別添１

令和７年度版
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

医療機関確認用

*立入検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	確認日	目標日	備考
1 体制構築	医療情報システム安全管理責任者を設置している。(1-①)	はい・いいえ (/)	(/)	
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。**			
	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 (/)	(/)	
	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。(2-②) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	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。(2-③) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	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(2-④)	はい・いいえ (/)	(/)	
	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。(2-⑤)	はい・いいえ (/)	(/)	
	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。(2-⑥)	はい・いいえ (/)	(/)	
	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(2-⑦)	はい・いいえ (/)	(/)	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (/)	(/)	
	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。 (2-⑨)	はい・いいえ (/)	(/)	
	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 (/)	(/)	
	サーバについて、以下を実施している。			
	アクセスログを管理している。(2-⑪)	はい・いいえ (/)	(/)	
	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。(2-⑫)	はい・いいえ (/)	(/)	
	端末PCについて、以下を実施している。			
	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。(2-⑫)	はい・いいえ (/)	(/)	
	ネットワーク機器について、以下を実施している。			
	接続元制限を実施している。(2-⑬)	はい・いいえ (/)	(/)	
3 インシデント発生に備えた対応	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。(3-①)	はい・いいえ (/)	(/)	
	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。(3-②)	はい・いいえ (/)	(/)	
	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 (/)	(/)	
4 規程類の整備	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。(4-①)	はい・いいえ (/)	(/)	

- 各項目の考え方や確認方法等については、「医療機関等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～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。

令和７年度
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

事業者確認用

*以下項目は令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	（日付） 確認日	（日付） 目標日	備考
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-①)	はい・いいえ （ / ）	（ / ）	
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。**			
	リモートメンテナンス（保守）している機器の有無を確認した。(2-②)	はい・いいえ （ / ）	（ / ）	
	医療機関に製造業者/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）を提出した。(2-③)	はい・いいえ （ / ）	（ / ）	
	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(2-④)	はい・いいえ （ / ）	（ / ）	
	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。(2-⑤)	はい・いいえ （ / ）	（ / ）	
	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。(2-⑥)	はい・いいえ （ / ）	（ / ）	
	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(2-⑦)	はい・いいえ （ / ）	（ / ）	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ （ / ）	（ / ）	
	USBストレージ等の外部接続機器や情報機器に対して接続を制限している。 (2-⑨)	はい・いいえ （ / ）	（ / ）	
	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 （ / ）	（ / ）	
	サーバについて、以下を実施している。			
	アクセスログを管理している。(2-⑪)	はい・いいえ （ / ）	（ / ）	
	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。(2-⑫)	はい・いいえ （ / ）	（ / ）	
	端末PCについて、以下を実施している。			
	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。(2-⑫)	はい・いいえ （ / ）	（ / ）	
	ネットワーク機器について、以下を実施している。			
	接続元制限を実施している。(2-⑬)	はい・いいえ （ / ）	（ / ）	

事業者名：

- 各項目の考え方や確認方法等については、「医療機関等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～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。