令和６年度版

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

～薬局・事業者向け～

本マニュアルは、「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（医療に関する患者情報（個人識別情報）を 含む情報）の流出や、不正な利用を事前に防ぐことが重要です。令和５年４月には、改正薬機法施行規則が施行され、薬局の管理者が遵守すべき事項として、薬局の管理者はその薬局のサイバーセキュリティの確保について必要な措置を講じることが追加されました。

○　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、薬局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ています。

本マニュアルは、薬局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。

○　薬局においても調剤レセプトコンピューターや電子薬歴システム等の医療情報システムが導入されており、法令やガイドラインに基づき、適切な管理の下でこれらのシステムを利用することが求められています。薬局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 3

Ⅱ　各チェック項目の解説 5

医療情報システムの有無　【薬局確認用】 5

医療情報システムを導入、運用している。 5

1　体制構築　【薬局確認用・事業者確認用】 5

（1）医療情報システム安全管理責任者を設置している。 5

2　医療情報システムの管理・運用　【薬局確認用・事業者確認用】 6

（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） 6

（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） 7

（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） 7

（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。
（サーバ、端末 PC） 8

（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。
（サーバ、端末 PC） 8

（6）アクセスログを管理している。（サーバ） 9

（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。
（医療情報システム全般） 10

（8）接続元制限を実施している。（ネットワーク） 11

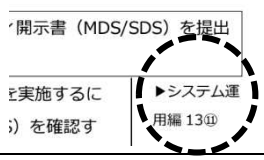
（9）バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。
（サーバ、端末 PC） 11

3　インシデント発生に備えた対応　【薬局確認用】 12

（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）の連絡体制図がある。 12

（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。 13

（3）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。 13

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。

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、薬局においては「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薬局においては「事業者確認用」による確認は不要です。

○　薬局は事業者に「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１回目の確認で「いいえ」の場合は、対策の実施にかかる令和６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で使用して頂いても構いません。

○　薬局は「薬局確認用」について令和６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。薬局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。

○　薬局と直接契約関係にない事業者においては、「事業者確認用」の提出は不要です。

～立入検査時、チェックリストを確認します～

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「薬局確認用」、「事業者確認用」の全ての項目について、１回目の確認の日付と回答等が記入されていることを確認します（※）。このうち、３（１）の連絡体制図は現物を確認します。

チェックリストを用いて、日頃からサイバーセキュリティ対策の状況を確認することが重要です。

なお、薬局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、「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。

Ⅱ　各チェック項目の解説

医療情報システムの有無　　【薬局確認用】

医療情報システムを導入、運用している。

本チェックリストが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定します（例：レセコン、電子薬歴システム等）。これには、事業者により提供されるシステムだけでなく、薬局において自ら開発・構築されたシステムが含まれます。

本項目の「いいえ」にマルがつく場合、以下すべての項目は確認不要です。

▶概説編 2.3

1　体制構築　　【薬局確認用・事業者確認用】

（１）　医療情報システム安全管理責任者等を設置している。

薬局において、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。

▶経営管理編
3.1.2②
3.2

2　医療情報システムの管理・運用　【薬局確認用・事業者確認用】

各項目の実施者について、例えば（１）はシステム管理責任者が実施するとしているが、記載は例示であり、各薬局の運用体制により、異なる場合も想定される。

（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：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、システム管理責任者は薬局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、薬局の開設者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、自身の薬局で保有する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	主な利用者属性	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	薬剤師・事務職員・システム管理者	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	薬剤師・事務職員・システム管理者	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	薬剤師・システム管理者	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	薬剤師・システム管理者	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、システム管理責任者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、システム管理責任者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。

▶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。システム管理責任者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、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） 利用者の属性等に応じた情報区分毎のアクセス利用権限を設定している。
（サーバ、端末 PC）

医療情報システムの利用権限は、薬局内の権限規程等に応じて設定することが重要です。システム管理責任者は情報の種別、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。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、利用者属性・氏名・ユーザーID・権限等が想定されます。

▶企画管理編 13④ 13.1.3

●利用者 ID 台帳の例

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している。
（サーバ、端末 PC）

システム管理責任者は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、速やかに削除してください。

▶企画管理編 13⑦

（６） アクセスログを管理している。（サーバ）

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに、システム管理責任者はそのログを定期的に確認してください。例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録することが必要です。

（補足）

アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を併せて講じてください。

▶経営管理編 4.2
▶企画管理編 5.3
▶システム運用編 17①②

●アクセスログの例

ユーザーID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16 8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16 8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16 8:31:00	入力メニュー	起動
abc@def	abcdef	2023/5/16 8:32:00	入力メニュー	カルテ入力
abc@def	abcdef	2023/5/17 12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17 8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 8:45:00	管理メニュー	ログオフ
・	・	・	・	・

（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。
（医療情報システム全般）

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが挙げられます。

（用語の解説）

パターンファイル：ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。

（補足）

古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

▶システム運用編
8③
8.1
8.2
13.2

（８） 接続元制限を実施している。（ネットワーク）

外部ネットワークに接続する際には、ネットワークや機器等を適切に選定し、監視を行うことが必要です。特に、無線 LAN を使用する際は不正アクセス対策として適切な利用者以外に無線 LAN を利用されないようにすることが重要です。システム運用担当者は、例えば、ネットワーク機器に接続出来る MAC アドレスを限定すること等、不正アクセス対策を実施してください。

（用語の解説）

MAC アドレス：Media Access Control アドレスの略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号。インターネットでは IP アドレス以外にも MAC アドレスを使用して通信を行っています。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、通常であれば、同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはありません。

（補足）

MAC アドレスによるアクセス制限の効果は限定的であることに留意する必要がありますので、追加の対策はガイドラインや事業者とも確認をお願いします。

▶システム運用編 13⑪

（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。（サーバ、端末 PC）

不正ソフトウェアは電子メール、ネットワーク等の様々な経路を利用して医療情報システム内に侵入する可能性があります。システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合はシステム管理責任者に相談の上、対策を講じてください。

▶システム運用編 8.1

3　インシデント発生に備えた対応　　【薬局確認用】

（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）の連絡体制図がある。

▶経営管理編
3.4.2①
3.4.3①
▶企画管理編
12.3

薬局の開設者は情報セキュリティインシデント発生に備え、事業者や外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、システム管理責任者に指示することが重要です。システム管理責任者はサイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成して下さい。連絡体制図には薬局内の連絡先や会社本部の連絡先等に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定されます。

このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

立入検査時は、連絡体制図が作成されていることを確認します。

（用語の解説）

CSIRT: 「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるイシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

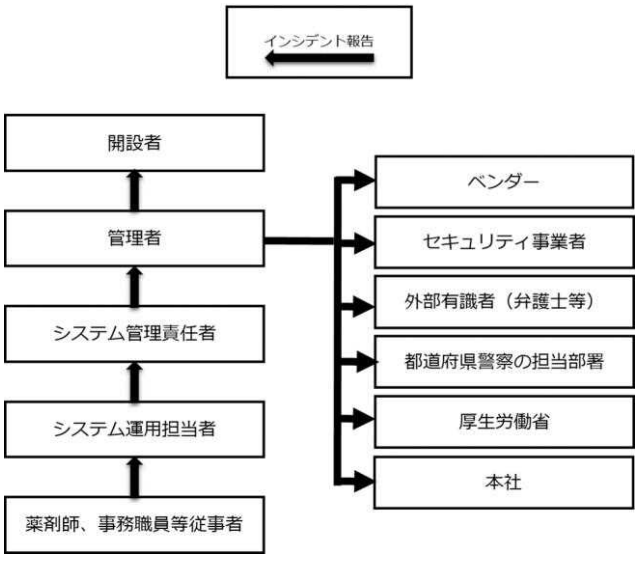
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

サイバー攻撃を受けた疑いがある場合は、下記の厚生労働省の連絡先に御連絡ください。なお、いたずら防止のため、184 発信、公衆電話発信は受信不可とします。

【連絡先】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室　03-6812-7837

●連絡体制図の例



（２）インシデント発生時に調剤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。

稼働が損なわれた医療情報システムを速やかに復旧できるよう、情報システムやデータ等のバックアップを適切に確保し、その復旧手順を整備・確認しておくことが求められます。システム管理責任者はバックアップを確保する際、重要なファイルについては、不正ソフトウェアの混入による影響が波及しないよう複数の方式で世代管理するよう設計し、システム運用担当者は手順に従いバックアップを確保してください。復旧手順の整備については、例えば、BCP に復旧手順を定めるなどの方法が挙げられます。

（用語の解説）

世代管理：バックアップの一種で、最新データだけでなく、それ以前のデータもバックアップする方法を指します。例えば、３世代以上で管理する場合、日次でバックアップを行うならば、「3 世代以上」とは「３日以上」のバックアップを確保することになります。

（補足）

３世代目以降のバックアップはオフライン（物理的あるいは論理的に書き込み不可の状態）にする等の対策が望ましいです。

▶経営管理編
3.4.1
▶企画管理編
11.2
▶システム運用編
11.1
12.2
18.1

（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。

薬局の開設者はシステム管理責任者と連携して非常時における業務継続の可否の判断基準や継続する業務選定等の意思決定プロセスを検討し、サイバー攻撃を想定した BCP 等を整備することとしています。この BCP を整備しておくことにより、万がーサイバー攻撃を受けても重要業務が中断しない、または中断しても短い期間で再開することが期待できます。

▶経営管理編
3.4.1
▶企画管理編
11.1

～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。