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～

本マニュアルは、「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」または「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」（以下「チェックリスト」という。）をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

○　医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関等が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○　医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関等が優先的に取り組むべき事項をチェックリストにまとめました。

本マニュアルは、医療機関等におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○　医療機関等および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

目次

Ⅰ　チェックリストの使い方

1．チェックリストの用意

○　チェックリストを使用するにあたり、医療機関等においては「医療機関確認用」または「薬局確認用」、事業者においては「事業者確認用」を用いて確認してください。事業者と契約していない*医療機関等においては「事業者確認用」による確認は不要です。

＊以下、「事業者と契約していない」とは製品購入の売買契約のみで、運用又は管理・保守に関する契約等がない場合を指します。

○　医療機関等は事業者に「事業者確認用」を送付し、対策の状況を確認するよう求めてください。複数の医療情報システムを利用している場合、システムを提供している事業者ごとに確認を求めてください。なお、事業者に対しても別途本取組について周知を行っていきます。

2．チェックリストの記入方法

○　各項目の実施状況を確認し、「はい」または「いいえ」にマルをつけて、確認した日付を記入してください。もし「いいえ」の場合は、対策の実施にかかる令和７年度中の目標日を記入するようにしてください。チェックリストは紙媒体または電子媒体のどちらを使用して頂いても構いません。

○　医療機関等は「医療機関確認用」「薬局確認用」について令和７年度中に全てのチェック項目で「はい」にマルがつくように、事業者と連携して取り組むようにしてください。

（※）　事業者と契約していない場合には、２-②及び２-③の記入は不要です。

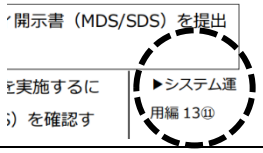
○　複数の事業者と契約している場合、契約内容によっては「事業者確認用」の一部の項目の確認が不要になることもあります。「事業者確認用」には、事業者名を記入する欄を設けています。医療機関等は各事業者から回収してください。

3．その他

○　チェックリストの確認結果は随時参照して、日頃の対策の実施に役立ててください。

○　少なくとも年に１回は、チェックリストを用いた点検を実施してください。

○　医療機関等と直接契約関係にない事業者においては、「事業者確認用」の作成は不要です。

凡例		本マニュアルの「Ⅱ各チェック項目の解説」では、それぞれのチェック項目に紐づく「医療情報システムの安全管理に関するガイドライン第 6.0 版」の該当箇所を右側に「▶」で示しています。

～立入検査時、チェックリストを確認します～

医療法第 25 条第１項に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。また、薬機法に基づく立入検査では、薬局においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

立入検査では「医療機関確認用」または「薬局確認用」、「事業者確認用」の全ての項目について、確認日と回答等が記入されていることを確認します（※）。このうち、２-①の台帳、３-①の連絡体制図、３-③の事業継続計画（BCP）、４の規程類は現物を確認しますので、立入検査までに作成してください。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関等は各事業者からチェックリストを回収しておきましょう。

（※）事業者と契約していない場合には、「医療機関確認用」または「薬局確認用」２-②及び２-③についての確認は求められません。

～参考資料～

◇[特集]　小規模医療機関等向けガイダンス

診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する人材が十分に確保できないというケースも多くみられます。本ガイダンスは、小規模医療機関等において、ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示しています。

◇[特集]　医療機関等におけるサイバーセキュリティ

本ガイダンスはサイバーセキュリティに関係する部分を要約し、サイバー攻撃の典型例など具体的な事例などもまとめています。チェックリストを用いた確認と併せて一読いただき、ぜひサイバーセキュリティに対する理解をさらに深めてください。

※　厚生労働省 HP「医療情報システムの安全管理に関するガイドライン第 6.0 版　特集」に掲載しています。

Ⅱ　各チェック項目の解説

1　体制構築　　【医療機関等確認用・事業者確認用】

①　医療情報システム安全管理責任者を設置している。

▶経営管理編
3.1.2②
3.2

医療機関において、医療機関の経営層は安全管理を直接実行する医療情報システム安全管理責任者を設置する必要があります。医療情報システム安全管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。情報セキュリティ対策の実効性を確保するために、経営層が医療情報システム安全管理責任者に就くことが望ましいですが、医療機関の規模・組織等によっては企画管理者が兼務することもあります。

また、薬局においては、医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う「企画管理者」や医療情報システムの安全管理を直接実行する「医療情報システム安全管理責任者」（以下併せて「システム管理責任者」という。）や、医療情報システムの実装・運用を担う「システム運用担当者」を設置する必要があります。システム管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。なお、小規模な薬局の場合には、薬局の管理者が、システム管理責任者やシステム運用担当者を兼任する場合があると考えられます。

また、事業者においても医療情報システム等の提供に係る管理責任者を設置する必要があります。

（用語の解説）

企画管理者：医療機関等において医療情報システムの安全管理の実務を担う担当者を指します。

2　医療情報システムの管理・運用　【医療機関等確認用・事業者確認用】

（用語の解説）

医療情報システム全般：サーバ、端末 PC、ネットワーク機器を指します。

サーバ：電子カルテサーバやレセコンサーバ等、ネットワーク上で情報やサービスを提供するコンピュータを指します。

ネットワーク機器：無線 LAN やルータ等を指します。

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。（医療情報システム全般）

▶経営管理編 1.2.1 〈管理責任〉②
▶企画管理編 9.1

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者等は医療機関等で所有する医療情報システムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。また、医療機関等の経営層等は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

（用語の解説）

情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。

（補足）

サーバ、端末 PC、ネットワーク機器のうち、自身の医療機関等で保有するすべての医療情報システムについて台帳管理を行っていれば、「はい」にマルをつけてください。

●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

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に確認した。
（医療情報システム全般）

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、企画管理者等に報告する必要があります。そのため、システム運用担当者は、2-①で整理した情報をもとにリモートメンテナンスを利用している機器の有無を事業者に確認し、企画管理者等へ報告してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

システム運用担当者：医療機関等において医療情報システムの実装・運用を担う担当者を指します。

▶企画管理編 9.1
▶システム運用編 10.1

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。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。企画管理者等は事業者へ当該医療情報システムに関するMDS/SDS の有無を確認し、事業者から回収してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security：医療情報セキュリティ開示書（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の略称です。各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）を JIRA(一般社団法人 日本画像医療システム工業会)/JAHIS で定めた物で、厚生労働省標準規格として認定されています。製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、医療機関等側において必要な対策の理解を容易にすることなどの用途に用いられることが想定されています。

▶概説編 4.5

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　（医療情報システム全般）

▶企画管理編
13④
13.1.3

医療情報システムの利用権限は、医療従事者の資格や医療機関等内の権限規程に応じて設定することが重要です。企画管理者等は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。

特に管理者権限を与えるアカウントは最低限のユーザに付与することを徹底してください。これはサイバー攻撃を受けた際の水平展開を防ぐためです。

利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、所属部署・氏名・ユーザ ID・権限等が想定されます。

●利用者 ID 台帳の例

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可
.	.	.	.	.	.	.	.	.

No.	利用者属性	性	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年３月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

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をしている。
（医療情報システム全般）

▶企画管理編
13⑦

企画管理者等は２-④で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。長期間使用されていない等の不要な ID は不正アクセスに利用されるリスクがありますので、適宜削除や無効化をする等の対応をしてください。