

医療機関におけるサイバーセキュリティ対策チェックリスト 「サイバー攻撃リスク低減のための最低限の措置」編

医療機関確認

医療機関名 _____

※ このチェックリストは、医療機関等におけるサイバーセキュリティ対策の取組みについて（令和6年8月1日事務連絡 各都道府県等衛生主管部(局)宛厚生労働省医政局特定医薬品開発支援・医療情報担当参事官及び厚生労働省政策統括官付サイバーセキュリティ担当参事官室）により、特に迅速に対応すべき事項として示された「サイバー攻撃リスク低減のための最低限の措置」の内容を基に、岡山県が作成したものです。

※ 本チェックリストの項目について直ちに確認を行い、「いいえ」の項目については速やかに取り組むよう対応をお願いします。

※ 1回目の確認で「いいえ」の場合、実施可能な直近の対応目標日を記入してください。

※ 立入検査時、本チェックリストを確認します。

チェック項目	確認結果			備考	
	（日付）				
	1回目	目標日	2回目		
○パスワードを強固なものに変更し、使い回しをしない					
システム運用担当者は、VPN装置等のID・パスワードについて、強固なID・パスワード設定を行っている。	はい・いいえ (/)	(/)	はい・いいえ (/)		
複数の機器や外部サービス等で、同一のパスワードを設定していない。	はい・いいえ (/)	(/)	はい・いいえ (/)		
利用者認証に使用するパスワードについて、類推されやすいパスワードを使用しないよう、すべての利用者に対し周知を徹底している。	はい・いいえ (/)	(/)	はい・いいえ (/)		
○IoT 機器を含む情報資産の通信制御を確認する					
関係事業者と協力してすべてのネットワーク接続点を確認（閉域網と認識されているネットワークにおける接続点の有無の確認を含む）している。	はい・いいえ (/)	(/)	はい・いいえ (/)		
ネットワーク接続点へのアクセス制御を適切に実施している。	はい・いいえ (/)	(/)	はい・いいえ (/)		
各種システムや通信制御を行っている機器のログを記録・保存し、定期的にその内容をチェックして不正利用がないことを確認している。	はい・いいえ (/)	(/)	はい・いいえ (/)		
○ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する					
すべてのネットワーク機器のバージョンアップやパッチ適用、ファームウェアアップデートを適切な頻度で行っているか、事業者と連携して確認している。	はい・いいえ (/)	(/)	はい・いいえ (/)		
セキュリティ対策ソフトの稼働状況（最新の定義ファイルが適用されるようになっているか等）について確認している。	はい・いいえ (/)	(/)	はい・いいえ (/)		