別添資料X：訪問インタビュー調査結果の要約

該当チェックリスト／調査項目	病院H	病院I	病院J	病院K
病院区分	国公立病院	国公立病院	一般病院	一般病院
インタビュー実施日	2026年2月16日	2026年2月16日	2026年2月16日	2026年2月16日
医療情報部門の体制	医療情報部（部長は医師）の下に情報企画室があり、セキュリティについては、主に教員6名、研究員・技術職員3名で運用している。	教員1名、事務員2名、SE4名（常駐委託含む）で運用している。	情報システム管理室（放射線科医が室長）。6人で運用している（全員が臨床と兼務）。	院長1名、副院長1名の元、情報企画室2名で運用している。
【医療情報システム安全管理責任者を設置している。(1-①)】	医療情報システム安全管理責任者を設置しており、実務レベルにおいて、高度な専門知識を持つ教員が、具体的な立案や運用を主導している。	医療情報システム安全管理責任者を設置しており、実務レベルにおいて、高度な専門知識を持つ教員が、具体的な立案や運用を主導している。	医療情報システム安全管理責任者（病院長）を設置しているが、様々な対策を行うのに十分な体制とは言えない。	医療情報システム安全管理責任者（病院長）を設置しているが、様々な対策を行うのに十分な体制とは言えない。
【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)】	Excelにて台帳管理を行っている。	資産管理ソフト「SSI」で電子カルテネットワークを管理。	Excelにて台帳管理を行っている。	Pleasnter（WEBデータベースにて管理）と電子カルテのアプリで管理。
【リモートメンテナンスを利用している機器の有無を確認した。(2-②)】	自施設が設置するリモート接続の仕組み使った接続を原則とするが、ベンダー側の理由で例外を認めている。 古い機器で管理部門が把握・管理できていない接続点もあることが懸念。	20回線のリモート接続を把握。ベンダーが希望する場合に例外的にベンダー主導の回線を許容。	ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握している）。	セキュリティ調査時にチェックした時に全体を把握している。リモートの運用ルールについてセキュリティが担保されたものを使っているかベンダーに説明を求めている。
【医療情報セキュリティ開示書（MDS/SDS）を提出してもらっている。(2-③)】	取得しているが、現状は具体的なネクストアクションには至っていない。	取得しており、必要に応じてベンダーへのヒアリングおよび対策を行っている。	取得しているが、現状は具体的なネクストアクションには至っていない。	取得しているが、現状は具体的なネクストアクションには至っていない。
【職種・業務別のアクセス利用権限設定／不要アカウントの削除。(2-④、2-⑤)】	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している（一部、サーバについては不要アカウントの削除はできていない）。	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している（一部、サーバについては不要アカウントの削除はできていない）。	administrator権限のみ設定し、全ての機器群で同じパスワードを設定している	すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している。退職時に手動で不要アカウントを削除している。
【アクセスログを管理している。(2-⑥)】	端末PCについてはアクセスログを残している。サーバについても一部の機器のアクセスログを残しているが、定期的には確認できていない。	全ての機器のアクセスログを残している。サーバ・VPNは保守事業者が定期的に確認している。	電子カルテの操作ログ、サーバーについては把握できていない。NWログについては収集の仕組みを検討している。	現在電子カルテのログ以外保存できていない。復旧のため、サーバ・NWについては、今後検討する。
【セキュリティパッチを適用している。(2-⑦)】	端末PCは定期的に実施。サーバについては、ベンダーからの提案に基づき実施。外部接続用のネットワーク機器は、情報を認知後速やかにアップデートを行う運用。	端末PCは定期的に実施。サーバについては、ベンダーからの提案に基づき実施。外部接続用のネットワーク機器は、情報を認知後速やかにアップデートを行う運用。	サーバ、端末PCについては、適用できていない。NW機器については、全ての機器に対して適用している。	サーバーはパッチ適用していない。端末は手動でバージョン適用をしている。ネットワーク機器は適宜行うが、都度更新はできていない。
【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。(2-⑩)】	電子カルテ端末については二要素認証（職員カード+パスコード）を実装済み サーバ、ネットワーク機器は二要素認証までできていない。	電子カルテ端末については二要素認証（職員カード+パスコード）を実装済み サーバ、ネットワーク機器は二要素認証までできていない。	二要素認証ができていない。次期システム更新で実装する予定。	現在は導入していない。二要素認証は今後導入を前向きに検討している。
【USBストレージ等の外部記録媒体の接続を制限している。(2-⑨)】	許可されたUSBのみ接続できるようにしている。	許可されたUSBのみ接続できるようにしている。	許可されたUSBのみ接続できるようにしている。	サーバー上で各端末において外部記憶媒体の接続や起動の制限を管理している。 通常、USBは病棟や外来では起動しないが、必要な場合、適宜、可否を判断している。
【バックアップの実施と復旧手順の確認。(3-②)】	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	すべての医療情報システムのデータはバックアップが取れている（復旧手順については医療機関側で十分に確認できていない）。	バックアップサーバーにデータが保存され、ベンダーのデータセンターにもバックアップが保存されている。
【サイバー攻撃を想定したBCPを策定している。(3-③)】	自施設で独自に策定したものを運用（ただし、定期的な見直しはできていない）。	自施設で独自に策定したものを運用（ただし、定期的な見直しはできていない）。	厚労省のひな形をベースに独自マニュアルを整備。ただし、定期的な見直しはできていない。	自然もIT-BCPもどちらも対応可能な形のマニュアルにしている。