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「医療情報の安全管理に関するガイドライン（5.2 版）」・「医療機関のサイバーセキュリティ対策チェックリスト」・「医療情報システム等の障害発生時の対応フローチャート」及び厚生労働省等から発出された通知・事務連絡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 5.2 版）、「医療機関のサイバーセキュリティ対策チェックリスト、医療情報システム等の障害発生時の対応フローチャート

https://www.mhlw.go.jp/stf/shingi/0000516275_00002.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。

【調査項目について】

Ｑ１　回答者の情報

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、医療情報システム安全管理責任者を設置することとされています。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」6.3.組織的安全管理対策（体制、運用管理規程）

C. 最低限のガイドライン

1. 医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定すること。ただし、小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。

Ｑ３　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、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。

（※）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。

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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

C. 最低限のガイドライン

5.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）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発 1029 第１号医政地

発 1029 第３号、医政研発 1029 第１号　平成 30 年 10 月 29 日）に基づき、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。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。

参考：「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発 1029 第１号、医政地発 1029 第３号、医政研発 1029 第１号　平成 30 年 10 月 29 日）（抜粋）

１　「医療情報システムの安全管理に関するガイドライン」の周知徹底について

医療機関等においてサイバー攻撃を受けた際の非常時の対応については、「医療情報システムの安全管理に関するガイドライン 第５版」（平成 29 年５月 30 日政統発 0530 第１号。以下「ガイドライン」という。）に定められているところです。医療機関等に対するサイバー攻撃の危険性がさらに高まっていることに鑑み、貴職におかれましては、管内の医療機関等に対して、ガイドラインの更なる周知徹底を図るとともに、医療機関等においてコンピュータウイルスの感染などによるサイバー攻撃を受けた疑いがある場合にあっては、別紙を活用して直ちに医療情報システムの保守会社等に連絡の上、当該サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、速やかに当該医療機関等から厚生労働省医政局研究開発振興課医療技術情報推進室（以下「医療技術情報推進室」という。）に連絡を行うよう、注意喚起をお願いいたします。

※2023 年１月現在の厚生労働省報告先は、「医政局特定医薬品開発支援・医療情報担当参事官室」となります。

Ｑ４　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、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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

(4) 非常時に備えたセキュリティ体制の整備非常時やサイバー攻撃などに対して、的確に対応できるためにセキュリティ体制を医療機関等においても構築することが求められる。非常時等において必要な原因関係の調査、必要なセキュリティ対応等に関する指揮、所管官庁等への報告などの体制については、医療の継続を確保する観点からも平常時から明確にする必要がある。また、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなどが強く求められる。また、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。

Ｑ５　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)」（厚生労働省標準）を用いて点検しているか。

「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)」とは、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）において定められた文書です。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.4.0
https://www.jahis.jp/standard/detail/id=779

Ｑ６　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」6.10. 災害、サイバー攻撃等

の非常時の対応（抜粋）

また、サイバー攻撃によるセキュリティインシデントが発生した際、数世代前までのバックアップデータは既に不正ソフトウェアが混入による影響が及んでいる可能性が高く、不用意にバックアップデータから復旧することで被害を繰り返し、場合によっては被害を拡大することになりかねない。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、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

Ｑ６－１は、Ｑ６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、Ｑ７に進んでください。

Ｑ６－１　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、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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

また、サイバー攻撃によるセキュリティインシデントが発生した際、数世代前までのバックアップデータは既に不正ソフトウェアが混入による影響が及んでいる可能性が高く、不用意にバックアップデータから復旧することで被害を繰り返し、場合によっては被害を拡大することになりかねない。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、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

Ｑ７　自組織において、電子カルテシステムを使用しているか。
※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、

- 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

を指します。

Ｑ８は、Ｑ７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。

Ｑ８　電子カルテシステムのバックアップデータ作成について、当てはまるものを選択してください。
①バックアップデータを１つ作成している
②バックアップデータを２つ以上作成している
③バックアップデータを作成していない

「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、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、サイバー攻撃等により、電子カルテシステムのデータが消失又は使用不可能な状態（暗号化等）になった場合でも、バックアップデータを作成し診療に大きな支障がないように復旧が可能か、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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

何らかのシステム障害が発生した場合においても、診療に重大な支障がない最低限の見読性を確保する対策も考慮に含める必要がある。特に、災害等の非常時には、システムが完全に停止してしまうおそれもあるため、定期的なバックアップを実施して、診療録等に記載された患者情報を確認できるようにしておくことが望ましい。

Ｑ９およびＱ９－１は、Ｑ８に対して「②バックアップデータを２つ以上作成している」を選択した方が対象となる質問です。

「①バックアップデータを１つ作成している」を選択した場合はQ10 に、「③バックアップデータを作成していない」を選択した場合は、Q11 に進んでください。

Ｑ９　バックアップデータの作成方式について、当てはまるものを選択してください。

①「追記可能な設定がなされた媒体」と「追記不能設定がなされた媒体」を組み合わせて取得している。

②「追記可能な設定がなされた媒体」または「追記不能設定がなされた媒体」のどちらか一方のみで取得している。

「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複数の方式（「追記可能な設定がなされた媒体」と「追記不能設定がなされた媒体」）を組み合わせてバックアップデータを保管することが重要とされています。複数の方式を組み合わせて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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

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媒体と追記不能設定がなされた媒体の組み合わせ、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）で取得することが重要である。

Ｑ９－１　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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

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媒体と追記不能設定がなされた媒体の組み合わせ、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）で取得することが重要である。

Ｑ10 からＱ10－２は、Ｑ８に対して「①バックアップデータを１つ作成している」または「②バックアップデータを２つ以上作成している」を選択した方が対象となる質問です。

Ｑ10　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、当てはまるものを選択してください。
①１か月以内に１回
②１か月～３か月以内に１回
③３か月～半年以内に１回
④半年～１年以内に１回
⑤バックアップデータを更新していない。

「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、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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、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。例えば、日次でバックアップを行う場合、数世代（少なくとも３世代）確保し、遅くとも 3 世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。

Q10－１　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世代管理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」6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、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。例えば、日次でバックアップを行う場合、数世代（少なくとも３世代）確保し、遅くとも 3 世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。

Q10－２　バックアップデータは、漏洩対策を講じているか。
（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。

Q11 からQ13 は、令和４年 11 月 10 日に厚生労働省より発出された事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」を参照の上、回答すること。

Q11　「１　サプライチェーンリスク全体の確認」に記載の内容をもとに、関係事業者のセキュリティ管理体制を確認し、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施したか。

本年 10 月に発生した大阪急性期・総合医療センターにおいて発生したサイバー攻撃では、攻撃の侵入経路は医療機関自身のシステムではなく、院外の調理を委託していた給食事業者のシステムを経由したものである可能性が高いことが、厚生労働省から派遣した専門家チームの調査により判っています。本事務連絡に記載のサプライチェーンリスクを認識し、点検を行ったか回答を選択してください。

参考：令和４年 11 月 10 日厚生労働省事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（抜粋）

１　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

Q12　「２　リスク低減のための措置」に記載の内容を確認し、自組織に必要な措置を講じたか。

自組織の医療情報システムに対しリスク分析を行い、明らかとなった脅威について対策を行うことで、その脅威の発生可能性を低減することができます。事務連絡記載の事項について点検を行い、必要な措置を講じたか回答を選択してください。ただし、具体に講じた措置まで問うものではありません。

引用：令和４年 11 月 10 日厚生労働省事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（抜粋）

２　リスク低減のための措置

〇パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。

〇IoT 機器を含む情報資産の保有状況を把握する。

〇VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。
〇悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。
〇VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。
〇メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

Q13　「３　インシデントの早期検知」に記載の内容を確認し、各種ログの確認・通信の監視などを行ったか。

サイバー攻撃またはその兆候を早期に検知し封じ込むことで、被害の拡大を防止するだけでなく、システム復旧に要する時間を短縮することが可能となります。事務連絡記載の事項について点検を行ったか回答を選択してください。

参考：令和４年 11 月 10 日厚生労働省事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（抜粋）

３　インシデントの早期検知

〇サーバ等における各種ログを確認する。（例：大量のログイン失敗の形跡の有無）
〇通信の監視・分析やアクセスコントロールを再点検する。（例：不審なサイトへのアクセスの有無）。

Q14 およびQ15 は、回答にあたり院内のサーバ室等を点検し、リモートゲートウェイ装置（以下「VPN 機器」）が存在するか保守ベンダー含め確認した上、回答してください。

確認の結果、VPN 機器が設置されていない場合は、次問以降の回答は不要ですので、回答を提出してください。

Q14　自組織内の VPN 機器の設置場所を把握しているか。
※自組織が設置したものだけでなく、保守点検等を目的に、保守ベンダーや業務外注事業者が設置した VPN 機器を含む。

医療情報システム（※）の保守点検等を目的とし、事業者とシステムを接続するために VPN 機器を設置している場合があります。

システム設置業者や保守業者などに照会し、当該機器が設置されているか回答を選択してください。

（※）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。

Q15　VPN 機器は、Fortinet 製品を使用しているか。使用している場合、機種名・台数・OS のバージョンをすべて記載すること。

上記で確認した VPN 機器が Fortinet 製品だった場合、機種名・台数・OS のバージョンをすべて記載してください。（記述方式）

Q16 からQ16－２は、Fortinet 製品の VPN 機器を使用している病院が対象となる質問です。回答にあたっては、令和４年 12 月 16 日に厚生労働省より発出された事務連絡「FortiOS に関する脆弱性情報への対応について（注意喚起)」を参照の上、回答してください。

Fortinet 製品以外の VPN 機器を使用している病院は、Q17 に進んでください。

Q16　Fortinet 製品の脆弱性情報に基づき、対象となるソフトウェアが使用されているか及びサポート期限が切れていないか確認したか。または、医療情報システムの保守ベンダーに確認を依頼したか。

令和４年 12 月に、NISC より Fortinet 製品の脆弱性情報が発信されています。この脆弱性が悪用され、組織内ネットワークが侵害された場合、ランサムウェア等により被害が甚大になる恐れがあることから、即時のバージョンアップを強く推奨されています。確認結果について回答を選択してください。

参考：令和４年 12 月 16 日厚生労働省事務連絡「FortiOS に関する脆弱性情報への対応について（注意喚起)」（抜粋）

１　ゲートウェイ装置の使用状況の確認

各医療機関のシステムを管理するベンダーに対し、セプター等から提供された脆弱性情報の対象となるソフトウェアが使用されているか、及びサポート期限が切れていないかを確認するよう依頼すること。

Q16－１　最新のソフトウェアにバージョンアップを実施したか。

ソフトウェアの脆弱性が放置されると、外部から攻撃を受けたり、不正なソフトウェアが混入されてしまう危険性があります。対象のソフトウェアを使用していた場合、速やかにバージョンアップを実施したか、また、サポート期限内の機種を使用しているか回答を選択してください。

Q16－２　VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施しているか。

意図しない第三者からの不正アクセスを防ぐために、信頼している保守業者などのみにアクセスを制限しているか、回答を選択してください。

Q17 からQ17－２は、Fortinet 製品以外の VPN 機器を使用している病院は回答してください。

Fortinet 製品の VPN 機器が設置されている場合は、次問以降の回答は不要ですので、回答を提出してください。

Q17　VPN 機器のメーカー名・機種名・台数・OS のバージョンをすべて記載すること。

Q14－１で確認した Fortinet 製品以外の VPN 機器のメーカー名・機種名・台数・OS のバージョンをすべて記載してください。（記述方式）

Q17－１　VPN 機器は最新のソフトウェアが使用されているか、また、サポート期限を把握し、アップデートを適切に行っているか。

ソフトウェアの脆弱性が放置されると、外部から攻撃を受けたり、不正なソフトウェアが混入されてしまう危険性があります。VPN 機器のソフトウェアが最新か、また、サポート期限内の機器を使用しているか回答を選択してください。

Q17－２　VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施しているか。

意図しない第三者からの不正アクセスを防ぐために、信頼している保守業者などのみにアクセスを制限しているか、回答を選択してください。