令和８度版

医療機関・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

～医療機関・薬局・事業者向け～

本マニュアルは、「医療機関・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・薬局（以下「医療機関等」という。）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。

○　医療機関等及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
1　体制構築　【医療機関・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　【医療機関・薬局確認用　事業者確認用】 6
① 《医療機関・薬局確認用》サーバ、端末、ネットワーク機器の台帳管理を行っている。 6
② 《医療機関・薬局確認用》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。 7
③ 《医療機関・薬局確認用》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。 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。 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又は無効化をしている。 8
⑥ 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。 9
⑦ パスワードは英数字の混在した８文字以上としている。 10
⑧ パスワードの使い回しを禁止している。（医療情報システム全般） 11
⑨ 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。 11
⑩ 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） 12
⑪ アプリケーションログイン時の二要素認証を実装している。 12
⑫ OS ログイン時の二要素認証を実装している。 13
⑬ アクセスログを管理している。（サーバ） 14
⑭ 接続元制限を実施している。（ネットワーク機器） 15
3　インシデント発生に備えた対応　【医療機関・薬局確認用　事業者確認用】 16
① 《医療機関・薬局確認用》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。 16
② 《医療機関・薬局確認用》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。 17
③ サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。 17
4　規程類の整備　【医療機関・薬局確認用】 18
①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。 18

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・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*医療情報システムにおいては「事業者確認用」による確認は不要です。ただし、この場合の医療情報システムのセキュリティアップデートなどの責任は医療機関等が負います。

＊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」又は「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８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又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・薬局確認用」について令和８年度中にすべ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。

○　システムの機能や契約内容によっては「事業者確認用」の一部の項目が、「対象外」となることがあります。「対象外」の場合には医療機関等側が当該項目の責任を負います。事業者が医療機関等側に責任分界の認識齟齬がないか確認してください。「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。

・「はい」：医療機関等との保守契約範囲に含まれる項目であり、事業者側の責任で対応できていることを指します。

・「いいえ」：医療機関等との保守契約範囲に含まれる項目であるが、事業者側が対応できていない項目となります。

事業者としての令和８年度中の対応目標日を記入してください。

・「対象外」：医療機関等との保守契約範囲外となり、当該項目の責任を医療機関等が負います。

医療機関等に対して、責任分界の認識齟齬がないか、事業者側から必ず確認して下さい。

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。

～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、診療所及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・薬局確認用」、「事業者確認用」のすべての項目について、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）、４-①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・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。ただし、その場合の医療情報システムの保守管理について医療機関等が責任を負っていることとなりますのでご留意下さい。

Ⅱ　各チェック項目の解説

1　体制構築　　【医療機関・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を設置している。

医療機関等において、医療機関等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、医療機関等の規模・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、医療情報システム安全管理責任者は情報セキュリティマネジメント試験の合格や、情報処理安全確保支援士の資格を有していることが望ましいです。

なお、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。

▶経営管理編
3.1.2②
3.2

2　医療情報システムの管理・運用　【医療機関・薬局確認用　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、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 《医療機関・薬局確認用》サーバ、端末、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）

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。

▶経営管理編 1.2.1 〈管理責任〉②
▶企画管理編 9.1

（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、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 《医療機関・薬局確認用》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。
《事業者確認用》リモートメンテナンス（保守）している機器の有無を医療機関等に伝えた。（医療情報システム全般）

リモートメンテナンス（保守）に用いる外部接続点からのサイバー攻撃が相次いでいます。これは医療機関等側がリモートメンテナンス用の外部接続点を把握しきれていないことが大きな要因のひとつです。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、医療情報システム安全管理責任等へ報告してください。

リモートメンテナンスを受託している事業者は医療機関等に対して、事業者確認用チェックリストを医療機関等に提出する際など、定期的に外部接続点の存在を医療機関等に通知してください。

▶企画管理編 9.1
▶システム運用編 10.1

（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。

③ 《医療機関・薬局確認用》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。
《事業者確認用》医療機関等に製造業者/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。（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及びリスク管理を実施するに当たっては、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。ただし、その場合すべての医療情報システムの保守管理について医療機関等が責任を負っていることとなりますのでご留意下さい。

▶概説編 4.5

（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。

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）

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。

▶企画管理編
13④
13.1.3

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。すべてのユーザに管理者権限が付与されていることで、ウイルス対策ソフトを無効化されるなどして、被害が拡大した事例が多発しています。

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又は無効化をしている。
（医療情報システム全般）

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。

▶企画管理編
13⑦

⑥　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）

▶システム運用編
8③
8.1
8.2
13.2

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、すべ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。

なお、医療情報システムを、今後新規導入又は更新するに際しては、保守契約の見直しや運用管理規程の変更により、セキュリティパッチを定期的に適用できる等適切な安全管理体制の構築に努めることが重要です。その際、事業者等との契約時の取り決めについては、参考資料として「医療情報システムの契約における当事者間の役割分担に関する確認表」（※）が挙げられます。

テスト環境などを用意して上記の作業を行い、実際に稼働している運用環境に影響が生じないようにすることが重要ですが、予算や運用上の制約でテスト環境の用意が難しい場合は、運用環境全体への影響が最小限となるよう、例えば影響の少ないセグメントから順にパッチを適用し、稼働を確認する等の対応が考えられます。

（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。

※医療情報システムの契約における当事者間の役割分担等に関する確認表　（METI/経済産業省）

⑦　パスワードは英数字の混在した８文字以上としている。
※二要素認証を採用するまでの期間は 13 桁以上としている　（医療情報システム全般）

単純なパスワードを利用していることで、サイバー攻撃を受ける被害が相次いでいます。情報機器に対して出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避ける等の対策を実施することが求められます（※）。

端末のログインパスワードのみならず、サーバやネットワーク機器のパスワードが推定しやすいものであると、サイバー攻撃の起点となります。サーバ、ネットワーク機器のパスワードを事業者が管理している場合、医療機関等は事業者確認用チェックリストを用いて、事業者の設定、運用しているパスワードがガイドラインの要件を満たすものであるかを確認してください。

この際、事業者側は各医療機関等のパスワードのリストについて、漏洩リスクを最小限とする様、厳重に管理する必要があります。

医療機関等の端末においても、ユーザ向けログインパスワードをモニターに付箋で貼る等の管理は絶対に避けなければなりません。

※強固なパスワード
・英数字混在させた 13 桁以上の推定困難な文字列
・二要素以上の認証の場合、英数字を混在させた８文字以上の推定困難な文字列

▶システム運用編
8.⑤

⑧　パスワードの使い回しを禁止している。（医療情報システム全般）

▶システム運用編 8.⑤

パスワードの使い回しは漏えいリスクを高め、一度の漏えいにより被害範囲が拡大するため、複数の機器や外部サービス等で、同一のパスワードを設定しないことが必要です。

事業者においては、事業者内及び、医療機関等に設置したサーバ、ネットワーク機器等について、パスワードの使い回しが行われていないか確認してください。

事業者が顧客となるすべての医療機関等に対して同じパスワードを使い回し、サイバー攻撃を受けた事案が報告されています。医療機関等は、事業者確認用チェックリストを通して、事業者がパスワードを使い回していないことを宣言させてください。

〈危険なパスワード使い回し例〉

- 施設内のサーバ、ネットワーク機器等に同一のパスワードを用いている
- 事業者が契約している複数施設に対して同一のパスワードを用いて管理している

⑨　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。（医療情報システム全般）

▶企画管理編 8.2.2
▶システム運用編 8.①

記録媒体や情報機器等の利用は、持ち出し先での紛失や盗難のほか、医療情報システムの端末やサーバに USB ストレージ経由での不正ソフトウェア混入が想定されます。

他の医療情報システムや医療機器等にマルウェア感染が広がる事を防ぐべく、USB ストレージ等の外部接続機器に対して接続の制限を行う必要があります。業務の必要性に応じて外部接続機器を利用する場合には、記録媒体及び記録機器の保管及び取扱いについて適切に行う必要があります。

・医療情報の持ち出しが可能となる記録媒体や情報機器等を限定する（※）。
・医療情報の持ち出しに対する手続等の運用管理規程を策定する。
・記録媒体・情報機器等を医療機関等に持ち帰った場合のそれらの確認に関する手続等の運用管理規程を策定する。

等を行うことが求められます。

※例えば病院等の情報システム部門が管理する特定の記録媒体以外の読み込みを不能とし、利用前の記録媒体へのウイルススキャンや利用後の初期化を行う等の対策が想定されます。

事業者においては、医療機関等からの依頼に基づいて USB 等の接続制限を行っている、又は医療情報システムがその機能を有するか医療機関等への情報提供を行ってください。

⑩ 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）

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企画管理者等に相談の上、対策を講じてください。

▶システム運用編 8.1

⑪ アプリケーションログイン時の二要素認証を実装している。
又は令和９年度以降初回のシステム更改時に実装予定である（端末）

ガイドラインでは令和３年１月に発出された 5.1 版以降すべての版において、令和９年度時点で稼働していることが想定される医療情報システムを、新規導入又は更新するに際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うことを求めています。二要素認証の導入・改修に当たっては、一定程度の費用が見込まれますので計画的なシステム更新を推奨します。

端末においては、アプリケーションログイン時の二要素認証が必要となります。

医療機器に対する二要素認証の導入については、ガイドライン第 7.0 版への改定時には改変が見送られました。このため、本マニュアル公開時点で医療機器に対して二要素認証の実装、実装を予定していることを必須とするものではありません。一方で、今後医療機器についても二要素認証が求められていく方向性に変わりはないため、二要素認証を採用している医療機器を積極的に採用していくことを推奨します。また、次期ガイドライン改定で検討されることが示唆されており、最新のガイドラインの内容に留意して対応してください。

▶システム運用編 14.⑤ 14.1.1

⑫　OS ログイン時の二要素認証を実装している。
　　又は令和９年度以降の初回システム更改時に実装予定である。（サーバ）

ガイドラインでは令和 3 年 1 月に発出された 5.1 版以降すべての版において、令和 9 年度時点で稼働していることが想定される医療情報システムを、新規導入又は更新するに際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うことを求めています。二要素認証の導入・改修に当たっては、一定程度の費用が見込まれますので計画的なシステム更新を推奨します。

サーバにおいては、医療情報システムにおけるサーバの OS にログインする際の認証技術実証を指します。

なお、セキュリティ・デバイスの破損等を想定し、緊急時の代替手段によるバイパス等、一時的なアクセスルールを用意することが重要です。また、バイパス利用時にはシステム及び利用者を適切に管理できる体制を整えておくことが求められます。

●二要素認証の採用例（記憶・生体情報・物理媒体の２種類を組み合わせたもの）
①パスワード＋指紋認証　②IC カード＋パスワード　③IC カード＋指紋認証

▶システム運用編
14.⑤
14.1.1

●サーバ二要素認証の「みなし措置」

クライアント端末のアプリケーションログイン時の二要素認証の実装は普及しつつありますが、サーバ OS ログイン時の二要素認証については、導入のために大規模な院内のネットワークやシステムの再構築が必要となる場合があります。このため、サーバ OS については以下①②いずれか、又はそれと同等以上の措置(※)が施されていれば、二要素認証を実装できているものとみなすことができます。

※同等以上の措置とは、例えば医療法に基づく立入検査の際に同等性を検査職員に対して説明できることなどが想定される。

▶システム運用編
14.1.1

① 以下 2 つを満たすもの
・医療情報システムのサーバ群（以下、サーバ群と呼ぶ）へのアクセスを別ドメインに設置された踏み台端末からの RDP や SSH 等による接続のみに限定する。
・踏み台端末の OS ログイン時に二要素認証を実装する。

② 以下 3 つを満たすもの
・サーバ群へのアクセスを、別ドメインに設置された踏み台端末からの RDP、SSH 等による接続に限定する。
・踏み台端末には EDR 機能を具備し、運用上想定されない振る舞いを検知可能とする。
（必ずしも EDR 製品を要せず、例えば Windows 標準機能等によって振る舞い検知が可能であればよい。）
・医療機関等の外部からの接続は VPN を経由し、踏み台端末への RDP、SSH 等による接続に限定する。

上記措置を講じる際には、以下 3 つが適用されていることが前提となります。これらが満たされない場合、十分な措置とは見なされません。

・外部から踏み台端末にログインするユーザに管理者権限を与えない
・十分な OS のセキュリティアップデート
・医療情報システムサーバ群と踏み台端末で共通のパスワードを利用しない

⑬　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、企画管理者等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。

アクセスログは立入検査の際に直接確認する可能性があります。

（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。

●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
・	・	・	・	・

▶経営管理編 4.2
▶企画管理編 5.3
▶システム運用編 17①②

⑭　接続元制限を実施している。（ネットワーク機器）

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、IP アドレスや MAC アドレス、電子証明書等を用いて接続元を限定することで、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、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。

IP アドレス：Internet Protocol アドレスの略。IP ネットワーク上で通信相手や送信元を識別し、データを適切な宛先へ届けるために、機器やインターフェースに割り当てられる番号です。

（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

3　インシデント発生に備えた対応　　【医療機関・薬局確認用　事業者確認用】

①　《医療機関・薬局確認用》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
3.4.2
3.4.3
▶企画管理編
12.3

医療機関等の経営層等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、企画管理者等に指示することが重要です。

企画管理者等は情報セキュリティ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。連絡体制図には施設内の連絡先に加え、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。

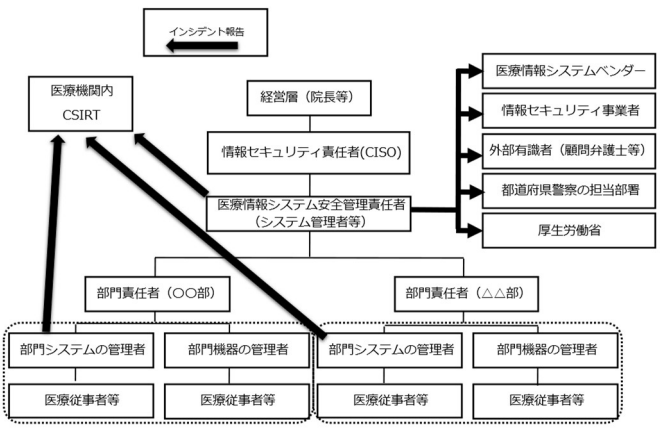
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

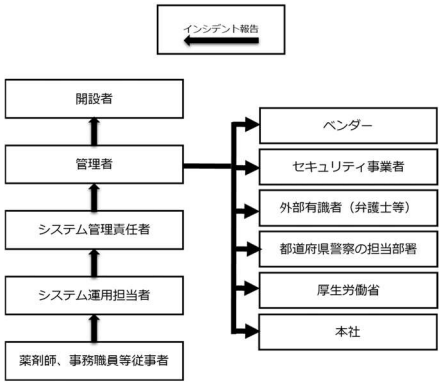
情報セキュリティインシデント発生時（医療情報システムに障害が発生した場合を含む）は、下記の厚生労働省の連絡先に御連絡ください。

【連絡先】厚生労働省医政局医療情報担当参事官室　03-6812-7837

●連絡体制図の例１（医療機関）



●連絡体制図の例２（薬局）



② 《医療機関・薬局確認用》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。

非常時でも、稼働が損なわれた医療情報システムを復旧できるよう、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。企画管理者等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
12.2
▶システム運用編
11.1
12.2
18.1

② サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。

医療機関等の経営層等は企画管理者等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、サイバー攻撃の想定を含む 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、万が一サイバー攻撃を受けても重要業務が中断しない、又は中断しても短い期間で再開することが期待できます。

また、昨今サプライチェーンを構成する事業者が攻撃を受けることにより、サービスや物資の途絶が起こる、事業者を通じて医療機関等がサイバー攻撃を受ける、と言う事案が多発しています。事業者確認用チェックリストを通して、事業者が BCP を策定して、非常時の対応に備えていることを確認して下さい。

BCP を策定していても、実際には運用できず、バックアップが復旧できない事例も多数発生しています。医療機関等、事業者のいずれにおいても、BCP 訓練を実施していることが望ましいです。

▶経営管理編
3.4.1
▶企画管理編
11.1

4　規程類の整備　【医療機関・薬局確認用】

①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。
（医療情報システム全般）

医療情報システムの安全管理が適切に行われるためには、組織内において明文化されたルールが必要となります。例えば、

・医療情報システムの利用ができる機器の管理方法
　例）システム管理者は不正な利用の防止及び発見に向け、情報システムの利用者ごとに適切なアクセス権限を付与したアカウントを登録し、定期的に操作ログを確認する。
・医療情報システムに異常が生じた場合の対応
　例）災害、サイバー攻撃等により、一部医療行為の停止等、医療サービス提供体制に支障が発生する非常時の場合、別途定める事業継続計画（BCP）に従って運用を行う。
・職員の情報セキュリティなどに関する教育や訓練に関すること
　例）システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行う。

などが挙げられ、経営層や企画管理者が管理できるようにすることが求められます。これらの内容について、医療情報システムの安全管理に関するガイドラインや小規模医療機関等向けガイダンス等を参考にして策定してください。

立入検査時は、本規程類も確認対象となります。

▶企画管理編 4.1