医療情報システムの安全管理に関するガイドライン

第 6.1 版(案)

概説編

[Overview]

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 6.0 版からは、本ガイドラインの内容の理解を促進し、実効性を高めるため、本文について経営管理編、企画管理編及びシステム運用編に分け、各編で想定する読者に求められる遵守事項及びその考え方を示した。そのほか、近時のサイバー攻撃及びクラウドサービス利用の普及等を踏まえ、医療機関等に求められる安全管理措置を中心に内容面の見直しを行った。
- 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。

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、本ガイドライン全て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。
- 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。
- なお、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は本ガイドラインの対象外となる。その後、当該医療情報について患者から提供を受けた事業者等の第三者が取り扱う場合には、PHR（Personal Health Record）として、「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）の対象となり得る。

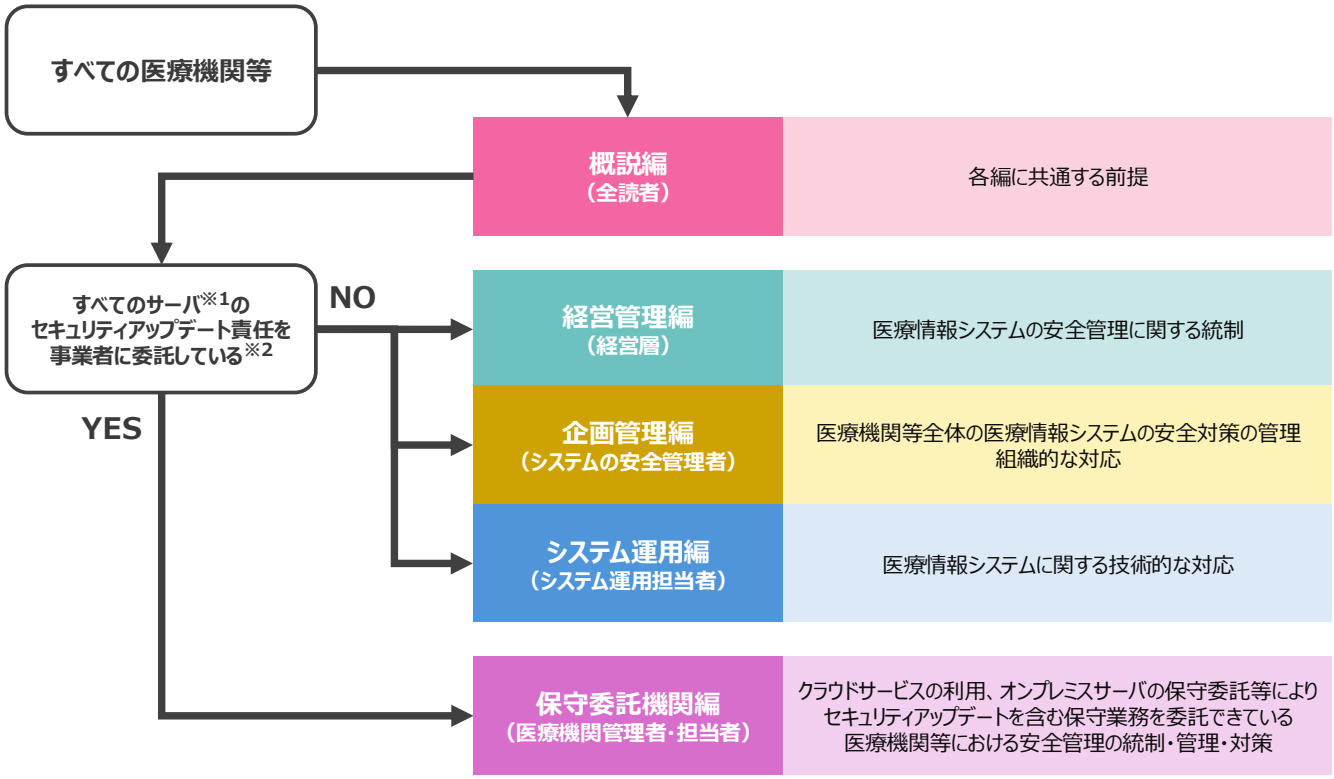
2．3　医療情報システムの範囲

- 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（Overview）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（Governance）、企画管理編（Management）、システム運用編（Control）、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追うこと」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 6.1 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（Overview）

- 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（Governance）

- 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（Management）

- 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（Control）

- 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全体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を配置されておらず、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。
- さらには一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（以下、「e-文書法」という）、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・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、当該情報の見読性・真正性・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「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」)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環境要因によるもの、医療情報の漏洩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[1]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

[1] 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。

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。

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管を委託し、医療機関の外部に医療情報を保管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、情報漏洩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。