資料１

令和６年７月19日
医　療　政　策　課

令和６年度 県立保健所管内病院立入検査の方針等

１　検査期間
令和６年９月２日　から　令和７年１月31日まで

２　対象施設
県立保健所管内　７８病院（長崎市、佐世保市は除く）

３　検査方針
（１）実施体制
県立保健所及び県医療政策課による合同検査
（２）重点項目
「医師の働き方改革」
（３）注意確認項目
「サイバーセキュリティ」
事前提出：「令和６年度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」
＊検査時には、特に連絡体制図の策定、BCPの策定、訓練の実施状況、機器の脆弱性対策を確認する予定です。

（４）「医師の働き方改革」の追加項目に関する当日の準備書類
（ア）医師の勤務状況がわかる書類（タイムカード、PCの利用状況がわかるもの）
（イ）労働時間時間が把握できる書類（勤務日、勤務時間がわかるもの）
（ウ）面接対象指導対象医師の一覧表（時間外・休日労働時間100時間/月超）
（エ）長時間労働医師面接指導結果及び意見書
（オ）労働時間短縮のために必要な措置の内容の記録

４　事前提出書類
様式は県ホームページにて７月30日(火)より公開予定
＜掲載場所＞
県ホーム（分類で探す）
福祉･保健 ＞ 医療 ＞ 病院･診療所の手続き ＞ 県立保健所病院立入検査関係様式
＜医療従事者の基準日等＞
医師　　令和６年７月２２日（月）～２８日（日）の１週間
他従事者　令和６年７月２２日（月）

令和５年度 県立保健所管内病院立入検査結果

1　結果総括　　令和５年度は全病院 79 施設に定期の病院立入検査を実施。全指摘件数は、675 件であった。令和元年度と比較し、指摘が 52 件増加している。増加の主な要因は、令和 5 年度から追加したサイバーセキュリティ対策の不備によるものであった。

なお、分野別では、「院内感染」に関する指摘（計 158 件）が最も多く、軽微な担当指摘の占めている割合が多い。なお、文書指導が多い分野は「医事全般」(７件)、口頭指導が多い分野は「医師」（12 件）であった。

2　実施期間　　令和５年８月 25 日（金）　～　令和６年２月 16 日（金）

3　実施施設　　県立保健所管内の病院　79 施設　（実施率 100%）

4　令和 5 年度病院立入検査分野別集計（令和元年度との比較）

指導項目及び内容		R 元年度	R５年度
医師	文書指導	0	0
	口頭指導	12	12
	改善要望	32	36
	担当指摘	18	7
委託･防火健診等	文書指導	0	1
	口頭指導	11	8
	改善要望	1	0
	担当指摘	59	42
医薬品	文書指導	0	1
	口頭指導	4	5
	改善要望	3	6
	担当指摘	24	25
水道・クリーニング・循環式浴槽	文書指導	0	0
	口頭指導	0	1
	改善要望	0	0
	担当指摘	4	10
環境･廃棄浄化槽	文書指導	0	0
	口頭指導	0	0
	改善要望	1	1
	担当指摘	19	40
給食･調理	文書指導	0	0
	口頭指導	1	1
	改善要望	6	5
	担当指摘	26	35

指導項目及び内容		R 元年度	R５年度
放射線	文書指導	0	5
	口頭指導	1	4
	改善要望	0	0
	担当指摘	19	27
院内感染	文書指導	0	0
	口頭指導	7	6
	改善要望	11	12
	担当指摘	149	140
医療安全	文書指導	1	1
	口頭指導	3	1
	改善要望	7	1
	担当指摘	35	15
医療機器	文書指導	0	3
	口頭指導	7	0
	改善要望	1	3
	担当指摘	91	64
医事全般	文書指導	5	7
	口頭指導	9	5
	改善要望	5	2
	担当指摘	33	125
災害	文書指導	0	0
	口頭指導	0	0
	改善要望	4	4
	担当指摘	14	14
合計	文書指導	6	18
	口頭指導	55	43
	改善要望	71	70
	担当指摘	491	544
	合計	623	675

5　分野別指摘事項（令和 5 年度）

（1）　医師に関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	診療録の記載不備（診断名、指示記載等）	6
	診療録の開示手続きの不備(管理、不備含む)	1
	死亡診断書の記載不備	2
	身体拘束にかかる記録の記載不備	2
	入院診療計画未作成	1
改善要望	診療録の記載不備（医師名､見読不可、禁忌情報の記載欄追加等）	13
	死亡診断書の記載不備（外因死、終末期患者の死亡原因等の記載不足）	9
	退院療養計画書の不備（作成なし）	3
	処方箋システムの改修（誤投薬防止機能等の追加）	2
	身体拘束にかかる記録の記載不備	4
	身体拘束にかかる検討の不備	2
	診療録の開示手続きの不備(管理、不備含む)	1
	看護計画の記載不備	2
担当指摘	診療録の記載不備（手術記録の麻酔医のサイン漏れ、看護師のサイン漏れ、検査結果の確認等）	5
	診療録の開示手続きの不備(管理、不備含む)	2

（2）　委託・防火・健診に関する指摘事項

指導区分	指導の内容	指導数
文書指導	医療ガスに係る安全管理研修未実施	1
口頭指導	委託契約書の不備（記載内容不備、現状乖離）	2
	委託業者が法の基準に適合するか確認不足	1
	医療ガスの研修会未実施（記録不備含む)	1
	医療ガスの日常点検未実施（記録不備含む)	1
	避難方法・経路の確保	3
改善要望	なし	0
担当指摘	委託契約書不備（未作成、記載不備）	9
	医療ガスの研修会未実施（記録不備含む)	6
	医療ガス委員会未開催（記録不備含む)	2
	EOG（エチレンオキシドガス）の手順書不備	1
	防火管理者変更の検討要望	1
	避難方法・経路の確保	3
	消防計画変更時の消防署未届	1
	防火設備の設置・点検・管理不備（要措置未改善含む）	8
	夜間想定訓練の未実施	1
	消防訓練の未実施(記録不備含む)	1
	入院患者の避難方法等の教育・説明なし	2
	トラッキング防止対策不備	2
	ストレスチェック未実施(管理、記載不備含む)	4
	定期健康診断の未実施（保管方法、記載漏れ、一部項目漏れ含）	1

（3）　医薬品に関する指摘事項

指導区分	指導の内容	指導数
文書指導	麻薬保管の不備	1
口頭指導	業務手順書に基づく業務の確認と記録	1

	処方せんの記載不備（氏名含む）	1
	医薬品の保管不備	2
	食事提供体制の不備	1
改善要望	医薬品・毒薬等の管理不備	1
	業務手順書に基づく業務の確認と記録	1
	業務手順書の見直し	2
	薬剤オーダーリングシステムの誤選択防止	2
担当指摘	処方せんの記載不備	3
	麻薬・覚せい剤原料廃棄時の手続き不備	1
	業務手順書に基づく業務の確認と記録	4
	業務手順書不備（未作成含む）	5
	調剤所の清潔保持	1
	麻薬帳簿の記載不備	8
	医薬品安全使用のための研修未実施	3

（4）　水道・ｸﾘｰﾆﾝｸﾞに関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	水道技術管理者の届出不備（変更届等）	1
改善要望	なし	0
担当指摘	循環式浴槽の管理不備（管理マニュアルと齟齬）	1
	残留塩素濃度検査不備	1
	構造等変更手続き不備	1
	簡易専用水道事業者に係る法定点検未実施	1
	水質汚濁防止法に係る変更届未提出	1
	水道技術管理者の届出不備（変更届等）	1
	水道技術管理者の健康診断・検便検査結果記録なし	4

（5）　環境・廃棄物に関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	なし	0
改善要望	感染性廃棄物処理計画の未作成	1
担当指摘	委託契約の契約確認できない（期限切れ含む）	1
	感染性廃棄物処理計画・管理規定の記載不備（未改訂含む）	4
	感染性廃棄物処取扱い管理規定の未作成	1
	感染性廃棄物保管場所の不備（掲示を含む）	3
	フロンガスの点検・点検記録簿作成なし（未実施含む）	7
	フロンガスの点検・点検記録簿記録不備	6
	排出水（浄化槽放流水）の自主検査未実施	1

	変更届出未提出	9
	紙マニフェストの報告未実施	5
	マニュフェスト記載不備	3

（6）　調理・栄養に関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	衛生面遵守事項の不備	1
	施設整備（冷蔵庫の修繕要望、蛍光灯の錆、床のひび、食品庫の壁、計量器の錆等）	2
	食材の管理不備	3
改善要望	なし	0
担当指摘	疾病ごとの約束食事せんなし	1
	職員の衛生管理	1
	調理環境の管理不備（温度・清潔保持等）	6
	調理器具の管理不備（包丁、まな板の混同）	1
	食材の管理不備	2
	食品の管理不備	2
	食事提供後の検食	1
	食事内容の検討不備	2
	食事摂取基準の見直し不備	5
	検食の不備（記録簿の不備、検食時間）	4
	委託できない給食業務の委託（記載不備含む）	1
	非常時マニュアルの改正依頼	6
	栄養に係る目標量の不達成（食物繊維、カロリー、未確認等）	1
	施設整備（冷蔵庫の修繕要望、蛍光灯の錆、床のひび、食品庫の壁、計量器の錆等）	2

（7）　放射線に関する指摘事項

指導区分	指導の内容	指導数
文書指導	診療用放射線の安全利用に係る職員研修未実施	2
	診療用放射線の安全利用のための指針未策定	1
	診療用放射線の利用に係る安全な管理のための責任者未配置	2
口頭指導	漏洩線量測定結果の管理責任者の確認と記録	1
	エックス線室の掲示不備（使用中ランプ動作不良含む）	2
	装置の日常・定期点検の未実施（不備含む）	1
改善要望	なし	0
担当指摘	電離放射線健康診断の未実施	1
	電離放射線健康診断の健診項目一部未実施（記載不備含む）	6
	漏洩線量測定結果の管理責任者の確認と記録	2
	漏洩線量測定の未実施	1
	照射録の記載不備	1
	診療用放射線の安全管理に係る指針の記載不備	2

	診療用放射線の安全管理に係る研修未実施	5
	診療用放射線の安全管理に係る研修（記録不備）	3
	診療用放射線の安全利用のための最適化の担保	1
	適切な撮影条件の不備（見直し含む）	2
	医薬品業務手順書に造影剤に関する記載がない	3

（8） 院内感染に関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	感染症法に基づく感染症発生届等の未届け（遅れ含む）	5
	リキャップ	1
改善要望	経管栄養チューブの再利用	9
	院内感染対策マニュアルの記載不備	3
担当指摘	院内感染対策指針の記載不備	4
	院内感染対策マニュアルの記載不備	8
	院内感染対策委員会開催記録の記載不備	4
	院内感染委員の委員会欠席	2
	院内感染研修記録の記載不備	3
	院内感染研修参加率向上の取り組み不足（特定職種欠席含）	3
	手指消毒薬の適切な配置不備	2
	手指消毒薬の適切な使用と管理不備	2
	汚物処理室の管理不備	9
	点滴調整台の清潔維持管理不足	16
	感染性廃棄物ゴミ箱の配置場所不適	9
	リキャップ	4
	リネン庫の保管・管理不備	11
	洗浄後物品の保管・管理不備	4
	浸漬消毒の管理不備	15
	衛生材料等の配置・保管・管理不備（滅菌期限切れ含む）	18
	内視鏡検査時の個人防護具の使用不備(洗浄時含む)	3
	内視鏡管理(保管)不備	4
	経管栄養チューブの再利用	10
	清拭車の管理不備	2
	浴室の管理不備	2
	適切なゴミの分別	5

（9）医療安全に関する指摘事項

指導区分	指導の内容	指導数
文書指導	医療安全管理委員会未実施	1
口頭指導	医療安全管理指針の不備	1
改善要望	酸素ボンベ等の転倒防止要望	1

担当指摘	医療安全指針の記載不備(改定未実施含む)	2
	医療安全委員の欠席者への対応（周知）	3
	安全管理委員会の規定の記載不備	2
	医療安全対策の評価未実施	2
	ｲﾝｼﾃﾞﾝﾄ・ｱｸｼﾃﾞﾝﾄについて集計・分析の要望	3
	医療安全研修記録の記載不備	1
	医療法第 6 条の 10 第 1 項の報告を管理者が把握する体制未整備・不十分	1
	検査結果報告の未確認防止対策の不備	1

（10）医療機器に関する指摘事項

指導区分	指導の内容	指導数
文書指導	保守点検計画の記載不備	3
口頭指導	なし	0
改善要望	保守点検計画の記載不備	1
	検体検査の責任者配置なし	1
	標準作業書の未作成（不備含む）	1
担当指摘	検体検査の責任者配置なし（不備含む）	4
	標準作業書の未作成（不備含む）	2
	作業日誌の未作成（不備含む）	9
	試薬台帳の未作成（不備含む）	3
	内部精度管理台帳記載不備	4
	統計学的管理台帳の未作成	6
	外部制度管理台帳不備（未実施含む）	2
	保守点検計画の未作成（一部機器の未作成を含む）	2
	保守点検計画の記載不備	6
	保守点検計画に基づく点検結果確認の未実施・要改善(記録なし・不備含む)	5
	点検結果記録の記載不備	5
	責任者が不適当	1
	検体検査に係る研修未受講	7
	検体検査に係る研修記録の作成・記載不備	3
	医療機器に係る研修未実施	1
	医療機器に係る研修の記録不備	4

（11）医事に関する指摘事項

指導区分	指導の内容	指導数
文書指導	変更許可・構造設備使用許可申請のない用途等変更	3
	医師不足	2
	薬剤師不足	1
	超過入院の常態化	1
口頭指導	超過入院の常態化	2
	オーダリング、電カル等の管理規定の不備	2

	廊下の管理	1
改善要望	免許書の「原本照合済み」の旨の記載なし	1
	救急カート内の衛生材料等の配置・保管・管理不備（滅菌期限切れ含む）	1
担当指摘	医療機能情報の院内閲覧なし	6
	免許書の「原本照合済み」の旨の記載なし（一部記載不備含む）	3
	オーダリング、電カル等の管理規定の不備	1
	救急カート内の衛生材料等の配置・保管・管理不備（滅菌期限切れ含む）	3
	廊下の管理	2
	トイレの管理	1
	院内掲示の不備	1
	サイバーセキュリティ対策（BCP 未策定）	24
	サイバーセキュリティ対策（連絡体制未作成、訓練未実施等）	72
	転落防止対策の不備	1
	室の目的外用途使用	1

（12）災害に関する指摘事項

指導区分	指導の内容	指導数
文書指導	なし	0
口頭指導	なし	0
改善要望	災害マニュアル（BCP,搬送計画,記載不備）	4
担当指摘	災害マニュアル（BCP,搬送計画,病院の行動・役割等）の記載不備	8
	災害マニュアル未作成	1
	避難確保計画の未作成	2
	避難確保計画に基づく訓練未実施（市町への報告含む）	3

－令和６年度　病院立入検査重点項目－（案）

これまでの我が国の医療は医師の長時間労働により支えられており、今後、医療ニーズの変化や医療の高度化、少子化に伴う医療の担い手の減少が進む中で、医師個人に対する負担がさらに増加することが予想されます。

こうした中、医師が健康に働き続けることのできる環境を整備し、患者に対して提供される医療の質・安全を確保すると同時に、持続可能な医療提供体制を維持するため、医療法等が改正され令和６年４月１日から施行されました。

つきましては、貴施設の取り組み状況について、以下の項目を確認の上、書類及び体制が未整備の場合は、ご対応の程、よろしくお願いいたします。

なお、病院立入検査時には、下記に沿って確認を行う予定としていますので、チェック後は事前提出書類と共に管轄の保健所に提出いただきますようお願いします。

１．医師の労働時間の状況の把握等

（１）　医師の労働時間の把握（医療法施行規則第 61 条第１項）

□　下記のいずれかの方法で医師の労働時間を把握している

［□　タイムカード　　□　パーソナルコンピュータ等の使用時間の記録
□　その他（　　）］

（２）　労働時間の状況の記録（医療法施行規則第 61 条第２項）

□　労働時間記録を作成している（　大学病院等の派遣医師を含む　）。

□　作成した記録は３年保管している。（※保管予定含む）

（３）　労働時間、面接指導及び労働時間短縮などの措置の対象医師

（医療法施行規則第 61 条第１項・第３項、第 62 条第１項、R.6.3.15 付事務連絡）

□　労働時間記録で措置の対象となる医師を毎月定期的に確認している。

（４）　時間外・休日労働が１月に 100 時間以上と見込まれる医師数

令和６年４月［　　］人、５月［　　］人、６月［　　］人

※以下の「２.面接指導の実施方法等」については、時間外・休日労働が１月に 100 時間以上と見込まれる医師がいない場合、以下の確認（チェック記載）は不要です。

＜裏面に続く＞

２．面接指導の実施方法等

管理者は、面接指導対象医師に対し次に掲げる事項を確認し時間外・休日労働時間が１箇月について 100 時間に達するまでの間に面接指導を行っている。

（１）　管理者は、面接指導医師に対して、以下の項目を確認している。

（医療法施行規則第 63 条、R6.4.1 付通知、R.6.3.15 付事務連絡）

□ア　面接指導対象医師の勤務の状況

□イ　面接指導医師の睡眠の状況

□ウ　面接指導対象医師の疲労の蓄積の状況

□エ　面接指導対象医師の心身の状況

□オ　面接指導対象医師の面接指導を受ける意思の有無

（２）　面接指導実施医師は、面接指導対象医師に対して、以下の項目を確認し、記録を保管している。（医療法施行規則第 64 条、第 71 条、R6.4.1 付通知、R6.3.15 付事務連絡）

□　ア　面接指導対象医師の勤務の状況

□　イ　面接指導対象医師の睡眠の状況

□　ウ　面接指導対象医師の疲労の蓄積の状況

□　エ　その他面接指導対象医師の心身の状況

□　ア～エの面接指導した記録は、5 年間保管している（※保管予定含む）

□　面接指導年月日　　令和　　年　　月　　日（※直近の実施年月日）

（３）　面接指導実施医師は、医師の健康管理を行うのに必要な知識を習得させるための講習（「面接指導実施医師養成講習会」）を受講している。

（医療法施行規則第 64 条、R6.4.1 付通知、R6.3.15 付事務連絡）

□　受講済み（受講年月日＿＿＿＿年　　月　　日）

３．面接指導対象医師に講ずべき措置（就業上の措置）

（１）　管理者は、面接指導医師の意見を勘案し、その必要があると認めるときは、面接指導対象医師の実情を考慮し必要な措置を講じている。

（医療法施行規則第 69 条第 1 項、第 71 条、R6.4.1 付通知、R6.3.15 付事務連絡）

□　労働時間の短縮

□　宿直回数の減少

□　その他適切な措置（　　）

□　必要な措置の記録を 5 年間保管している。（※保管予定含む）

４．労働時間が特に長時間である医師に講ずべき措置

（１）　管理者は、面接指導対象医師の労働時間が 155 時間/月を超える場合、労働時間短縮のための必要な措置を講じ、記録を保管している。

（医療法施行規則第 70 条第 1 項、第 71 条、R6.4.1 付通知、R6.3.15 付事務連絡）

□　必要な措置（　　）

□　記録を 5 年間保管している。（※保管予定含む）

（参　考　1）

面接指導対象医師一覧（例）

年月	所属	役職	氏名	超勤
202404	呼吸器内科	医員	○○　○○	115
202404	循環器内科	副院長	○○　○○	108.5
202404	循環器内科	専攻医	○○　○○	109
202406	循環器内科	研修医	○○　○○	100.5
202406	小児科	研修医	○○　○○	101
202406	心臓血管外科	専攻医	○○　○○	119.35
202407	心臓血管外科	部長	○○　○○	110.63
202408	心臓血管外科	医長	○○　○○	102.28
202409	消化器内科	専攻医	○○　○○	103
202409	整形外科	専攻医	○○　○○	152.33
202410	心臓血管外科	専攻医	○○　○○	105.5
202410	整形外科	専攻医	○○　○○	136.41
202410	外科	研修医	○○　○○	101.5
202410	呼吸器内科	専攻医	○○　○○	102.95
202411	心臓血管外科	研修医	○○　○○	100.5
202411	整形外科	医長	○○　○○	118.91
202411	脳神経外科	専攻医	○○　○○	111.5
・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・
・・・	・・・	・・・	・・・	・・・

※　上記資料は、関係法令等で定められた様式ではなく参考に示ししているものであるため、様式は医療機関ごとに異なることに留意すること。

（参　考　２）

長時間労働医師面接指導結果及び意見書

面接指導結果・面接指導実施医師意見			
対象者氏名		所　　属	
		生年月日	年　　月　　日
勤務の状況 （労働時間、労働時間以外の項目）			
睡眠負債の状況	（低）０　　１　　２　　３　（高）（本人報告･睡眠評価表） （特記事項）		
疲労の蓄積の状態	（低）０　　１　　２　　３　（高）（労働者の疲労蓄積度自己診断チェックリスト） （特記事項）		
その他の心身の状況			
本人への指導内容　及び　管理者への意見（複数選択可・該当項目の左に〇をつける）			
	就業上の措置は不要です		
	以下の心身の状況への対処が必要です（〇で囲む） 専門医受診勧奨　・　面談を含む産業医連携　・　その他（特記事項へ記載）		
	以下の勤務の状況への対処が必要です（〇で囲む） 上司相談　・　面談を含む産業医連携　・　その他（特記事項へ記載）		
（特記事項）			

面接実施年月日	年　　月　　日	
面接指導実施医師	（所属）	（氏名）※署名等

第一の２（２）①関係

「長時間労働医師面接指導結果及び意見書」に以下の事項が記載されており、適切な時期に面接指導が実施されていることを確認すること。

（ア）　面接指導の実施年月日　　（イ）　面接指導対象医師の氏名

（ウ）　面接指導を行った面接指導実施医師の氏名

（エ）　面接指導対象医師の勤務の状況

（オ）　面接指導対象医師の睡眠の状況

（カ）　面接指導対象医師の疲労の蓄積の状況

（キ）　その他面接指導対象医師の心身の状況

（参　考　３）

長時間労働医師面接指導結果及び意見書

面接指導結果・面接指導実施医師意見			
対象者氏名		所　　属	
		生年月日	年　　月　　日
勤務の状況 （労働時間、労働時間以外の項目）			
睡眠負債の状況	（低）０　　１　　２　　３　（高）（本人報告･睡眠評価表） （特記事項）		
疲労の蓄積の状態	（低）０　　１　　２　　３　（高）（労働者の疲労蓄積度自己診断チェックリスト） （特記事項）		
その他の心身の状況			

本人への指導内容　及び　管理者への意見（複数選択可・該当項目の左に〇をつける）	
	就業上の措置は不要です
	以下の心身の状況への対処が必要です（〇で囲む） 専門医受診勧奨　・　面談を含む産業医連携　・　その他（特記事項へ記載）
	以下の勤務の状況への対処が必要です（〇で囲む） 上司相談　・　面談を含む産業医連携　・　その他（特記事項へ記載）
（特記事項）	

面接実施年月日	年　　月　　日	
面接指導実施医師	（所属）	（氏名）※署名等

面接指導実施医師は、この点線上まで記載した段階（管理者が「面接指導実施医師意見に基づく措置内容」を記載する前）で、本書面を被面接医に渡してください。

面接指導実施医師意見に基づく措置内容（管理者及び事業者が記載）
※時間外・休日労働が月 155 時間を超えた被面接医には労働時間短縮のための措置が必要です。 年　　月　　日

確認欄（署名等）※提出を受けた医療機関で記載してください。	
医療機関名	
（管理者）	（事業者）

第２の２（２）関係

措置の要否や措置の内容についての記録があることを確認するため、「長時間労働医師面接指導結果及び意見書」の「措置の要否や措置の内容」が記載されていることを確認すること。

（参　考　４）

時間外・休日労働が 155 時間超となった医師の措置について

労働時間短縮のための措置内容	
（管理者）	年　　月　　日

※　上記資料は、関係法令等で定められた様式ではなく参考に示ししているものであるため、様式は医療機関ごとに異なることに留意すること。

第３の２（２）関係

労働時間短縮のための必要な措置の内容について、記載された記録があることを確認する。

なお、その際には月の時間外・休日労働時間が 155 時間を超える場合、医療法第 108 条第６項に基づき、医療機関の管理者は労働時間短縮のために必要な措置を講じなければならないため、上記資料に労働時間短縮のための措置の内容が記載されていることが必要であることに留意すること。

医政参発 0513 第６号
令和６年５月 13 日

各 都道府県 保健所設置市 特別区 医務主管部（局）長　殿

厚生労働省医政局参事官
（特定医薬品開発支援・医療情報担当）
（　　公　　印　　省　　略　　）

令和６年度版「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
「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～」について

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

医療機関等のサイバーセキュリティ対策において優先的に取り組むべき事項については、「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」及び「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～」（令和５年６月９日付け医政参発 0609 第１号、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通知。以下「チェックリスト等」という。）によりお示ししてきたところです。

チェックリスト等の一部項目について、令和６年度に確認するものを参考項目として位置づけていましたが、令和６年度からはすべての項目を確認する必要があることから、「令和６年度版　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「令和６年度版　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マニュアル～医療機関・事業者向け～」として、別添１及び２のとおり改訂しました。

貴職におかれては、本通知について御了知の上、関係団体、関係機関等に周知徹底を図るとともに、その実施に遺漏なきよう御配慮願います。

なお、チェックリストの項目中、「サイバー攻撃を想定した事業継続計画（BCP）を策定している。」については、今後 BCP 策定に関する手引きを作成し、別途お示しする予定です。

別添１

令和6年度版
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

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中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	R5年度項目
		1回目	目標日	2回目		
1 体制構築	医療情報システム安全管理責任者を設置している。(1-(1))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	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。(2-(1))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2)) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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。(2-(3)) ※事業者と契約していない場合には、記入不要	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	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。(2-(7)	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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る。(2-(9))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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。(2-(7))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	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る。(2-(9))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	ネットワーク機器について、以下を実施している。					
	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。(2-(7))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-(1))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		※
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-(2))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-(3))	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）		

- 各項目の考え方や確認方法等については、「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～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和 5 年度中に対応することを目標として掲げた項目

令和6年度
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

事業者確認用

*以下項目は令和6年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和6年度中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	R5年度項目
		1回目	目標日	2回目		
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**					
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	医療機関に製造業者/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）を提出した。(2-(3))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	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。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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る。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	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る。(2-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	ネットワーク機器について、以下を実施している。					
	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。(2-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※

事業者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

- 各項目の考え方や確認方法等については、「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～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和 5 年度中に対応することを目標として掲げた項目

別添２

令和６年度版

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マニュアル

～医療機関・事業者向け～

本マニュアルは、「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（以下「チェックリスト」という。）」をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

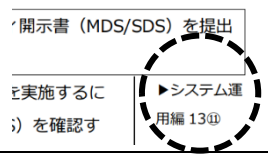
○　医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○　医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。

本マニュアルは、医療機関におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○　医療機関および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

目次

凡例		本マニュアルの「Ⅱ各チェック項目の解説」では、それぞれのチェック項目に紐づく「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」の該当箇所を右側に「▶」で示しています。

Ⅰ　チェックリストの使い方

1．チェックリストの用意

○　チェックリストを使用するにあたり、医療機関においては「医療機関確認用」、事業者においては「事業者確認用」を用いて確認してください。事業者と契約していない医療機関においては「事業者確認用」による確認は不要です。

○　医療機関は事業者に「事業者確認用」を送付し、対策の状況を確認するよう求めてください。複数の医療情報システムを利用している場合、システムを提供している事業者ごとに確認を求めてください。なお、事業者に対しても別途本取組について周知を行っていきます。

2．チェックリストの記入方法

○　各項目の実施状況を確認し、「はい」または「いいえ」にマルをつけて、確認した日付を記入してください。もし１回目の確認で「いいえ」の場合は、対策の実施にかかる令和６年度中の目標日を記入するようにしてください。チェックリストは紙媒体または電子媒体のどちらで使用して頂いても構いません。

○　医療機関は「医療機関確認用」について令和６年度中に全てのチェック項目で「はい」にマルがつくように、事業者と連携して取り組むようにしてください。

（※）　事業者と契約していない場合には、２（２）及び２（３）の記入は不要です。

○　複数の事業者と契約している場合、契約内容によっては「事業者確認用」の一部の項目の確認が不要になることもあります。「事業者確認用」には、事業者名を記入する欄を設けています。医療機関は各事業者から回収してください。

3．その他

○　チェックリストの確認結果は随時参照して、日頃の対策の実施に役立ててください。

○　少なくとも年に１回は、チェックリストを用いた点検を実施してください。

○　医療機関と直接契約関係にない事業者においては、「事業者確認用」の作成は不要です。

～立入検査時、チェックリストを確認します～

医療法第 25 条第１項に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

立入検査では「医療機関確認用」、「事業者確認用」の全ての項目について、１回目の確認の日付と回答等が記入されていることを確認します（※）。このうち、３（１）の連絡体制図は現物を確認しますので、立入検査までに作成してください。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関は各事業者からチェックリストを回収しておきましょう。

（※）　事業者と契約していない場合には、「医療機関確認用」２（２）及び２（３）についての確認は求められません。

Ⅱ　各チェック項目の解説

医療情報システムの有無　　【医療機関確認用】

医療情報システムを導入、運用している。

本チェックリストが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定します（例：レセコン、電子カルテ、オーダリングシステム等）。これには、事業者により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれます。

本項目の「いいえ」にマルがつく場合、以下すべての項目は確認不要です。

▶概説編 2.3

1　体制構築　　【医療機関確認用・事業者確認用】

（1） 医療情報システム安全管理責任者を設置している。

医療機関等において、医療機関の経営層は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を設置する必要があります。医療情報システム安全管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。情報セキュリティ対策の実効性を確保するために、経営層が医療情報システム安全管理責任者に就くことが望ましいですが、医療機関の規模・組織等によっては企画管理者が兼務することもあります。

また、事業者においても医療情報システム等の提供に係る管理責任者を設置する必要があります。

（用語の解説）

企画管理者：医療機関において医療情報システムの安全管理の実務を担う担当者を指します。

▶経営管理編
3.1.2②
3.2

2　医療情報システムの管理・運用　【医療機関確認用・事業者確認用】

（用語の解説）

医療情報システム全般：サーバ、端末 PC、ネットワーク機器を指します。

サーバ：電子カルテサーバやレセコンサーバ等、ネットワーク上で情報やサービスを提供するコンピュータを指します。

ネットワーク機器：無線 LAN やルータ等を指します。

（1） 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。（医療情報システム全般）

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、企画管理者は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できるようにしてください。また、医療機関の経営層は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。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。

▶経営管理編 1.2.1＜管理責任＞②

▶企画管理編 9.1

（用語の解説）

情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。

（補足）

サーバ、端末 PC、ネットワーク機器のうち、自身の医療機関で保有する医療情報システムについて台帳管理を行っていれば、「はい」にマルをつけてください。

●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（２） リモートメンテナンス（保守）を利用している機器の有無を事業者に確認した。（医療情報システム全般）

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、企画管理者に報告する必要があります。そのため、システム運用担当者は、２（１）で整理した情報をもとにリモートメンテナンスを利用している機器の有無を事業者に確認し、企画管理者へ報告してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

システム運用担当者：医療機関において医療情報システムの実装・運用を担う担当者を指します。

▶企画管理編 9.1
▶システム運用編 10.1

（３） 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。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。企画管理者は事業者へ当該医療情報システムに関する MDS/SDS の有無を確認し、事業者から回収してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

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。

▶概説編 4.5

（４） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
（サーバ、端末 PC）

医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程に応じて設定することが重要です。企画管理者は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、所属部署・氏名・ユーザーID・権限等が想定されます。

▶企画管理編 13④ 13.1.3

●利用者 ID 台帳の例

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可
・	・	・	・	・	・	・	・	・

（５） 退職者や使用していないアカウント等、不要なアカウントを削除している。
（サーバ、端末 PC）

企画管理者は２（４）で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。長期間使用されていない等の不要な ID は不正アクセスに利用されるリスクがありますので、速やかに削除してください。

▶企画管理編 13⑦

（6） アクセスログを管理している。（サーバ）

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに、企画管理者はそのログを定期的に確認してください。例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録することが必要です。

（補足）

アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を併せて講じてください。

▶経営管理編 4.2
▶企画管理編 5.3
▶システム運用編 17①②

●アクセスログの例

ユーザーID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16 8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16 8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16 8:31:00	入力メニュー	起動
abc@def	abcdef	2023/5/16 8:32:00	入力メニュー	カルテ入力
abc@def	abcdef	2023/5/17 12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17 8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 8:45:00	管理メニュー	ログオフ
・	・	・	・	・

（７） 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。
（医療情報システム全般）

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挙げられます。

（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。

▶システム運用編 8③
8.1
8.2
13.2

（８） 接続元制限を実施している。（ネットワーク）

外部ネットワークに接続する際には、ネットワークや機器等を適切に選定し、監視を行うことが必要です。特に、無線 LAN を使用する際は不正アクセス対策として適切な利用者以外に無線 LAN を利用されないようにすることが重要です。システム運用担当者は、例えば、ネットワーク機器に接続出来る MAC アドレスが限定すること等、不正アクセス対策を実施してください。

（用語の解説）

MAC アドレス：Media Access Control アドレスの略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号。インターネットでは IP アドレス以外にも MAC アドレスを使用して通信を行っています。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはありません。

（補足）

MAC アドレスによるアクセス制限の効果は限定的であることに留意する必要がありますので、追加の対策はガイドラインや事業者とも確認をお願いします。

▶システム運用編 13⑪

（９） 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る。（サーバ、端末 PC）

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ります。システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者に相談の上、対策を講じてください。

▶システム運用編 8.1

3　インシデント発生に備えた対応　【医療機関確認用】

（1）インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。

医療機関の経営層は情報セキュリティインシデント発生に備え、事業者や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が重要です。企画管理者はサイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成して下さい。連絡体制図には施設内の連絡先に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定されます。

このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

立入検査時は、連絡体制図が作成されていることを確認します。

（用語の解説）

CSIRT: 「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるイシデントに対処するための組織の総称。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する。

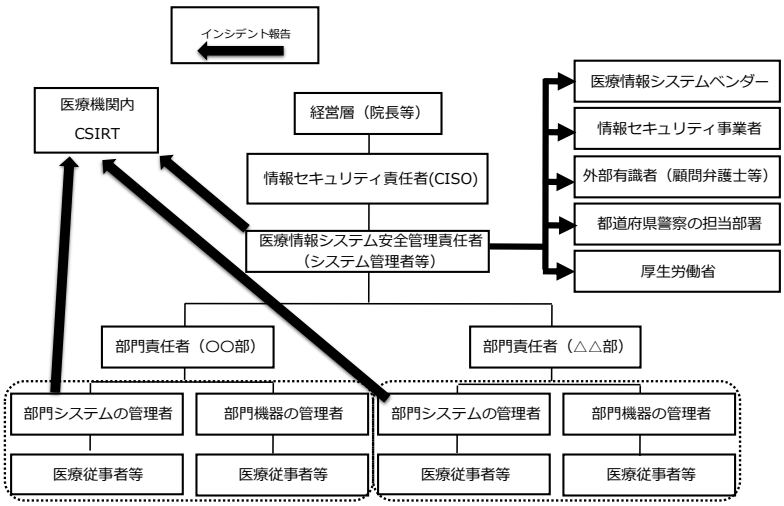
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

サイバー攻撃を受けた疑いがある場合は、下記の厚生労働省の連絡先に御連絡ください。なお、いたずら防止のため、184 発信、公衆電話発信は受信不可としますので、医療機関の電話で御連絡願います。

【連絡先】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　03-6812-7837

●連絡体制図の例



▶経営管理編
3.4.2①
3.4.3①
▶企画管理編
12.3

（２）インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

非常時でも、稼働が損なわれた医療情報システムを復旧できるよう、情報システムやデータ等のバックアップを適切に確保し、その復旧手順を整備・確認しておくことが求められます。企画管理者はバックアップを確保する際、重要なファイルについては、不正ソフトウェアの混入による影響が波及しないよう複数の方式で世代管理するよう設計し、システム運用担当者は手順に従いバックアップを確保してください。復旧手順の整備については、例えば、BCP に復旧手順を定めるなどの方法が挙げられます。

（用語の解説）

世代管理：バックアップの一種で、最新データだけでなく、それ以前のデータもバックアップする方法を指します。例えば、３世代以上で管理する場合、日次でバックアップを行うならば、「3 世代以上」とは「３日以上」のバックアップを確保することになります。

（補足）

３世代目以降のバックアップはオフライン（物理的あるいは論理的に書き込み不可の状態）にする等の対策が望ましいです。

▶経営管理編
3.4.1
▶企画管理編
11.2
▶システム運用編
11.1
12.2
18.1

（３）サイバー攻撃を想定した事業継続計画（BCP）を策定している。

医療機関の経営層は企画管理者と連携して非常時における業務継続の可否の判断基準や継続する業務選定等の意思決定プロセスを検討し、サイバー攻撃を想定した BCP 等を整備することとしています。この BCP を整備しておくことにより、万が一サイバー攻撃を受けても重要業務が中断しない、または中断しても短い期間で再開することが期待できます。

▶経営管理編
3.4.1
▶企画管理編
11.1

～参考資料～

◇[特集]　小規模医療機関等向けガイダンス

診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する人材が十分に確保できないというケースも多くみられます。本ガイダンスは、小規模医療機関等において、ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示しています。

◇[特集]　医療機関等におけるサイバーセキュリティ

本ガイダンスはサイバーセキュリティに関係する部分を要約し、サイバー攻撃の典型例など具体的な事例などもまとめています。チェックリストを用いた確認と併せて一読いただき、ぜひサイバーセキュリティに対する理解をさらに深めてください。

※　厚生労働省 HP「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　特集」に掲載しています。

事　務　連　絡
令和６年６月６日

各 都道府県 保健所設置市 特別区 医務主管部局　御中

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

「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

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

「「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「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～」について」（令和６年５月 13 日付け医政参発 0513 第６号、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通知）において、サイバー攻撃を想定した事業継続計画（BCP）については、「今後 BCP 策定に関する手引きを作成し、別途お示しする予定です。」とお示ししたところです。

今般、別添１のとおり、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（以下「確認表」という。）を作成するとともに、別添２のとおり、確認表を分かりやすく解説した「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き」、及び別添３のとおり、医療情報システム部門等における事業継続計画（BCP）のひな形を作成しました。

貴職におかれては、本通知について、御了知の上、関係団体、関係機関等に周知徹底を図るとともに、その実施に遺漏なきよう御配慮願います。

なお、本内容については、下記の厚生労働省 HP に公表していることを申し添えます。

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

別添１

サイバー攻撃を想定した
事業継続計画（BCP）策定の確認表

令和６年６月

厚生労働省

サイバー攻撃を想定した事業継続計画（BCP）の作成について

厚生労働省では、令和５年度から、医療法に基づく医療機関に対する立入検査の項目に、サイバーセキュリティ対策を位置付けました。立入検査の際に確認する項目は、「医療情報システムの安全管理に関するガイドライン」から優先的に取り組むべき項目について、「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」（以下「チェックリスト」という。）によりお示ししてきたところです。

昨今の巧妙化したサイバー攻撃の現状において、セキュリティ対策を講じることでリスクを低減させることはもちろん重要ですが、リスクを完全に排除することはできません。

例えば、過去には、

・インシデント発生時の初動対応について十分に協議されておらず、証拠保全が不十分となり、被害範囲の特定ができなかった、
・インシデント発生時に、ネットワーク機器が院内のどこに配置されているかわからず、原因究明に時間を要した、
・ランサムウェアによる攻撃の際に、バックアップが適切に確保できておらず、復旧が難航した、

といった事例が実際に発生しており、このようなケースでは、診療継続を含めた医療機関の機能に重大な影響が生じます。

サイバー攻撃を「どのように防ぐか」だけでなく「発生時にどのように対応するか」という意識で、非常時に診療への影響を最低限に抑えるための対応を、あらかじめ「サイバー攻撃を想定した事業継続計画（BCP）」（以下「BCP」という。）として策定しておくことで、適切な復旧対応等を行うことが可能となります。

こうしたことから、チェックリストの項目としても、医療機関に対してBCPの策定を求めており、今般、BCPの策定に際して参考としていただけるよう、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（以下「確認表」という。）を作成しました。医療機関の特性に応じて必要とされるBCPは様々ですが、今般作成した確認表等や関係団体より発出されている資料等を参考に、貴施設においてもサイバー攻撃を想定したBCPの策定をお願いします。

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※医療機関がBCPを策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです

※BCP策定や見直しの際にご活用ください

項番	大項目	確認項目	確認欄
1	平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）		
1-1	情報機器等の把握と適切な管理、全体構成図の作成	サーバ、端末PC、ネットワーク機器を把握できているか。	
		ネットワーク構成図・システム構成図が整備できているか。	
		システム停止が事業継続に与える影響を把握できているか。	
		サーバ、端末PC、ネットワーク機器の脆弱性への対応ができているか。	
1-2	非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図が整備できているか。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	
2	検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）		
2-1	システム異常の報告先の把握	異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。	
2-2	システム異常の検知	院内で発生した異常が院内職員によって覚知できるか。	
2-3	CSIRT/経営者によるシステム異常の覚知	院内職員から発出されたサイバー被害情報が組織を通じて速やかにCSIRT（対応者）ならびに意思決定者まで到達するか。	
3	初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）		
3-1	原因調査（必要に応じて事業者に依頼）	原因調査のため、「ネットワーク機器やケーブル等の調査」 「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。	
3-2	事業者等への連絡と作業履歴の確認	事業者等への連絡と作業履歴の確認ができるか。	
3-3	被害拡大防止	被害拡大防止に向けた対応ができるか。	
3-4	経営層への報告、経営層による確認と指示、組織内周知と対応	経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。	
3-5	被害状況等調査（フォレンジック調査＋証拠保全）と被害状況等の報告	被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。	
3-6	組織対応方針確認と外部関係機関への報告等の対応	組織対応方針を確認できるか。また、外部関係機関への報告ができるか。	

4	復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）		
4-1	経営層からの復旧指示の確認と実施	復旧指示の確認と実施ができるか。	
4-2	医療情報システム等の事業者等へ復旧対応依頼	医療情報システム等の事業者等への対応依頼ができるか。	
4-3	再設定や再インストール、バックアップデータの復旧等	再設定や再インストール、バックアップデータの復旧等ができるか。	
4-4	復旧結果の確認	復旧結果の確認ができるか。	
5	事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）		
5-1	復旧結果と情報漏えい事実の有無の報告	復旧結果と情報漏えい事実の有無、可能性について、院内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-2	再発防止策の検討・策定	再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-3	再発防止策の周知	再発防止策の周知を院内に周知する方法と体制が整備されているか。	
5-4	再発防止策の実施	再発防止策の実施が行えるか。	
5-5	事業者等への再発防止策の指示	事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。	
5-6	外部関係機関への報告と情報公開の検討	情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。 経営者と担当者により外部関係機関への報告が行えるか。	

別添２

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き

○ 本手引きは、「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、サイバー攻撃を想定した BCP 作成の一助となるよう、解説を加えたものです。貴組織において BCP を作成する際の参考として活用してください。

※ サイバー攻撃を想定した BCP 策定時の留意点

・ 本手引き及び確認表は最低限必要な事項を記したものです。医療機関の特性に応じて、自機関が主体となり必要な事項を整理し定めてください。

・BCP 策定には先だってリスク分析が重要となります。リスク分析は全過程において自機関だけでなく、事業者、その他の関係者の間で、情報および意見を相互に交換（リスクコミュニケーション）することが必要です。

・ BCP は定期的に見直し、必要な項目を更新してください。

・ 医療情報システムとは、医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステムを指します。例えば、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・取得するコンピュータや携帯端末等も、範ちゅうとして想定されます。また、患者情報の通信が行われる院内・院外ネットワークも含みます。

・ 医療機関の規模により作成する BCP の内容も異なると想定されるため、関係団体等により示されている BCP の手引きについても適宜参照して作成してください。

・本手引きの各項目の解説の下部には、それぞれの項目に紐づく「医療情報システムの安全管理に関するガイドライン」関連文書の該当箇所を括弧内に示しております。

【１．平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）】

1-1）情報機器等の把握と適切な管理、全体構成図の作成

必要に応じて医療情報システム事業者等の協力を得ながら、自医療機関が保有する情報機器等の全体を網羅する医療情報システムに関する構成図（外部接続点を含むネットワーク構成図等）を作成する。

サーバ、端末 PC、ネットワーク機器を把握できているか。

院内のサーバおよび端末 PC の OS、IP アドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく。なお、各 PC にログオンする際に管理者権限でログオンする PC が分かるようにしておく。また、院内設置のすべての VPN 装置、ファイアウォール、ルータ-等の所在と、IP アドレス、使用用途等を明記した一覧を作成する。

（企画管理編：9.1、システム運用編：8.4）

ネットワーク構成図・システム構成図が整備できているか。

HIS 系、インターネット系等の院内 LAN、外部接続点（ファイアフォール、VPN、地域連携、オンライン資格確認等）のネットワーク構成が判別できるように IP アドレスおよびルーティングがわかる構成図を整備しておく。

（企画管理編：4.4、システム運用編：2、Q&A：概 Q- 6 ）

システム停止が事業継続に与える影響を把握できているか。

各システムが利用できなくなると、どの業務が継続できなくなるか（検査部門システムの場合、検査の受付と検査結果の電子カルテ送信ができなくなる等）といった被害を想定し、代替運用の手順を作成しておく。また、代替運用サーバ、参照サーバ、バックアップデータの保持といった非常時対策状況を確認しておく。

（経営管理編：3.4、企画管理編:11）

サーバ、端末 PC、ネットワーク機器の脆弱性への対応ができているか。

サーバ、端末 PC、ネットワーク機器について、医療機関が管理する機器と、事業者が管理する機器を明確化し、脆弱性情報の収集、脆弱性対応プログラムの適用基準等を定めておく。

（経営管理編：3.4.2、企画管理編：12）

1-2) 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集

インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図が整備できているか。

非常時の役割や手順を定め、医療機関の内部や外部関係機関との緊急連絡先や情報伝達ルートを整備し関係者へ周知しておく。契約書やサービス・レベル合意書(SLA）により、非常時の責任分界点や役割分担について事業者等との明示的な合意内容を確認しておく。

（経営管理編：3.4.3、企画管理編：2.1、12.3、Q&A：企 Q-16）

リスク検知のための情報収集体制が整備できているか。

自医療機関に重要な脆弱性情報が事業者から報告されるスキーム（保守契約等）を確立しておく。ファイアウォール、VPN 等外部接続点のアクセスログを定期的に確認する体制を整備しておく。

（企画管理編：12.2、システム運用編：8.2、17）

教育訓練が実施できているか。

策定した BCP が迅速かつ適切に利用できるように、教育訓練を定期的に実施する。システムが利用できなくなることを想定して、障害時マニュアルや伝票運用マニュアルを準備しておく。教育訓練の結果、必要に応じて改善計画を作成する。

（企画管理編：11.⑥）

バックアップの実施と復旧手順が確認できているか。

オフラインバックアップ等サイバー攻撃を想定したデータとシステムのバックアップの実施と復旧手順の確認をしておく。また、復旧手順においては、業務フローを意識して復旧するシステムの優先度（復旧する順序）をあらかじめ設定しておくことが望ましい。

（経営管理編：3.4.1、企画管理編：11.2、システム運用編：11）

【２．検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）】

2-1）システム異常の報告先の把握

異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。

相談窓口の一本化や体系化を組織内で行う。連絡先を院内に掲示したり、情報セキュリティマニュアルなどのわかりやすい箇所に明示する。

（経営管理編：3.4.2）

2-２）システム異常の検知

院内で発生した異常が院内職員によって覚知できるか。

発生部署、発生個所、発生日時、連絡者、異常の状態について、口頭、報告様式等を用いて正確に伝達する。

（経営管理編：3.4.3）

2-３）CSIRT/経営者によるシステム異常の覚知

院内職員から発出されたサイバー被害情報が組織を通じて速やかに CSIRT（対応者）ならびに意思決定者まで到達するか。

連絡経路を組織化し、院内のどの部署から生じたシステム障害であっても、CSIRT と経営者に必ず伝達されるように担当者を整備する。また、組織変更に応じて適宜最新化し、連絡経路が機能することを担保する。

※CSIRT（Computer Security Incident Response Team）：

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。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する。

【３．初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）】

3-1）原因調査（必要に応じて事業者に依頼）

原因調査のため、「ネットワーク機器やケーブル等の調査」、「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。

障害の原因としてサイバー攻撃の兆候があるか、医療情報システムのメンテナンス等の問題か、医療情報システム自体の問題か、LAN 設備やケーブルの問題か、設備の電源系統の問題か等調査を実施する。また、情報漏えいの有無を調査する。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制にする。

3-2）事業者等への連絡と作業履歴の確認

事業者等への連絡と作業履歴の確認ができるか。

障害の前日等に医療情報システムのメンテナンスやデータ移行等の作業の有無を確認し、該当する場合は、当該作業が障害の原因であるかを確認する。

3-3）被害拡大防止

被害拡大防止に向けた対応ができるか。

3-1 による原因調査の結果、サイバー攻撃の兆候がある場合は、ネットワークの遮断により通信を遮断し感染拡大を防止する。その他、バックドアの無効化、無効にされたセキュリティ機能の復帰、攻撃された脆弱性への対応等の被害拡大防止措置を行う。必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制を整えておく。

（企画管理編：3.1.5、システム運用編：18.1）

3-4）経営層への報告、経営層による確認と指示、組織内周知

経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。

サイバー攻撃の兆候等がある場合は、経営層に報告し、対象となる医療情報システム等の使用の中止を指示する。経営層は、対応チーム設置、及び対象となる医療情報システム等の使用中止に伴う業務運用（診療体制等）方針について検討し、必要に応じて組織内に周知し、対応を求める。（サイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性について検討する。）経営層は診療を継続する観点で「医療施設の災害対応のための事業継続計画」も参考にしながら医療機関全体の事業継続計画を策定する。対象となる医療情報システム等の異常・障害時の、診療体制、及び医療情報システム等を代替した業務運用方法（紙カルテ運用、参照系環境構築等）に関する対処についても定めておく。

例）◯紙カルテ運用

・紙伝票の最新化と帳票準備

・運用フローの作成と共有

○ 参照系環境構築

・サーバおよび端末 PC の構築

・プリンタ、印刷用紙、トナー準備

（経営管理編：3.4、企画管理編：11）

3-5）被害状況等調査（フォレンジック調査＊＋証拠保全）と被害状況等の報告

被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。

アクセスログの分析や情報の改ざんや暗号化の有無等からサイバー攻撃の範囲、個人情報漏洩の有無等について調査し、経営層へ報告する。必要に応じて、事業者へ協力を依頼して調査を進める。自機関で証拠保全が可能か検討し、困難な場合は事業者等へ依頼する。経営層へ被害状況等を適時報告する。あらかじめ初動対応の流れについて事業者等と事前に確認しておくこと。

＊フォレンジック調査：

サイバー攻撃で消去・改竄されたデータや攻撃活動のログを取得し、攻撃対象、方法、被害範囲などを解明する調査のこと

（企画管理編：11）

3-6) 組織対応方針確認と外部関係機関への報告等の対応

組織対応方針を確認できるか。

被害状況（診療継続への影響や個人情報漏洩への有無等）に基づいた経営層による対応方針を確認し、対応する。また、被害状況について所管省庁への報告、法的措置、機密情報漏洩等の対応を確認して報告する。

（経営管理編：3.4.3）

【４．復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）】

4-1）経営層からの復旧指示の確認と実施

復旧指示の確認と実施ができるか。

復旧計画、復旧時間、費用等を踏まえて、経営層は復旧計画を指示し、情報システム担当者等は復旧計画の実施を行う。特に、ワークフローを意識してあらかじめ設定した医療情報システムの「復旧優先度」を基に復旧を行う。復旧優先度は、診療継続を意識して定める「重要度」と異なる場合がある。（Q&A：企 Q-42）

4-2) 医療情報システム等の事業者等へ復旧対応依頼

（医療情報システム等の）電子カルテシステム等の事業者等への対応依頼ができるか。

自機関で復旧が困難な場合、事業者等へ復旧作業を依頼する。

例）・情報システム担当者と事業者間で、バックアップ復元手順や対応者を、平時に定めておく。

・復旧に時間を要する場合、代替として、紙カルテ運用、参照系環境構築を検討する。

（企画管理編：11）

４-3) 再設定や再インストール、バックアップデータ復旧等

再設定や再インストール、バックアップデータの復旧等ができるか。

端末 PC/サーバ復旧手順について、情報システム担当者、事業者等と連携して事前に定め、それに基づき、再設定や再インストール、バックアップからデータ復旧等を実施する。

復旧の際、既知の脆弱性、漏洩した可能性のあるパスワード等に注意する。

（[特集] 医療機関等におけるサイバーセキュリティ:3.3 必要最小限の対策：バックアップ（システム・データ））

４-4) 復旧結果の確認

復旧結果の確認ができるか。

復旧処理について、医療情報システム等が正常に稼働することを確認する。

作業者は手順の進捗状況に合わせて経営層に報告を行い、経営層は組織方針に合わせて運用を変更する。

【5.事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）】

5-1) 復旧結果と情報漏えい事実の有無の報告

復旧結果と情報漏えい事実の有無、可能性について、院内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。

下記を、経営層に報告する（組織内への周知も行う。）。

・異常の内容、原因、被害状況、復旧工数及び費用等について

・復旧結果について

・情報漏えいの有無、範囲について

5-2）再発防止策の検討・策定

再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。

経営層や対策チームを交え、再発防止策の検討・策定を行う。

（経営管理編：1.2.2、3.4.3、企画管理編：2.1.3、3.1.5）

5-3）再発防止策の周知

再発防止策の周知を院内に周知する方法と体制が整備されているか。

確定した再発防止策を、関係者等に周知する。

5-4) 再発防止策の実施

再発防止策の実施が行えるか。

定期的なチェック箇所を割り出し、日々の保守業務へのチェック箇所、実施内容、実施者の落とし込みを行う。

5-5) 事業者等への再発防止策の指示

事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。

策定した再発防止策を事業者へ周知し業務への反映を指示する。指示した再発防止策が実施できているか定期的に確認する。

（企画管理編：2.1.3）

5-6) 外部関係機関への報告と情報公開の検討

情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。経営者と担当者により外部関係機関への報告が行えるか。

経営層と担当者が情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できる体制を備えておく。関係省庁等外部関係機関への報告とサイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性および内容について検討し、経営層の意思決定として策定する。

（経営管理編：1.2.2）

別添３

医療情報システム部門
事業継続計画（BCP）

〇〇年〇〇月〇〇日　初版

〇〇病院

〇〇部門

目次

第 1 章 総則

1.1　策定目的

本事業継続計画（以下、本 BCP という）は、○○病院（以下、当院という）においてサイバーインシデント発生時における組織的対応の基本方針及び職員の取るべき行動の基本原則を示すことによって、医療安全、情報保全を担保しつつサイバー攻撃に対応するセキュリティ体制の構築、ならびに早期復旧までを視野に入れた活動の実現により、国民に信頼される医療機関として社会福祉に貢献することを目的とする。

1.2　基本方針

当院は、個人情報の保護と医療サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。

I.　安全かつ持続的な医療サービス提供を実現する
II.　サイバーセキュリティに対する脅威からの被害から事業を保護する
III.　リスクマネジメントの対象としてサイバーセキュリティを確保する
IV.　平時、非常時を通じて事業継続に関する説明責任を果たす
V.　被害後、医療安全を担保しつつ、迅速かつ合理的な医療業務復旧を行う

1.3　対象範囲

1.3.1 対象とする医療情報システム

対象とする医療情報システムは以下の通り。

I.　電子カルテシステム
II.　医事会計システム（レセプト）
III.　医用画像システム
IV.　各種部門システム（検査、処方など）
V.　オーダリングシステム
VI.　○○○○

1.3.2 想定する事象

本 BCP で想定される事象において、診療業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。

I. 診療情報・参照情報・指示情報の確認・参照不能
II. 診療情報・参照情報・指示情報の入力不能
III. スタッフ間の連絡不能
IV. 情報機器・医療機器の操作不能・誤動作
V. ○○○○○○

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

I. 不正アクセス等
II. 標的型メール攻撃
III. マルウェア感染（ランサムウェアを含む）
IV. 分散型サービス妨害（DDoS 攻撃）
V. ○○○○○○
VI. 上記の予兆と思われる現象

1.4 文書の管理および周知

本 BCP は○○部門にて、現状を適切に反映した原本および関連資料の整備ならびに管理を行い、経営層の承認を受けた上で、当院の全職員に開示周知する。

第２章 体制整備

2.1　情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

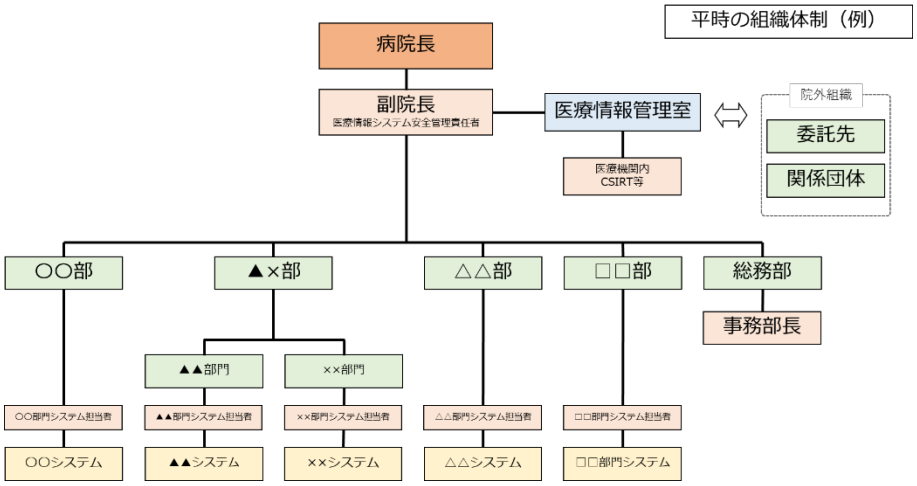
2.1.1 医療情報システム安全管理責任者

○○を、医療情報システム安全管理責任者として定める。△△（理事長、病院長）を当院におけるサイバーセキュリティに関する最高責任者とする。

（医療機関の規模・組織等によっては上記が兼務することも想定される。）

2.1.2 組織体制図

診療継続及び医療情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。



図◯：平時の組織体制図（例）

表◯：担当者の役割（例）

役割	担当部署・担当者	役割の概要
医療情報システム最高責任者	病院長	診療継続及び医療情報システムの復旧の計画策定を統括し、最終的な責任を負う。
医療情報システム安全管理責任者	○○	医療情報システム復旧の計画策定に関する各種検討作業を行う。
病院事務部	○○	診療継続の計画策定に関する各種検討作業を行う。
診療部門システム担当者	○○課	各診療部門システムの運用継続計画策定に関する各種検討作業を行う。
委託先	○○社	医療情報システムの運用保守及び緊急時の状況に関する情報提供・対策調整

2.1.3 情報機器台帳

医療情報システム安全管理責任者は、情報機器の現況を反映した管理台帳を以下（または別紙資料）のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

表◯：情報機器台帳（例）

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（出典：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～ ）

2.1.4 ネットワーク・システム構成図

医療情報システム安全管理責任者は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する（ネットワークの全体像が分かりやすいものを作成）。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2.1.5 リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

表◯：業務内容に対する代替手段（例）

業務内容	システム	代替手段
診療録等	電子カルテシステム	紙運用
処方・検査	オーダリングシステム	紙運用（カーボンコピー）
放射線画像診断	PACS	撮影機器ワークステーションにて画像閲覧
会計	医事会計システム	未収扱いを検討
○○○○○○	○○○○○○	○○○○○○

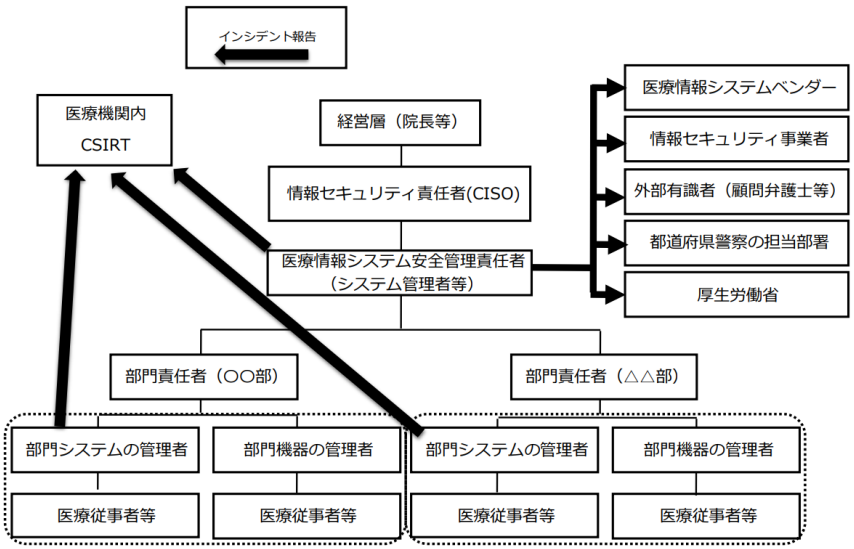
2.1.6 脆弱性に関する対策

医療情報システム安全管理責任者は、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について事業者等と合意した上で取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1 連絡体制図

診療継続及び医療情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制（連絡先、担当、メールアドレス、電話番号、連絡目的等）及び外部関係機関の連絡先を以下のとおり定める。



（出典：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～）

図〇：連絡体制図（例）

表〇：外部関係機関の連絡先一覧（例）

外部関係機関	連絡先
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	03-6812-7837 igishitsu@mhlw.go.jp
〇〇（都道府県警察の担当部署）	××-××××-××××
〇〇	××-××××-××××
〇〇	××-××××-××××

2.2.2 情報収集体制

当院における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を以下のとおり構築する。

表◯：事業者等の連絡先（例）

システム	担当	連絡先
電子カルテ	◯◯社	××-××××-×××× ◯◯@◯◯
保守委託先	◯◯社	××-××××-×××× ◯◯@◯◯
放射線撮影機器	◯◯社	××-××××-×××× ◯◯@◯◯
検査機器	◯◯社	××-××××-×××× ◯◯@◯◯
◯◯	◯◯社	××-××××-×××× ◯◯@◯◯

2.2.3 教育体制

本 BCP が迅速かつ適切に利用できるよう、年◯回以上の教育、訓練を実施する。情報セキュリティ責任者（CISO）、医療情報システム安全管理責任者は年間の教育計画に沿った訓練が適切に実施されるように監督する。訓練結果により、事前対策やサイバーインシデント発生時の対応計画等に解決すべき課題が発生した場合、課題の解決もしくは改善に向けた計画の立案をする。

2.2.4 バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法及び復旧方法について以下のとおり定める。

表◯：バックアップの作成と復旧方法（例）

システム	頻度	作成方法	復旧方法
電子カルテ	1 日	バックアップサーバにデータベースのバックアップを作成する	データベースを再構築した後に、バックアップサーバのデータを復元する
	7 日	磁気テープ・光学メディア・外付け HDD 等にデータベースとシステムファイルのバックアップを作成する	システムの OS を再構築した後に、磁気テープのシステムファイルとデータベースのデータを復元する
◯◯	◯◯	◯◯	◯◯
◯◯	◯◯	◯◯	◯◯

第３章 サイバーインシデント発生時の対応

3.1　異常発見時の連絡先

異常発見時の連絡経路は 2.2.1 の表◯に示す通りとする。あわせて、各担当部門の連絡先は以下のとおり示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。

表◯：部門連絡先一覧（例）

部署名	担当者	連絡先
◯◯部門	◯◯	××-××××-××××
システム管理室	◯◯	××-××××-××××
医療情報システム安全管理責任者	◯◯	××-××××-××××

システム	事業者	担当者	連絡先
電子カルテシステム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××

3.2　システム異常の検知と経営層への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、院内職員から発出された異常において、医療情報システム安全管理責任者によりサイバー攻撃の可能性が思慮された場合、2.2.1 で作成した連絡体制図を基に、速やかに経営層ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する

3.3.1 原因調査

医療情報システム安全管理責任者はサイバーインシデントの原因や被害範囲の特定のために、医療情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

I.　ネットワーク機器やケーブル等の調査
II.　電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査
III.　情報漏えいの有無に関する調査
IV.　メンテナンスやデータ移行等の作業に関する調査
V.　○○○○○○

3.3.2 被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション境界において、通信を遮断して感染拡大防止を図る。

3.3.3 経営層への報告

医療情報システム安全管理責任者はサイバーインシデントについて経営層に対して、現在の被害状況を報告するとともにインシデント対応方法と患者安全を担保する運用方針案を提案する。この内容を踏まえて、経営層はシステム停止に伴う診療継続方針（診療体制の確保等）を検討し意思決定する。決定した内容は、速やかに 2.2.1 の連絡体制図で定める組織内ならびに外部関係機関へ周知を行う。

3.4　診療継続

サイバーインシデント対応と診療継続について報告を受けた経営層は以下のとおり対応する。

3.4.1 医療情報システムの縮退運転判断

経営層は医療情報システム安全管理責任者からの提案を受け、医療情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の診療継続においては、紙カルテの運用等、自然災害時を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

3.4.2 被害状況等調査（フォレンジック調査＋証拠保全）

医療情報システム安全管理責任者は、証拠保全の作業と診療継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査について医療安全を担保しつつ行う。必要に応じて医療情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時経営層に報告する。

3.4.3 組織対応方針の確認と外部関係機関への報告

医療情報システム安全管理責任者の被害状況および調査結果に基づき、経営層は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。また、2.2.1 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

3.5　復旧処理

復旧計画に基づいて、以下のとおり対応する。医療情報システム安全管理責任者は医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。

3.5.1 復旧指示と復旧作業

医療情報システム安全管理責任者は、経営層からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ医療情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。経営層は、アナログ情報の反映時期ならびに程度を医療安全の観点を踏まえて意思決定する。

3.5.2 結果の確認

医療情報システム安全管理責任者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、経営層に報告する。経営層は診療状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章 事後対応

4.1　報告

復旧後、復旧結果と情報漏えい事実の有無等について、経営層及び組織内に報告する。不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

4.2　再発防止

4.2.1 再発防止策検討・策定

4.1 の後、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、経営層に提案する。経営層は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。経営層は決定した再発防止策について、連絡経路を用いて全職員に周知する。

4.2.2 事業者への指示

経営層によって決定された再発防止策は、医療情報システム安全管理責任者等により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、医療機関側と誠実に議論し、計画を立てて実施する。

4.3　情報公開

経営層は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また当院を受診する患者への診療に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1 次対応、患者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。