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

保守委託機関編

目次

【はじめに】

現代では、多くの分野で ICT 技術が普及し、業務の効率化、正確性の向上、従来にない付加価値の提供等に活用されている。医療分野においても同様で、医療情報を適切に利用、管理するために、医療情報システムが活用されている。

一方で、ICT を活用したシステムに対しては、様々なリスクがある。特に医療分野においては**医療情報の漏えいや破壊は、患者の生命、身体に対する侵害、医療業務の継続性を損なうリスク**もあり、適切な対策を講じることが求められる。この対策を示すために、「医療情報システムに関する安全管理ガイドライン」（以下「安全管理ガイドライン」という）が策定されている。

安全管理ガイドラインでは、医療情報システムを取扱う組織や人、システムに対する対応策を網羅的に示している。特にシステム担当者に対しては、年を追うごとに専門的な知識を要する対応が求められてきた。医療情報システムの開発や導入、運用は、医療情報システム・サービス事業者[1]（以下「事業者」という）への委託がますます増加しており、特に、**専任のシステム担当者が不在の医療機関等においては、利用する医療情報システムのほとんどの管理を、外部の事業者に委ねることが通常**と言える状況にある。

このような医療機関等においては、システム運用編を含めた安全管理ガイドラインのすべてを詳細に理解し、対応することが困難となっている。これを踏まえ、**医療機関等の管理者は、事業者の選定、契約内容の確認、事業者が行う導入や運用の管理監督**などの形で技術的な対策を実施することが期待される。特にクラウドサービスの中でも **SaaS（Software as a Service）を利用することでセキュリティアップデートを含めた保守管理を完全に事業者に委託**することも可能となっている。

今般、このような実態を踏まえて、安全管理ガイドラインに示す対策（遵守事項)のうち、主に下記のような小規模医療機関等を想定し、対策の必要な項目一覧を示す事とした。ただし、実際の対象については図１（p3）を参照して判断すること。

・システム運用担当者が不在

・小規模で、経営管理と企画管理の部門が区別されていない

・セキュリティアップデートを含めたシステム保守を十分に事業者に委託している

（積極的な SaaS の活用や、保守契約による委託が想定される。）

本編では、医療機関等が自ら実施すべき遵守事項を端的にまとめた。特に**「システム運用編」における事項については、MDS/SDS を用いて機器、サービスのセキュリティ対応状況を確認することで、遵守事項に対応されたものとみなす。**

これらの対応によって、専任のシステム担当者が不在の医療機関等においても、クラウドサービスの積局極的な活用により、十分なセキュリティ対応が可能となることを目指している。

---

[1] 医療情報システムの製造、開発、販売及び保守を行う事業者や、医療情報システムを活用したサービスの提供、保守等を行う事業者など、医療機関等が医療情報システムを利用・管理する上で関係する事業者全般を想定する。

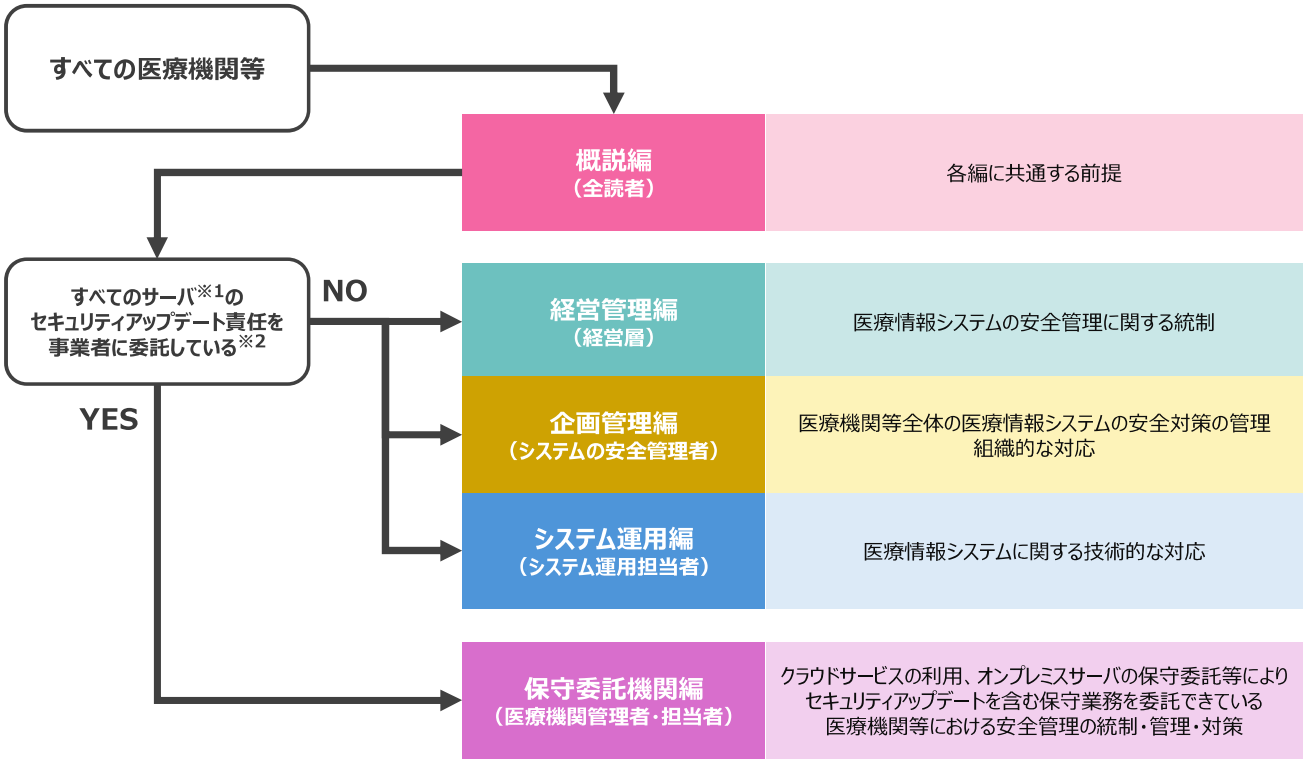
1．本編の対象

保守委託機関編（以下、本編という）では、下図 1 のフローチャートにおいて、「すべてのサーバのセキュリティアップデート責任を事業者に委託している」で「YES」を選んだ医療機関等を対象とする。

具体的には、クラウド型電子カルテ（SaaS 型）等のクラウドサービスの採用や、オンプレミスのサービス利用においても契約の中で、すべての医療情報システムのセキュリティアップデートを含む保守を外部の事業者に委託していることを想定している。なお、本編の適用対象となる医療機関等は、以下「保守委託機関」と呼ぶ。

SaaS への移行が容易な小規模医療機関等が主な対象となることを想定している。

- フローチャートの YES または NO の判断の際に不明点があれば、必ず当該事業者に確認をすること。



※1：ここでいう「サーバ」は、医療情報の保存や主要な処理を担う機器を指す。原則としてPCやタブレット等のクライアント端末は含まない。
ただし、電子カルテアプリ等を端末にインストールし、当該機器上で処理が完結する場合はPC等の端末も「サーバ」に含む。
※2：「事業者がセキュリティアップデート責任を負うこと」が、契約書や約款、サービスレベル合意書等に記載されている場合にのみ「YES」を選択可能となる。
記載がない場合や不明確な場合には医療機関側の責任となっている可能性がある。不明確な場合は必ず契約事業者に直接確認し、責任の所在を明確にすること。

図 1 本編の対象となる医療機関等の判断フローチャート

2. 保守委託機関における遵守項目

※遵守項目の内容は医療機関等が運用管理規程等を作成する際に含めるべき項目

項目区分	遵守項目	チェック
1．安全管理に関する責任･責務		
1.1 安全管理に関する法令の遵守	①法令上求められる要件（個人情報保護法[2]、e-文書法[3]等）について、必要な技術的対応、手順、資料の作成を行うこと。または、事業者に提出させて、その内容を確認すること。	□
1.2 医療機関等における責任	①通常時における責任：医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。	□
	②非常時における責任：非常時における業務継続の可否の判断基準等を検討し、BCP（Business Continuity Plan:業務継続計画）を整備すること。	□
1.3 委託における責任	①事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。	□
1.4 第三者提供における責任	①医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。	□
	②医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、書面等により可視化し、適切に管理すること。	□
2．責任分界		
	①医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。	□
	②委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム･サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。	□
	③委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。	□
3．リスクマネジメント（リスク管理）		
	①医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。	□
	②事業者から技術的対策等の情報（サービス仕様適合開示書、	□

[2] 個人情報の保護に関する法律（平成 15 年法律第 57 号）

[3] 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（平成 16 年法律第 149 号）

項目区分	遵守項目	チェック
	MDS/SDS[4]等）を収集すること。	
４．安全管理全般（統制、設計、管理等）		
4.1 統制	①統制の実効性を確保するために必要な規程類、管理体制等を整備すること。	□
	②医療情報システム安全管理責任者を設置すること。	□
4.2 設計	①リスク評価及びリスク管理方針を踏まえて、下記を整備すること -情報セキュリティ方針 -医療情報の取扱いや保護に関する方針 -医療情報システムの安全管理に関する方針	□
	②情報の重要度や患者ごとの識別を踏まえ、情報を適切に管理するための手順等を作成・運用すること。	□
	③必要に応じて、説明責任等を果たせるように、法令で求められる医療情報の取扱いに関する証跡を管理すること。	□
	④医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。	□
4.3 安全管理対策の点検	①定期的に安全管理対策の自己点検を行い、必要に応じて改善に向けた対応を指示すること。 また、自己点検に加え、必要に応じて外部監査を実施すること。	□
５．安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）		
	①医療情報を取り扱う職員を採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含めること。	□
	②個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。	□
	③外部保存の委託先事業者選定の際は、プライバシーマーク[5]、ISMS[6]又はこれと同等の規格の認証を受けている事業者を選定すること。	□

[4] Manufacture/Service Provider Disclosure Statement for Medical Information Security（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）

[5] プライバシーマークは、「個人情報を適切に管理している」と評価された事業者が使用できるマークを指す。JIS Q 15001 に基づく。

[6] ISMS とは、「情報セキュリティマネジメントシステム（Information Security Management System）」の意味で、情報セキュリティのリスクを管理する仕組みを指す。ISO/JIS 27001 に基づく。

項目区分	遵守項目	チェック
	また、安全管理方針、体制、バックアップ状況、信用度、認証（ISMAP[7]や、プライバシーマーク、ISMS 等）の取得状況、保存場所を確認し、情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること。	
	④医療情報の外部保存の委託先事業者との契約に、下記を含むことを事業者に確認すること。 -事業者が安全管理ガイドラインと「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省、経済産業省）を遵守すること -許可なく分析する等の、目的外利用をさせないこと -匿名化情報の取扱いの配慮 -患者アクセス時の権限設定 -情報提供は原則患者同意に基づくこと -再委託を行う場合は、事前に医療機関等に情報を提供し、承認を得ること。 -委託契約終了に際しての医療情報の返却とその方法の取り決め。 -サーバのセキュリティアップデートを含む保守責任が事業者にあること -PC やネットワーク機器等、端末の保守責任が医療機関等と事業者のいずれにあるか	□
	⑤必要に応じて個人情報が特定の外部の施設に送付・保存されること、またその安全性やリスクを含めて院内掲示等を通じて説明すること。	□
6．情報管理（管理、持ち出し、破棄等）		
	①医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順を含む規程を定めること。	□
	②医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順を定めること。	□
	③医療情報の破棄に関する手順等を定める際は、情報種別ごとに手順（条件、担当者、具体的な方法）を定めること。	□
7．医療情報システムに用いる情報機器等の資産管理		
	①医療情報システムの資産管理を行うために必要な規程類を整備すること。	□
	②整備された規程に基づいて医療情報システムの台帳管理を行うこと。	□
	③医療情報システムは、可能な限りクラウドサービスを選定し、ソフトウェアアップ	□

[7] ISMAP は「Information system Security Management and Assessment Program」の略称で、「政府情報システムのためのセキュリティ評価制度」と呼ばれる。クラウドサービスに関して、高水準のセキュリティ要件を政府が設定しており、同様に高いセキュリティが求められる情報システムの評価にも利用される。

項目区分	遵守項目	チェック
	デート等の保守管理を事業者に委託すること。 （困難な場合は医療機関等自ら、定期的なアップデートを要する。）	
	④盗難・紛失時の対応手順を作成し、事前対策を講じること。	□
	⑤BYOD[8]端末の利用について、利用許諾条件や管理方法等を規程に含め、台帳管理を行うこと。	□
	⑥IoT 機器を患者へ貸し出す際は、リスク説明と同意取得、連絡先提供を行うこと。	□
８．サイバーセキュリティ		
	①インシデント発生時は、ネットワーク切断、機器隔離、システム停止、バックアップからの復元（複数方式・数世代確保、オフライン管理等が重要）などを行うこと。	□
	②サイバー攻撃等により医療提供体制に支障が生じるおそれがある場合は、厚生労働省、都道府県警察、その他の所管官庁等への連絡を行うこと。	□
	③接続サービスのセキュリティ確保の範囲を事業者に確認すること。	□
９．医療情報システムの利用者に関する認証等及び権限		
	①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すること。特に、管理者権限を与えるアカウントは最低限のユーザとすること。	□
	②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すること。	□
	③電子カルテにおける記録の確定（入力者・確定者の識別、確定手順、更新履歴、代行入力等）に関して、真正性、見読性、保存性の確保が可能なシステムを選定し、必要なルールを規程等に含めること。	□
	④クライアント端末のアプリケーションログイン時には、令和９年度までに二要素認証を採用すること。対応が困難な場合には、令和９年度以降のシステム更新時に対応可能な事業者を選定すること。	□
	⑤オンプレミスのサーバが院内に存在する場合はOS（Operating System）のログイン時に二要素認証を採用すること。対応が困難な場合には、令和９年度以降のシステム更新時に対応可能な事業者を選定すること。	□
１０．技術的な安全管理対策の管理		
	①サーバルーム等のセキュリティ境界への入退室管理（施錠、識別、記録）を行うこと。	□
	②離席時の不正利用防止対策（画面ロック等）を実施すること。	□
	③記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、周知徹底・教育を実施すること。	□

[8] BYOD は「Bring Your Own Device」の略称で、業務において個人所有の情報機器を利用することを指す。

項目区分	遵守項目	チェック
	④全体構成図（ネットワーク・システム構成図）及び関係者一覧を作成し、変更が生じた際には速やかに反映すること。	□
	⑤医療機関等が用いる端末、ネットワーク機器については、医療機関等の責任で脆弱性対応（セキュリティパッチへの対応、マルウェア対策ソフトのパターンファイルの更新、ネットワーク機器のファームウェアの更新等）を行うこと。これらの対応を事業者に委託する場合には、委託内容・範囲を明確にすること。	□
	⑥医療機関等で利用する IoT 機器のリスク分析・評価のうえ、ファームウェア等のアップデートを行い、使用終了時には接続解除をすること。	□
	⑦利用者の ID の台帳管理、棚卸し、削除手順を作成すること。	□
	⑧パフォーマンス管理、死活監視については、事業者に対する委託契約に含まれる SLA[9]において明確にすること。	□
	⑨医療情報システムを導入する際には、事業者に MDS/SDS の提出を求め、本編【別紙】に示す部分について、「はい」または「対象外」であることを確認すること。	□
	⑩汎用的な医療情報システムについて、委託等を行わずに導入したシステム・サービス等（PC 等の端末やネットワーク機器を除く）を利用する場合は、システム運用編における遵守事項への対応を行うこと。	□
１１．法令で定められた記名・押印のための電子署名、紙媒体等で作成した医療情報の電子化		
	①「法令で定められた記名・押印のための電子署名、紙媒体等で作成した医療情報の電子化」を導入する場合には、法令等に従ったシステム・サービスの導入をすること。	□
	②導入にあたっては提供する事業者に対して、法令等に適合していることを確認すること。	□

[9] SLA （Service Level Agreement）とは、事業者が提供するサービスの内容と提供水準について委託者と受託者が合意した文書のことを指す。保守等の委託契約のほか、クラウドサービスの提供などに用いられる。

3．遵守項目解説

1．安全管理に関する責任・責務

1.1　安全管理に関する法令の遵守

① 法令上求められる要件（個人情報保護法、e-文書法等）について、必要な技術的対応、手順、資料の作成を行うこと。または、事業者等に提出させて、その内容を確認すること。

■ 「事業者等」には、医療情報システムで用いるネットワーク等の構築、機器の設置、サービスなどを提供する事業者に加え、端末（PC、タブレット等）やネットワーク機器の保守・運用を受託する事業者も含まれる。

■ 法令上求められる要件に必要な技術的対応、資料等は、委託先事業者に提出させることも十分想定される。MDS/SDS（厚生労働省標準規格 HS040「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」ガイドで示されているチェックリスト）[10]の提出を事業者に求め、項目の適合性を確認すること。

1.2　医療機関等における責任

① 通常時における責任：医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。

② 非常時における責任：非常時における業務継続の可否の判断基準等を検討し、BCP（Business Continuity Plan：業務継続計画）を整備すること。

■ 非常時（システム障害、災害、サイバー攻撃の発生）に、その内容に応じて、診療行為の継続や、医療情報システムの利用の継続等の判断を行うための基準を平常時から用意すること。これに基づいて、検知、封じ込め、復旧などの段階に応じた BCP を策定することを想定する。

■ 例えば短時間のシステム障害であれば、一時的に医療情報システムの利用を控えて他の手段により、診療行為を継続する、回復に数日以上を要する場合には、診療を縮小する、紙を用いた対応に切り替える、などの判断基準と対応策を整理すること。

1.3 委託における責任

① 業務の一部等を事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。

■ 専任のシステム担当者が不在の医療機関等においては、技術的仕様について、事業者から MDS/SDS 等の提出を受け、本編末尾の【別紙】に示す内容の適合性を確認することで、適切な

[10] MDS/SDS は Manufacture/Service Provider Disclosure Statement for Medical Information Security の略で、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を指す。具体的には「「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」の概要」（厚生労働省）を参照。

事業者選定と管理を行うこと。

1.4 第三者提供における責任

① 医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。

② 医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、書面等により可視化し、適切に管理すること。

■ 医療情報を第三者提供する場合については、個人情報保護法及びこれに関連するガイドライン、ガイダンスを踏まえた対応をすることが想定される。
特に委託先との関係では、医療情報の第三者提供に該当する場合と該当しない場合について、同意取得を含む適切な手続きを行うことが求められる。

■ また医療機関等の間でネットワークを通じて医療情報の授受を行う場合には、両者の責任範囲を明確にすること。原則として、PC や VPN 装置を含むネットワーク機器等のアップデート対応を事業者側の保守範囲として契約書に含むこととし、そのような対応が可能な事業者を選定することが望ましい。困難な場合は医療機関が独自にアップデート対応をする責任が生じるため、注意すること。クラウド型 VPN や自動アップデートを採用することが望ましい。

2．責任分界

① 医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。

② 委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。

③ 委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、関与する関係者への管理なども責任分界の取決めに含めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。

■ 医療情報システムの利用において、責任分界を医療機関等と事業者の間で具体的な項目に落とし込むことが重要である。特にセキュリティを含む安全管理に関しては、契約書や SLA などでも一般的な記載（例：非常時の対応は協議において決定する、等）に留まり適切な対応ができないケースが存在する。

■ VPN 機器をはじめとする外部ネットワークとの接続点となる機器については、脆弱性の管理が適切に行われず、サイバー攻撃の起点となる事案が頻発している。脆弱性の管理等について保守契約の範囲を明確にし、確実に管理可能な体制を整備すること。原則として、脆弱性対応を事業者の保守範囲として契約に含むことを想定する。昨今のサイバー攻撃事案では、事業者側が脆弱なパスワードや、他院と共通のパスワードを使い回すことで被害に遭った事案も発生している。例えば、事業者の設定するパスワードが本ガイドラインに適合していることや、電子証明書の利用によって認

証すること等を契約書によって担保することが考えられる。

- またクラウドサービスなどの利用では、利用規約や約款で、利用の取決めを行うケースがある。この場合も、サービスに関する責任分界を意識し、【別紙】等を活用して適切なサービスを選定すること。
- 「委託先事業者等において複数の関係者が関与する場合」には、複数の委託先に関する情報を整理しておく必要がある。医療機関等で利用する医療情報システムのすべてについて、一つの事業者が取りまとめて契約する場合には、委託先事業者との間で責任分界を整理すれば足りる。
- 一方で医療機関等が複数の事業者と契約している場合には、事業者相互で、他の事業者が提供しているサービスなどを知り得ないので、医療機関側で責任分界の整理を依頼する必要がある。医療情報システムに関する導入や利用、運用等に関する委託等の状況をあらかじめ整理したうえで、各事業者と責任分界を定める(場合によっては、複数の事業者を交えて整理する)こと。具体的には下表に示すようなシステムの一覧を作成したうえで、責任分界の整理を行うことを想定する。

小規模医療機関等における医療情報システム一覧の例

導入している 医療情報システム	委託先事業者	製品名	委託業務概要
例：電子カルテシステム	××システム株式会社	○○クラウド電子カルテ	クラウドサービスの導入 クラウドサービスの運用
例：ネットワークシステム	株式会社■■通信	△△ひかり通信ネット	ネットワーク回線サービス ネットワーク接続機器導入 ネットワーク接続運用
・・・	・・・	・・・	・・・

3．リスクマネジメント（リスク管理）

① 医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。

② 事業者から技術的対策等の情報（サービス仕様適合開示書、MDS/SDS 等）を収集すること。

- 安全管理対策を施す対象を明確にするため、医療情報等のリストを作成する必要がある。この時の情報分類の粒度としては、管理方法が変化し得る単位が想定される。例えば、詳細な血液検査項目ごとに管理方法が変化することは考えにくいが、尿検査と血液検査では管理方法が変化し得る。このため、血液検査結果、放射線画像、といった粒度の情報管理が考えられる。
- 一般的に、安全管理対策は、医療機関等がリスクを踏まえて行うことになる。しかし、リスクアセスメントやその管理については、専門的な分析などが必要となるため、**本編では医療機関等において最低限実施すべきことを記載している。**特にクラウドサービスを積極的に利用することにより、リスクや脅威への対応を事業者側に委ねることが可能となるため、これを推奨する。
- 医療情報を取扱うシステムについて、事業者から技術的な安全対策の状況を整理したサービス仕

様適合開示書やMDS/SDSの提供を受け、【別紙】の事業者における遵守事項対応状況と併せて、安全性を確認することでリスク管理を行うこと。

■ 医療情報システムに関するリスクは、技術の発展や脆弱性の発見等、時間に応じて変化する。リスク管理は継続的に行うべきであり、遵守事項の対応状況についても、委託契約などに基づいて、年次などの頻度で定期的に確認する必要がある。

４．安全管理全般（統制、設計、管理等）

4.1 統制

① 統制の実効性を確保するために必要な規程類、管理体制等を整備すること。
② 医療情報システム安全管理責任者を設置すること

■ 医療情報システムの安全確保は、医療機関等における事業経営の一つに位置付けられる。小規模医療機関等においても院長や事務責任者等、経営層による統制が求められる。

■ 医療情報システム安全管理責任者は、医療情報を取扱うシステム全体の安全性の管理を担うことが想定されており、医療機関等において必ず設置すること。

■ 小規模医療機関等では院長等の経営層が医療情報システム安全管理責任者を担うことは十分想定される。各医療機関等の実態に即して、統制のための体制やルールを整理することが重要である。なお、医療従事者等を含む職員のほか、派遣社員、委託先等、医療機関等が管理する医療情報を取り扱う者のすべてが統制の対象となる。

4.2 設計

① リスク評価及びリスク管理方針を踏まえて、下記を整備すること
—情報セキュリティ方針
—医療情報の取扱いや保護に関する方針
—医療情報システムの安全管理に関する方針
② 情報の重要度や患者ごとの識別を踏まえ、情報を適切に管理するための手順等を作成・運用すること。
③ 説明責任等を果たせるよう、法令で求められる医療情報の取扱いに関する証跡を、管理すること。
④ 医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。

■ 小規模医療機関等における安全管理の設計では、システムの利用者に対する内容と、委託先事業者の管理に関する内容が重要となる。前者の設計は、各医療機関等としてのセキュリティや医療情報保護に関する方針を明確にし、ルールや運用を整理する。後者の設計では委託先事業者に委ねる内容を明確にすることが求められる。特に医療情報システム等の機能、運用状況、非常時の対応、契約終了時の対応等や、これらの責任分界について、定期的に確認できるようにすること。

4.3 安全管理対策の点検

① 定期的に安全管理対策の自己点検を行い、必要に応じて改善に向けた対応を指示すること。また、自己点検に加え、必要に応じて外部監査を実施すること。

■ 策定した安全管理対策が「適切に実施されているか」を確認することも重要であり、これには定期的な第三者監査を受けることが考えられる。一方で本編の主な対象となる小規模医療機関等では、第三者監査の負担が大きいと想定される。

■ このため、最低限の対応として、年次などの頻度で、策定した安全対策の運用状況を、医療情報システム安全管理責任者等が点検し、問題や懸念事項があった部分については、内部でのルールの見直しや、委託契約内容の見直しなどの検討を行うこと。

■ 一方で、「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」に含まれる項目については、医療法に基づく立入検査において、第三者により確認されるため、各項目が「適切に実施されているか」を十分に確認すること。

5．安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）

① 医療情報を取り扱う職員を採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含めること。

② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。

③ 外部保存の委託先事業者選定の際は、プライバシーマーク、ISMS 又はこれと同等の規格の認証を受けている事業者を選定すること。
また、安全管理方針、体制、バックアップ状況、信用度、認証（ISMAP やプライバシーマーク、ISMS 等）の取得状況、保存場所を確認し、情報機器等が、国内法の適用及び執行の及ぶ範囲にあることを確実にすること。

④ 医療情報の外部保存の委託先事業者との契約に、下記を含むことを事業者に確認すること。
-事業者が安全管理ガイドラインと「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省、経済産業省）の遵守すること
-許可なく分析等する等の、目的外利用をさせないこと
-匿名化情報の取扱いの配慮
-患者アクセス時の権限設定
-第三者への情報提供は原則患者同意に基づくこと
-委託契約終了に際しての医療情報の返却とその方法の取り決め
-サーバのセキュリティアップデートを含む保守責任が事業者にあること
-PC 等、端末の保守責任が医療機関等と事業者のいずれにあるか

⑤ 必要に応じて個人情報が特定の外部の施設に送付・保存されること、またその安全性やリスクを含めて院内掲示等を通じて説明すること。

■ 小規模医療機関等では、人的なリソースが限定されることから、できるだけクラウドサービスの利用や

業務委託により、システム導入や運用、保守（セキュリティアップデート含む）などの管理を事業者に委ねることが推奨される。この際、医療機関等が実施すべき安全管理は人的管理が中心となる。

- 人的管理については、職員に対する管理と、委託先の選定や契約内容の管理が挙げられる。
- 職員に対する管理には、医療情報の取扱いに関する雇用契約内容や、教育・訓練などがある。
- 委託先管理は、適切な安全管理を実施させるために、必要な事項を確認して、事業者を選定することや、医療情報を取扱う事業者として必要な対応を契約内容に含めることなどが挙げられる。例えば、委託先における従業員等に対する情報の取扱いに関する教育や訓練、雇用時、雇用中、退職後の守秘義務が雇用契約に含まれていること、情報に関する運用管理規程などが整備されており、これに基づいて管理されていることなどがある。
- 委託先の選定は、事業者において下記の認証等を確認して、実施能力を確認の上選定することが求められる。
  - プライバシーマーク認定又は ISMS 認証の取得
  - プライバシーマーク認定、ISMS 認証のいずれも取得していない場合は、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（令和７年５月 27 日デジタル社会推進会議幹事会決定）の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無
    - 政府情報システムのためのセキュリティ評価制度（ISMAP）（ISMAP-LIU は含まない）
    - JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
    - 米国 FedRAMP（LI-SaaS は含まない）
    - AICPA SOC2／SOC3（又はこれに準じる公認会計士による監査報告書）
    - 「民間事業者による医療情報に係るクラウドサービスの評価」（一般社団法人保健医療福祉情報安全管理適合性評価協会：HISPRO）
  - 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること
    - システム監査技術者試験合格者
    - Certified Information Systems Auditor ISACA 認定
- 医療情報の外部保存は、民間事業者等に委託することが想定される。このための要件として「診療録等の保存を行う場所について」[11]により、外部保存の基準が示されている。

６．情報管理（管理、持ち出し、破棄等）

① 医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順を含む規程を定めること。

---

[11] 令和８年５月時点の最新は「「診療録等の保存を行う場所について」の一部改正について」（平成 25 年３月 25 日／医政発 0325 第 15 号／薬食発 0325 第９号／保発 0325 第５号）

② 医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順を定めること。

③ 医療情報の破棄に関する手順等を定める際は、情報種別ごとに手順（条件、担当者、具体的な方法）を定めること。

■ 医療機関等が保有する医療情報の管理や外部に持ち出す際の対応、破棄（委託先における破棄を含む）について管理する必要がある。電子媒体だけでなく、紙媒体も管理対象となる。

■ また保存等を委託している医療情報を破棄する場合、委託先事業者に対して破棄等の証跡等の提出を求めること。適切に破棄されていることの報告を委託契約に含めることが求められる。破棄等の証跡の提出が困難な場合（例えばクラウド上仮想環境のデータを破棄する場合）は事業者の破棄手順や破棄に関する仕様の提供を求めるなどの対応も想定される。

■ 外部への情報の持ち出しは、媒体での持ち出し以外に、外部のサーバへの送信などが含まれる。

７．医療情報システムに用いる情報機器等の資産管理

① 医療情報システムの資産管理を行うのに必要な規程類を整備すること。

② 整備された規程に基づいて医療情報システムの台帳管理を行うこと。

③ 医療情報システムは、可能な限りクラウドサービスを選定し、ソフトウェアアップデート等の保守管理を事業者に委託すること。
（困難な場合は医療機関等自ら、定期的なアップデートを要する。）

④ 盗難・紛失時の対応手順を作成し、事前対策を講じること。

⑤ BYOD 端末の利用について、利用許諾条件や管理方法等を規程に含め台帳管理を行うこと。

⑥ IoT 機器を患者へ貸し出す際は、リスク説明と同意取得、連絡先提供を行うこと。

■ 医療情報システムに用いる情報機器等については、原則医療機関等に管理責任がある。一方、管理を委託している機器に対しては、事業者から管理状況の報告等を受けられるようにすること。

■ 職員の私物を利用する場合（BYOD：Bring your own device）も医療機関等が管理する機器と同等の管理が求められる。具体的には、BYOD 端末の登録等に関する手順と設定、台帳管理を行うことや、医療機関等の所有する機器と同等の管理をするための手順を作成すること。

■ 医療機関等が利用を認めていないアプリケーション等の利用を制限することも重要である。一般ユーザに管理者権限を与えない設定等により、管理外のサービスが利用されないよう対策すること。

８．サイバーセキュリティ

① インシデント発生時は、ネットワーク切断、機器隔離、システム停止、バックアップからの復元（複数方式・数世代確保、オフライン管理等が重要）等を行うこと。

② サイバー攻撃等により医療提供体制に支障が生じるおそれがある場合は、厚生労働省、都道府県警察、その他所管官庁等への連絡を行うこと。

③ 接続サービスのセキュリティ確保の範囲を事業者に確認すること。

■ サイバーセキュリティ対策は、医療情報の漏えいリスクを軽減するものと、インシデント発生時の業務継続に関するものに別れる。インシデント発生時に業務継続を必要とする場合は、被害範囲を特定してネットワークの切断やバックアップの復元等、BCP に基づく対応を要する。警察や所管省庁等に報告を行うことも求められるので、直ちに報告できるように、報告先の名称及び連絡手段等をリスト化し、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）への連絡体制図を整備しておくこと。クラウドサービスを利用している場合や、運用を委託している場合には、バックアップの復元等の対応は事業者に対して依頼することが想定される。

■ 個人情報の漏えい等（又はそのおそれ）が生じた場合には、個人情報保護法上の対応を図ること。

■ 「接続サービス」においても、サービスの内容と責任分界（委託先事業者は VPN 装置に関するセキュリティアップデート等の管理責任を有するかなど）を明確にすること。例えば、サイバー攻撃発生時に侵入経路の特定や影響範囲の把握を行えるよう、委託先が保有するログ等について、提供される情報の内容、提供条件、提供範囲をあらかじめ確認しておくことが重要である。

９．医療情報システムの利用者に関する認証等及び権限

① 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すること。
特に、管理者権限を与えるアカウントは最低限のユーザとすること。

② 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すること。

③ 電子カルテにおける記録の確定（入力者・確定者の識別、確定手順、更新履歴、代行入力等）に関して、真正性、見読性、保存性の確保が可能なシステムを選定し、必要なルールを規程等に含めること。

④ クライアント端末のアプリケーションログイン時には、令和 9 年度までに二要素認証を採用すること。対応が困難な場合には令和 9 年度以降のシステム更新時に対応可能な事業者を選定すること。

⑤ オンプレミスのサーバが院内に存在する場合は OS（Operating System）のログイン時に二要素認証を採用すること。対応が困難な場合には、令和 9 年度以降のシステム更新時に対応可能な事業者を選定すること。

■ 医療情報システムでは、許可された利用者だけが閲覧、作成、変更、削除できることがシステム上で実現される必要がある。このため、医療情報システムでは、適切な利用者を識別するための認証機能や利用者ごとに適切な権限を付与する機能も要する。

■ 特に、**すべてのユーザに OS の管理者権限が付与されていることで、攻撃者がマルウェア対策ソフトを無効化やパスワードを窃取するためのソフトウェアインストールが可能となり、医療情報にアクセス**される事案が複数発生している。管理者権限を付与するユーザは最小限とすることが必須であり、このアクセス権限管理を事業者に委託する場合には、その業務の実施状況を管理すること。

■ 退職者アカウントや使用していないアカウントは不正アクセスに利用されるリスクがある。退職者アカウントや不要なテスト用アカウント等を定期的に削除する等の運用を取り決め、実行すること。この

ようなアカウント管理を事業者に委託する場合には、不要なアカウントを確実に削除できる運用を事業者と取り決め文書化すること。

- また、昨今ではユーザ 1 人あたりが管理すべきパスワード数の増加、PC の計算能力の向上等により、パスワード単独による認証では十分な安全性を確保することが困難となってきている。
  このため、医療情報システムの認証方法としては、二要素認証など、記憶情報以外の情報を併用して認証する機能を有するシステムであることが有効である。
  医療情報システムではクライアント端末上のアプリケーション（電子カルテ、オーダリングシステム等）や、これを稼働させるサーバの OS については、令和 9 年度までに二要素認証が可能なシステムを選定することが求められる。
- なお、令和 9 年度までの導入が、現状のシステム導入計画などの関係で困難な場合には、次期システムの導入時に確実に対応可能な事業者を選定することが求められる。
- 認証した情報をアプリケーションの資格情報等と連携し、適切な権限付与が可能な場合は OS やミドルウェアでの二要素認証を許容する。ただし、OS で一要素、アプリケーションで一要素のような認証は許容されない。
- 診療録等の記録については、真正性、見読性及び保存性を確保しなければならない。電子カルテシステムにおいては、入力者・確定者の識別、確定手順、更新履歴、代行入力等の内容が明確になるよう、認証や権限付与が行われる必要がある。医療機関等はこのような機能を有するシステムの選定を行い、これらの要件に関するルールを定めた規程等を準備すること。
  - 真正性：故意または過失による虚偽入力、書換え、消去及び混同を防止すること。
    作成の責任の所在を明確にすること。
  - 見読性：情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。
    情報の内容を必要に応じて直ちに書面に表示できること。
  - 保存性：法令に定める保存期間内、復元可能な状態で保存すること。

１０．技術的な安全管理対策の管理

① サーバルーム等のセキュリティ境界への入退室管理（施錠、識別、記録）を行うこと。
② 離席時の不正利用防止対策（画面ロック等）を実施すること。
③ 記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、周知徹底・教育を実施すること。
④ 全体構成図（ネットワーク・システム構成図）及び関係者一覧を作成し、変更が生じた際には速やかに反映すること。
⑤ 医療機関等が用いる端末、ネットワーク機器については、医療機関等の責任で脆弱性対応（セキュリティパッチへの対応、マルウェア対策ソフトのパターンファイルの更新、ネットワーク機器のファームウェアの更新等）を行うこと。これらの対応を事業者に委託する場合には、委託内容・範囲を明確にすること。
⑥ 医療機関等で利用する IoT 機器のリスク分析・評価のうえ、ファームウェア等のアップデート

を行い、使用終了時には接続解除をすること。

⑦ 利用者の ID の台帳管理、棚卸し、削除手順を作成すること。

⑧ パフォーマンス管理、死活監視については、事業者に対する委託契約に含まれる SLA において明確にすること。

⑨ 医療情報システムを導入する際には、事業者に MDS/SDS の提出を求め、本編別紙に示す部分について、「はい」又は「対象外」であることを確認すること。

⑩ 汎用的な医療情報システムについて、委託等を行わずに導入したシステム・サービス等（PC 等の端末やネットワーク機器を除く）を利用する場合は、システム運用編における遵守事項への対応を行うこと。

- 技術的な安全管理対策の多くはシステム運用編に示されている。専任のシステム担当者を要さない機関ではこれを詳細に理解し、適切な事項を選出して対策することは困難であると想定される。
- クラウドサービスの利用や保守の委託を行うことを想定し、「システム運用編」において対応が求められる項目に対して、事業者が対応していることを確認、管理することで実施しているものとみなす。
- 具体的には、事業者から提出される MDS/SDS や約款等と、本編末尾の【別紙】と照らし合わせることで、適切な安全管理が実施されることを確保すること。
- 但し、医療機関等内部での医療情報の利用については医療機関等自らが管理する必要がある。例えばサーバルーム等のセキュリティ境界への入退室管理や、媒体や機器の保管ルール、利用端末の画面ロックアウト設定、などが挙げられる。
- 医療機関等が導入しているネットワークや機器、システム（アプリケーションのほか、これに接続している検査機器のシステム等）、クラウドサービスなどの整理が必要となる。職員のみで作成することが困難な場合には、各事業者への照会や協力を得るなどして作成すること。「利用者の ID の台帳管理、棚卸し、削除手順」の作成についても、医療機関等が自ら実施することが想定されるが、内容等について不明点があれば、事業者へ照会、委託するなどして、対応すること。
- 医療機関等が用いる端末、ネットワーク機器については、不定期にセキュリティパッチや、マルウェア対策ソフトのパターンファイルなどが公表され、その内容に従って更新することが求められる。上記のセキュリティ対応について事業者に委託していない場合（特に PC 等の医療機関等が自ら購入したもの）には、医療機関等が自ら対応する必要がある。事業者に委託している場合には、委託する内容や範囲を明確にし、対応の漏れがないようにすること。実際には、端末は OS の自動アップデートを適用することや、可能な限りセキュリティアップデートを保守契約に含めて事業者の責任範囲とすることが考えられる。ネットワーク機器についてはリスク低減のため、クラウド型 VPN、自動アップデートを採用することが望ましい。
- 医療機関等で IoT 機器を利用する際には、外部接続点が追加されることも想定されるため、十分なリスク分析が必要となる。この際もアップデートを可能な限り事業者に委託することや、自動アップデート等を採用することが望ましい。また、断続的に利用するシステムが外部と常時接続されている状態となることでサイバー攻撃リスクが高まり、実際に攻撃を受ける事例も発生している。外部との接続は必要時のみに限定すること。

■ 事業者が提供するサービスにおける「パフォーマンス管理、死活監視」については、一般的に事業者が対応するものと想定される。一方で、サービスや委託内容によっては、この旨が不明瞭なサービスも存在するため、委託を行う場合には、SLA 等において明確にすること。

■ 医療情報システムを事業者から導入し、運用などを委託している場合には、可能な限り MDS/SDS を事業者から入手すること。このうち、本編末尾の【別紙】で示す MDS/SDS の項目について十分に対応できている必要がある。【別紙】のすべてにおいて「はい」または「対象外」となっている事業者を選定すること。

「いいえ」が選択されている MDS/SDS を含む事業者を選定する場合や、約款に十分な記載がない場合は、各項目について十分なリスク評価、リスク対応を実施し、立入検査や監査等の際に適切な説明が可能な状態とすること。

■ 事業者に委託せず、医療機関等が自らシステムを構築して利用する場合には、保守管理をしていく責任が生まれる。このような場合には、本編の対象とはならず、システム運用編に示す遵守事項を十分に確認し、自ら対策を講じること。

１１．法令で定められた記名・押印のための電子署名、紙媒体等で作成した医療情報の電子化

① 「法令で定められた記名・押印のための電子署名、紙媒体等で作成した医療情報の電子化」を導入する場合には、法令等[12]に従ったシステム・サービスの導入をすること。

② 導入にあたっては提供する事業者に対して、法令等に適合していることを確認すること。

■ 医療情報システムの中には、法令で定められた記名・押印のための電子署名、紙媒体等で作成した医療情報の電子化などを行うシステムが含まれる。これらのシステムの利用がある場合には、医療機関においても、必要な法令等に基づいたシステム・サービスを導入することが求められる。

12 「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」表二

【別紙】 MDS/SDS におけるセキュリティ確認事項

MDS における確認事項

ガイドライン項目	MDS 項番	MDS 項目	適合状況
５．システム設計の見直し（標準化対応等）	No.28	システムの移行の際に診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能があるか？	はい/いいえ/対象外
	No.29	マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えているか？	はい/いいえ/対象外
７．情報管理（管理・持出し・破棄等）	No.10	管理区域外への持ち出しの際、起動パスワード等のアクセス制限機能または暗号化機能があるか？	はい/いいえ/対象外
	No.8	持ち出し機器にソフトウェアインストール制限があるか？	はい/いいえ/対象外
	No.9	持ち出し機器において、外部入出力装置の機能を無効にすることができるか？	はい/いいえ/対象外
	No.12.4.1	不要なリモートログインを制限する仕組みがあるか？	はい/いいえ/対象外
８．利用機器・サービスに対する安全管理措置	No.6	不正ソフトウェア対策機能を有しているか？	はい/いいえ/対象外
	No.22	不正ソフトウェアによる情報の破壊、混同等が起こらないようにするための防護機能があるか？	はい/いいえ/対象外
９．ソフトウェア・サービスに対する要求事項	No.20	目的に応じて速やかに検索結果を出力する機能があるか？	はい/いいえ/対象外
１１．システム運用管理（通常時・非常時等）	No.11	非常時アカウント等で医療サービス継続機能があるか？	はい/いいえ/対象外
	No.21 / 21.1 / 21.2	システム障害に備えた冗長化手段や代替的な見読化手段はあるか？	はい/いいえ/対象外
１２．物理的安全管理措置	No.3	離席時の不正入力防止の機能があるか？	はい/いいえ/対象外
	No.23	記録媒体及び記録機器の保管及び取扱いについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？	はい/いいえ/対象外
	No.24	情報の保存やバックアップについて、医療機関等が運用管理規程を定めるために必要な情報が、取扱説明書等の文書として提供されているか？	はい/いいえ/対象外
	No.27	媒体劣化前に複写できる機能があるか？	はい/いいえ/対象外

ガイドライン項目	MDS 項番	MDS 項目	適合状況
１３．ネットワークに関する安全管理措置	No.12.3.1.1	通信方式として、下記いずれかに対応しているか？ ・専用線 ・IP-VPN ・IPsec-VPN+IKE （セッション間の回り込み対策含む） ・TLS1.2(高セキュリティ型)以上のクライアント認証	はい/いいえ/対象外
	No.12.2	データの暗号化が可能か？	はい/いいえ/対象外
	No.12.1	なりすまし対策を行っているか？	はい/いいえ/対象外
	No.7	無線 LAN のセキュリティ対策機能があるか？	はい/いいえ/対象外
１４．認証・認可に関する安全管理措置	No.4.1	利用者の認証方式について、下記のうち二要素を組み合わせた認証が可能か？ ・記憶（ID・パスワード等） ・生体認証（指紋等） ・物理媒体（IC カード等） （二要素認証に対応済、もしくは医療機関等の次期システム更改までに二要素認証とみなすことが可能な措置に対応予定の場合は「はい」を選択してください。）	はい/いいえ/対象外
	No.4.1.2	デバイス破損時の代替機能があるか？ （破損によりログインができなくなった際に、認証のバイパスを許可することができる場合は「はい」を選択してください。）	はい/いいえ/対象外
	No.4.2	職種・担当別アクセス管理機能があるか？	はい/いいえ/対象外
	No.14	入力者・確定者を識別し認証する機能があるか？	はい/いいえ/対象外
	No.14.1	区分管理に応じた権限管理機能があるか？	はい/いいえ/対象外
	No.15	端末管理による不正アクセス防止機能があるか？	はい/いいえ/対象外
	No.16	記録確定機能があるか？	はい/いいえ/対象外
	No.16.1	識別情報と正確な時刻を含め作成できるか？	はい/いいえ/対象外
	No.16.3	故意の書換え・消去を防止する機能があるか？	はい/いいえ/対象外
	No.17	装置が確定機能を持たない場合、識別情報を記録する機能があるか？	はい/いいえ/対象外
	No.18	確定記録の更新時に履歴保存と参照が可能	はい/いいえ/対象外

ガイドライン項目	MDS 項番	MDS 項目	適合状況
		か？	
１５．電子署名、タイムスタンプ	No.13.1	HPKI 認証局、認定認証局又は公的個人認証サービスが発行する証明書対応の署名機能があるか？	はい/いいえ/対象外
	No.13.3	認定事業者のタイムスタンプ付与が可能か？	はい/いいえ/対象外
	No.13.5	保存期間中の文書の真正性を担保する仕組みがあるか？（長期署名等）	はい/いいえ/対象外
１６．紙媒体等で作成した医療情報の電子化	No.30	スキャナで原本として保存する機能があるか？	はい/いいえ/対象外
	No.30.1/31.1	スキャナが基準を満たしているか？	はい/いいえ/対象外
	No.30.2	電子署名を行える機能があるか？	はい/いいえ/対象外
１７．証跡のレビュー・システム監査	No.4.3	アクセス記録（アクセスログ）機能があるか？	はい/いいえ/対象外
	No.25	システムが保存する情報へのアクセスについて、履歴を残す機能があるか？	はい/いいえ/対象外
	No.4.3.2	アクセスログへのアクセス制限機能があるか？	はい/いいえ/対象外
	No.5	時刻情報の正確性を担保する機能があるか？	はい/いいえ/対象外
１８．外部からの攻撃に対する安全管理措置	No.26	システムが保存する情報が毀損した時に、バックアップされたデータを用いて、毀損前の状態に戻すための機能があるか？	はい/いいえ/対象外

SDS における確認事項

ガイドライン項目	SDS 項番	SDS 項目	適合状況
２．システム設計・運用に必要な規程類と文書体系	No.56	医療機関等に提供可能なサービス事業者の BCP 手順書が用意されているか？	はい/いいえ/対象外
	No.57.1	「非常時のユーザアカウントや非常時用機能」の管理手順を提供できるか？	はい/いいえ/対象外
３．責任分界	No.7	医療機関等との契約に安全管理に関する条項を含めているか？	はい/いいえ/対象外
	No.72	脅威に対する管理責任の範囲について、医療機関等に明確に示し、その事項を示す文書等を提示できるか？	はい/いいえ/対象外
	No.73	医療機関等から委託をされた範囲において、脅威に対する管理責任の範囲を医療機関等に明確に示し、その事項を示す文書等を提示できるか？	はい/いいえ/対象外
４．リスクアセスメントを踏まえた安全管理対策の設計	No.2、	扱う情報のリストを医療機関等に提示できるか？	はい/いいえ/対象外
５．システム設計の見直し（標準化対応等）	No.101	システムの移行の際に診療録等のデータを標準形式で出力・入力できるか？	はい/いいえ/対象外
	No.102	マスタデータベースの変更時に過去の診療録等の情報が変更されないようにしているか？	はい/いいえ/対象外
	No.103	旧データ形式使用機関がある間は対応を維持しているか？	はい/いいえ/対象外
	No.93	電子媒体に保存された情報と見読化手段を対応付けて管理しているか？	はい/いいえ/対象外
７．情報管理（管理・持出し・破棄等）	No.51.3 / 53.7	持出時に暗号化等を実施しているか？	はい/いいえ/対象外
	No.51.4 / 53.8	外部ネットワーク接続時に情報漏えい対策を行っているか？	はい/いいえ/対象外
	No.51.1、	持ち出し機器にソフトウェアインストール制限があるか？	はい/いいえ/対象外
	No.33	機器廃棄時に読み出し可能な情報が残らないことを確認しているか？	はい/いいえ/対象外
	No.34	廃棄委託業者の監督と破棄確認を行っているか？	はい/いいえ/対象外
	No.74.1 / 91、	不要なリモートログインを制限する仕組みがあるか？	はい/いいえ/対象外

ガイドライン項目	SDS 項番	SDS 項目	適合状況
８．利用機器・サービスに対する安全管理措置	No.19	不正ソフトウェア混入を確認しているか？	はい/いいえ/対象外
	No.96	利用ソフトウェアや媒体の管理を行っているか？	はい/いいえ/対象外
	No.20 / 21	実行プログラムを含むデータ送受信禁止または無害化処理を行っているか？	はい/いいえ/対象外
	No.54	情報機器・媒体の所在を台帳で管理しているか？	はい/いいえ/対象外
	No.55	個人保有機器の利用を禁止しているか？	はい/いいえ/対象外
９．ソフトウェア・サービスに対する要求事項	No.85	システム構成および利用用途を明確にしているか？	はい/いいえ/対象外
１０．事業者による保守対応等に対する安全管理措置	No.38	作業終了後に個人情報を含むデータを消去しているか？	はい/いいえ/対象外
	No.30	外部委託先にも同等の個人情報保護対策を契約で義務付けているか？	はい/いいえ/対象外
	No.39	改造・保守アカウントを作業員専用で運用しているか？	はい/いいえ/対象外
	No.48	リモート保守時にアクセスログを収集するか？	はい/いいえ/対象外
	No.40	改造・保守作業の記録を提供できるか？	はい/いいえ/対象外
	No.49	送付ファイルが無害化処理されているか？	はい/いいえ/対象外
１１．システム運用管理（通常時・非常時等）	No.57	非常時アカウント等で医療サービス継続機能があるか？	はい/いいえ/対象外
	No.57.1 / 57.2	非常時アカウントの管理・監査手順が提供できるか？	はい/いいえ/対象外
	No.57.3	非常時アカウントが正常復帰後に継続使用できないよう変更できるか？	はい/いいえ/対象外
	No.57.4	標的型攻撃発生時の連絡手段を準備しているか？	はい/いいえ/対象外
	No.58.1 / 58.2	バックアップを複数世代・複数方式で実施しているか？	はい/いいえ/対象外
	No.58.3	バックアップ復元手段が整備されているか？	はい/いいえ/対象外
１２．物理的安全管理措置	No.1.1 / 1.2	保存場所がガイドラインの要件を満たしているか？	はい/いいえ/対象外
	No.12 / 12.1	個人情報機器設置区画で入退管理を行っているか？	はい/いいえ/対象外
	No.97	院内保管・取扱情報を文書提供しているか？	はい/いいえ/対象外
	No.98	保存・バックアップに必要な情報を文書提供して	はい/いいえ/対象外

ガイドライン項目	SDS 項番	SDS 項目	適合状況
		いるか？	
１３．ネットワークに関する安全管理措置	No.67	送信元と送信先の相手確認を行っているか？	はい/いいえ/対象外
	No.59 / 60 / 61 / 62 / 63	通信方式として、下記いずれかに対応しているか？ ・専用線 ・IP-VPN ・IPsec-VPN+IKE （セッション間の回り込み対策含む） ・TLS1.2(高セキュリティ型)以上のクライアント認証	はい/いいえ/対象外
	No.66	なりすまし対策を行っているか？	はい/いいえ/対象外
	No.65	盗聴防止対策を行っているか？	はい/いいえ/対象外
	No.64	改ざん防止対策を行っているか？	はい/いいえ/対象外
	No.22、	無線 LAN のセキュリティ対策機能があるか？	はい/いいえ/対象外
１４．認証・認可に関する安全管理措置	No.17	アクセス管理機能があるか？	はい/いいえ/対象外
	No.17.1	利用者の認証方式について、下記のうち二要素を組み合わせた認証が可能か？ ・記憶（ID・パスワード等） ・生体認証（指紋等） ・物理媒体（IC カード等） （二要素認証に対応済、もしくは医療機関等の次期システム更改までに二要素認証とみなすことが可能な措置に対応予定の場合は「はい」を選択してください。）	はい/いいえ/対象外
	No.17.1.2、	セキュリティデバイスが使えない場合の代替手段が規定されているか？	はい/いいえ/対象外
	No.17.2、	職種・担当別アクセス管理機能があるか？	はい/いいえ/対象外
	No.80 / 81 / 82	確定操作・識別情報記録機能があるか？	はい/いいえ/対象外
	No.84	代行入力承認機能があるか？	はい/いいえ/対象外
１５．電子署名、タイムスタンプ	No.77.1	HPKI 又は公的認証対応の署名機能があるか？	はい/いいえ/対象外
	No.77.3 / 77.4	認定事業者のタイムスタンプが付与・検証可能か？	はい/いいえ/対象外
１６．紙媒体等で作成した医療情報の	No.105	スキャン電子化して原本として保存できるか？	はい/いいえ/対象外
	No.105.1	スキャナが一定規格を満たすか？	はい/いいえ/対象外

ガイドライン項目	SDS 項番	SDS 項目	適合状況
電子化			
１７．証跡のレビュー・システム監査	No.17.3 / 17.4	アクセス記録（アクセスログ）機能があるか？	はい/いいえ/対象外
	No.17.3.2	アクセスログへのアクセス制限があるか？	はい/いいえ/対象外
	No.18	時刻情報の正確性を担保しているか？	はい/いいえ/対象外
１８．外部からの攻撃に対する安全管理措置	No.100	データ破損時にバックアップから戻せるか？	はい/いいえ/対象外

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

医療機関・薬局確認用

*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」にマルが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 (/)	(/)	
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、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 (/)	(/)	
	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接続元制限を実施している。	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。	はい・いいえ (/)	(/)	
	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 (/)	(/)	
	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 (/)	(/)	
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 (/)	(/)	

- 各項目の考え方や確認方法等については、「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マニュアル～医療機関・薬局・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8年度
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

事業者確認用

＊ 以下項目は令和8年度中にすべての項目で「はい」または「対象外」にマルが付くよう取り組んでください。

・「はい」　：医療機関・薬局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・薬局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・薬局との保守契約範囲外となり、当該項目の責任を医療機関・薬局が負います。**
　　医療機関・薬局に対して、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。

	チェック項目	（日付）		備考
		確認日	目標日	
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。	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医療機関等に伝えた。	はい・いいえ （　/　）	（　/　）	
	③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。	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・対象外 （　/　）	（　/　）	
	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・対象外 （　/　）	（　/　）	
	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・対象外 （　/　）	（　/　）	
	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接続機器や情報機器に対して接続を制限している。	はい・いいえ・対象外 （　/　）	（　/　）	
	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・対象外 （　/　）	（　/　）	
	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・対象外 （　/　）	（　/　）	
	ネットワーク機器について、以下を実施している。			
	⑭接続元制限を実施している。	はい・いいえ・対象外 （　/　）	（　/　）	
3 インシデント発生に備えた対応	⑬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 （　/　）	（　/　）	

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・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～」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

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）

▶企画管理編
13④
13.1.3

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。

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）

▶企画管理編
13⑦

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。

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）

▶システム運用編
8.⑤

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

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）

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。

▶システム運用編 8.⑤

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）

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。

▶企画管理編 8.2.2
▶システム運用編 8.①

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。

▶システム運用編
14.⑤
14.1.1

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

●サーバ二要素認証の「みなし措置」

▶システム運用編
14.1.1

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。

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。

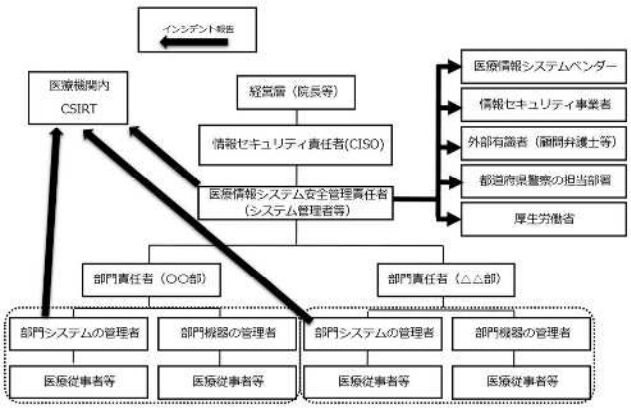
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

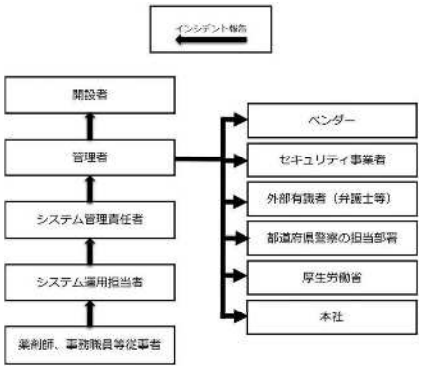
情報セキュリティインシデント発生時（医療情報システムに障害が発生した場合を含む）は、下記の厚生労働省の連絡先に御連絡ください。

【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、万がー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