令和8年度版
医療機関・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

医療機関・薬局確認用

*立入検査時、本チェックリストを確認します。令和8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8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	①医療情報システム安全管理責任者を設置している。	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。**			
	①サーバ、端末、ネットワーク機器の台帳管理を行っている。	はい・いいえ (/)	(/)	
	②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。	はい・いいえ (/)	(/)	
	③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。	はい・いいえ (/)	(/)	
	④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	はい・いいえ (/)	(/)	
	⑤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。	はい・いいえ (/)	(/)	
	⑥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。	はい・いいえ (/)	(/)	
	⑦パスワードは英数字の混在した8桁以上としている。※二要素認証を採用するまでの期間は13桁以上としている	はい・いいえ (/)	(/)	
	⑧パスワードの使い回しを禁止している。	はい・いいえ (/)	(/)	
	⑨USB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。	はい・いいえ (/)	(/)	
	⑩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。	はい・いいえ (/)	(/)	
	端末について、以下を実施している。			
	⑪アプリケーションログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ (/)	(/)	
	サーバについて、以下を実施している。			
	⑫OSログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ (/)	(/)	
	⑬アクセスログを管理している。	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。			
	⑭接続元制限を実施している。	はい・いいえ (/)	(/)	
3 インシデント発生に備えた対応	①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。	はい・いいえ (/)	(/)	
	②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、バックアップを確保のうえ、復旧手順を確認している。	はい・いいえ (/)	(/)	
	③サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。	はい・いいえ (/)	(/)	
4 規程類の整備	①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。	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・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～医療機関・薬局・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8年度
医療機関・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

事業者確認用

＊以下項目は令和8年度中にすべての項目で「はい」または「対象外」にマルが付くよう取り組んでください。

・「はい」　：医療機関・薬局との保守契約範囲に含まれる項目であり、事業者側の責任で対応できていることを指します。
・「いいえ」：医療機関・薬局との保守契約範囲に含まれる項目であるが、事業者側が対応できていない項目となります。
　事業者としての令和8年度中の対応目標日を記入してください。
・「対象外」：医療機関・薬局との保守契約範囲外となり、当該項目の責任を医療機関・薬局が負います。
　医療機関・薬局に対して、責任分界の認識齟齬がないか、事業者側から必ず確認して下さい。

	チェック項目	（日付）		備考
		確認日	目標日	
1 体制構築	①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。	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。**			
	②リモートメンテナンス（保守）している機器の有無を医療機関等に伝えた。	はい・いいえ （　/　）	（　/　）	
	③医療機関等に製造業者/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。	はい・いいえ （　/　）	（　/　）	
	④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。	はい・いいえ・対象外 （　/　）	（　/　）	
	⑤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。	はい・いいえ・対象外 （　/　）	（　/　）	
	⑥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。	はい・いいえ・対象外 （　/　）	（　/　）	
	⑦パスワードは英数字の混在した8桁以上としている。 ※二要素認証を採用するまでの期間は13桁以上としている。	はい・いいえ （　/　）	（　/　）	
	⑧パスワードの使い回しを禁止している。	はい・いいえ （　/　）	（　/　）	
	⑨USB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。	はい・いいえ・対象外 （　/　）	（　/　）	
	⑩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。	はい・いいえ・対象外 （　/　）	（　/　）	
	端末について、以下を実施している。			
	⑪アプリケーションログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）	（　/　）	
	サーバについて、以下を実施している。			
	⑫OSログイン時の二要素認証を実装している。または令和９年度以降初回のシステム更改時に実装予定である。	はい・いいえ （　/　）	（　/　）	
	⑬アクセスログを管理している。	はい・いいえ・対象外 （　/　）	（　/　）	
	ネットワーク機器について、以下を実施している。			
	⑭接続元制限を実施している。	はい・いいえ・対象外 （　/　）	（　/　）	
3 インシデント発生に備えた対応	③サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。	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・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～医療機関・薬局・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。