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

記入者	日付

NO	チェック項目	チェック欄（○or×）
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こと	
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	