経営管理者向け　サイバーセキュリティ対策チェックリスト

No	チェック項目	チェック欄
1	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	運用管理規程等において次の内容を定めているか ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合はその情報端末等の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	
3	経営者がサイバーセキュリティリスク(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃により損害を被るリスク）を経営リスクの1つとして認識しているか	
4	サイバー攻撃により医療情報が暗号化され、復元のための身代金を請求された医療機関等、公表されているサイバー攻撃の情報を定期的、必要時に確認しているか	
5	サイバーセキュリティ（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）にかかる監査を実施しているか	
6	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為や取組状況）を外部に公開しているか	
7	ウェブサイトの運営において、サーバやネットワーク機器、ウェブアプリケーションに対する脆弱性検査（診断）、監査を実施しているか	
8	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）の現状を調査しているか	
9	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）の現状に基づいて、医療機関で可能な対策を実施しているか	
10	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）を進めるための予算や人材を医療機関で確保しているか	
11	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）について医療機関内部で講じることが難しい場合、外部の組織への相談等を検討しているか	
12	不正防止の観点から、担当者間、部門間等で相互に情報管理に関して、運用状況の点検を実施し、相互牽制（各病棟間、外来部門、医事課事務部門間等）を働かせているか	
13	サイバーセキュリティに関する取組方針を常日頃から従業員や外部委託先等に伝えてコミュニケーションを取っているか	
14	法令上の守秘義務のある者以外の者を従業員として採用するにあたって雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施しているか	
15	従業者の退職後の個人情報保護規程を定めているか	
16	インシデント対応の専門チーム（CSIRT等）を設置しているか	
17	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めているか	
18	医療機関等において、コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合は、直ちに医療情報システムの保守会社等に連絡の上、医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断した場合には、厚生労働省医政局研究開発振興課医療情報技術推進室に連絡することに決めているか	

医療従事者・一般のシステム利用者向け　サイバーセキュリティ対策チェックリスト

No	チェック項目	チェック欄
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っているか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン（画面が他人から見えないようにするために、操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体を使用していないか又は業務上、外部媒体の使用が必要な場合は事前に申請し、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行う	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	