

周 知 文 書 等 の ご 案 内

令和 7 年 5 月 27 日

○ 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」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

標記の件につきまして、日本医師会より鹿児島県医師会を通じて周知依頼がありました。

本件は、「令和 6 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」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」につきまして、厚労省よりチェックリスト項目の見直し、および医療機関・事業者向けと薬局向けに分かれていたマニュアルの統合を行い、令和 7 年度版として改訂した旨、日本医師会を通じて周知依頼がありました。

なお、日本医師会では今回の改訂を受け、日医メンバーズルーム掲載の「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の実践ガイド」の更新を行い、別途示される予定とのことです。

つきましては、内容を良くご確認頂き、ご対応頂きますようお願い申し上げます。

なお、この文書は、医師会ホームページ（<http://www.izumigun-med.or.jp/>）の会員専用ページにも掲載しております。

会員専用ページの ID とパスワードは、 [ID : izumigun PW : 1818]

FAX 送信元：出水郡医師会 TEL63-0646 FAX62-6336

E-mail : info@izumigun-med.or.jp

日医発第 298 号（情シ）
令和 7 年 5 月 19 日

都道府県医師会長 殿

公益社団法人 日本医師会
会長 松本 吉郎
（公印省略）

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」
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

平素より本会会務の運営に特段のご理解・ご支援を賜り厚く御礼申し上げます。

先般、令和 6 年 5 月 17 日付 日医発第 361 号（情シ）「令和 6 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」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」にて、医療機関で取り組んでいただきたいチェックリストについてお示ししていたところです。

今般、実際に医療機関で起きたサイバー攻撃被害事例を受けて、チェックリスト項目の見直し行われ、医療機関・事業者向けと薬局向けに分かれていたマニュアルの統合が実施されました。これらをうけて、令和 7 年度版として改訂され、厚生労働省より本会宛にその周知依頼がありました。医療機関等への立入検査時にこのチェックリストを確認することになりますので、ご承知おきください。

つきましては、貴会におかれましても、本件についてご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、ご高配を賜りますようお願い申し上げます。

また、日本医師会サイバーセキュリティ支援制度では、上記に対応するため「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の実践ガイド」を日医メンバーズルーム内に掲載しておりますが、今回の改訂を受け、更新を予定しております。時期は未定ですが、更新できましたら、改めてお知らせいたします。

同制度では、「日本医師会セキュリティガイドライン相談窓口」も開設しておりますので、上記チェックリストにご対応いただく際に、不明点等がございましたら、是非ご活用ください。

以上

【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の実践ガイドおよびセミナー動画】

●概要

厚生労働省が策定している「医療情報システムの安全管理に関するガイドライン」とそのガイドラインから必要最低限の項目を抽出した「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」をよりわかりやすく解説した資料および動画です。

●公開場所

「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の実践ガイドおよびセミナー動画」は日本医師会メンバーズルーム内専用ページにて公開しております。

https://www.med.or.jp/japanese/members/info/cyber_shien.html

【日本医師会セキュリティガイドライン相談窓口】

TEL：0120-339-199 平日 9 時～18 時（土日、祝日、年末年始は休業）

※詳細は日本医師会メンバーズルーム内専用ページをご確認ください。

https://www.med.or.jp/japanese/members/info/cyber_shien.html

【別添資料】

- ・医政参発 0514 第 2 号：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」及び「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～」について
- ・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」
- ・別添 2：令和 7 年度版「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～医療機関等・事業者向け～」

医政参発0514第2号
令和7年5月14日

公益社団法人 日本医師会会長 殿

厚生労働省医政局参事官
(医療情報担当)
(公 印 省 略)

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」及び
「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
～医療機関等・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。

医療機関等のサイバーセキュリティ対策において優先的に取り組むべき事項については、令和6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」及び令和6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マニュアル～医療機関・事業者向け～」(令和6年5月13日付け医政参発0513第7号、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通知別添。以下「チェックリスト等」という。)によりお示ししてきたところです。

今般、チェックリスト等の一部項目について見直しや医療機関・事業者向けと薬局向けに分かれていたサイバーセキュリティ対策チェックリストマニュアルの統合を行い、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」及び令和7年度版「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～医療機関等・事業者向け～」として、別添1及び2のとおり改訂しました。

医療機関等への立入検査時にこのチェックリストを確認いたしますのでご承知おきください。

貴職におかれては、内容を御了知の上、貴下団体会員等に周知徹底を図るよう、お願いいたします。

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

*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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
		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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		
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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)		

- 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。
- 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)		備考
		確認日	目標日	
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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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 (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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。(2-⑬)	はい・いいえ (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	
	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。(2-⑭)	はい・いいえ (<input type="checkbox"/> / <input type="checkbox"/>)	(<input type="checkbox"/> / <input type="checkbox"/>)	

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。
- 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。