

これを読めばよく分かる！

令和8年度版 医療機関・薬局向け
「サイバーセキュリティ対策チェックリスト」

ポイントを詳しく解説！

目次

- 01 サイバーセキュリティ対策の義務化について
- 02 チェックリストの準備
- 03 チェックリストの使い方

【参考情報】 立入検査時の確認項目について

【サイバーセキュリティ対策チェックリスト個別項目の解説】

- 05 【1 体制構築】 安全管理責任者の設置
- 06 【2 医療情報システムの管理・運用】 台帳管理
- 07 【2 医療情報システムの管理・運用】 リモートメンテナンス
- 08 【2 医療情報システムの管理・運用】 医療情報セキュリティ開示書 (MDS/SDS)
- 09 【2 医療情報システムの管理・運用】 アクセス利用権限・不要アカウントの削除
- 10 【2 医療情報システムの管理・運用】 セキュリティパッチの適用
- 11 【2 医療情報システムの管理・運用】 パスワード管理①
- 12 【2 医療情報システムの管理・運用】 パスワード管理②
- 13 【2 医療情報システムの管理・運用】 外部記録媒体・情報機器の制限
- 14 【2 医療情報システムの管理・運用】 不要なソフトウェア・サービスの停 □
- 15 【2 医療情報システムの管理・運用】 二要素認証の実装・予定
- 16 【2 医療情報システムの管理・運用】 アクセスログの管理
- 17 【2 医療情報システムの管理・運用】 接続元制限の実施
- 18 【3 インシデント発生に備えた対応】 連絡体制図・外部連絡リストの作成
- 19 【3 インシデント発生に備えた対応】 インシデント時の対応準備
- 20 【3 インシデント発生に備えた対応】 サイバー攻撃を想定した BCP対策
- 21 【4規定類の整備】 運用管理規定の整備
- 22 医療機関・薬局ががすべきこと
- 23 サイバーセキュリティサイト開設のご案内

【参考情報】 厚労省サイト・各種資料

本資料は、立入検査の項目に含まれたサイバーセキュリティの対応・対策に向けた「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」の書き方解説(初級編)です。



出典:厚労省 令和5年3月10日「医療法施行規則の一部を改正する省令について」より抜粋
(<https://www.mhlw.go.jp/content/10808000/001075881.pdf>)

[illegible]

【令和8年度版 サイバーセキュリティ対策チェックリスト】

出典:厚労省「令和8年度版 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」より抜粋
(<https://www.mhlw.go.jp/content/10808000/001716185.pdf>)

- ・ 2023年4月1日より医療機関・薬局等は
サイバーセキュリティ確保のための措置を講じる。
→ 必要な措置として、「医療情報システムの
安全管理に関するガイドライン」を参照する。
- ・ セキュリティ対策について適切な措置を行うこと。
- ・ 別途、「サイバーセキュリティ対策チェックリスト」を
作成すること。

- 立ち入り検査時には、チェックリストに基づいて確認が実施される。（本資料：P.5に詳細を記載）
→ チェックリストと合わせて運用管理規定の更新も必要となる。

チェックリストの準備

厚生労働省のサイトより「サイバーセキュリティ対策チェックリスト」とマニュアルをダウンロードできます。

対象施設	タイトル(チェック項目は医療機関および薬局が同一であることから統合)	ファイル形式
医療機関 薬局	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(令和 8年6月) https://www.mhlw.go.jp/content/10808000/001716185.pdf	PDF
	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～(令和8年6月) https://www.mhlw.go.jp/content/10808000/001716186.pdf	PDF
	(医療機関・薬局確認用) 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(Excel)(令和8年6月) https://www.mhlw.go.jp/content/10808000/001716187.xlsx	Excel
事業者	(事業者確認用) 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(Excel)(令和8年6月) https://www.mhlw.go.jp/content/10808000/001716188.xlsx	Excel

出典:厚生労働省サイト「医療情報システムの安全管理に関するガイドライン 第0版(令和8年6月)」より抜粋 (https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html)

立入検査時の 確認項目について

医療機関・薬局への立入検査では、

- ・「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
いることを確認されます。

～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。

出典：厚労省「令和 8 年度版 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～」より抜粋
(<https://www.mhlw.go.jp/content/10808000/001716186.pdf>)

立ち入り検査時には、下記の現物を確認されるため、事前に準備しておく必要があります。

- 2-① 台帳
- 3-① 連絡体制図
- 3-③ 事業継続計画 (BCP)
- 4-① 規定類

チェックリストの使い方

チェックリストは、全ての項目を「はい」にするよう努めます。チェック項目は年度ごとに更新される場合があります。

※ 立入検査時に確認日:「はい」に対して具体的に内容説明を求められることがあります。

②「はい・いいえ」を選択し、日付を記入。
「いいえ」を選択した場合は、目標日を記入する。
(令和8年度中にすべて「はい」に○がつくように取り組む)

*立入検査時、本チェックリストを確認します。令和8年度中にすべての項目で「はい」にマル○付くよう取り組んでください。
*「いいえ」の場合、令和8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	①医療情報システム安全管理責任者を設置している。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	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、ネットワーク機器の台帳管理を行っている。	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。	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。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	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	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または無効化している。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	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。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
2 医療情報システムの管理・運用	⑦パスワードは英数字の混在した8桁以上としている。※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	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	⑧パスワードの使い回しを禁止している。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	⑨USB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。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	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。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	端末について、以下を実施している。			
	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。または令和9年度以降初回のシステム更改時に実装予定である。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	サーバについて、以下を実施している。			
	⑫OSログイン時の二要素認証を実装している。または令和9年度以降初回のシステム更改時に実装予定である。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	⑬アクセスログを管理している。	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。			
	⑭接続元制限を実装している。	はい・いいえ (☐ / ☐)	(☐ / ☐)	

③目標日の後、2回目のチェックを各自実施する。
はい・いいえを確認し、チェック日を記入する。

サイバーセキュリティ対策チェックリスト

個別項目の解説

	チェック項目	確認日	目標日	備考
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。	はい・いいえ (/)	(/)	

運用管理規定の更新も必要です。



(医療情報の安全管理に関するガイドライン第 7.0版の内容を反映)

お客様で安全管理責任者を設置して……「はい」

Q. どのような□が適任か□

A. 例えば、非常時にシステムの停□や、ネットワークの遮断要否を判断できるような経営層が適任です。

Q. 責任者がシステムに関する知識を持っていない場合は□

A. 前提知識を有する担当者等に上記のような対応が□える権限を委譲するか、セキュリティ研修を活□してスキルアップを図りましょう。

なお、システム管理者を配置しないような小規模な施設(クリニック・薬局)の場合には、その施設の管理者が、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ります。
(クリニック:院長、薬局:管理薬剤師 など)

運用管理規程雛形での記載例

Ⅱ 一般管理における運用管理 (一部抜粋)

医療機関

【管理体制】

1. (運用責任者、個人情報保護責任者、安全管理責任者、システム管理者)

1) ・当院に運用責任者、個人情報保護責任者及びシステム管理者を置き、**院長をもってこれに充てること。**

1) 院長は、必要な場合、システム管理者を別に指名すること。

Ⅱ 一般管理における運用管理 (一部抜粋)

薬局

【管理体制】

1. (運用責任者、個人情報保護責任者、安全管理責任者、システム管理者)

1) 当薬局に運用責任者、個人情報保護責任者、安全管理責任者及びシステム管理者を置き、**管理薬剤師をもってこれに充てること。**

2) 管理薬剤師は必要な場合、個人情報保護責任者、安全管理責任者及びシステム管理者を別に指名することができる。

	チェック項目	確認日	目標日	備考
	①サーバ、端末、ネットワーク機器の台帳管理を行っている。	はい・いいえ (/)	(/)	

サーバ、端末、ネットワーク機器についてご自身のクリニック・薬局で保有する医療情報システムについて台帳を作成して管理している…「はい」

クリニック、薬局内にある医療情報システムや機器の全てが対象となります。主にレセコン・電子カルテ・電子薬歴に関係するサーバや PC、外部接続を□うためルータなどのネットワーク機器、医事会計システムのサーバや端末など。管理者は、定期的に状況を確認し、実態や責任の所在が明確になるように監督します。



▶ハードウェアの所在や利用者だけでなく、ソフトウェアのバージョンも台帳で管理します。(弊社にてひな型は準備しております。)

管理する項目:機器メーカー、OS、使用しているソフトウェア(バージョン)、 IPアドレス、コンピュータ名、設置場所、利用者など

●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	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	

＜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・電子薬歴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ーを指します。
ネットワーク機器:無線LANやルータ等を指します。

	チェック項目	確認日	目標日	備考
	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。	はい・いいえ (/)	(/)	

機器管理台帳をもとに事業者リモートメンテナンスを利用している機器の有無を確認したら… 「はい」

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るため、注意が必要です。
確認したら、管理台帳にリモートメンテナンスの有無を明確にし、□書化しましょう。



レセコン・電子カルテ・薬歴以外のシステムや機器（院内機器・調剤機器・会計ソフトなど）も管理しましょう！

EMシステムズでは、「RemoteCall」を使用してお客様へのリモートメンテナンスを行っています。（オフラインのお客様は未使用）



【2医療情報システムの管理・運用】

医療情報セキュリティ開示書(MDS/SDS)

	チェック項目	確認日	目標日	備考
	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。	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。(医療情報システム全般)・・・「はい」



EMシステムズ製品の医療情報セキュリティ開示書(MDS/SDS)は、

弊社運営サイト「EM-AVALON」の マイページ(My AVALON)からダウンロードできます。

【未更新】R8.8月時点
医療情報セキュリティ開示書

JAHIS「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」ガイドVer.5.0(第6.0版対応)未更新のため

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
サービス事業者による医療情報セキュリティ開示書 (医療情報システムの安全管理に関するガイドライン第5.2版対応)																					回答欄	
作 成 日																						
サービス事業者																						
サービス名称																						
バージョン																						
本書書を作成したJAHES/JARAは、製品設計・保守・提供等の認証・試験・検査等を行っています。また、特定の医療機関等における特定の目的・ニーズを満たすため、あるいは他の医療機関等と共有・提供されるものがあるため、この書面の記入内容は、記入した製品製造者/サービス事業者が責任を負います。																						
診療情報と診療情報以外を外部に提供することの要否																						
診療情報と診療情報以外の外部に提供を受けるかどうか？ (6.3)																					該当する場合 備考 -	
1. 1. 保存場所が病院、診療所、医療法人等が設置・管理する場所の場合、安全管理ガイドラインで示された規定に基づいて診療情報の提供を受けるかどうか？ (6.3.C.1)～(6.3.C.2)																					はい いいえ 対象外 備考 -	
2. 2. 保存場所が「医療機関等以外の関係者」として特定した個人や企業・安全な場所の場合、安全管理ガイドラインで示された規定に基づいて情報の提供を受けるかどうか？ (6.3.C.2)～(6.3.D)																					はい いいえ 対象外 備考 -	
医療機関等における情報セキュリティマネジメントシステム (ISMS) の実施 (6.2)																						
医療情報のシステムを医療機関等に請求できるかどうか？ (6.2.C)																					はい いいえ 対象外 備考 -	
組織別の安全管理対策 (体制、運用管理規程) (6.3)																						
医療情報システムを運用する間に、医療情報システムを安全管理責任者が管理しているかどうか？ (6.3.C.1)																					はい いいえ 対象外 備考 -	
医療情報システムを運用する間に、運用担当者を選任しているかどうか？ (6.3.C.1)																					はい いいえ 対象外 備考 -	
個人情報等「他機関等」に対しては、上述の管理のルールを定めているかどうか？ (6.3.C.2)																					はい いいえ 対象外 備考 -	
情報システムのアクセス記録、記録、点検等を実施して安全管理措置を行っているかどうか？ (6.3.C.3)																					はい いいえ 対象外 備考 -	
情報システムの契約に安全管理に関する条項を含んでいるかどうか？ (6.3.C.4)																					はい いいえ 対象外 備考 -	
個人情報を含む医療情報システムを開発してサービス事業者が提供する場合、その外で委託先の契約に再委託先を含む安全管理に関する条項を含んでいるかどうか？ (6.3.C.4)																					はい いいえ 対象外 備考 -	
運用管理規程において医療情報の安全管理対策に関する事項を定めているかどうか？ (6.3.C.5)																					はい いいえ 対象外 備考 -	
組織別の安全管理対策 (6.4)																						
使 用 予 定																					SDSチェックリスト	
SDSチェックリスト																					MDSチェックリスト (6版対応)	
SDSチェックリスト (6版対応)																					SDSチェックリスト (6版対応)	

【2医療情報システムの管理・運用】

アクセス利用権限・不要なアカウントの削除

	チェック項目	確認日	目標日	備考
	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	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または無効化している。	はい・いいえ (/)	(/)	

アクセス権限を設定して台帳等で管理し、不要アカウントがないことを確認したら上記 2項目・・・「はい」

事業者確認用チェックリストにおいては、「対象外」(保守契約範囲外)としてご案内しているため、誰が、どの部署が、情報にアクセスする権限があるのかを確認、設定、規程化してください。

また、管理者権限を付与するアカウントは最低限のユーザーに付与することを徹底するようにしてください。

※ 退職者や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。

※ 利用者ごとにアカウント・アクセス権限を設定する必要があります。(同一アカウント使用NG)



弊社システムの場合、システム上でアカウントごとにアクセス利用権限を管理・運用ができます。
(弊社にてひな形は準備しております。)

●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

	チェック項目	確認日	目標日	備考
	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。	はい・いいえ (/)	(/)	

ESET等の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、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、Windows UpdateなどOSの更新プログラムを適用して…「はい」

できる限り、最新のソフトウェア更新します。サポート内ソフトウェアであることは必須です。



EMシステムズではESETをご提供しています。

インターネットに接続していない PCは、Windows UpdateなどOSの更新がされませんのでご注意ください。

	チェック項目	確認日	目標日	備考
	⑦パスワードは英数字の混在した8桁以上としている。※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	はい・いいえ (/)	(/)	

情報機器の起動時パスワードを確認・設定して… 「はい」

情報機器ではパスワード設定が必要ですが、特に端末PC、サーバ、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場合には、サイバー攻撃の起点となってしまいます。**必ず英数字、記号等が混在しており、13文字以上であるパスワードを設定してください。**

(パスワードを機器、端末、モニター等に貼り付けすることはNGです)

 システム管理では、パスワードは重要になりますので、油断せず
きちんと設定するようにしてください。

企 Q-44 「医療情報システムで利用する認証方法が安全なものとなるよう」にするために、どのようなリスクを想定すればよいか。

A 利用者の識別・認証に用いられる情報が第三者に漏れないように以下のようなリスクに対処することが想定されます。

- ・ ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- ・ パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- ・ 初期設定のパスワードが変更されておらず、利用者以外の者でもシステムにログインできてしまう。
- ・ 代行作業等のために ID・パスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- ・ **一つの ID を複数の利用者が使用している。**
- ・ 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- ・ 安全性が高くないパスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- ・ 認証用の個人識別情報を格納するセキュリティ・デバイス(IC カード、USB キー等)を他人に貸与する、又は持ち主に無断で借用することにより、利用者が特定できない。
- ・ 退職した職員の ID が有効になったままで、ログインができてしまう。
- ・ 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- ・ 不正ソフトウェアにより、ID やパスワードが盗まれ、悪用される。

出展：厚生省「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」に関する Q&A より抜粋
(<https://www.mhlw.go.jp/content/10808000/001145860.pdf>)

	チェック項目	確認日	目標日	備考
	⑧パスワードの使い回しを禁止している。	はい・いいえ (/)	(/)	

情報機器の起動時パスワードを確認・設定して… 「はい」

安易なパスワードを設定しており、さらにクリニックおよび薬局内の情報機器において、1つのパスワードをそのまま使いまわしてしまっていた場合、非常に危険です。

仮に第三者がその点を把握・悪用するとすべての機器へのアクセスが可能となり、危険にさらされてしまいます。**必ず情報機器ごとに異なるパスワードを設定するようにしてください。**



当社システム導入後、速やかに操作される方ごとにパスワードをそれぞれ設定していただくようお願いいたします。

○パスワードを強固なものに変更し、使い回しをしない

VPN 装置等の ID・パスワードの漏洩は、システムへの侵入に直結し、医療機関等にとって重大なリスクとなります。実際にこれまで攻撃を受けた医療機関では、パスワードが容易に推測可能なものであったり、4 桁と短かった例が確認されています。被害を未然に防ぐためには、強固な ID・パスワード設定の徹底が必要です。

また、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も重要です。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しうるため、非常に危険です。

＜危険な ID/パスワードの例＞

- Administrator（工場出荷時の設定等）
- 12345678（単純な羅列）
- pa\$\$w0rd、i234567&9（単純な置換、流出済）
- qwerty、7410（キーボードの配列）
- KoroHospital、KoroTaro（予測可能、施設の名称、代表者名など）

＜強固なパスワードとは＞

- 長く、複雑で、推測困難なものが推奨されます。
- 13 桁以上（桁数が多いほど、機械的な総当たりでの解析が困難）
- 英数字、大文字・小文字、記号が混在（組み合わせが多いほど解析が困難）
- ランダムな文字列（単語等の組み合わせによる解析を回避）

出展：厚労省「医療機関等におけるサイバーセキュリティ対策の取組みについて」より抜粋
(<https://www.mhlw.go.jp/content/10808000/001283914.pdf>)

13 【2医療情報システムの管理・運用】 外部記録媒体・情報機器の制限

	チェック項目	確認日	目標日	備考
	⑨USB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。	はい・いいえ (/)	(/)	

USBストレージ等の外部記録媒体を利用しないようにしている (制限している)ことを確認して・・・「はい」

事業者確認用チェックリストにおいては、「対象外」(保守契約範囲外)としてご案内しており、USBストレージ等は、媒体の紛失やデータの盗難、USBを経由して端末PCやサーバに不正ソフトウェアが侵入するなどのリスク起因になります。具体的な制限ルールや対策としては、下記の手法をご検討ください。

	対応方法	対応ツール／具体的手法
①最低限	利用を運用で制限	- 医療情報の持ち出しが可能となる記録媒体、情報機器等の利用を限定する。 - 運用管理規定に医療情報の持ち出しに関するルールを設けて、手続きをしないと持ち出せないようにする。 - 記録媒体、情報機器等を持ち帰った場合、それらの確認に関するルールや手続きを決める。
②標準	接続制限を端末個別に設定	【有料】ESETやMicrosoft Defender for Endpointなどのセキュリティソフトを使用し、デバイス制御を行う。 【無料】Windows11pro→グループポリシーで「リムーバブル記憶領域へのアクセス」を拒否に設定。
③組織的対応	資産管理ツール	SKY-SEAやDefender for Endpoint + Intuneなど * 資産管理ツールを使用することで、多様な管理が可能 - デバイス、メディアごとに使用制限を設定し集中管理(1台ずつ適切に管理、細やかに使用制限を設定) - IT資産棚卸で守るべき対象を明確化(2-①台帳管理)、脆弱性の把握、不正ソフト検出など - セキュリティインシデント対応の迅速化(感染端末特定、影響範囲分析、隔離指示など)



レセコン、電子薬歴では、USBストレージ等の利用は**原則禁止**とすることをお勧めいたします。

14【2医療情報システムの管理・運用】 不要なソフトウェア・サービスの停

	チェック項目	確認日	目標日	備考
	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。	はい・いいえ (/)	(/)	

※ サーバ、端末PCそれぞれにて確認・対応が必要となります。

Windowsの設定やタスクマネージャーなどから不要なソフトウェアが動いていないか確認し、不要なソフトウェアがあった場合は停 ☐ して…「はい」

<Windows 設定画面>

不要なソフトウェアはオフにする

アプリ

インストールされているアプリ
PC上のアプリのアンインストールと管理

アプリの詳細設定
アプリの取得、アプリのアーカイブ、更新プログラムのアンインストールを行う場所を選択します

既定のアプリ
ファイルの既定値、リンク種類の既定値、その他の既定値

アクション
Windowsでは、これらのアプリからのアクションを推薦できます。

オフラインマップ
ダウンロード、保存場所、マップ更新

Webサイト用のアプリ
ブラウザではなくアプリで開くことができるwebサイト

ビデオの再生
ビデオ調整、HDRストリーミング、バッテリーオプション

スタートアップ
サインイン時に自動的に開始されるアプリ

再開
デバイス間で作業を移行する

アプリ > インストールされているアプリ

アプリの検索

94個のアプリが見つかりました

3Dビューアー
Microsoft Corporation | 2026/02/13

7-Zip 22.01 (x64)
22.01 | Igor Pavlov | 2025/08/22

Adobe Acrobat (64-bit)
26.001.21771 | Adobe | 2026/08/03

詳細オプション
移動
アンインストール

アプリ > インストールされているアプリ > 3Dビューアー

仕様

発行元
Microsoft Corporation

バージョン
7.2602.8012.0

アプリ
0バイト

データ
16.0KB

合計使用量
16.0KB

バックグラウンドアプリのアクセス許可

常にオン
電力最適化(推奨)
常にオフ

令和8年度版
変更項目

	チェック項目	確認日	目標日	備考
2 医療情報シ ステムの管理・	端末について、以下を実施している。			
	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。または令和9年度以降初回のシステム更改時に実装予定である。	はい・いいえ (☐ / ☐)	(☐ / ☐)	
	サーバについて、以下を実施している。			
	⑫OSログイン時の二要素認証を実装している。または令和9年度以降初回のシステム更改時に実装予定である。	はい・いいえ (☐ / ☐)	(☐ / ☐)	

医療情報システムに対して「二要素認証」が実装、もしくは実装予定としていることを確認して… 「はい」

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が必要となります。

- 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
- サーバ二要素認証の「みなし措置」

サーバ本体への二要素認証導入が難しい場合、安全な「踏み台パソコン」を経由させることで導入済とみなすことができます。
具体的には「踏み台側での二要素認証」または「踏み台での異常検知+外部からのVPN接続」のどちらかを設定すれば対象となります。
(前提条件:「踏み台への管理者権限を与えない」「OSを最新に保つ」「パスワードを使い回さない」が適用されている)



弊社システムでは、令和9年度までの実装に向けて検討・準備中のため、詳細については、決まりましたらご案内させていただきます。

	チェック項目	確認日	目標日	備考
2 医療情報シス	⑬アクセスログを管理している。	はい・いいえ (/)	(/)	

事業者にアクセスログの管理方法を確認 →定期的に確認したら・・・「はい」

「アクセスログ」とは、PCやサーバまたはアプリケーションやデータへの接続履歴のことです。

医療情報システムに不正なアクセスや操作が無いかログを確認し、追跡できる状況であれば、「はい」を選択して問題ありません。

アクセスログリストなどを作成し、どのようなアクセスログが取れているのかを整理し、組織としての管理体制の確 固を目指しましょう。

※ 退職者や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。

※ 利用者ごとにアカウント・アクセス権限を設定する必要があります。(同一アカウント使用はNG)



弊社システムの場合、システム上にてアクセスログを確認、CSV出力できます。

	チェック項目	確認日	目標日	備考
2 医療情報シス	⑭接続元制限を実施している。	(はい・いいえ (☐ / ☐)	(☐ / ☐)	

接続元制限を実施して・・・「はい」

事業者確認用チェックリストにおいては、「対象外」(保守契約範囲外)としてご案内しているため、下記の手法をご検討ください。

＜実施例＞(ネットワーク機器)

- ・ 無線LANのセキュリティ対策を行う
- ・ ファイアウォールなどを用いて、接続できるIPアドレスを制限する
- ・ 特定の地域(国内)のアドレスからしかアクセスできないようにする。

	行うべき無線LANのセキュリティ対策
1	最新のセキュリティ規格を使用する
2	SSIDを外部からわかりにくくする
3	SSIDのステルス機能を利用
4	初期設定のID・パスワードは必ず変更する
5	ファームウェアは常に最新版に
6	MACアドレス認証を利用する

 弊社システムをご利用中のお客様では、「ホワイトリスト方式」※を採用しており、弊社が管理しているホワイトリストに未登録先については、アクセスできないように制限をかけております。(オフライン環境は除く)

※ ホワイトリスト方式:

事前に『安全なWEBサイト』を定義したWEBのフィルタリングサービスとなります。弊社とサービス提供元ベンダーであるNTTPCコミュニケーション社で協議決定したポリシーにもとづき、安全性が高いと判断したWEBサイトのみアクセス許可します。

18【3インシデント発生に備えた対応】 連絡体制図・外部連絡リストの作成

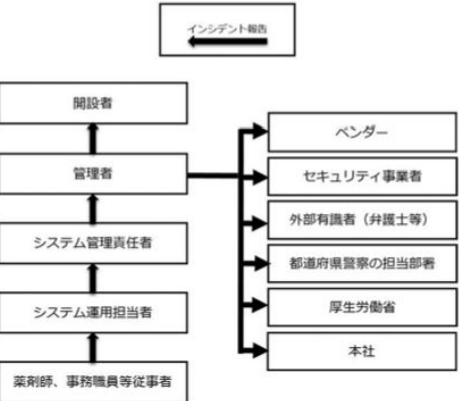
	チェック項目	確認日	目標日	備考
3	①インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ (☐ / ☐)	(☐ / ☐)	

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、外部連絡リストを作成して…「はい」



「連絡体制図」と「外部連絡リスト」のひな形をご用意しました。 EMシステムズ製品をご利用のお客様は、弊社運営サイト「EM-AVALON」の マイページ(My AVALON)からダウンロードできます。

●連絡体制図の例 2（薬局）



【外部連絡リスト】				
No	カテゴリ	組織名	担当者名	電話番号
1	公的機関	** 警察		
2		厚生労働省		
3	事業者	A社		
4		B社		
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・



EM-AVALON マイページ(MyAVALON)

<https://em-avalon.jp/login?r=yes>

- ※ 弊社システムをご利用中のお客様限定となります。
- ※ ログインには、「EMお客様コード」、「ログインID」、「パスワード」が必要となります。

19【3インシデント発生に備えた対応】 インシデント時の対応準備

	チェック項目	確認日	目標日	備考
3 インシデント	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、バックアップを確保のうえ、復旧手順を確認している。	はい・いいえ (/)	(/)	

インシデント(予期しない出来事や問題、事故など)が発生した際のデータ・システムバックアップ
および復旧手順を確認して・・・「はい」

通常の日時バックアップだけでなく、非常時のデータ保存、システムバックアップ手順やマニュアルを準備しておきましょう。
また、システムの復旧が必要な際にきちんと対応できるように事前に設定、手順の把握をするようにしましょう。



弊社システムごとに運営サイト「EM-AVALON」の
マイページ(My AVALON)へログインしていただく
ことで、必要書類等をダウンロード可能です。



EM-AVALON マイページ(MyAVALON)

<https://em-avalon.jp/login?r=yes>

- ※ 弊社システムをご利用中のお客様限定となります。
- ※ ログインには、「EMお客様コード」、「ログインID」、「パスワード」が必要となります。

20 【3インシデント発生に備えた対応】 サイバー攻撃を想定した BCP対策

	チェック項目	確認日	目標日	備考
3 インシデント	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。	はい・いいえ (/)	(/)	

実際のサイバー攻撃を受けた際の業務継続の判断基準や意思決定を事前に検討した上で・・・「はい」

現在は、大きな病院だけでなくクリニック、薬局もサイバー攻撃の対象となり、実際に攻撃を受ける事件も発生しています。防止する対策はもちろんのこと、実際にサイバー攻撃を受けた際にどのように対処するかを検討する・検討しないでその場での対応が大きく異なってきます。この点も考慮し、業務を継続できる計画（BCP）を策定して備えておきましょう。



弊社システムごとに運営サイト「EM-AVALON」のマイページ(My AVALON)へログインしていただくことで、BCPひな形をダウンロード可能です。



EM-AVALON マイページ(MyAVALON)

<https://em-avalon.jp/login?r=yes>

- ※ 弊社システムをご利用中のお客様限定となります。
- ※ ログインには、「EMお客様コード」、「ログインID」、「パスワード」が必要となります。

	チェック項目	確認日	目標日	備考
4 規程類の整備	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。	はい・いいえ (/)	(/)	

ガイドラインで定められている運用管理規定の中で具体的実施方法等を記載・更新して… 「はい」

現在クリニック、薬局内にて管理されている「運用管理規定」では、サイバーセキュリティ対策に関連してきちんと具体的実施方法等の更新をしておく必要があります。クリニック、薬局に合わせた運用方法を検討して、記載しておくようにしましょう。



弊社システムごとに運営サイト「EM-AVALON」のマイページ(My AVALON)へログインしていただくことで、運用管理規定(ひな形)をダウンロード可能です。



EM-AVALON マイページ(MyAVALON)

<https://em-avalon.jp/login?r=yes>

※ 弊社システムをご利用中のお客様限定となります。

※ ログインには、「EMお客様コード」、「ログインID」、「パスワード」が必要となります。

医療機関・薬局が 対応すべきこと

専門的知識も一部必要となるため、まずはご利用中のベンダーへお問い合わせ、ご相談ください。サイバーセキュリティ対策は“義務化”となっており、継続した対応が求められてきます。

01



現在の環境を確認する

ガイドライン第7.0版の内容を参考としつつ、「サイバーセキュリティ対策チェックリスト」を用いて現在の環境の把握を行います。チェックリスト上で、何ができていないかをまずは明確にしてください。

02



チェックリスト上未対応箇所への 対応措置を取る

チェックリストに基づいて項目内容で対応の不足があれば、対応措置が必要となります。チェックリストについては、専用のマニュアルにて各項目を詳しく解説していますので、参考としてください。

03



必要書類を準備する (ベンダーより入手する)

チェックリストに基づいて現在、お客様がご利用中の電子カルテ・電子薬歴・レセコン等のベンダーより必要書類の入手を行い、管理をしておく必要があります。(運用管理規程ひな型、サービス仕様適合開示書 など)

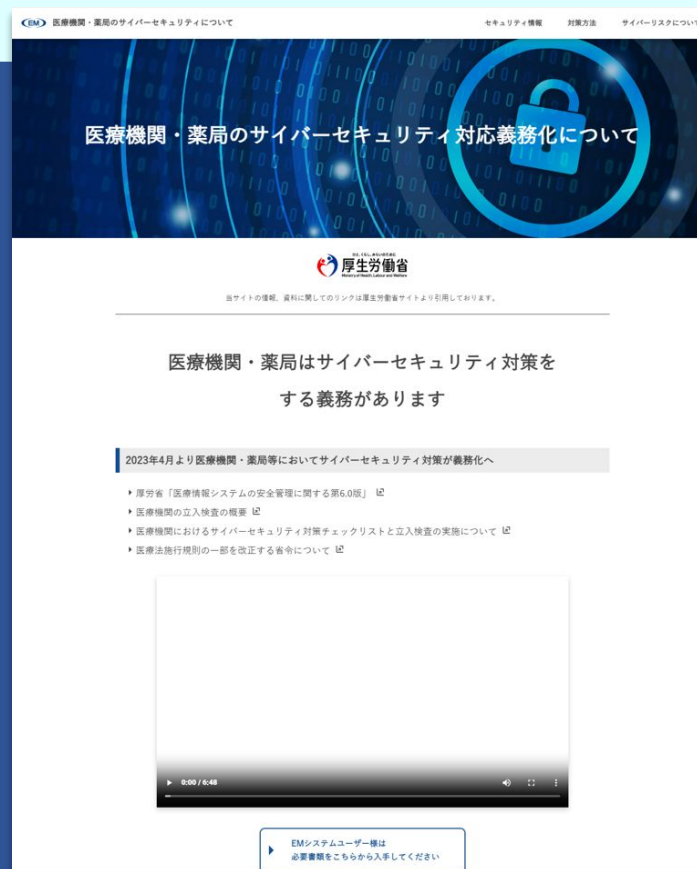
サイバーセキュリティサイト開設のご案内

弊社運営サイト「EM-AVALON」にてサイバーセキュリティサイトを開設いたしました。（下記リンク先よりアクセスしてください。）



EM-AVALON

<https://em-avalon.jp>



サイバーセキュリティサイト

弊社システムをご利用中のお客様限定として、EM-AVALONサイトのマイページ(MyAVALON)へアクセスしていただければ、必要資料がダウンロード可能です。



EM-AVALON マイページ (MyAVALON)

<https://em-avalon.jp/login?r=yes>

- ※ 弊社システムをご利用中のお客様限定となります。
- ※ ログインには、「EMお客様コード」、「ログイン ID」、「パスワード」が必要となります。

必要資料のダウンロード

「サービス仕様適合開示書」、「サイバーセキュリティ対策チェックリスト(ひな形)」、「医療情報セキュリティ開示書(MDS/SDS)」、「運用管理規程ひな型(ガイドライン第7.0版反映)」

【参考情報】

厚労省サイト・各種資料

- ・ 医療情報システムの安全管理に関するガイドライン 第 7.0版(令和 8年6月)
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
- ・ 医療情報システムの安全管理に関するガイドライン第 7.0版の概要および主な改定内容
<https://www.mhlw.go.jp/content/10808000/001102596.pdf>
- ・ 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(令和 8年6月)
<https://www.mhlw.go.jp/content/10808000/001716185.pdf>
- ・ 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～(令和 8年6月)
<https://www.mhlw.go.jp/content/10808000/001716186.pdf>
- ・ 医療分野のサイバーセキュリティ対策について
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/cyber-security.html

