医政参発０６０９第１号
令和５年６月９日

各 都道府県知事
保健所設置市長
特別区長 殿

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
（　公　印　省　略　）

「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」及び
「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～」について

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

医療機関のサイバーセキュリティ対策について、「医療法施行規則の一部を改正する省令」（令和５年３月 10 日付け産情発 0310 第２号厚生労働省大臣官房医薬産業振興・医療情報審議官通知）の「第４　留意事項」において「安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省において別途チェックリストを作成し、後日通知する。」とお示ししたところです。

今般、第 16 回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和５年３月 23 日開催）での議論を踏まえ、別添１のとおり「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」（以下「チェックリスト」という。）を作成しました。また、チェックリストを分かりやすく解説した「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、別添２のとおり作成しました。さらに、別添３のとおり、医療法（昭和 23 年法律第 205 号）第 25 条第１項及び第３項の規定に基づく検査の際に確認する事項等を示した「医療機関におけるサイバーセキュリティ確保に係る立入検査の手引き～立入検査担当者向け～」を作成しました。

貴職におかれては、本通知について、御了知の上、関係団体、関係機関等に周知徹底を図るとともに、その実施に遺漏なきよう御配慮願います。

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

	チェック項目	確認結果 （日付）
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）		
		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 （　/　）		

- 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）		
		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）		
		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）		
		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。