産情発 0629 第 1 号
令和８年６月 29 日

各 都道府県知事
保健所設置市長
特別区長 殿

厚生労働省大臣官房
医薬産業振興・医療情報審議官
（公印省略）

「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」の策定について

日頃より厚生労働行政に御協力を賜り、厚く御礼申し上げます。

「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。）については、令和５年５月に第 6.0 版を策定し、医療情報システムの適切な取扱い等についてお示ししてきたところですが、同版の公表以降も医療機関等を対象としたサイバー攻撃事案の発生が継続しているほか、サイバー対処能力強化法（重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第 42 号）をいう。）の成立等を背景に、サイバーセキュリティに対する社会的関心及び重要性は一層高まっております。

このような状況を踏まえ、制度的動向として、内閣官房国家サイバー統括室（NCO）による「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（令和５年７月４日サイバーセキュリティ戦略本部決定）の改定、並びに経済産業省及び総務省が策定する「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」（以下、２省ガイドライン）の第 2.0 版への改定が行われたことを受け、ガイドラインの見直しを実施しました。

併せて、医療情報システムの利用・運用に際してクラウドサービスを導入する医療機関が増加している状況を踏まえ、新たに保守委託機関編を作成しました。

ガイドラインの改定の概要等については、下記のとおりですので、貴職におかれましては本通知の内容を御了知の上、関係団体および関係機関等へ周知徹底を図るとともに、その実施に遺漏のないよう御配慮願います。

記

第１　改定の概要

１　全体構成の見直し

・　保守委託機関編の追加

２　制度的な動向

・　重要インフラのサイバーセキュリティに係る安全基準等策定指針への対応として、ガイドラインに関連する法令にサイバーセキュリティ基本法を追加するとともに、サプライチェーンリスクについて追記。

・　２省ガイドラインの改定による影響を確認し、医療機関等と事業者との役割分担や医療機関とのリスクコミュニケーション等を追記。

・　クラウドサービスの積極的な活用を推進する旨を追記。

３　技術的・社会的な動向

・　パスワードルールに関して、使い回しの禁止、アカウントロックの導入について追記する一方で、セキュリティ面の強化につながらないとされる「定期的な変更」の要件を削除。

・　二要素認証の導入について、医療情報システムのうち、クライアント端末及びサーバにおいて対応することを明確化するとともに、これまで対象が明確化されていなかった点も踏まえ、令和９年４月１日時点での対応が困難な医療機関等においては、次期システム改修での対応を許容する旨の緩和措置を設定。

・　保守委託機関編においては、専門人材が不足している小規模医療機関を想定し、すべてのサーバ（※）におけるセキュリティアップデートを委託（クラウドサービスの利用を含む）している医療機関等においては、保守委託機関編を遵守することで、その他の編の項目も遵守できているものとみなす旨を追記。

（※）例えばCD-Rで電子カルテのアプリケーションをインストールして運用するなど、サーバ機能を果たすPC等の端末も含む。

第２　留意事項

ガイドライン及び別途通知するガイドラインに基づくチェックリスト（別添）については厚生労働省ホームページに掲載する予定

以上

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

システム運用編

目次

【はじめに】

＜システム運用編が想定する読者＞

システム運用編は、主に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対象にしており、医療機関等の経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の各種資源の設計、実装、運用等の実務を担う担当者（以下「システム運用担当者」という。）として適切に対応すべき事項とその考え方を示している。

なお、医療情報システムの実装・運用において、医療機関等が事業者に委託し、その業務や責任を分担することも考えられる。そのため、委託事業者におかれても本編を参照のうえ、医療機関等と協働されたい。その際、業務や役割、責任の分担の在り方については、あらかじめ両者で取り決めておくことが望ましい。

１．情報セキュリティの基本的な考え方

【遵守事項】

① 法令上求められる医療情報システムの要件等について、企画管理者の指示のもと、各システムの措置や、必要な手順、資料の作成を行うこと。

１．１ 安全管理に関する法制度等による要求事項

- システム運用担当者は、本編に記載の技術的対策を講じる際、法制度により求められる対応を行う必要がある。
- 特に、下記に掲げる事項について適切に対応すること。
  - 個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）における安全管理措置
  - 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。以下「e-文書法」という。）に関する対応
  - 電子署名、タイムスタンプ

２．システム設計・運用に必要な規程類と文書体系

【遵守事項】

① 採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。

② 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態を維持すること。

③ 医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。

④ 医療情報システムを適切に利用できるよう、マニュアル等の整備を行うこと。

⑤ 非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。

２．１　システム運用担当者において作成すべき文書類

- システム運用担当者は、企画管理者が策定した各種規程等を踏まえて、実際の運用に求められる手順や、システム等を構築するための資料等を整備することが求められる。これらの資料は、常に最新化すること。古い手順や技術資料が混入すると、脆弱性が残存する、正常な情報システムの稼働が損なわれる、などのリスクが生じる。
- 通常時だけではなく非常時や情報セキュリティインシデントが生じた場合の対応についても手順を整理するほか、即応できるための資料を整備すること。特に体制面や情報照会・収集の対象なども明示することが重要である。

3．責任分界

【遵守事項】

① 医療情報システムに関する委託において、役割分担を検討するため、事業者から必要な情報等の収集を行うとともに、提供された情報が正確であることを事業者に確認すること。

② 事業者と技術的な対応に関する責任分界を調整する際には、医療機関でのリスク評価に基づく要求仕様への適合性を十分に確認し、必要な調整を行うこと。

③ 技術的な対応に関する役割分担を、委託先事業者との間で調整し、企画管理者に対してその結果を報告すること。

④ サイバー攻撃等が生じた場合の技術的な対応や対外的な説明に関する役割について、事業者と調整し、その結果を企画管理者に報告すること。

⑤ 第三者提供を行う際には、企画管理者と協議の上、医療機関等のリスク評価を踏まえて技術的な対応に関する責任分界を検討し、企画管理者に報告すること。

3．1 技術的な対応における責任分界決定の考慮事項

- 医療情報システムの運用等を委託する場合、提供されるシステム・サービスの機能仕様が、法令、本ガイドラインや関連ガイドラインに適合していることを、医療機関等で直接確認できない可能性がある。
- システム運用担当者は、技術的な対応に関する情報システム・サービスの機能仕様に関する情報と、その内容が正確であることを示す資料を、事業者から提出を求め、その確認を行うこと。

3．2 要求仕様適合性の確認を踏まえた調整

- 技術的な対応に関する責任分界を設定する際は、提供される情報システム・サービスについて、事業者がどのようなリスク評価を踏まえて、対応を分担するのかに関する情報を収集することが求められる。
- 例えば、厚生労働省標準規格となっている「『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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリストの提供を受け、リスクコミュニケーションを図ることが想定される。
- その他、総務省・経済産業省の定める「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」（以下「２省ガイドライン」という）において、医療機関等と事業者との間でリスクコミュニケーションを図る際には、合意形成に必要な情報を提供することとされている。具体的な内容は同ガイドライン別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」 により示されているため、参考とすること。
- システム運用担当者はこれらの資料を収集し、医療機関等におけるリスク評価との差異などを確認すること。また、必要に応じて事業者と個別の調整を行い、リスク分担などを行うこと。
- クラウドサービスなどを利用する場合には、利用者側でも設定等の役割を果たすことなどが求められる。このような役割分担については、「クラウドサービス提供・利用における適切な設定に関するガイドライン」（総務省令和４年10 月 31 日）などでも示されている。

３．３　医療機関等が負う責任に関する責任分界

３．３．１　通常時の運用における責任分界

- 通常時における技術的な対応の責任分界は、主に運用責任や管理責任に関する取り決めを指す。情報システム・サービスが提供される際の運用が、本ガイドライン等に従っていることは、事業者でしか把握できない場合もある。システム運用担当者は運用に関する実施報告などに関する情報の提出を事業者に求めて管理すること。事業者が業務の一部を再委託している場合には、再委託先における実施状況なども併せて報告を求めること。
- このように、システム運用担当者は、委託する情報システム・サービス全般の管理を担う中で、具体的な運用や管理については、事業者に役割を委ねることが想定される。

３．３．２　非常時の運用における責任分界

- 非常時の運用における技術的な対応の責任分界は、主に被害の拡大防止や原因究明などシステム対応のほか、外部への説明責任に関する支援などに関する取り決めを指す。
- 被害拡大防止や原因究明などに関しては、医療機関等側で把握できる運用に関する情報と、委託先である事業者が管理するシステム運用上の資料などを併せて検討することが求められる。それぞれの役割の分担などを事前に取り決めておくことが重要である。
- 外部への説明責任についても、技術的な面から、事業者側でしか把握できない内容がありえる。専門的な観点から適切な資料の準備と提供に関する内容も含めた、責任分担を行うことが求められる。

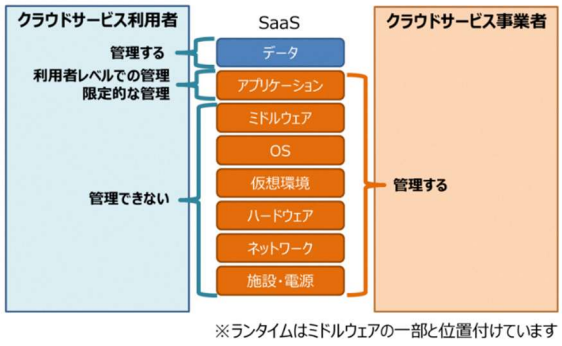
３．４　提供される情報システム・サービスに応じた責任分界

３．４．１　事業者が提供するサービスの類型による責任分界

- 事業者が提供するサービス類型により、医療機関等が直接責任を管理できる範囲が異なる。
- クラウドサービスの場合には、一般的に SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）などの類型で提供される。
- SaaS ではアプリケーション部分、PaaS ではミドルウェア部分、IaaS ではインフラ部分がサービスとして提供される。
- 例えばSaaS を利用する場合には、アプリケーション部分の管理や責任を事業者に委ねることになる。そこで本ガイドラインの遵守を確認するにあたっても、アプリケーション部分に関する安全管理対策項目などについて、事業者との責任分界を検討することになる。
- このように、利用するサービスの内容により、責任を分担する内容が異なるため、医療機関等が行うべき安全管理のうち、明確に責任分界を定め、具体的な管理内容について、事業者と取り決めること。

表３－１　SaaS の場合の技術的な対応における利用者と事業者の管理対象範囲

利用者側の管理対象範囲	事業者側の管理対象範囲
・ 利用者は、アプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集 ・削除等の行為）をする権限と責任を有する。 ・ アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。	・ クラウドサービス事業者は、契約 ・SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書） に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に限定的な管理権限等を提供する場合がある

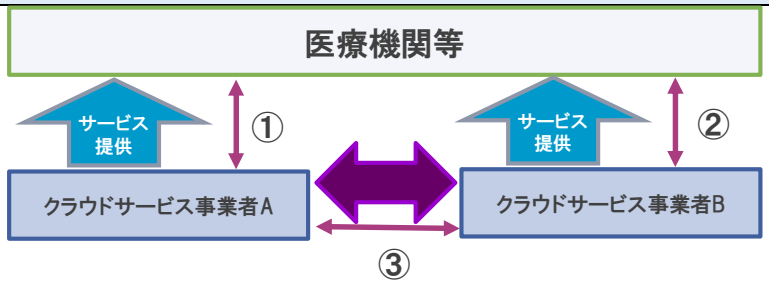


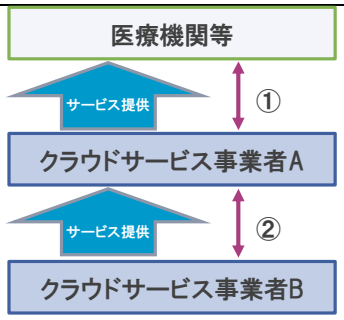
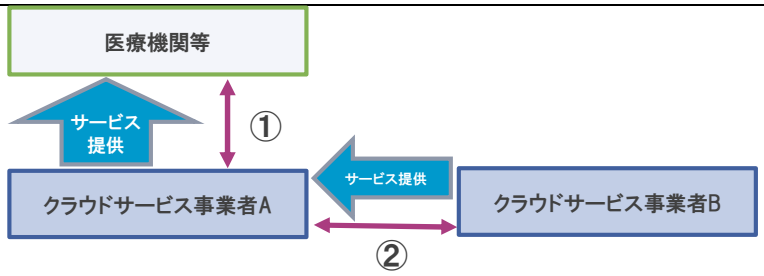
出所：「クラウドサービス提供における 情報セキュリティ対策ガイドライン（第 3 版）」
（総務省、2021 年 9 月）より作成

3．4．2　複数の事業者に対する委託を含む場合の責任分界

- 事業者に委託を行う場合、この情報システム・サービスの利用に際して複数の事業者が関与する場合がある。
- 医療機関等が複数の情報システム・サービスのサービスを組み合わせて利用するような場合と、事業者が複数のサービスを組み合わせて、医療機関等に提供する場合などが想定される（表 3 － 2 参照）。
- 前者では、医療機関等が各事業者と責任分界を取り決めることになるが、複数の事業者のサービスを連携する部分についても併せて取決めを行うこと。これには、技術的な機能仕様等に関する取決めだけではなく、障害時などの対応などの事業者間での役割分担も含まれる。
- 後者の場合には、医療機関等と、情報システム・サービス等を取りまとめて提供する事業者との間で責任分界を定めることが一般的である。この場合、取りまとめ事業者が利用する他の事業者のサービスとの関係では、再委託などの関係となることが多い。これらの契約関係に留意して取決めを行うこと。
- 企画管理者はこれらのケースについて、各事業者に必要な対応を依頼できるよう、責任分界を設定し、契約や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）などにおいて取り決めること。

表 3 － 2　クラウドサービスの提供パターンと責任分界

パターン	概要
医療機関等が複数の事業者の提供するサービスを組み合わせて利用	 ・　医療機関等が事業者 A、B をそれぞれ別に契約してサービスを利用（①、②） ・　A、B の連携が取れるように③の部分を各①、②の契約内容を盛り込む必要がある。

事業者が複数のサービスを組み合わせて提供するサービス	 ・ 医療機関等は利用する事業者 A と取り決め（①）、A が他のサービス B を利用（②：別の階層サービスを利用）
	 ・ 医療機関等が利用する事業者 A と取り決め(①)、A が他のサービス B を利用（②：別の機能のサービスを利用）

出所：クラウドサービス提供における情報セキュリティ対策ガイドライン （第 3 版）より作成

3．5 第三者提供における責任分界

- 医療機関等が、管理する医療情報を第三者に提供する場合に、医療機関等と提供先との間で責任分界を取り決めることになる。第三者提供を実施する方法としては、下記などが想定される。
  - ・メール等による情報の送信、及び受信
  - ・サーバやクラウドサービス等への提供
  - ・アプリケーションが連携する際のデータの提供
  - 提供方法に応じたデータの送受信に係る責任分界など技術的対策に関する内容を定める必要がある。例えば、メール送信の場合、医療機関等が利用するメールサーバまでは、医療機関等が責任を有する等が考えられる。
- システム運用担当者は、企画管理者が取り決めた第三者提供における責任分界と整合性をとれる責任範囲を設定し、企画管理者に報告すること。

４．リスクアセスメントを踏まえた安全管理対策の設計

【遵守事項】

① 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者ごとに識別できるような措置を講じること。

③ 事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた２省ガイドラインにおける「サービス仕様適合開示書」を利用することが考えられる。

４．１ 情報資産の種別に応じた安全管理の設計

- 情報資産の把握に基づくリスク分析は、安全管理の設計の起点となる。システム運用担当者は、企画管理者と協働して保有する情報の棚卸を行うこと。システム運用担当者は、医療情報システムが直接取り扱う医療情報や、医療情報システムに関する情報などについて、棚卸を行い、情報種別を整理する必要がある。
- 医療情報システムであれば、各システムに情報が保管されている患者数、情報の種別、それらの利用者の範囲、利用権限の設定ルール、持ち出し状況などを整理すること。バックアップについても、どのくらいの医療情報が、どこで、どのような形式で保管されているか、等を把握することが求められる。また情報のライフサイクルを踏まえ、必要な取扱制限（例：複製禁止、持出禁止、配布禁止）を実施する。
- 上述の「医療情報システムに関する情報」は、全体構成図（ネットワーク図、システム構成図等）、各システムを構築・導入するための資料やその管理状況（保管場所、作成時期等）、運用上の設定情報やログ等の管理状況などが挙げられる。
- 情報種別を整理する際に、法令により保存などの要件が定められているものは、その要件への適合状況も併せて確認する必要がある。具体的には「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等の施行等について」（平成 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年３月 31 日最終改正。以下「施行通知」という。）や「診療録等の保存を行う場所について」（平成 14 年３月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長連名通知。平成 25 年３月 25 日最終改正。）が求める要件などがある。

４．２ リスクアセスメントを踏まえた安全管理対策の設計

- システム運用担当者は、医療情報等の情報種別や重要度を整理したうえで、企画管理者とともにリスクアセスメント（リスク分析、リスク評価）を行い、技術的対応を実装、運用することになる。
- 対策を講じる場合には、組織の規模等の実情や、システムの利用形態等のリスクに応じて、さまざまな方法が考えられる。また実装の検討に際しては、医療機関等における負担（要員、費用等）を踏まえることも重要である。
- 安全管理対策の設計においては専門的な知見が必要だが、医療機関等においては、十分な資源（要員、費用等）を有していない場合もある。このような場合には、利用を想定する事業者によるリスクアセスメント結果を踏まえた対策を参考にすることなどが想定される。なお、事業者には「サービス仕様適合開示書」を提供させること。
- 特に専任のシステム担当者を要しない場合には、事業者から安全なシステムを導入し、構築と運用等は事業者に委ねるほうが、安全性や経済性で優れていることが多い。
- システム運用担当者は、上記を踏まえた技術的な対応を整理し、企画管理者に報告すること。

5．システム設計の見直し（標準化対応、新規技術導入のための評価等）

【遵守事項】

① システム更新の際の迅速な移行を可能とするため、診療録等のデータについて、原則として標準形式（標準形式が存在しない項目は変換が容易なデータ形式）で出力及び入力が可能なシステムを選定すること。

② 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たシステムを選定すること。

③ データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられるが、その際にも以前のデータ形式や転送プロトコルに対応可能な事業者を選定すること。

④ 電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態に保つこと。

5．1 医療情報システム等における情報の相互運用性と標準化の重要性

- 医療機関等における電子化は、従来の指示、報告、連絡等の意思の共有の業務を効率化し、入力作業の軽減等、業務の総量を減ずることにもつながる。また紙媒体の誤記・誤読リスクも低減し、医療安全にも資する。
- 電子化の過程では、段階的に導入されたシステム間や、異なる事業者から提供されたシステム間で電子情報のやりとりを行う際の相互運用性の確保が必要となる。
- 医療情報システムの安全な管理・運用における重要な観点として、情報セキュリティの重要な要素の一つである「可用性」が挙げられる。ここでいう可用性とは、必要なときに情報が利用可能であることを指し、任意の時点で可用性が確保されなければならない。例えば、システム更新を経ても旧システムで保存された医療情報を確実に利用できるようにしておくこと、すなわち相互運用性を確保することなどが挙げられる。
- なおプロトコルについては、危殆化したものを継続して使用するのではなく、最新のプロトコルに移行する等、安全性確保に配慮した対応が求められる。その際にも以前のデータ形式や転送プロトコルに対応可能な事業者を選定すること。
- 地域連携等における医療機関等間の情報の共有、蓄積、解析、再構築、返信、再伝達等といった場面においても、相互運用性の確保が求められる。
- 医療情報の相互運用性を確保するため、誰もが参照可能かつ利用可能で将来にわたり保守の継続が期待される標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）を利用することや、それらに容易に変換できる状態で保管することが望ましい。
- 経済産業省・厚生労働省においても、種々の国際規格との整合を図り、これを推奨する取組みを進めてきた。特に、厚生労働省では、「厚生労働省標準規格」を示し、その実装を強く推奨しており、標準化の一層の推進が期待される。
- 医療機関等において、自らこれらの用語・コードの保守や標準規格の実装作業をすることは稀であろうが、標準規格に基づく相互運用性の確保の推進のため、システム・サービス事業者に対して標準規格の採用を要件として求めていくことが重要である。
- システム運用担当者は、医療情報システムの導入や運用に当たって、下記事項について事業者から説明を受ける等して、一定の理解を共有しておく必要がある。
  - 標準化に対する基本スタンス
  - 標準規格に対応していないならばその理由

・ 将来のシステム更新、他社システムとの接続における相互運用性に対する対応案

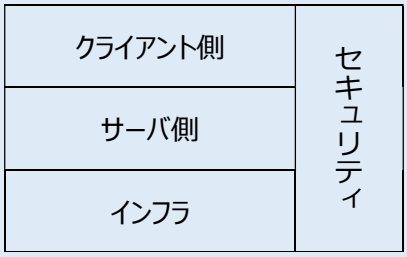
５．２　標準化対応、データ形式・プロトコルの互換性の確保

- システム運用担当者は、５．１の観点から、医療情報システムで用いるデータの構造や項目、形式等のほか、外部との連携に際して用いるプロトコル等について、標準的な規格や機能仕様を採用する必要がある。特に施行通知では保存性の要件として、「保存すべき期間中において復元可能な状態で保存することができる措置を講じていること」が求められており、標準規格を採用するなどして対応すること。

6．安全管理を実現するための技術的対策の体系

【遵守事項】

① システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。



– クライアント側
・情報の持出し・管理・破棄等に関する安全管理措置
・利用機器・サービスに対する安全管理措置

– サーバ側
・ソフトウェア・サービスに対する要求事項
・事業者による保守対応等に対する安全管理措置
・事業者選定と管理
・システム運用管理（通常時・非常時等）

– インフラ
・物理的安全管理措置（サーバルーム等、バックアップ）
・ネットワークに関する安全管理措置
・インフラ運用管理（通常時・非常時等）

– セキュリティ
・認証・認可に関する安全管理措置
・電子署名、タイムスタンプ
・証跡のレビュー、システム監査
・外部からの攻撃に対する安全管理措置

6．1 安全管理対策に関するシステムアーキテクチャ（クライアント側、サーバ側、インフラ、セキュリティ）

➢ 医療情報システムは、
・職員などの利用に関する情報資産
・情報システムの提供元となるサービスに関する情報資産
・インフラに関する情報資産
などから構成される。またセキュリティに関連する内容も共通して把握すべき要素となる。

➢ 本ガイドラインでは、これらにつきクライアント側、サーバ側、インフラ、セキュリティとして区分し、それぞれに関する技術的な遵守事項を整理した。

６．２　医療機関の規模や導入システム等の形態に応じた対応

- 医療情報システムには、さまざまな形態のものがある。
  - 医療機関等の内部で自ら開発するシステムやサービスを利用する場合（アプリケーションのマクロ機能の利用や、簡易データベースソフトを用いて構築する場合等）
  - 情報システム・サービスベンダーが提供するアプリケーションを導入して、運用は医療機関等が行う場合（医療機関等がサーバを設置し、調達したアプリケーションを導入する等）
  - 事業者が提供するアプリケーションを用いて、運用も外部に委託する場合（クラウドサービスの利用等）
- システム運用担当者が直接対応するべき内容も、このようなシステムの形態によって変化することに留意すること。
- 医療機関等では、技術的な対応を行う専任のシステム運用担当者がいない場合もある。このとき、技術的な対応に関する内容の多くは、外部に委託することになる。
- システム運用担当者が行うべき技術的な対応を、事業者に委ねる場合には、本ガイドラインの該当部分について、事業者にその実施状況の確認を行うこと。

7．情報管理（管理･持出し･破棄等）

【遵守事項】

① 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。

② 保守業務を行う事業者に対して、原則として個人情報を含むデータの持出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。

③ 医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。

④ 持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続する場合は、マルウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施すること。

⑤ 持ち出した情報機器等について、公衆無線 LAN の利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。

⑥ 持ち出した情報機器には、必要最小限のアプリケーションのみをインストールし、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については削除又は停止すること。

⑦ 医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行うこと。併せて定期的に棚卸を行う手順も作成すること。

⑧ セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や連絡方法について、患者等に情報提供すること。

⑨ 破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。

⑩ 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。

⑪ 外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑または事業者の説明により確認すること。

⑫ リモートログインは、保守作業等の必要な場合に限定し、適切に管理されたものに限り実施できるよう制御すること。

⑬ 利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。

⑭ 患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI（Public Key Infrastructure：公開鍵暗号基盤）認証等の対策を実施すること。

⑮ 医療情報を格納する情報機器等の盗難や紛失（ネットワークサービスの利用等による漏えいの可能性の発生含む）が生じた場合の対応手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。

７．１　外部へ持ち出す医療情報の管理対策

- システム運用担当者は、企画管理者が策定する規程を踏まえて、外部への医療情報の持出しに関する具体的な手順を作成する。手順は、持ち出す医療情報や記録媒体、持出し方法の種類や特性に応じて策定すること。持出し前の手続から、外部からの持ち帰り等に関する手順も対象となる。
- 情報機器等を持ち出す場合には、盗難や紛失のリスクを想定した内容を含めること。例えば端末の起動パスワード等の設定は必須であり、このパスワード等は認証ルールに沿った内容であることが求められる。
- 医療情報が保存されている場合には、記録媒体に暗号化を施す必要があるほか、患者等の医療情報を表示や編集できる場合は、その機能を持つアプリの起動にパスワードを設定するなどの措置も必要である。
- またタブレット PC 及びスマートフォンの持出しに際して、その目的から見て不要なプログラム等はインストールしない/させないことや、情報機器等に対する管理者権限等を原則付与しないなどの措置を講じることも重要である。
- ネットワークを通じて外部に保存する場合、システム運用担当者は利用可能な保存先やサービスを限定する必要がある。クラウドサービスは、容易に医療情報の外部保存ができるため、システム運用担当者が管理しないものが使われるリスクがある。医療機関等が定める安全管理の基準や、プライバシーポリシー、その他のルールに適合したサービスを利用させること。
- 例えば、医療機関等が許可したサービス以外の接続を遮断する等の技術的対応を取ることや、許可されていないサービスの利用禁止を規則等に盛り込むなどの対応が想定される。
- 漏えい防止等の観点から、保守等の目的で、事業者が医療情報を持ち出す行為は原則として禁止する必要がある。業務上、やむを得ず持ち出す場合には、持ち出しの目的や件数、項目、持出し先での保存環境等を事前に示したうえで、システム運用担当者の許可を要すること等を手順として定めること。

７．２　医療機関等外から医療情報システムに接続する利用の場合への対策

- システム運用担当者は、外部から医療情報システムに接続して利用する場合の、技術的対応を講じることが求められる。利用場面としては、下記が想定される。
  - ・ 職員が、訪問先やテレワークなどにより、医療機関等が管理する端末を通じてアクセスする場合
  - ・ 患者等が、自宅から自らの医療情報にアクセスする場合
  - ・ 事業者が外部から医療情報システムにアクセスして保守等を行う場合

７．２．１　医療機関等の職員による外部からのアクセス

- 職員が自宅等や訪問先などから医療情報システムへアクセスする場合、安全管理のため、
  - ・ 接続できる職員に対する事前の許可
  - ・ 外部から接続する際の技術的対応

  等の対応が考えられる。
- 事前の許可については、システム運用担当者が具体的手順等を定めて、接続可能な利用者と権限の範囲を設定すること。また、その結果を企画管理者に報告すること。
- 技術的な対応については、下記を含む措置を、システム運用担当者が講じる必要がある。
  - ・ 外部からのアクセスに関する認証・認可
  - ・ 外部から利用する際のネットワークの要件
  - ・ 外部から利用する端末等の要件

- 外部からの認証・認可については、外部の環境から医療機関等が管理するネットワークに接続するための認証等の措置を講じることが求められる。認証等の要件は、「１４．１利用者認証」に示す。
- 外部からネットワークを利用する場合、医療機関等が接続先を管理するネットワークに接続する前に、オープンなネットワーク（13.1 参照）を経由することが想定される。この場合、「１３．１　ネットワークに対する安全管理」に示す対策を講じて、十分なチャネル・セキュリティを確保すること。
- 外部から利用する端末等の要件については、医療機関等により支給された端末を使うことが想定される。一方で、医療機関等によっては、「９．ソフトウェア・サービスに対する要求事項」に示す措置を講じて、個人の所有する端末（ノートパソコン、スマートフォン、タブレット等）を業務利用すること（Bring Your Own Device：以下「BYOD」という。）も想定される。端末等の要件に関しては、考慮すべき点が 3 つある。
  - PC 等の安全管理対策を確認するためには一定の知識と技能が必要で、一般職員にその知識と技能を要求することは難しい。
  - 運用管理規程等で定めた内容の実施状況を確認するためには、運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは負担が大きい。
  - 医療機関等の管理が及ばない私物の PC や、不特定多数の人間が使用する PC の場合、医療機関等の想定と異なる環境で使用され、安全管理上の支障が生じる可能性がある。したがって、職員による外部からのアクセスを行う場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術等により安全性を確保した上で、仮想デスクトップを利用する等の運用要件を設定すること。ここでいう仮想デスクトップ等とは、利用する端末の作業環境内に、ユーザ認証を経た後で、医療機関等に設置した機器の画面を表示する仕組みである。その他、ユーザ権限を厳格に管理した専用端末の貸与等も考えられる。

７．２．２　患者等に診療情報等を提供する場合の外部からのアクセス

- 診療情報等の開示が進み、ネットワークを介して患者等に診療情報を提供したり、患者等が医療機関等内の診療情報を第三者に参照閲覧させることなどが想定される。
- 患者等に診療情報等を提供する場合には、ネットワークのセキュリティ対策、医療機関等内部のセキュリティ対策などに関する措置を講じるとともに、手順等を作成する必要がある。
- ネットワーク対策に関しては、基本的には「７．２．１　医療機関等の職員による外部からのアクセス」に示すものと同様の対策を講じること。なお、患者への情報提供は、一般的には参照のみとなること、患者等においては職員以上に単純な仕組みが求められることなどを考慮して、対応策を検討すること。

７．２．３　医療機関等が保有する医療情報システムに対して、事業者が外部からアクセスして保守等を行う場合

- こちらについては、「１０．システム・サービス事業者による保守対応等に対する安全管理措置」に示す。

７．３　医療情報の破棄

- システム運用担当者は、企画管理者が作成した手順を踏まえて、医療情報の種別ごとに破棄の具体的なルールを作成することが求められる。
- 破棄の対象となるのは、
  - 情報機器等に格納した医療情報（過去に格納して削除したものを含む）
  - クラウドサービス、外部委託先のシステム等に保存された医療情報

  等が想定される。

- 医療情報を格納した情報機器等に対しては、格納されている医療情報を確実に破棄するため、OS のファイル管理システムによる削除のみでは不十分であり、専用のソフトウェア等により復元不能な形で確実に情報を削除するなどの対応が求められる。なお、記録媒体などを物理的に破壊することも選択肢となる。リース等により情報機器等を返却する場合も、同様の措置が求められる。情報機器等の廃棄を外部の事業者に委託した場合には、委託先の事業者から廃棄の証跡の提供などを求めて、確認すること。
- 例えば、下記のような対応が考えられる。
  - 情報機器等の廃棄時に、医療機関担当者による立ち会いや、HDD（Hard Disk Drive）などの記録媒体を含む全ての機器等が廃棄された写真やソフトウェア消去に係るログの提出を求めること
  - 医療機関等が指定した第三者の廃棄事業者により、情報機器等の廃棄を実施すること
    その際、廃棄事業者から、廃棄対象、方法、実施日、実施者および結果を含む廃棄証明書その他の証跡を入手し、内容を確認すること
  - 委託契約時においても、契約条項として HDD などの記録媒体を含めた情報機器等の廃棄について明確に合意すること
- 医療情報システムのデータベース等に格納したデータは、システム管理機能により破棄することになる。なお、データベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄することで、その他の情報が利用不能となるリスクがあることに留意すること。
- 事業者が保有するシステムに医療情報を格納している場合、破棄の証明等が難しい場合も想定される。このような場合、システム運用担当者は、企画管理者と連携して、事業者のデータ破棄手順などの確認をすることで破棄の状況を把握すること。

７．４　医療情報を格納する記録媒体、情報機器等の紛失、盗難等が生じた場合の対応

- システム運用担当者は、医療情報を格納する情報機器等の紛失、盗難が生じた場合の対応手順等を作成する必要がある。紛失や盗難に関する報告を受けた場合には、対象となる情報機器等の特定、ネットワークへの接続防止等の対応が想定される。また、記録媒体の暗号化を図るほか、例えばモバイル端末については、MDM（Mobile Device Management）を導入して遠隔制御を行うなど、可能な対策を事前に講じることも必要である。
- ネットワークを通じて外部サービスを利用する際には、設定のミスなどによる漏えいのリスクについても、同様に対応の手順を作成することが求められる。

８．利用機器・サービスに対する安全管理措置

【遵守事項】

① システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等のマルウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。

② 常時マルウェアの混入を防ぐ適切な措置を実施し、その対策の有効性・安全性の確認・維持を行うこと。

③ 医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、マルウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。

④ メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるファイル等の送受信の禁止、実行の停止又は無害化処理等を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。

⑤ 情報機器に対するパスワードの設定に関しては、製品等の出荷時におけるパスワードから変更し、「１４．認証・認可に関する安全管理措置」に示すパスワードの要件を満たすこと。

⑥ IoT 機器を利用する場合、次に掲げる対策を実施すること。医療機器、及びそれらに付属するシステム・機器についても同様である。

(1) IoT 機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。

(2) IoT 機器のファームウェア等の脆弱性リスクに対応するため、システムやサービスの特徴を踏まえてセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。

(3) 不正な接続を防ぐため、使用を終了、又は停止した IoT 機器をネットワークに接続したまま放置しないこと。

⑦ 企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。

⑧ BYOD の運用に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。

⑨ BYOD 端末であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。

８．１　マルウェア対策

- コンピュータウイルス、ワーム等様々な形態・呼称を持つマルウェアは、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る。マルウェアが侵入すると、セキュリティ機構の破壊、システムダウン、情報の漏えいや改ざん、破壊、資源の不正使用等、重大な問題が引き起こされる。
- 対策としてはマルウェア対策ソフトウェアの導入が効果的である。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、マルウェアの検出と除去が期待できる。
- システム運用担当者は、企画管理者と協働して、このようなマルウェア対策についての措置を講じるほか、これに必要な規則等の策定を行うこと。
- マルウェアは常に変化しているため、検出するためのパターンファイル等を、可能な限り、常に最新のものに更新しておくこと。システム運用担当者は、パターンファイルの更新による医療情報システムへの影響を調査しておくことも必要である。
- また、マルウェア対策ソフトを導入したとしても、全てのマルウェアが検出できるわけではない。医療情報システム側の脆弱性を可能な限り小さくしておくことや被害拡大の防止策を講じておくことが重要である。対策としてはセキュリテ

ィ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの閉鎖、ネットワークの構成分割やネットワーク間のアクセス制御、マクロ等の利用停止、メールやファイルの無害化がある。また、EDR（Endpoint Detection and Response）等による「振る舞い検知」も有効な方策である。いずれの対策を行う場合も、業務への影響や、処理の速度、可用性について、事前に十分検討すること。

- 医療機関等の外部で利用する端末や PC 等についても同様のリスクがあり、これらの情報機器等についても、上記の対応を行うこと。

８．２ 情報機器等の脆弱性への対策

- システム運用担当者は、医療情報システムが利用する情報機器等の脆弱性に関する情報を常に収集し、脆弱性への対応を速やかに行う必要がある。
- 情報機器等には、利用者が直接利用する PC 等の端末のほか、医療情報システムで利用する機能等のサービスを提供するサーバや、ネットワークに関連する機器等、様々なものがある。
- 近年のサイバー攻撃では、情報機器等に内蔵されるファームウェアや、格納されるプログラム等の脆弱性、EOS（End of Support：サポート終了）の対象となった情報機器等が起点となり、攻撃を受ける事案が多くみられている。必要な脆弱性対策が見逃されたことに起因するランサムウェア攻撃も見られる。
- システム運用担当者は、情報機器等に関して、定期的に脆弱性スキャンを行うほか、脆弱性に関する最新の情報を収集することが求められる。PC の OS に関する脆弱性情報は、OS やマルウェア対策ソフトを提供する事業者などが提供している。また、重大な脆弱性情報は「国家サイバー統括室（NCO）」や「独立行政法人情報処理推進機構（IPA）」などが定期的に公表している。これらの情報を確認するほか、契約事業者に対応を確認するなどして、最新の情報を入手すること。
- 利用するソフトウェアについて、SBOM[1]（Software Bill of Materials：ソフトウェア部品表）が事業者から提供されることもある。システム運用担当者は SBOM を用いることで、脆弱性を適切に管理し、安全性及び可用性を脅かすリスクを低減できる。そのため、システム運用担当者は、医療情報システムの導入時、及び保守時などにおいて適宜、SBOM の提供、またはこれに基づく安全性の確認を医療情報システム等提供事業者に求めること[2]。
- 必要に応じて速やかに脆弱性対策を講じる必要があるが、他のソフトウェアの動作等に影響することも想定される。事前に事業者に脆弱性対策の実施の可否を確認し、対応が難しい場合には、当該リスクに対する対策や管理方法を協議の上、代替策を講じること。
- 検査装置等に付属するシステム・機器についても同様である。また医療機器が EOS を迎えた場合の対応等については、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」を踏まえ、医療機器安全管理責任者等の医療機器を管理する部署の担当者と医療情報システム安全管理責任者等のシステム担当者が十分に連携を取りながら管理すること。

[1] ソフトウェアの構成部品や依存関係等を網羅したリストであり、脆弱性管理などの安全対策における基礎情報となるもの

[2] SBOM の取扱いについては、「医療機器のサイバーセキュリティ導入に関する手引書」の「附属書 A. ソフトウェア部品表（SBOM）の扱い」が参考になる。

- 本ガイドラインは、医療情報の適切な保全を目的として IoT 機器の適切な取扱いに関する要件を定めており、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」（昭和 35 年 8 月 10 日法律第 145 号）の定める医療機器のサイバーセキュリティの対策については、「医療機器におけるサイバーセキュリティの確保について」[3]、「医療機器のサイバーセキュリティ導入に関する手引書」[4]、「医療機関における医療機器のサイバーセキュリティ確保のための手引書」[5]等を踏まえて、医療機器の製造販売業者と必要な連携を図ること。

8．3　端末やサーバの安全な利用の管理

- システム運用担当者は、端末やサーバ等の情報機器が安全に利用されていることを確認する必要がある。
- 安全な利用については、8．1、8．2に示す対策のほか、例えば情報機器の起動にパスワード等の設定を行うなど、必要な措置を講じることが求められる。また製品出荷時にパスワード等が設定されているものは、必ず製品出荷時から変更すること。サーバで利用するソフトウェアの管理者権限を有するアカウントのパスワードにおいても同様である。
- 外部からの攻撃等のリスクを下げる方法の一つとして、不要な情報機器等を使用しない、不要な医療情報システムを稼働させない、などの対応も必要である。利用されていないにもかかわらず、外部と接続可能な情報機器がある場合、攻撃対象となり得る。また業務によっては、明らかに利用する可能性がない（または低い）時間帯にはシステムの稼働を停止することにより、業務時間外の攻撃リスクを低減できる。システム運用担当者は、業務での必要性や利便性などを勘案して、システムの稼働時間等を整理の上、適切な設定を行うこと。

8．4　情報機器等の棚卸

- システム運用担当者は、企画管理者が行う台帳管理を踏まえて、企画管理者と協働して情報機器等の棚卸をすることが求められる。棚卸を行うことで、情報機器の所在が明確になり、紛失、漏えい等のリスクを効率的に発見することが期待される。また情報機器等の滅失状況なども併せて確認することにより、利用の可否も確認でき、バージョンアップや買換え等、必要な対応が可能となる。

8．5　医療機関等が管理する以外の情報機器の利用に対する対策

- システム運用担当者は、医療機関等が管理する以外の情報機器を、医療情報システムにおいて利用するために必要な措置を講じ、そのための手順等を策定したうえで、企画管理者に報告することが求められる。
- BYOD を許可する場合は、上記の要件を実現するため、下記に掲げるような対策を選択・採用し、十分な安全性を確保する必要がある。

  ・管理者以外による端末の OS 設定の変更を技術的あるいは運用管理上で制御する

  ・他のアプリケーション等からの影響を遮断しつつ、端末内で医療情報を取り扱うことを制限する。さらに個人でその設定を変更できないよう制御し、OS レベルで管理領域を分離する。

  ・運用管理規程によって利用者による OS の設定変更を禁止し、かつ安全性の確認できないアプリケーションがモ

[3] 平成 27 年 4 月 28 日薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号「医療機器におけるサイバーセキュリティの確保について」

[4] 令和 5 年 3 月 31 日薬生機審発 0331、第 11 号薬生安発 0331 第 4 号「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」

[5] 令和 5 年 3 月 31 日医政参発 0331 第 1 号、薬生機審発 0331 第 16 号、薬生安発 0331 第 8 号「医療機関における医療機器のサイバーセキュリティ確保のための手引書について」

バイル端末にインストールされていないことを管理者が定期的に確認する。

- マルウェアや不適切な設定がなされたソフトウェアにより、外部からの不正アクセスが発生することも想定されるため、管理されていない端末での BYOD は許可してはならない。また、BYOD の導入に際して、管理者はコスト・利便性とリスクを評価して検討すること。

9．ソフトウェア・サービスに対する要求事項

【遵守事項】

① システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。

② 情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。

③ 医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成すること。また、これに従い必要な措置を講じ、企画管理者に報告すること。

④ 医療情報システムの目的に応じて情報を速やかに検索表示、又は書面に表示できるよう措置を講じること。

9．1 ソフトウェアの構成管理

- システム運用担当者は、医療情報システムで利用するソフトウェアが、適切な構成となっていることを確認する必要がある。特に医療情報システムをオンプレミスで構築している場合には、医療情報システムを構成するソフトウェアのバージョンや組み合わせ等を適切に管理することが求められる。ソフトウェアの構成が適切に管理されない場合、医療情報システムの動作に支障をきたす、セキュリティ上の脆弱性が残存するなどのリスクが生じる。
- システム運用担当者は、このような構成管理について、手順（あるいはこれに相当するバッチ処理のための仕組み等）が整備されているか、本来構成すべきソフトウェアのバージョンが適切に管理されているか等を、事業者に確認すること。構成管理に関する計画の策定、実施がなされていることを確認することが重要である。
- クラウドサービスの場合は特に、このような構成管理を直接、医療機関等が行うことは困難であり、同様に手順や計画の整備状況、実施状況の確認を行うこと。

9．2 情報機器・ソフトウェアの導入や変更時における品質管理

- 医療情報システムの導入や変更時は、想定した品質で稼働することの確認が必要である。施行通知では、「目的に応じて速やかに検索表示又は書面に表示できる」ことを求めている。安定的な医療の提供のため、このようなソフトウェアの品質を適切に管理すること。
- システム運用担当者は、医療情報システムの導入や変更時に直接品質を確認するほか、要求仕様書等において特に重視する品質について明示することで、事業者に品質確保を求めることが想定される。
- システムの移行時についても同様である。移行時の特殊性として、移行前のデータが正しく移行後のシステムに反映され、利用可能であることが求められる。利用者権限をはじめ、各種設定が移行前の設定が、適切に移行後にも設定されていること等を確認すること。
- 求められる品質は、医療情報システムの特性や目的に応じて異なる。e-文書法によれば、画面上での見読性が求められているが、業務の要求によっては対象の情報の内容を直ちに書面等に表示できることも必要となる。

１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置

【遵守事項】

① 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。

② 診療録等の外部保存を受託する事業者に対しては、個人情報の保護を厳格に監督する必要がある。受託する事業者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みを設けること。（ただし、事業者が個人情報を保存するのみで、取り扱わない契約となっている場合、医療機関等には個人情報保護法第 27 条第 5 項第 1 号に基づく監督義務は生じない。この時、適切に事業者に対してアクセス制御がされている必要がある。）

③ 保守作業のためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びにアクセスした対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。

④ リモートメンテナンスを行う場合には、外部からの攻撃等のリスクを低減するために、外部接続等への対策等、必要な措置を講じること。

⑤ リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集すること。作業終了時には、保守に関する作業計画書と照合することなどにより確認を実施し、終了後速やかに企画管理者に報告し、確認を求めること。

⑥ リモートメンテナンスにおいて、事業者がやむを得ずファイルを医療機関等へ送信する場合、送信側で無害化処理が行われていることを確認すること。

⑦ 事業者がやむを得ず診療録等を参照する必要がある場合も、医療機関等に許可を受けたうえでアクセスし、医療機関等で求められる水準と同等の秘密保持を行うこと。

１０．１ 保守時の安全管理対策

- 医療情報システムの適切な稼働を維持するためには、定期的な保守（メンテナンス）が必要である。保守作業には主に障害対応や予防保守、ソフトウェア改訂等があり、障害対応時は、原因特定や解析等のために障害発生時のデータを利用する。この際、保守要員が管理者権限で直接医療情報に触れる可能性があるため、想定される脅威に対する対策が必要になる。具体的には、下記が想定される。
  - 保守要員等からの医療情報の流出・漏えい
  - 保守に伴う医療情報の破壊・破棄
  - 保守に伴う医療情報システムの破壊、障害の発生
  - 保守作業または保守環境に対するサイバー攻撃
- システム運用担当者は、このようなリスクに対応するために必要な措置を講じるほか、手順等を作成し、企画管理者に報告すること。
- システム運用担当者は、保守に当たって以下の内容について、確認することが求められる。
  - 保守計画等の策定・確認
  - 作業の監督・報告・確認
  - アクセス権限管理（不要な管理者権限を付与しない）
  - ログ取得
  - 動作確認時のテストデータに個人情報が含まれる際の対策

・　リモートメンテナンス（保守）時の対策

- 保守には、原則として事前申請・承認が必要だが、障害時や緊急を要する脆弱性対応などにおいては、事後承認によることも想定される。
- オンプレミスの場合には、保守に関しては個別の申請や承認により行うことが可能であるが、パブリッククラウドによるサービスにおいては、個々の利用者に対する保守の申請や承認によることが難しい場合がある。システム運用担当者は、クラウドサービスにおける保守の場合には、保守の対象時間について事業者に確認したうえで、医療機関等内部で利用している情報システムへの影響範囲、必要があれば代替措置等について確認し、企画管理者に報告の上、医療機関等内部及び関係者に周知することが求められる。
- また保守を行う際には、サーバ上の OS や DBMS などで製品出荷時に設定されている管理者 ID（例えば Administrator）などは使わず、各保守担当者の ID を設けて、管理者権限を付与する等、保守した者が特定できるようにすることも求められる。

１０．２ リモートメンテナンスにおける安全管理対策

- リモートメンテナンスの採用は、業務効率化が期待されるものの、攻撃者にとって「正規のルートを装って侵入できる絶好の裏口」となり、サイバー攻撃の起点となり得る。
- リモートメンテナンスにおけるリスクとしては、認証・アクセス管理に関するリスク、通信経路・接続方式に起因するリスク、システム・ツール関連のリスク、人的・運用関連のリスク等が指摘される。これらのリスクは、医療情報システム全体に共通するものであるため、本ガイドラインで示す対策を適切に講じること。
- また、リモートメンテナンスでは、システムの管理者権限を要する場合があり、高いリスクを伴うことから、下記の対策を行うこと。

表１０―１　リモートメンテナンスにおいて実施すべき事項

想定されるリスク	実施すべき事項（各リスクに示される実施すべき事項は、選択して対応すること）
認証・アクセス管理に関するリスク	・OS の二要素認証の採用（「１４．１．１　利用者の識別・認証」参照） ・特権 ID 権限の厳格管理（管理者共通アカウントの禁止等） ・アクセス経路の制限（端末・IP アドレスを限定等） ・セッション・タイム・アウト機能の導入
通信経路・接続方式に起因するリスク	・暗号化（SSH、VPN 等、「１３．ネットワークに関する安全管理措置」に記載されている安全なプロトコルの採用、RDP・VNC などを直接インターネットに開放しない利用等） ・リモートアクセス用ゲートウェイの利用
システム・ツール関連のリスク	・管理端末のセキュリティ強化（マルウェア対策、USB 端末規制等）
人的・運用関連のリスク[6]	・ログの定期的レビュー ・管理監督強化 ・外部委託管理強化 （外部委託者用アカウントの管理、契約上の責任管理等）

[6] 医療機関等は、事業者がリモートメンテナンスをする場合には、適時、実施状況を確認することが求められる。事業者が行うリモートメンテナンスについては、「リモートサービス　セキュリティガイドライン」が一般社団法人保健医療福祉情報システム工業会(JAHIS)より示されているので、上記の確認において参考となる。なお、同ガイドラインは適宜改定しているため、最新の版を参照することが求められる。

１１．システム運用管理（通常時･非常時等）

【遵守事項】

① 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。

(1) 「非常時のユーザアカウントや非常時用機能」の手順を整備すること。

(2) 非常時機能が通常時に不適切に利用されることのないように管理するとともに、もし使用された場合には検知できるよう、適切に管理及び監査すること。

(3) 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。

(4) 医療情報システムにマルウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。

(5) サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分離されたネットワークを整備すること。

(6) 重要なファイルは数世代バックアップを複数の方式で確保し、その一部はマルウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

② 医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。

１１．１　通常時における運用対策

- システム運用担当者は、通常時から非常時を想定した技術的対応を、講じることが求められる。
- 非常時の原因としては、下記が想定される。
  - 災害
  - サイバー攻撃
  - システム障害（ネットワーク障害含む）
- 上記対策として共通することは、非常時の医療情報システムの利用に関する手順等について、通常時から整理をすることや、非常時を想定した訓練を行うことなどが挙げられる。
- 通常時における対策例については、企画管理編「11．２　非常時に備えた通常時からの対応」の「非常時の事象発生原因に応じた通常時からの対策例」に示しているが、技術的な対応としては、
  - ネットワーク（論理的／物理的な構成分割など）
  - バックアップ（冗長化、データバックアップなど）
  - 非常時用の情報システム、情報機器

  等を検討することが求められる。技術的な検討は、経営層が行うリスク判断や企画管理者によるリスク評価に整合する内容とすること。特にサイバー攻撃の場合、バックアップデータには既にマルウェアの混入による影響が及んでいる可能性も高く、不用意にバックアップデータから復旧することで被害を拡大する等のリスクもある。総合的な観点からのリスク評価を踏まえて技術的な検討を行い、結果を企画管理者に報告すること。

表１１－１　通常時に対応すべき技術的対応例

対応目的	バックアップ	非常時用の臨時システム
災害	・広域災害対策（遠隔地バックアップ等）　など	・代替するバックアップサイトの構築 ・臨時の認証方法の採用　など
サイバー攻撃	・論理的／物理的なネットワークの構成分割	・サイバー攻撃時においても利用可能な情報システム資源の確保　など

	・追記不能型のデータバックアップの記録媒体の整備（一定期間追記不能型の WORM[7]ストレージを含む） ・システム再構築のための情報機器等のインフラバックアップ など	
システム障害 （ネットワーク障害も含む）	・即時切換え可能なシステムバックアップ など	・冗長化と切換え対応 など

- 医療情報システムの稼働状況が正常であることを把握するため、医療情報システムのパフォーマンス管理や、死活管理を行い、パフォーマンスが低下した場合やシステムがダウンした場合に、速やかに把握可能な状態とする必要がある。医療情報システムの運用に専任の担当者を設けることができない場合には、適宜、事業者から、システムのパフォーマンスの状況等で異常が発生した場合に、速やかに連絡を受けられるような体制を設けること。
- また非常時に備えた対策として、OS のセキュリティ・パッチ適用後やマルウェア対策ソフトのパターンファイル最新化後の稼働確認、あるいはバックアップファイルの復旧テストなどを実施することが求められる。この際に、これらの作業は、実際の運用環境とは分離して行うこと。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必要である[8]。

１１．２ 非常時における対応

- システム運用担当者は、非常時において、あらかじめ作成した手順に従い必要な措置を行うことが求められる。併せて通常時の運用への復旧手順も整備すること。
- 非常時における対応の一つとして、非常時用ユーザアカウントの運用が挙げられる。災害等により通常時のユーザ認証が困難な場合や正規のアクセス権限者による操作が望めない場合、非常時用アカウントの運用により、医療情報の利用を円滑化し、医療サービス低下を最小限とすることが想定される。通常時への復旧・復帰後には非常時ユーザアカウントを更新するなどの措置を行うこと。
- 非常時は、通常時とは異なる運用が想定される。例えば、災害時は、受付での患者登録を経ないような運用が考えられ、必要に応じて運用に対応した機能を実装する必要がある。一方で非常時への対応機能の用意は、逆にリスクを増加させる懸念もあるため、慎重に管理すること。
- 非常時の運用に関する事前の準備や周知不足は医療情報システムや医療機器の円滑な利用を阻害するリスクがある。システム運用担当者を含む関係者間で十分な準備を実施し、情報を共有しておくこと。

[7] WORM：WORM=Write Once Read Many。データを一度書き込んだ後は、内容の変更や削除をできないようにする仕組みで、保存後のデータ不変性を仕組みとして担保し、改ざんや意図しない消失を防ぐことを目的とする。

[8] 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を最小限とするため、まず影響の少ないセグメントから段階的にパッチを適用し、稼働状況に問題がないことを確認しながら、順次適用範囲を拡大していく対応等が考えられる。

１２．物理的安全管理措置

【遵守事項】

① 医療情報及び医療情報システムを保管する場所を選定する際には、リスク評価を踏まえ、企画管理者と協働して検討、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。

② 医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。

③ サーバルーム等の十分なセキュリティ確保が求められる領域においては、持ち込まれる物品の確認・制限を実施すること。 個人情報の保管等、重要な用途に利用される情報機器には盗難防止策を講じること。

④ 医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等に基づく措置を実施し、非常時に利用できるよう、適切に管理すること。

⑤ 記録媒体、ネットワーク回線、設備の劣化による情報の読み取りが不能となる等のリスクを防止するため、記録媒体が劣化する前に、新たな記録媒体への複写を実施する等、適切な保管措置を講じること。

⑥ 利用者が医療情報を入力・参照する端末から長時間離席する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。

１２．１ サーバルーム等の物理的要件

- システム運用担当者は、医療情報及び医療情報システムを保管する場所（サーバルーム、マシンルーム等）を、リスク分析の結果を踏まえて、企画管理者と協議の上、選定することが求められる。災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造であるよう考慮するほか、結露や高温による情報機器の暴走するリスク等にも留意すること。
- サーバルーム等の医療情報システムが格納されているセキュリティ区域は、職員を含め、入退管理がなされており、カメラによる監視などがなされていることも必要である。
- 医療情報の記録媒体や医療情報システムが格納されるキャビネットやシステムラックなどは、施錠管理すること。
- サーバルーム等のセキュリティ境界へ持ち込む物品を確認・制限すること。例えば可搬型記録媒体の持ち込みは、大量のデータ漏えいにつながるリスクがある。

１２．２ バックアップの管理

- システム運用担当者は、企画管理者が運用管理規程等に定めたルールに基づいて、適切にバックアップを確保し、非常時に利用可能な状態で管理することが求められる。運用管理規程では、バックアップ頻度、方法等を明らかにし、原因に応じて、「１１．１ 通常時における運用対策」に示すバックアップ対応を行うこと。またサイバー攻撃を想定したバックアップの確保については、「１８．外部からの攻撃に対する安全管理措置」を参照すること。
- バックアップの外部保存を委託している場合は、委託先事業者に対して、バックアップの対象、頻度、復旧できる世代、バックアップ方法、保存場所等を確認し、SLA 等において明らかにすること。
- バックアップを含む記録媒体について、媒体そのものや設備等の劣化によって情報の読み取りが不能となることを防止するための措置を講じること。保管環境に留意するほか（高温多湿を避ける、直射日光等を避ける等）、記録媒体が劣化する前に、保管されている情報を新たな記録媒体に複写する等の措置を講じること。また記録媒

体及び情報機器ごとに劣化が起こらずに正常に保管が可能な期間を明確にするとともに、使用開始日、使用終了予定日を管理して、定期的に可読性に関するチェックを行うこと。また、この手順を作成すること。

- 診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報の保護には十分に配慮する必要がある。また、バックアップにおける個人情報の取扱いについても、オリジナルデータと同様の水準が求められる。
- 具体的には、システム運用担当者は以下についての対応が求められる。
  （1） 診療録等の記録された可搬媒体が搬送される際の個人情報保護
  （2） 診療録等の外部保存を受託する事業者内における個人情報保護

１２．３ その他

１２．３．１ 記録媒体等の経年変化の管理・委託事業者への配送等

- ネットワークに接続されない可搬媒体を用いて外部保存を行う場合、ネットワーク上の脅威に基づくなりすましや盗聴による情報の大量漏えい等のリスクは低減される。
- 可搬媒体を目視しても内容が見えるわけではないので、搬送時の機密性は比較的確保しやすい。暗号化機能を有する媒体では、パスワードによるアクセス制限により、さらに機密性は増す。一方で、可搬媒体には耐久性の低い製品も存在し、経年変化等に対して慎重に対応する必要がある。また、一記録媒体あたりに保存される情報量が極めて多いことから、紛失リスクに対してより慎重な対応が必要である。
- 診療録等を可搬媒体に記録して搬送する場合は、混同や紛失を防止するため、以下の点に注意すること。
  － 診療録等を記録した可搬媒体の紛失防止
    運搬用車両や搬送用ケースの施錠等の処置を施すこと
  － 診療録等を記録した可搬媒体と他の搬送物との混同の防止
    他の搬送物との混同が予測される場合には、別のケースや系統に分け、同時に搬送しないこと
  － 搬送業者との守秘義務に関する契約
- 外部保存を委託する医療機関等は、受託事業者に個人情報を取り扱わせる場合、個人情報保護法を遵守させる管理義務を負う。したがって両者の間での責任分担を明確化し、守秘義務に関する事項等を契約上明記すること。
- なお、受託事業者に個人情報を取り扱わせない契約としている場合には、医療機関等は、自医療機関等の安全管理措置の一環として、個人情報保護法を遵守しつつ、安全管理に関する措置をとることが求められる（個人情報保護法に関するガイドライン Ｑ７－５４参照）。

１２．３．２ 端末・サーバ装置等の不適切な利用等に関する対策

- システム運用担当者は、利用者が医療情報を入力・参照する端末から長時間離席する際に、正当な利用者以外の者による入力・参照を防止するため、自動での画面ロックアウト等の対策を実施すること。

１３．ネットワークに関する安全管理措置

【遵守事項】

① ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。

② セッション乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。

③ オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。

④ オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、通信方式や、認証手段を採用すること。採用する認証手段は、PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。また、暗号を用いる場合は、電子政府推奨暗号の暗号方式を採用すること。

⑤ ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なソフトウェア等の混入が生じないよう、セキュリティ対策を実施すること。特に VPN 接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。また、機器の管理インターフェイスやログインページ、管理ポートに対して接続を許可されていない機器が、外部からアクセスできないよう設定すること。

⑥ オープンなネットワークにおいて、IPsec による VPN 等を利用せずプロトコルを限定した TLS 接続をする場合（HTTPS、FTPS 等）、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証（mutual-TLS）、または、これと同等以上の安全性を有する、端末の識別・認証による接続端末制限の措置をすること。ただしシステム・サービス等の対応が困難な場合には TLS1.2 の設定によることも可能とする。TLS の設定はサーバ/クライアントともに「TLS 暗号設定ガイドライン[9]」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。

⑦ 医療機関等が管理する医療情報システムと接続する際に用いる通信経路の暗号化を図る場合には、原則として専用線、IP-VPN、又は IPsec＋IKEv2(PSK 認証を除く)によること。SSL-VPN は、偽サーバへの対策リスクや長時間の接続におけるリスク等が含まれるため、使用する場合には⑥に示す対策を行ったうえで、「クライアント型」を選択すること。クライアント型では専用のクライアントソフトがインストールされた端末との間でのみアクセスが可能となる。

また、ソフトウェア型の IPsec 又は TLS1.2 以上により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。

⑧ 利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。

⑨ 医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。

⑩ ネットワーク経路でのメッセージ挿入、マルウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。

[9] IPA より公表。なお、随時改定されるため、最新のものを参照すること。

⑪ 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。

⑫ 医療機関等がネットワークを通じて通信を行う際には、正当な通信の相手であることを確認するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等との間でも同様に相互認証機能を設けること。

⑬ 医療情報システムにおいて無線 LAN を利用する場合、次に掲げる対策を実施すること。

(1) 適切な利用者のみに無線 LAN の利用を制限すること。例えば、ANY 接続拒否等の対策を実施することが考えられる。

(2) 不正アクセス対策を実施すること。例えば電子証明書、IP アドレス、MAC アドレス等によるアクセス制限を実施すること。ただし、例えば MAC アドレスによるアクセス制限の場合、モバイル端末においてプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることや、詐称可能であることから、MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。

(3) 不正な情報の取得を防止するため、WPA2-EAP、WPA3 等により通信を暗号化すること。

(4) 利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること。

１３．１ ネットワークに対する安全管理

- システム運用担当者は、リスク評価を踏まえ、企画管理者と協働して利用するネットワークを選定すること。
- 本ガイドラインでは、下図のようにネットワークに関する用語の整理を行った。ネットワークの安全性を検討する際には、ネットワークにおける各レイヤで、対策が講じられると想定される。

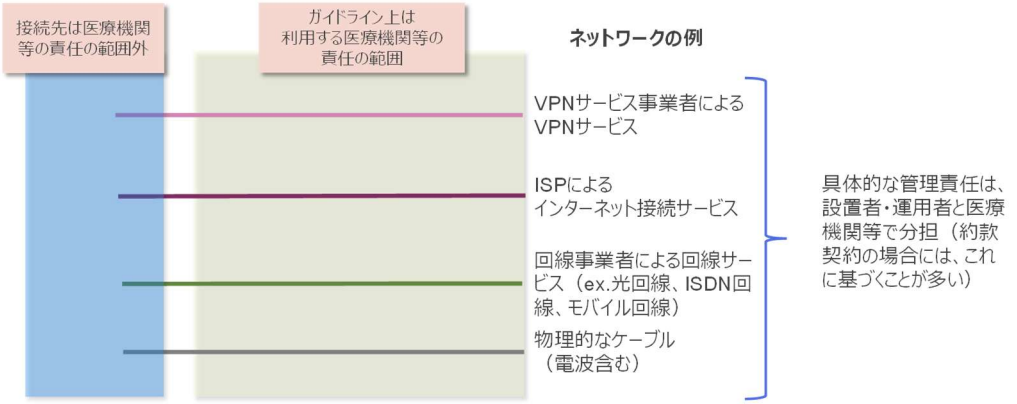


図１３－１ ネットワークの管理に対する考え方

- 本ガイドラインでは回線のレイヤと接続先が限定されているか否かは別の概念であると考える。このとき、ネットワークの安全性は、「接続先が限定されているか」と「経路が管理されているか」を考慮するのが妥当である。
- 図１３－２のように、ネットワークの接続先の限定は、さまざまな形で実現できる。リスクの違いはあるものの、回線の暗号化を講じることで、いずれの場合にも、従来の境界防御として整理することができる。
- 一方、接続先が限定されていなかったり、経路が管理されていない場合には、「オープンなネットワーク」に位置付けられる。この場合も、インターネット VPN 等のサービスを利用することで、境界防御に近い対応が可能である。

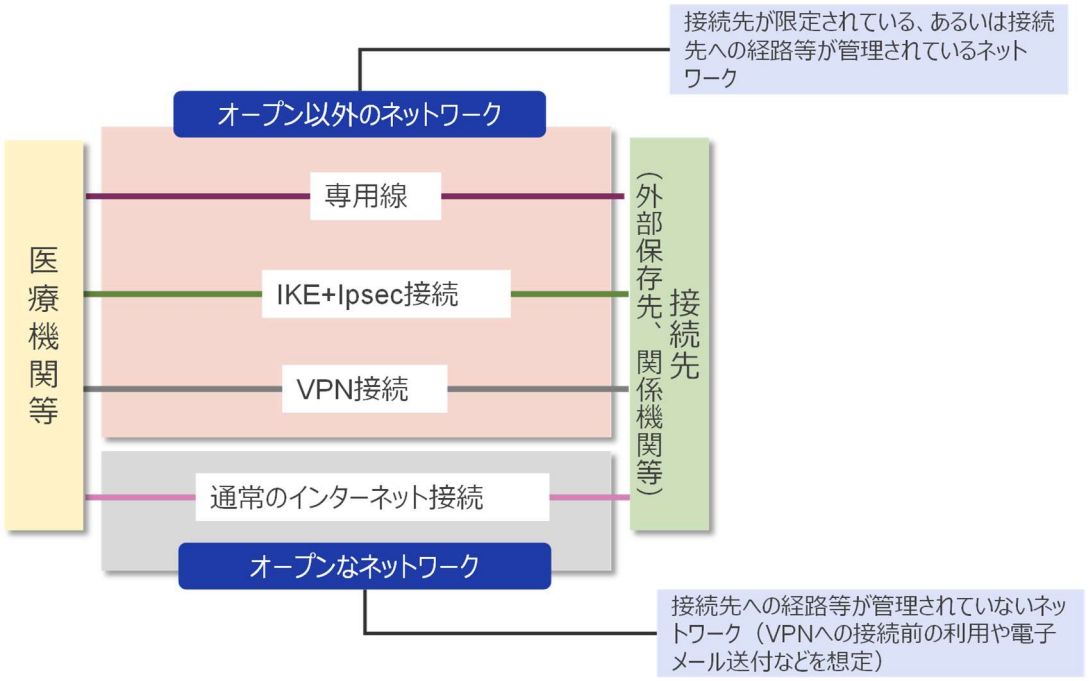


図１３－２　本ガイドラインにおけるネットワークの整理

- 本ガイドラインでは、接続先等の管理がなされていないネットワークを「オープンなネットワーク」とし、接続先が限定されている、あるいは接続先までの経路等が管理されているオープンではないネットワークを「セキュアなネットワーク」と称する。医療情報システムの利用は、原則として「セキュアなネットワーク」を用いること。但し「セキュアなネットワーク」と同様の安全性を確保する途中経過として「オープンなネットワーク」を用いたり、電子メールの送信時において、データを暗号化して送信する際に用いることなどが想定されるため、併せて利用のための遵守事項を整理する。

１３．１．１　セキュアなネットワークの構築

- システム運用担当者には、医療情報システムへの不正な機器の接続、不正ソフトウェア等の混入、異常データ通信を防止するため、セキュアなネットワークを構築し、接続する機器の構成を適切に管理することが求められる。
- セキュアなネットワークを構築するために、ネットワークの論理的または物理的な構成分割、接続機器の制御、通信するデータの制御等のセキュリティ対策を実施すること。
- ネットワーク構築にあたり、使用する IP アドレスの割当の規格として IPv6（Internet Protocol Version 6）の採用が進んでいる。IPv6 は透明性、完全性、可用性、管理性などの観点から、有効なセキュリティ対策として期待される。

  一方で、IPv6 の採用に伴い、新しい機能に関連する脆弱性（拡張ヘッダーの複雑な設定に伴う攻撃パケットの透過、一時 IPv6 アドレスを採用する場合に生じるリスクや、管理上の煩雑性の増加、IPv6 との併用に伴うトンネリング技術に内在するリスク等）が指摘されている。IPv6 を採用する場合にも、ネットワーク構成を踏まえたリスクの精査を行ったうえで、適切な対応を行うこと。

１３．１．２　選択すべきネットワークのセキュリティ

- システム運用担当者は、医療情報の安全管理が確保できるネットワークを選定することが求められる。
- ネットワークに関しては、専用線を用いることが最も安全であると言われてきた。専用線は、2 拠点間を物理的に接続し、利用者が独占的に使用する回線であることから、外部からの侵入や盗聴のリスクが小さいとされる。一方で専用線による場合には、高コストであることや、多目的な利用にはなじみにくいというデメリットもある。

- 専用線以外の仕組みを利用する際には、VPN（Virtual Private Network）と呼ばれる専用線同様のサービスを仮想的に実現する仕組みがある。VPN にはいくつかの実装方法がある。
- IP-VPN は、通信事業者が管理する閉域ネットワークを利用するため、通信事業者以外の侵入のリスクは小さい。但し専用線ほどではないものの、利用コストは高いものとなる。
- オープンなネットワークであるインターネットを用いるサービスとしては、IPsec＋IKE で実現する VPN と SSL-VPN がある。IPsec は、ネットワーク層レベルでの暗号化を図る方法で、インターネット VPN の中でも安全性が高いとされる。SSL-VPN は SSL 技術を利用した VPN でセッション層における暗号化を図るものである。端末側でのアプリケーションが不要など、導入が容易である反面、偽サーバへの対策リスクや長時間の接続におけるリスク等があるとされる。
- IKE が使われている機器については、すでに寿命を迎えた暗号技術（DES, 3DES, MD5, SHA-1 など）がデフォルト設定になっている機器が多いことに伴うリスクが内在する。従って、新規に購入する場合には、IKEv2 に対応したものを購入すること。また IKE が使われている機器については、「電子政府における調達のために参照すべき暗号のリスト」[10]に準拠していることを確認し、アグレッシブモードを使用している場合は、速やかに IKEv2 に移行すること。基本的には IPsec など安全性が高いネットワークを利用することが望ましいが、医療機関等のシステム化計画なども踏まえて、適切なものを選択すること。

表１３－１　通信経路・接続方式の適合性

<table>
<tr><th colspan="4">通信経路・接続方式</th><th>適合性[11]</th></tr>
<tr><td colspan="4">専用線</td><td rowspan="3">適合</td></tr>
<tr><td colspan="4">IP-VPN</td></tr>
<tr><td rowspan="4">インターネット</td><td rowspan="3">インターネット VPN</td><td colspan="2">IPsec ＋ IKE、IKEv2</td></tr>
<tr><td rowspan="2">SSL-VPN</td><td>クライアント型</td></tr>
<tr><td>その他</td><td>―</td></tr>
<tr><td rowspan="2">オープンなネットワーク</td><td colspan="2">TLS1.3 (高セキュリティ型)+クライアント証明書</td><td rowspan="2">適合</td></tr>
<tr><td colspan="2">TLS1.2 (高セキュリティ型)＋クライアント証明書</td></tr>
</table>

- オープンなネットワークを通じて接続先が限定されているセキュアなネットワークへ接続する場合、セキュアなネットワークに到達するまでのオープンなネットワーク（インターネット）経由において、事業者によるチャネル・セキュリティが確保されないリスクがある。チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前に事業者との契約を確認し、確実にチャネル・セキュリティを確保すること。
- 最新の VPN 技術を利用する場合であっても、それが盗聴防止、なりすまし防止、アクセス管理、適切な認証手段の確保といったガイドラインが要求するセキュリティレベルを確実に満たし、特に外部アクセスにおいて求められる厳格な安全対策（例：二要素認証に相当する措置）を組み合わせて実現できるのであれば、利用可能と解釈できる。ただし、実際に新しい VPN 技術を採用する際には、事前のリスク評価に基づいて、そのプロトコルが要求される安全水準を満たしていることを確認すること。また、システム関連事業者からサービス仕様適合開示書な

[10] 「電子政府における調達のために参照すべき暗号のリスト」(CRYPTREC 暗号リスト)。デジタル庁、総務省及び経済産業省が、CRYPTREC の活動を通して安全性・実装性能等を評価したうえで公表するリスト。電子政府推奨暗号リスト、推奨候補暗号リスト及び運用監視暗号リストで構成される。

[11] ここで言う適合性はあくまで表１３－１における適合性であり、「１３．ネットワークにおける安全管理措置」の遵守事項をすべて満たして初めて本ガイドラインに適合しているとみなすことができる。

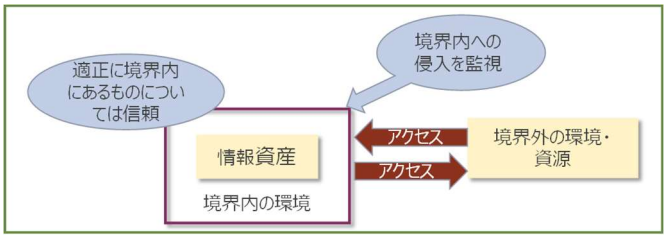
どの必要な情報提供を受けて、責任分界を含めた具体的な運用を取り決めること。

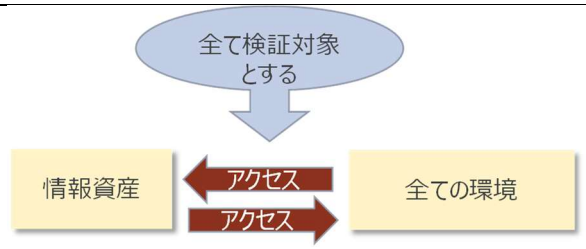
- なお、VPN 機器への脆弱性対策として、クラウド型 VPN の採用や、自動アップデートに対応した製品を選定することが望ましい。ルータ等のネットワーク機器は管理インターフェイスやログイン画面が露出していることが侵害される原因になっているので、これらを露出させない必要がある。そのため、機器の管理インターフェイスやログインページ、管理ポートに対して接続を許可されていない機器が、外部からアクセスできないようにすること。
- 医療機関等がクラウドサービスを利用する場合、事業者との間の通信経路が暗号化されていれば、当該経路の盗聴のリスクは小さい。TLS の設定を適切に行い、TLS クライアント証明書による認証を受けることにより通信経路のセキュリティは確保されるが、クラウドサービス事業者内部での通信について、十分な安全性は保証されない。医療機関等は、クラウドサービス事業者内部で用いる通信について、暗号化等十分な安全性を講じることを求めること。
- 医療機関等が管理する医療情報システムに対して、外部から接続する場合（リモートメンテナンス、テレワーク等）には、内部のネットワークにおける盗聴のリスクも考慮し VPN 等を用いたセキュアなネットワークによる接続を要する。このとき、併せて「７．２　医療機関等外から医療情報システムに接続する利用の場合への対策」、「１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置」に示す対策を講じること。
- なお、システム運用担当者はネットワークを選定した際に、その管理や非常時の対応など、具体的な技術的な対応について、ネットワークを提供する電気通信事業者や、情報システム・サービスを提供する事業者との間での責任分界の範囲を明らかにしたうえで、企画管理者に報告すること。

１３．２　不正な通信の検知や遮断、監視

- 医療分野では、セキュアなネットワークを選択し、境界防御を想定した対応が一般的である。一方で、クラウドサービスの普及や、テレワークによる業務システム環境の変化等、情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界防御のみによる十分なセキュリティ対策は困難になりつつある。例えばVPN 装置による境界での対策を過信しており、内部に侵入された際の横断的侵害（水平展開）への対策が不足していたことで、サイバー攻撃の被害が拡大した例も複数存在する。
- 近年は、境界防御の思考による安全性に限らず、全てのトラフィックについての安全性を検証するという「ゼロトラスト」の概念が普及しつつある。ゼロトラスト思考は、利用者の行動も含めて全て検証し、異常とみられる事象が発生したタイミングで、利用者の正当性などを確認する仕組み等で構成される。

表１３－２　境界防御型思考とゼロトラスト思考の比較

境界防御型思考 	・　オープンな環境（管理者により管理されていない環境）とオープンではない環境（管理者により管理されている環境）を想定したうえで、オープンではない環境については、その境界部分への侵入を防ぐため、監視を行う。 ・　オープンではない環境では、医療情報等、特に重要な情報の管理を行う。
ゼロトラスト思考	・　オープンではない環境とオープンな環境のいずれにおいても、情報資産へのアクセスについては、不正なものが含まれうることを

	前提（ゼロトラスト）に、全てを検証対象とする。 ・ 検証は、情報資産に対するアクセスにおいて、不正なトラフィックやアクセス等の異常行動などを起点として捉える。

- 例えば振る舞い検知機能により、利用者のアクセスを監視し、通常の運用と異なるアクセスが生じた際に、必要な制御を行うことができる。一方で、これを実装するためには、現時点では費用や管理に対する負担が大きいとされており、医療機関等においても小規模の医療機関等で導入することは必ずしも容易ではない。導入に当たってはリスク分析の結果を踏まえて判断することが望ましい。
- 医療機関で境界防御を採用する場合でも、トラフィックの監視等、多層防御による対策が必要である。
- 例えば、クラッカーやマルウェアによる攻撃から情報を保護するための一つの手段として、ファイアウォールの導入があるが、これに加えて、不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）などを採用することが考えられる。またシステムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断や脆弱性スキャン）を定期的に実施し、パッチ適用等の対策を講じておくことも重要である。これは、「８．２　情報機器等の脆弱性への対策」と併せて実施すること。
- 内部脅威監視や EDR などの措置を講じることも、有効な対策として挙げられる（「８．１　マルウェア対策」参照）。モニタリングについては、費用対効果を鑑みて、リスクの高い箇所に対し重点的に実施することも想定される。

１３．３　通信の暗号化・盗聴等の防止

- システム運用担当者は、医療情報システムが利用するネットワークの安全性を確保するために、利用するネットワークの回線、または送信する医療情報に対して暗号化措置を講じることが求められる。
- また送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威に対して適切な対策を講じること。

１３．３．１　ネットワーク回線の暗号化

- 特にオープンなネットワークでは、盗聴のリスク等があることから、医療機関等の外部と医療情報のやり取りする場合には、TLS の設定を適切に行って、暗号化することが求められる。またオープンなネットワークを経由して SSL-VPN を利用する場合には、クライアント型を採用すること。
- 医療機関等がクラウドサービスを利用する場合、クラウドサービス事業者との間の通信経路の暗号化が保証されていれば、当該経路の盗聴のリスクは小さい。TLS の設定を適切に行い、TLS クライアント証明書（2026 年以降のパブリック認証局による制限に留意し、公的認証局から発行されたクライアント証明書、又はプライベート認証局の利用を検討すること）[12]等による認証を受けることにより、必要な暗号化がなされる。但しこの場合、クラウドサービス事業者内部での通信は暗号化されないため、医療機関等は、クラウドサービス事業者内部で用いる通

[12] 公的認証局から発行されたサーバ証明書をクライアント証明書に利用してはならない。サーバ証明書をクライアント証明書にも利用するとセキュリティ上のリスクを有することから、大手ブラウザ事業者において、2026 年 6 月 15 日以降、「正当な端末」と認識されなくなるとされる。

信についても十分な安全性対策を求めること[13]。

- 医療情報システムに対して、医療機関等の外部から接続する場合（例えばリモートメンテナンスによる場合や、テレワーク、訪問看護など）、医療機関等の内部のネットワークにおける盗聴リスクがあることから、セキュアなネットワークによる接続が必要となる。これに対応するため、VPN 等を用いた経路の暗号化措置を施すこと。このとき、併せて「７．２　医療機関等外から医療情報システムに接続する利用の場合への対策」、「１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置」に示す対策を講じること。

１３．３．２　情報に対する暗号化

- 医療機関等の内部のネットワークを通じて外部に医療情報を送信する場合、必要に応じて、送信する医療情報自体に暗号化を施すことが求められる。特にオープンなネットワークの場合には、医療情報が相手先までに到達する経路が保証されないリスクに留意すること。

１３．３．３　盗聴防止等

- ネットワークを利用して医療情報を外部と交換する場合、送信先に確実に情報を送り届ける必要がある。システム運用担当者は下記脅威に対して適切な措置を講じることが求められる。
  - 盗聴
  - 改ざん
  - なりすまし
  - マルウェアの混入等や中間者攻撃

  措置としては、ネットワークや機器、サービス等の監視、通信の相手先との相互認証などが想定される。

１３．４　無線 LAN の利用における対策

- システム運用担当者は、医療情報システムにおいて無線 LAN を利用する際に、不正利用や盗聴などのほか、可用性にも配慮した対策を講じることが求められる。
- 無線を用いたネットワークであることから、本来利用が許されない第三者の利用に利用される、侵入者による攻撃を受ける等のリスクがある。また適切な暗号化を講じないと、盗聴やマルウェアの混入などのリスクも生じる。さらに無線 LAN で使用される電波は、その特性や、医療機関等の構造により接続がしにくくなるケースが生じることから、可用性に留意した対応が求められる。

  無線 LAN 通信の暗号化に際しては、通信内容の漏えいリスクを低減するため、安全な方法による暗号鍵の管理が求められる。WPA2-PSK など事前入手方式は、利用者が同一の暗号鍵を共有することで、鍵が漏えいするリスクが高いため、利用を避けること。

[13] クラウドサービス事業者において、外部からの不正なアクセスを防止する観点から、併せて WAF（Web Application Firewall）を用いることも効果的であることから、このような対策を講じている事業者を選択することで、より安全性が向上すると考えられる。

１４．認証・認可に関する安全管理措置

【遵守事項】

① 医療情報システムへアクセスする際には、利用者の識別・認証を行うこと。また、利用者認証方法に関する手順等は、規則、マニュアル等で文書化すること。

② 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。

③ 利用者の識別・認証にセキュリティ・デバイス（例：IC カード）等を用いる場合、セキュリティ・デバイス等の破損等を想定し、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。

④ 規程に基づいてアクセス権限を付与する場合、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成すること。

⑤ 令和９年度（令和 9 年 4 月 1 日時点）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、今後、新規導入又は機器の入替等を伴うシステム更改をするに際しては、二要素認証を採用、又はこれに相当する対応を行うこと。なお技術的な理由等により令和９年度までの対応が困難な場合には、令和９年度以降、直近の次期の医療情報システムの更新までを期限とする。

- クライアント端末とサーバのいずれも二要素認証の実装を要する。
- クライアント端末では電子カルテ等のアプリケーションのログイン時に二要素認証を実装すること。
- サーバについては OS での二要素認証を実装すること。

⑥ パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。

(1) 類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。

(2) 異なる医療情報システムにおいて用いるパスワードの使い回しは行わないこと。

(3) 医療情報システム内のパスワードファイルは、パスワードのハッシュ値を保存するなどして平文パスワードを復元できない状態にした上で、適切な手法で管理・運用すること。

(4) 利用者のパスワードの失念や、パスワード漏えいのおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏えいのおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。

(5) システム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。

(6) 一定回数、認証に失敗した場合には、以降一定時間ログイン試行が不能となる仕組みを講じること。

⑧ 医療情報システムにおいて用いる ID について、台帳管理等を行うほか、定期的に棚卸しを行い、不要なものは適宜削除すること。また、これを実施するうえでの手順を作成すること。

⑨ 電子カルテシステムにおける識別情報の記録について、以下の機能があることを確認すること。または、記録の確定手順等を確立すること。

(1) 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

(a) 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含む。

(b) 「記録の確定」を行うに当たり、内容を十分に確認できる。

(c) 「記録の確定」を、確定を実施できる権限を持った利用者に限定する。

(d) 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策と、原

状回復のための手順を検討すること。

(e)　一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。

(f)　確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。

(2) 臨床検査システム、医用画像ファイリングシステム等の装置又はシステムにより記録が作成される場合

(a)　運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。

(b)　確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

(3) 一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができる。

(4) 同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できる。

(5) 代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。

(6) 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。

１４．１　利用者認証

１４．１．１　利用者の識別・認証

- アクセスを正当な利用者のみに限定するため、医療情報システムは利用者の識別・認証を行う機能を備えなければならない。システム運用担当者は、リスク分析の結果を踏まえ、企画管理者と協働して、適切な利用者認証のための措置を講じるほか、その運用の具体的な手順の作成を行うこと。
- これは、小規模な医療機関等で医療情報システムの利用者が限定される場合においても、同様である。
- 認証をするためには、医療情報システムへアクセスする全ての職員及び関係者に対し ID・パスワードや IC カード、電子証明書、生体認証等、本人の識別・認証に用いる手段を用意し、医療機関等の内部で統一的に管理する必要がある。また更新が発生する都度速やかに更新作業を行うこと。
- このような利用者の識別・認証に用いられる情報は、本人しか知り得ない、又は持ち得ない状態を保つ必要がある。利用者認証を ID とパスワードにより行う際には、システム運用担当者は、推定困難なパスワードが設定されるよう、安全性を考慮した機能仕様とすること。また、システム運用担当者も利用者のパスワードが把握不能となるような措置を講じることが求められる。
- 本ガイドラインでは令和３年度より二要素認証技術の実装を促してきた。令和９年度時点（令和９年４月１日時点）で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用すること。
- ここでいう、医療情報システムとは、医療情報を作成、更新、閲覧、削除等を行うアプリケーションまたはサービスのほか、医療情報を格納するサーバも含まれる。アプリケーションまたはサービスについては、これらを提供する事業者が技術的な対応を行っていないことで、二要素認証が実装不能なケースも想定される。令和 9 年度時点までに

システム更新を行う場合には、二要素認証対応をしているアプリケーションまたはサービスを選定することが求められる。令和 9 年度時点の対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。

- また、医療情報を格納するサーバの OS についても、原則として二要素認証の実装を目指すこと。サーバでは例えばアプリケーションを介さずにデータベースにアクセス可能であることから、OS のログイン時に二要素認証を実施することが合理的である。ただし、運用対応等の技術的な理由で対応が間に合わない場合には、令和９年度以降、直近のシステムの更改、新規導入までの間を経過措置とする。
-

表１４－１　医療情報システムにおける二要素認証の要否

	アプリケーション	ミドルウェア	OS
クライアント端末	要※	―	―
サーバ	―	―	要

※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。

- 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るが、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る。
- このため、サーバ OS については以下①②いずれか、またはそれと同等以上の措置が施されていれば[14]、二要素認証を実装できているものとみなす。

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る。これらが満たされない場合、十分な措置とは見なされない。

・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

- 認証により実現される対策の強度は、単に認証方法だけで判断されるものではない。二要素認証等の認証強化と併せて他の対策（ネットワーク接続管理や端末管理等）を講じることが必要である。二要素認証を採用してい

[14] 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。

ることを前提とした場合、パスワードの桁数は 8 桁（PIN であれば 4 桁）以上が求められる。この際、英数字の混在（大文字小文字は問わない）を求める。ただし、二要素認証を採用していない場合には 13 桁以上とすること。システムの仕様上、13 桁以上の設定ができない場合には、設定可能な最大桁数を設定し、直近のシステムの更改、新規導入時に必ず対応すること。

- いずれの場合においても、パスワードの定期的な変更は不要とする。
- PIN の定義としては、「特定のデバイスにおける電子証明書等の使用のための 4-8 桁の暗証番号」とする。
- また、VPN 装置においてもパスワードの使い回しや、単純なパスワードの利用によりサイバー攻撃被害が多発している。VPN 装置においても記憶認証のみに依存するのではなく、二要素認証等を導入することが望ましい。

１４．１．２　外部のアプリケーションとの連携における認証・認可

- クラウドサービスの普及から、医療機関でも外部のアプリケーションを連携して用いる場面が増えている。この時、アプリケーション間でデータが引き渡されることが想定される。昨今、システム間連携のインターフェイスとして、Web 技術のうち、REST API（Representational State Transfer Application Programming Interface）が活用されている。REST API は Web の技術を用いてサーバにアクセスして情報をやりとりする手順であるが、インターネット上で公開されることにより、IoT 機器やアプリケーションサーバ等も含め、広くシステム間での情報連携の促進が期待できる。一方で、このような API がサイバー攻撃の起点となる可能性を踏まえ、セキュリティ上の対応策が求められる。
- システム運用担当者は、API 連携のセキュリティ確保のため、外部からの攻撃や意図せぬアクセスを防止する措置を講じること。ネットワークセキュリティの確保や、API 連携により利用するユーザ・アプリケーションやデバイスの範囲の限定、責任分界とアクセスポリシーやログ管理を明確にした上での認証・認可の実装などが想定される。

１４．２　アクセス権限の管理

- 医療情報システムの利用に際しては、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（業務単位等）ごとに利用権限を規定する必要がある。また付与する権限は必要最小限とすることが重要である。医療情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定が可能なシステムを採用し、適切に活用すれば、さらにリスクを低減できる。
- アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜更新する必要がある。システム運用担当者は、組織の規程等と照合して、アクセス権限の設定を行う必要がある。
- 医療情報システムによっては、利用者がアプリケーション等を利用する際に、端末の OS の管理者権限を要するものがある。利用者に対する過度の権限付与を避けるため、このようなアプリケーション等の選定は避けること。
- クラウドサービスを利用する場合、利用するサービスによっては、医療機関等の規程に基づいて定めたシステム上の設定（ポリシー）が、デフォルトの設定となる等、自動的に意図しない内容に変更されてしまうことがある。これにより、アクセス権限等が変更され、医療情報が意図しない相手先に送信されるなどのリスクが想定される。
- このような状況を防ぐため、システム運用担当者は、意図せぬ設定の変更を検知できるよう措置を講じること。特に自動的に検知し、運用に反映できることが重要である。
- 利用するクラウドサービスの事業者から必要な情報を収集し、これらに対応できる措置を講じること。

１４．３　電子カルテデータの確定

- 法的に保存義務のある文書等を電子的に保存するためには、日常の診療や監査等において、電子化した文書

を利用可能であることの担保に加え、その内容の正確さについても訴訟等において証拠能力を有するレベルを担保することが要求される。誤った診療情報は、患者の生命に関わる可能性もあり、電子化した情報の正確さの確保には最大限の努力が必要である。また、診療に係る文書等の保存期間が各種の法令に規定されているため、所定の期間において安全に保管されなければならない。

- 法律上、保存義務のある文書等の電子保存の要件として、施行通知では真正性などを要件としている。真正性とは、正当な権限で作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることを指す。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。
- ネットワークを通じて外部に保存を行う場合、委託元の医療機関等から委託先の外部保存施設への転送途中で、診療録等に改ざんや混同が発生しないよう、措置を講じる必要がある。故意又は過失、使用する情報機器・ソフトウェアなどそれぞれの原因に対して、運用も考慮したうえで対応すること。
- 作成責任の所在を明確にすることも求められる。入力者及び確定者について、識別、認証を適切に行うとともに、記録の確定、識別情報の付与及び更新履歴の保存のための措置を講じること。なお、代行入力を行う場合には、入力者と確定者の責任関係が明確となるよう、識別及び認証の方法に留意すること。

１５．電子署名、タイムスタンプ

【遵守事項】

① 法令で定められた記名・押印のための電子署名について、企画管理編「１４．法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。

１５．１ 電子署名、タイムスタンプが求められる場面での対策

- システム運用担当者は、法令で定められた記名・押印のための電子署名については、企画管理編「14．法令で定められた記名・押印のための電子署名」で示す要件を満たしたものを選択し、措置を講じることが求められる。
- 法令で医師等の国家資格を有する者による作成が求められている文書の場合は、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第 2 条第 1 項を満たす電子署名であることに加えて、署名者の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いることなどが求められる。システム運用担当者は、必要に応じて、求められる要件を満たす電子署名を付すことができるよう、技術的対応を行うこと。
- 医療情報について、作成時刻又は変更時刻を証明する必要がある場合には、適切なタイムスタンプを付与し、保存義務のある期間中にその時刻及び真正性を検証できるよう、必要な技術的措置を講じること。
- システム運用担当者は、タイムスタンプの付与対象、付与のタイミング、検証手順及び保存期間中の検証可能性の維持方法を定め、必要な情報及び検証手段を保全すること。
- なお共通鍵、秘密鍵を格納する機器、媒体については、FIPS 140-3 レベル 1 [15]相当以上の対応を図ること。

[15] FIPS 140-3 では、製品に求めるセキュリティ要件として、Level 1 から Level 4 の 4 段階のレベルのものを定めている。このうち最も低い Level 1 では、「少なくとも 1 つの承認されたセキュリティ機能または機微なセキュリティパラメータ（SSP）を含み、かつ最低限の物理的セキュリティ要件を満たすこと」などが求められる。（"FIPS PUB 140-3: SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES" （NIST、2019.3.22））

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① 紙媒体等で作成した医療情報を電子化する際には保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャン等を行う前に対象書類に他の書類が重なって貼り付いている等、電子化可能な範囲外に情報が存在しないか確認すること。

② スキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、必要時に閲覧できるよう、紙媒体等の検索性にも留意して保管すること。

１６．１ 保存義務がある書面等に関する紙媒体等の電子化における技術的な対応

- システム運用担当者は、紙媒体等を電子化する際は、スキャン後も保存義務を満たす文書として必要な情報量を確保するための措置を講じることが求められる。
- なお、スキャナ等で電子化した場合、どのように精密な技術を用いても、元の紙等の媒体の記録と同等にはならない。また、スキャニングにより、保存できない有用な情報も存在し得るため、電子化は慎重に行う必要がある。電子化後に、元の紙媒体も保存することは真正性・保存性確保の観点から極めて有効であり、可能であれば外部への保存も含めて検討すること。

１６．２ 運用の利便性のためにスキャナ等で電子化を行う場合における技術的な対応

- スキャナ等による電子化後も、紙等の媒体の保存を継続する場合、電子化した情報はあくまでも参照情報であり、保存義務等の要件は課せられない。一方で、個人情報保護上の配慮は同等に行う必要がある。また業務等に差し支えない精度の確保も必要である。

１７．証跡のレビュー・システム監査

【遵守事項】

① 利用者のアクセスについて、アクセスログ等を記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。

② ログへのアクセス制限を行い、ログの不当な削除／改ざん／追加等を防止する対策を実施すること。

③ ログの記録に用いる時刻には、信頼できる情報を利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。

④ 監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。

１７．１ 証跡のレビュー

- システム運用担当者は、医療情報システムが適切に運用されていることを確認するため、システム上のログを収集し、レビューすることが求められる。特に個人情報を含む資源については、全てのアクセスログを収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。この確認は、全てのログを目視確認することを指すのではなく、システムでの監視や、実際の運用に基づく適切な閾値を用いたスクリーニング後のログを確認することを想定する。
- アクセスログは、それ自体に個人情報が含まれている可能性があること、情報セキュリティインシデントが発生した際の調査に非常に有用な情報であることから、その保護は必須である。システム運用担当者は、ログへのアクセス制限や不当な削除／改ざん／追加等を防止する対策を講じること。
- なお、例えば外部ネットワークとの接続点の集約に際しては、外部に接続されているサービス毎にログ管理等を分散させるのではなく、接続先制御・監査ログ集約・責任分界整理を一元管理することが負担軽減のために有効である。
- ログの正確性を保つため、記録する時刻の精度も重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取ること。
- アクセスログを分析し、緊急時にアラートを発する仕組みを講じることも求められる。
- 医療情報システムの管理を委託している場合には、事業者との間でログの管理方法や提供等に関して、明確に取り決めを行うこと。
- なお、医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理するなどの代替策を講じることが必要となる。

１７．２ 監査の実施の支援

- システム運用担当者は、企画管理者が監査実施計画を作成する際に、技術的な対応に該当する内容を作成し、企画管理者に報告することが求められる。また監査に必要な証跡（手順等の実施証跡や、システムログ及びレビューの結果等）を整理したうえで、企画管理者に報告すること。監査で指摘された事項については、企画管理者と協議し、改善に向けた対応を行うこと。
- 日々のセキュリティ対策の発展に対応するためには、システムセキュリティ監査（内部・外部）を継続的に実施す

ることが重要である。例えば、毎年テーマを決めて部分的に監査を実施することで、各回の負荷が軽減され、継続的に実施することが可能となる。医療機関全体での安全管理に関する認知度を向上させ、医療従事者全員に意識づけを行うことにも資する。

１８．外部からの攻撃に対する安全管理措置

【遵守事項】

① 医療情報システムに対するマルウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。

- 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
- 他の情報機器への混入拡大の防止や情報漏えいの抑止のための当該混入機器の隔離
- 他の情報機器への波及の調査等、被害の確認のための業務システムの停止
- バックアップからの重要なファイルの復元（数世代バックアップを複数の方式で確保すること）。

１８．１ サイバーセキュリティ対応

- システム運用担当者は、サイバーセキュリティ対応の必要が生じた際に、技術的な対応を行う。またサイバー攻撃等に備え、関係先への連絡手段や紙での運用等の代替手段を準備しておく必要がある。
- PC や VPN 機器等の脆弱性対策については、「８． ２ 情報機器等の脆弱性への対策」を参照するほか、NCO から示されている最新の「政府機関等のサイバーセキュリティ対策のための統一基準群」（令和７年７月１日サイバーセキュリティ戦略本部決定）[16]、令和３年４月30日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照すること。
- JPCERT/CC と IPA が提供する MyJVN を利用することで、登録した情報資産に関する Japan Vulnerability Notes のアラートが配信され脆弱性情報の検知が可能となる製品もある。資産管理台帳と組み合わせて有効活用するとよい。

  十分な情報収集やシステム担当者自身による VPN 機器等のアップデートが困難と想定される場合には、クラウド型 VPN の採用や、自動アップデートに対応した製品を選定、活用することが望ましい。
- 非常時に備えたバックアップの実施と管理については、「１１．システム運用管理（通常時・非常時等）」、「１２． ２ バックアップの管理」も参照すること。
- なお、医療情報システムは一般に複雑で、医療機関の規模等によって運用やバックアップの方法も様々である。一様に指針を示すことは困難であるが、医療機関においては、重大な障害により医療提供体制に支障が生じた場合であっても、診療の継続や早期復旧が求められる。全ての情報をバックアップから復元するのではなく、診療のために直ちに必要な情報をあらかじめ十分に検討し、確実に運用できるバックアップを確保しておくこと。
- 特に、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、バックアップデータまでランサムウェア等の被害が拡大することのないよう、バックアップデータの記録媒体を端末及びサーバ装置やネットワークから切り離して保管することが強く求められる。また、世代管理を行うことも重要である。日次でバックアップを行う場合、数世代（少なくとも３世代）を保持し、少なくとも３世代目以降の古い世代はネットワーク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必要となる。
- また、複数の方式でバックアップを確保することにより、単一の障害で全てのバックアップが利用不能となるリスクを低減できる。例えば下記から２つ以上を選択することが想定される。
- ・外部ストレージ/内蔵ストレージ（HDD：Hard Disk Drive、SSD：Solid State Drive 等）

[16] 統一基準群は https://www.cyber.go.jp/policy/group/general/kijun.html を参照。統一基準群を構成する文書は、適宜改訂されることがあるため、最新のものを参照すること。

- ・リムーバブルメディア（RDX：Removable Disk Exchange system、磁気テープ、DVD 等）
  ・NAS（Network Attached Storage）
  ・クラウドサービス
- サイバー攻撃による情報セキュリティインシデントが発生した際、数世代前までのバックアップデータは既にマルウェアの影響が及んでいる可能性があり、不用意にバックアップデータから復旧すると被害を繰り返すことになる。復旧するための手順をあらかじめ検討し、BCP として定めておくこと（電子カルテシステムが長期間にわたり停止した場合に、医師法（昭和 23 年法律第 201 号）第 24 条に定める診療録の作成への対応を整理する等）。また、BCP が機能することを訓練等により確認することも重要である。
- なお、復旧するにあたっては、侵入継続と被害拡大を防ぐ観点から、
  - バックドアを残さない
  - 無効にされたセキュリティ機能を復旧する
  - 利用された脆弱性に対処する
  - 他にリスクとなる既知の脆弱性がないか十分に検証、対応する
  - 不正に作成されたり、侵害された可能性のある機器に保存されていた ID・パスワード等を無効化する

  などの方策をとり、同様の被害を繰り返したり、盗まれた情報による被害を拡大させないよう対処すること。なお専門的な知見に関して、IPA が、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口[17]を開設している。

[17] サイバーセキュリティ 相談・届出窓口 （IPA）

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

概説編

目次

１．はじめに

- 本ガイドラインは、医療情報システムの安全管理や、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。以下「e-文書法」という。）等の法令等への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。平成 17 年 3 月に初版が策定され、以降、技術の進展及び制度改定などに対応する観点から、数度の改定を行ってきた。（これまでの改定経緯については Q&A 等を参照。）
- 第 7.0 版からは、本ガイドラインの根拠法に「サイバーセキュリティ対策基本法」（平成 26 年法律第 104 号）を追加し、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」[1]との整合性を確保した。また、すべてのサーバのセキュリティアップデートを事業者に委託している医療機関等の負担軽減を図るため、保守委託機関編を創設した。
- 医療情報システムを取り巻く環境は刻一刻と変動していくものであるため、今後も技術的な記載の陳腐化を避けるために随時内容を見直す予定である。本ガイドラインを利用する場合は、最新の版であることに十分留意することが求められる。
- なお、医療情報システムの安全管理は、患者の診療情報をはじめとする機微な個人情報を取り扱うことから、本ガイドライン関係者は、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（個人情報保護委員会、厚生労働省（平成 29 年 4 月 14 日））を十分理解すること。

[1] 国家サイバー統括室（NCO）2023 年 7 月 4 日公表

2．本ガイドラインの対象

- 本ガイドラインは、医療機関等において、全ての医療情報システムの導入、運用、利用、保守及び廃棄に関わる者を対象とする。

2．1　医療機関等の範囲

- 医療機関等とは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等を想定する。ただし、「保守委託機関編」の対象となる機関においては、「概説編」と「保守委託機関編」に対応することで、本ガイドラインを遵守しているものとみなす。

2．2　医療情報・文書の範囲

- 本ガイドラインで対象とする医療情報とは、医療に関する患者情報（個人識別情報）を含む情報を想定する。
- なお、医療機関等が作成した医療情報を、患者の指示に基づいて事業者に直接提供した場合、提供された情報は、「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。以下「２省ガイドライン」という。）の対象となる。また、当該事業者の提供するサービスによっては、「PHR サービス提供者による健診等情報の取扱いに関する基本的指針」（総務省・厚生労働省・経済産業省。以下「ＰＨＲ指針」という。）の対象ともなり得るので留意されたい。
- ただし、医療機関等が作成した医療情報を患者の管理に委ねた場合、患者の管理下にある当該情報は本ガイドラインの対象外となる。その後、当該情報について患者から提供を受けた事業者が取り扱う場合には、その情報は PHR 指針の対象となり得る。
- 本ガイドラインで対象とする文書は、医療情報を含む文書全般を想定し、法定の保存義務の有無を問わない。

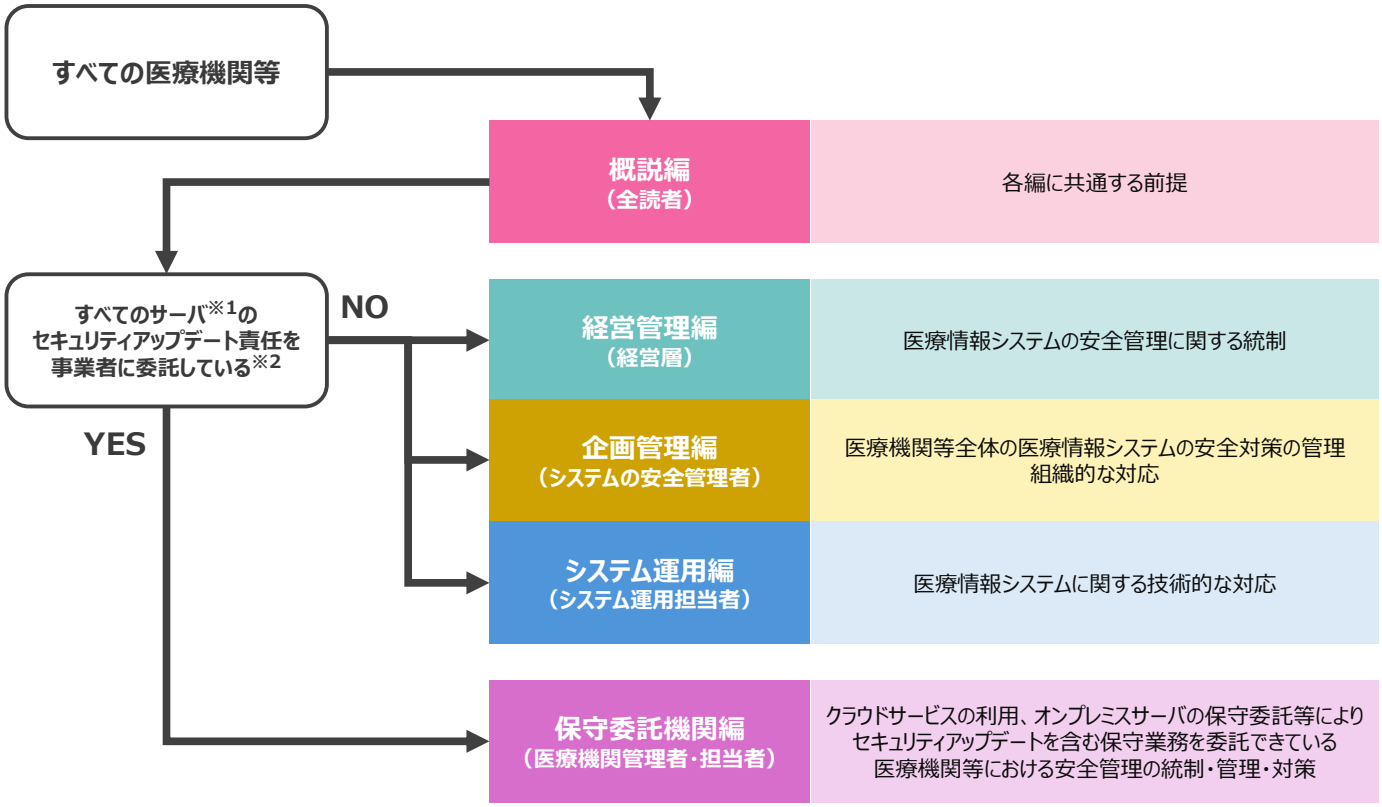
2．3　医療情報システムの範囲

- 本ガイドラインが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定する。これには、医療情報システム・サービス事業者（※）により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムも含まれる。
- なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。

（※）本ガイドラインで用いる「医療情報システム・サービス事業者」とは、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。

3．本ガイドラインの構成、読み方

本ガイドラインは、各編に共通する内容を整理した概説編と、医療情報システムの安全管理を実施するための統制・管理について各編で想定する読者類型ごとに整理した、経営管理編、企画管理編、システム運用編、保守委託機関編の５編から構成する（図３－１参照）。



※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３－１　ガイドライン第 7.0 版を構成する各編

- 各編の目的と概要は以下のとおりである。

３．１ 各編の目的・概要

３．１．１ 概説編

- 概説編は、本ガイドラインの目的や対象、全体構成に加え、経営管理編、企画管理編、システム運用編、保守委託機関編を理解する上で前提となる考え方等を示している。

３．１．２ 経営管理編

- 経営管理編は、主に医療機関等において組織の経営方針を策定し、意思決定を担う経営層を対象にしており、経営層として遵守・判断すべき事項、並びに企画管理やシステム運営の担当部署及び担当者に対して指示又は管理すべき事項及びその考え方を示している。

３．１．３ 企画管理編

- 企画管理編は、主に医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う担当者（企画管理者）を対象にしており、組織体制や情報セキュリティ対策に係る規程の整備等の統制等の安全管理の実務を担う担当者として遵守すべき事項、医療情報システムの実装・運用に関してシステム運用担当者に対する指示又は管理を行うに当たって遵守すべき事項及びその考え方を示している。

３．１．４ システム運用編

- システム運用編は、主に医療機関等において医療情報システムの実装・運用の実務を担う担当者を対象にしており、医療機関等の経営層又は企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の各種資源の設計、実装、運用等の実務を担う担当者として適切に対応すべき事項とその考え方を示している。
- なお、医療情報システムの実装・運用において、医療機関等が医療情報システム・サービス事業者に委託し、その業務及び責任を分担することも考えられる。そのため、委託事業者においても本編を参照の上、医療機関等と協働する必要がある。その際、業務や役割、責任の分担の在り方については、あらかじめ両者で取り決めておくことが必要になる。

３．１．５ 保守委託機関編

- 本ガイドラインが対象とする医療機関等のうち、「セキュリティアップデートを含むサーバの保守を事業者に全て委託できている医療機関等」においては、「概説編」と「保守委託機関編」のみを参照し、その遵守事項に対応することで本ガイドラインを遵守できているものとみなす。一般的な保守委託機関編の対象としては、専任のシステム担当者が配置されておらず、経営管理者や企画管理者が分離していないことが多い小規模医療機関等を想定している。このような医療機関等ではガイドラインの遵守項目全てを把握し、対応することが困難であると考えられ、事業者に技術的安全対策を委託する前提での安全管理措置を示したものである。
- サーバ保守の委託については、オンプレミス型のシステム採用を妨げるものではないが、クラウドサービス（特にSaaS 型システム）を積極的に採用することで特別な契約を交わすことなく保守の委託を実現することを想定している。

4．本ガイドラインの前提

4．1　医療情報システムの安全管理の目的

4．1．1　医療情報システムで取り扱う医療情報の重要性

- 医療情報システムで取り扱う医療情報は、病歴等、機微性の高い情報を含む患者の個人情報である。当該情報は、患者の生命、身体の安全に直接影響を及ぼす可能性もあるため、適切な取扱いが求められる。加えて、医療情報は、インフォームド・コンセントの観点からも、医療機関等と患者等との信頼関係に基づいて取り扱われるため、適切な管理が求められる。
- また、継続した医療の提供の観点から、医療機関等の間で絶え間なく患者の医療情報が共有されることも重要である。

4．1．2　医療情報システムの有用性

- 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る。医療情報を電子化して活用することにより、医療機関等内の複数の部門で同時かつ正確な医療情報を共有可能となり、医療提供の効率化に資する。
- さらには個々の医療機関等を越えて、外部の医療機関等や患者自身などと医療情報の共有や連携を図ることにより、より質の高い医療の提供や、個人の健康増進に寄与することが期待される。

4．1．3　医療情報システムの安全管理の必要性

- 医療情報の機微性や重要性を鑑みると、医療情報システムに対して求められる安全管理は、一般の情報システムに求められる安全管理よりも高い水準が求められる。

4．2　医療情報システムの安全管理に必要な要素

- 医療情報システムの安全管理において、情報セキュリティ対策は必須であり、医療機関等の特性を踏まえ、情報セキュリティの要素である「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」のバランスを取りながら、リスクに対応することが求められる。
- 「機密性（Confidentiality）」は、情報資産に対して、許可された者のみがアクセスできることを指す。機密性が確保されていない場合、許可していない者による情報システムの利用や改ざん、破壊などを含む、医療情報の不正な利用（参照、登録、改変）や漏えいが生じうる。
- 「完全性（Integrity）」は、情報資産が正確かつ完全な形で利用できることを指す。完全性が確保されない場合、表示されるべき情報が欠落したり、不完全又は不正確な形で表示されたりすることなどが生じうる。
- 「可用性（Availability）」は、情報資産に対して、許可された者が必要な時点でアクセスできることを指す。可用性が確保されない場合、情報システムが利用できなくなることや、利用目的に応じた適切な速度等での処理がなされないことで、医療情報の利用が妨げられうる。
- 医療情報システムにおける安全管理は、これら３要素への対応を想定するものであるが、医療機関等の業務内容や導入する医療情報システムなどを踏まえたリスク評価により、これら３要素への対応を随時検討し判断することになる。
- これら３要素への対応を踏まえて講じた安全管理措置を的確かつ継続的に実施・改善するために、体系的な仕

組みである情報セキュリティマネジメントシステム（ISMS：Information Security Management System）を構築・運用することが求められる。

４．３　医療情報システムの安全管理に関連する法令

- 医療情報システムに直接関連する法令としては、
  ・個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）
  ・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）、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（平成 17 年厚生労働省令第 44 号）及び「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等の施行等について」（平成 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年３月 31 日最終改正。）
  ・「診療録等の保存を行う場所について」（平成 14 年３月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知。平成 25 年３月 25 日最終改正。）
  ・サイバーセキュリティ基本法（平成 26 年法律第 104 号）
  が挙げられる。
- また、サイバー攻撃の脅威が近年増大していることに鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第２項は、「病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。」とし、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項第 1 号は、薬局の管理者が遵守すべき事項として「保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ、その他その薬局の業務につき、必要な注意をすること。」としている。本ガイドラインの直接の目的は個人情報保護法と e-文書法への対応であるが、加えて、本ガイドラインはサイバーセキュリティ基本法に基づく「重要インフラのサイバーセキュリティに係る安全基準等策定指針」を参照して作成されている。もっとも、サイバーセキュリティ基本法の対象は重要インフラ事業者であり、必ずしも本ガイドラインが対象としている医療機関と同一となるものではないことに留意されたい。
- なお、医療従事者等が作成する文書については、関係する法令により示されており（例えば医師法における診療録）、各法令が求める内容に従って作成しなければならない。その上で、電磁的記録による保存を行うことができる文書等に記録された情報を電子媒体に保存する場合には、当該情報の真正性・見読性・保存性が確保されている必要がある。
- また、医療情報を含む文書のうち、署名を求めるものに対して、電子署名を施す場合には、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）第 2 条に基づく電子署名を行うほか、本ガイドラインに基づき適切な措置を講じることが求められる。

４．４　医療情報システムに関する統制

- 医療情報システムの安全管理を行うためには、医療機関等において、医療情報システムの運営や利用に対する

統制が行われていることが求められる。

- 内部統制としては、
  - 組織としての安全管理等に関する基本的な方針や計画の策定
  - 安全管理等に必要な組織・体制の整備
  - 組織における安全管理のルールとなる規程類の整備
  - 上記に基づく運用

  等を実施することが求められる。
- 適切な統制を行うためには、体系的な運用を行うとともに、適宜、企画管理者が管理運営状況を把握して必要な情報を経営層に報告すること。また、経営層が組織全体の医療情報システムの安全性を継続的に管理することが求められる。
- また、医療情報システムの安全管理については、医療機関等向けには本ガイドライン、医療情報に関するシステム・サービスを提供する事業者向けには、総務省・経済産業省により 2 省ガイドラインが定められている。医療情報システムの運営や利用に際しては、様々な医療情報システム・サービス事業者と協働しながら安全管理措置を実施する場合がある。医療情報システムに求められる安全管理の水準に鑑み、本ガイドライン、2 省ガイドライン、その他の法令等に掲げる基準を満たした医療情報システム・サービス事業者を選定し、当該事業者との契約等において、双方の認識の齟齬が生じないよう、提供される情報システムやサービスの内容、当該事業者が行う業務内容、当該事業者との責任分界、役割分担、協働体制などを明確にした上で合意形成を図ること。
- 加えて、当該事業者に対して、必要に応じて、2 省ガイドラインの遵守状況を確認するなど、当該事業者の管理も求められる。

４．５ リスク評価とリスク管理

- 安全に医療情報システムを管理し、医療情報を取り扱うに当たっては、安全を脅かす原因となる「脅威」を認識する必要がある。この脅威としては、地震等の自然災害や、サイバー攻撃、システム障害などの技術的脅威によるもの、医療情報の漏えいや改ざんなどの人的要因によるものが挙げられる。
- また、これらの脅威によって生じる被害が発生する可能性を「リスク」と呼ぶ。
- 各医療機関等においては、自組織にとっての脅威を特定し、そのリスクを評価した上で対策を講じることが重要である。特に、自然災害やサイバー攻撃、システム障害などについては、被害の影響がより大規模となる可能性が高いため、高度なリスク評価を踏まえた対策を要する。
- なお、医療情報システムの安全管理上のリスク評価、リスク管理を実施するに当たっては、医療情報システム・サービス事業者から技術的対策等の情報を収集することが重要である。例えば、厚生労働省標準規格となっている「『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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリスト[2]や 2 省ガイドラインにおける「サービス仕様適合開示書」等の提供を受け、当該事業者とリスク管理に関する合意形成（リスクコミュニケーション）を図ることが求められる。
- また、合意した内容を契約書や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）等の形で双方の合意文書として明らかにした上で、具体的な責任分界を踏まえた運用を行うこと。

---

[2] 厚生労働省標準規格 HS040。なおこれに対応し、一般社団法人日本画像医療システム工業会（JIRA）の工業会規格（JESRA：Japanese Engineering Standards of Radiological Apparatus）及び一般社団法人保健医療福祉情報システム工業会（JAHIS）の JAHIS 標準として MDS/SDS のチェックリストが提供されている。最新のものを参照すること。

４．６　医療情報システムにおける認証・認可

- 医療情報システムでは、医療機関等が利用権限を認めた利用者に対して、設定した利用範囲内で適切に利用することを保証するために、利用者の認証・認可を行うことになる。
- 情報システムの認証に際しては、利用者を特定するための識別子（ID など）と、利用者が本人であることを確認するための符号（パスワードや指紋認証データなど）が必要である。
- 医療情報によっては、医師等の法令で定められた者以外の作成等が認められていないものがある。加えて、医療情報は、患者の生命や心身の安全に影響を及ぼす可能性があることから、通常の情報システムよりも高くリスクを算定する必要がある。このため、医療情報システムにおいて用いる認証方式は、特に安全なものを採用すべきであり、例えば ID の発行については、対面など確実に身元確認が取れる方法を採用する、認証方法については、多要素認証を採用するなどの方法が挙げられる。

４．７　医療情報の外部保存

- 医療情報の外部保存[3]については、「４．３　医療情報システムの安全管理に関連する法令」で示した「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等の施行等について」や「診療録等の保存を行う場所について」に掲げる基準を満たすことを前提に、外部の事業者に医療情報の保存を委託し、医療機関の外部に医療情報を保存することが可能となっている。これを踏まえ、本ガイドラインでは、適切な外部保存委託先としての医療情報システム・サービス事業者の選定に関する対策項目を示している。
- 外部保存に際しては、外部と接続するネットワークを利用するという観点から、情報漏えいや不正アクセス等のリスクが生じる。一方、適切な医療情報システム・サービス事業者に委託することで、専門的な知識に基づいて、必要な情報セキュリティ対策が講じられた環境での医療情報やデータの管理が可能となる。そのため、医療機関等においては、事業者に一部の業務を委託する方が、結果としてより安全な情報セキュリティ対策を講じることが可能となり得る。加えて、情報システム等の運用に係る要員などの負担軽減にもつながる。
- このように、クラウドサービスの利用等、適切な外部保存を実施することで、セキュリティを向上させることは適切な安全管理策のひとつである。特に小規模医療機関等を含む医療情報システムの専任の運用担当者がいない施設においては、適切なクラウドサービスの利用によって安全管理を事業者に委託することが望ましい。

[3] 診療録等を医療機関等以外の場所へ外部保存する場合をいう。

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

企画管理編

目次

53 -

【はじめに】

＜企画管理編が想定する読者＞

企画管理編は、主に医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う担当者（企画管理者）を対象にしている。

本編では、組織体制や情報セキュリティ対策に係る規程の整備等の統制等の安全管理の実務に当たり具体的に遵守が必要な事項、医療情報システムの実装・運用に関する適切な対応をシステム運用担当者に指示、管理するために必要な事項を示す。

１．管理体系

【遵守事項】

① 医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。

② 委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。

③ 医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認を取ること。また、遵守状況に応じて必要な改善措置を講じること。

④ 医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。

⑤ 組織における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及び医療情報システムの安全管理に関する方針を策定し、経営層の承認を得ること。

⑥ ⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。

⑦ 患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。

１．１　安全管理に関連する法制度等

１．１．１　医療機関等における医療情報の取扱いに関する法令の遵守

➢ 医療情報の取扱いに関しては、さまざまな法令が関係する。例えば、医療情報は患者の個人情報であることから、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という）を遵守する必要がある。さらに、医療情報は基本、医療従事者や医療機関等が作成することから、医師法等の各種医療関係の法令の規定を遵守する必要があり、医療従事者や医療機関等には法律上の責任が生じる。（表１－１）

表１－１　医療情報の取扱いに関する法律上の責任

責任分野	関連法	情報に対する責任の内容の例
行政法上の責任	個人情報保護法	個人情報取扱事業者責任
	各種医療関係法※	医療従事者・医療機関等における業法責任
刑事上の責任	刑法等	秘密漏示罪など
民事上の責任	民法（契約）	診療契約（準委任）及びこれに関する安全配慮義務

※　医師法、歯科医師法、薬剤師法、医療法等を想定

- このように、医療機関等における医療情報システムの安全管理に関する責任は、業法責任（行政法上の責任）が中心となる。それと同時に、医療機関等で業務に従事する職員や関係する医療情報システム・サービス事業者（以下「システム関連事業者」という。）等による秘密漏えいや医療情報の漏えい等による損害賠償を防ぐ責任もある。
- 企画管理者は、このような医療機関等が負う責任の根拠となる各種法令等（ガイドライン等を含む。）が、医療機関等の組織全体として遵守されるよう管理すること。
- そのため、企画管理者には、医療情報の取扱いに関する法令等の内容を理解した上で、医療機関等や医療機関等で業務に従事する職員や関係するシステム関連事業者等が遵守すべき内容を整理し、必要な措置を行うことが求められる。
- また、医療機関等内における法令遵守状況の管理は、当該医療機関の経営層の責務でもあることから、企画管理者はその遵守状況について、経営層に適宜報告し、必要に応じて改善策を講じること。

１．１．２　医療情報システムに関係する法令

- 医療機関等が遵守すべき法令の中には、特に医療情報システムで取り扱うデータ等に関係するものが含まれている。例えば、個人情報保護法では、利用目的や第三者提供に関する適切な同意取得のない利用等の禁止等の個人情報の保護に関する必要な対応のほか、安全管理措置義務や委託先の監督等の個人データの保護に関する必要な対応を求めている。
- また、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。以下「e-文書法」という。）により電子化して保存することが認められる文書については、e-文書法及びその関係法令に従うことが求められる。
- なお、関係する法令に従って医療従事者が作成する文書（例えば医師法における診療録）の電子媒体による保存については、「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等の施行等について」（平成 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年３月 31 日最終改正。以下「施行通知」という。）第二の２（３）に掲げる３条件を満たす必要がある。

（参考：施行通知第二の２（３））

① 見読性の確保

必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。

（ア）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。

（イ）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。

② 真正性の確保

電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。

（ア）故意又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。

（イ）作成の責任の所在を明確にすること。

③ 保存性の確保

電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。

- また、診療録等を病院又は診療所等以外の場所に外部保存する場合は、「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知。平成 25 年 3 月 25 日最終改正。以下「外部保存通知」という。）に従うことが求められる。
- さらに、医療従事者等が作成する医療情報を含むデータに対して電子署名を施す必要がある場合には、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号。以下「電子署名法」という。）等に従うこと。
- サイバー攻撃の脅威が近年増大していることに鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項は、「病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（略）を確保するために必要な措置を講じなければならない。」とし、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項第 1 号は、薬局の管理者が遵守すべき事項として「保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係るサイバーセキュリティ（略）の確保のために必要な措置を講じ、その他その薬局の業務につき、必要な注意をすること。」としている。
- 本ガイドラインでは、これらの法令で規定している内容を前提として、遵守が必要な事項を示している。
- 企画管理者は、これらの法令等の内容を把握、整理した上で、必要な措置を講じることが求められる。具体的な方法については、医療情報システムに関する運用やシステム仕様の検討等に関わるシステム運用担当者に検討を求める必要がある。その上で、担当者の検討結果を踏まえて、講ずる措置の中に盛り込むことが求められる。

表１－２　医療情報システムに関係する法令

法令名	概要
個人情報保護法	個人情報及び個人データ（検索性のある個人情報）の管理に関する内容（安全管理措置義務、漏えい等の報告義務、第三者提供の制限等）を規定。
e 文書法省令[1] 施行通知	e-文書法を踏まえ、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の要件等を規定。（対象となる書面（文書）は、表１－３のとおり。）
外部保存通知	診療録等の外部保存を行う際の基準や電子媒体により外部保存を行う際の留意事項等を規定。（対象となる記録等は表１－４のとおり。）
電子署名法	電磁的記録として作成される情報に行われる電子署名に関する要件等を規定。 医療情報を含む情報に関しては、電子署名を行うものについて電子署名法に基づく電子署名の要件に加え、署名者の資格確認に係る要件もあわせて満たす必要がある。

[1] 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（平成 17 年 3 月 25 日厚生労働省令第 44 号）

表１－３　電磁的記録の保存、作成及び交付等を行うことができる文書

１. 医師法（昭和 23 年法律第 201 号）第 24 条の診療録
２. 歯科医師法（昭和 23 年法律第 202 号）第 23 条の診療録
３. 保健師助産師看護師法（昭和 23 年法律第 203 号）第 42 条の助産録
４. 医療法（昭和 23 年法律第 205 号）第 51 条の財産目録及び貸借対照表並びに損益計算書
５. 歯科技工士法（昭和 30 年法律第 168 号）第 19 条の指示書
６. 薬剤師法（昭和 35 年法律第 146 号）第 28 条の調剤録
７. 外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条の診療録
８. 救急救命士法（平成 3 年法律第 36 号）第 46 条の救急救命処置録
９. 医療法施行規則（昭和 23 年厚生省令第 50 号）第 30 条の 23 第 1 項及び第 2 項の帳簿
10. 保険医療機関及び保険医療養担当規則（昭和 32 年厚生省令第 15 号）第 9 条の診療録等（作成については、同規則第 22 条）
11. 保険薬局及び保険薬剤師療養担当規則（昭和 32 年厚生省令第 16 号）第 6 条の調剤録（作成については、同規則第 5 条）
12. 臨床検査技師等に関する法律施行規則（昭和 33 年厚生省令第 24 号）第 12 条の 3 の書類（作成については、同規則第 12 条第 14 号及び第 15 号）
13. 医療法第 21 条第 1 項の記録（同項第 9 号に規定する診療に関する諸記録のうち医療法施行規則第 20 条第 10 号に規定する処方せんに限る。）、第 22 条の記録（同条第 2 号に規定する診療に関する諸記録のうち医療法施行規則第 21 条の 5 第 2 号に規定する処方せんに限る。）、同法第 22 条の 2 の記録（同条第 3 号に規定する診療に関する諸記録のうち医療法施行規則第 22 条の 3 第 2 号に規定する処方せんに限る。）及び同法第 22 条の 3 の記録（同条第 3 号に規定する診療及び臨床研究に関する諸記録のうち医療法施行規則第 22 条の 7 第 2 号に規定する処方せんに限る。）※
14. 薬剤師法第 26 条及び第 27 条の処方せん※
15. 保険薬局及び保険薬剤師療養担当規則第 6 条の処方せん※
16. 医療法第 21 条第 1 項の記録（医療法施行規則第 20 条第 10 号に規定する処方せんを除く。）、同法第 22 条の記録（医療法施行規則第 21 条の 5 第 2 号に規定する処方せんを除く。）、同法第 22 条の 2 の記録（医療法施行規則第 22 条の 3 第 2 号に規定する処方せんを除く。）及び同法第 22 条の 3 の記録（医療法施行規則第 22 条の 7 第 2 号に規定する処方せんを除く。）
17. 麻薬及び向精神薬取締法（昭和 28 年法律第 14 号）第 27 条第 6 項の処方せん※
18. 歯科衛生士法施行規則（平成元年厚生省令第 46 号）第 18 条の歯科衛生士の業務記録
19. 医師法第 22 条の処方せん※
20. 歯科医師法第 21 条の処方せん※
21. 健康保険法施行規則（大正 15 年内務省令第 36 号）第 54 条の処方せん※
22. 船員保険法施行規則（昭和 15 年厚生省令第 5 号）第 45 条第 1 項の処方せん※
23. 保険医療機関及び保険医療養担当規則第 23 条第 1 項の処方せん※
24. 国民健康保険法施行規則（昭和 33 年厚生省令第 53 号）第 25 条の処方せん※
25. 高齢者の医療の確保に関する法律施行規則（平成 19 年厚生労働省令第 129 号）第 30 条

の処方せん※

26. 診療放射線技師法（昭和 26 年法律第 226 号）第 28 条第 1 項の規定による照射録

※ 処方せんについては、施行通知第二の２（４）の要件を充足する必要がある。

また、介護事業者が取り扱う文書等のうち、下記文書等は、e-文書法の対象範囲であり、かつ当該文書の内容には医療情報が含まれることがある。

1．指定居宅サービス等の事業の人員、設備及び運営に関する基準（平成 11 年厚生省令第 37 号）第 73 条の 2 第 2 項の規定による訪問看護計画書及び訪問看護報告書

2．指定居宅サービス等の事業の人員、設備及び運営に関する基準第 154 条の 2 第 2 項（第 155 条の 12 において準用する場合を含む。）の規定による短期入所療養介護計画

3．指定居宅サービス等の事業の人員、設備及び運営に関する基準第 191 条の 2 第 2 項及び第 192 条の 11 第 2 項の規定による特定施設サービス計画

4．指定介護老人福祉施設の人員、設備及び運営に関する基準（平成 11 年厚生省令第 39 号）第 37 条第 2 項の規定による施設サービス計画

5．介護老人保健施設の人員、施設及び設備並びに運営に関する基準（平成 11 年厚生省令第 40 号）第 38 条第 2 項の規定による施設サービス計画

6．健康保険法等の一部を改正する法律の一部の施行に伴う厚生労働省関係省令の整備に関する省令（平成 24 年厚生労働省令第 10 号）による廃止前の指定介護療養型医療施設の人員、設備及び運営に関する基準（平成 11 年厚生省令第 41 号）第 36 条第 2 項の規定による施設サービス計画

7．指定訪問看護の事業の人員及び運営に関する基準（平成 12 年厚生省令第 80 号）第 30 条第 2 項の規定による訪問看護記録書、訪問看護指示書、特別訪問看護指示書、精神科訪問看護指示書、精神科特別訪問看護指示書、在宅患者訪問点滴注射指示書、訪問看護計画書及び訪問看護報告書

8．指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準（平成 18 年厚生労働省令第 35 号）第 73 条第 2 項の規定による介護予防訪問看護計画書及び介護予防訪問看護報告書

9．指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準第 194 条第 2 項（第 210 条において準用する場合を含む。）の規定による介護予防短期入所療養介護計画

10. 指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準第 244 条第 2 項及び第 261 条第 2 項の規定による介護予防特定施設サービス計画

11. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 3 条の 40 第 2 項の規定による定期巡回・随時対応型訪問介護看護計画及び訪問看護報告書

12. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 40 条の 15 第 2 項の規定による療養通所介護計画

13. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 128 条第 2 項の規定による地域密着型特定施設サービス計画

14. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 156 条第 2 項（第 169 条において準用する場合を含む。）の規定による地域密着型施設サービス計画
15. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準第 181 条第 2 項の規定による居宅サービス計画、看護小規模多機能型居宅介護計画及び看護小規模多機能型居宅介護報告書
16. 介護医療院の人員、施設及び設備並びに運営に関する基準（平成 30 年厚生労働省令第 5 号）第 42 条第 2 項（第 54 条において準用する場合を含む。）の規定による施設サービス計画

なお、法令等によって作成や保存が定められている文書等のうち、e-文書法の対象範囲でない医療関係文書等については、たとえ電子化したとしても、その電子化した文書等を法令等による作成や保存が定められた文書等として取り扱うことはできないため、別途紙媒体による作成・保存が必要となる。

表１－４　外部保存を認める記録等

1. 医師法第 24 条に規定されている診療録
2. 歯科医師法第 23 条に規定されている診療録
3. 保健師助産師看護師法第 42 条に規定されている助産録
4. 医療法第 46 条第２項に規定されている財産目録、同法第 51 条の２第１項に規定されている事業報告書等、監事の監査報告書及び定款又は寄附行為、同条第２項に規定されている書類及び公認会計士等の監査報告書並びに同法第 54 条の７において読み替えて準用する会社法（平成 17 年法律第 86 号）第 684 条第１項に規定されている社会医療法人債原簿及び同法第 731 条第２項に規定されている議事録
5. 医療法第 21 条、第 22 条及び第 22 条の２に規定されている診療に関する諸記録及び同法第 22 条及び第 22 条の２に規定されている病院の管理及び運営に関する諸記録
6. 診療放射線技師法第 28 条に規定されている照射録
7. 歯科技工士法第 19 条に規定されている指示書
8. 薬剤師法第 27 条に規定されている調剤済みの処方せん
9. 薬剤師法第 28 条に規定されている調剤録
10. 外国医師等が行う臨床修練に係る医師法第 17 条等の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条に規定されている診療録
11. 救急救命士法第 46 条に規定されている救急救命処置録
12. 医療法施行規則第 30 条の 23 第１項及び第２項に規定されている帳簿
13. 保険医療機関及び保険医療養担当規則第９条に規定されている診療録等
14. 保険薬局及び保険薬剤師療養担当規則第６条に規定されている調剤済みの処方せん及び調剤録
15. 臨床検査技師等に関する法律施行規則第 12 条の３に規定されている書類
16. 歯科衛生士法施行規則第 18 条に規定されている歯科衛生士の業務記録
17. 高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準（昭和 58 年厚生省告示第 14 号）第９条に規定されている診療録等
18. 高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準第 28 条に規定されている調剤済みの処方せん及び調剤録

１．２　医療情報システムの安全管理に関する方針の策定

１．２．１　情報セキュリティ方針等の策定

- 医療機関等の組織全体として医療情報システムの安全管理に対する共通の認識を有し、適切な安全管理を行うためには、一組織としての方針を定める必要がある。
- この方針は、医療情報システムに対する情報セキュリティ方針（ポリシー）[2]、患者の医療情報の保護に関する方針及び医療情報システムの安全管理に関する方針に分けられる。企画管理者は、このような情報セキュリティ方針等の方針を策定した上で、経営層の承認を受けて、組織の方針として定めることが求められる。なお、医療機関等が所属する法人等において情報セキュリティ方針等が別に定められている場合には、当該医療機関等に特有の事項等について検討し、必要に応じて補則等を整備すること。

１．２．２　個人情報保護に関する方針の策定

- 医療機関等における個人情報保護に関する方針としては、いわゆるプライバシーポリシー等があるが、これは、医療機関等が行う個人情報の保護に関する措置の透明性の確保と対外的な明確化を目的としており、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（個人情報保護委員会、厚生労働省（平成 29 年４月 14 日））（以下「ガイダンス」という）においても求められているものである。企画管理者は、医療情報システムに関する情報セキュリティ方針等と併せて、個人情報保護に関する方針についても策定の上、経営層による承認を得て、組織の方針とすることが求められる。

[2] 情報セキュリティ方針（ポリシー）には、セキュリティ対策の目的や方向性や、関係主体等からの要求事項への対応を含むことが求められる。

2．責任分界

【遵守事項】

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。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。

② 取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。

③ 責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。

④ 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。

⑤ 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。

⑥ 第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。

2．1 運用管理における責任分界

2．1．1 医療機関等における責任と責任分界

- 医療機関等の医療情報システムの安全管理に関する責任として、通常時における責任と非常時における責任がある。
- 医療機関等がシステム関連事業者に委託を行い、医療情報システムの実装や運用を図る場合には、この委託契約に基づいて、医療機関等とシステム関連事業者との間で、医療情報システムの実装や運用に関する責任の分担（責任分界）を決める必要がある。従って責任分界の設定においては、通常時における責任を果たすための責任分界と、非常時における責任を果たすための責任分界の二つが想定される。
- また、このような責任分界の設定に際しては、医療機関等とシステム事業者等において、それぞれ医療情報システムに根差すリスクに関する共通の理解を得た上で、それぞれがどのリスクに対してどのような対応を行うかを決めることにより、具体的な責任分界の内容を決めることができる。このようなリスクに関する合意を図るためのリスクコミュニケーションを行うことも、委託においては重要である。
- 運用管理においては、医療機関等とシステム関連事業者との間で決定された責任分界を、契約書や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）などの形で双方の拘束力ある合意文書として明らかにした上で、具体的に責任分界を踏まえた運用を行うことが求められる。

２．１．２ 通常時における責任

- 医療機関等が負う通常時における責任としては、
  ・説明責任
  ・管理責任
  ・定期的な見直し、必要に応じて改善を行う責任
  がある。

（１）説明責任

- 説明責任とは、医療情報システムの運用状況等が適切に行われていること等を患者等に説明する責任である。医療情報システム・サービスの運用等についてシステム関連事業者に委託している場合には、委託している範囲の医療情報システム・サービスの運用状況等について、医療機関等において直接把握することが難しい。そこで医療機関等は、委託先事業者に対して、提供を受ける医療情報システム・サービスが本ガイドラインを遵守した仕様や運用となっていることの説明を求めることができるよう、委託先事業者と取決めを行う必要がある。
- 例えば、医療情報システム・サービスの採用に際しては、システム関連事業者からサービス仕様適合開示書等の提供などを受けることになるが、当該文書の中に本ガイドラインを遵守している旨（あるいは遵守できていない部分がある場合はその旨）を記載することのみならず、委託決定後も必要に応じて当該遵守状況を示す資料の提供を求めることができる旨の取決めを行うことが求められる。（なお、このような説明責任に関する分担の取決めがない場合には、医療機関等は自ら委託している医療情報システム・サービスの運用状況に関する説明のための資料を用意することが必要となる。）

（２）管理責任

- 医療機関等における管理責任とは、医療情報システムの運用管理を医療機関等が適切に行う責任である。これも医療情報システム・サービスを委託している場合には、委託している範囲の医療情報システム・サービスの運用状況等について医療機関等において直接把握することが難しいため、委託先事業者に適切な運用管理の実施を委ねるとともに、医療機関等は適宜委託先事業者において適切な運用がなされていることを管理することで、責任の分担を図る必要がある。
- 特に委託先事業者が再委託を行う場合、再委託先事業者において生じた漏えい等の情報セキュリティインシデントの責任も、委託元の医療機関等の責任となりうることから、再委託先事業者の管理だけではなく選定などについても、委託先事業者と適切に分担することが求められる。また、医療機関等が購入した機器等については、別途、事業者と当該機器についての保守契約を締結しない場合には、原則、管理責任は医療機関等にあり、事業者との間での管理責任の分担は生じない。
- 以上の内容を踏まえながら、企画管理者は、管理責任を全うするため、委託先事業者に対して、委託先事業者の運用状況の報告資料の提供や、委託先事業者による再委託が行われる場合には再委託先事業者も含めた責任分界についての取決めを行うことが求められる。

（３）定期的な見直し、必要な改善を行う責任

- 医療機関等において定期的な見直しを実施し、必要な改善を行う責任は、基本的には医療機関等が自ら負うものである。ただし、医療情報システム・サービスを委託している場合には、委託先事業者から、適宜、情報提供や提案等を求め、医療機関等における見直しの参考とすることなどが想定される。
- また、サイバーセキュリティ対策の観点から、委託先事業者に対して、委託している医療情報システム・サービスに関して、自発的な見直し対応を求めることも想定される。企画管理者は、委託先事業者に対して、委託しているサービスの特徴に応じて、必要であれば自発的な対策の見直しを求める項目などを、SLA 等に含めるなどの対応を行うことが求められる。

２．１．３　非常時における責任

- 医療機関が負う非常時における責任としては、
  ・情報セキュリティインシデントの原因・対策等に関する説明責任
  ・善後策を講ずる責任
  が挙げられる。

（１）情報セキュリティインシデントの原因・対策等に関する説明責任

- 医療情報に関して、例えばサイバー攻撃などで、医療情報が破壊されたり、漏えいしたりした場合には、対策を講じるために、原因を特定し、その上で対策の検討、それらに関する対外的説明などを行う必要がある。
- 対外的な説明に関しても、専門的な見地からの対応が求められることもあるため、医療機関等とシステム関連事業者との間での分担等の取決めを行うことが求められる。
  - 企画管理者は、対外的説明の範囲や内容などをあらかじめシステム関連事業者と取り決めておく必要がある。

（２）善後策を講ずる責任

- 医療機関等が果たすべき善後策を講ずる責任の中には、「情報セキュリティインシデントの原因を究明する責任」、「再発防止策を講ずる責任」がある。
- 医療情報システム・サービスを委託している場合には、情報セキュリティインシデントの原因が直ちに判明しない場合が想定されることから、医療機関等と委託先事業者とで協力して対応する必要があり、これらの責任分界についても医療機関等と委託先事業者とであらかじめ取り決めておく必要がある。具体的には、情報セキュリティインシデント発生後から収束に至るまでの期間の対応における分担や協力の内容に関して、あらかじめ委託先事業者と取り決めておくことで、的確かつ迅速な原因究明が可能となるとともに、究明された原因に応じた再発防止策を講じる際の分担や協力についても取り決めておくことで、情報セキュリティインシデントの発生後、システム関連事業者への医療情報システム・サービスの委託を継続する場合に、再発防止策を含むインシデントを踏まえた委託内容の更新を的確かつ迅速に行うことが可能となる。
- 以上のとおり、企画管理者はこれらの責任を適切に果たすことができるよう、システム関連事業者との間での役割分担を含む責任分界を定める必要がある。

２．１．４　リスク分析を踏まえた要求仕様適合性の確認への対応

- 医療機関等とシステム関連事業者との間で、役割分担、当該事業者が受容したリスクの内容等について合意形成を図るため、医療情報システムについて、医療機関等におけるリスクアセスメントを踏まえた医療機関等の要求仕様への適合性を確認する必要がある。

- 医療機関等によるリスクアセスメントの結果、一部のリスクを委託先事業者で負うことになることが想定される。その際に、委託先事業者が想定していたリスクの内容とリスクアセスメントを踏まえたリスクの内容に不一致があると、リスク管理が不十分となり得る。そこで、医療機関等が責任分界を定めるに際しては、その前提としてそれぞれが負うことが想定されるリスクの内容について、合意を得るための調整を行うことになる。
- 実際には、システム関連事業者が提供する情報やサービス仕様適合開示書等の内容を踏まえて、遵守している対策項目等の状況が医療機関等で求める内容と乖離があるかどうかを把握すること。乖離がある場合には対応を両者で協議し、合意した上で、医療情報システム・サービスの提供を受けることが想定される。
- 企画管理者は、このような要求仕様適合性の調整・確認に必要な情報をシステム関連事業者から収集し、必要な調整を行った上で、責任分界に関する取決めを行うことが求められる。

2．1．5　医療情報システム等提供事業者との取決めにおける留意点

- 医療情報システム等提供事業者との間で取決めを行う場合、事業者が提供するシステム・サービスの内容や、その契約形態などに応じて、具体的なコミュニケーションについて留意する必要がある。例えば、個々に契約内容等の調整を行うことを想定した医療情報システム等の提供と、パブリッククラウドサービスのように約款契約による画一的な契約内容による場合では、コミュニケーションの進め方は異なる。特に約款契約による場合には、個々の契約内容の調整が難しいことから、医療機関等は対象事業者に対して、より丁寧にサービス内容やリスクについて、わかりやすい情報提供を求めること。具体的には、以下のような対応を事業者に求めることが挙げられる。
  - リスク判断に必要な基礎資料の提供（MDS/SDS[3]等の提供、主なセキュリティ事項に関するチェック結果の提供等）
  - 医療機関等側が説明を求めた場合の対応の表示
  - 約款契約におけるリスクの表示（民法第 548 条の 2 関係）
  - 医療機関等が、リスクや役割分担等を確認した上でサービス利用する旨を明示することを求め、合意すること

2．2　責任分界の決め方

2．2．1　委託と第三者提供における責任分界

- 医療機関等が責任分界を取り決める場面として大きく 2 つの場面が想定される。
- 一つが医療情報システムに関連して、委託を行う場合に委託先事業者との間で取り決める責任分界である。
- もう一つは、医療機関等が保有する医療情報を、第三者に提供する際に、提供元の医療機関等と提供先の第三者との間で取り決める責任分界である。

2．2．2　委託における責任分界（複数事業者が関与する場合を含む）

- 医療機関等の医療情報システム・サービスが一事業者のみから提供されたもので構成されている場合には、2.1 に示す内容で責任分界を決定することになる。
- しかし実際には、医療機関等が利用する医療情報システム・サービスは複数の事業者が提供するサービスから構成されており、医療機関等と各事業者との関係を考慮した上で、責任分界を取り決めることになる。

---

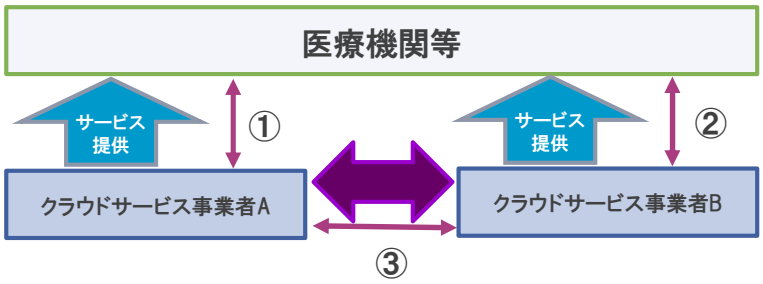
[3] MDS/SDS：Manufacturer/Service Provider Disclosure Statement for Medical Information Security。厚生労働省標準規格 「HS040「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド」参照なお具体的には「「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要」を参照。

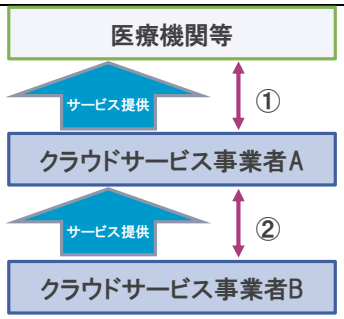
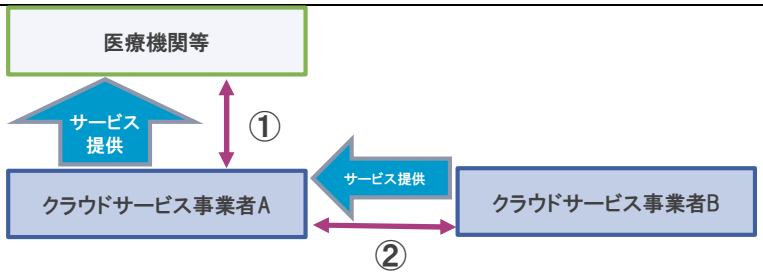
- システム関連事業者が提供するサービスの類型により、医療機関等が直接管理する医療情報システムに関する情報機器やソフトウェアなどの範囲が異なるため、サービス類型に応じた責任分界を取り決めること。

（１）複数のシステム関連事業者に対する委託を含む場合の責任分界

- 医療情報システム・サービスを委託する場合、複数のシステム関連事業者が関わる場合があり、具体的には医療機関等が複数のシステム関連事業者の提供するサービスを組み合わせて利用する場合と、一システム関連事業者が複数のサービスを組み合わせて提供するサービスを利用する場合などが想定される。
- 前者の場合は、基本的には医療機関等が各事業者と責任分界を取り決めることになるが、複数のシステム関連事業者のサービスの連携部分についても併せて取決めを行うことが求められる。これには、技術的な仕様等に関する取決めだけではなく、非常時におけるシステム関連事業者間での対応なども含めて取り決めることが求められる。
- 後者の場合には、基本的には医療機関等は最終的に医療情報システム・サービス等を取りまとめて提供するシステム関連事業者との間で責任分界を定めることになる。この場合、当該事業者が利用する他の事業者のサービスとの関係では、委託先事業者による再委託の関係になることが多いため、医療機関等は、取りまとめを担うシステム関連事業者との間で、当該事業者が再委託や提携に当たり他のシステム関連事業者との間で責任分界が整理されていることを確認した上で、取決めを行う。
- 前者はシステム関連事業者間の責任分界の取決めにも医療機関等が関与していく必要があり、システム関連事業者の数だけ対応が必要となることから、一般的には後者の形態でのサービスの利用を行い、責任分界を定めることが望ましい。
- 企画管理者はこれらの場合について、各事業者に必要な対応を依頼できるよう、責任分界について契約や SLA などにおいて取り決めることが求められる。
- 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。

表２－１　クラウドサービスの提供パターンと責任分界

パターン	概要
医療機関等が複数のシステム関連事業者の提供するサービスを組み合わせて利用	 ・　医療機関等が事業者 A、B をそれぞれ別に契約してサービスを利用（①、②） ・　A、B の連携が取れるように③の部分についても各①、②の契約内容に盛り込む必要がある。

システム関連事業者が複数のサービスを組み合わせて提供するサービスを利用	 ・ 医療機関等は利用する事業者 A と取り決め（①）、A が他のサービス B を利用（②：別の階層サービスを利用）
	 ・ 医療機関等が利用する事業者 A と取り決め(①)、A が他のサービス B を利用（②：別の機能のサービスを利用）

出所：クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）より作成

（2）医療機関等が利用するサービスの類型による責任分界

- 医療機関等が利用するサービス類型により、医療機関等が直接管理できる医療情報システムの範囲が異なる場合がある。
- クラウドサービスの場合、医療情報システムが利用するソフトウェア・ミドルウェア・ハードウェアなどのクラウドサービスのリソースの層により、SaaS、PaaS、IaaS などの類型に分類される。このうち SaaS では、医療情報システムのアプリケーションの層、PaaS では、医療情報システムが利用するミドルウェアの層、IaaS では医療情報システムが利用するサーバやネットワークなどのインフラの層がサービスとして提供されることになる。
- 従って、例えば SaaS を利用する場合には、医療情報システムのうち、アプリケーション部分の管理や責任をシステム関連事業者に委ねることになるため、アプリケーション部分に関する安全管理ガイドラインの遵守状況を確認するに当たって、システム関連事業者との責任分界の検討は必要となる。
- このように、利用するサービスの内容により、それぞれが負うべき責任の内容が異なるため、企画管理者は、委託により医療機関等が行うべき安全管理のうちどの部分の責任をどちらが負うのかといった責任分界を取り決めるとともに、それぞれが対応する安全管理の具体的な内容についてシステム関連事業者と取り決めることが求められる。
- クラウドサービスなどを利用する場合には、利用者側でもルールの策定や設定等の役割などを果たすことが求められる。このような役割分担については、「クラウドサービス提供・利用における適切な設定に関するガイドライン」（総務省　令和 4 年 10 月 31 日）などでも示されている。システム運用担当者は、このような資料を参考にして、システム関連事業者との技術的な役割分担についても調整することが求められる。

2．2．3　第三者提供における責任分界

- 医療機関等が管理する医療情報を第三者に提供する場合には、医療機関等と提供先の第三者との間で責任分界を取り決めることになる。この場合、医療情報データの送信、受信に係る責任分界など技術的対策に関する内容のほか、医療情報の提供に係る法律上の義務への対応（第三者提供に関する手続等）の分担なども確

認する必要がある。

- 責任分界を定めるのは、例えば

  ・医療情報連携ネットワークにおける医療情報の提供

  ・個々の医療機関等間での医療情報の提供

  ・患者の依頼に基づく、医療機関等から特定の場所（患者宅、患者が利用するサービスを提供する事業者等）への当該患者の医療情報の送付

  ・その他法令に基づく第三者提供

  等の場面が想定される。

3．安全管理のための体制と責任･権限

【遵守事項】

① 情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規程等を策定し、経営層の承認を得ること。委員会等が設置されない場合も、情報システムの導入や変更に当たっては、経営層や医療情報システム安全管理責任者等の承認を必要とする仕組みを構築すること。

② 非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者（CISO）や CSIRT などの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。

③ 法律上の対応を含め医療情報の漏えい等が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。

④ 医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。

⑤ 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。

⑥ 医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。

⑦ 患者等からの相談や苦情への対応を行うための体制を構築すること。

⑧ 医療情報システムの安全管理の責任を担う者としての位置付け、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。

⑨ 安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。

⑩ ①～⑨までの対応においては、整備した内容を可視化できるようにすること。

3．1 医療情報システムの安全管理体制の構築

3．1．1 医療情報システムの安全管理のための企画管理者の設置

- 企画管理者とは、医療情報システムの安全管理を行うために必要な運用管理の管理責任者を指す。ここでいう「運用管理」には、安全管理のうち「組織的な対応」と「技術的な対応」のいずれをも含んだものである。

3．1．2 非常時の体制･CSIRT 等の整備

- 医療機関等で情報セキュリティインシデントが発生した場合、この非常時対応として、迅速な判断や対応を要する。これに対応するための体制整備も必要であり、特にサイバー攻撃を受けた場合には、初動対応等専門的な対応が可能な体制を要する。企画管理者は、こうした体制の構築について、通常時からその内容について検討し、必要な措置を講じること。
- ここでいう非常時の体制における対応としては、
  ・影響範囲や損害の特定
  ・被害拡大防止を図るための初動対応
  ・復旧措置のための対応
  ・再発防止策の検討
  などがある。
- 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。

- また、医療情報の漏えいが生じた場合も、法令上必要な対応（個人情報保護法に基づく漏えい等の報告など）や説明責任の実施等の必要な措置を講じる必要があるため、体制や手順等を整備して、経営層の承認を得ること。

３．１．３　医療機関等の内部における職員等に対する教育・訓練等の体制

- 医療情報システムの安全管理においては、医療機関等において医療情報システムに関与する全ての者において当該安全管理に対する知識と意識付けが求められる。そのため、企画管理者は、職員に対して安全管理に関する教育・訓練等を行うとともに、必要な体制を整備することが求められる。

３．１．４　委託等における安全管理の体制

- 医療情報システムの安全管理においては、何らかの形でシステム関連事業者が関与する場合が多く、運用等をシステム関連事業者へ委託することも多い。
- 個人情報保護法第 25 条において委託先の監督義務が示されているとおり、医療機関等においては委託先事業者の安全管理の体制も含めて把握することが必要となる。
- 企画管理者は、委託等における安全管理を行うため、委託先事業者については、委託先事業者の運用等の体制や連絡体制を明確にするほか、運用状況を定期的に把握するために必要な体制を整備すること。

３．１．５　監査体制の整備と監査責任者の設置

- 医療情報システムの安全管理が適切に行われていることを担保するためには、担当者による自己点検だけではなく、客観的な監査によることが重要である。監査は、担当者や企画管理者以外の医療機関等内の第三者による方法や、外部の第三者による方法などが挙げられる。
- 企画管理者は、安全管理が適切に行われていることを確認するために監査等の必要な体制を整備すること。

３．１．６　患者等からの苦情・質問の受付体制

- 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」では、医療機関等が患者などに対して説明責任を果たすためには、個人情報の取扱いに関し患者等からの問い合わせや苦情への対応等を行う窓口機能等を整備することが必要とされている。
- 企画管理者は、患者等からの相談や苦情への対応を行うための受付体制の整備を行うこと。

３．１．７　体制整備の可視化

- 医療情報システムの安全管理の体制を明確にすることは、医療機関等内において医療情報を取り扱う者が滞りなく安全管理に関する対応を行うために必要であり、また非常時において迅速かつ適切な対応をとる上でも重要である。
- 企画管理者は、医療情報システムの安全管理に関して整備した体制に関する内容を文書化等によって可視化し、関係者に共有できるようにする必要がある。

３．２　安全管理の責任・権限

３．２．１　企画管理者の業務範囲と権限

- 経営層は医療情報システムにおける安全管理について医療機関としての最終的な管理責任を負うが、企画管理者はその経営層の判断をサポートし、医療機関等において円滑に安全管理を行うことができるようにすることが重要な業務である。
- 具体的な企画管理者の業務範囲としては、医療機関等の医療情報システムの安全管理について、
  ・経営層が行う管理をサポートするために必要な資料の作成や報告
  ・日常的な医療情報システムの安全管理
  が想定される。また、これらを行うのに必要な承認権限等を有することが想定される。

３．２．２　情報システム管理委員会の業務範囲と権限

- 複数の部門（担当する業務毎に区分された組織）が存在する医療機関等においては経営層の行う管理等の一部又は全部を担うものとして、情報システム管理委員会やセキュリティ委員会等の設置が求められる。委員会を設置する場合には、設置の根拠、目的、業務範囲、構成員の選定・任命方法、権限などを規程等で設け、これに基づいて運営すること。
- また、各部門に委員会に参加するセキュリティ担当者等を配置し、統制に実効性を持たせること。
- 企画管理者は、これらの規程等を策定の上、経営層の承認を得る必要がある。
- 昨今、各部門が独自に調達したシステムやそれに伴う回線が、管理不十分なシャドーIT（※）となり、サイバー攻撃の起点となる事案が起きている。医療機関等の規模を考慮して、委員会が設置されない場合も、情報システムの導入や変更に当たっては、経営層や医療情報システム安全管理責任者等の承認を必要とする仕組みを構築すること。
  ※　IT 部門の管理・許可を受けずに、独自に導入・利用している IT 機器やソフトウェア
- また、多数の外部接続点が存在することは、それ自体が管理を困難にし、VPN 装置等の脆弱性が放置されるリスクが増大する。新たに導入するシステムに保守回線が必要な場合は、医療機関側で集約した回線を利用可能な事業者を選定する等、管理の実効性を高めるための対策を講じること。

３．２．３　担当者の任命、業務範囲、権限

- 企画管理者は、医療情報システムの安全管理のうち特に技術的な対応を行う担当者を任命し、経営層の承認を得る必要がある。
- ここでいう技術的な対応の内容としては、
  ・技術的な対応に必要なリスクアセスメント
  ・採用すべき技術等の選定と実装、関連資料の作成
  ・医療情報システムの運用とそのための規則やマニュアル等の作成
  ・上記に対する企画管理者への報告や協議
  等が考えられる。
- 担当者の権限としては、技術的な対応のうち、通常時における運用に関する判断権限、非常時における一次対応の判断権限などが想定される。そのほか、技術的な対応のうち重要なものについては、企画管理者へ協議を行い、対応することが想定される。

４．医療情報システムの安全管理において必要な規程・文書類の整備

【遵守事項】

① 医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。

② 規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。

③ 医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。

④ 非常時における医療情報システムの運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。

４．１　運用管理において必要な文書の体系（方針、規程、規則、マニュアル等）

- 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である。医療機関等においては安全管理に関する方針を定めるが、これを実際に運用するためには、より詳細な規程等の整備が必要となる。
- 企画管理者は、必要な規程の内容を検討した上で、経営層に諮り、承認を得ることが求められる。安全管理の運用上特に重要なルール等は経営層の判断も必要であることから、規程として定めた上で、経営層において承認する必要がある。
- 整備した規程を踏まえて、細則を定めたり、通常時における対応の手順や内容をルールとして定めたりする必要がある。これらについては、内容に応じて企画管理者が策定、あるいはその策定権限を担当者に移譲するなどして整理することが求められる。

４．２　規程の整備（運用管理規程ほか）

- 規程は、医療機関等においても特に重要なルールが対象となる。規程の位置づけは組織ごとに異なるが、医療情報システムの安全管理に関するものとして、
  ・組織規程
  ・個人情報保護規程
  ・運用管理規程
  ・人事・権限規程（認証との関係で対応）
  などが挙げられるほか、
  ・情報管理に関する規程
  ・資産管理に関する規程
  ・監査に関する規程
  等についても組織の方針に応じて整備することが想定される。
- 企画管理者は、作成する規程の対象や重要度などを考慮した上で規程の整備を行う必要がある。また、整備を行った規程については、関係者に対して周知を図ること。

４．３　規則等の整備

- 規則類は、主に通常時における運用に必要なルールを明文化したものであり、規程を踏まえて具体的な内容を定めるものである。
- 規則のうち、組織的な対応に関するものは、企画管理者自ら策定し、技術的な対応に関するものは、担当者に策定権限を移譲することになる。規則についても、規程と同様、関係者に対して周知を図ること。

４．４　マニュアル等及び各種資料の整備

- マニュアル等は、医療情報システム・サービスの利用者が当該システム・サービスを適切に利用できるようにするためのものである。マニュアル等のうち、医療情報システムの利用の手続に関する内容（システム利用期間や利用権限の設定など）については、企画管理者と担当者とで分担して作成し、医療情報システムの操作等の利用に関する内容のシステム設定作業については、企画管理者が担当者に作業に係る権限移譲を行うなどして設定する。
- そのほか、医療情報システムに関する資料（仕様書、システムに関連するドキュメント（設計書、プログラム開発資料等）、システムの全体構成図、ネットワークの構成図、各システムの担当責任者（委託の場合には、委託先事業者の責任者等）など、運用等に必要な資料については、企画管理者が担当者に対して、適切に整備した上で最新の状態に更新をするよう指示することが求められる。

5．安全管理におけるエビデンス

【遵守事項】

① 医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。

② 証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改ざん等を防止する措置を講じること。

③ 収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。

④ 法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。

5．1 証跡の整備の目的

- 医療情報システムの安全管理においては、医療機関等で策定した規程や規則などに基づく当該システムの適切な利用、運用が求められる。システムの利用又は操作の証跡（操作ログ、システムログ）を収集し、レビューすることで、医療情報システムが適切に利用・運用されているかどうか等を確認できる。
- 証跡のレビューでは、当該システムの利用、運用が規程や規則等に定めた内容のとおりに行われていることを確認するほか、本来想定されていない利用や不正な利用などを確認する目的で用いることができる。例えば、外部から侵入があった場合に、その痕跡を発見して、不正な攻撃を追跡する起点としたり、本来業務を行わない時間にもかかわらず、職員などが頻繁に医療情報システムを利用しているなどの事実を確認して、不正利用を探知するきっかけとしたりすることなどが想定される。
- 企画管理者には、このような観点から、医療情報システムに関連する証跡等の整備を行うことが求められる。

5．2 整備する証跡の種類

- 証跡については、あらかじめシステムの利用に際して必要な手続などが適切に行われていることを確認するためのものと、システムログのように、利用されている医療情報システム等が自動的に記録するものが挙げられる。
- 前者は、例えば ID の申請など、医療情報システム・サービスを利用するに際して必要な手続や判断が適切になされていることをあらかじめ確認するものである。こうした予防的な確認を行うことで、不適切な利用の防止が可能となる。
- 後者は、医療情報システムにおける利用者の操作やシステムの動作が自動的に記録されることで、システム障害やサイバー攻撃などが生じた際の原因の追跡、あるいは一見、正常に動作しているシステムが不適切に利用されていることをログのレビューから発見するなど、事後の発見に寄与するものが多い。
- なお、証跡に関しては、過大に収集することにより、運用上の負担が過大となり、結果として医療情報システムの運用に支障が出ることも想定される。
- 企画管理者は、このような特性を理解した上で、担当者と協議して、リスク評価などを踏まえて、適切な証跡を適宜選択して整備することが求められる。

5．3 証跡のレビュー

- 証跡には不正利用の探知の起点ともなるため、単に収集するだけではなく、適宜レビューを行うことが重要である。

そのため、企画管理者は、適宜証跡のレビューを行うことが求められる。

- また、証跡のレビューは、その周期が長すぎると発見までの間に不正な利用が継続してしまうリスクなどがある。一方で、レビュー対象が多いことで作業負担が過大になるため、リスクと負担のバランスを勘案すること。そのため企画管理者は、担当者と協議の上でレビューの対象や周期などを決定することが求められる。

５．４　証跡の管理

- 証跡は適切な安全管理を確認するための根拠（エビデンス）であり、改ざんや変更などがなされないように、適切な管理が求められる。システムログ等の管理に関する技術的な対応については、担当者と協議の上で必要な措置を講じること。

6．リスクマネジメント（リスク管理）

【遵守事項】

① 医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講じること。

② 医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、常に最新の状態で管理すること。

③ 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。

④ 安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。

⑤ ②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。

⑥ リスク評価を踏まえ、経営層がリスク判断をする際に必要な資料を整理すること。

⑦ リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。

⑧ リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。

⑨ PDCA（Plan-Do-Check-Act）モデルに基づく ISMS（Information Security Management System：情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMS が適切に実施されていることを確認し、経営層にその状況を報告すること。

⑩ PDCA モデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。

6．1 運用管理におけるリスクマネジメント

6．1．1 リスクマネジメントの役割

- 医療情報システムにおける情報セキュリティ対策を講じるにあたっては、組織としてのマネジメントが必要なため、運用管理としてリスクマネジメントを適切に行うことが求められる。
- リスクマネジメントとしては、リスク分析とリスク評価、そしてこれらを踏まえたリスク管理を行う必要があるところ、運用管理において、この一連のリスクマネジメントサイクルが適切に行われるよう管理を行うことが求められる。
- リスク分析とリスク評価については、医療機関等における情報資産の状況などを把握しながら、医療機関等で利用する医療情報システム・サービスを踏まえて行うことから、情報システムの技術担当者などとも協働して行うことになる。その上で、リスクに対する判断は最終的には経営層に委ねられることになるが、運用管理上は、企画管理者において経営層による判断に必要な資料の整理などを行うことが求められる。
- サイバー攻撃など日々新しい形態の脅威が発生することから、医療情報システムにおけるリスク分析やリスク評価なども定期的に行うことが求められ、これら一連のマネジメントサイクルが適切に実施されるよう管理することが運用管理において求められる。
- 企画管理者は、経営層に対して、医療機関等内でリスクマネジメントが適切に実施されているかどうかを報告し、不備があれば改善策を講じることも求められる。

6．1．2 リスクアセスメント（リスク分析、リスク評価）の役割

- リスクアセスメントは、企画管理者と情報システムの技術担当者とで協働して実施することになるが、運用管理上

は、特に取り扱う情報の把握とこれに対するリスク評価を担当者と行うことが求められる。

- 取り扱う情報の把握は、医療機関等において取り扱う医療情報と、医療情報システムで扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認することである。そのため、取り扱う情報等に関するリストを作成し、企画管理者が必要に応じて速やかに確認できる状態で管理することが求められる。近年では、医療情報システムに係る外部委託先や製品供給などとのサプライチェーンに関するリスクも大きく、リスク分析の対象とすることが求められる。
- 安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等の視点からみた影響の大きさと、業務継続の視点からみた影響の大きさを考慮する必要がある。このほかにも、医療機関等の経営上の視点、人事管理上の視点等の必要な視点を加えて重要度を分類する。例えば、医療情報の安全性に問題が生じた場合、患者等に極めて深刻な影響を与える可能性があるため、医療情報は最も重要度の高い情報として分類される。また、医療情報システムについても、医療サービスの提供継続性への影響の観点から重要度を判断して分類し、管理状況を把握する必要がある。
- リスク評価は、リスクの発現率と影響の大きさから算定することになる。そのため、リスクの影響の大きさに関する判断は企画管理者が行い、リスクの発現率に関する技術的な判断は担当者と協働して行うことが求められる。

6．2 ISMS（Information Security Management System：情報セキュリティマネジメントシステム）

- 医療情報システムの情報セキュリティを確保するために、ISMS を構築することが重要である。ISMS は、PDCA モデルに基づいて行われる（※）が、運用管理においては、このような PDCA モデルが適切に行われるよう ISMS を構築し、管理することが求められる。

  ※ JIS Q27001:2023 では PDCA との記述は使われていないが、「情報セキュリティマネジメントシステム」として「組織は、この規格の要求事項に従って ISMS を確立し、実施し、維持し、かつ、継続的に改善しなければならない。」と記述されている。継続的改善のモデルとして PDCA サイクルが理解しやすいため、旧版（JIS Q27001:2006）より引用している。
- ISMS の構築のために、JIS Q27001:2006 では下表のように PDCA モデルが規定される。運用管理においては、PDCA モデルを採用し、管理、確認をすることが求められる。

表６－１　ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実行 (ISMS の導入及び運用)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及び見直し)	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P（Plan）では、ISMS 構築の骨格となる文書（基本方針、運用管理規程等）により、ISMS 構築手順を確立する。

D（Do）では、P で準備した文書や手順を使って実際に ISMS を構築する。

C（Check）では、構築した ISMS が適切に運用されているか、監視と見直しを行う。

A（Act）では、改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

7．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）

【遵守事項】

① 医療情報を取り扱う者を職員として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等の安全管理対策を実施すること。

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。また、教育・訓練の実施状況について定期的に経営層に報告すること。

③ 医療機関等の事務、運用等を外部の事業者に委託する場合は、委託契約の契約書に守秘・非開示に関する内容を含めること。

④ ③の委託契約の際に、当該委託先事業者の就業規則等に①及び②の対応を含めるよう求めること。

⑤ 外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。

- 保存した医療情報の取扱いに関して監督可能とするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。
- 医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。
- 総務省・経済産業省の定めた「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」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。
- 外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「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」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。）
- 外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。
- 保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。）を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏えいや、誤った情報閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。
- 保存された情報を格納する情報機器等が、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。

⑥ 外部保存等の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。

a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況

b 医療情報等の安全管理に係る実施体制の整備状況

c マルウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況

d 実績等に基づく個人データ安全管理に関する信用度

e 財務諸表等に基づく経営の健全性

f プライバシーマーク認定又は ISMS 認証の取得

g 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）

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

h　医療情報を保存する情報機器が設置されている場所(地域、国)
i　委託先事業者に対する国外法の適用可能性

⑦ 医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。
– 委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。
– 保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。
– 匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。
– 保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏えいや、誤った情報閲覧が起こらないように配慮すること。
– 情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。

⑧ 委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、必要に応じてその改善を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。

⑨ 委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。

⑩ 外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。

7．1　職員管理

- 医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、人による誤りの防止を目的とした人的安全管理対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育・訓練に関する事項が含まれる。
- 以下の者については、医療機関等の職員に対する人的安全管理の対象として整理される。

（a） 医師、看護師等の業務で診療に関わる情報を取り扱い、法令上の守秘義務のある者
（b） 医事課職員等、業務に携わることで医療情報を取扱い、守秘義務を負う者

- いずれも、医療情報を取り扱う者として、守秘義務や教育・訓練等を受ける義務を課す雇用契約等を締結することで、企画管理者は人的管理を行うことができる。なお、この場合、直接雇用する職員だけではなく、派遣雇用

の者も対象となる。

- 守秘義務については、就業時はもちろん、退職後においても遵守される必要がある。医療機関等の職員に対して退職後を含めて医療情報に関する守秘義務を課すこと。

7．2　委託先事業者管理

- 医療情報システム等を委託する場合には、委託先事業者である法人だけではなく、実際にその業務にあたる者に対して、医療機関等の職員と同様の責任や守秘義務を課すことで、医療機関等としての人的管理を実現する必要がある。
- 企画管理者は、委託先事業者との契約に際して、委託先事業者と当該事業者で業務にあたる者との雇用契約等において、守秘義務等を含んでいることを確認し、委託先事業者において人的管理が適切に行われることを確認する必要がある。

7．3　教育・訓練

- 医療機関等の職員が医療情報の安全管理に関して遵守すべき内容を十分理解できるよう、教育を行うことが求められる。また、非常時などでも適切に行動できるよう、通常時における訓練の実施も求められる。
- 企画管理者は、職員に対する教育・訓練を定期的に行うことが必要である。また、就業時間内に実施すること。
- 医療情報システムの利用に関連する教育内容については、システムの担当者と協議の上、必要な事項を整理することが求められる。特に、近年、医療機関等におけるサイバー攻撃被害により、地域医療の安全性を脅かす事案も発生していることから、公表されている各種資料を参考に、職員への教育・育成を実施すること。
- 医療情報システムの安全管理やセキュリティ対策業務に従事する人材に対し、独立行政法人情報処理推進機構（IPA）の実施する「情報処理安全確保支援士」資格の取得、「情報セキュリティマネジメント試験」等の試験合格、演習・訓練への参加等を推進することが望ましい。

7．4　委託先事業者選定

- 適切な委託先事業者の選定は、個人情報保護法における委託先の監督（第 25 条）の一環として必要であるほか、医療情報を医療機関の外部に保存する場合に、「外部保存通知」（第２　1（2））にあるとおり安全が確保された場所に保存する観点からも必要である。
- 外部のシステム関連事業者との契約に基づいて、医療情報を外部保存する場合には、データセンター等の情報処理の委託先事業者が総務省・経済産業省の定めた「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」の要求事項を満たしていることを確認し、契約等においてもそれらを遵守することを明確に定めること。
- 委託先事業者の選定を法令等の要求に基づいて適切に行う必要があるほか、リスク評価を踏まえた観点からも適切に選定を行う必要がある。また、当該選定に際しては、担当者と協議し、技術的な観点からの妥当性なども加味すること。なお、選定時に認識されたリスク評価内容はその後変化しうる。特にサイバーセキュリティにおいては、攻撃方法の巧妙化に伴い、適宜、リスク対応の再検討を要する。対象事業者が行うリスクの管理体制や、リスクが選定時以降に上昇した場合の対応も想定することが望ましい。契約時の取決め内容においてもこれに関する随時の情報提供等を含めることが重要である。
- 重要度の高い委託の場合は、経営層に丁寧に報告の上、承認を得ること。

７．５　外部保存･外部委託の終了

- 医療情報が機微な個人情報であることから、外部保存を終了する場合や外部保存の委託を終了する場合には、医療機関等及び委託先事業者の双方で適切な配慮が求められる。
- 外部保存の開始時に、保存の期限等の保存期間に関する条件が明確に示されている必要があり、外部保存の終了は、この条件に基づいて適切に実行されなければならない。期限には具体的な期日が指定されている場合もあれば、「一連の診療の終了後○○年」といった一定の条件が示されている場合も想定される。
- 医療機関等は、委託先事業者に保存されている医療情報を定期的に確認し、外部保存を終了すべき医療情報が、速やかかつ厳正に処理されているかを監査しなくてはならない。また、委託先事業者も、委託元の医療機関等の求めに応じて、保存している医療情報を厳正に取り扱い、保存の終了を適切に処理している旨を委託元の医療機関等に明確に示す必要がある。
- 外部保存の保存期間や委託の終了に伴う医療情報の破棄や返却に関する規定は、外部保存を開始する前に契約書にも明記をしておく必要がある。また、実際の破棄や返却に備えて、事前に破棄や返却等の手順を明確化した資料等を作成しておくこと。
- 委託する医療機関等及び委託先事業者の双方に厳正な取扱いが求められるのは、同意された期間を超えて個人情報を保持することが個人情報の保護上問題となり得るためであり、十分な留意が必要である。
- また、患者の医療情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索履歴等も厳正な取扱いの後に破棄されなければならない。
- 医療情報の破棄に関しては、可搬媒体で保存している場合でも責任を持って対応する必要がある。

７．６　患者への説明等

- 医療機関等は、患者から医療情報を預かっているという観点から、患者に対しては適切な説明と理解を得ることが求められる。医療情報の取扱いを医療機関等以外に委ねる場合には、患者の理解を得た上で行うこと。
- 外部保存の委託について、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。

8．情報管理（管理、持ち出し、破棄等）

【遵守事項】

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等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。

② 医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。

③ 医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。

④ 医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。

⑤ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。

⑥ 医療機関等外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。

⑦ 持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。

⑧ 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等を定めること。

⑨ 患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。

⑩ 医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。

⑪ 医療情報の破棄に関する手順等を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。

⑫ 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、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業者における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。

8．1 情報管理

8．1．1 情報管理方針の整備

- 医療機関等が保有する情報の管理について、組織としての管理方針を定める必要がある。小規模な医療機関等であって、情報管理体制が明文化されていない場合でも、情報の持ち出しは想定されることから、リスク分析を実施して対策を検討しておくこと。
- 企画管理者は、情報管理方針を策定し、経営層による承認を得ること。

８．１．２　情報管理の手順

- 情報管理方針を踏まえて、具体的な情報管理の手順を定める必要がある。情報管理の手順等は、管理対象となる情報により異なる。各情報を主に管理する者を管理責任者として、それぞれで適切に管理できるよう手順の策定や管理方法などを定めること。
- 情報については、一般的には、作成、利用、保存、廃棄などのライフサイクルが想定される。それぞれの過程ごとに、セキュリティが確保できるよう、適切に管理すること。

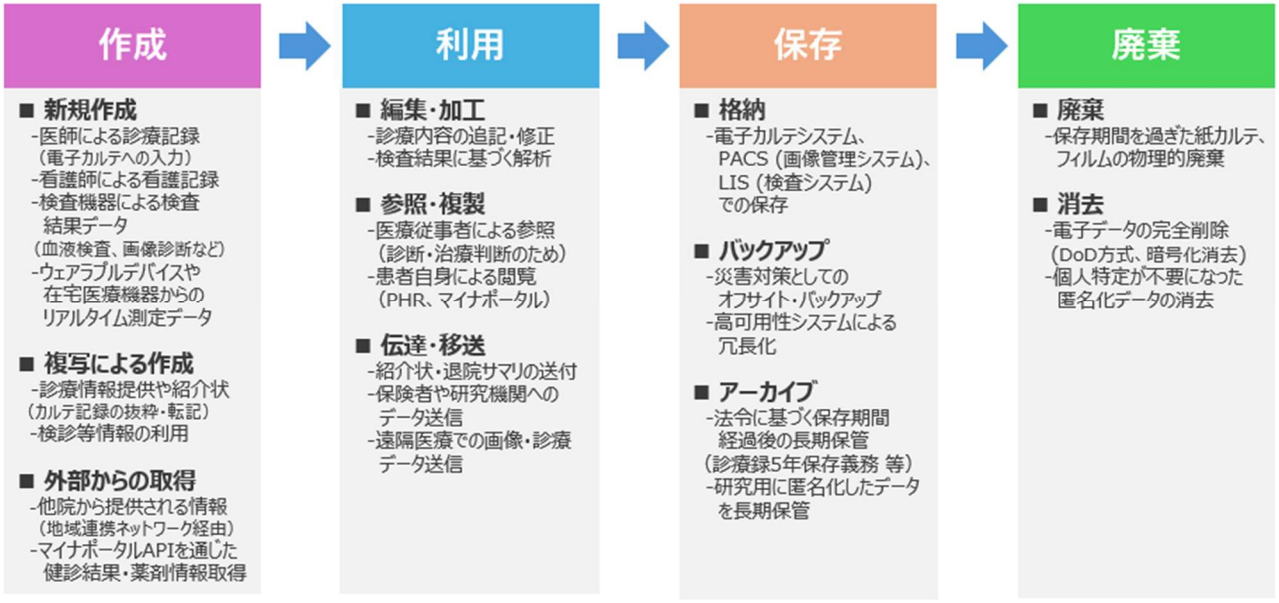


図８－１　情報のライフサイクル

- 企画管理者は、これらの管理手順等について、各情報の管理責任者から整備状況等の報告を受け、把握する必要がある。
- 漏えいや不正利用を防ぐ観点から、医療情報が保存されている施設、情報機器等へのアクセスを制限し、管理を行うための規則等を設ける必要がある。

８．１．３　情報の安全管理状況の報告

- 企画管理者は情報の管理状況の把握を行う必要がある。管理状況の把握対象は、医療機関等が保有している情報、特に医療情報の状況（どの程度の人数の情報が管理されているか、どのような情報が管理されているか）などと、それらに対する管理状況（システムによる管理か、紙媒体によるものか、内部管理か外部管理か）などについて定期的に把握し、経営層に対して報告を行うこと。
- 医療情報に関しては、患者の取り違い等の様々なリスクを避ける等の観点から、的確に各患者を識別し、適切に管理されるように運用する必要がある。

８．２　医療情報の持ち出し

８．２．１　医療情報の持ち出し手順等の策定

- 医療機関等が管理する情報又は情報機器の持ち出しには、漏えいのリスクが伴う。このリスクを低減するため、組織として情報又は情報機器の持ち出しに関する取扱いを整理した方針が必要である。当該方針は、物理媒体での持ち出しだけではなく、外部のクラウドサービスなどを用いたデータ等の持ち出しや、テレワークなどによる外部か

らの作業に伴う持ち出しなども想定した内容とすることが求められる。

- 特に可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤、誤送信等のリスクが大きいことから、人的安全管理対策と併せて対応する必要がある。
- これらのリスクを低減するため、医療情報の持ち出しに関する手順等を策定し、職員等の教育など周知を図ること。

８．２．２　記録媒体・情報機器等による持ち出し

- 医療機関等の外部に医療情報を持ち出す方法の一つとして、記録媒体や情報機器等への格納による持ち出しが想定される。持ち出し先での紛失や盗難のほか、外部の情報機器へ接続した場合にはマルウェアの混入なども想定されることから、持ち出す前だけではなく、持ち出した後の対応についても検討する必要がある。
- 記録媒体・情報機器等による医療情報の持ち出しに際しては、
  ・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
  ・医療情報の持ち出しに対する手続等を策定
  ・記録媒体・情報機器等を持ち帰った際の確認に関する手続等の策定
  等を行うことが求められる。
- 医療情報を持ち出す際の記録媒体や情報機器に関する安全性について、担当者と協議すること。
- ネットワークを通じて外部保存を行い、外部保存の委託先事業者においてこのデータを可搬媒体に保存する場合も、同様の対策を講じるよう委託先事業者に求めること。

８．２．３　ネットワークサービスを用いた持ち出し

- 医療機関等の外部に容易にデータを保管し、加工や共有もできるクラウドサービスなどが普及している。特に容量が大きいデータの外部との交換においては、ネットワークを通じたクラウドサービスを利用することも想定される。
- このようなクラウドサービスの中には、管理者の承認なく容易に外部への保存などが可能となるものもあることから、ネットワークを通じた医療情報の持ち出しについても、適切な対応を講じること。
- 医療情報の持ち出しが可能なネットワークサービスについては、企画管理者が承認したもののみを利用できる措置を講じることが必要となる。その上で、ネットワークサービスを通じた医療情報の持ち出しに関する手順やルール等を定めること。
- ネットワークサービスの利用と管理に際して、担当者と協議し、必要に応じて接続制御などを行うことも想定される。

８．２．４　外部からのアクセスによる持ち出し

- 医療機関等が管理する医療情報システムに、医療機関等の外部からアクセスして、医療情報を参照・利用することが想定される。具体的には、
  ・ 医療機関等の職員が、訪問先やテレワークなどにより、医療機関等が管理する端末等を通じてアクセスする場合
  ・ 患者が、自宅等から自らの情報にアクセスする場合
  ・ 医療機関等が保有する医療情報システムに対して、事業者が外部からアクセスして保守等を行う場合
  等が想定される。
- 企画管理者は、このような外部からのアクセスによる医療情報の参照や利用を認めるかどうか、どのような場合に認めるか、認める際の条件や制限、技術的な対応による安全管理対策などについて整理し、規則や手順を策定する必要がある。また、技術的な対応による安全管理対策については、担当者に具体的な内容の検討を指示すること。

- 患者等が自らの情報にアクセスする場合には、必要な説明を行い、責任範囲等を明らかにすることも求められる。

８．２．５　持ち出した医療情報を格納する記録媒体等の紛失等への対応

- 持ち出した医療情報を格納する記録媒体等の紛失や盗難、あるいは利用するネットワークサービスに関する設定や誤操作により医療情報が漏えいした場合には、組織として速やかに必要な対応を行う必要がある。
- 漏えい時の初期対応などについて、企画管理者は情報管理規程や運用管理規程等の中で定めておくこと。例えば、紛失等が発覚した場合の連絡先や対応手順、対応方法などについてあらかじめ整理することが想定される。
- 漏えい又はその可能性がある場合には、医療情報の漏えいが生じた場合の対応（「３．１．２　非常時等の体制・CSIRT 等の整備」）や、非常時の対応（「１１．３　非常時の対応」）に基づいた対応が求められる。

８．２．６　持ち出し状況のレビュー

- 医療情報の外部への持ち出しを最小限とし、不正な持ち出し等が生じないように、定期的に持ち出し状況のレビューを行う必要がある。
- 不自然な持ち出し等がある場合には、その理由を確認する等、必要な管理を行うこと

８．３　医療情報の破棄

８．３．１　破棄の手順等の策定

- 医療情報の破棄に際しては、安全性を確保した上で適切に破棄するための手順の策定が必要となる。
  当該手順には、下記違いに応じた内容を示すこと。
  ・情報種別
  ・管理形態（紙媒体、システム管理等）
  ・破棄対象（情報だけか、記録媒体も対象か）
- 特にシステム上のデータの破棄や記録媒体・情報機器等の破棄については、漏えいや不正利用のリスクが生じることに留意が必要である。

８．３．２　外部保存をシステム関連事業者に委託している場合の対応

- 委託先事業者において医療情報を破棄する際、適切に破棄されたことを、医療機関等においても確認する必要がある。企画管理者は、破棄されたことを確認できる証跡の提供を、委託先事業者に求めること。
- クラウドサービス上での破棄など、その証明を行うことが困難な場合もある。その場合、破棄の手順や実際に行った処理に関する証跡の提供など、証明に代替する対応を委託先事業者に求めること。その上で、委託先事業者における破棄の手順や基準が、医療機関等における破棄の手順や基準に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。

９．医療情報システムに用いる情報機器等の資産管理

【遵守事項】

① 医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、物理的な資産のほか、医療情報システムが利用するサービス、ライセンスなども含む。）

② 医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。

③ 台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。また担当者と協働して、滅失状況などについても適宜確認すること。

④ 医療情報システムにおけるサプライチェーンについて、医療情報システム等の情報資産に関係する事業者にシステムの管理体制や供給体制を確認し、サプライチェーンリスクの所在について整理すること。

⑤ 医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況、脆弱性に関する対応状況等）を確認するよう指示し、報告を受け、適宜必要な対応を行うこと。

⑥ 医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。

⑦ 医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えばBYOD[4]端末の利用）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規程等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。

⑧ 医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。

９．１　情報機器等の台帳管理

- 医療情報システムで用いる情報機器等に関する安全性を確保するためには、利用を予定している情報機器等の所在、またそれらの情報機器等の使用可否等を、適切に管理する必要がある。
- 企画管理者は、医療情報システムで用いる情報機器等について、台帳管理を行い、情報機器等が利用に適した状況にあることを確認可能としておく必要がある。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、使用するソフトウェアやサービスのバージョン、ライセンスの状況などが想定される。
- 昨今の医療情報システムでは、BYOD 端末などの利用も想定される。企画管理者は、こうした医療機関等が管理しない端末の利用についても、その利用条件や利用範囲、管理方法などについての規則を策定した上で、併せて台帳管理すること。加えて、BYOD での利用に関する具体的な条件等について担当者と協議し、必要に応じて技術的な対応を講じ、規則の内容に含めること。
- 整備した台帳を定期的に棚卸しして、適切な状況にあることを確認する必要がある。

[4] BYOD：Bring Your Own Device。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。

９．２　サプライチェーン管理

- サプライチェーンとは、一般的には原材料の調達から製造・物流・販売まで、製品やサービスが顧客に届くまでの一連のつながり（企業群）を指す。この連鎖のどこかでトラブルが起きると、自社への供給が止まる可能性があり、これをサプライチェーンリスクと呼ぶ。近年は自然災害などの物理的リスクだけでなく、取引先や委託先の IT の弱点を突く「サイバー起因のサプライチェーンリスク」が特に問題視されている。
- サプライチェーンリスクでは、不正機能等の埋め込み、サービスの供給途絶、外部サービスにおける情報の不適切な取扱い、海外拠点、グループ組織、取引先等を経由したサイバー攻撃などが挙げられる。
- 近年のサプライチェーンにおけるサイバー攻撃では、最終的な攻撃目標を生産している、セキュリティが堅牢な組織を狙うのではなく、そのサプライチェーン（供給の連鎖）工程上の、セキュリティレベルの低い組織（企業、委託先等）を狙って攻撃を仕掛け、最終的な攻撃目標に、マルウェアなどを仕込む手法がみられる。
- またサイバー攻撃以外でも、複数の事業者が提供するシステム・サービスを組み合わせて利用する際に、一部の事業者のシステム・サービスの提供終了や機能向上を図らないことによるリスクなども指摘されている。
- このような脅威に対するリスクを低減するため、医療情報システムに係る委託先や機器に関するサプライチェーン関係を整理し、リスクアセスメントや対策の整備を行うことが重要である。

９．３　情報機器等の安全性の確認

- 管理している情報機器等を医療情報システムとして利用するためには、情報機器等の安全性が確認されている必要がある。特にサイバー攻撃等への対応という観点からは、必要なファームウェアの更新や脆弱性対策の実施、EOS（End of Support：サポート終了）の対象となっていないことなどを確認すること。
- EOS を越えている場合、製造販売事業者等と連携し、補完的対策を講じること。
- 情報機器等の安全性の確認を行うためには、安全性に関する情報を的確に把握することが求められる。企画管理者は、担当者に安全に関する情報の収集（利用している情報機器等やシステム、プログラム等）と、それを踏まえた対応を指示し、その対応状況を確認すること。
- 安全性確認の対象は、情報機器だけではなく、利用するサービスも含まれる。サービスの場合、当該サービス提供事業者との委託契約等に、安全性の状況を定期的に確認する旨を含めることなどが想定される。
- クラウドサービスなどの場合は、サービス内容によっては、利用可能な情報システムの容量に上限があることが想定される。十分な容量を確保できないなどといった、可用性に関するリスクを低減するよう、システム関連事業者に対して、必要な事項を適宜確認すること。

９．４　情報機器等の資産管理状況の報告

- 情報機器の管理状況については、企画管理者が把握した上で、経営層に報告し、承認を得る必要がある。管理状況を把握する際は、担当者と協議の上、資料を整理すること。
- この際、情報機器やソフトウェアのアップデートの履行状況や、EOS の対象となった情報機器やソフトウェアの状況、委託契約の範囲（アップデート等に関する責任分界含む）を含めること。

１０．運用に対する点検･監査

【遵守事項】

① 医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「５． 安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。

② 医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム･サービスの性格上、報告に基づく確認が難しい場合は、SLA に対する評価等の中で確認すること。

③ 医療情報システムの取扱いに関する点検結果を、経営層に報告し、承認を得ること。

④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。

１０．１ 運用に対する点検

- 医療情報システムの運用の安全管理を把握するために、企画管理者は、自ら通常時の運用状況を確認することが重要である。組織的な対応について、適切に運用できているか、改善点があるとすればどこか、定期的に点検することが求められる。併せて、担当者に対して、技術的な対応についての点検を指示し、改善すべき部分があればその旨の報告を求めることも必要となる。

１０．２ 運用に対する監査

- 安全管理が適切になされていることを担保するために、第三者による確認や監査を行うことは有効である。
- 監査については、企画管理者等から独立した組織等による内部監査と、外部の第三者による外部監査がある。医療機関等の組織形態や、医療情報システムの規模、利用形態に応じた確認であることが重要である。監査への対応の負担が過大となり、運用に多大な支障が出るような事態はさけるように留意すること。
- 企画管理者は、このような観点も踏まえて監査方針を策定し、経営層の承認を得て、必要な監査を実施すること。また、当該監査結果を経営層に報告し、監査における指摘事項等に対応するため、改善を図っていく必要がある。

１１．非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定

【遵守事項】

① 医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、BCP（Business Continuity Plan：事業継続計画）を策定すること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含め、経営層の承認を得ること。

② 医療機関等が定める非常時の定義や BCP との整合性を確認して対応方針を策定すること。

③ 非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。

④ 各種規程等に非常時における対応手順・内容も含めること。

⑤ 非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。

⑥ 非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。

⑦ 非常時の対応状況を定期的に確認し、経営層に報告の上、承認を得ること。

⑧ 非常時には、安全管理の状況を適宜把握し、経営層に報告すること。また、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。

⑨ 非常時に対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。

１１．１ 非常時における対応方針の策定

- 医療サービスを継続して提供可能とするため、非常時における医療情報システムに関する対応は重要である。
- 災害やサイバー攻撃、システム障害が生じた場合に、経営層及び非常時における意思決定担当者は
  - 医療サービスの提供をどのように継続するか
  - どの医療情報システムをどのように利用するか

  等を総合的に判断する必要がある。
- 企画管理者は、経営層等の判断を見据えて、非常時における対応方針や手順などを策定する必要がある。その内容は、医療機関等で策定される BCP との整合性を踏まえた内容とすること。併せて「非常時」の定義も明らかにすることが求められる。策定した方針や手順等については、経営層に対して報告の上、承認を得ること。
- 非常時の発生原因としては、主に災害、サイバー攻撃、システム障害などが挙げられ、それぞれの原因に対して、具体的な対応が異なる。対応方針や手順等を策定する際も、具体的な事象発生原因や被害の規模等を勘案して、それぞれに対応した内容とすること。

表１１－１　非常時の事象発生原因に応じた必要な対応例

原因	概要	必要な対応
災害	・災害による医療情報システムの停止、あるいは損傷・破壊 ・災害による医療情報システムの運用管理に必要な資源（要員、機材、電源等）の不足等に伴う運用等への支障　など	・災害発生時のフェールセーフ ・復旧、復帰に向けた対応 ・資源配分、運用規模の変更　など
サイバー攻撃	・外部からの攻撃による医療情報システムの停止、あるいは損傷・破壊 ・医療情報の改ざんや漏えい　など	・被害状況の把握 ・証拠・証跡の保全 ・被害拡大の防止 ・原因の究明 ・復旧計画の策定　など
システム障害（ネットワーク障害含む。）	・医療情報システム（サービス）の停止・パフォーマンス低下　など	・障害状況の把握 ・障害の原因究明 ・復旧、改修の計画策定　など

- 企画管理者は、非常時に法令で求められる対応についても、適切かつ迅速に対応できるよう体制を整備しておく必要がある。また、サイバー攻撃に際しては、「１２．サイバーセキュリティ」に示すように、所管官庁等への迅速な連絡が求められる。

１１．２　非常時に備えた通常時からの対応

- 非常時に適切に対応するためには、通常時からの準備等が重要である。通常時から対応する内容としては、非常時の具体的な手順や連絡体制等の構築のほか、医療情報システムにおける被害極小化や迅速な復旧のための対策、冗長化等が挙げられる。
- 具体的な対応は、発生原因によって異なる。例えばバックアップの設計・確保も、災害の場合は大規模災害を視野に入れた内容となるが、サイバー攻撃においては、耐攻撃性や業務継続性という観点から対応が必要となる。また、システム障害においては、システム復旧や原因究明の迅速性などが優先されることもある。
- 企画管理者は、このような非常時の発生原因による違いを考慮して、通常時に実施できる対応を整理し、経営層の承認を得ること。

表１１－２　非常時の事象発生原因に応じた通常時からの対策例

原因	必要な対応	求められる対策例
災害（主に地震、水害、火災等、医療情報システムのみに限らず、医療機関等全体への被災が想定されるもの）	災害発生時のフェールセーフ	・情報システムの冗長化（電源、ネットワーク、サーバ等） ・情報システム・サービスの安全な停止のための手順の整備 ・非常時のリスクを踏まえたセキュリティ対策の準備（認証方法等） ・遠隔制御等による対応方法に関する手順等の整備 ・利用者等の関係者の教育・訓練　など
	復旧、復帰に向けた対応	・BCP に基づく情報システムにおける運用手順の整備 ・発災直後の運用から、通常時の運用への復帰手順の整備 ・最新の医療情報システムの状態に復旧・復帰するための手順整備 ・バックアップ整備（大規模災害等を想定した遠隔保管を含む。） ・臨時措置(仮復旧など)として必要な情報システム資源（情報機器等）の確保方法の準備　など
	資源配分、運用規模の変更	・資源不足の程度に応じた対応の確認　など
サイバー攻撃	攻撃による被害発生のリスク回避や低減	・緊急時対応体制（CSIRT）の整備 ・利用者等の関係者の教育・訓練 ・脆弱性対策等 ・情報共有体制の構築（外部有識者、事業者） ・攻撃を受けた際の代替運用や手段の確保　など
	被害拡大の防止	・BCP を踏まえた情報システムに関する手順整備 ・ネットワークやバックアップ等に関する安全性の確保（論理的／物理的ネットワークの構成分割、追記不能型のバックアップなど）　など
	復旧計画の策定	・医療情報システムに関する各種ドキュメント（構成、設定、手順など）の整備 ・臨時措置（仮復旧など）に必要な情報システム資源（情報機器等）の確保方法の準備　など
システム障害（ネットワーク障害含む）	障害発生時のリスク回避やリスク低減	・組織内外の周知、障害対応体制の整備 ・冗長化対策（ホットスタンバイ／コールドスタンバイ、ネットワーク等の二重化など） ・長期間にわたる障害の場合の方針や手順の整備 ・データやシステムのバックアップの確保　など

１１．３　非常時の対応

- 非常時の対応には、主に状況把握・拡大防止・原因究明等と、通常時への復旧・復帰に向けた対応などがある。
- 非常時には、あらかじめ準備した手順等に基づいて対応する必要がある。一方で、事前に想定していない事象の発生もありうることから、想定外の状況に対する方針などもあらかじめ定めておく必要がある。
- 企画管理者は、想定される非常時の原因に応じた具体的な対応や措置を整理する必要がある。

表１１－３　非常時の原因に応じた対応例

非常時の原因	必要な対応	求められる対応や措置例
災害 （主に地震、水害、火災等、医療情報システムのみに限らず、医療機関等全体への被災が想定されるもの）	災害発生時のフェールセーフ	・要員・情報システムの安全性の確保 ・冗長化した情報システム等の切り替え ・情報システム・サービスの安全な停止 ・リスクを踏まえた臨時措置（認証方法の変更など）の実施　など
	復旧、復帰に向けた対応	・発災直後の非常時の運用から、通常時の運用への復旧、復帰 ・医療情報システムの復旧、最新化　など
	資源配分、運用規模の変更	・要員（臨時要員含む）確保　など
サイバー攻撃	攻撃による被害発生のリスク回避やリスク低減	・被害状況、業務影響の把握 ・不正アクセスやマルウェアに対する検知・遮断・隔離 ・代替運用や手段への切り替え　など
	被害拡大の防止	・発生原因の特定と被害拡大防止策の検討（サービスの遮断等） ・組織内の連絡・情報共有体制の整備 ・システム関連事業者を含む対策を実施するための協働体制の整備 ・外部有識者、システム関連事業者からの情報収集・支援 ・所管官庁・関係者への報告や広報（状況説明等）など
	復旧、復帰に向けた対応	・証拠、証跡の分析検証、原因の特定 ・医療情報システムの復旧、最新化 ・安全性の確認（被害原因の封じ込め・解消等） ・所管官庁・関係者への報告、広報（復旧予定等）など
システム障害 （ネットワーク障害含む。）	障害発生時のリスク回避やリスク低減	・障害状況、業務影響の把握 ・代替運用や手段への切り替え　など
	復旧、復帰に向けた対応	・障害原因の特定 ・改修予定や再発防止措置の策定　など

１２．サイバーセキュリティ

【遵守事項】

① サイバーセキュリティに関する組織的対策、職員や委託先事業者への対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。

② 整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。

③ サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。

④ サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認すること。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。

⑤ サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。

⑥ サイバーセキュリティインシデントが発生した際に、情報交換等を行う関係者の情報をあらかじめ整理し、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）

⑦ サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏えいや医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成 30 年 10 月 29 日付け医政総発 1029 第 1 号・医政地発 1029 第 3 号・医政研発 1029 第 1 号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。

⑧ サイバーセキュリティインシデントが発生した際には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。

⑨ サイバーセキュリティインシデントによる非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定」に示す内容を実施すること。

１２．１ サイバーセキュリティ対応計画の策定

- 非常時の原因の一つであるサイバー攻撃は、攻撃者が悪意を以て行う犯罪行為であり、その方法も様々である。情報システムの高度化に合わせて変化することや、システム利用者側の過失や知識の不足などを利用した攻撃も存在することから、システム側のみの対応では防御が不十分となることもあり、対策を困難にしている。
- 企画管理者は、具体的に、医療機関等や企業、行政機関等でどのような被害が生じているのか等を含めたサイバーセキュリティ事案の実情を把握することが重要である。
- その上で、組織的な対応と技術的な対応の両面から担当者と協議し、対策を整理する必要がある。
- 攻撃を受ける前の通常時における対応、攻撃を受けた場合の非常時としての対応、被害からの復旧・復帰などのフェーズの対応策をサイバーセキュリティ対応計画等の形で整理し、経営層の承認を得ること。
- 対応計画の具体的な内容の検討に際しては、経済産業省及び独立行政法人情報処理推進機構において策定している「サイバーセキュリティ経営ガイドライン」などが参考となる。

１２．２　サイバーセキュリティ対応計画の実践

- サイバーセキュリティ対応計画には、通常時と攻撃を受けた際の非常時における対策のいずれをも含んだものとする必要がある。通常時に適切な対策を実施することで、攻撃に備えるとともに、非常時の対応計画に盛り込んだ対策が想定通りに機能するかどうかをあらかじめ確認・検証することが重要である。企画管理者は、担当者と協働して、定期的に非常時を想定した訓練や機能テストなどを行うこと。また、訓練の結果得られた課題等については、サイバーセキュリティ対応計画等に反映することが求められる。
- 情報機器等の脆弱性や利用者の過失等が起点となって被害が生じている事象もみられている。通常時における情報収集や点検、未然防止策を検討するためのシステム関連事業者も含めた協働体制づくりが重要である。
- サイバー攻撃は日々巧妙化、多様化、高度化することから、サイバーセキュリティ対応計画等については、少なくとも年１回以上の頻度で見直しを図ること。

１２．３　サイバー攻撃被害時の対応

- サイバー攻撃を受けた際には、医療機関等独自の対応では対処しきれない事案も想定される。所管官庁への迅速な連絡や情報共有を行うことができるよう、通常時から連絡先や連絡手順、連絡体制を整備しておくこと。被害の拡大を防ぐために、早急に状況を厚生労働省、都道府県警察、その他所管官庁等に報告することを含めること。
- 非常時は、医療機関等内の職員や契約事業者だけでなく、一時的に医療情報システムに接続する関係者に対しても、速やかに情報共有が可能な体制を講じることも重要である。

１３．医療情報システムの利用者に関する認証等及び権限

【遵守事項】

① リスク評価に基づいて、医療情報システムにおける利用者の認証及びアクセス権限等に関する規程を整備し、管理すること。

② 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、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。

③ 医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者の ID 等を付与する等の必要な手順を作成するよう指示すること。

④ 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内の権限規程に応じて管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。

⑤ 医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じて ID やアクセス権限を付与すること。この際、管理者権限の付与については細心の注意を払って、最小限の対象者にのみ付与すること（例えば、OS の管理者権限がなければ稼働しないシステムを利用している場合は、次期システム改修時に必ず管理者権限がなくとも稼働するシステムを選定すること）。その具体的な手順については、担当者に作成を指示すること。

⑥ 医療情報システム等の管理権限や ID の安全管理を行うこと。管理権限の種類とその ID、利用が認められている者等を管理して一覧化し、必要に応じて認証に関する情報の変更等を指示すること。

⑦ 医療情報システムで利用する ID 等についての棚卸を定期的に行い、不要なものは削除すること。棚卸については、担当者に具体的な手順の策定を指示すること。また、棚卸結果を経営層に報告し、承認を得ること。

⑧ 電子カルテにおける記録の確定に関して、以下の事項を規程等に含めること。

- 入力者及び確定者の識別・認証
- 記録の確定手順、識別情報の記録の保存
- 更新履歴の保存
- 代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者

１３．１　医療情報システムに共通する利用者に関する認証等及び権限

１３．１．１　医療情報システムの利用者

- 利用者認証に関するルールを策定する際は、企画管理者はまず想定される利用者について整理する必要がある。
- 利用者としては、医療情報システムを業務等で利用する医療機関等の内部の職員や、自身の情報を参照する患者等の医療機関等の外部関係者が想定される。
- そのほか、利用者に付与される ID としては、医療情報システムの管理権限を有する ID や、ソフトウェア、システムに接続する情報機器等において便宜的に利用する ID なども想定される。
- 企画管理者は、担当者と協議して、利用者の種類などを整理し、その利用目的に応じて ID の運用規則等を定めること。

１３．１．２　医療情報システムの利用者の登録と認証

- 適切な情報セキュリティを確保するため、医療情報システムの利用に必要な ID を登録する必要がある。医療情報システムでは機微な情報を取り扱うため、利用者の登録や認証をする際の本人確認の方法については、厳格な信頼性が要求される。
- 利用者登録の際には、高い強度の身元確認を行うことが必要であり、対面又はこれに準じた形で確認することが求められる[5]。医療機関等では、例えば人事名簿において職員登録をするなどのプロセスを経ることから、職員登録の内容と整合性が取れる形で利用者登録を行う必要がある。職員が退職する場合なども、削除状況に応じて、医療情報システムの利用者登録からも削除すること。
- 登録された ID を利用する際の当人認証についても、厳格な認証方法が求められており、二要素認証やこれに準じた方法によること等を要する。企画管理者は、身元確認と当人認証の方法を、アクセス管理に関する規程に含めるとともに、担当者に対して、これに対応した措置を講じることを指示する必要がある。

１３．１．３　医療情報システムの利用者の権限設定

- 医療情報システムでは、利用者に応じてアクセスできる情報の範囲や、作業の内容（参照のみ、作成権限あり、更新権限あり等）に関する権限が付与される。医療機関等の人事で定めた権限規程や、医療従事者の資格などに応じて適切な権限を設定すること。
- システム上は利用権限が付与されていても、医療機関等内部のルール等により、利用範囲が制限されることがある。このような場合には、システムの利用ルールについて規程等として文書化し、権限の範囲を明確にすること。

１３．２　電子カルテにおける記録の確定

- 施行通知では、電子カルテ記録に関して、記録の確定、更新履歴、代行入力などに関する利用者の識別や権限等の機能を備えることを求めている。
- 企画管理者は、運用管理規程等にこれらの内容を含めるほか、担当者に対して、規程等に定めた内容に対応する措置をシステムに反映するよう指示し、管理すること。

---

[5]「Digital Identity Guidelines」（NIST SP800-63-4)では、身元確認は IAL（Identity Assurance Level）の強度として整理され、個人の安全への影響に鑑みると、IAL：Level 3 が望ましいとされるが、一定程度の情報セキュリティレベルが担保された環境下で管理されている医療機関等であれば、IAL：Level 2 以上が望ましいとされる。レベル区分については「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン」（令和 7 年 9 月 30 日デジタル社会推進会議幹事会決定）のレベル区分を参照。

表１３－１　当人認証の保証レベルと考え方

当人認証保証レベル	保証レベルの位置づけ
Level 1	当人認証に関するリスクの影響度が「高位」となる対象手続が 該当する保証レベル。多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を全ての利用者が利用することを必須とすることで、厳格な 耐性を確保する。
Level 2	当人認証に関するリスクの影響度が「中位」となる対象手続が 該当する保証レベル。多要素認証を必須とし、さらにフィッシング耐性をもつ認証手法を希望する利用者が選択的に利用できるようにすることで、 標準的な耐性を確保する。
Level 3	当人認証に関するリスクの影響度が「低位」となる対象手続が該当する保証レベル。単要素認証により、簡易的な耐性を確保する。

１４．法令で定められた記名・押印のための電子署名

【遵守事項】

① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。

1. 以下の電子証明書を用いて電子署名を施すこと

(1)「電子署名及び認証業務に関する法律」（平成 12 年法律第 102 号）第２条第１項に規定する電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。

(2) 法令で医師等の国家資格を有する者による作成が求められている文書については、以下の（a）～（c）のいずれかにより、国家資格の確認が電子的に検証可能な電子証明書を用いた電子署名等を用いること。

(a) 厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす HPKI（Healthcare Public Key Infrastructure）認証局の発行する電子証明書を用いて電子署名を施すこと。

HPKI 認証局が発行する電子証明書内には、医師等の保健医療福祉に係る資格情報が含まれている。したがって、HPKI 認証局の発行する電子証明書を使用して電子署名をすると、電子的な本人確認に加え、医師等の国家資格を電子的に確認することが可能である。

ただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名を正確に検証できる必要がある。

(b) 認定認証事業者（電子署名法第２条第３項に定める特定認証業務を行う者として主務大臣の認定を受けた者をいう。以下同じ。）又は認証事業者（電子署名法第２条第２項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、国家資格の確認を電子的に検証でき、電子署名を正確に検証できる必要がある。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14．法令で定められた記名・押印のための電子署名」において同じ。）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様）。

・ 事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、 オンラインの場合、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）第３条第１項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ（いずれも本項と同等の電子署名（資格確認を除く）を施すこと）により確認を行うこと。郵送の場合は、身分証明書のコピー（署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること））、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用すること。

※ 身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか１種類により、又はその他の身分証明書であれば２種類以上により行うこ

と。

・ 事業者による利用者の国家資格保有の確認は、

(イ) 利用者が HPKI 認証局の発行する署名用証明書を用いた電子署名を事業者へ提供することによりオンラインで行う方法

(ロ) 利用者が官公庁の発行した国家資格を証明する書類（以下「国家資格免許証等」という。）の原本又はコピー等（紙媒体の場合は、国家資格免許証等のコピーに署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること）があること。電子媒体の場合は、本項と同等の電子署名（資格確認を除く）をスキャンしたデータに施すこと。）を事業者へ持参、郵送又は送信する方法

(ハ) 利用者が電子署名による確認方法以外の電子的に国家資格等情報と連携して提示できる仕組みを用いて事業者へ提示する方法

(ニ) 利用者の所属又は運営する医療機関等が利用者の国家資格保有の事実の立証を事業者へ行う方法

のいずれかによって利用者の登録時において確認すること（電子署名を行う都度、事業者による医師等の国家資格保有の確認を求めるものではない）。

なお、(イ)～(ハ)の場合、事業者は、資格確認に用いた国家資格免許証等のコピーや証明書等について、保存年限を定めて保存しておくこと。(ニ)の場合、次に掲げる事項が適切に行われていることについて事業者が確認を行うこと。

– 医療機関等の管理者が、自組織の実在性を事業者に対して立証すること。

– 医療機関等の管理者が国家資格保有の確認を行った者の「氏名、生年月日、性別、住所」（以下「基本４情報」という。）を事業者へ提出すること（これによって、利用者が実在性、本人性及び利用者個人の申請意思を立証した際に、国家資格保有の立証もなされたものとみなすこととする。）。

– 医療機関等による国家資格保有の立証に当たって、医療機関等が責任の主体としての説明責任を果たすため、資格確認を行った実施記録の作成を行うこと。また、資格確認を実施した国家資格免許証等のコピーや利用者の基本４情報を提出した書類のコピー等について保存年限を定めて保存し、医療機関等の内部の独立した監査部門による定期的な監査を行うこと。

・ 事業者が、上記の事項について、適切な外部からの評価を受けていること。

※ (イ)～(ニ)のいずれかによって資格確認を行った後、利用可能となった当該電子署名を利用者が他の事業者に提供した場合、提供を受けた事業者が別途資格の確認を行う必要はない。なお、この場合であっても以下の事項を行うこと。

- 適切な外部からの評価を受けること。
- 資格確認に用いた証明書等について、保存年限を定めて保存しておくこと。

(c) 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく国家資格が検証時に電子的に確認できること、当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証できることが必要である。

2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること

(1) タイムスタンプは、第三者による検証を可能にするため、時刻認証業務の認定に関する規程（令和 3 年総務省告示第 146 号）に基づき認定された事業者（認定事業者）が提供するものを使用すること。

(2) 法定保存期間中、タイムスタンプの有効性を維持するための対策を実施すること。
(3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省庁の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。
(4) タイムスタンプを付与する時点で有効な電子証明書を用いること。

② 電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。

１４．１　法令で定められた記名・押印のための電子署名の要件

- 平成 12 年 5 月に電子署名法が成立した。また、e-文書法省令において指定された医療関係文書においては、電子署名法第 2 条第 1 項に規定する電子署名によって、記名・押印に代わり電子署名を施すことで、作成・保存が可能となった。
- 近年、ローカル署名に加え、リモート署名や、クラウド技術を活用した立会人型電子署名を用いたサービスが登場している。電子署名法第 2 条第 1 項の要件を満たすものは、電子署名法における電子署名に該当する。
- 利用者と認証局あるいは電子署名サービス提供事業者の間で行われる本人確認（利用者の実在性、本人性、利用者個人の申請意思の確認及び当人認証）等のレベルや電子署名サービス提供事業者内部で行われるプロセスのセキュリティレベルは様々である。各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の性質や、利用者間で必要とする本人確認レベルに応じて、適切なサービスを選択すること。
- 立会人型電子署名の選択に当たっては、総務省・法務省・経済産業省から令和 2 年 7 月 17 日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法 2 条 1 項に関する Q&A）」も参照すること。

表１４－１　電子署名の種類

署名方式	概要
ローカル署名	IC カードやパソコン等の記録媒体に格納された、本人が管理する鍵で署名するもの
リモート署名	クラウド上のサーバに利用者※自身の署名鍵を格納し、利用者が当該サーバにリモートでログインした上で行う電子署名 ※電子署名法第 2 条第 2 項における自らが行う電子署名についてその業務を利用する者
立会人型電子署名	利用者の指示に基づき電子署名サービス提供事業者※自身の署名鍵による暗号化等を行う電子署名 ※電子署名法に規定する電子署名に関するサービスを提供する者のうち、立会人型電子署名に関するサービスを行う者

- また、施行通知に示される電磁的記録の保存等が可能な文書は、正当な権限で作成された記録であり、虚偽入力、書換え、消去及び混同が防止され、かつ、第三者から見て作成の責任の所在が明確であることが求められる。電子署名法第 3 条では、電子文書（デジタル情報）について、本人すなわち当該電子文書の作成名義人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われていると認められる場合には、当該作成名義人が当該電子文書を作成したことが推定されることとしている。
- 医療分野において電子署名に係る争訟が生じた場合に備え、立証責任を軽減する観点から、下記のような特徴を備えた措置の利用を検討すること。
  - 十分な暗号強度を有し、他人が容易に同一の鍵を作成できないものであること
  - 電子署名が本人の意思に基づき行われたことを確認できること
- 立会人型電子署名の選択に当たっては、総務省・法務省・経済産業省から令和２年９月４日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A（電子署名法 3 条に関する Q&A）」も参照すること。
- 処方箋のように、医師等の有資格者に作成が求められる文書が医師法等の法令で定められている場合がある。これらの多くには記名・押印が求められており、記名・押印は本人の証明だけでなく、有資格者としての当該行為に対する責務も示す。当該資格者による行為であることの証明を電子的に担保する考え方を「Nonrepudiation（否認防止）」と呼び、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等により担保可能となる。
- また、特に医療に係る文書では一定期間、信頼性を持って署名を検証可能である必要がある。電子署名は紙媒体への署名や記名・押印と異なり、電子署名法第２条第１項の要件該当性は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり、失効させた場合は検証不能となるという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。
- このような点を踏まえ、電子証明書を利用する場合には、有効期間や失効の有無、暗号アルゴリズムの脆弱化の影響を受けることなく、法定保存期間等の一定期間にわたり電子署名の検証を継続できることが求められる。また、対象文書は行政による監査等の対象となるため、付与された電子署名は行政機関等においても検証可能でなければならない。
- なお、デジタルタイムスタンプ技術を用いた長期署名方式の標準化が進んでおり、長期的な署名検証の継続を可能とする方式が ISO 規格として制定されている[6]。
- 医療情報の保存期間は、生物由来製剤に係る文書として 20 年以上の長期にわたるものも存在する。システム更新や検証システムの互換性等の観点からも、例えば、前述の標準技術を用い、必要な期間、電子署名の検証を継続して検証可能とすることが想定される。

[6] ISO14533-1：2022CMS 利用電子署名(CAdES)の長期署名プロファイル、ISO14533-2:2021XML 署名利用電子署名(XAdES)の長期署名プロファイル、ISO14533-3:2017PDF 長期署名プロファイル(PAdES)、ISO14533-4:2019proofofexistenceobjects

１４．２　電子署名を含む文書全体に付与するタイムスタンプの要件

- タイムスタンプは、タイムスタンプに刻印されている時刻以前にその文書が存在し（存在証明）、その時刻以降文書が改ざんされていないことを証明する（非改ざん証明）。
- 法令で保存が義務付けられた文書の場合においては、第三者による電子署名の検証を可能とするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者が提供するタイムスタンプを使用すること。また、法定保存期間中、タイムスタンプの有効性を継続できるようにするために必要な対策を実施すること。
- なお、法令保存期間等がない文書についても、「時刻認証業務の認定に関する規程」（令和３年総務省告示第１４６号）の要件を満たす時刻認証事業者が発行する認定タイムスタンプまたはこれと同等のサービスを使用することも可能である。タイムスタンプの利用や長期保存に関しては、今後も、関係府省庁の通知や指針、標準技術、関係ガイドラインに留意しながら適切な対策を実施すること。
- 電子証明書は、タイムスタンプを付与する時点で有効なものを用いて電子署名を行わなければならない。本来法定保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明される。具体的には、電子証明書が有効な期間内に、電子署名の検証に必要な情報（関連する電子証明書や失効情報等）を収集し、署名対象文書及び署名値と併せてタイムスタンプを付与する等の対策が求められる。

１５．技術的な安全管理対策の管理

【遵守事項】

① 物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所の選定について、リスク評価を踏まえて、担当者と検討すること。またその結果を経営層に報告の上、承認を得ること。医療情報システムに関する整備計画等を策定している場合には、これと整合性をとって選定すること。

② 個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定すること。

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、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。

④ 医療情報システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規程に定め、その運用を関係者全員に周知徹底すること。

⑤ 記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。

⑥ システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（マルウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。

⑦ 医療機関等において利用するネットワークは、リスク評価を実施したうえで選定し、経営層の承認を得ること。なお、医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を企画管理者等が実施した場合には、その内容を確認の上、経営層に報告し、承認を得ること。

⑧ 保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約や SLA 等により管理項目（OS やソフトウェアのアップデート、パッチ適用に関する役割分担含む）について取決めを行うこと。

⑨ 医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規程等に含めること。また、やむを得ず医療情報を用いる場合には、漏えい等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。

⑩ 医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。

⑪ 情報機器、ソフトウェアの品質管理に関する対応を運用管理規程で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。

⑫ システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。

⑬ 医療情報システムが法令等で求められている要件を満たすよう適切に管理すること。特に施行通知、外部保存通知などで求める要件を満たしていることを確認し、調達においては当該要件を満たすシステムを選定すること。具体的な確認項目や、医療情報システムにおける実装内容等については、担当者に確認の上、必要な検討を行うよう指示すること。

⑭ ①～⑬において、担当者が整備した対策について、関連規程等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、経営層に報告して承認を得ること。

１５．１　技術的な対応の管理

- 企画管理者は、通常時から経営層に代わって医療情報システムの様々な運用管理を担う。
- 一方で、医療情報システムにおける技術的対応については、専門的な知見が必要であり、これを有する担当者に委ねることが想定される。この場合、技術的な対応のうち、基本的なルールを規程や規則などで定め、具体的な運用管理は担当者に権限移譲することとなる。また、運用管理は事業者に委託することも想定される。特に、アップデートについては可能な限り、事業者の保守範囲に含めることが望ましい。保守範囲とならない場合は、医療機関等の責任でアップデートが必要となる。
- この場合、企画管理者は、技術的な対応のうち特に重要な部分について指示するほか、通常時における運用、事業者からの情報収集等の実施を担当者に指示すること。また、実施状況の報告を受けて状況を把握すること。また、医療情報システム全般の運用状況について、経営層に報告し、承認を得ながら管理すること。

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① 医療情報を含む文書等の紙媒体をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規程等に定めること。

② スキャナにより読み取った電子情報と元の文書等から得られる情報が同等であることを担保する情報作成管理者を配置すること。

③ 医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りに係る責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規程等に定めること。なお、電子署名については「14．法令で定められた記名・押印のための電子署名」を参照すること。

④ 情報作成管理者に対して、スキャナによる読み取り作業が運用管理規程に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。

⑤ 診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うことを運用管理規程等に定めること。

⑥ 過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。

・ 対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。

・ 必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。

– 運用管理規程の作成と妥当性の評価方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を確保した委員会等で行うこと（倫理委員会を用いることも可））

– 作業責任者

– 患者等への周知の手段と異議の申立てに対する対応方法

– 相互監視を含む実施体制

– 実施記録の作成と記録項目（次項の監査に耐え得る記録を作成すること）

– 事後の監査人と監査項目

– スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法

・ 事後の監査は、システム監査技術者や Certified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ外部監査人によって実施すること。

⑦ 企画管理者は、紙の調剤済み処方箋をスキャナ等で電子化して保存する場合、以下の措置を講じること。

・ 紙の調剤済み処方箋の電子化のタイミングに応じて、⑤又は⑥の措置を講じること。

・ 「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。

⑧ スキャナ等で電子化を行った後も、紙等の媒体をそのまま保存する場合、元の紙媒体やフィルムの安全管理を行うこと。

１６．１ 診療録等をスキャナ等により電子化して保存する場合の共通要件

➢ 「診療録等をスキャナ等により電子化して保存する場合」とは、診療録等の「施行通知」に示される電磁的記録による保存等が可能な文書を、スキャナ等により電子化して保存する場合を指す。具体的には、

・ 電子カルテ等により、診療に用いる文書の大部分が電子化されている一方、他院から紙やフィルムでの診療情報提供書等の受け入れが必要な場合
・ 電子カルテ等の運用を開始し、電子保存を施行したが、施行前の診療録等が紙やフィルムで残り、一貫した運用ができない場合
・ 電子化の対象が、オーダエントリシステムや医事システムのみの運用であって、紙等の保管に窮している場合

が挙げられる。

- 企画管理者は、このような場合の手順等や情報機器等の条件について、業務に支障が生じることのないよう整理し、運用管理規程等に定めること。

１６．２　診療等の都度スキャナ等により電子化して保存する場合

- 診療に用いる文書の大部分が電子化されている一方、他院から紙やフィルムでの診療情報提供書等の受け入れが必要な場合、診療等の都度スキャナ等による電子化が実施されることも想定される。
- 企画管理者は、スキャナ等により電子化して保存する場合の共通要件や、改ざん動機が生じないと考えられる時間内に適切に電子化を行うことなどを、運用管理規程等に定めること。

１６．３　過去に蓄積された紙媒体等をスキャナ等により電子化して保存する場合

- 電子カルテ等の運用を開始した後も、過去の診療録等が紙又はフィルム媒体で残存し、一貫した記録管理ができない状況が生じ得る。この場合は、診療の都度電子化して保存する場合と異なり、既存の原本を後日電子化することになるため、記録の真正性に疑義が生じ得る。説明責任を担保する観点から相応の対策が必要となり、スキャナ等により電子化して保存する場合の共通要件に加え、厳格な監査の実施が求められる。
- 企画管理者は、このような説明責任への対応の観点から、本項の遵守事項①～④に加えて、遵守事項⑥に記載する措置を講じること。

１６．４　紙の調剤済み処方箋をスキャナ等により電子化して保存する場合

- 紙の調剤済み処方箋の電子化とは、記名押印又は署名を行い調剤済みとした処方箋を電子化することをいう。
- 紙の処方箋を薬局で受け取った場合、調剤済みとなるまでは電子化したものを原本としてはならない（誤った運用例：薬局で紙の処方箋を受け付けた時点で電子化し、それを原本として調剤を行い、薬剤師の電子署名をもって調剤済みとする等）。
- 調剤終了時までは特段の問題なく経過した処方箋であっても、その後内容の修正が発生することがある（例：記載事項を確認したものの修正を忘れた場合等）。
- 企画管理者は、診療録等をスキャナ等により電子化して保存する場合の共通要件に加えて、一旦電子化した紙の調剤済み処方箋の修正等、実際の運用を踏まえて、遵守事項⑦に記載のとおり、対応を行うこと。

１６．５　運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合

- スキャナ等で電子化した後も、紙等の媒体の保存は継続して行う場合、電子化した情報には、保存義務等の要件は課せられない。しかし、個人情報保護上の配慮は同等に行う必要がある。
- またスキャナ等による電子化の際に医療に関する業務等に差し支えない精度の確保も必要である。
- 企画管理者は、このような観点から、遵守事項⑧に記載する措置を講じること。

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

経営管理編

目次

【はじめに】

＜経営管理編が想定する読者＞

経営管理編は、主に医療機関等において組織の経営方針を策定し、意思決定を担う経営層に認識していただく考え方や関連法制度等を示している。具体的には、経営層として遵守又は判断すべき事項並びに企画管理やシステム運営の担当部署及び担当者に対して指示及び管理すべき事項並びにその考え方を示している。

＜医療機関等における情報セキュリティ＞

医療情報システムの利用が進んでいる中、サイバー攻撃の脅威も近年増大している。その攻撃手法は日々高度化、巧妙化しており、医療機関等の経営や地域医療の安全性に直接影響が生じる事案も生じている。また、医療 DX の進展に伴い、直接的にサイバー攻撃を受けた医療機関等を踏み台にし、他の医療機関等にも被害が拡大するなど、重大な影響を及ぼす危険性も生じている。

情報セキュリティインシデントが起きた場合、医療の提供が停止し、患者の生命・身体に影響を与える可能性がある。安全管理上の対応が不十分であれば、行政処分の対象となるリスクや、民事上の賠償責任を負うリスクもあるうえ、医療機関等の公共社会インフラとしての役割からの謝罪が必要となった例も複数ある。さらには、インシデントからの復旧に多大な費用を要するなど、経営に大きな影響を及ぼすことも想定される。

安全管理対策は、事業継続性の確保やサイバー攻撃に対する防衛力の向上にとどまるものではなく、医療情報を高度に活用して、質の高い医療の提供や個人の健康の維持増進の前提にもなる。医療機関等の経営層においては、安全管理対策の実施を「コスト」と捉えるのではなく、質の高い医療の提供等に不可欠な「投資」と捉え、その実施に必要となる資源（予算・人材等）の確保に努めることも重要である。

本ガイドラインの「経営管理編」では、このような医療機関等の経営管理の観点から求められる医療情報システムの安全管理についての遵守事項及びその考え方を示す。

医療機関等の経営層においては、本編を閲読し、理解した上で、必要な措置を講じることが求められる。

１．安全管理に関する責任･責務

【遵守事項】

① 医療情報システムの安全管理に関係する法令等を遵守すること。

② 医療機関等で業務に従事する職員や関係する医療情報システム・サービス事業者（以下「システム関連事業者」という。）等に対して、医療情報システムに関係する法令等を遵守させること。

③ 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。

④ 患者等への説明を適切に行うための窓口の設置等の対策を行うこと。

⑤ 医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。

⑥ 定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。

⑦ 医療情報システムに関する安全管理を適切に維持するための計画を策定すること。

⑧ 医療情報の安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。

⑨ 情報セキュリティインシデントが生じた場合、原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。

⑩ 情報セキュリティインシデントが生じた場合、可能な限り医療継続を図ること。

⑪ 情報セキュリティインシデントが生じた場合、医療機関等内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。

⑫ 情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。

⑬ ⑨、⑩、⑪、⑫の対応を可能とするため、通常時から非常時を想定した体制や措置を講じておくこと。

⑭ 医療情報システムの安全管理について、システム関連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。

⑮ 業務等を委託する場合には、委託する内容、役割分担等の責任分界を明確にすること。また、認識の齟齬が生じないよう、書面等により内容、責任分界を可視化し、保管すること。

⑯ 医療情報を第三者提供する場合、法令等を遵守し、手続きの記録等を適切に管理する体制を整備すること。

⑰ 医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任範囲をあらかじめ明確にすること。また、認識の齟齬が生じないよう、書面等により責任範囲を可視化し、適切に管理すること。

１．１　安全管理に関する法令の遵守

１．１．１　医療情報システムに対する医療機関等の責任

- 医療情報は患者等に関する機微な個人情報であることから、患者等との関係において、医療情報を取り扱う医療情報システムを適正に管理する責任がある。
- 医療は重要な社会インフラであり、医療サービスの提供の継続性を確保することは社会的な責務と考えられる。この点からも医療サービスの提供を支える医療情報システムを適正に管理する責任がある。

１．１．２　医療機関等における法令上の責任

- 医療機関等における医療情報の取扱いに関する責任には、法律の観点から見ると、行政法上・刑事上・民事上の責任などがある。
- 医療機関等における医療情報システムの安全管理に関する責任は、医療機関等の運営上の責任であることから、

業法責任（行政法上の責任）が中心となる。また、医療機関等で業務に従事する職員や関係するシステム関連事業者等による秘密漏えいや医療情報の漏えい等による損害賠償を防ぐ責任もある。

- なお、サイバー攻撃の脅威が近年増大していることに鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項において、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じなければならないとしている。
- 同様に、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項において、薬局の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じなければならないとしている。

１．２　医療機関等における責任

- 医療情報システムの安全管理に関する責任には、通常時において対応すべき責任と、非常時において対応すべき責任がある。
- 医療機関等が直接行う業務における責任のほか、医療機関等が業務の委託を行った場合の委託先事業者の業務における責任や、医療情報を第三者に提供する際に生じる責任なども存在する。
- これらの責任についての概要を以下の表１－１に示す。

表１－１　医療機関等における責任

全ての医療機関等における責任	通常時における責任	管理方法・体制等に関する説明責任
		管理及び監査を実施する責任
		定期的に見直し、必要な改善を行う責任
	非常時における責任	情報セキュリティインシデントの原因・影響等に関する説明責任
		再発防止策等の善後策を講じる責任
第三者に業務を委託する場合		適切な事業者を選定する責任 受託事業者の過失等に対する管理責任
第三者に医療情報を提供する場合		第三者提供が適切に実施されたかに対する責任

１．２．１　通常時における責任

＜管理方法・体制等に関する説明責任＞

- 通常時における説明責任とは、医療情報システムの機能や運用について、必要に応じて患者等に説明する責任である。
- 説明責任を果たすためには、医療情報システムの機能仕様や運用手順等を文書化しておく必要がある。また通常時の運用に関する仕様や手順が医療機関等の要求仕様や運用方針に則って機能しているか、定期的に監査を行い、その結果についても文書化することが求められる。
- 監査の結果、問題や課題が覚知された場合は、真摯に対応して、その記録を文書化すること。また、第三者が対応の妥当性等を検証することが可能な状態にすること。
- 説明窓口を確保するなど、患者等が医療情報システムについて説明を求めることが可能な体制を整えること。

＜管理及び監査を実施する責任＞

- 管理責任とは、医療情報システムの管理や運用を医療機関等が適切に行う責任であり、システムの形態や構成

に関わらず、当該システムを利用する限りにおいて医療機関等で負う責任である。

- 個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 23 条において、「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定されており、医療機関等はこの規定に従い、必要な措置を講ずる必要がある。
- 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、監督する必要がある。

＜定期的な見直し、必要な改善を行う責任＞

- 情報システムの安全管理に関する技術や手法は日進月歩であり、安全管理体制が陳腐化するおそれがあるため、安全管理の仕組みの改善を常に心がけ、評価・検討を定期的に行う責任がある。
- 医療情報システムの管理に関する状況を定期的に検証し、問題や課題を洗い出し、必要な対策を講じて、管理方法や体制を改善することが求められる。
- 医療機関等のみで最新の技術動向を随時把握することが難しい場合は、システム関連事業者に技術動向や管理手法等に関する情報提供を依頼することで、安全管理の改善に必要な情報を収集することも想定される。

１．２．２　非常時における責任

＜情報セキュリティインシデントの原因・影響等に関する説明責任＞

- 非常時における説明責任とは、医療情報システムの安全管理上望ましくない事象、例えば、情報漏えいや情報システム障害等の情報セキュリティインシデントが生じた場合に、事態の発生を公表し、その原因と影響、対応方針や対処方法等を説明する責任である。
- 患者等への説明に加え、所管官庁への報告や公表なども必要である。

＜再発防止策等の善後策を講ずる責任＞

- 情報セキュリティインシデントが生じた場合は、医療情報システムを用いた診療の継続に向けた業務復旧等を図るために、善後策を講じる必要がある。善後策を講ずる責任には、「原因を究明する責任」と「再発防止策を講ずる責任」が含まれる。
- 「原因を究明する責任」とは、情報セキュリティインシデントの発生原因を明らかにする責任である。原因が不明な状態では、再発の可能性が解消されない。このため、可及的速やかに原因を究明すること。
- 「再発防止策を講ずる責任」とは、究明された発生原因に対して、同様の事象が再び発生しないよう必要な防止策を講じる責任である。医療機関等のみでは具体的な再発防止策の検討が困難な場合もあるため、適宜システム関連事業者や外部有識者などと連携して進めること。

１．３　委託における責任

１．３．１　委託（第三者委託）における責任

- 医療情報システムの安全管理について、システム関連事業者に委託する場合は、医療機関等には委託先事業者を監督する責任がある。個人情報保護法第 25 条では、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合[1]は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受け

[1] 対象事業者がクラウドサービスを提供する事業者であって、当該事業者が個人データを取り扱わないこととなっている場合（契約条項によって当該事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等）には、医療機関等は個人データを「提供」したことにならず（「個人情報の保護に関する法律についてのガイドライン」に関する Q&A A7-53 参照）、個人情報保護法 25 条に基づきクラウドサービス事業者を監督する義務はない。一方で、医療機関等は、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。

た者に対する必要かつ適切な監督を行わなければならない。」と規定されており、具体的内容については、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」の「Ⅳ 医療・介護関係事業者の義務等 7．安全管理措置、従業者の監督及び委託先の監督（法第 23 条～第 25 条）」において示されている。

- 委託先事業者における医療情報システムの管理も、医療機関等の管理責任に含まれる。
- 委託先事業者の過失による情報セキュリティインシデントについても医療機関等が責任を免れることはできず、医療機関等が患者等に対する責任を負うため、適切なシステム関連事業者の選定が求められる。一方で、情報セキュリティインシデントが生じた際、具体的な運用や技術的要因などの分析や対応は、契約内容に基づき、委託先事業者が実施することになる。

1．3．2 委託（第三者委託）における責任分界

- 契約等の取決めを踏まえて業務等を委託する際には、以下の点に留意しながら、システム関連事業者と認識の齟齬等が生じないよう協議することが求められる。
  - 医療機関等が委託先事業者との間で締結する委託契約では、委託する内容や分担する役割を明確にし、その責任の所在を明確にした上で、契約書等に示す必要がある。特に複数のシステム関連事業者が関係する場合もあるため、医療機関等と各システム関連事業者における責任の内容を整理し、適切に管理すること。
  - 責任分界には、「法律上の責任の範囲を明確にする責任分界」「具体的な運用及び対応の範囲を明確にする責任分界」等が想定される。インシデント発生時における原因究明のための具体的運用及び対応範囲についても、法律上の責任の範囲を踏まえ、認識の齟齬等が生じないよう設定すること。

    法律上の責任範囲を示す一般的な契約書などでは、具体的な記載がなじまない場合があるため、具体的運用及び対応範囲については、企画管理者やシステム運用担当者のマニュアル等をシステム関連事業者と共有し、明確にするなどの方法が考えられる。
- 委託先事業者との責任分界については、「５．医療情報システム・サービス事業者との協働」も参照されたい。

1．4 第三者提供における責任

- 第三者提供とは、第三者が何らかの目的で医療情報を利用するために行われるものである。医療機関等が第三者提供を行う場合の対応については、個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に示されており、医療機関等は、安全に医療情報を提供する責任を負う。
- 提供された医療情報を受領した第三者は、当該情報を適切に管理する責任が生じる。なお、原則として適切な第三者提供がなされる限り、提供元の医療機関等は、提供先の当該情報の保護に関する責任を免れる。ただし、提供元の医療機関等において、第三者提供の元となった情報を保有する限り、引き続き提供元における当該情報に対する適切な管理責任を負う。
- 医療機関等側から医療情報を送信し、第三者側で受信するまでの医療情報の取扱いに関して、責任の範囲を明確にすること。具体的な責任の範囲については、例えば医療情報連携ネットワークへの情報提供や患者等の指示による提供など実際に第三者提供を行う業務やその目的により異なるため、事象に応じて整理を行う必要がある。

2．リスク評価を踏まえた管理

【遵守事項】

① 取り扱う医療情報に応じたリスク分析・評価を踏まえ、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。

② リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、ルール等について、企画、整備、管理を、企画管理者に指示すること。

③ 方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。

④ リスク評価を踏まえ、医療情報の重要性、医療の継続性、経営資源、対策の継続可能性等に鑑みて、リスク管理方針を決定すること。

⑤ リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。

⑥ リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMS を策定し、実施すること。

⑦ 医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。

2．1　医療情報システムにおけるリスク評価の実施

- 医療情報システムは機微性の高い個人情報を取り扱い、かつ、効率的かつ正確に医療を提供するためにも有用であるので、リスクを回避・低減するためには高度な水準の安全管理対策が求められる。
- リスク分析・評価は、医療機関等が医療情報システムを利用する上でのリスク管理の方針を決める基礎となるほか、医療機関等の特性や事情を加味して、実施可能な対策を選定するための資料にもなる。
- 医療情報システムに関する各リスクに対してどのようなリスク管理方針(リスクの回避・低減・移転・受容)を決定し、対策を講じるのかの判断を行う際には、
  - 医療の提供を継続するために、どの程度の経営資源を投入し、どのような対策を講じるか、
  - 選定したリスク管理方針に基づき、残存するリスクにどのような対策を講じるか（例えば、稼働率を 100%に近づけることが困難なシステムの場合には、一部紙媒体等での代替方策で診療等を継続できるようにする等）

  を判断すること。
- リスク管理方針を検討するに際し、情報セキュリティの３要素である「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」のバランスを考慮することも重要である。
- 企画管理者に、リスク分析を踏まえてリスク管理が必要な場面の整理や、対策を進める体制やルール等の整備、管理を実施させること。
- 企画管理者に対して、リスク管理方針やリスク評価を踏まえ、具体的なシステム面からの最適なリスク管理措置を検討、実装、運用させること。このとき、例えば直接の作業をシステム運用担当者に実施させることを妨げるものではない。

２．２ リスク評価を踏まえた判断

２．２．１ リスク評価を踏まえたリスク管理

- リスク管理方針は、情報・データや情報システム等の情報資産に対するリスク評価の結果を踏まえ判断される。一般的には、リスク管理方針には、リスクの回避（リスク発生の根源となる事業や行為を取りやめる）、低減（リスクを低減するための対策を講じる）、移転（発生したリスクを、保険等により移転する）、受容（リスクが実際に生じることを想定した上での対応を検討する）が挙げられる。
- 医療継続の必要性を考慮すると、医療機関等において選択される主なリスク管理方針は「リスクの低減」になると考えられる。継続的にリスク評価、リスク管理を実施する必要がある。
- 医療機関の運営継続の観点から、リスク管理方針を策定する際には医療機関等の経営の視点、人事管理の視点等を考慮すること。
- リスク評価とリスク管理方針の策定は、医療機関等における情報セキュリティ対策に関する説明責任を果たすことにもつながる。

２．２．２ 情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の実践

- 医療機関等における PDCA（Plan-Do-Check-Act）サイクルの実施については、「良質な医療を提供する体制の確立を図るための医療法の一部を改正する法律の一部の施行について」（平成 19 年 3 月 30 日付け医政発第 0330010 号厚生労働省医政局長通知）において、医療の安全管理としてその重要性が示されている。情報セキュリティに関しても、医療の安全管理と同様の考えのもと、リスク管理方針を踏まえ、ISMS を策定して PDCA サイクルを実施することが有効であると考えられる。

２．２．３ リスク分析を踏まえた要求仕様適合性の管理

- リスク管理の実効性を維持・向上するために、リスク分析を踏まえた医療機関等の要求仕様に対する適合性の確認を行う必要がある。この確認において、医療機関等とシステム関連事業者との間で、医療情報及び医療情報システムに対するリスク管理への共通理解や共通認識を得る必要がある。
- リスク管理対策の詳細は企画管理者やシステム運用担当者が実施するが、経営層は医療機関等とシステム関連事業者との間でのリスク分析を踏まえたリスク管理や要求仕様適合性の確認が適切に実施されているかどうかを把握しておく必要がある。

3．安全管理全般（統制、設計、管理等）

【遵守事項】

① 統制の体系を理解し、情報セキュリティ対策に関する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。また、適切に統制が機能しているかを確認すること。

② 医療機関等の規模や組織構成、特性等を踏まえた統制の内容を検討すること。

③ 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及び企画管理者を設置すること。

④ 情報セキュリティ対策に関する統制は、医療機関等内の組織等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。

⑤ 情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。

⑥ 複数の部門（担当する業務毎に区分された組織）が存在する医療機関等においては、情報システム管理委員会等を設置し、定期的に調達情報を部門間で共有すること。その際、各部門に委員会に参加する担当者等を配置し、統制に実効性を持たせること。委員会等が設置されない場合も、情報システムの導入や変更に当たっては、経営層や医療情報システム安全管理責任者等の承認を必要とする仕組みを構築すること。

⑦ リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。

⑧ 情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な内容で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。

⑨ 整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者全てに対して定期的な教育・訓練を実施すること。

⑩ 医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。

⑪ 医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査又は医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。

⑫ 内部監査又は外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。

⑬ 情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP 等を整備すること。

⑭ 情報セキュリティインシデントにより、医療機関等内の医療情報システムの全部又は一部に影響が生じる場合に備え、適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示すること。また、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて、改善に向けた対応を指示すること。

⑮ 通常時に整備していた BCP が、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。

⑯ 企画管理者に対し、システム関連事業者又は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指示すること。

⑰ 通常時から医療情報システムに関係する脆弱性対策や EOS（End of Support：サポート終了）等に関する情報を収集し、迅速な対策が可能な体制を整えるよう、企画管理者やシステム運用担当者に指示するこ

と。

⑱ 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察、その他の所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。

⑲ 情報セキュリティインシデントが発生した場合に、厚生労働省等への報告のほかに、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。

3．1 統制

3．1．1 情報セキュリティ対策のための統制

- 医療情報システムの情報セキュリティ対策は、医療情報の適正な取扱いの確保や保護を図る観点から、医療機関等における重要な経営課題の一つである。情報セキュリティリスクに対する十分な対応を行うためには、具体的な情報セキュリティ対策の検討に加え、具体的な対策を講じるためのリスク対応計画の策定[2]、当該計画の内容を実現するために必要な規程類の整備、計画の内容の実施や進捗管理を行うために必要な組織体制の整備等による内部統制が適切に行われている必要がある。
- 上記計画の策定に当たっては、その具体化のための予算計画と併せて策定することが求められる。
- また、情報セキュリティ対策に関わる各組織（医療従事者等含む。）が適切に協働できるようにするために、具体的な業務内容や各業務を行う者の権限等を明確化した規程類の整備が求められる。
- 加えて、策定した計画を実現するために必要な組織統制が発揮されるよう、情報セキュリティに関する最高責任者や通常時・非常時の運用、対応する組織の構成、役割、職務権限等を明確にすること。
- 医療情報システムの運営や利用に際しては、様々なシステム関連事業者も関与することから、情報セキュリティ対策に関する統制の実効性の確保には、システム関連事業者との適切な協働体制等の整備が必要となる。（「５．医療情報システム・サービス事業者との協働」に、事業者の選定、管理及び事業者との間での責任分界管理に関する考え方を示す。）
- 情報セキュリティ対策に関する統制が適切に機能していることを確認することは、リスク管理方針や情報セキュリティ対策の見直しの観点からも重要である。そのため、情報セキュリティ対策に関する業務や措置の実行記録や行動証跡類を確保すること。

3．1．2 医療情報システムにおける統制上の留意点

- 情報セキュリティを確保するためには、組織全体として適切な統制がなされていることが重要であり、統制の実効性確保に当たっては、医療機関等の規模や組織構成、特性等に応じて留意すべき点が存在する。例えば、小規模の医療機関等では、担当する業務ごとに区分された組織（部署）がないことも多い。このような場合、過度に詳細な計画や規程類を策定しても、単に医療機関等の負担が増大し実効性が伴わないリスクがある。こうした規程類の策定に当たっては、医療機関等の組織や規模等に鑑みてリスク評価を行い、必要な内容を定めること。

---

[2] 計画には、下記が含まれることが望ましい。

- 目標とする将来像
- 実施事項
- 必要な資源
- 責任者
- 達成期限
- 結果の評価方法

また、情報セキュリティ対策に関する説明責任や管理責任を果たしながら業務を運用可能かも念頭に置きながら、実効性のある統制の内容を考える必要がある。実際の統制には、例えば下記の観点も含まれる。

- 患者等への情報セキュリティ対策に関する説明
- インシデントが生じた場合の関係者への報告
- システム関連事業者の管理を行うための資料の確保

- 統制の実効性を確保するために、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及び企画管理者を設置する必要がある。企画管理者が把握していない、シャドーIT（※）を通じた攻撃を防ぐためにも、セキュリティ委員会や、情報システム管理委員会等を設置することで定期的に調達情報を部門間で共有することが非常に重要である。経営層が企画管理者等の職務を兼務することは妨げられない。

  また、医療情報システム安全管理責任者は、経営層が担うことを想定しているが、企画管理者が医療情報システム安全管理責任者を兼務することも妨げない。

  ※ IT 部門の管理・許可を受けずに、独自に導入・利用している IT 機器やソフトウェア
- 医療機関等においては、人事権が各部局に帰属し、各部局でそれぞれ情報セキュリティ対策に係る組織編成を行っている場合がある。一方で、情報セキュリティ対策に関する統制は組織全体の問題であり、組織横断的に実現されることが求められる。情報セキュリティ対策に係る組織編成においては、人事権の帰属先を越えて、組織横断的な対応を要する。セキュリティ責任者を各部門に配置するなど、他部門と協力して医療機関等全体のガバナンスを効かせることも重要である。
- 情報セキュリティ対策に関する統制は、医療機関等に直接雇用されている職員だけではなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も対象に含み、行われる必要がある。

3．2 設計

3．2．1 情報セキュリティ方針を踏まえた情報セキュリティ対策の整備

- 情報セキュリティ方針は、リスク評価及びリスク管理方針に基づいて策定されるものであり、情報セキュリティ方針に基づき、医療機関等は医療情報システムに対する情報セキュリティ対策を実装する。
- 具体的な情報セキュリティ対策の検討や設計等は、企画管理者やシステム運用担当者が実施するが、経営層においても、対策の整備に関する理解は必要である。
- 具体的な情報セキュリティ対策の整備に当たっては、自医療機関等の実態を踏まえて、実際に運用可能な内容を整備すること。例えば、他の医療機関等で策定された運用管理規程等をそのまま自医療機関等に転用したとしても、当該機関の運用実態との不一致により、適切な運用がなされずかえって情報セキュリティリスクが増大するおそれがある。また、極端に厳格な内容の規程類を整備しても、実際の運用が困難である場合には、実質的には死文化して、有効な対策とはならない。
- また重要インフラとなる医療機関等においては、厚生労働省、医療機関等、サプライチェーンに関わる事業者等の関係主体を網羅的かつ具体的に記載し、セキュリティ対策に関するそれぞれの役割を明記することが求められる。その際、経営層の取組についても記載すること。
- 規程類の整備に際しては、参考資料を利用する場合でも、実態との整合性を図り、実際に運用可能かつ適切な内容を記載すること。

3．2．2 情報セキュリティ対策を踏まえた訓練・教育

- 規程類が適切に整備されている場合でも、その内容が医療情報システムの利用者をはじめ、関係者に認知されて

いなければ、当該規程類が遵守されていないことと同義である。このような場合、災害、サイバー攻撃等の非常事態が発生した際にも適切に実行できない可能性が高い。

- このため、整備した規程類及び情報セキュリティ対策については、関係者が認知し、遵守することができるよう、通常時から定期的に教育・訓練することが重要である。この教育・訓練については、医療情報システムに関係する者全員に対して行うことが重要である。
- 教育・訓練は、過度の負担にならない範囲で定期的に実施することが求められる。医療情報システムを取り巻く情報セキュリティに関する脅威が日々変化していることも踏まえると、その対策も随時更新されるものであるため、更新内容に応じた教育・訓練の実施が重要である。

3．3　安全管理対策の管理

3．3．1　安全管理状況の自己点検

- 情報セキュリティ対策の実効性を担保するためには、医療情報システムに関する安全管理対策が適切に実施されていることを確認し、その結果を把握・分析する必要がある。具体的には、規程類に基づく医療機関等内の運用状況のほか、規程類を踏まえた医療情報システム・サービスの機能の実装状況、運用状況、利用者における遵守状況等を内部で点検することが必要である。
- 当該点検は、医療機関等の各システム運用担当者が自ら行うことが想定される。この自己点検により、職員等が自らの役割に応じた適切な対策事項を実施しているか確認することができる。個々の情報セキュリティ対策の妥当性を確認することで、組織全体の対策水準の適切性の確認に資することも期待される。
- 経営層においては、企画管理者やシステム運用担当者に定期的に自己点検を実施するよう指示し、その点検結果を把握した上で、必要に応じて、改善に向けた対応を指示すること。

3．3．2　情報セキュリティ監査

- 医療機関等における主な説明責任の 1 つとして、医療情報システムの運用等が適切に行われていることを患者等に説明できるようにすることがあげられる。この説明責任を果たすために、医療情報システムが、情報セキュリティ方針に基づいて機能・運用されているかどうかを定期的に監査し、その結果を文書で整理することが必要である。
- 監査は、結果の信頼性という観点から、例えば、企画管理者や医療情報システムの運用担当者から独立した組織による内部監査や、外部機関による監査など、独立性を有する者により実施されることが望ましい。
- 監査の結果で課題や問題点が明らかになった場合は、経営層や情報セキュリティに関する最高責任者においては、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示し、必要な対応を講じさせるとともに、その対応結果を適切にフォローすることが重要である。

3．4　情報セキュリティインシデントへの対策と対応

3．4．1　事業継続計画（BCP：Business Continuity Plan）の整備と訓練

- 情報セキュリティインシデントが発生し、医療情報システムの可用性が損なわれるような事態に備えて、通常時から、非常時における医療情報システムの運用に関する対応を整理することが重要である。この際、業務継続の可否の判断基準や継続する業務内容の選定等に係る意思決定プロセスを検討した上で、BCP 等を整備すること。例えば、電子カルテシステムが止まっている間、紙運用で診療業務を継続するのか等、経営層はその対応内容について、BCP に応じて判断しなければならない。また、上記の非常時に至る主な原因としては、災害、サイバー攻撃、

システム障害等が想定され、原因の違いに応じた適切な対応をとることが求められる。企画管理編及びシステム運用編では、事象発生原因に応じた必要な対応例について記載しており、必要に応じて参照すること。

- 非常時の対応として重要なことは、稼働が損なわれた情報システムを非常時発生前の状態に適切に復旧できることである。そのためには情報システムやデータ等のバックアップを適切に確保・保管することが重要である。
- 情報セキュリティインシデントによって医療情報システムに影響が生じる場合に備え、適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について、情報システムの更新・改変時等、随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて、改善に向けた対応を指示する必要がある。
- 通常時に整備していたBCPが非常時において迅速かつ的確に実施できるよう、定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示する必要がある。また、情報セキュリティインシデントには情報漏えいなども含まれる。これらは医療情報システムの可用性に影響を及ぼすものではないが、医療情報は患者の生命、身体に大きな影響を及ぼす危険性があるほか、風評被害等により経営にも影響し得るため、情報漏えい等が起こった場合の対応についても、あらかじめ整理しておくこと。

3．4．2 情報共有・支援、情報収集

- 情報セキュリティインシデントの発生に備え、システム関連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、企画管理者に指示することが重要である。特にサイバー攻撃の場合、初動の対応が重要であることから、速やかな情報共有のための緊急連絡網（システム関連事業者、情報セキュリティ事業者や外部有識者等の連絡先）、医療機関等外を含む情報開示の通知先一覧を整備し、医療機関等において対応に従事するシステム運用担当者に共有しておくこと。また、システム関連事業者とは、このような対応も見据えた取決めを事前に交わすこと。
- 情報セキュリティインシデントの未然防止策として、通常時から情報機器等を含めた医療情報システムに関係する脆弱性対策や重要なアップデート（更新）、ならびに、EOS（End of Support：サポート終了）等に関する情報を収集し、迅速な対策が可能な体制を整えるよう、企画管理者やシステム運用担当者に指示すること。さらには、セキュリティ上のリスクを総合的に評価し、システム更新のための予算の確保、補完的対策の承認、または当該システム・機器の運用廃止等について、責任をもって経営判断を行うこと。

3．4．3 情報セキュリティインシデントへの対応体制

- 情報セキュリティインシデントが発生した場合、速やかに情報セキュリティの最高責任者への報告と関係者への連絡を行い、被害発生の事象特定、拡大防止等に努める必要がある。
- 具体的には、情報セキュリティインシデントの発生に対して、影響範囲や損害の特定、被害拡大防止を図るための初動対応、原因の究明、再発防止策の検討を速やかに実施するための CSIRT（Computer Security Incident Response Team（緊急対応体制））等を整備することが望ましい。特に一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、地域医療に与える影響の大きさを鑑みると、CSIRTの整備が強く求められる。
- 情報セキュリティインシデントが発生した場合には、法令等に基づく報告に加え、必要に応じて、所管官庁等の関係者に対して報告することも重要である。特に、サイバー攻撃を受けた又はその疑いがある場合には、早急にその状況を厚生労働省、都道府県警察、その他所管官庁等に報告し、共有することにより、被害の拡大を防ぎ、復旧のための対策を講ずることが可能となるためである。
- 「医療機関等におけるサイバーセキュリティ対策の強化について」（平成 30 年 10 月 29 日付け医政総発 1029

第１号・医政地発 1029 第３号・医政研発 1029 第１号厚生労働省医政局関係課長連名通知）では不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏えいや医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、所管官庁への連絡等、必要な対応を行うこととされている。

- なお、ランサムウェア攻撃においては、暗号化された情報の復号と引き換えに攻撃者から金銭を要求されることがある。「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」（令和４年 11 月 10 日付け厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室・厚生労働省政策統括官付サイバーセキュリティ担当参事官室事務連絡）[3]のとおり、金銭の支払いは、犯罪組織に対して支援を行うことと同義であり、厳に慎むこと。
- また、医療情報を含む個人情報の漏えい等の疑いが生じた場合には、個人情報保護法に基づく報告等が必要である（同法第 26 条、同法施行規則第８条）。

[3] https://www.mhlw.go.jp/content/10808000/001079508.pdf

４．安全管理に必要な対策全般

【遵守事項】

① 医療情報システムの安全管理に必要な対策項目（下表参照）の概要を認識し、企画管理者やシステム運用担当者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。

② 対応ができていない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。

③ 医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。

４．１　必要な対策項目の概要

- 医療情報システムが情報セキュリティ上安全な状態を維持するために、企画管理者やシステム運用担当者が実施する具体的な技術的安全管理対策の項目を下表に示す。
- 安全管理対策は運用的対策と技術的対策の両面でなされて初めて有効なものとなる。技術的対策には複数の選択肢があることが想定される。採用した技術的対策に相応した運用的な対策を実施すること。

表４－１　技術的な対策（参照：システム運用編　６．安全管理を実現するための技術的対策の体系）

クライアント側	・情報の持出し・管理・破棄等に関する安全管理措置 ・利用機器・サービスに対する安全管理措置
サーバ側	・ソフトウェア・サービスに対する要求事項 ・システム関連事業者による保守対応等に対する安全管理措置 ・事業者選定と管理 ・システム運用管理（通常時・非常時等）
インフラ （ネットワーク、サーバルーム、媒体）	・物理的安全管理措置（サーバルーム等、バックアップ） ・ネットワークに関する安全管理措置 ・インフラ運用管理（通常時・非常時等）
セキュリティ	・認証・認可に関する安全管理措置 ・電子署名、タイムスタンプ ・証跡のレビュー、システム監査 ・外部からの攻撃に対する安全管理措置

４．２　必要な措置

- 対策項目の分類として、予防的措置と発見的措置が挙げられる。予防的措置は、想定されたリスクが実際に生じないようにするための措置であり、例えば許諾された者以外に患者の医療情報を閲覧できないようにするためのデータに対するアクセスコントロールなどが挙げられる。発見的措置は、仮にインシデントが発生しても、速やかに検知をすることで、被害拡大を最小限にコントロールするための措置である。例えば、医療情報へのアクセス状況についてログ監査を実施し、不審なアクセスがないかどうかを確認し、必要に応じて措置を講じることなどが挙げられる。

- 対策項目としては、可能な限り予防的措置を講じることが望ましい。医療提供の継続性を考慮すると、リスクを未然に防止することが妥当である。
- 多様化・巧妙化が進む昨今のサイバー攻撃に対しては、予防的措置だけでは対応が不十分となる可能性があり、速やかに攻撃、あるいは攻撃された痕跡を検知するなどの発見的措置も、適宜組み合わせること。

5．医療情報システム・サービス事業者との協働

【遵守事項】

① 委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。

② 委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001 又はこれと同等の規格の認証を受けているシステム関連事業者を選定するよう指示すること。

③ 医療機関等で導入する医療情報システムは、システム運用編で求める要件を満たすシステムを選定するよう指示すること。

④ 委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取扱い等、医療機関等が負う医療情報システムの管理に関して、協働する上で認識の齟齬等が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。

⑤ 委託先事業者が、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。

⑥ システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。

5．1　事業者選定

5．1．1　事業者選定

- 外部委託により、医療情報システムの安全管理を行うためには、適切な情報システム・サービスを選定することが求められる。選定に際しては、それらの機能や仕様等が、医療機関等が要求・想定する内容と合致することのみならず、情報セキュリティの観点からも十分な対策が講じられていることの確認が必要である。
- システムの機能や仕様等だけでなく、システム関連事業者自体の評価を行うことも重要であり、組織として情報セキュリティマネジメントを適切に講じていることが求められる。
- 個人情報保護法では委託先の監督が、個人情報取扱事業者の義務とされているが（同法第 25 条）、「個人情報の保護に関する法律についてのガイドライン」（個人情報保護委員会）においては、適切な委託先の選定を行うことがその義務に含まれており、安全管理措置が適切に行われている委託先を選定することとされている（「個人情報の保護に関する法律についてのガイドライン（通則編）」P55）。また、医療情報を医療機関等の外部に委託して保存する場合には、「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長連名通知。平成 25 年 3 月 25 日最終改正。）により、本ガイドライン及び「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）を遵守しているシステム関連事業者であることが必要とされている。

5．1．2　事業者選定の基準

- 外部委託においては、医療情報の取扱いに関する内容が含まれることから、委託先事業者においても、個人情報保護等に関する対応の安全性が確保されていることが求められる。
- 個人情報保護に関しては「JIS Q 15001 個人情報保護マネジメントシステム」（プライバシーマーク制度と呼ば

れる）があり、情報の安全管理に関しては「JIS Q 27001 情報セキュリティマネジメントシステム」（ISMS 認証制度と呼ばれる）などの規格の認証により、システム関連事業者における情報管理等の安全性を確認することができる。[4]

- 医療情報の取扱いに関する委託先事業者を選定する際には、これらの認証を取得しているシステム関連事業者から選定すること。委託する内容に応じて、適宜、第三者認証などを活用して、システム関連事業者に対する信頼性を確認した上で選定することが望ましい。
- システム運用編においては、物理的安全管理、技術的安全管理の観点から求められる対策が示されており、医療機関等では、これらの対応を行うために、システムやサービスの選定を行うことになる。例えば二要素認証に対応したシステムは、原則、令和 9 年度時点で対応したものを選定することとしている。経営層においても、これらの趣旨を理解し、適切に事業者選定を行うことを指示することが求められる。
- パスワードの使い回しや推測が容易なパスワードの設定が、内部での不正利用やサイバー攻撃による被害の主要な要因のひとつとなっている。これらのリスクを最小限とするため、パスワードに加えて別の要素を組み合わせる二要素認証を可能な限り迅速に採用すること。

5．2 事業者管理

5．2．1 契約管理

- 外部委託先事業者との契約においては、委託業務の内容や責任分界、委託先事業者の体制、医療情報の取扱いを明確にすることが重要である。委託先事業者の個人情報の取扱いに関する遵守義務や、委託業務に従事する者に対する教育の実施状況などを確認、管理しておくことが必要である。

5．2．2 体制管理

- 医療情報の取扱いに関しては、外部委託先事業者による再委託先などの監督も重要である。再委託先における安全管理が不十分な場合には、サプライチェーン攻撃等の被害が生じ得る。特に海外のシステム関連事業者を再委託先とする場合には、個人情報保護法等が求める要件を具備しているか十分留意する必要がある。
- 委託先事業者が再委託等を行う場合、医療機関等は事前に事業者に情報提供を受けて協議を行い、その実施可否を判断すること。

5．3 責任分界管理

- 委託先事業者との責任分界については、委託先事業者と委託する業務内容に応じて、具体的なセキュリティに関する責任の範囲も明確にする必要がある。責任の範囲が明確でない場合には、医療機関等が講じるべき情報セキュリティ対策のうち、一部が抜け落ちてしまうリスクがある。例えばサイバー攻撃などの非常時には、医療機関等と委託先事業者で協働して原因の究明を進めることなどを取り決めておくことが考えられる。
- 委託先事業者が別事業者のクラウドサービスなどを用いる場合、責任関係が複雑になることが想定される。医療機関等においては、ネットワークサービスのほか、各種クラウドサービスを利用することにより、医療情報システムに支

[4] 特に、プライバシーマーク認定を取得している事業者であることが望ましい。また ISMS 認証については、情報システム管理が適正になされていることを認証するものであり、安全対策の有効性までを認証するものではないことに留意する必要がある。そのため、ISMS 認証のみを取得している事業者については、事業者における具体的な管理方法の説明等、有効性を示す資料の提供を求めることが望ましい。

障が生じた場合には、どのシステム関連事業者と原因究明や対策を講じるべきかが不明瞭になることがある。

- そのため、利用する医療情報システム・サービスに関連する情報機器等の管理がどの主体にあるのかを明確にし、安全性の確保の対応の役割分担についても明らかにする必要がある。情報機器の所有者、設置責任者、その安全管理措置のための保守管理者等がそれぞれ異なることもあり、事前に明確にすること。
- 外部委託を行う際の責任分界の重要性を認識し、医療機関等と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理するよう、企画管理者やシステム運用担当者に指示することが求められる。

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。

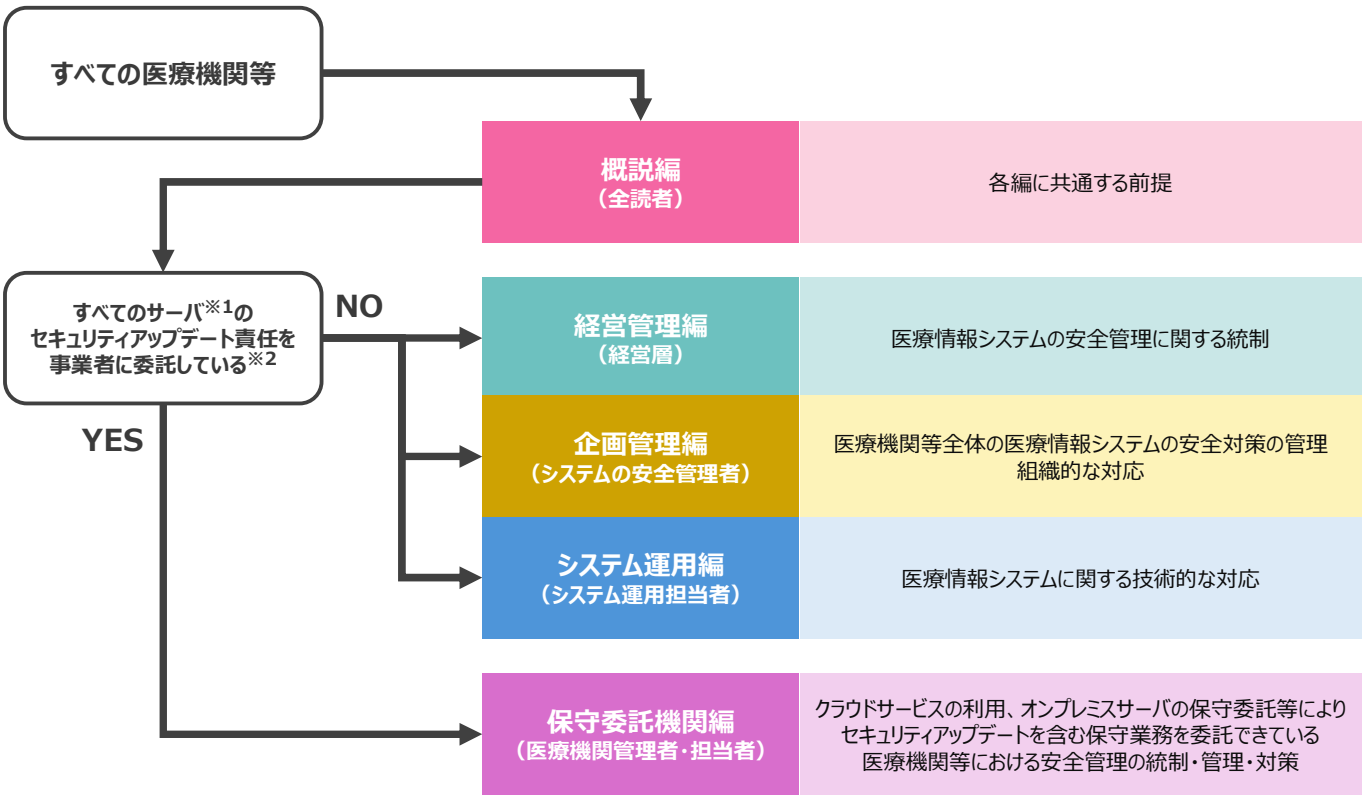
1．本編の対象

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	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 （　/　）	（　/　）	

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）

医療情報システムの利用権限は、医療従事者の資格や医療機関等内の権限規程に応じて設定することが重要です。企画管理者等は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。

▶企画管理編
13④
13.1.3

特に管理者権限を与えるアカウントは最低限のユーザに付与することを徹底してください。これはサイバー攻撃を受けた際の水平展開を防ぐためです。すべてのユーザに管理者権限が付与されていることで、ウイルス対策ソフトを無効化されるなどして、被害が拡大した事例が多発しています。

利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、所属部署・氏名・ユーザ ID・権限等が想定されます。

●利用者 ID 台帳の例

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可
・	・	・	・	・	・	・	・	・

No.	利用者属性	性	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年３月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

⑤　退職者や使用していないアカウント等、不要なアカウントを削除又は無効化をしている。
（医療情報システム全般）

企画管理者等は２-④で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。長期間使用されていない等の不要な ID は不正アクセスに利用されるリスクがありますので、適宜削除や無効化をする等の対応をしてください。

▶企画管理編
13⑦

⑥　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

▶システム運用編
8③
8.1
8.2
13.2

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、すべての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが挙げられます。

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

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

（用語の解説）

パターンファイル：ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。

（補足）

古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

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

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

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

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

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

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

※強固なパスワード

・英数字混在させた 13 桁以上の推定困難な文字列

・二要素以上の認証の場合、英数字を混在させた８文字以上の推定困難な文字列

▶システム運用編
8.⑤

⑧　パスワードの使い回しを禁止している。（医療情報システム全般）

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。

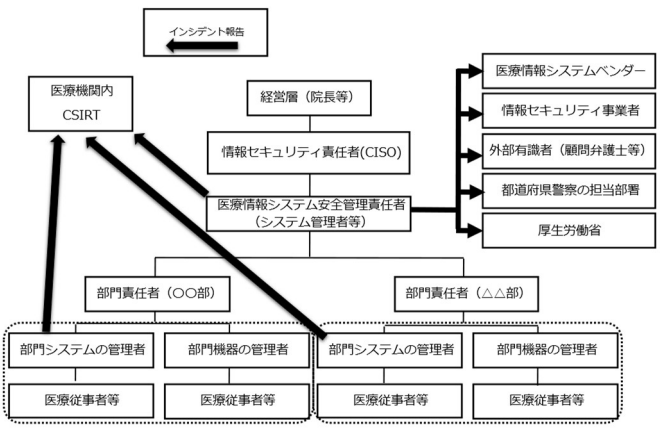
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

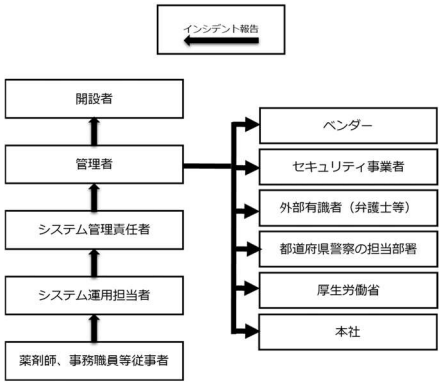
情報セキュリティインシデント発生時（医療情報システムに障害が発生した場合を含む）は、下記の厚生労働省の連絡先に御連絡ください。

【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、万が一サイバー攻撃を受けても重要業務が中断しない、又は中断しても短い期間で再開することが期待できます。

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

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

▶経営管理編
3.4.1
▶企画管理編
11.1

4　規程類の整備　【医療機関・薬局確認用】

①上記 1－3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。
（医療情報システム全般）

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

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

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

立入検査時は、本規程類も確認対象となります。

▶企画管理編 4.1