「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」への対応状況調査

本調査は、令和 7 年度厚生労働行政推進調査事業「医療機関におけるサイバーセキュリティ対策向上に向けた課題調査と解決策の検討（25IA2012）」（研究代表者：武田理宏（大阪大学）」で実施するものです。
本調査は、最初に各医療機関のサイバーセキュリティ人材の配置状況を確認したのち、令和 6 年度版の「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」に沿って対応状況をご回答いただきます。
あわせて、令和 7 年度版で追加される事項についてもお尋ねいたします。
【 】内は、質問に対応するチェックリストの項目を記載しています。
参考） 令和 6 年度版の「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」
https://www.mhlw.go.jp/content/10808000/001262036.pdf
令和 7 年度版の「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」
https://www.mhlw.go.jp/content/10808000/001450189.pdf
https://www.mhlw.go.jp/content/10808000/001490741.pdf

セクション 1 貴施設についておしえてください。

1.**所在地（都道府県）についてお教えください。**【必須】【単一選択】
[ ]

2.**貴施設に該当するものをお選びください。**【必須】【単一選択】
※ 公的な医療機関とは、次に掲げる者が開設する医療機関を指します。
国、都道府県、市町村、地方公共団体の組合、国民健康保険団体連合会及び国民健康保険組合、日本赤十字社、社会福祉法人恩賜財団済生会、厚生農業協同組合連合会、社会福祉法人北海道社会事業協会
※ 国立病院機構等も公的な医療機関としてご回答ください。
○ 国公立大学病院
○ 公的な医療機関（大学病院を除く）
○ 私立大学病院
○ 私立の医療機関

3.**貴施設の認定、指定についてお教えください**【必須】【複数選択】
□ 特定機能病院
□ 地域医療支援病院
□ 災害拠点病院（基幹）
□ 災害拠点病院（地域）
□ 第三次救急医療機関
□ 第二次救急医療機関
□ 総合周産期母子医療センター
□ 地域周産期母子医療センター
□ 小児中核病院
□ 小児地域医療センター
□ 小児地域支援病院
□ 上記の認定、指定は受けていない

4.**許可病床数についてお教えください。**【必須】【単一選択】

- ○ 1000 床以上
- ○ 800 床以上 1000 床未満
- ○ 600 床以上 800 床未満
- ○ 400 床以上 600 床未満
- ○ 300 床以上 400 床未満
- ○ 200 床以上 300 床未満
- ○ 100 床以上 200 床未満
- ○ 100 床未満

5.**診療録管理体制加算の算定状況をお聞かせください。**【必須】【単一選択】

- ○ 加算1
- ○ 加算2
- ○ 加算3
- ○ 算定していない

6.**医療情報システムを管理する部門を設置していますか。**【必須】【単一選択】

- ○ はい
- ○ いいえ

7.**専門知識を有する情報セキュリティ人材を配置していますか。**【必須】【単一選択】

※ IPA IT スキル標準レベル 4 は、「プロフェッショナルとしてスキルの専門分野が確立し、自らのスキルを活用することによって、独力で業務上の課題の発見と解決をリードするレベル。社内において、プロフェッショナルとして求められる経験の知識化とその応用（後進育成）に貢献しており、ハイレベルのプレーヤとして認められます。スキル開発においても自らのスキルの研鑽を継続することが求められます。」と定義され、サイバーセキュリティ領域では情報処理安全確保支援士試験が相当します。
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html

- ○ 高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有する情報セキュリティ人材を配置している
- ○ 専門知識を有する情報セキュリティ人材を配置している
- ○ 配置していない

8.診療録を電子的に管理していますか（電子カルテを導入していますか）。【必須】.【単一選択】.

- ○ はい
- ○ いいえ

セクション 2【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))】

9.**情報セキュリティ責任者（CISO:　Chief Information Security Officer）を配置していますか。**
【必須】【単一選択】

※ 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 版では、「サイバー攻撃に対しては情報セキュリティ責任者（CISO（Chief Information Security Officer））の配置や、CSIRT（Computer Security Incident Response Team）の構築が有効とされており、企画管理者はこれらの整備の要否や、必要な場合にはその構成や非常時の対応内容などについて検討し、経営層の承認を得ることが求められる。」と記載されています。

※ 情報セキュリティ責任者（CISO）に相当する役割（呼称は各施設で異なって問題ありません）の設置の有無をお答えください。

- ○ 配置している（医療情報システム安全管理責任者とは別の人物）　→ **設問 10 に**
  ※例）副院長が CISO、医療情報部長が医療情報システム安全管理責任者など
- ○ 配置している（医療情報システム安全管理責任者を配置と同一人物）　→ **設問 15 に**
- ○ 配置していない　→ **設問 14 に**

10.**情報セキュリティ責任者（CISO）はサイバーセキュリティに対する知識をどの程度保有していますか。**
【必須】【単一選択】

- ○ 高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有しており、単独でも対策を進めることができる
- ○ 一定の専門知識を有しているおり、単独でも対策を進めることができる
- ○ 一定の専門知識を有しているが、対策には情報セキュリティ人材のサポートが必要である
- ○ ほとんど知識を有していない
- ○ 全く知識を有していない

11.**情報セキュリティ責任者（CISO）の職位をお答えください。**【必須】【単一選択】

※ 兼任等されている場合、上位の職位をお答えください。

- ○ 医療機関の責任者（院長など）
- ○ 院長を補佐する立場（副院長、院長補佐など）
- ○ 医療情報システム管理部門の長
- ○ 医療情報システム管理部門（部門長以外）
- ○ 事務部門の長、　○事務部門（部門長以外）
- ○ 上記以外の部門の長
- ○ 上記以外の部門（部門長以外）
- ○ その他（　　）

12.**情報セキュリティ責任者（CISO）が保有する医療系資格についてお答えください。**
【必須】【複数選択】

- ☐ 医師・歯科医師
- ☐ 看護師・助産師・保健師
- ☐ 薬剤師
- ☐ 診療放射線技師
- ☐ 臨床検査技師
- ☐ 臨床工学技士
- ☐ 医学物理士
- ☐ 医療情報技師（上級医療情報技師を含む）
- ☐ 診療情報管理士
- ☐ リストにある医療系資格を保持していない

13.**情報セキュリティ責任者（CISO）が保有する情報処理推進機構（IPA）が認定する資格・試験についてお答えください。**【必須】【複数選択】

- ☐ 情報処理安全確保支援士（登録情報セキュリティスペシャリスト）
- ☐ 情報処理安全確保支援士（試験に合格のみ）
- ☐ 応用情報技術者試験
- ☐ 基本情報技術者試験
- ☐ 情報セキュリティマネジメント試験
- ☐ IT パスポート試験
- ☐ リストされる資格・試験は保持していない

14.**医療情報システム安全管理責任者を配置していますか。**【必須】【単一選択】

- ○ 配置している（情報セキュリティ責任者（CISO）とは別の人物） → **設問 15 に**
- ○ 配置していない → **設問 19 に**

15.**医療情報システム安全管理責任者はサイバーセキュリティに対する知識をどの程度保有していますか。**【必須】【単一選択】

- ○ 高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有しており、単独でも対策を進めることができる
- ○ 一定の専門知識を有しているおり、単独でも対策を進めることができる
- ○ 一定の専門知識を有しているが、対策には情報セキュリティ人材のサポートが必要である
- ○ ほとんど知識を有していない
- ○ 全く知識を有していない

16.**医療情報システム安全管理責任者の職位をお答えください。**【必須】【単一選択】
※兼任等されている場合、上位の職位をお答えください。

- ○ 医療機関の責任者（院長など）
- ○ 院長を補佐する立場（副院長、院長補佐など）
- ○ 医療情報システム管理部門の長
- ○ 医療情報システム管理部門（部門長以外）
- ○ 事務部門の長
- ○ 事務部門（部門長以外）
- ○ 上記以外の部門の長、
- ○ 上記以外の部門（部門長以外）
- ○ その他（ ）

17.**医療情報システム安全管理責任者が保有する医療系資格についてお答えください。**
【必須】【複数選択】

- □ 医師・歯科医師
- □ 看護師・助産師・保健師
- □ 薬剤師
- □ 診療放射線技師
- □ 臨床検査技師
- □ 臨床工学技士
- □ 医学物理士、
- □ 医療情報技師（上級医療情報技師を含む）
- □ 診療情報管理士
- □ リストにある医療系資格を保持していない

18.**医療情報システム安全管理責任者が保有する情報処理推進機構（IPA）が認定する資格・試験についてお答えください。**【必須】【複数選択】 **→ 設問 20 に**

- □ 情報処理安全確保支援士（登録情報セキュリティスペシャリスト）
- □ 情報処理安全確保支援士（試験に合格のみ）
- □ 応用情報技術者試験
- □ 基本情報技術者試験
- □ 情報セキュリティマネジメント試験、
- □ IT パスポート試験
- □ リストされる資格・試験は保持していない

19.**情報セキュリティ責任者（CISO）や医療情報システム安全管理責任者を設置しない理由を教えてください。**【必須】【複数選択】

- □ 許可病床数が 200 床以上であるが、医療情報システム安全管理責任者の設置の必要性を感じない（診療録管理体制加算の算定を行わない）から
- □ 許可病床数が 200 床以上であるが、医療情報システム安全管理責任者に適任な人材がいないから
- □ 許可病床数が 200 床未満で、医療情報システム安全管理責任者の設置の必要性を感じないから
- □ 許可病床数が 200 床未満で、医療情報システム安全管理責任者に適任な人材がいないから
- □ その他（ ）

20.**貴院のサイバーセキュリティ対策の方針を決定する際に関わる情報セキュリティ人材を選択してください。**【必須】【複数選択】

- □ 情報セキュリティ責任者（CISO）
- □ 医療情報システム安全管理責任者
- □ 院内に配置する高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有する情報セキュリティ人材
- □ 院内に配置する専門知識を有する情報セキュリティ人材
- □ 同一法人等の中央組織に配置する高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有する情報セキュリティ人材
- □ 同一法人等の中央組織に配置する専門知識を有する情報セキュリティ人材
- □ 同一法人等の他医療機関に配置する高度な専門知識（IPA IT スキル標準レベル 4 以上相当）を有する情報セキュリティ人材
- □ 同一法人等の他医療機関に配置する専門知識を有する情報セキュリティ人材
- □ 保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認している）
- □ 保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認できていない）
- □ 情報セキュリティ対策を専門とする企業等（医療情報システムベンダー以外）の情報セキュリティ人材
- □ その他

21.**「その他」を選ばれた場合、貴院のサイバーセキュリティ対策の方針を決定する際に関わるその他の情報セキュリティ人材についてご記載ください**【テキスト入力】

[ ]

セクション 3【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))】

22.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理を行っていますか。**
【必須】【単一選択】

- ○ サーバ、端末 PC、ネットワーク機器、全てで台帳管理をしている → **設問 23 に**
- ○ サーバ、端末 PC、ネットワーク機器、いずれかで台帳管理をしている → **設問 23 に**
- ○ 台帳管理を行っていない → **設問 27 に**

23.**台帳管理を行っている医療情報システムに接続するサーバ、端末 PC、ネットワーク機器について**
【必須】

	全ての機器を把握している	全ての機器を把握していると思うが、漏れがあるかもしれない	全ての機器を把握できていない	ほとんどの機器を把握できていない	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

24.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理を行っているのは誰ですか。**【必須】

	自施設の職員	機器を導入した事業者（保守契約など）	導入事業者以外の事業者	その他	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

25.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理の方法をお答えください。**【必須】

	用紙運用	エクセル等の汎用ソフトを使用	専用ソフトを使用	その他	台帳管理を行っていない
サーバ	○	○	○	○	○
端末 PC	○	○	○	○	○
ネットワーク機器	○	○	○	○	○

26.**医療情報システムに接続するサーバ、端末 PC、ネットワーク機器の台帳管理に専用ソフトを使っている場合、メーカとソフト名をご記載ください。**【テキスト入力】

[ ]

27.**外部から医療情報システムネットワークに接続している回線を把握していますか。**
【必須】【単一選択】
- ○ 全て把握している → **設問 28 に**
- ○ 一部のみ把握している → **設問 28 に**
- ○ 把握していない → **設問 29 に**

28.**外部から医療情報システムネットワークに接続していることを把握している回線数を記載してください。**【必須】【数字入力】
[ ]

29.**外部から医療情報システムネットワークに接続している回線数を減らす努力をしていますか。**
【必須】【単一選択】
- ○ 努力をしている
- ○ 回線数を減らす必要性は感じているが、努力はできていない
- ○ 回線数を減らす必要性は感じていない

30.**貴施設が、外部から医療情報システムネットワークに接続している回線を、全数把握し、管理する場合、何回線以下であれば適切に管理できますか。**【必須】【数値入力】
※「適切な管理」とは、「それぞれの回線の機器に対し最新のセキュリティパッチを当てたり、リスクアセスメント（異常な通信の増加を検知し、適切な対策を取るなど）を実施したりすることなど」を想定し、貴施設が適切に管理できると考える回線数をご記入ください。
※ 貴施設で回線を管理することができない場合、管理すべきでないとお考えの場合は、「0」と入力してください。
※ ご意見、お考えがない場合は、「9999」と入力してください。
[ ]

【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))】
31.**リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法についてお答えください。**
【必須】【単一選択】
- ○ 自施設が設置するリモート接続の仕組みを使った接続のみ許可している
- ○ 自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握している）
- ○ 自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握できていない）
- ○ 自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握している）
- ○ 自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している（接続する全てのリモートメンテナンス回線を把握できていない）
- ○ リモート接続はベンダーに任せており、リモート接続の許可を行っていない（接続する全てのリモートメンテナンス回線の把握はできている）
- ○ リモート接続はベンダーに任せており、リモート接続の許可を行っていない（接続する全てのリモートメンテナンス回線の把握ができていない）
- ○ リモートメンテナンス（保守）は行っていない

【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))】

32.**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）の提出を受けていますか。**【必須】【単一選択】

- ○ 提出を受け、内容を確認し、必要があれば具体的な対応を行っている → **設問 33 に**
- ○ 提出を受け、内容を確認しているが、具体的な対応までは行っていない → **設問 34 に**
- ○ 提出を受けているが、内容は十分に確認していない → **設問 34 に**
- ○ 提出を受けていない（必要性を感じていない） → **設問 34 に**
- ○ 提出を受けていない（事業者が対応してくれない） → **設問 34 に**
- ○ 事業者と契約していない → **設問 34 に**

33.**医療情報セキュリティ開示書（MDS/SDS）の内容を確認した結果、具体的な対応事例があれば、ご記載ください。**【テキスト入力】

[ ]

セクション 4 【医療情報システムの管理・運用】

【サーバ、端末 PC、ネットワーク機器について、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))】
【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。(令和 7 年度 2-④)】

34.**サーバ、ネットワーク機器に対するアクセス権限の付与方法について、教えてください。**【必須】

	administrator 権限のみ設定し、全ての機器群で同じパスワードを設定している	administrator 権限のみ設定し、機器群ごとに異なるパスワードを設定している	組織ごと（病院やベンダー）にユーザ ID と利用権限を設定し、ユーザパスワードは全ての機器群で同じである	組織ごと（病院やベンダー）にユーザ ID と利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	ユーザごとに ID と利用権限を設定し、ユーザパスワードは全ての機器群で同じである	ユーザごとに ID と利用権限を設定し、ユーザパスワードは機器群ごとに異なっている
サーバ	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

35.**端末 PC のエンドユーザに対するユーザ認証について、教えてください。**【必須】【単一選択】

- ○ OS のユーザ認証を活用したユーザ認証を行っている
- ○ OS のユーザ認証とソフトウェアでユーザ認証を組み合わせたユーザ認証を行っている
- ○ OS は administrator 権限で自動ログインを行い、ソフトウェアでユーザ認証を行っている
- ○ OS は administrator 以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- ○ その他（ ）

36.**端末 PC のエンドユーザに対するアクセス利用権限について教えてください。**【必須】【単一選択】

- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定している（複数のユーザで使いまわしをしているユーザ ID はない）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしはない）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしがある）
- ○ すべてのユーザに対して個別のユーザ ID を発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザ ID がある（管理者権限の ID 使いまわしがあるか否かは把握できていない）
- ○ 必要に応じて、ユーザごとの ID 付与と、組織、グループごと（外部委託業者など）の ID 付与を使い分けている
- ○ その他（ ）

【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))】

37.**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ますか。**【必須】

	全て、削除または無効化できている	一部、削除または無効化できていない	全て、削除または無効化できていない
サーバ	○	○	○
端末 PC	○	○	○

38.**不要なアカウントを削除または無効化するタイミングをお答えください。**【必須】

	退職日を有効期限に設定するなどリアルタイムでアカウントを削除または無効化している	年に 1 回など棚卸作業を行い、不要なアカウントを削除または無効化している（退職後にアカウントが有効な期間が存在する）	削除または無効化できていない
サーバ	○	○	○
端末 PC	○	○	○

【アクセスログを管理している。(2-(6))】

39.**サーバ、端末 PC のアクセスログを残していますか。**【必須】【単一選択】

○ サーバ、PC 端末、いずれかのアクセスログを残している → **設問 40 に**

○ アクセスログを残していない → **設問 43 に**

40.**アクセスログを残している範囲をお答えください。**【必須】

	全ての機器のアクセスログを残している	一部の機器のアクセスログを残している	アクセスログを残していない
サーバ	○	○	○
端末 PC	○	○	○

41.**アクセスログを確認していますか。**【必須】

	病院職員がアクセスログを定期的に確認している	保守事業者がアクセスログを定期的に確認している	アクセスログを定期的に確認していないが、必要があれば病院職員が確認をすることが可能である	アクセスログを定期的に確認していないが、必要があれば保守事業者が確認をすることが可能である	アクセスログを残しているが、確認方法は把握していない	アクセスログを残していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○

42.**アクセスログの保管期間を把握していますか**【必須】

	医療機関がアクセスログの保管期間を指定している	保守事業者が定めたアクセスログの保管期間を医療機関として把握している	アクセスログの保管期間を把握していない	アクセスログを残していない
サーバ	○	○	○	○
端末 PC	○	○	○	○

43.**≪アクセスログを残していない場合にお答えください≫**
アクセスログを残していない理由は何ですか。【単一選択】

○ 医療機関としてアクセスログを残す必要性を感じていない
○ 医療機関としてアクセスログを残す必要性を感じているが、コストがかかるため残すことができない
○ 医療機関としてアクセスログを残す必要性を感じているが、保守事業者が対応してくれない
○ その他（ ）

【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))】
44.**サーバ、端末 PC、ネットワーク機器に対し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）を適用していますか。**【必須】【単一選択】

○ サーバ、端末 PC、ネットワーク機器のいずれかに対し、セキュリティパッチを適用している
→ 設問 45 に
○ セキュリティパッチを適用していない
→ 設問 49 に

45. サーバ、端末 PC、ネットワーク**機器に対し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）を適用していますか。**【必須】

	全ての機器に対して適用している	一部の機器に対して適用している	適用していない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

46. サーバ、端末 PC、ネットワーク機器に対し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）を適用するタイミングを教えてください。【必須】

	セキュリティパッチごとにリアルタイムで（システム検証は行わない）	セキュリティパッチごとにできるだけ早いタイミングで（システム検証を行った後）	定期的に（○ヶ月に 1 回など時期を決めて）、セキュリティパッチをまとめて適用を行う	適用が必要なセキュリティパッチが出てきた時に、保守事業者と打ち合わせを行った上、適用時期を決める	その他	セキュリティパッチを適用していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

47. **サーバ、端末 PC、ネットワーク機器に適用する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）はどのように選択していますか。【必須】**

	全てのセキュリティパッチを適応している	医療機関が必要と判断したセキュリティパッチと保守事業者が推奨するセキュリティパッチを適用している	医療機関が必要と判断したセキュリティパッチを適用している	保守事業者が推奨するセキュリティパッチを適用している	その他	セキュリティパッチを適用していない
サーバ	○	○	○	○	○	○
端末 PC	○	○	○	○	○	○
ネットワーク機器	○	○	○	○	○	○

48.**≪セキュリティパッチを適用している場合にお答えください≫**
サーバ、端末 PC、ネットワーク機器に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）を適用する費用についてお答えください。【必須】

	保守費用に含まれる	随時、作業費用を支払っている	セキュリティパッチを適用していない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

49.**≪セキュリティパッチを適用していない場合にお答えください≫**
セキュリティパッチを適用しない理由についてお答えください。【単一選択】

○ 医療機関として必要性を感じていない
○ 医療機関として必要性を感じているが、事業者が対応をしてくれない
○ 医療機関として必要性を感じているが、作業費用の捻出が困難である
○ その他（ ）

50.**セキュリティパッチの適用について、ご意見があればご記載ください。【テキスト入力】**
[ ]

【接続元制限を実施している。(2-(8))】

51.**ネットワーク機器の接続元制限を実施していますか。【必須】【単一選択】**
※ 接続元制限とは、特定の IP アドレスからのみサービスへのアクセスを許可する、または拒否するセキュリティ対策ことを言います。

○ はい → **設問 52 に**
○ いいえ → **設問 54 に**

52.**ネットワーク機器の接続元の管理設定は誰が行っていますか。**【必須】【単一選択】

- ○ 病院
- ○ 病院とネットワーク事業者が協力して
- ○ ネットワーク事業者に任せている
- ○ その他（ ）

53.**ネットワーク機器の接続元の監視は誰が行っていますか。**【必須】【単一選択】

- ○ 病院
- ○ 病院とネットワーク事業者が協力して
- ○ ネットワーク事業者に任せている
- ○ その他（ ）

【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))】

54.**バックグラ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ますか。**【必須】

	はい（システム導入時に確認したのみ）	はい（定期的に確認している）	いいえ
サーバ			
端末 PC			

55.**≪前問で「いいえ」を選択した場合にお答えください≫**
バックグラ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ない理由を教えてください。
【テキスト入力】
[ ]

56.**端末 PC にエンドユーザが希望するソフトウェアをインストールすることが可能ですか。**
【必須】【単一選択】

- ○ ソフトウェアを端末 PC にインストールすることは、システム設定で禁止している。エンドユーザの希望による端末インストールは行わない
- ○ ソフトウェアを端末 PC にインストールすることは、システム設定で禁止している。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。エンドユーザの希望による端末インストールは行わない
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う
- ○ ソフトウェアを端末 PC にインストールすることは、運用で禁止している（システム設定で制限はかけていない）。ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみエンドユーザがインストールを行う
- ○ エンドユーザが自由にソフトウェアを端末 PC にインストールできる

セクション 5【医療情報システムの管理・運用(令和 7 年度)】

【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(令和 7 年度 2-⑦)】
【パスワードの使いまわしを禁止している(令和 7 年度 2-⑧)】
【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。(令和 7 年度 2-⑩)】

57.**機器に対するパスワード管理について、教えてください。**【必須】

	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	パスワードは、英数字、記号が混在した 13 文字以上としている	左記を実現できていない
サーバ	○	○	○
端末 PC	○	○	○
ネットワーク機器	○	○	○

58.**サーバ室の入退室管理について、お答えください。**【必須】【複数選択】

- □ 用紙記録による入退室者の把握
- □ 防犯カメラのよる監視(出入口付近)
- □ 防犯カメラによる監視(サーバ室内)
- □ 物理鍵による入退室管理(貸出記録を保管)
- □ 物理鍵による入退室管理(貸出記録の保管は行わない)
- □ 知識認証(ID とパスワードなど)による入退室管理(入退室者の記録が残る)
- □ 知識認証(パスワードのみ)による入退室管理(入退室者の記録は残らない)
- □ 物理認証(カード認証など)による入退室管理(入退室者の記録が残る)
- □ 物理認証(カード認証など)による入退室管理(入退室者の記録が残らない)
- □ 生体認証(指紋認証、静脈認証、顔認証など)による入退室管理(入退室者の記録が残る)
- □ 生体認証(指紋認証、静脈認証、顔認証など)による入退室管理(入退室者の記録が残らない)
- □ サーバ室は設置していない

59.**サーバに対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証(パスワードなど)、所有物認証(ID カードなど)、生体認証(例、顔認証、指紋認証、静脈認証、虹彩認証など)の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 60 に**
- ○ 二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証。ただし、リモート接続では一要素認証となっている) → **設問 62 に**
- ○ 二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証。リモート接続でも二要素認証を実現している) → **設問 62 に**
- ○ サーバに対する二要素認証を実装している(リモート接続では一要素認証となっている) → **設問 62 に**
- ○ サーバに対する二要素認証を実装している(リモート接続でも二要素認証を実現している) → **設問 62 に**
- ○ その他 (　　) → **設問 62 に**

60.**サーバに対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 62 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 62 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 62 に**
- ○ 実装を行わない → **設問 61 に**

61.**サーバに対する二要素認証の実装を行わない理由をおしえてください。**【テキスト入力】

[ ]

62.**端末 PC に対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証（パスワードなど）、所有物認証（ID カードなど）、生体認証（例、顔認証、指紋認証、静脈認証、虹彩認証など）の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 63 に**
- ○ 端末 PC は二要素認証を導入しているが、医療情報システムネットワークに接続する部門システム端末（ワークステーション等）は一要素認証の端末がある → **設問 65 に**
- ○ 医療情報システムに接続する端末は全て二要素認証を導入している → **設問 65 に**
- ○ その他（ ） → **設問 65 に**

63.**端末 PC に対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 65 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 65 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 65 に**
- ○ 実装を行わない → **設問 64 に**

64.**端末 PC に対する二要素認証を実装しない理由を教えてください。**【テキスト入力】

[ ]

65.**ネットワーク機器に対する二要素認証の有無について教えてください。**【必須】【単一選択】

※ 二要素認証とは、知識認証（パスワードなど）、所有物認証（ID カードなど）、生体認証（例、顔認証、指紋認証、静脈認証、虹彩認証など）の三要素のうちの二要素を認証に用いることを言います。

- ○ 一要素認証である → **設問 66 に**
- ○ 二要素認証（物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証。ただし、リモート接続では一要素認証となっている） → **設問 68 に**
- ○ 二要素認証（物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証。リモート接続でも二要素認証を実現している） → **設問 68 に**
- ○ ネットワーク機器に対する二要素認証を実装している（リモート接続では一要素認証となっている） → **設問 68 に**
- ○ ネットワーク機器に対する二要素認証を実装している（リモート接続でも二要素認証を実現している） → **設問 68 に**
- ○ その他（ ） → **設問 68 に**

66.**ネットワーク機器に対する二要素認証を令和 9 年度までに実装予定である。**【必須】【単一選択】

- ○ 必ず実装する → **設問 68 に**
- ○ 実装を検討中（実装の可能性が高い） → **設問 68 に**
- ○ 実装を検討中（実装の可能性が低い） → **設問 68 に**
- ○ 実装しない → **設問 67 に**

67.**ネットワーク機器に対する二要素認証を実装しない理由を教えてください。**【テキスト入力】
[ ]

【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。(令和 7 年度 2-⑨)】
68.**USB ストレージ等の外部記録媒体や情報機器に対してサーバへの接続を制限している。**
【必須】【単一選択】
- ○ 外部記録媒体や情報機器を接続しても、サーバが認識できないシステム設定となっている
- ○ 許可された外部記録媒体や情報機器だけが、サーバが認識できるシステム設定なっている
- ○ 外部記録媒体や情報機器を認識するが、接続は運用で禁止されている
- ○ 外部記録媒体や情報機器を認識するが、許可された外部記録媒体や情報機器のみ、サーバに接続する運用となっている（運用での制限）
- ○ 外部記録媒体や情報機器のサーバへの接続を制限していない
- ○ その他（ ）

69.**端末 PC に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**
【必須】【単一選択】
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる
- ○ その他（ ）

70.**部門システム管理者が使用する部門システム端末（医療情報システムネットワークに接続）に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**【必須】【単一選択】
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる。
- ○ その他（ ）

71.**エンドユーザが使用するワークステーション等の部門システム端末（医療情報システムネットワークに接続）に対する USB ストレージ等の外部記録媒体や情報機器の接続についてお答えください。**
【必須】【単一選択】

- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続を許可していない（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定による接続制御）
- ○ 外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う（システム設定ではなく、運用による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定による接続制御）
- ○ 病院に申請し許可された外部記録媒体や情報機器のみ端末 PC に接続することができる（システム設定ではなく、運用による接続制御）
- ○ 外部記録媒体や情報機器を自由に接続できる。
- ○ その他（　　）

セクション 6【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))】

72.**インシデント発生時における組織内の連絡体制図が整備されていますか。**【必須】【単一選択】

- ○ 整備しており定期的な見直しを実施している
- ○ 整備しているが定期的な見直しは実施していない
- ○ 整備を計画している
- ○ 整備する計画はない

73.**【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))】**
データやシステムのバックアップの対象を検討していますか。【必須】【単一選択】

- ○ すべての医療情報システムのデータはバックアップが取れている → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討し、必要と判断したデータはバックアップが取れている → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討しているが、バックアップが取れているのは、必要と判断した情報の一部である → **設問 74 に**
- ○ 診療を継続するために必要な情報を検討しておらず、ベンダーが提案したデータのバックアップを取っている → **設問 74 に**
- ○ データのバックアップを取っていない → **設問 79 に**

74.データやシステムのオフラインバックアップを実施していますか。【必須】【単一選択】

- ○ オフラインバックアップを実施している → **設問 75 に**
- ○ オフラインバックアップを実施できていない → **設問 76 に**

75.**データやシステムのオフラインバックアップの状況についてお答えください。**【必須】【複数選択】

- ○ テープバックアップ等によるオフラインバックアップ
- ○ イミュータブルバックアップによるオフラインバックアップ
- ○ クラウド保存でのオフラインバックアップ

76.**サイバーセキュリティ対策を想定したデータやシステムのバックアップのタイミングをお答えください。**【必須】【単一選択】

- ○ 日次
- ○ 2 日に 1 回
- ○ 3 日に 1 回
- ○ 4 日から 7 日に 1 回
- ○ 8 日から 14 日に 1 回
- ○ 15 日以上

77.**サイバーセキュリティ対策を想定したデータやシステムのバックアップは何世代行っていますか**
【必須】【単一選択】
- ○ 1 世代
- ○ 2 世代
- ○ 3 世代
- ○ 4 世代
- ○ 5 世代
- ○ 6 世代以上

78.**データバックアップの復旧手順の確認についてお答えください。**【必須】【単一選択】
- ○ データバックアップの復旧手順を確認し、復旧の実証訓練を行っている
- ○ データバックアップの復旧手順を確認しているが、復旧の実証訓練は実施していない
- ○ データバックアップの復旧は保守事業者に一任しており、医療機関として復旧手順の確認は行っていない
- ○ その他（ ）

【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))】

79.**サイバー攻撃を想定した事業継続計画（BCP）を策定していますか。**【必須】【単一選択】
- ○ 厚生労働省が作成した医療情報システム部門事業継続計画（BCP）を参考に策定した
  → 設問 80 に
- ○ 他院が作成した医療情報システム部門事業継続計画（BCP）を参考に策定した
  → 設問 80 に
- ○ 自施設で独自に策定した **→ 設問 80 に**
- ○ 策定していない **→ 設問 81 に**

80.**サイバー攻撃を想定した事業継続計画（BCP）を定期的に見直していますか。**【必須】【単一選択】
- ○ はい
- ○ いいえ

セクション 7【4. 規程類の整備（令和 7 年度）】

【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。(令和 7 年度 4-①)】

81.**体制構築について、具体的な実施方法を運用管理規程等に定めていますか。**【必須】【単一選択】

○ はい（定期的に見直している）
○ はい（定期的な見直しはできていない）
○ いいえ

82.**医療情報システムの管理・運用について、具体的な実施方法を運用管理規程等に定めていますか。**【必須】【単一選択】

○ はい（定期的に見直している）
○ はい（定期的な見直しはできていない）
○ いいえ

83.**インシデント発生に備えた対応について、具体的な実施方法（サイバー攻撃を想定した事業継続計画（BCP））を運用管理規程等に定めていますか。**【必須】【単一選択】

※ サイバー攻撃を想定した事業継続計画（BCP）が医療情報システム管理部門だけでなく、医療機関として承認され、共有されているかをご回答ください。

○ はい
○ いいえ

セクション 8　インタビュー調査へのご協力

本研究班では、本調査にご協力をいただいた医療機関のうち、いくつかの医療機関を選定し、インタビュー調査を行うことが求められています。
インタビュー調査をご協力いただく医療機関は研究班で選ばせていただきます。

84.**インタビュー調査にご協力いただけますか。**【必須】【単一選択】

※ オンラインで 60 分程度のインタビューを予定しています。
※ サイバーセキュリティ対策の責任者と実務担当者からのインタビューを想定しています。
※ 貴院でのサイバーセキュリティ対策をお聞かせいただいた後、サイバーセキュリティ対策について意見交換を行わせていただきます。

○ はい　→ **設問 85 に**
○ いいえ　→ **回答終了**

85.**研究班がご連絡をさせていただく連絡先をご記載ください。**
医療機関名【必須】【テキスト入力】
[　　]

86.ご担当部署【必須】【テキスト入力】
[　　]

87.ご担当者名【必須】【テキスト入力】
[　　]

88.ご連絡先（電話番号）【必須】【テキスト入力】
[　　]

89.ご連絡先（メールアドレス）【必須】【テキスト入力】
[　　]

別添１

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

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 （　/　）	

*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	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。**					
	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 （　/　）	（　/　）	はい・いいえ （　/　）		※
	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 （　/　）		※
	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。					
	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 （　/　）		※
	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。					
	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 （　/　）		※
	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	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

令和6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	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。**					
	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（　/　）		※
	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。					
	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（　/　）		※
	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。					
	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（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※

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。
- 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

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

医療機関確認用

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

- 各項目の考え方や確認方法等については、「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～」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（ / ）	（ / ）	
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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	
	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（ / ）	（ / ）	

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～」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。