

医療安全管理対策の基礎知識（2024年2月改訂版）正誤及び追補

(2025年1月8日現在)

※訂正箇所は**ゴシック太字下線**で表示する。但し、下線等の訂正については「訂正箇所」欄に注釈で示す。

※追補は■印を付した。

頁	訂正箇所	誤	正
15	上から9行目	…医療安全委員会…	…医療安全 管理 委員会…
15	上から16行目		
55	上から6行目	(2022年 4月 26日、医政地発0726第1号)	(2022年 7月 26日、医政地発0726第1号)
95	上から13行目を右の通り修正	<p>報告書(様式第2号)を所轄労働基準監督署長に提出する。 なお、令和3年4月1日から、下記の通り取り扱われることとされた。 ※雇入れ・配置替えの際の健康診断では、④の項目は使用する線源の種類等に応じて省略することができる。 ※6か月以内ごとに1回、定期に行う健康診断では、</p> <ul style="list-style-type: none"> ・ 医師が必要でないと認めるときは、②から⑤までの項目の全部または一部を省略できる。 ・ 健康診断を行おうとする日の属する年の前年1年間に受けた実効線量が5mSvを超えず、かつ、健康診断を行おうとする日の属する1年間に受ける実効線量が5mSvを超えるおそれがない方は、②から⑤までの項目は、医師が必要と認めないときには、行う必要がない。 ・ ただし、健康診断を行う年の前年1年間に、眼の水晶体に受けた等価線量が20mSvを超え、かつ当年1年間に眼の水晶体に受ける等価線量が20mSvを超えるおそれのある方については、電離放射線健康診断の白内障に関する眼の検査を省略することは(電離則第56条第3項)、適当ではない。また、このような方の白内障に関する眼の検査は、眼科医により行われることが望ましい。 	
95	上から19行目	<p>※眼の水晶体に受ける等価線量が年間20mmSvを超えた放射線診療従事者等について、適切な被ばく線量の管理を図るため、作業環境、作業方法、作業時間等の改善を行うとともに、当該「5年間」で100mmSvを超えることのないよう、随時、累積線量を確認することが望ましい。</p>	<p>※令和3年4月1日から、電離放射線障害防止規則が改正され、眼の水晶体に受ける等価線量限度は、5年間で100mSvかつ1年間で50mSvとなった。</p>
95	下から13行目	第5章 放射線の過剰被ばくその他の…	第4章 放射線の過剰被ばくその他の…
96	下から8行目	第6章 医療従事者と患者間の情報共有	第5章 医療従事者と患者間の情報共有
98	上から1行目	第7章 その他	第6章 その他
98	下から7行目	【編注】「皮膚への高線量照射」を行わない場合は、 第19条 は不要です。	【編注】「皮膚への高線量照射」を行わない場合は、 第20条 は不要です。
■100	下から5行目	また、次頁に掲げる診療報酬(2022~2023)は、…	また、次頁に掲げる診療報酬(2024~2025)は、…
■101	枠囲み	2024年診療報酬改定を受けて、別紙1の通り修正する。	
■102	下段~105頁	2024年5月に厚労省が更新した「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」に基づき、別紙2の通り修正する。	
■106	頁~108頁	<p>2024年5月に厚労省が更新した「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」に基づき、別紙3の通り修正する。 なお、新しいチェックリスト(エクセル表)は、下記を参照 ○医療機関確認用 https://www.mhlw.go.jp/content/10808000/001297168.xlsx ○事業者確認用 https://www.mhlw.go.jp/content/10808000/001297169.xlsx</p>	
124	上から7行目	https://anshin.pref.tokushima.jp/med/experts/docs/2023022200010/	https://www.pref.tokushima.lg.jp/med/categoryMedical/sonota/kikan/7234660/
127	上から3行目		
130	上から2行目、中央タイトル下		

※ 101 頁の枠内を、2024 年診療報酬改定を受けて、下記の通り修正する。

- (1) 点数又は加算そのものの要件とであるもの
- ・ A000 初診料の「医療DX推進体制整備加算」
 - ・ A207 診療録管理体制加算（許可病床数 200 床以上の病院は、ガイドラインの遵守に加えて、専任の医療情報システム安全管理責任者を配置し、当該責任者は、職員を対象として、少なくとも年 1 回程度、定期的に必要な情報セキュリティに関する研修を行っている。なお、200 床以上 400 床未満の病院については令和 7 年 5 月 31 日までは当該基準を満たしているものとみなす）
 - ・ A207-2 医師事務作業補助体制加算
 - ・ A245 データ提出加算（ガイドラインに準拠）
 - ・ A246-3 医療的ケア児（者）入院前支援加算
 - ・ A301 特定集中治療室管理料の「特定集中治療室遠隔支援加算」
 - ・ B001・9 外来栄養食事指導料の注 4・注 6
 - ・ B009 診療情報提供料（I）の検査・画像情報提供加算
 - ・ B009-2 電子的診療情報評価料
 - ・ C002 在宅時医学総合管理料の「在宅医療情報連携加算」
 - ・ C002-2 施設入居時等医学総合管理料の「在宅医療情報連携加算」
 - ・ C102 在宅自己腹膜灌流指導管理料の「遠隔モニタリング加算」
 - ・ C102-2 在宅血液透析指導管理料の「遠隔モニタリング加算」
- (2) 電子的方法により個々の患者の診療情報等を他の医療機関、保険薬局等に提供する場合
- ・ 当該対応を行う全ての行為
 - ~~・ B000 診療情報提供料（I）~~
 - ~~・ C005-2 在宅患者訪問点滴注射管理指導料~~
- (3) 電子カルテなどを含む医療情報システムと共通のネットワーク上の端末において 共同指導又はカンファレンスを実施する場合若しくは又は個人情報を画面上で取り扱う場合
- ・ 基本診療料及び特掲診療料の施設基準等に掲げる全ての点数において、保険医療機関の電子カルテなどを含む医療情報システムと共通のネットワーク上の端末においてカンファレンスを実施する場合（基本診療料の施設基準等の通則 9 及び特掲診療料の施設基準等の通則 5 に規定）
 - ~~・ A000 初診料及び A001 再診料の外来感染対策向上加算~~
 - ~~・ A234-2 感染対策向上加算~~
 - ~~・ A246 入退院支援加算 1~~
 - ・ A301-3 脳卒中ケアユニット入院医療管理料
 - ・ B004 退院時共同指導料 1 ~~の注 1~~
 - ・ B005 退院時共同指導料 2 ~~の注 1、注 3~~
 - ・ B005-1-2 介護支援等連携指導料
 - ・ B005-10 ハイリスク妊産婦連携指導料 1
 - ・ B005-10-2 ハイリスク妊産婦連携指導料 2
 - ・ B015 精神科退院時共同指導料
 - ・ C000 往診料の「往診時医療情報連携加算」
 - ・ C002 在宅時医学総合管理料の「在宅療養移行加算」
 - ・ C002-2 施設入居時等医学総合管理料の「在宅療養移行加算」
 - ・ C005 在宅患者訪問看護・指導料の「在宅患者緊急時等カンファレンス加算」
 - ・ C005-1-2 同一建物居住者訪問看護・指導料の「同一建物居住者緊急時等カンファレンス加算」
 - ・ C011 在宅患者緊急時等カンファレンス料
 - ・ C013 在宅患者訪問褥瘡管理指導料
 - ・ C014 外来在宅共同指導料
 - ・ C015 在宅がん患者緊急時医療情報連携指導料
 - ・ I016 精神科在宅患者支援管理料
- (4) ~~電子的方法によって、個々の患者の診療に関する情報等を送受信する場合（上記(3)へ統合）~~
- ~~・ E 画像診断管理加算~~
 - ~~・ E 遠隔画像診断~~
 - ~~・ E 歯科画像診断管理加算~~
- (5) ~~患者の個人情報を含む医療情報の送受信を行う場合~~

~~A301-3 脳卒中ケアユニット入院医療管理料~~ (上記(3)へ統合)

- (6) ガイドラインに準拠した体制であることが望ましいとされている施設基準
- ・ 外来データ提出加算
 - ・ 在宅データ提出加算
 - ・ リハビリテーションデータ提出加算
- (7) 電子カルテシステム (オーダーリングシステムを含む) 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」等に準拠した体制であり、当該体制について、規程を文書で整備していることが求められる施設基準
- ・ A207-2 医師事務作業補助体制加算

別紙 2

※ 102 頁下段～105 頁の「I 医療機関確認用チェックリスト」を、令和 6 年 5 月に厚労省が更新した「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」に基づき、次の通り修正する。

I 医療機関確認用チェックリスト

年度ごとのチェック項目を確認し、「はい」または「いいえ」にマルをつけて、確認した日付を記入する。1 回目の確認で「いいえ」となる場合は、対策の実施にかかる目標日を記入し、整備を行う。

なお、下記に記載上のポイントを整理したが、各項目の考え方や確認方法等の詳細は、「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～」(下記 URL) を参照いただきたい。

~~<https://www.mhlw.go.jp/content/10808000/001105752.pdf>~~

<https://www.mhlw.go.jp/content/10808000/001253953.pdf>

一. 医療情報システムの有無欄

(1) 医療情報システムを導入、運用している。

- ① 「医療情報システムの有無」欄は、レセコン、電子カルテ、オーダーリングシステム等の医療事務や診療を支援するシステムの他、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末、患者情報が通信される院内・院外ネットワーク、インターネットと接続した監視カメラなどが含まれる場合には、「はい」に○をつけ、体制整備、医療情報システムの管理・運用、インシデント発生に備えた対応が求められる。
- ② これらの医療情報システムが全くない場合は、「いいえ」に○をつけ、その他の項目は確認が不要となる。

二. ~~チェックリストの解説~~令和 5 年度中に整備が必要なもの

全ての項目について、~~令和 5 年度中に~~、「はい」に○がつくようにする必要がある。

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。

- ① 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の推進に責任を持つ「医療情報システム安全管理責任者」を設置しなければならない。
- ② 院長などの経営層が「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が、企画管理者（医療情報システムの安全管理の実務担当者）が兼務しても良い。
- ③ 「安全管理責任者」は、厚生労働省ガイドライン「企画管理」編の内容を把握する。

2. 医療情報システムの管理・運用

2-1. 医療情報システム全般について

(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。

- ① サーバ、端末 PC（パソコン）、ネットワーク機器など医療機関で所有する「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、情報機器等が利用に適した状況にあることを確認する。

- ② 機器台帳の内容は、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）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る（下表参照）。
- ③ 機器台帳の作成にあたっては、事業者等に確認する。

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	〇〇電子カルテ	2.0	192.168.〇.〇	Room1のPC1	Room1	a医師（〇〇科）	2020/12/1	稼働	
002	A社	Win11	〇〇電子カルテ	1.2	192.168.〇.〇	Room1のPC2	Room1	b医師（〇〇科）	2020/12/1	停止	メンテナンス
003	A社	Win8	〇〇電子カルテ	2.0	192.168.〇.〇	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	〇〇管理システム	5.0.1	192.168.〇.〇	Room3のPC1	Room3	a医師（〇〇科）、b医師（〇〇科）、c医師（△△科）	2021/8/1	稼働	

※ 「医療情報システムで用いる情報機器」台帳管理の一例

(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。

- ① 機器台帳もとにリモートメンテナンス利用機器の有無を事業者を確認する。
- ② 事業者とリモートメンテナンスの契約がない場合は、記入不要である。

(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。

- ① 事業者から、医療情報セキュリティ開示書（MDS / SDS）を提出させる。
- ② 開示書は、「一般社団法人保健医療福祉情報システム工業会」（下記URL参照）で書式が示されている。

<https://www.jahis.jp/standard/detail/id=987>

- ③ 事業者と契約がない場合は、記入不要である。

2-2. サーバについて

(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。

- ① 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する。
- ② 利用者に付与したID等については、所属部署・氏名・ユーザID・権限等を台帳等に一覧化することが望ましい（下表参照）。

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
.

※ 「アクセス利用権限」台帳の一例

(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。

- ① 利用者に付与したID等の管理台帳等の情報を元に、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する。

- ② 長期間使用されていない等の不要なIDは、速やかに削除する。

(6) アクセスログを管理している。

利用者のアクセスログ（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を記録し、保管する。

●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
.

2-3. ネットワーク機器について

(7) セキュリティパッチを適用している。

- ① 事業者に対して、使用しているOSやソフトウェアのセキュリティパッチ（修正プログラム）が発表された場合にメールなどで連絡をするよう、求める。
- ② 事業者からセキュリティパッチが配布された場合、速やかに適用している。

(8) 接続元制限を実施している。

- ① 特定の機器や人からしか、接続できないようにしている。
- ② 外部ネットワークに接続する際には、事業者と相談し、ネットワークや機器等を適切に選定し、監視を行。

(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。

- ① プログラム一覧やタスクマネージャー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、不要なものは停止させる。
- ② Windowsでは「Ctrl+Shift+ESC」で「タスクマネージャー」を開くと、動作しているソフトウェア及びサービスを全て見ることができる。
- ③ 不審なものがある場合は、事業者と相談する。

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。

- ① 組織内の連絡体制（医療情報システム安全管理責任者の所属・緊急連絡先）
- ② 事業者の緊急連絡先
- ③ 厚生労働省

ア. 医政局特定医薬品開発支援・医療情報担当参事官室

TEL: 03-6812-7837 mail: igishitsu@mhlw.go.jp

イ. 個人情報保護委員会（個人情報保護法第26条に基づく場合）

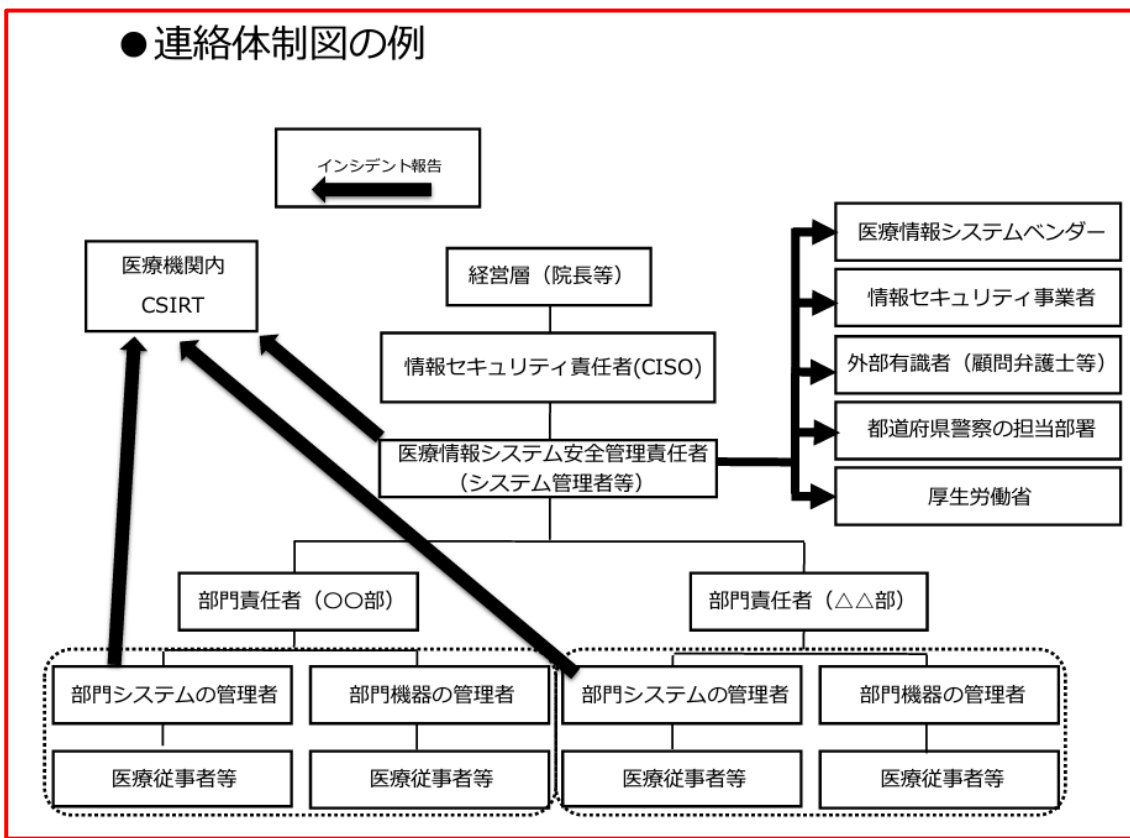
<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

- ④ 都道府県警のサイバー犯罪窓口

※下記参照（下記ページで不明な場合は都道府県警へ）

<https://www.npa.go.jp/bureau/cyber/soudan.html>

立入検査時は、連絡体制図が作成されていることが確認されます。



三. 令和6年度中に整備が必要なもの

~~1. 体制構築と、2-1. 医療情報システム全般、2-2. サーバの(4)~(6)、2-3. ネットワーク危機には、令和5年度中に整備していなければならない。~~

2-2. サーバについて

~~(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。~~

~~① 事業者に対して、使用しているサーバのセキュリティパッチ(修正プログラム)が発表された場合にメールなどで連絡をするよう、求める。~~

~~② 事業者からセキュリティパッチが配布された場合、速やかに適用している。~~

~~(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。~~

- ~~① プログラム一覧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、不要なものは停止させる。~~
- ~~② Windows では「Ctrl+Shift+ESC」で「タスクマネージャー」を開くと、動作しているソフトウェア及びサービスを全て見ることができる。~~
- ~~③ 不審なものがある場合は、事業者と相談する。~~

~~2-4. 端末PCについて~~

~~(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。~~

~~※ 端末PCについて、上記二の2-2の(4)と同様の対策を行う(参照⇒P8)~~

~~(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。~~

~~※ 端末PCについて、上記二の2-2.の(5)と同様の対策を行う(参照⇒P8)~~

~~(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。~~

~~※ 端末PCについて、上記二の2-2.の(7)と同様の対策を行う(参照⇒P8)~~

~~(9) バックグラウンドで動作している不要なランサムウェア及びサービスを停止している。~~

~~※ 端末PCについて、上記2-2.の(9)と同様の対策を行う(参照⇒P8)~~

~~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。~~

- ~~① 復旧手順の方法をあらかじめ、事業者を確認しておく。~~
- ~~② BCPに復旧手順を記載しておく。~~

~~(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。又は令和6年度中に策定予定である。~~

~~○ BCPの策定例は、第2部別紙3(参照⇒25~27)。~~

別紙3 106頁～108頁の「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」（医療機関確認用）及び（事業者確認用）について、厚労省が更新した下記のチェックリストに変更する。

○医療機関確認用 <https://www.mhlw.go.jp/content/10808000/001297168.xlsx>

○事業者確認用 <https://www.mhlw.go.jp/content/10808000/001297169.xlsx>

なお、参考として「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」の変更点を見え消しで下記に示す。

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)	備考
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。

※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6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)			備考	R5年度項目
		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。(1-(1))	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。(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 (/)	(/)	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。(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 (/)	(/)	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。(2-(4))	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。(2-(5))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	(6) アクセスログを管理している。(2-(6))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	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-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	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-(9))	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。					
	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。(2-(4))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	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。(2-(5))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	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-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	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-(9))	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。(2-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		※	
(8) 接続元制限を実施している。(2-(8))	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。（3-1）	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	※
	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（ / ）	（ / ）	はい・いいえ（ / ）	
	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（ / ）	（ / ）	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。
- 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。
- R5年度項目欄（※）：「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（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目
- ~~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。~~

○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)			備考
		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。~~

II 事業者確認用チェックリスト

医療情報機器の管理を事業者に委託している場合は、下記（事業者確認用）のチェックリストを事業者に渡して、対策の状況を記載してもらい、回収・保管しておく。

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。

※1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果(日付)			備考	R5年度項目
		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。(1-(1))	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。(2-(2))	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。(2-(3))	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。(2-(4))	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。(2-(5))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	(6) アクセスログを管理している。(2-(6))	はい・いいえ (/)	(/)	はい・いいえ (/)		※
	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-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		
	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-(9))	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。(2-(7))	はい・いいえ (/)	(/)	はい・いいえ (/)		※	
(8) 接続元制限を実施している。(2-(8))	はい・いいえ (/)	(/)	はい・いいえ (/)		※	

○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)			備考	
		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。
- 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。
- R5年度項目欄（※）：「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（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目