厚生労働行政推進調査事業「医療機関におけるサイバーセキュリティ対策向上に 向けた課題調査と解決策の検討（25IA2012）」
施設訪問インタビューシート（Ver6. 2026.02.04）

A. 基本情報

No	大分類	小分類	調査結果
A-1	病院情報	病院名	
		所在地	
		病床数	
		病院区分	
		医療情報部門の有無、人数	
A-2	電子カルテベンダー、構築ベンダー	電子カルテシステムベンダーについて教えてください。 あわせて、実際に構築したベンダーが電子カルテシステムベンダーでない場合は、そのベンダーを教えてください。	製品名およびベンダー名： 構築ベンダー：
A-3	ネットワーク機器ベンダー、構築ベンダー	ネットワーク機器ベンダーについて教えてください。 あわせて、ネットワーク構築ベンダーについても教えてください。	製品名： 構築ベンダー：
A-4	セキュリティベンダー	セキュリティ対策について最もやり取りのある（相談する）ベンダーについて教えてください。	
A-5	主要ベンダー	医療情報システム関連で最もやり取りのある（相談する）ベンダーについて教えてください。	

B. 調査項目

No	大分類	調査の視点	調査結果	該当チェックリスト／調査項目	ヒアリングポイント
B-1	セキュリティ人材	・セキュリティ立案に関与する職員（立場、経験値、人数） ・セキュリティ運用に関与する職員（立場、経験値、人数） ・人材が確保できない要因、確保に向けて取り組んでいることは何かあるか。 ・医療情報技師（上級医療情報技師）の役割、どのように活動しているか。 ・IPA資格取得者の役割、どのように活動しているか。		【医療情報システム安全管理責任者を設置している。(1-(1))】 情報セキュリティ責任者（CISO: Chief Information Security Officer）を配置していますか。 ※医療情報システムの安全管理に関するガイドライン第6.0版では、「サイバー攻撃に対しては情報セキュリティ責任者（CISO（Chief Information Security Officer））の配置や、情報セキュリティ責任者（CISO）はサイバーセキュリティに対する知識をどの程度保有していますか。	・どの程度のエフォートか（ほぼ専任？） ・情報セキュリティに関する定期的なWGの有無など ・セキュリティ人材の教育などの課題 ・経営層（院長レベル）のセキュリティへの人・金の投資への理解など
B-2	資産管理	・実際にどのような手段（方法）で台帳管理しているか。 ・棚卸のタイミング、棚卸に要する工数はどうか。 ・問題点と対応にはどのようなものがあるか。		【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))】 医療情報システムに接続するサーバ、端末PC、ネットワーク機器の台帳管理を行っていますか。	・部門（診療科）が管理する機器などの把握
B-3	外部接続点管理	・外部接続点の把握方法 ・どのように調査、整理整頓を行い、棚卸を実施するか ・リモート接続時の運用ルールについて ・外部接続点における課題、運用がうまくいかない理由は何か。		【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))】 リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法についてお答えください。	・外部接続の主な用途 ・外部接続の方法（施設主導の接続／ベンダー提案の接続） ・すべての外部接続点（FW）を把握・管理できているか ・部門が管理する機器の外部接続点の有無 ・外部接続の希望があった場合の対応フローが施設で整理されているか
B-4	MDS／SDSへの対応	・MDS/SDSからどのようなアクションをとったか。 ・現在の活用状況、また将来的にどう活用しようとしているか？		【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）の提出を受けていますか。	
B-5	ユーザー管理	・システムの利用者管理についてどのように運用しているか。 ・アプリの利用者管理はどのように行なっているか（新規追加から削除停止までのフロー、権限変更手順） ・OS、ミドル、ネットワークの利用者管理はどうしているか？ ・ロックアウト設定、パスワード変更タイミング、MFA対応などは実施できているか。またその範囲はどうか。		【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))】 【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。(令和7年度2-④)】 サーバ、ネットワーク機器に対するアクセス権限の付与方法について、教えてください。 【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))】 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または無効化していますか。	
B-6	各種ログ管理	・各種ログ管理について（電子カルテなど部門システムの利用ログでない） ・各種ログの収集方法 ・各種ログの確認タイミング ・各種ログの解析は誰がいつ、どのくらいの時間をかけて行なっているか。 ・ログ管理がうまくいかない理由はなにか？		【アクセスログを管理している。(2-(6))】 サーバ、端末PCのアクセスログを残していますか。	
B-7	セキュリティパッチ管理	・セキュリティパッチの実態について ・セキュリティパッチの適用方法と対応タイミング（情報認知から実施までの手順） ・対応範囲（アプリ、ミドル、OS） ・対応している中での課題（ベンダー、院内との意識） ・ベンダー等との契約はどのようになっているか？仕様書への記載文言はどのような内容か？ ・セキュリティパッチの対応がうまくいかない理由は何か？		【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))】 サーバ、端末PC、ネットワーク機器に対し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）を適用していますか。	
B-8	二要素認証への対応	・機器に対する二要素認証の有無について ・一要素認証の場合の進められない課題、対応予定など		【二要素認証を実装している。または令和９年度までに実装予定である。(2-(10))】 サーバ、端末PC、ネットワーク機器に対する二要素認証の実装状況について。	
B-9	外部記憶媒体管理	・接続制限はどのように行っているのか？技術的対策？組織的対策？ ・その他ルールは何か？		【USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。(令和7年度 2-⑨)】 USBストレージ等の外部記録媒体や情報機器に対してサーバへの接続を制限している。	
B-10	システムバックアップ運用管理	・バックアップの取得方法、どのシステムで取得しているか？ ・取得したバックアップの管理方法はどうか？オンライン？オフライン？		【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))】 データやシステムのバックアップの対象を検討していますか。	
B-11	IT-BCPの策定と訓練	・IT-BCPで厚労省提示のものから追記した項目はあるか。 ・自然災害を想定したBCPとどこまで融合させているか。 ・誰が、どのくらいの期間で構築したか。 ・見直しを定期的に実施しているか。 ・IT-BCPに基づく訓練はどう対応しているか。 ・IT-BCPの対応がうまくいかない理由はなにか？		【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)) 】 サイバー攻撃を想定した事業継続計画（BCP）を策定していますか。	
B-12	その他	・セキュリティ対策に対して伝えたいこと、今後期待すること等			・セキュリティソフトの導入・保守は規模によって数百～数千の場合もある ・医療機器と違って診療報酬に結びつかず、導入のハードルは高い ・導入したからとって対策が完了する訳ではなく、運用できる人材が不可欠 ・施設の創意工夫に依存するか、何かトップダウンの施策が望ましいか