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。