CISA-CDM	1: Data Protection Management	2: Network Security Management		3: Identity and Access Management		4: Asset Management				
チェック項目／病院情報システム構成要素	バックアップ/復旧基盤	ネットワーク/境界	外部接続/保守/事業者	ID/権限基盤	権限管理	電子カルテ	端末PC/VDI	医療機器/IoT	検体検査・放射線・薬剤等部門(RMF-High)	サーバ/仮想基盤
1-① 安全管理責任者設置	復旧統括者・担当者明確化	NW責任者・連絡先明確化	事業者窓口・連絡先明確化	権限承認者・連絡先定義	責任者・代行・委員会・連絡先設置	システム責任者・連絡先選出	端末管理責任部門選出・連絡先明確化	機器管理責任者選出・連絡先明確化	各部門で責任者を選出・連絡先明確化	基盤(ハードウェア)オーナー明確化・連絡先明確化
2-① 資産台帳管理	バックアップ対象・RTO/RPO台帳	IP・FW・アクセス制御リスト台帳	回線・接続元・契約台帳	ID・特権ID台帳	CMDB・棚卸周期	版数・DB・連携先台帳	所属・権限・EDR台帳	IP/MAC・保守形態台帳	装置・接続先台帳	機種・OS・EOL・XDR
2-② リモート保守有無確認	緊急遮断手順	閉域/VPN・送信元制限	全台数把握・作業画面・環境録画・作業許可制	保守ID分離・MFA(多要素認証)	承認制・申請台帳	対象機能明確化	常時許可禁止	装置別可否・手順化	対象機能明確化	Jump経由・時間制限
2-③ MDS/SDS提出	復旧支援範囲明確化	暗号・管理IF仕様確認	提出義務・更新通知条項	認証方式の明示	調達要件化・改版時再提出	MDS/SDS受領	端末制約確認	同・保守条件確認	MDS/SDS受領	OS/脆弱性対応仕様確認
2-④ 職種/業務別権限設定	非常時権限付与手順	NW管理権限分離	保守権限最小化	職務ベースアクセス制御・特権管理・定期棚卸	権限基準・職務分掌	職種別権限・緊急閲覧統制	ローカル管理者禁止	操作/設定権限分離	技師/医師/保守分離	管理者権限分離
2-⑤ 不要アカウント削除/無効化	緊急失効手順	共有ID廃止	契約終了時停止	アカウントライフサイクル管理自動化	入退職連動型サービス品質保証(SLA)	退職者ID即時停止	休眠端末ID停止	保守ID失効	退職者ID即時停止	孤立ID・共有ID棚卸
2-⑥ パッチ適用	パッチ起因障害の復旧手順	FW/SW/無線更新	SLA・緊急連絡体制	認証情報管理システム/アクティブディレクトリ更新	パッチ方針・例外管理	アプリ/DB/OS更新計画	OS/EDR/アプリ更新	ファーム更新・代替策	ベンダ協調更新	OS/ミドル/DB更新
2-⑦ パスワード強度/更新	非常時保管手順	機器秘密情報管理	保守IDへ強制適用	長パス・辞書禁止・MFA	パスワード標準強度設定	個人ID徹底・共有禁止	LAPS等で端末PW分離	既定PW変更	個人ID徹底・共有禁止	サービスアカウント管理
2-⑧ パスワード使い回し禁止	緊急PWも一意化	機器ごと別PW	事業者共通PW禁止	シングルサインオン(SO)・秘密情報管理庫	禁止規程	個人認証徹底	端末ローカルPW個別化	装置既定PW個別化	個人認証徹底	共通管理PW廃止
2-⑨ USB等外部媒体制限	災害時代替媒体手順	NAC/ポート制御	持込媒体申請・消毒手順	例外申請者限定	媒体持込規程・例外承認	データ書出し制御	Device Control・暗号化	FW更新媒体の許可制	装置取込の例外管理	USB無効
2-⑩ 二要素認証	緊急代替認証手順	VPN/管理GUIで必須	保守接続で必須	IdP/FIDO2/OTP	MFA方針・対象定義	院外利用・管理操作で必須	VDI/端末管理で必須	可能機種は管理面で必須	管理機能で必須	管理者・遠隔接続で必須
2-⑪ アクセスログ管理	復旧/演習ログ保全	Syslog/NetFlow	保守セッション録画	認証/特権操作ログ	保管基準・監査体制	参照・更新監査証跡	EDR/OS操作ログ	設定変更・操作ログ	検査/画像操作ログ	OS/DB/Sysmon/SIEM連携
2-⑫ 不要ソフト/サービス停止	復旧後の再無効化	未使用管理IF停止	不要保守口閉鎖	不要連携停止	ハードニング基準	不要モジュール停止	不要アプリ削除	未使用ポート/サービス停止	不要機能停止	不要サービス停止・allowlist
2-⑬ 接続元制限	非常時暫定許可手順	VLAN/ACL/セグメンテーション	固定IP・Jump host	管理系接続元限定	通信許可基準	AP-DB間など通信最小化	管理接続元限定	医療機器専用セグメント・物理キー	装置-部門鯖間限定	Host FW・allowlist
3-① インシデント時連絡体制	指揮命令系統の作成と組織合意	NW当番体制	24時間窓口・警察/厚労省連携	認証基盤障害連絡先制定	CSIRT(サイバー初動対応者)・連絡網・報告順序の制定	EHR責任者・ベンダ連絡先	HD/現場支援窓口設置	ME/機器業者連絡先連絡先決定	部門責任者連絡先決定	基盤当番体制決定
3-② バックアップと復旧手順確認	Offline/Immutable保有・復旧訓練	機器設定backup	復旧支援SLA	ディレクトリ/秘密復旧	優先復旧順序定義	DB/帳票/IF復旧手順	Gold image・予備機	設定export・再設定手順	検査/画像データ復旧	仮想環境イメージ/DB/設定backup
3-③ サイバー攻撃想定BCP	RTO/RPO・訓練・演習	分断/迂回設計	保守停止/緊急接続統制	代替認証・停止判断	Cyber BCP・ダウンタイム運用手順・実施指示権限制定	紙カルテ・ダウンタイム運用	代替端末・紙運用	スタンドアロン運用	検査依頼紙運用	隔離/再構築手順
4-① 1-3を規程化	Backup/復旧/BCP台帳・手順文書	FW/ACL/分離手順	リモート保守規程・契約条項	ID管理手順書	運用管理規程・委託契約取り交わし	権限/監査/変更管理規程	端末管理基準	医療機器接続基準	装置別運用手順	構築/ハードニング手順
鳥飼追加:サイバー攻撃検知(CSF-Detection能力チェック)	負荷トレンド異常監視	IPS/NDRによる異常トラフィック量・経路検知	異常検知時に速やかに連絡照会	異常振る舞いアカウントの検知・管理者通知	管理者権限アカウントの監視	XDRなどによる攻撃予兆検知	挙動監視・なりすまし監視	設定(流量など)の適性値監視	挙動監視・なりすまし監視	挙動監視・なりすまし監視
鳥飼追加:サイバー攻撃対処(CSF-Response能力チェック)	バックアップ経路即時遮断	アタックサーフェス経路即時遮断	サイバー攻撃状態での安全な異常確認・設定セキュア化作業実施	異常検知アカウントの権限停止	管理者権限アカウントの異常時停止	カルテ隔離後参照系自動切換えなど保護手段実施	異常端末をネットワーク自己隔離やネットワークスイッチ連動隔離	異常設定値時に医療安全側に動作モードが遷移する(フェイルセーフ)	異常サーバをネットワーク自己隔離やネットワークスイッチ連動隔離 紙運用一斉同報・切り替え	異常サーバをネットワーク自己隔離やネットワークスイッチ連動隔離 幹事社に異常自動通知