保守ベンダーなどの緊急連絡先を把握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」
経営管理編 3.4.3 情報セキュリティインシデントへの対応体制
① 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。

Ｑ８　厚生労働省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・確認していますか。

「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、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されています。自組織において、厚生労働省および関係省庁など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 3.4.2　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。

Ｑ９　自組織が使用している情報機器・システム・サービスが「医療情報システムの安全管理に関するガイドライン」に準拠しているかを確認するために、一般社団法人保健医療福祉情報システム工業会（JAHIS）および一般社団法人日本画像医療システム工業（JIRA）が策定した「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)」を用いて点検していますか。

「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されています。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か、回答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.4.1
https://www.jahis.jp/standard/detail/id=987
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。

Q10　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）を策定していますか。

「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、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されています。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 3.4.1 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。

Q10－１は、Q10 に対して「はい」を選択した方が対象となる質問です。「いいえ」を選択した場合は、Q11 に進んでください。

Q10－１　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ますか。

「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、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 3.4.1 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。

Q11　自組織において、電子カルテシステムを使用していますか。
※電子カルテシステムは「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」を指す。

診療録の記載・保存を電子カルテシステムで行っているか回答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

以下、Q12 は、Q11 に対して「はい」を選択した方が対象となる質問です。「いいえ」を選択した場合は、Q13 に進んでください。

Q12　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ますか。

「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。

以下、Q12-１～６は、Q12 に対して「はい」を選択した方が対象となる質問です。

Q12-１　電子カルテシステムのバックアップデータの更新頻度について、当てはまるものを回答してください。
① 毎日
② 週１回
③ 月１回
④ 年１回
⑤ その他

「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、バックアップの周期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の更新頻度について回答を選択してください。
複数の記録媒体でバックアップデータを更新している場合は、最も高い頻度で更新している期間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　18.1 サイバーセキュリティ対応
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、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した記録媒体を端末及びサーバ装置やネットワークから切り離して保管すること等を考慮して対策を講じることが強く求められる。

Q12-２　バックアップデータを何個作成していますか。
① ３つ以上
② ２つ
③ １つ

「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。

Q12-3　バックアップデータは複数の時点による保存（世代管理）を行っていますか。当てはあるものを回答してください。
① ３世代以上
② ２世代
③ １世代

「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の世代管理の状況について、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。

Q12-4　バックアップデータは、何種類の電磁的記録媒体で取得していますか。
① ３種類以上
② ２種類
③ １種類

「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。

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）

Q12-5　バックアップデータのうち、一つは、端末及びサーバ装置やネットワークから切り離された環境（オフライン）で保管していますか。

「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　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）

Q12-6　バックアップデータは、漏洩対策を講じていますか。
（例：バックアップデータの暗号化、秘密分散管理、アクセス権限の設定）

作成しているバックアップデータが、仮にサイバー攻撃等を受ける事態が起こった場合等においても、解読できない等、漏洩対策（暗号化や秘密分散管理等）を講じているか、回答を選択してください。ただし、具体の管理方法まで

問うものではありません。

Q13-１　サーバについて、バックグラウンドで動作している不要なソフトウェア及びサービスを停止していますか。

「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、不正ソフトウェアは電子メール、ネットワーク等の様々な経路を利用して医療情報システム内に侵入する可能性があるため、システム側の脆弱性を低減するため、利用していないサービス等を非活性化させることが重要であるとされています。サーバにおいて、不要なソフトウェアやサービスを停止しているか、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　8.1 不正ソフトウェア対策
不正ソフトウェアの対策としては、医療情報システム側の脆弱性を可能な限り小さくしておくことや被害拡大防止策を講じておくことが重要である。そのために実施すべき対策として、利用していないサービスや通信ポートの非活性化等がある。

Q13-２　端末ＰＣについて、バックグラウンドで動作している不要なソフトウェア及びサービスを停止していますか。

「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、不正ソフトウェアは電子メール、ネットワーク等の様々な経路を利用して医療情報システム内に侵入する可能性があるため、システム側の脆弱性を低減するため、利用していないサービス等を非活性化させることが重要であるとされています。端末ＰＣにおいて、不要なソフトウェアやサービスを停止しているか、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　8.1 不正ソフトウェア対策
不正ソフトウェアの対策としては、医療情報システム側の脆弱性を可能な限り小さくしておくことや被害拡大防止策を講じておくことが重要である。そのために実施すべき対策として、利用していないサービスや通信ポートの非活性化等がある。