

歯科医院 日常セキュリティ点検シート

日次・週次ルーチン確認用

点検月日: 年 月 日

医院名:

点検責任者:

点検項目	確認ポイント(具体的な点検内容)	確認
画面・付箋確認	受付や診療台(ユニット)のPCモニター、机上にID・パスワードを書いた付箋やメモが貼られていないか	☐
セキュリティ警告	PC起動時にウイルス対策ソフト等から異常を知らせる赤色警告やポップアップが表示されていないか	☐
通信機器ランプ確認	ルーター、ONU(光回線終端装置)、UTM等の機器に赤点滅などの通信エラー・異常ランプが出ていないか	☐
OSの更新状態	Windows等の再起動待ちマーク(更新保留)がある場合、診療開始前または夜間に再起動を完了できるか	☐

点検項目	確認ポイント(具体的な点検内容)	確認
離席時の画面ロック	受付カウンターやユニットを離れる際、必ずショートカットキー Win + L 等でロックしているか	☐
不審メール・添付警戒	心当たりのない差出人からの「請求書」「納品書」「発注書」等の添付ファイルやURLを安易に開いていないか	☐
私用端末・機器の接続禁止	電子カルテやレセコン端末に、私物スマホ(充電目的含む)や許可のない私物USBメモリを接続していないか	☐
カルテ・予約の覗き見防止	待合室や会計窓口の患者・付添者から、電子カルテ画面や予約表の患者個人情報が見えない角度に調整されているか	☐
外部媒体の接続管理	デジタルレントゲンやCAD/CAM等でUSB等を使用する場合、ウイルススキャン済み等の院内ルールを守っているか	☐

点検項目	確認ポイント(具体的な点検内容)	確認
システムログアウト	電子カルテ、レセプトコンピュータ、アポイント帳、オンライン資格確認端末から確実にログアウトしたか	☐
書類・媒体の施錠保管	技工指示書、問診票、紙カルテ、バックアップ用USB/ポータブルHDDを施錠可能なキャビネットに保管したか	☐
PC本体の完全シャットダウン	スリープ状態のまま放置せず、OSメニューから「シャットダウン」を実行して電源を完全に切ったか	☐
バックアップ稼働確認	クラウドバックアップや外付けHDD等への自動退避処理が正常に完了・進行しているか確認したか	☐

⚠️【緊急初動手順】ランサムウェア感染・身代金要求画面・異常動作発生時

STEP 1

PCの電源は切らない

(メモリ上の調査証拠を残すため)

STEP 2

有線LANを抜く / Wi-Fi切断

(他端末への感染拡大を直ちに遮断)

STEP 3

直ちに院長・管理責任者へ報告

(保守事業者・専門機関への初動連絡)

院内緊急連絡先(院長等): TEL:

システム保守業者担当: TEL:

医療機関サイバーセキュリティ対策 チェックリスト

厚生労働省「令和7年度版チェックリスト」対応

確認年度: 令和 年度

医療機関名:

安全管理責任者:

※立入検査時、本チェックリストが確認されます。令和7年度中にすべての項目で「はい」にマルが付くよう計画的に整備してください。
※「いいえ」の場合は、改善目標日を記入し事業者等と連携して対応を進めてください。(各番号は厚生労働省チェックリストマニュアルに対応)

1. 体制構築

大項目	確認項目(厚労省基準要件)	確認結果	確認日 / 目標日	備考・対策状況
責任者設置	医療情報システム安全管理責任者を院内に設置している。 1-1	☐ はい ☐ いいえ	確認: / 目標: /	院長または指定スタッフ名:

2. 医療情報システムの管理・運用

対象範囲	確認項目(厚労省基準要件)	確認結果	確認日 / 目標日	備考・対策状況
資産・保守 事業者管理	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	確認: / 目標: /	機器管理台帳の整備
	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保守事業者を確認した。 2-2	☐ はい ☐ いいえ	確認: / 目標: /	※保守契約なしの場合は対象外
	事業者から医療情報セキュリティ開示書(MDS / SDS)の提出を受けている。 2-3	☐ はい ☐ いいえ	確認: / 目標: /	電子カルテ・レセコン事業者へ要請
アカウント 認証管理	職種・業務別のアクセス権限設定、および管理者権限対象者を明確化している。 2-4	☐ はい ☐ いいえ	確認: / 目標: /	院長・歯科衛生士・受付等
	退職者や未使用のアカウントを遅滞なく削除または無効化している。 2-5	☐ はい ☐ いいえ	確認: / 目標: /	退職時チェックリストの徹底
セキュリティ 設定・運用	OSやネットワーク機器に最新パッチや更新プログラムを適用している。 2-6	☐ はい ☐ いいえ	確認: / 目標: /	ルーター等のファームウェア含む
	パスワード要件(英数記号混在8文字以上・使い回し禁止)を遵守している。 2-7,8 ※二要素認証または13文字以上の場合は定期変更不要	☐ はい ☐ いいえ	確認: / 目標: /	共通パスワードの禁止
	USBストレージ等の外部記録媒体や情報機器への接続制限を実施している。 2-9	☐ はい ☐ いいえ	確認: / 目標: /	外部メモリ接続制御・物理管理
	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	☐ はい ☐ いいえ	確認: / 目標: /	オンライン資格確認端末やサーバ
サーバ・NW 端末管理	サーバアクセスログ管理、不要サービス・ソフト停止、ネットワーク接続元制限。 2-11~13	☐ はい ☐ いいえ	確認: / 目標: /	保守業者ヒアリング・設定確認

大項目	確認項目(厚労省基準要件)	確認結果	確認日 / 目標日	備考・対策状況
インシデント 対応準備	組織内および外部機関(事業者、厚労省、警察等)への連絡体制図がある。 3-1	☐ はい ☐ いいえ	確認: / 目標: /	緊急連絡フロー表の掲示
	診療継続に必要な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	確認: / 目標: /	オフラインバックアップ等の確保
	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	確認: / 目標: /	紙カルテ移行手順・診療継続方針
規程類の整備	上記項目について具体的な実施方法を「情報セキュリティ運用管理規程」等に定めている。 4-1	☐ はい ☐ いいえ	確認: / 目標: /	院内規程の保管場所周知