薬局におけるサイバーセキュリティ対策チェックリスト

薬局確認用

薬局名（　　）

サイバーセキュリティを確保するための対策等が適切に実施されているかを点検するためのチェックリストです。
自己点検欄に、次の区分で該当する記号を記入してください。

（チェックリスト記入要領）
記号 摘要
○　適正に実施している。
×　不適：一部は実施しているが、不十分な場合を含む。
－　該当なし（２（２）及び２（３）で確認不要であるとき以外に使用することは不可。）

・×が付いた項目については、目標日を記入してください。
・「薬局確認用」は「事業者確認用」の結果を踏まえて、薬局全体の状況を報告するものであるため、医療情報システムが導入されている場合は、すべての項目に○か×を記入する必要があります。（２（２）及び２（３）で確認不要である場合を除く。）
・薬局が事業者と契約していなければ「事業者確認用」は不要です。
・各項目の考え方や確認方法については、「薬局におけるサイバーセキュリティ対策チェックリストマニュアル～薬局・事業者向け～」をご覧ください。

★以下項目はすべての項目で「○」が付くよう取り組んでください。
（※）事業者と契約していない場合には、２（２）及び２（３）の 記入 は 不要です。
★１回目の確認で「×」の場合、対応目標日を記入してください。

				確認日（R　．　．）		
	番号	チ　ェ　ッ　ク　項　目	自己点検1回目	目標日(例:R6.9.30)	自己点検2回目	備考・参考
医療情報システムの有無	医療情報システムを導入、運用している。（はい：○、いいえ：×）（「いいえ」の場合、以下のすべての項目は確認不要）					
1 体制構築	1	医療情報システム安全管理責任者を設置している。				
2 医療情報システムの管理・運用	医療情報システム全般について、以下を実施している。					
	2	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。				
	3	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事業者等に確認した。（事業者と契約していない場合は不要。）				
	4	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。（事業者と契約していない場合は不要。）				
	5	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている				
	6	退職者や使用していないアカウント等、不要なアカウントを削除または無効化している				
	7	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。				
	8	パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要				
	9	パスワードの使い回しを禁止している				
	10	USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。				
	11	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。				
	サーバについて、以下を実施している。					
	12	アクセスログを管理している。				
	13	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。				
	端末PCについて、以下を実施している。					
	14	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。				
	ネットワーク機器について、以下を実施している。					
	15	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。				
	16	接続元制限を実施している。				
3 インシデント発生に備えた対応	17	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省警察等）への連絡体制図がある。				
	18	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。				
	19	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。				
4 規定等の整備	20	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。				