

# 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

	チェック項目	確認結果 (日付)	備考
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。 (「いいえ」の場合、以下すべての項目は確認不要)	はい・いいえ ( / )	

## ○ 令和5年度中

\*以下項目は令和5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。

\*2(2)及び2(3)については、事業者と契約していない場合には、記入不要です。

\*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果 (日付)			備考
		1回目	目標日	2回目	
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 ( / )	( / )	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PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ ( / )	( / )	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 ( / )	( / )	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 ( / )	( / )	はい・いいえ ( / )	
	サーバについて、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	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している。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(6) アクセスログを管理している。	はい・いいえ ( / )	( / )	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。				
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
(8) 接続元制限を実施している。	はい・いいえ ( / )	( / )	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 ( / )	( / )	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。

● 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

# 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

## ○ 参考項目（令和6年度中）

\*以下項目について、令和6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。

	チェック項目	確認結果 (日付)			備考
		1回目	目標日	2回目	
2 医療情報システム の管理・運用	サーバについて、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(9) 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 ( / )	( / )	はい・いいえ ( / )	
	端末 PC について、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	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している。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
(9) 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 ( / )	( / )	はい・いいえ ( / )		
3 インシデント発生に備えた対応	(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、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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(3) サイバー攻撃を想定した事業継続計画 (BCP) を策定、又は令和6年度中に策定予定である。	はい・いいえ ( / )	( / )	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。

# 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

## ○ 令和5年度中

\*以下項目は令和5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。

\*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果 (日付)			備考
		1回目	目標日	2回目	
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 ( / )	( / )	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確認した。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(3) 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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	サーバについて、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	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している。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(6) アクセスログを管理している。	はい・いいえ ( / )	( / )	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。				
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
(8) 接続元制限を実施している。	はい・いいえ ( / )	( / )	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。

# 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

## ○ 参考項目（令和6年度中）

\*以下項目について、令和6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。

	チェック項目	確認結果 (日付)			備考
		1回目	目標日	2回目	
2 医療情報システム の管理・運用	サーバについて、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(9) 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 ( / )	( / )	はい・いいえ ( / )	
	端末 PC について、以下を実施している。				
	(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。	はい・いいえ ( / )	( / )	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している。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(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。	はい・いいえ ( / )	( / )	はい・いいえ ( / )	
	(9) 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 ( / )	( / )	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。