令和６年度医療機関立入検査（サイバーセキュリティ対策関係）支援事業実施要領

１　目的

県内の医療機関における重大インシデント発生を受け、各医療機関におけるサイバーセキュリティ対策の状況を重点的に確認するため、医療法第２５条第１項の規定に基づき保健所が定期的に実施する令和６年度立入検査項目のうち、サイバーセキュリティ対策関係の項目について、チェック体制を強化する。

２　実施方法

（１）　保健所は、立入検査の際に岡山県医療推進課（以下、「医療推進課」という。）があらかじめ指定する別紙１「サイバーセキュリティ対策関連書類一覧」の資料について、現認に代えて医療機関から写しの提供を受けるものとする。なお、写しの提供は医療機関側の任意とし、事前に医療推進課から各医療機関に対し、文書により協力を依頼する。

（２）　保健所は、立入検査が終了したものから順次、医療機関から提供のあった資料を、医療推進課に送付する。

（３）　医療推進課は、保健所から提出のあった資料を元に、各医療機関のサイバーセキュリティ対策の実施状況を確認する。この際、資料に不備があれば、文書により確認又は修正依頼を行う。なお、医療機関への確認等については、原則として保健所を通じて行うこととする。

※　事業の流れは別紙２をご参照ください。

３　実施時期　　令和６年１０月１日から令和７年３月３１日まで

４　対象医療機関　令和６年度に立入検査を実施する医療機関（但し、倉敷市内に所在する医療機関を除く。）

５　共通認識事項

・　本事業により、医療推進課が行う資料確認は、医療法に基づき保健所が行う立入検査を補完する目的で実施するものであり、医療推進課が直接、医療法に基づく指導を行うものではないことに留意すること。

・　任意による資料の提出があった医療機関については、立入検査の当日は、サイバーセキュリティ関係の検査項目の結果を「保留」とし、医療推進課による書類の確認及び修正依頼が終わった後の資料の内容を踏まえて、立入検査の結果を出すことが望ましい。（保健所の責任において先に結果を出すことを妨げるものではない。）

・　別紙の資料を提出されない医療機関については、保健所は他の検査項目と同様に現地での目視による資料確認及び口頭での質疑応答を行うこととし、保健所は、検査終了後、速やかに医療機関名を医療推進課へ連絡することとする。

（別紙１）

医療法第２５条第１項の規定に基づく立入検査において写しの提供を求めるサイバーセキュリティ対策関連書類一覧

	書類の名称	提出にあたっての注意点
1	チェックリスト（医療機関確認用）	令和６年５月１３日付け、医政参発０５１３第６号により厚生労働省から示されている、令和６年度版のチェックリスト様式を使用することとし、チェックリストの記入に当たっては、「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マニュアル～医療機関・事業者向け～」（以下「マニュアル」という。）を参照してください。
2	チェックリスト（事業者確認用）	上記と同じ。なお、医療機関のネットワークを構成するすべての**医療情報システム※**（電子カルテ、レセプトコンピューター、医療機器など）の委託事業者に対し、漏れなくチェックリストの記入、提出を求めてください。（事業者ごと又はシステムごとにチェックリストを分けること）
3	チェックリスト（最低限の措置編）	別添のチェックリスト様式を使用することとし、チェックリストの記入に当たっては、（令和６年８月１日付け、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取組みについて」の別添「サイバー攻撃リスク低減のための最低限の措置」を参照してください。
4	機器管理台帳	情報機器（サーバーやＰＣ）、ルータ等のシステムやネットワークを構築する際に用いられる機器等を記載した台帳を提出してください。台帳の書式については、マニュアル 2-(1) を参照してください。
5	インシデント発生時の連絡体制図	診療継続及び医療情報システムの復旧を迅速に行う目的でサイバーセキュリティの連絡体制を記載したものを提出してください。連絡体制図の書式については、マニュアル 3-(1) を参照してください。
6	ネットワーク構成図及びシステム全体構成図	システム全体構成図及びネットワーク構成図を作成していれば提出してください。 構成図については、「医療情報システムの安全管理に関するガイドライン第 6.0 版」 ▶企画管理編　４．４、 ▶システム運用編　２②　を参照してください。
7	サイバー攻撃を想定した事業継続計画（BCP）	サイバー攻撃を想定した事業継続計画（BCP）を作成していれば提出してください。BCP については、令和６年６月６日付け、厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室事務連絡「「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」について」を参照してください。

※（参考）

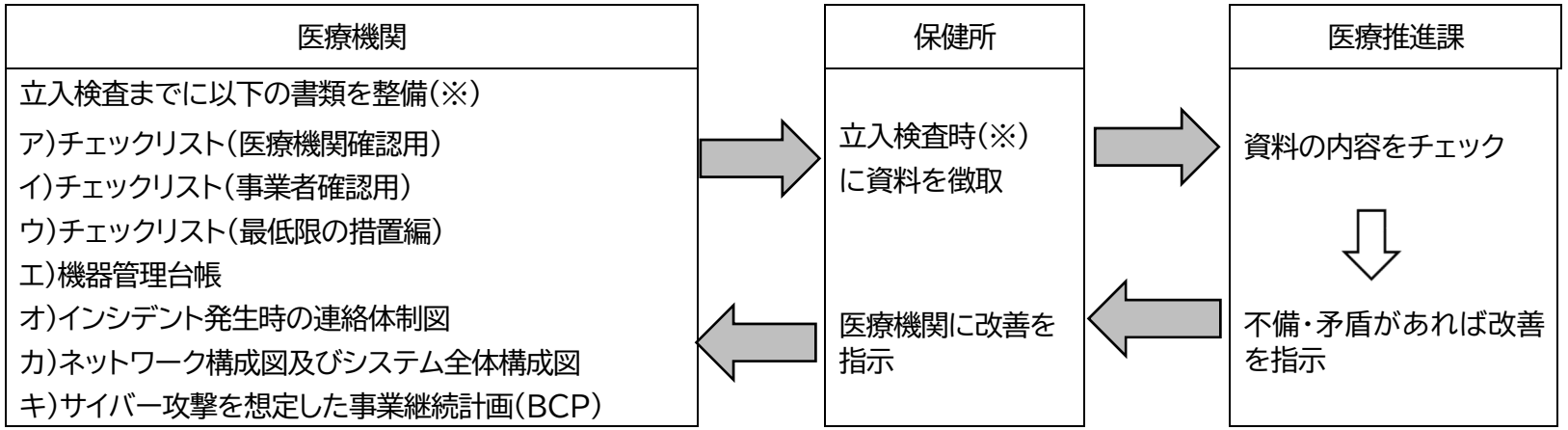
「医療情報システムの安全管理に関するガイドライン第 6.0 版」に関するＱ＆Ａ

Ｑ５　「医療情報システム」とは具体的に何を示すのか。

Ａ　医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末も範ちゅうとして想定しています。また、医療情報が通信される院内・院外ネットワークも含まれます。

（別紙2）

事業の流れ



（※）立入検査が既に実施済みの場合は、書類の提出について保健所へご相談ください。

別添

医療機関確認用

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
「サイバー攻撃リスク低減のための最低限の措置」編

医療機関名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

※ このチェックリストは、医療機関等におけるサイバーセキュリティ対策の取組みについて（令和６年８月１日事務連絡　各都道府県等衛生主管部(局)宛厚生労働省医政局特定医薬品開発支援・医療情報担当参事官及び厚生労働省政策統括官付サイバーセキュリティ担当参事官室）により、特に迅速に対応すべき事項として示された「サイバー攻撃リスク低減のための最低限の措置」の内容を基に、岡山県が作成したものです。

※ 本チェックリストの項目について直ちに確認を行い、「いいえ」の項目については速やかに取り組むよう対応をお願いします。

※ １回目の確認で「いいえ」の場合、実施可能な直近の対応目標日を記入してください。

※ 立入検査時、本チェックリストを確認します。

チェック項目	確認結果（ 日付 ）			備考
	１回目	目標日	２回目	
〇パスワードを強固なものに変更し、使い回しをしない				
システム運用担当者は、VPN 装置等の ID・パスワードについて、強固な ID・パスワード設定を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
複数の機器や外部サービス等で、同一のパスワードを設定していない。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
利用者認証に使用するパスワードについて、類推されやすいパスワードを使用しないよう、すべての利用者に対し周知を徹底している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
〇IoT 機器を含む情報資産の通信制御を確認する				
関係事業者と協力してすべてのネットワーク接続点を確認（閉域網と認識されているネットワークにおける接続点の有無の確認を含む）している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
ネットワーク接続点へのアクセス制御を適切に実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
各種システムや通信制御を行っている機器のログを記録・保存し、定期的にその内容をチェックして不正利用がないことを確認している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
〇ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する				
すべてのネットワーク機器のバージョンアップやパッチ適用、ファームウェアアップデートを適切な頻度で行っているか、事業者と連携して確認している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
セキュリティ対策ソフトの稼働状況（最新の定義ファイルが適用されるようになっているか等）について確認している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	