| 監査技法（NISC） | 医療における患者死亡リスク | 医療におけるワークフロー停止リスク | 望ましい対策ならびに能力<br>（NIST CSF・IT-BCP 観点） | 関連付く項目<br>（医療情報システム安全管理 GL 第 6.0 版） |
|---|---|---|---|---|
| **質問（ヒアリング）** | リスクを「患者死亡リスク」「医療ワークフロー停止」の2つに大別する。「患者死亡リスク」においてこれらが影響する1系・4系（手術/ICU等における生命維持装置、麻酔・手術、救急）について、サイバー攻撃や長時間障害時に「どの時点で何を止める／続けるか」「誰が最終判断を行うか」を各職種から聴取する。代替ワークフロー（紙カルテ・スタンドアロン機器など）を具体的に説明できるかを確認する。 | 「医療ワークフロー停止」のリスク視点から、外来受付～検査～会計、入退院事務、検査・調剤・地域連携が停止した場合の縮小診療や手動運用の手順を、診療科長・看護部・医事部・情報部門・ベンダから聴取する。ネットワーク分断や院外連携停止時の運用（地域連携システムやクラウドサービス停止時）を説明できるか確認する。 | RMFによって重点指定された箇所について、CSF Identify／Protect に基づき「重要業務・重要システムの定義」「RMF 1～4系の優先順位」を説明できること。CSF Respond／Recover の観点から、インシデント発生時の指揮命令系統、広報・説明責任、善後策の検討プロセスを、経営層・企画管理者・システム運用担当者が共通言語で明確に回答できること。 | 概説編：医療機関等の責務とサイバー攻撃を踏まえた IT-BCP の必要性全般。経営管理編：1章「責任（平常時・非常時）」「委託・第三者提供の責任」、2.1～2.2「リスク評価とリスク管理方針・説明責任」、3.1「統制の体系」。 |
| **チェックリスト** | RMF 1系・4系のハイリスク機能（ICU／SCU、手術室、救急、生命維持 IoT）が、医療機関向けサイバーセキュリティ対策チェックリストや院内独自チェックリスト上で別立ての管理対象になっているかを確認する。停電・ネットワーク断・ランサムウェア時に患者が死亡し得るシナリオが網羅されているかを点検する。 | 受付・会計・オーダリング・LIS／RIS・調剤支援・地域連携など各系統について、停止時の代替運用（縮小外来、紙運用、ローカルモードなど）と復旧順位がチェックリストに組み込まれているかを確認する。NIST CSF 各機能に対する達成度を自己点検できる形式になっているかをみる。 | CSF Identify に基づく資産・業務の棚卸と重要度区分、Protect／Detect に基づく技術的・組織的対策項目、Respond／Recover に基づく IT-BCP チェック項目を、ガイドライン付属のチェックリストとローカルチェックリストで一貫して管理する能力。 | 概説編・別添「サイバーセキュリティ対策チェックリスト」、経営管理編 2章「リスク評価を踏まえた管理」、企画管理編「リスク評価とリスク管理」「システム・サービス事業者からの情報収集とチェックリスト活用」（MDS／SDS 等）。 |
| **査閲（レビュー：規程・ログ等）** | 「患者の生命・身体への影響を最小化しつつ診療継続を図る」ことが、情報セキュリティポリシー、IT-BCP、医療安全管理規程、救急・集中治療関連マニュアルのいずれにも一貫して書かれているかを査閲する。生命維持装置や手術支援機器の運用手順にサイバーインシデント時の取扱い（院内 LAN 切断、リモート保守遮断など）が明記されているかを確認する。 | 電子カルテ・LIS／RIS・調剤支援・地域連携システムの障害対応手順書、ネットワーク構成図、バックアップ・リストア手順、手動運用マニュアルを突き合わせ、RMF 2～4系のワークフローが停止した場合にどこまで代替可能かを文書から検証する。重大障害ログ・インシデント記録から、復旧時間と診療影響の整合性もレビューする。 | CSF Identify／Protect：資産台帳・ネットワークトポロジー・責任分界表が最新であり、ガイドラインに沿って文書化されていること。Detect／Respond／Recover：ログ管理規程・インシデント対応手順・BCP 訓練記録から、検知～分析～復旧までのプロセスが実際に運用されているかを評価する能力。 | 経営管理編：1.3「委託・責任分界」、2.1～2.2「リスク評価とリスク管理方針」「ISMS の実践」、2.2.3「リスク分析を踏まえた要求仕様適合性」、3.1「統制」。企画管理編：組織体制規程、ネットワーク・クラウド・リモートサービス・情報管理に関する規程。システム運用編：アクセス管理、ログ管理、バックアップ・障害対応・災害対策に関する章全般。 |
| **観察（視察）** | ICU・手術室・救急室等で、運用担当者が手順書に従って機器を運用しているかを現場で確認する。ネットワーク遮断や院内システム停止を想定した訓練時に、患者安全を優先した縮小医療や転送判断が実際に行われているかを観察する。 | 外来受付・検査部門・病棟・薬剤部・地域連携窓口で、障害時の暫定フロー（紙受付、紙オーダ、手書きラベル、電話連絡など）が現実的に回るかをウォークスルーする。復旧時のデータ再入力・照合作業が過大な負荷や入力ミスにつながっていないかを確認する。 | CSF Protect／Detect：物理・環境・アクセス管理が現場で実効性を持っているか、観察を通じて評価する能力。Respond／Recover：訓練時に HICS などの指揮系統が実際に動作しているか、代替運用の起動・停止の判断が明確かを確認すること。 | 概説編：医療現場での安全管理と情報セキュリティの関係。経営管理編：3.1「統制」、4章（医療安全管理体制等）。企画管理編：運用手順・教育訓練・物理・環境対策に関する章。システム運用編：日常運用・障害対応手順、運用監視。 |
| **再実施** | 生命維持装置のネットワーク遮断試験、非常電源切替え試験、EHR／LIS の停止を想定した模擬診療などを、監査人立会いの下で限定的に再実施し、「患者に危険を与えずフェイルセーフに移行できるか」「医療安全上の判断が適切か」を検証する。 | 電子カルテ・ネットワーク・VPN・ゲートウェイ等の切替え試験を再実施し、外来や入退院事務、検査・調剤・地域連携がどの程度の停止時間であれば許容できるか、RTO／RPO が実測値と整合しているかを確認する。 | CSF Protect／Detect：アクセス制御・セグメント間通信制御・EDR 等が期待どおりに動作するかを実証する能力。Respond／Recover：システム切替え、バックアップからのリストア、業務復旧手順が手順書通りに実行できるかをテストする能力。 | 経営管理編：2.1「リスク評価の実施」および 2.2「リスク管理」「ISMS の PDCA」、3.1「統制」。企画管理編：BCP／DR 設計、ネットワーク・電源・クラウド構成。システム運用編：バックアップ・切替え手順、定期訓練・テスト。 |
| **サンプリング** | 重大インシデントやヒヤリハットの記録から、RMF 1系・4系に関わる事例をサンプリングし、「サイバー要因の有無」「診療継続の可否」「患者転帰」を追跡する。重点リスクに対する再発防止策が講じられているかを評価する。 | 障害ログ、変更管理記録、運用日誌、ヘルプデスク記録から、システム停止や性能劣化の事例をサンプリングし、受付～検査～会計、入退院、地域連携に与えた影響と復旧時間を分析する。サンプリング結果と IT-BCP の想定が整合しているかを確認する。 | CSF Detect：ログ・監査証跡・インシデント記録を継続的に分析する能力。Respond／Recover：サンプリング結果をもとに、リスク管理方針・BCP の見直しに反映する ISMS／PDCA の運用能力。 | 経営管理編：2.1～2.2「リスク評価とリスク管理」「説明責任」、3章「安全管理全般」。企画管理編：ログ・監査証跡管理、変更管理、インシデント管理。システム運用編：運用記録・障害記録の保存とレビュー。 |
| **脆弱性診断** | 電子カルテ、LIS／RIS、手術・麻酔装置の管理端末、院内 IoT（1-1／1-2）など、停止が直接生命に影響するシステムについて、パッチ管理や設定不備などの脆弱性を洗い出し、「攻撃されれば致死的結果になり得る箇所」を特定する。医療機器ベンダとの責任分界も確認する。 | 外来・病棟端末、VPN、ゲートウェイ、地域連携システム、クラウドサービスなどについて、脆弱性スキャンや設定レビューを実施し、ランサムウェアや侵入拡大の起点となる弱点を特定する。診療ワークフロー全体に波及する経路を可視化する。 | CSF Protect／Detect：構成管理・パッチ管理・脆弱性管理プロセスの整備と、定期的な診断結果の評価能力。Identify：診断対象の選定が RMF 1～4系のリスクに基づいていること。Respond：緊急度に応じた是正計画の立案・実施能力。 | NISC 監査手引書 表 2.1-2「脆弱性診断の概要」と注意点。 ガイドライン：概説編・企画管理編におけるサイバー攻撃対策・技術的対策、経営管理編のリスク評価とリスク管理、システム運用編の脆弱性管理・パッチ管理等。 |
| **ペネトレーションテスト** | 生命維持系ネットワークに対しては、原則として本番環境への直接攻撃は避ける前提で、検証環境やシミュレーションを用いつつ「侵入された場合にどこまで安全機能が維持できるか」「医療機器のフェイルセーフ設計が有効か」を検証する。テスト範囲と安全条件の合意が必須である。 | 受付・会計・オーダリング・LIS／RIS・地域連携・VPN・ゲートウェイなどを対象に、院外からの侵入、権限昇格、横移動、データ暗号化・窃取を想定した疑似攻撃を実施し、診療ワークフローがどの段階で機能不全に陥るか、検知・封じ込め・復旧の実力を評価する。 | CSF Detect／Respond：SOC／EDR／ログ分析・アラート対応が、実際の攻撃シナリオに対して有効に機能するかを検証する能力。Recover：テスト結果を踏まえたネットワーク再設計、ゼロトラスト化、IT-BCP 強化の計画立案能力。Governance：テスト方針・スコープ・安全基準を経営層が承認し、責任分界を契約で整理していること。 | NISC 監査手引書 表 2.1-2「ペネトレーションテストの概要」。 ガイドライン：概説編におけるサイバー攻撃リスクの位置付け、経営管理編のリスク低減と説明責任、企画管理編のネットワーク・クラウド・リモートサービスに関する安全管理、システム運用編のインシデント対応・事業継続。 |