医療情報システムの安全管理に関するガイドライン

第 6.0 版

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 版では、本ガイドラインの内容の理解を促進し、医療情報システムの安全管理の実効性を高める観点から、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すとともに、Q&A 等で現状選択可能な具体的技術にも言及するかたちとすべく、構成の見直しを行った。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について適切な取り扱いが行われていることが前提となることから、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」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、すべ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。

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。

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が含まれる。

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）の４編から構成する（図３－１参照）。

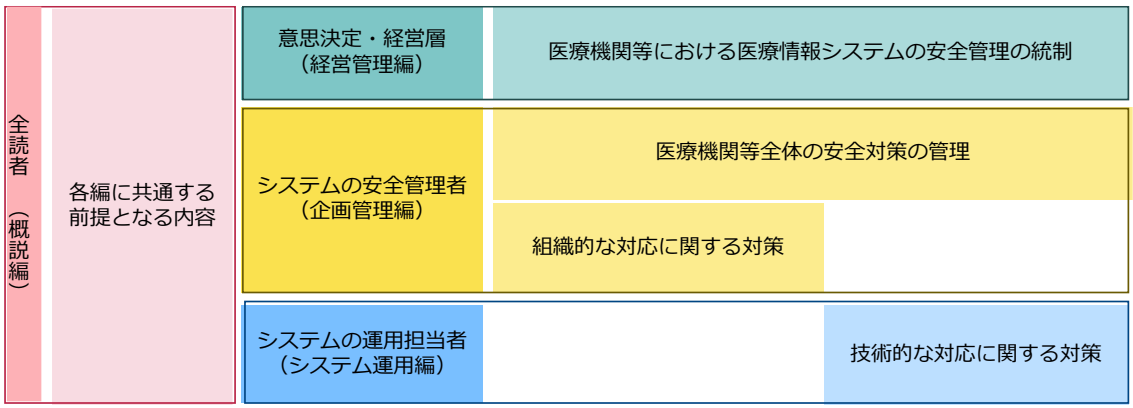


図３－１　ガイドライン第 6.0 版を構成する各編

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（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。

３．２．医療機関等の特性に応じた読み方

３．２．１　医療機関等の特性についての考え方

本ガイドラインは、すべての医療機関等における医療情報システムを対象とした安全管理に関して、各編で遵守事項及びその考え方等を示している。

医療機関等の組織体制、稼働している医療情報システムの構成、採用しているサービス形態等の特性は様々であるため、それぞれの医療機関等の特性に応じたかたちで本ガイドラインを遵守する必要がある。そのため、本項では、医療機関等の特性ごとに、医療機関等が必要な安全管理を確保するために本ガイドラインで最低限参照すべき箇所について明記する。

具体的には、医療機関等における専任のシステム運用担当者の有無と導入している医療情報システムの形態に応じた、4種の参照パターンを例示する（表３－１）。自施設の特性を分析した上で、最も近しい参照パターンに基づく対応を行っていただきたい。（なお、参照パターンに示した参照箇所以外の箇所についても、必要に応じてご参照いただきたい。）

表３－１　医療機関等の特性に応じた本ガイドラインの参照パターン

	医療情報システムを 医療機関等に保有し運用 （いわゆるオンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆるクラウドサービス型）
システム運用専任の 担当者がいる	Ⅰ	Ⅱ
システム運用専任の 担当者がいない	Ⅲ	Ⅳ

なお、医療機関等において、カルテ等の医療情報を紙媒体で扱い、情報システム上では医療情報を扱わない業務のみ行っている場合でも、医療機関等内の端末上又はシステムとの連携によって、医療機関等外の医療情報へのアクセスが発生する場合は、参照パターンⅡやⅣに基づき本ガイドラインを参照する必要がある。

ただし、システム全体の構成等により、参照パターンが異なるので、必要に応じて、システムの提供元である医療情報システム・サービス事業者に参照パターンを確認することが必要になる。

３．２．２　医療機関等の特性に応じたガイドライン参照箇所

前項で例示した「医療機関等の特性に応じた本ガイドラインの参照パターン」（表３－１）による参照箇所の詳細を次頁に示す（表３―２）。

表３－２　参照パターンに応じた参照箇所

<table>
<tr><th>パターン</th><th>経営管理編</th><th>企画管理編</th><th>システム運用編</th></tr>
<tr><td>Ⅰ
担当者あり</td><td rowspan="4">すべて

参照</td><td colspan="2">すべて参照</td></tr>
<tr><td>Ⅱ
担当者あり
クラウド</td><td>基本的にすべて参照

※ 医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、以下について簡略化が可能。
４．４　マニュアル等及び各種資料の整備
５．安全管理におけるエビデンス
１５．技術的な対策の管理
遵守事項：④、⑥、⑦、⑧、⑬以外</td><td>以下項目は参照
１～４、６～８、１１、１２．３、１４，１８

※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。</td></tr>
<tr><td>Ⅲ
担当者なし</td><td colspan="2">すべて参照
※　各編内の「担当者」という記載を「企画管理者」に置換し、参照。</td></tr>
<tr><td>Ⅳ
担当者なし
クラウド</td><td>基本的にすべて参照

※「担当者」という記載を「企画管理者」に置換し、参照。
※医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、以下について簡略化が可能。
４．４　マニュアル等及び各種資料の整備
５．安全管理におけるエビデンス
１５．技術的な対策の管理
遵守事項：④、⑥、⑦、⑧、⑬以外</td><td>以下項目は参照
１～４、６～８、１１、１２．３、１４，１８

※「担当者」という記載を「企画管理者」に置換し、参照。
※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。</td></tr>
</table>

３．３　第 5.2 版との関係

第 5.2 版では、本編及び別冊編に分けて、原則として医療機関等の情報システムの安全管理に必要な内容を本編に、前提となる考え方及び具体的な方策の例を別冊編に示した。

第 6.0 版では、システム運用担当者並びに、経営層や企画管理者に対しても本ガイドラインの内容を理解してもらい、医療情報システムの安全管理の実効性を高める観点から、全体構成を大幅に変更した。具体的には、主に第 5.2 版の本編について、「１．１　背景・経緯」に示す観点から分冊化を図り、第 5.2 版の本編及び別冊編の一部について、Q&A へ移動するなどにより、読みやすさの向上を図っている。

４．　本ガイドラインの前提

ここでは、各編における遵守事項を理解する上で、前提となる考え方等について示す。

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、病歴等の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、適切な管理がなされなければ、患者の生命、身体の安全に直接影響を及ぼす可能性があるものであるため、慎重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ものであるため、医療機関等が行う業務の範囲内で適切に管理されることが求められる。

また、継続した医療の提供の観点からも、医療機関等の間で絶え間なく患者の医療情報が提供・共有されることが重要である。医療の継続性を支える観点からも、適切な管理の下、医療情報システムが利用され、医療情報が活用できる状態に置かれることが重要となる。

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確認することができることになり、医療従事者や患者の負担を軽減することが可能となる。

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、地域医療又はチーム医療などにおいて、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で行われることが求められる。

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。機密性が確保されないと、許可していない者による情報システムの利用や改ざん、破壊などが生じうるほか、医療情報システムで取り扱う医療情報の不正な利用（参照、登録、改変）や漏えいなどが生じうる。

「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と、表示されるべき情報が欠落したり、不完全な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と、情報システムが利用できなかったり、利用目的に応じた適切な速度等での処理がなされなかったりすることで、医療情報などの利用が妨げられることなどが生じうる。

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、３要素を保護するための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・運用することなどが求められる。

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）
- e-文書法、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。）

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、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。

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する必要がある。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であって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、医療機関等内において、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し、経営層において医療機関等の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想定される。医療機関等においては、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、総務省・経済産業省が定めている「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」、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が求められる。

加えて、当該事業者に対して、必要に応じて、「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、安全を脅かす又は損なう原因となる「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等が発生する可能性がリスクとして表される。

医療情報は、患者の生命・身体の安全に関わるものであり、これらの脅威にさらされると、医療の提供が停止するといった影響が生じることも考えられる。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が求められる。

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、総務省・経済産業省が定めている「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」における「サービス仕様適合開示書」や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）及び保健医療福祉情報システム工業会（JAHIS）の JAHIS 標準となっている「『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等を参考に、当該事業者から情報提供していただく等により、当該事業者と医療情報システムの安全管理上のリスクについて共通の理解を得た上で、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が求められる。

４．６　医療情報システムにおける認証・認可

認証された利用者等が、許可された範囲で情報やサービスを利用する情報システムは、今日多く存在する。医療情報システムも同様に、利用者や利用範囲を適切に管理することが求められ、そのためにシステム利用等において認証・認可の対策を講じる必要がある。

医療情報システムでは、医療機関等が組織として情報システムの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。

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や利用等が認められていないものがある。加えて、患者の医療情報が流出したり、不正に利用されたりした場合には、患者の生命や心身の安全に影響を及ぼす可能性がある。したがって、こうした医療情報を取り扱う医療情報システムにおいて算定するリスクは、通常の情報システムよりも高く算定する必要があるため、医療情報システムにおいて用いる認証・認可については、特に安全なものを採用する必要がある。

情報システムの認証では、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）等が必要とされる。医療情報システムにおいては、このような識別子の発行や、本人であることを確認するための仕組み（認証方法）のいずれも、高い水準のものを採用することが求められる。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、複数の要素を用いて認証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データの保管を委託し、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意味で、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、自機関のみで整備するよりも、医療情報システム・サービス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ることも想定される。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とがある。

このように、外部保存については、適切な運用により、医療機関等における医療情報の取扱いを向上させることも想定できる。そこで、医療機関等において取り扱う医療情報システムの種類や医療情報の量、組織体制などを勘案して、外部保存を適宜利用することも、安全管理との関係では重要な方策の一つである。

医療情報システムの安全管理に関するガイドライン

第 6.0 版

経営管理編

[Governance]

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＞

紙又はフイルムの媒体だけでなく、電磁的記録媒体、情報通信機器、その他情報通信環境を用いて電子的に医療情報を取り扱う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、対策が十分に行われていなかったことで、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、サイバー攻撃の被害が一医療機関等内で止まることなく、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、一医療機関等に限定されない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生じることはもちろん、安全管理上のリスクに対する対応の是非、さらには経営責任や法的責任が問われる可能性がある。その結果、行政処分の対象となったり、民事上の賠償責任などを負ったりする可能性があるほか、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を求められたり、インシデントによる被害拡大の防止を図るための初動対応やインシデントからの復旧に多大な費用の捻出を余儀なくされるなど、医療機関等の経営や運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。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。

＜経営管理編の構成と概要＞

本編では、医療機関等における医療情報と医療情報システムの安全管理において、医療機関等の経営層が、経営管理上、遵守すべき事項とその考え方を５章に分けて示す。各章の概要は以下のとおりである。

１．安全管理に関する責任・責務
- ・医療情報の取扱いや医療情報システムの安全管理に関する法令上の遵守事項や義務など
- ・通常時や非常時における安全管理上の説明責任や管理責任
- ・医療情報や医療情報システムに関して委託や第三者提供を行う場合の責任

２．リスク評価を踏まえた管理
- ・医療情報及び医療情報システムに対するリスク評価の重要性
- ・リスク評価を踏まえた経営資源・資産の安全管理に関する方針の策定、安全管理対策の必要性、情報セキュリティマネジメントシステム（ISMS）の確立

３．安全管理全般（統制、設計、管理等）
- ・意思決定・経営層による統制のもと、組織的な対応・技術的な対応として必要な体制や文書を整備し、リスク評価に基づく安全管理方針に従って、適切な安全管理対策を設計し、管理することなど
- ・安全管理対策の実効性を担保するための自己点検や監査の意義や必要性
- ・情報セキュリティインシデントが発生した場合の対応

４．安全管理に必要な対策全般
- ・技術的な安全管理対策について、情報システムの構成を踏まえた分類（クライアント側、サーバ側、インフラ、セキュリティ）と各分類で採用する安全管理措置

５．医療情報システム・サービス事業者との協働
- ・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。）に対して委託を行う場合の事業者の選定、委託契約や体制の管理、委託先事業者との責任分界や役割分担の明確化と協働体制の確立と管理など

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

【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システム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。

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。
- 医療は重要な公的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・維持することは公的な責務と考えられるため、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洩や医療情報の漏洩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、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、医療機関等の業務状況を踏まえ、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想定される。
- 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による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

【遵守事項】

＜説明責任＞

① 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 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。

＜管理責任＞

① 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。

② 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。

＜定期的な見直し、必要に応じた改善を行う責任＞

① 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。

② 医療情報に関する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。

＜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、対応の記録を文書化し、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必要がある。
- 医療機関等の規模に応じて、患者等への説明を行う窓口を確保することも必要となる。

＜管理責任＞

- 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洩、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、監督を実施する必要がある。

＜定期的な見直し、必要に応じた改善を行う責任＞

- 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。特に日々高度化、巧妙化するサイバー攻撃への対応を考えると、医療情報システムの安全管理を確保するためには、安全管理体制について随時必要な見直しが求められる。
- 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等により、安全管理の改善に必要な情報を収集することも考えられる。

１．２．２　非常時における責任

【遵守事項】

＜説明責任＞

① 情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その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。

＜善後策を講ずる責任＞

① 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。

② 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。

③ ①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、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。

＜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、情報漏洩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。

＜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、医療情報及び医療情報システムの管理上で生じた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。原因が不明のままであると、再発の可能性が解消されず、患者等が安心して医療情報を医療機関等に委ねたり医療サービスを受けたりすることができないため、可及的速やかに原因を究明することが求められる。
- 「再発防止策を講ずる責任」とは、究明された情報セキュリティインシデントの発生原因に対して、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。具体的な再発防止策の検討に際しては、医療機関等のみでは容易でない場合もあるため、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が求められる。

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

【遵守事項】

① 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。

- 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。

１．３．２　委託（第三者委託）における責任分界

【遵守事項】

① 業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに役割分担等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、適切に契約等の取決めを実施し、保管すること。

- 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を行うことが求められる。
  - 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、医療機関等が負う責任をきちんと果たせるよう、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、適切に管理する必要がある。
  - 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。法律上の責任範囲を示す一般的な契約書などでは、具体的な対応の詳細まで記述することがなじまない場合があるが、情報セキュリティインシデントが生じた場合の原因究明のための具体的な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必要がある。

    そのため、契約上の責任範囲は可能な範囲で具体的に特定しつつ、具体的な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に示して、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

【遵守事項】

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の範囲をあらかじめ明確にし、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。

- 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、医療機関等が外部の第三者に医療情報を提供する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有している。
- 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、提供元の医療機関等においては、原則として適切な第三者提供がなされる限り、その後の当該情報の保護に関する責任は離れる。なお、情報を第三者に提供しても、提供元の医療機関等の側で当該情報を完全に削除しない限り、当該情報はなお当該医療機関等の下に存在するため、その場合は当該情報に対する適切な管理責任が残ることになる。
- 第三者提供において、提供元の医療機関等と提供先の第三者との間で、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が求められる。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

2．1　医療情報システムにおけるリスク評価の実施

【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、対応方針を策定し、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、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。

③ 経営層の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。

- 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。
- 医療機関等が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、
  ・医療機関等に求められる医療の提供を維持・継続等するために、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、
  ・各リスクに対して、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%に限りなく近づけることが厳しい医療情報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）

  を判断することが求められる。
- 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。
- システム運用担当者に、企画管理者のもと、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。

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

【遵守事項】

① リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。

② 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。

- 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。
- 医療機関等は公的社会インフラであり、患者のために医療サービスの提供の継続性を確保・維持する必要があることを踏まえると、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」と考えられ、継続的に、リスク評価、当該評価を踏まえたリスク管理方針の決定、当該方針に基づくリスク管理を実施する必要がある。
- リスク管理方針を策定する際、医療機関等の経営の視点、人事管理の視点等を入れなければ、医療機関等の運営継続そのものに支障をきたすことになりかねないため、注意が必要である。
- 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

【遵守事項】

① 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。

- 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

【遵守事項】

①　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。

- 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）

3．1　統制

3．1．1　情報セキュリティ対策のための統制

【遵守事項】

① 統制の体系を理解し、医療機関等における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とともに、適切に統制が機能しれているかを確認すること。

- 医療情報システムの情報セキュリティ対策は、医療機関等における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。情報セキュリティを十分に確保するためには、具体的な情報セキュリティ対策の検討に加え、医療機関等においてどのような情報セキュリティ対策を講じていくのかを示した計画の策定、当該計画の内容を実現するために必要な規程類の整備、当該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適切な粒度で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で、的確で迅速な情報セキュリティ対策の実現が期待される。
- 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、医療情報システムの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、ならびに、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も求められる。

３．１．２　医療情報システムにおける統制上の留意点

【遵守事項】

① 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。

② 医療機関等において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。

③ 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や人事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。

④ 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。

- 医療情報を取り扱う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や「個人経営」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）がなく、組織運営のための計画等がない場合がある。このような場合、情報セキュリティ対策に係る詳細な計画や規程類を策定したとしても、実効性が伴わず、単に医療機関等の負担が増大してしまうことにつながるため、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、そのうえで必要な内容を定めることが必要である。

  また、実際の統制が患者等に対する説明や情報セキュリティインシデントが生じた場合の関係者への適切な報告として必要十分な内容となっているか、システム関連事業者に対する適切な管理を行うために必要十分な資料等が確保されているか、といった観点など、医療機関等において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できているかどうかも念頭に置きながら、医療機関等の規模や組織構成、特性等を踏まえた上で実効性のある統制の内容を考える必要がある。
- 医療機関等において、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、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り、必要に応じて、企画管理者等が行う管理を支援するための医療情報システム管理委員会等の組織を設置することも有用である。なお、医療機関等の規模、組織等を勘案して、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。

  なお、医療情報システム安全管理責任者としての職務は、経営層が担うことを想定しているが、医療機関等の規模・組織等を考慮して、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は妨げられない。
- 医療機関等の組織構成によっては、例えば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ような組織構成となっている場合があるが、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ため、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、組織横断的な実働ができているかどうかに留意が必要である。
- 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、医療情報システムに関係する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

【遵守事項】

① 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。

② 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。

- 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、情報セキュリティ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が求められる。例えば、他の医療機関等で策定された運用管理規程やアクセス管理規程等をそのまま自医療機関等の規程等に転用したとしても、実態と合致していない場合、情報セキュリティ対策の運用ルールが適切に示されていないことになり、却って情報セキュリティリスクが増大する危険性が生じる。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しまうこととなり、有効な対策とはならない可能性がある。
- 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ることが求められ、実際に運用可能なものであって、適切な内容が記載されたものを整備する必要がある。

3．2．2　情報セキュリティ対策を踏まえた訓練・教育

【遵守事項】

① 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すべてに対して定期的な教育・訓練を実施すること。

- 規程類が適切に整備され、また、必要な情報セキュリティ対策が医療情報システム上で実装されているとしても、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おらず、適切な対策が実行されていなければ、当該規程類が遵守されていないことと同義であり、情報セキュリティ対策の水準向上を望むことはできない。また災害、サイバー攻撃またはシステム障害に起因する非常時の対策についても、実際の状況下で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、その上で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、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

【遵守事項】

① 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。

- 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（「自己点検」）。自己点検により、医療機関等における医療従事者や職員等が自らの役割に応じて実施すべき対策事項を実際に実施しているか否かを確認することができ、日常業務におけ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ができるため、組織全体の情報セキュリティ対策の水準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が重要である。

3．3．2　情報セキュリティ監査

【遵守事項】

① 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、また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。

② 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。

- 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、医療情報システムの仕様や運用方法を明確に文書化し、情報セキュリティ方針に基づき、機能・運用し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必要がある。
- 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

【遵守事項】

① 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。

② 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、医療情報システムの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。

③ 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。

- 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稼働（可用性）が損なわれるような非常時に備えて、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し、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 等を整備することが求められる。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るが、これらの原因の違いに応じて、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。
- 医療情報システムの情報システム面において、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。
- また、非常時において、医療情報システムの利用が困難な場合の対応や復旧に至るまでの対応についても、通常時から明らかにしておく必要がある。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。
- 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、医療情報システムの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、経営層においては、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必要がある。

- なお、医療機関等が管理する医療情報の取扱いに関して、情報セキュリティインシデントが生じた場合の対応も考慮する必要がある。例えば、情報セキュリティインシデントには情報漏洩なども含まれており、これらは直ちに医療情報システムの稼働自体に影響を及ぼすものではないが、患者情報は大変機微な情報であり、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、医療機関等の経営にも大きな影響を及ぼす可能性があるため、情報漏洩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必要がある。

3．4．2　情報共有・支援、情報収集

【遵守事項】

① 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、企画管理者に指示すること。

② 情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策や EOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示すること。

- 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とされることから、速やかに情報共有等が行えるよう、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は有用である。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が重要である。
- 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 Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示することは重要である。

３．４．３　情報セキュリティインシデントへの対応体制

【遵守事項】

① 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、都道府県警察の担当部署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。

② 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。

- 情報セキュリティインシデントが発生した場合、医療機関等内の対応として、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またはその疑いがある場合には、早急にその状況を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。
- 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、個人情報の漏洩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、「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、必要な対応を行うこととなっている。
- また、患者の個人情報を含む医療情報の漏洩等が生じた場合には、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）。

４．安全管理に必要な対策全般

４．１　必要な対策項目の概要

【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。）の概要を認識した上で、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。

- 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。
- 安全管理対策には運用管理に関する対策と技術的な対策の両方があるが、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多いため、採用した技術的対策に相応した運用的な対策を実施していただきたい。

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 システム利用者に近いクライアント側において生じうるリスクに対する対策項目 ・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 システム利用者によるクライアント側での医療情報の利用を支える基幹または中枢の情報システム・サービスに関するリスクへの対策項目 ・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 医療機関等におけるクライアント側やサーバ側を支えるインフラサービス（ネットワーク、サーバルーム、媒体）に関するリスクへの対策項目 ・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 クライアント側、サーバ側、インフラ等、医療機関等で医療情報システムを利用する際に、共通して求められるセキュリティの観点で必要な対策項目 ・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

【遵守事項】

① 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。

- 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、仮にリスクとして想定する事象が発生しても、速やかに事象の発生を検知することで、具体的なリスクの発生を防止したり、被害拡大を防止したりするための措置であり、例えば医療情報に対するアクセス状況をシステム操作ログ等を用いて監査し、不審なアクセスがないかどうかを確認の上、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。リスクの発生を未然に防止することが妥当であるし、また費用や労力の点からも、発見的措置に比べて負担が大きくならない場合が多いことが想定されるためである。
- 多様化・巧妙化が進む昨今のサイバー攻撃に対しては、必ずしも予防的措置だけでは十分な対応が難しいため、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が求められる。

5．医療情報システム・サービス事業者との協働

5．1　事業者選定

【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。

5．1．1　事業者選定

- 医療機関等が外部委託により提供される情報システム・サービスを活用して、医療情報システムの安全管理を行うためには、実際に活用する情報システム・サービスが適切なものであることが重要である。情報システム・サービスの選定に際しては、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が必要であるが、併せてそれらの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が求められる。
- 情報セキュリティ対策に関する機能や仕様等については、システム関連事業者からの情報提供などにより、その安全性を確認する必要もあるが、併せてシステム関連事業者自体の評価を行うことも重要である。情報セキュリティ対策は情報システム・サービスにおける情報セキュリティ機能等だけではなく、システム関連事業者の組織としての情報セキュリティマネジメントが適切に講じられている必要もあるためである。
- 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)、同法ガイドラインにおいては、適切な委託先の選定を行うことがその義務に含まれているとされており、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（「個人情報保護法ガイドライン　通則編」P53)。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」（P 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 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。
- 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が求められる。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も望ましい。

５．２　事業者管理

５．２．１　契約管理

【遵守事項】

① 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。

- 外部委託先事業者との契約においては、委託業務の内容や委託先事業者の体制、委託先事業者との責任分界などについて示すほか、委託先事業者における医療情報の取扱いの状況を把握でき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、委託先事業者の業務に従事する者に対する教育等の実施状況などを確認し、管理しておくことが必要である。

５．２．２　体制管理

【遵守事項】

① 委託するシステム関連事業者に対して、業務実行体制を明確にし、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。

- 外部委託先事業者における医療情報の取扱いに関しては、再委託先などの体制の監督も重要である。医療機関等が委託先の選定をしても、委託先が再委託しており、その再委託先における医療情報の取扱いに関する安全性が確保されていない場合には、意図しないリスクが生じることになる。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、個人情報保護法が求める要件を具備しない場合などもあることから、十分留意する必要がある。
- 委託先事業者に対して、再委託等を行う場合には、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が求められる。

５．３　責任分界管理

【遵守事項】

① 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。

- 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可能性などがある。特にサイバー攻撃などの非常時に、原因の究明は医療機関等と委託先事業者との間で協力して進めることが不可欠であるが、その前提としても責任の範囲を明らかにしておく必要がある。
- クラウドサービスなどを用いる場合、サービスを提供する委託先事業者とクラウドサービス事業者等の間における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。また、クラウドサービス事業者においても、サービスのすべてをシステム関連事業者自らのシステム等で提供しているとは限らないことから、障害等が生じた場合の原因究明に時間を要することも想定される。
- 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医療機関等とシステム関連事業者のどちらにあるのかを明確にし、これに対する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、それぞれが異なる可能性もあることから、事前に明確にすることが求められる。
- 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 6.0 版

企画管理編

[Management]

目次

【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している。

＜医療機関等の特性に応じたガイドライン参照箇所＞

[医療機関等の特性についての考え方]

本ガイドラインは、すべての医療機関等における医療情報システムを対象とした安全管理に関して、各編で遵守事項や考え方等を示している。

医療機関等の組織体制や、稼働している医療情報システムの構成、採用しているサービス形態等の特性は様々であるため、それぞれの医療機関等の特性に応じたかたちで本ガイドラインを遵守していただく必要がある。そのため、以下のとおり、医療機関等の特性ごとに、医療機関等が必要な安全管理を確保するために本ガイドラインで最低限参照すべき箇所について明記する。

具体的には、医療機関等における専任のシステム運用担当者の有無と導入している医療情報システムの形態に応じた、4種の参照パターンを例示する。自施設の特性を分析した上で、最も近しい参照パターンに基づく対応を行っていただきたい。（なお、参照パターンに示した参照箇所以外の箇所についても、必要に応じてご参照いただきたい。）

医療機関等の特性に応じた本ガイドラインの参照パターン

	医療情報システムを 医療機関等に保有し運用 （いわゆるオンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆるクラウドサービス型）
システム運用専任の 担当者がいる	Ⅰ	Ⅱ
システム運用専任の 担当者がいない	Ⅲ	Ⅳ

なお、医療機関等において、カルテ等の医療情報を紙媒体で扱い、情報システム上では医療情報を扱わない業務のみ行っている場合でも、医療機関等内の端末上やシステムとの連携によって、医療機関等外の医療情報へのアクセスが発生する場合は、参照パターンⅡやⅣに基づき本ガイドラインを参照する必要がある。

ただし、システム全体の構成等により、参照パターンが異なるので、必要に応じて、システムの提供元である医療情報システム・サービス事業者に参照パターンを確認すること。

［医療機関等の特性に応じた企画管理編の参照箇所］

上記「医療機関等の特性に応じた本ガイドラインの参照パターン」による企画管理編の参照箇所の詳細を下表に示す。

パターン	**企画管理編**
Ⅰ 担当者あり	すべて参照
Ⅱ 担当者あり クラウド	基本的にすべて参照 ※　医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、以下について簡略化が可能。 ４．４ マニュアル等及び各種資料の整備 ５．安全管理におけるエビデンス １５．技術的な対策の管理 遵守事項：④、⑥、⑦、⑧、⑬以外
Ⅲ 担当者なし	すべて参照 ※　「担当者」という記載を「企画管理者」に置換し、参照
Ⅳ 担当者なし クラウド	基本的にすべて参照 ※　「担当者」という記載を「企画管理者」に置換し、参照。 ※　医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、以下について簡略化が可能。 ４．４ マニュアル等及び各種資料の整備 ５．安全管理におけるエビデンス １５．技術的な対策の管理 遵守事項：④、⑥、⑦、⑧、⑬以外

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ほか、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ところである。（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	秘密漏洩罪など
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、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。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。）等による秘密漏洩や医療情報の漏洩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必要がある。

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、経営層に適宜報告することが求められる。その上で、改善の必要が認められる場合には、適宜改善策を講じる必要がある。

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、利用目的による制限や不適正利用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、関係する法令が求める内容に従って医療従事者が作成する文書等（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。

（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。）等に従うことが求められる。

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、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。「必要な措置」としては、本ガイドラインを参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

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、漏洩等の報告義務、第三者提供の制限等）を規定。
e 文書法省令[1] 施行通知[2]	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[3]	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

[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）

[2] 「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。）

[3] 「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

	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。

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、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

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。）

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、例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（ポリシー）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。

そこで、医療機関等においては、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）、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を整備する必要がある。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、必要に応じて附則等を整備することが求められる。

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」[4]（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（ポリシー）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。

[4] 個人情報保護委員会、厚生労働省（平成 29 年 4 月 14 日）

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）を記載することを求めるほか、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洩等の情報セキュリティインシデントの責任も、すべて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。

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などの項目を、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、漏洩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、医療機関等におけるリスク管理が適切にできないことになる。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し、乖離がある場合にはその部分についてどのように対応するのかを両者で協議し、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。

２．２　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）

医療機関等と委託先事業者における責任分界については、2.1 で基本的な内容を示した。

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。

また、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も求められる。

（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

医療機関等がシステム関連事業者に医療情報システム・サービスを委託する場合として、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。

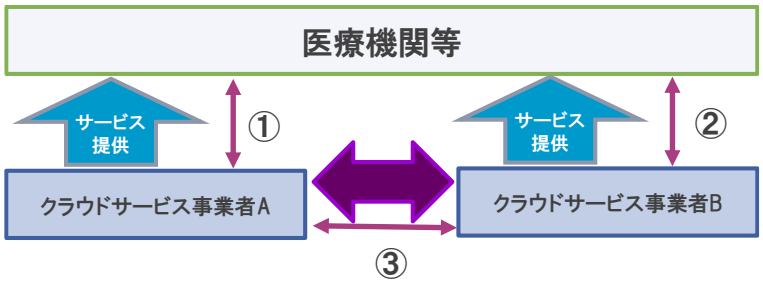
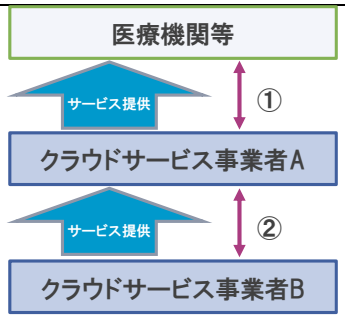
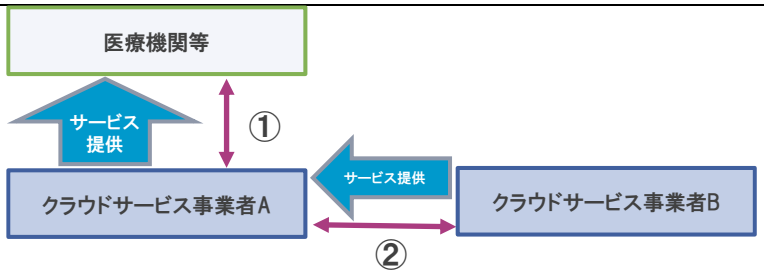
前者の場合は、基本的には医療機関等が各事業者と責任分界を取り決めることになるが、複数のシステム関連事業者のサービスの連携部分についても併せて取決めを行うことが求められる。これには、技術的な仕様等に関する取決めだけではなく、非常時におけるシステム関連事業者間での対応なども含めて取り決めることが求められる。

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。

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。
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	 ・　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ー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」[5]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。

[5] 総務省　令和 4 年 10 月 31 日

３．安全管理のための体制と責任・権限

【遵守事項】

① 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。

② 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。

③ 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。

④ 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。

⑤ 法律上の対応を含め医療情報の漏洩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。

⑥ 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。

⑦ 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。

⑧ 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。

⑨ 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。

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　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。

３．１．３　情報システム管理委員会の業務範囲と権限

情報システム管理委員会は、必ずしも設置が必要とされるものではなく、医療機関等において経営層の行う管理等の一部又は全部を担うものとして、各医療機関等の判断により医療機関等内に設置されるものである。情報システム管理委員会を設定して医療情報システムの安全管理を行う場合には、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が必要となる。

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。

３．１．４　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を有するほか、非常時における一次対応の判断権限などを有することが想定される。そのほか、技術的な対応のうち重要なものについては、企画管理者へ協議あるいは報告を行い、対応することが想定される。

３．１．５　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、迅速な判断や対応が求められるため、そのために必要な体制の整備が求められる。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も求められる。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が求められる。

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

などが想定される。

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が求められる。

また、医療情報の漏洩が生じた場合も、法令上必要な対応（個人情報保護法に基づく漏洩等の報告など）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、医療情報の漏洩が生じた場合の対応体制や手順等を整備して、経営層の承認を得ることが求められる。

３．１．６　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すべての者において当該安全管理に対する意識付けと知識が求められる。そのため、企画管理者は、医療機関等における医療従事者や職員に対する安全管理に関する教育・訓練等を行うとともに、そのために必要な体制を整備することが求められる。

３．１．７　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、医療機関等は医療情報システムの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必要がある。

３．１．８　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。

企画管理者には、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が求められる。

３．１．９　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必要がある。

３．１．10　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資料化等して可視化し、関係者に共有できるようにする必要がある。

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。

また、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し、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ため、組織の方針に基づくことになるが、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が求められる。

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、担当者に策定を指示するか、あるい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が求められる。

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り、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にも有効となる。

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や、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、運用上の負担が課題となり、結果として医療情報システムが適切に運用できないことも想定される。

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して利用することも想定されるため、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、証跡の性格上、レビューする対象が多いことなどで作業負担が大きくなる場合があるほか、発見までの間に不正な利用が継続してしまうなどのリスクがあることから、レビューの対象や周期などについては、バランスを勘案する必要がある。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必要がある。

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、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。

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 経営層がリスク評価を踏まえた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。

また、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。

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 Q27001:2014 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できるようにするため、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。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。

－ 保存した情報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、情報漏洩や、誤った閲覧（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、国内法の適用を受けることを確認すること。

⑥ 外部保存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 不正ソフト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　「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」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）

・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

・AICPA SOC2（日本公認会計士協会 IT7 号）

・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会 IT2 号）

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

・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、情報漏洩や、誤った閲覧（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、改善が必要である場合にはその旨を求めること。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、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取り扱い、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。そのため、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が求められる。

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としての事業者だけではなく、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。また教育に関しては、就業時においても実施することが求められる。

教育の内容のうち、医療情報システムの利用に関連する内容については、企画管理者は、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、サイバー攻撃への対策や対応について、職員への教育を実施する必要がある。

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。

医療機関等が外部のシステム関連事業者との契約に基づいて、当該事業者に委託し安全を確保した場所に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なくてはならない。

企画管理者は、このような観点から、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して、選定することが求められる。

また、企画管理者は、重要度の高い委託の場合は、経営層に丁寧に報告の上、承認を得ることが求められる。

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という観点から、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。

医療情報の外部保存を委託する医療機関等は、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、外部保存を終了しなければならない医療情報が、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外部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委託元の医療機関等と委託先事業者との間で取り交わす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、事前に医療情報の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べきである。

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に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。

委託元の医療機関等及び委託先事業者は、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、この点についても患者の理解を得た上で行うことが必要である。

そこで、企画管理者は、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、理解を得ることが求められる。

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 医療機関等において保有する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必要がある。

企画管理者はこのような観点から、情報管理方針を策定し、経営層による承認を得ることが求められる。

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ことから、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必要がある。

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。

また、医療情報については、漏洩や不正利用を防ぐ観点から、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

医療機関等が保有する情報について安全な管理がなされているかどうかを確認するため、企画管理者は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等）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必要がある。

患者の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、各患者の医療情報が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ついては、適切に行われなければ、漏洩のリスクを伴う。そのため、組織として情報又は情報機器の持ち出しをどのように取り扱うかを整理した方針が必要である。この点、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。

医療情報の持ち出しについては、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、誤送信等のリスクの方が大きいことから、人的安全管理対策と併せて対応する必要がある。

このような対応を図るため、企画管理者は、医療情報の持ち出しに関する手順等を策定し、職員等の教育など人的管理対策の中で周知を図る等の対応が必要である。

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、記録媒体や記録可能な情報機器等への医療情報の格納による持ち出しが想定される。記録媒体や情報機器等による持ち出しは、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不正ソフト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。

企画管理者は、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策定

等を行うことが求められる。

また、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も求められる。

さらに、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も必要となる。

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等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、ネットワークサービスを通じた医療情報の持ち出しについても、企画管理者は適切な対応を講じることが求められる。

企画管理者は、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が求められる。

また、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や医療情報の保存場所に、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
- 患者等が、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、システム関連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について、これを認めるかどうか、認める場合には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も求められる。

患者等が自らの情報にアクセスする場合には、患者に対して必要な説明を行い、責任範囲等を明らかにすることも必要となる。

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利用の誤りにより医療情報が漏洩した場合には、組織として速やかに必要な対応を行う必要がある。

そのため、企画管理者は情報管理規程や運用管理規程等において、初期対応などについて定めておく必要がある。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求められる。

また、漏洩又はその可能性がある場合には、医療情報の漏洩が生じた場合の対応（「３．１．５　非常時等の体制・CSIRT 等の整備」）や、非常時の対応（「１１．３　非常時の事象が生じた際の対応」）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

医療機関等から外部への医療情報の持ち出しは、基本的には限定された場合で生じることから、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。

企画管理者は、定期的に医療情報の持ち出し状況をレビューし、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が求められる。

８．３　医療情報の破棄

８．３．１　破棄の手順等の策定

医療機関等が管理する医療情報について、安全性を確保した上で適切に破棄するために必要な対応等を含む手順の策定が必要となる。当該手順には、情報種別や管理形態（紙媒体、システム管理等）、また破棄対象が情報だけか、記録媒体も対象かなどの違いに応じた内容を示すことが求められる。

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、適切に破棄しなければ、漏洩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

外部保存をシステム関連事業者に委託している場合、委託先事業者において医療情報を破棄する際、医療機関等においても適切に破棄されたことを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必要がある。

また、クラウドサービスの場合など、破棄の証明を行うことが難しい場合もある。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になる。その上で、委託先事業者における破棄の手順や基準が、医療機関等が定め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が求められる。

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。

⑤ 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。

⑥ 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（Bring Your Own Device：個人保有の情報機器）の利用による端末）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。

⑦ 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認するためには、医療情報システムで用いることを予定している情報機器等の所在が明らかになっているか、またそれらの情報機器等が使用できる状態なのか否か等を、適切に管理する必要がある。

そのため、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できるように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などが想定される。また、医療情報システムの適切な利用という観点では、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も管理対象として想定される。

医療情報システムの利用に際しては、医療機関等が管理しない情報機器等の利用も想定される。例えば BYOD（Bring Your Own Device：個人保有の情報機器）の利用などが想定される。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、利用可能としたものについては、併せて台帳管理することが求められる。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が求められる。

また、整備した台帳を定期的に棚卸して、適切な状況にあることを確認する必要がある。

９．２　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、EOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）の対象となっていないことなどを確認することが重要である。

情報機器等の安全性の確認を行うためには、情報機器等の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、担当者に情報機器等の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で、情報機器等の安全性を定期的に確認する必要がある。

安全性の確認は、情報機器だけではなく、利用するサービスも対象である。サービスの場合、当該サービスを提供するシステム関連事業者に対して、利用に適した状況にあることを定期的に確認する旨、委託契約等に含めることなどが想定される。

また、クラウドサービスなどのサービスの場合は、サービス内容によっては、利用できる情報システムの容量などが定められていることなどにより、必要な容量を確保できないなどといった、可用性の観点から考えられるリスクも想定される。システム関連事業者に対しては、このような観点からの確認も適宜求めていく必要がある。

９．３　情報機器等の資産管理状況の報告

医療情報システムで利用する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。企画管理者は、情報機器等の管理状況を把握するに際しては、担当者と協議の上、資料を整理する必要がある。

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、企画管理者やシステム運用担当者は、自ら通常時の運用状況を確認することが重要である。

よって、企画管理者は、自ら組織的な対応について日頃の管理の状況を点検し、適切に運用できているかどうか、改善点があるとすればそれはどこか、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

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担保するために、第三者による確認や監査を行うことは重要でかつ有効である。

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り、監査への対応の負担が過大となり本末転倒な事態にならないように留意が必要である。

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とともに、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措置を講じ、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、経営層の承認を得ること。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ること。

② 医療機関等が定める非常時の定義や BCP（Business Continuity Plan：事業継続計画）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 非常時へ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 非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。

⑨ 非常時の事象が生じた場合、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。

⑩ 非常時の事象発生に伴い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

非常時においても医療機関等が医療サービスを継続して提供できるようにするため、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て非常時となった場合に、

・医療機関等において医療サービスの提供をどのように継続するか

・継続する場合にどの医療情報システムをどのように利用するか

等を経営層及び非常時における意思決定担当者は総合的に見て判断する必要がある。

企画管理者はこのような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。内容としては、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が求められる。併せて非常時対応をする起点となる「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、承認を得る必要がある。

医療情報システム・サービスを取り巻く非常時の事象が発生する原因としては、主に災害、サイバー攻撃、システム障害などが挙げられる。それぞれの原因に対して、具体的な対応が異なることから、対応方針や手順等を策定する際も、具体的な非常時の事象発生原因や被害の規模等を勘案して、それぞれの内容を整理することが求められる。

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洩　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、非常時の際に法令で求められる対応についても、非常時に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

非常時の事象が生じた際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、非常時の事象が生じた際の具体的な手順等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や冗長化等が挙げられる。

具体的な考え方については、非常時の事象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ほか、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事象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、経営層への報告や承認を行うことが求められる。

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 ・非常時における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 ・発災直後の非常時の運用から、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（大規模広域災害等の場合の対応（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リスク低減	・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／物理的なネットワークの構成分割、追記不能型のデータバックアップなど）　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　非常時の事象が生じた際の対応

非常時の事象が生じた際の対応としては、主に状況把握・拡大防止・原因究明等への対応と、通常時への復旧・復帰に向けた対応などがある。

非常時の事象が生じた際には、あらかじめ準備した手順等に基づいて、適切に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事象発生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　非常時の事象発生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 ・不正アクセスや不正ソフト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	・被害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	障害発生時のリスク回避や	・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

非常時の原因	必要な対応	求められる対応や措置例
（ネットワーク障害含む。）	リスク低減	
	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、医療機関等の職員等や委託先事業者などの対策を検討し、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 医療機関等において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。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事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をあらかじめ整理した上で、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、個人情報の漏洩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事象による非常時対応が生じた場合には、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事象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

非常時の事象発生原因の一つであるサイバー攻撃は、攻撃者が悪意を以て攻撃する犯罪であり、その方法も様々な形で、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がされることもあるため、システム側のみで十分な防御ができないこともあり、対策を難しくしている。

企画管理者は、サイバーセキュリティ対応に際して、具体的にどのような攻撃等があるのか、医療機関等をはじめ、企業や行政機関等でどのような被害が生じているのか等のサイバーセキュリティ対応の必要性に関する実情把握は重要である。

その上で、医療機関等としての対策として、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。

これらを踏まえて、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、経営層の承認を踏まえて、組織としての対応計画を整備する必要がある。

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。通常時の対策について適切に実施することで、攻撃に備えるとともに、非常時における対策として対応計画に盛り込んだ事項が実際に攻撃を受けた際に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。そのため、企画管理者は、担当者と協働して、定期的にサイバー攻撃等のサイバーセキュリティに関する非常時対応が発生したことを想定した訓練や機能テストなどを行う必要がある。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。

また、サイバー攻撃に関しては、あらかじめ対応することが可能であったにもかかわらず、情報機器等の脆弱性や利用者の過失等を対象として攻撃を受け、被害が生じている事象もみられることから、通常時における情報収集や点検、未然防止策の検討を行う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。

また、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が重要である。

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、あらかじめ策定した対応計画等に従って対応することとなる。場合によっては、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ため、そのような場合に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必要がある。また、被害拡大を防止する観点から、医療機関等内の職員やシステム関連事業者だけではなく、非常時対応として臨時的に医療情報システムに接続する関係者に対しても、速やかに連絡・情報共有する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等及びアクセス権限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たものとなっていることが前提となるよう管理すること。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。医療情報システムの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。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 医療情報システムの管理権限や、医療情報システム、情報機器等で用いる ID 等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて利用される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するよう指示すること。システム等で用いる ID 等については、担当者に安全性の確認を指示し、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、不要なものについては削除すること。棚卸については、担当者に具体的な手順等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

医療情報システムにおける利用者認証に関するルールを策定するに際して、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。

医療情報システムにおける利用者としては、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、医療情報システムにおける自身の情報を参照する患者等の医療機関等の外部の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利用者に付与される ID や、医療情報システムのソフトウェア、医療情報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、医療情報システムの利用者の種類などを整理し、その利用目的に応じて、利用者に付与される ID 又はソフトウェアや情報機器等に利用される ID の運用規則等を定めることが求められる。

１３．１．２　医療情報システムの利用者の登録と認証

医療情報システムの利用者について、適切な情報セキュリティを確保する観点から、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。医療情報システムにおいては、機微な情報を取り扱うという観点から、利用者の登録や利用者を認証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。

利用者の登録においては、高い強度の身元確認を行うことが必要であるとされ、対面又はこれに準じた形で確認することが求められる[6]。医療機関等においては、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、職員登録の内容を確認した上で、これと整合性が取れる形で利用者登録を行う必要がある。職員が退職するなどの場合も、職員登録からの削除状況に応じて、医療情報システムの利用者登録からも削除することが求められる。

---

[6]「Digital Identity Guidelines」（NIST　SP800-63）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（身元識別情報が特定された担当者の対面で確認され、身分確認の信用度が非常に高い）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（身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある）以上が望ましいとされる。（レベル区分については「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成 31 年 2 月 25 日 CIO 連絡会議決定）のレベル区分を参照。）

登録された ID を利用する際の当人認証についても、医療情報を取り扱う医療情報システムにおいては、厳格な認証方法が求められており[7]、複数（多要素）認証によること等が求められるとされる。そこで、医療情報システムでは、複数認証かこれに準じた方法や頑強性を持った方法が求められる。

企画管理者は、身元確認と当人認証の本人確認の方法について、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

医療情報システムを利用する際には、実際に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。権限の付与に際しても、基本的には医療機関等の内部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設定される必要がある。

また、医療情報システムのシステム上は利用権限が付与されているにもかかわらず、医療機関等内の個別のルールなどによって、その利用場面が限定されていたり、原則として利用しないこととされていたりする場合もある。このような場合には、システムの利用ルールについては規程等として文書化するなどにより、権限の範囲を明確にすることも重要である。

企画管理者は、このような権限設定に関するルールについても、アクセス管理に関する規程等で示すことが求められる。

１３．２　電子カルテにおける記録の確定

「施行通知」では、電子カルテにおける記録の確定に関して、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の必要性を定めている。

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、運用管理規程等に定めた内容に対応する措置を医療情報システムに反映するよう指示し、管理する必要がある。

---

[7]「Digital Identity Guidelines」（NIST　SP800-63)では、当人認証は AAL（Authentication 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、AAL：Level 3（認証要求者が身元識別情報と紐付けられており、認証情報の 3 要素（知識情報、所持情報、生体情報）のうち耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い）以上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、AAL：Level 2（認証要求者が身元識別情報と紐付けられており、認証情報の 3 要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある）以上が望ましいとされる。（レベル区分については「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成 31 年 2 月 25 日 CIO 連絡会議決定）のレベル区分を参照。）

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、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保健医療福祉分野 PKI 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。

保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、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の検証を正しくできることが必要である。

(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、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。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」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医師等の国家資格保有の確認は、

①　利用者が保健医療福祉分野PKI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

②　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

③　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

④　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、①～③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。④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。）。

－　医療機関等による医師等の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とともに、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、さらに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。

※　①～④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」（平成14年法律第153号）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医

師等の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」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。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者（タイムビジネスに係る指針等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者。以下「認定時刻認証事業者」という。）については、令和 4 年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。

(2) 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、また、e-文書法の対象範囲となる医療関係文書として e-文書法省令において指定された文書においては、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（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）に加え、リモート署名（クラウド上のサーバに利用者（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をいう。以下同じ。）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）や、クラウド技術を活用した立会人型電子署名（利用者の指示に基づき電子署名サービス提供事業者（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をいう。以下同じ。）自身の署名鍵による暗号化等を行う電子署名）を用いたサービスが登場しているが、電子署名法第 2 条第 1 項の要件を満たすものについては、電子署名法における電子署名に該当する。なお、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ことから、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が求められる。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。

また、施行通知に示される電磁的記録の保存等を行うことができる文書は、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を定めている。

医療分野における電子署名に係る争訟が生じた場合に備え、立証責任を軽減したい医療機関等においては、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や、電子署名が本人の意思に基づき行われたものであること等の措置を講ずる手段も存在することに留意すること。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。

さらに、医療分野においては、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。これらに関しては、多くはその証明として記名・押印が求められており、記名・押印をすることは、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ことになる。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場合の考え方を「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を用いることで、それを担保することが可能となる。

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できることが必要である。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できないという特徴がある。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。

したがって、電子署名を付与する際はこのような点を考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名の検証が継続できる必要がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、ISO規格として制定されている（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)。

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あり、システム更新や検証システムの互換性等の観点からも、標準技術を用いる等して適切に保存することが望ましい。したがって、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行うことができるようにすることが重要である。

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）ものである。

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にするため、「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とともに、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が求められる。(なお、法令保存期間等がない文書については、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用することも可能である。)

また、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必要がある。

加えて、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ため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。

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について、リスク評価を踏まえて、その場所の選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において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。

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（不正ソフト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について、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において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行った場合には、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、漏洩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内容とすること。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、その状況を把握の上、経営層に報告し承認を得ること。

１５．１　技術的な対応の管理

企画管理者は、医療機関等における医療情報システムの安全管理として、通常時から様々な運用管理を担う。そのため、医療情報システムの全般に対して、経営層に代わって管理する職務を負うこととされる。

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、医療情報システム・サービスに関する専門的な知見なども必要であることから、これを有する担当者に委ねることになる。この場合、企画管理者は、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が想定される。

この場合、企画管理者は、医療情報システムの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、通常時における医療情報システムの運用、システム関連事業者からの情報収集等については、担当者において実施するよう指示した上で、実施状況の報告を受けて状況を把握することになる。そして、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していくことが求められる。

１６．紙媒体等で作成した医療情報の電子化

【遵守事項】

① 紙媒体で作成した医療情報を含む文書等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と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 紙媒体で作成した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 企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。

・ 情報作成管理者が、スキャナによる読み取り作業が適正な手続で確実に実施される措置を講

じる旨を運用管理規程等に定めること。
・　電子化した後、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の保存等を行うことができる文書を、スキャナ等により電子化して保存する場合が想定される。具体的には、

・　電子カルテ等の運用において、診療の大部分が電子化された状態で行われている一方、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避けられない事情がある場合
・　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、又は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、医療に関する業務等に支障が生じることのないことを確認しつつ整理し、運用管理規程等に定めることが求められる。

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

電子カルテ等の運用において、診療の大部分が電子化された状態で行われていながら、他院から紙やフィルムの媒体による診療情報提供書等を受け入れることが避けられない事情がある場合、媒体が混在することにより医療安全上の問題が生じるおそれがある。このような場合等に、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が想定される。

企画管理者は、このような場合を想定して、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、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よう、運用管理規程等に定めることが求められる。

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、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の媒体で残り、一貫した運用ができない場合が想定される。この場合には、「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」の状況と異なり、説明責任を果たすために相応の対策を行うことが求められる。そのため、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、患者等の事前の同意を得て、厳格な監査を実施することが必要である。

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が求められる。

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、紙の処方箋に記名押印又は署名を行い調剤済みとしたもの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)。

また、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、その後に内容の修正が発生することを完全には否定できない（例：記載事項を確認したものの修正を忘れた場合等)。そのため、一旦電子化した紙の調剤済み処方箋であっても、その修正が発生する可能性がある。

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、遵守事項⑦に記載のとおり、状況を踏まえた対応を行うことが必要である。

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

紙等の媒体で扱うことが著しく利便性を欠くためにスキャナ等で電子化するが、紙等の媒体の保存は継続して行う場合、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。しかしながら、個人情報保護上の配慮は同等に行う必要があり、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 6.0 版

システム運用編

[Control]

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。

＜医療機関等の特性に応じたガイドライン参照箇所＞

[医療機関等の特性についての考え方]

本ガイドラインは、すべての医療機関等における医療情報システムを対象とした安全管理に関して、各編で遵守事項や考え方等を示している。

医療機関等の組織体制や、稼働している医療情報システムの構成、採用しているサービス形態等の特性は様々であるため、それぞれの医療機関等の特性に応じたかたちで本ガイドラインを遵守していただく必要がある。そのため、以下のとおり、医療機関等の特性ごとに、医療機関等が必要な安全管理を確保するために本ガイドラインで最低限参照すべき箇所について明記する。

具体的には、医療機関等における専任のシステム運用担当者の有無と導入している医療情報システムの形態に応じた、４種の参照パターンを例示する。自施設の特性を分析した上で、最も近しい参照パターンに基づく対応を行っていただきたい。（なお、参照パターンに示した参照箇所以外の箇所についても、必要に応じてご参照いただきたい。）

医療機関等の特性に応じた本ガイドラインの参照パターン

	医療情報システムを 医療機関等に保有し運用 （いわゆるオンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆるクラウドサービス型）
システム運用専任の 担当者がいる	Ⅰ	Ⅱ
システム運用専任の 担当者がいない	Ⅲ	Ⅳ

なお、医療機関等において、カルテ等の医療情報を紙媒体で扱い、情報システム上では医療情報を扱わない業務のみ行なっている場合でも、医療機関等内の端末上やシステムとの連携によって、医療機関等外の医療情報へのアクセスが発生する場合、参照パターンⅡやⅣに基づき本ガイドラインを参照する必要がある。

ただし、システム全体の構成等により、参照パターンが異なるので、必要に応じて、システムの提供元である医療情報システム・サービス事業者に参照パターンを確認すること。

［医療機関等の特性に応じたシステム運用編の参照箇所］

上記「医療機関等の特性に応じた本ガイドラインの参照パターン」によるシステム運用編の参照箇所の詳細を下表に示す。

パターン	システム運用編
Ⅰ 担当者あり	すべて参照
Ⅱ 担当者あり クラウド	以下項目は参照 １～４、６～８、１１、１２．３、１４，１８ ※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。
Ⅲ 担当者なし	すべて参照 ※「担当者」という記載を「企画管理者」に置換し、参照
Ⅳ 担当者なし クラウド	以下項目は参照 １～４、6～８、１１、１２．３、１４，１８ ※「担当者」という記載を「企画管理者」に置換し、参照。 ※ 他の項目は、医療情報システムの構成に応じて、当該情報システム・サービス事業者に確認し、事業者と締結する契約等に含まれている場合は、簡略化が可能。

[システム運用編における参照パターンの付記]

システム運用編では、各章のタイトルの末尾に、以下のように、参照パターンを付記している。

１．情報セキュリティの基本的な考え方　[Ⅰ～Ⅳ]

↑

波線部の[　]内が参照パターンを示す。

１．情報セキュリティの基本的な考え方　　[Ⅰ～Ⅳ]

【遵守事項】

① 法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、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、システム運用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技術的な対応を行う必要がある。

特に、

- 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

等において必要な措置を行うことが求められる。

２．システム設計・運用に必要な規程類と文書体系　［Ⅰ～Ⅳ］

【遵守事項】

① 医療情報システムにおいて採用するシステム、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 医療情報システムの利用者が適切に医療情報システムの利用ができるよう、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、技術的な対応に関する実際の運用に求められる手順や、医療情報システム等を構築するのに必要な資料等を整備することが求められる。これらの資料は、最新のものであることが不可欠である。古い手順や技術資料が混入する場合に、脆弱性が残ったり、正常な情報システムの稼働が損なわれたりするなどのリスクが生じる。

システム運用担当者は、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が求められる。非常時の場合には、特に体制面や情報照会・収集の対象などについても明らかにすることが重要である。

3．責任分界　［Ⅰ～Ⅳ］

【遵守事項】

① 医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容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、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。

③ 通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である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に、技術的な対応や対外的な説明に関して必要な役割について、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の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、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

医療情報システムを委託する場合、提供される情報システム・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することができないものも含まれている。

従って、提供する情報システム・サービスの要求仕様に対する適合性に関しては、情報システム・サービス事業者（以下「事業者」という。）から資料の提供を受けるとともに、提供された情報が正確なものであることを確認する必要がある。

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が求められる。

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に際して、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、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」においては、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おり、その基礎となる内容はサービス仕様適合開示書等により示されている。

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し、必要があれば個別の調整を事業者と行うなどにより、技術的な対応に関するリスク分担などを行うことが求められる。

またクラウドサービスなどを利用する場合には、利用者側でも技術的な対応に関する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、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。

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

通常時の運用における責任分界は、技術的な対応という点で見ると主に、運用責任や管理責任などについて取り決めることになる。情報システム・サービスが提供される際の医療情報システムの運用が、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内容もあるため、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が求められる。その際、事業者が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、具体的なシステムの運用や管理などについては、事業者に役割を委ねることが求められる。

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責任分界は、技術的な対応という点で見ると主に、被害の拡大防止や原因究明などシステム対応に関する内容のほか、外部への説明責任に関する支援などについて、取り決めることが求められる。

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データ等の資料などを併せて検討することが求められるため、それぞれの役割の分担などを取り決めておくことが求められる。

特にサイバー攻撃による被害を受けた場合には、原因究明に際して専門的な知見が必要となり、この場合の責任分担などは非常に重要である。

外部への説明責任についても、事業者でしか、技術的にもわからない部分が存在することがあるため、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場合がある。

クラウドサービスの場合には、医療情報システムで利用する資源について SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）などの類型で提供することがある。

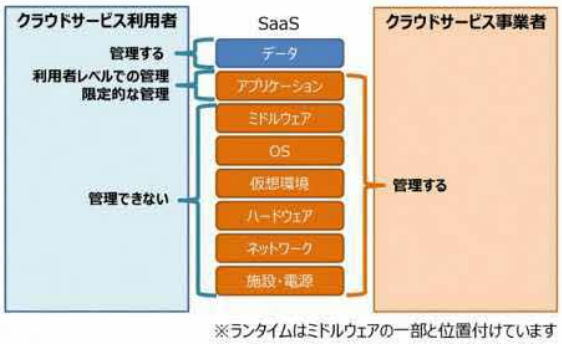
SaaS では、医療情報システムのアプリケーション部分、PaaS では、医療情報システムが利用するミドルウェアの部分、IaaS では医療情報システムが利用するインフラの部分をサービスとして提供することになる。

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、委託により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、委託により医療機関等が行うべき安全管理のうち、どの部分の責任を分担し、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が求められる。

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、クラウドサービス事業者が提供する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

医療機関等が事業者に委託を行う場合、この情報システム・サービスを利用するに際して複数の事業者が関与する場合がある。

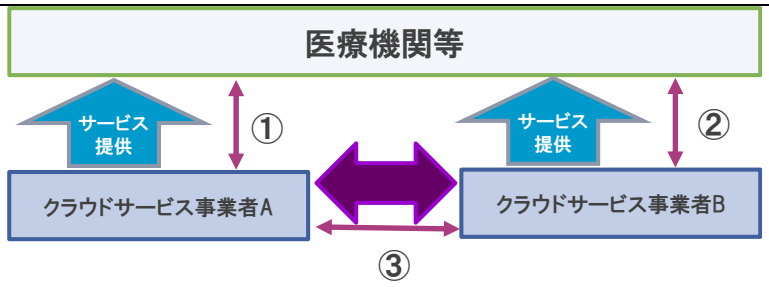
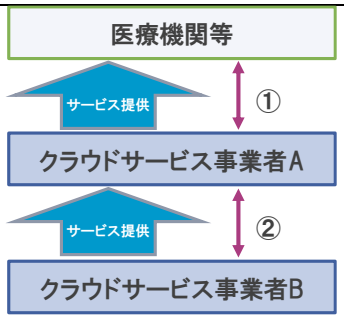
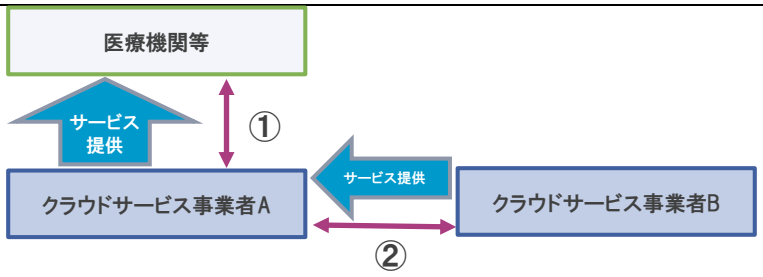
医療機関等が複数の情報システム・サービスのサービスを組み合わせて利用するような場合と、事業者が複数のサービスを組み合わせて、医療機関等に提供する場合などが想定される（表３－２参照）。

前者では、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が求められる。これは、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と、最終的に情報システム・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になる。この場合、事業者が利用する他の事業者のサービスとの関係では、再委託などの関係になることが多いので、これに従って取決めを行う。

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が求められる。

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

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、

・メール等による情報の送信

・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

等が想定される。

この場合、提供方法により利用する技術的な対応に応じて、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を定める。例えば、メールによる送信であれば、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、提供先への到着まで責任を有する等を決定することになる。

システム運用担当者は、このような具体的な内容について、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。

４．リスクアセスメントを踏まえた安全管理対策の設計　［Ⅰ～Ⅳ］

【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、患者情報については、患者ごとに識別できるような措置を講じること。

② 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「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」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

医療機関等において、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医療機関等が保有する情報の棚卸を行うことになる。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、各システムにおいて、それぞれどのくらいの患者数のどのような情報が保管されているのか、それらの利用者の範囲や利用権限がどのように整理されているのか、などを整理するなどが挙げられる。併せて、バックアップなどについても、どのくらいの医療情報が、どこでどのような形で保管されているか、その他持出し対象となっている医療情報の状況なども把握することが求められる。

医療情報システムに関する情報は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等)、各医療情報システムを構築・導入するのに必要な資料等の管理状況（保管場所、作成時期等)、運用において必要な設定に関する情報やログ等に関する管理状況などを把握することなどが挙げられる。

情報種別を行う際に、法令により保存などの要件が求められているものについては、その状況も併せて確認する必要がある。「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。）などが求める内容に則しているか等が挙げられる。

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、医療機関等が保有する医療情報等の情報種別や重要度を整理したうえで、リスクアセスメント（リスク分析、リスク評価）を企画管理者と行い、その結果を踏まえて、具体的な安全管理のための技術的な対応について、実装し、運用することになる。

医療情報システムの安全管理のための対策を、リスクアセスメント結果を踏まえて講じる場合には、医療機関等ごとの組織や規模等の実情や、医療情報システムの利用形態等のリスクに応じて、さまざま方法が挙げられる。また実装の検討に際しては、医療機関等における対応できる負担（要員、費用等）などを踏まえることも求められる。

そのため、安全管理対策の設計においては専門的な知見なども求められるが、医療機関等においては、必ずしもこのようなリスクアセスメントに基づく安全管理対策を行うのに十分な資源（要員、費用等）を有していないこともある。このような場合には、利用を想定する事業者において行うリスクアセスメントと、これを踏まえた技術的な対応における対策などを参考にすることなどが考えられる。なお事業者からは、「サービス仕様適合開示書」の提示を受けることが想定される。

特に専任の情報システムの要員がいない医療機関等の場合には、安全な医療情報システム・サービスを事業者から導入し、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、このような方法も含めて、リスクアセスメントを踏まえた技術的な対応における措置を整理し、企画管理者に報告することが求められる。

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）　［Ⅰ、Ⅲ］

【遵守事項】

① システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、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、それぞれ出力及び入力できる機能を備えるようにすること。

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。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。

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すること。

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

医療機関等の情報化においては、情報利用についての従来の指示、報告、連絡等の意思の共有等の業務を単に電子化するだけでなく、その電子化された情報の再利用が可能であれば、幾度もの同一情報の入力作業を軽減し、業務の総量を減ずることも求められている。また紙等の情報を読解して再入力する際のミスの防止、指示の誤記・誤読の防止という観点から、医療安全に資することにもなる。

このような電子化された情報のやりとりを、段階的に導入されたシステム間や、異なるシステムベンダ及びサービス事業者から提供されたシステム間で行う際に必要となるのが、相互運用性の確保である。

一方、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、情報を利用する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、医療機関等で医療情報を長期間保存する際に、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も意味する。

さらに、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、相互運用性の考え方は重要である。

このような医療情報の相互運用性を確保するためには、誰もが参照可能かつ利用可能で将来にわたり保守（メンテナンス）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）を利用するか、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、これを推奨する等の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ところである。

医療機関等において、自らこれらの用語・コードの保守（メンテナンス）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に向けて、システムベンダ及びサービス事業者にこういったこと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、医療情報システムを導入しようとするときや、現に保有する医療情報システムの運用に当たっても、下記のこと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データ項目、データ形式等のほか、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、遵守事項に示す内容が求められていることから、対象となる文書の電子化においては、標準化に対する措置が求められる。

6．安全管理を実現するための技術的対策の体系　［Ⅰ～Ⅳ］

【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）

医療情報システムにおいては、医療従事者のほか職員などの利用に関する情報資産、利用者が利用する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、医療機関情報システムが利用するインフラに関する情報資産などから構成される。またそれらに共通して求められるセキュリティに関連する内容も共通する要素となる。

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対応としての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

医療機関等が利用する医療情報システムは、今日、さまざまな形態のものがある。例えば

- 医療機関等の内部で自ら開発するシステムやサービス（例えばアプリケーションのマクロ機能などを使ったり、簡易データベースソフトを用いて構築したりする場合等）
- 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もの（例えば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場合等）
- 事業者が提供するアプリケーションサービスを用いて、運用も含めて外部に委託する場合（クラウドサービスの利用等）

等がある。

医療機関等のシステム運用担当者が直接対応するべき内容も、このような医療情報システムの形態により異なってくることに留意する必要がある。

また医療機関等の組織によっては、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こともある。この場合には、技術的な対応に関する内容の多くは、外部委託によることになる。

このように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、システム運用担当者の職務を行う者は、事業者にその実施状況の確認を適切に行うことが求められる。

7．情報管理（管理・持出し・破棄等）　［Ⅰ～Ⅳ］

【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したりする場合は、不正ソフト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、情報端末が情報漏洩、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 持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、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か、業務に対して影響がないことを確認すること。

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。併せて定期的に棚卸を行う手順を作成する。

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医療機関等への連絡方法について、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 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。

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記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき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、医療機関等の外部への医療情報の持出しに関する具体的な手順を、企画管理者が策定する規程を踏まえて作成する。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。また手順における策定対象は、持出し前の手続から、外部からの持ち帰り等に至るまでを想定する。

記録媒体や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が求められる。例えば端末自体の起動パスワード等の設定は必須であり、認証等のルールに沿った内容であることが求められる。また記録媒体や端末内に患者等の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、アクセス先に存在する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求められる。

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ようにする旨や、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なども有効である。

持出しについて、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してもよい保存先やネットワーク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。クラウドサービスの中には、医療機関等が定める安全管理の基準を満たさないものや、プライバシーポリシー、その他のルールが、医療機関が定めるものと整合性が取れないこともある。

システム運用担当者は、例えば医療機関等が許可したり、管理していないサービス以外の接続ができないようにしたりする等の技術的な対応を取りながら、許可されていないサービスの利用禁止を規則等で盛り込むなどの対応が想定される。

保守等の目的で事業者が、医療機関等から医療情報を持ち出す場合、患者の個人情報を持ち出すことは、漏洩防止等の観点から、原則として禁止する必要がある。業務の必要上、やむを得ず持ち出す場合には、目的や持ち出す個人情報の件数とデータ項目、持出し後の対応や、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得て持ち出す等の手続を定める必要がある。

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、医療機関等の外部から医療情報システムに接続して利用する場合の、技術的対応への方策を講じることが求められる。利用場面としては、下記の場面が想定される。

- 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
- 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

７．２．１　医療機関等の職員による外部からのアクセス

医療機関等の職員がテレワークを含めて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ことを許可することもあり得る。この場合、職員からの接続については、

- 接続できる職員に関する事前の許可
- 外部から接続する際の技術的対応

等が挙げられる。事前の許可については、具体的な手続等について、システム運用担当者で手順等を定めて、外部から接続できる利用者と利用権限の範囲を設定するための手続を行い、その結果を企画管理者に報告するなどの対応が必要となる。

技術的な対応については、

- 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

等の措置を、システム運用担当者は講じる必要がある。

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を行う措置を講じることが求められる。認証等の要件は、「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」に示す。

外部から利用する場合のネットワークについては、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を経由することが想定される。この場合、「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」に示すオープンなネットワークを利用する場合の対策を講じたうえで、チャネル・セキュリティが確実に確保される措置を講じることが必要である。

外部から利用する端末等の要件については、医療機関等が管理する端末を使うことが想定されるが、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対する安全管理措置」に示す措置を講じて、個人の所有する、あるいは個人の管理下にある端末（ノートパソコン、スマートフォン、タブレット等）の業務利用（Bring Your Own Device：以下「BYOD」という。）など医療機関等が管理しない端末を使用することも想定される。端末等の要件に関しては、考慮すべき点が 3 つある。

- PC 等といっても、そ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、一般の職員にその知識と技能を要求することは難しい。
- 運用管理規程や手順等で定めたことが確実に実施されていることを説明するためには適切な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、監査することは通常は困難である。
- 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等が管理する情報機器を使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性がある。

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。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表示する仕組みであること。これ以外には、ユーザー権限を厳格に管理した専用端末の貸与等が考えられる。

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む中、ネットワークを介して患者等に診療情報等を提供したり、患者等が医療機関等内の診療情報等を参照閲覧させたりす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、システム運用担当者は、ネットワークのセキュリティ対策、医療機関等内部の医療情報システム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。

ネットワーク対策等に関しては、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が求められる。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が求められる。

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、医療情報の破棄について企画管理者が作成した手順を踏まえて、情報種別ごとに破棄の具体的なルール等を作成することが求められる。

破棄の対象となるのは、

- 医療情報を格納した情報機器等（過去に格納して消去したものを含む）
- 医療情報システムのデータベース等に格納したデータ

等が想定される。

医療情報を格納した情報機器等については、単に OS 上のファイル管理システム上だけの削除では足りず、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により破棄することが求められる。なお、より確実なのは記録媒体などを物理的に破壊するなどが挙げられる。なお、リース等による情報機器等の返却についても、同様の措置が求められる。なお情報機器等の破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破棄に関する証明や証跡の提供などを求めて、確認することが求められる。

医療情報システムのデータベース等に格納したデータの削除については、通常利用するデータに関しては、システム管理機能が持つ削除等の機能によることになる。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したために、その他の情報が利用不可能になる場合もあるため、留意することが必要である。

外部保存などにより、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には、破棄の証明等が難しい場合も想定される。このような場合には、企画管理者と協働して、システム運用担当者は事業者のデータの破棄の手順などを確認して、破棄の状況を確認することが求められる。

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記録媒体、情報機器等の紛失、盗難が生じた場合の対応に関する手順等を作成することが求められる。紛失や盗難に関する報告を受けた場合に、対象となる記録媒体や情報機器等の特定、情報機器等の利用を目的として ID 等を発行している場合には、医療機関等におけるネットワークの接続防止等が挙げられる。また、事前に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求められる。

なお、ネットワークを通じて外部サービスを利用した際に、設定のミスなどにより漏洩のリスクが生じた場合についても、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　［Ⅰ～Ⅳ］

【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不正なソフト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 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・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、不正ソフト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）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。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 情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の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とともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。

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。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。

(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 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器の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) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。

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 の実施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 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　不正ソフトウェア対策

コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ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入る可能性がある。不正ソフトウェアの侵入に際して適切な保護対策が行われていなければ、セキュリティ機構の破壊、システムダウン、情報の漏洩や改ざん、情報の破壊、資源の不正使用等の重大な問題が引き起こされる。また不正ソフトウェアの侵入は、何らかの問題が発生して初めて気付くことが多い。

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、このような不正ソフト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が求められる。

ただし、これらの不正ソフト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、医療機関等のシステムの環境等の状況を勘案して、可能な限り、常に最新のものに更新しておく必要がある。システム運用担当者は、パターンファイルの更新に先立ち、医療情報システムへの影響等に関する情報を収集することも求められる。

また、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、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、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。そのために実施すべき対策として、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非活性化、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）や「振る舞い検知」などの方策も有効である。なお、いずれの対策を行う場合も、対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要である。

また、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ることから、これらの情報機器等についても、上記の対応を行うことが求められる。

８．２　情報機器等の脆弱性への対策

企画管理者は、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。

医療機関等において、医療情報システムが利用する情報機器等には、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、様々なものが挙げられる。

サイバー攻撃においては、近年は、情報機器等に内蔵されるファームウェアや、情報機器等に格納されるプログラム等の脆弱性、EOS（End of Sales, Support, Service：販売終了、サポート終了、サービス終了）の対象となった情報機器等を攻撃して、外部から攻撃するなどが多くみられている。特にランサムウェアなどのケースでは、必要な脆弱性対策が見逃されたことに起因するものも見られる。

システム運用担当者においては、医療機関等において利用している情報機器等に関して、どのような脆弱性があるか、最新の情報を収集することが求められる。PC 等の OS などに関する情報は、OS や不正ソフトウェア対策ソフトウェアを提供する事業者などが提供しているほか、重要なセキュリティ関する情報は、「内閣サイバーセキュリティセンター（NISC)」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、必要に応じて利用する情報機器等やソフトウェアを提供する事業者に対応を確認するなどして、最新の情報の入手を図ることが重要である。そのうえで、必要に応じて速やかに脆弱性対策を講じることが求められる。その際に、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ことから、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、代替策を講じる必要がある。

なお、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。

本ガイドラインにおいては、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いるものであり、「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」[1]において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」[2]、「医療機器のサイバーセキュリティ導入に関する手引書」[3]、「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」[4]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も求められる。

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、医療情報システムで利用する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については、必ず製品出荷時のものから変更することが重要である。サーバで利用するソフトウェアの管理者権限を有する ID 等においても同様である。企画管理者はこのような情報機器の起動や初期設定に関する対応を図ることが求められる。

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の稼働は行わない、などの対応も必要である。例えば、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には、その情報機器等が攻撃対象となることも想定される。また医療機関等の業務によっては、明らかに利用する可能性がない（または低い）時間帯を含めて医療情報システムを稼働することにより、業務で利用されない時間帯に攻撃を受けることも想定さ

---

[1] 昭和 35 年 8 月 10 日法律第 145 号

[2] 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」

[3] 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」

[4] 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」

れる。従って、企画管理者は、業務での必要性や利便性などと勘案して、利用する情報機器等や医療情報システムの稼働時間等を整理して、適切な設定を行うことが求められる。

８．４　情報機器等の棚卸

システム運用担当者は、医療情報システムで利用する情報機器等について、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棚卸をすることが求められる。棚卸を行うことにより、医療情報を格納した情報機器を含め、所在確認が明確になるほか、不明な情報機器等についてその所在状況を明確にすることにより、情報の漏洩等の可能性を速やかに発見することが期待される。また棚卸に際して、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、利用可能な情報機器であるのかを把握することができ、バージョンアップや買換え等、必要な方策を講じることが可能となる。なお情報機器等の滅失状況については、必要に応じて最新のソフトウェアへの対応の可否なども含めて、確認することも重要である。

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の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 においては、上記の要件を実現するために、管理者以外による端末の OS の設定の変更を技術的あるいは運用管理上で制御すること、あるいは、技術的対策として、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し、さらに個人でその設定を変更できないようにし、OS レベルで管理領域を分離すること、また、運用による対策として、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こと等、適切な対策を選択・採用し、十分な安全性が確保された上で行う必要がある。コンピュータウイルスや不適切な設定のされたソフトウェアにより、外部からの不正アクセスによって情報が漏洩することも考えられるため、管理されていない端末での BYOD は行わない。管理者が BYOD によるコスト・利便性とリスクを評価して検討することが求められる。

9．ソフトウェア・サービスに対する要求事項　［Ⅰ、Ⅲ］

【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し、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により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の管理を直接行うことが求められる。ソフトウェアの構成を適切に行わないと、医療情報システムの動作に支障をきたしたり、セキュリティ上の脆弱性が放置されたままになったりするなどのリスクが生じる。

ソフトウェアの構成については、ソフトウェアを開発・保守する事業者が行うことが多いが、適切な構成管理を行うための手順などにより行うことが想定される。

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（プログラム）のバージョンなどが適切に管理されているか等を、事業者に確認し、医療情報システムの導入や保守において、構成管理に関する手順に従った計画が策定され、実施されていることを確認することが求められる。

クラウドサービスなどの場合には、このような構成管理を直接、医療機関等が行うことは難しい。従ってクラウドサービスによる場合には、事業者において構成管理等の手順があり、それに基づいて実施していることの確認などを行うことなどが想定される。

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

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おいては、想定した品質で稼働することを確認することが求められる。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。このようなソフトウェアの品質が適切に確保されないと、結果として医療の提供に支障が生じるリスクがある（例えば迅速に診断ができないことにより、診断が滞るなど）。

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このような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などについて明示することで、事業者に品質確保を求めるなどが想定される。

なお、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。施行通知の基礎となるe-文書法の精神によれば、画面上での見読性が確保されていることが求められているが、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が求められることもある。品質を満たすかどうかについては、このような観点も考慮することが重要である。

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[Ⅰ、Ⅲ]

【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おいては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、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が必要である。

③ 保守を実施する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個人情報にアクセスした場合の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（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し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。

⑤ リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、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。

⑥ 診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

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（メンテナンス）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るが、特に障害対応においては、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とがある。この場合、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十分な対策が必要になる。

具体的には、

- 保守要員等からの医療情報の流出・漏洩
- 保守に伴う医療情報システムにおける医療情報の破壊・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

等が想定される。

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必要がある。

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
・　影響確認
・　作業の監督
・　作業報告・確認
・　アクセス権限管理
・　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

保守に関する手続きは、原則として事前申請・承認であるが、障害時や緊急を要する脆弱性対応などにおいては、事後承認など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。

１１．システム運用管理（通常時・非常時等）　　[Ⅰ～Ⅳ]

【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。

－ 「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。

－ 非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。

－ 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。

－ 医療情報システムに不正ソフト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。

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

－ 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、その一部は不正ソフト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、非常時において行うべき技術的対応を、通常時から講じることが求められる。

非常時が発生する原因については、

・ 災害
・ サイバー攻撃
・ システム障害（ネットワーク障害含む）

等が想定される。

それぞれの原因により、講じるべき対策が異なるところがあるが、共通することは、システム運用担当者は非常時が生じた際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、非常時を想定した措置について、通常時に訓練を行うなどが挙げられる。

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）
- 非常時用の臨時措置としての情報システム、情報機器

等に対する技術的な対応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を踏まえて、整合性のある内容のものを検討することが求められる。特にサイバー攻撃などの場合、医療情報や、医療情報システムのソフトウェアのバックアップデータには既に不正ソフトウェアの混入による影響が及んでいる可能性が高く、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繰り返し、場合によっては被害を拡大することになりかねない。加えて、ハードウェアについても原因検証のために利用できないなどのリスクもあることから、バックアップの設計や整備に関しては、総合的な観点からリスク評価を行った技術的な対応が求められる。

検討結果については、企画管理者に報告する必要がある。

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 ・追記不能型のデータバックアップの記録媒体の整備 ・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	・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
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

システム運用担当者は、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、死活管理を行うことが必要である。医療情報システムのパフォーマンスが低下した場合やシステムダウンが生じた場合に、速やかにその状況が把握できるようにする必要がある。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も求められる。

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などの対応を行うことが求められる。併せて非常時に講じた措置から、通常時の運用への復旧・復帰の手順なども整備する必要がある。

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不可能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に備え、非常時用ユーザアカウント運用が講じられることがある。非常時用ユーザアカウントを用意し、患者の医療情報へのアクセス制限が医療サービス低下を招かないように配慮するなどのほか、通常時への復旧・復帰後に非常時ユーザアカウントを更新するなどの措置が求められる。

非常時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮する等、必要に応じて非常時の運用に対応した機能を実装する必要がある。

非常時への対応機能の用意は、関係者に周知され非常時に適切に用いられる必要があるが、逆にリスクが増える懸念もあるため、運用管理は慎重でなくてはならない。

１２．物理的安全管理措置　［Ⅰ、Ⅲ　なお遵守事項⑤・⑥及び１２．３は、Ⅱ、Ⅳも参照］

【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について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、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 個人情報が保管されている情報機器等の重要な情報機器には盗難防止を講じること。

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と整合性がとれる措置とし、確保したバックアップは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不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の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）について、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。特に医療情報を保護するという観点から、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･構造にあるよう考慮するほか、医療情報システムの運用の確保の観点から結露や高温による情報機器等の暴走などが生じないような措置が講じられている環境を選定するなどが求められる。

サーバルームやマシンルームなどのうち、医療情報や医療情報システムが格納されているセキュリティ区域については、サーバルーム等の職員を含め、入退管理がなされており、カメラ等による監視などがなされていることなども考慮に入れる必要がある。

さらに、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については、施錠管理されていることが求められる。

１２．２　バックアップの管理

システム運用担当者は、バックアップについては、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、適切に確保し、非常時に利用できるよう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、方法等を明らかにすることとされているが、非常時に利用できることを想定し、「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、非常時の事象発生原因に応じて行うことが求められる。またサイバー攻撃への対応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」参照。

外部保存で委託を行っている場合には、委託先の事業者に対して、バックアップの対象、バックアップ頻度、復旧できる世代、バックアップ方法、保存場所等について確認し、SLA 等において明らかにすることが求められる。

またシステム運用担当者は、バックアップを含む記録媒体について、記録媒体や、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止するための措置を講じることが求められる。記録媒体の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、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写する等の情報の保管措置を講じることが求められる。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行える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、記録媒体の保管場所の特徴等に応じて、定期的に可読に関するチェックを行うことが求められる。併せてシステム運用担当者は、この手順を作成することが求められる。

なお、患者の個人情報の保護等に関する事項は、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、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。

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

記録媒体による外部保存を、可搬媒体を用いて行う場合、委託する医療機関等と受託する事業者はネットワークで結ばれないため、ネットワーク上の脅威に基づくなりすましや盗聴、改ざん等による情報の大量漏洩や大幅な書換え等の危険性は少なくなる可能性がある。

可搬媒体による保存の安全性は、紙やフィルムによる保存の安全性と比べて概ね優れているといえる。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可搬媒体等のパスワードによるアクセス制限が可能な記録媒体を用いればさらに機密性は増す。

しかしながら、可搬媒体の耐久性の経年変化については、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、記録媒体を遺失した際に紛失、漏洩する情報量も多くなるため、より慎重な取扱いが必要である。

そこで、システム運用担当者は、診療録等を可搬媒体に記録して搬送する場合は、可搬媒体の遺失や他の搬送物との混同を防止するために、以下の点に注意する必要がある。

－　診療録等を記録した可搬媒体の遺失防止

運搬用車両を施錠する等、搬送用ケースを封印する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、他の搬送物と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保存を受託する事業者、搬送業者に対して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。

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・参照のおそれがある場合には、クリアスクリーン等の対策を実施することが求められる。

１３．ネットワークに関する安全管理措置　［Ⅰ、Ⅲ］

【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、採用する通信方式や、採用する認証手段を決めること。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。

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データやソフトウェア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。

⑥ オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、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 クライアント認証を実施すること。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。その際、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 3.0.1 版」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。なお、SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。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。

⑦ 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。

⑧ 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。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。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。

⑨ ネットワーク経路でのメッセージ挿入、不正ソフト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。

⑩ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。

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、通信の相手先が正当であることを認識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が、互いに通信目的とする正当な相手かどうかを認識するための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。

－　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。例えば、ANY 接続拒否等の対策を実施すること。

－　不正アクセス対策を実施すること。例えば MAC アドレスによるアクセス制限を実施すること。ただし、MAC アドレスは詐称可能であることや、最近のモバイル端末においては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。

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

－　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、医療情報システムにおいて利用するネットワークについて、リスク評価を踏まえて、その選定を企画管理者と協働して検討することが求められる。

医療情報システムで利用するネットワークという場合、その語は多義的であるため、本ガイドラインでは、下図のように整理を行った。ネットワークの安全性を検討する場合には、実際には、ネットワークにおける各レイヤで、対策が講じられることになり、その結果、アクセス先が限定されたり、アクセス先がオープンになったりする。

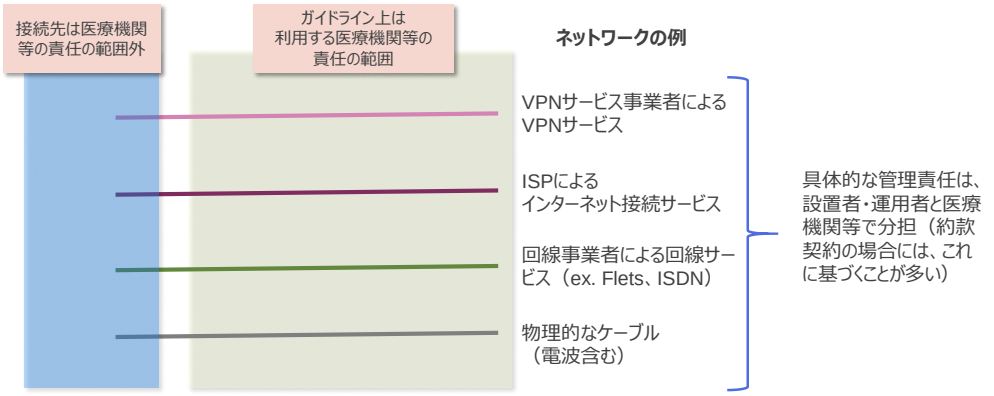


図１２－１　ネットワークの管理に対する考え方

このように回線のレイヤと接続先が限定されているか否かは別であると考えた場合、医療機関等が利用するネットワークの安全性については、その接続先が限定されている、あるいは経路等が管理されているか否かで、考慮するのが妥当であると考える。

図１２－２のように、ネットワークの接続先の限定等は、さまざまな形で実現できるが、いずれの場合にも、回線の暗号化などを講じることで、リスクの違いはあるものの、従来の境界防御としてのネットワーク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かったりする場合には、いわゆるオープンなネットワークとして位置付けられ、境界防御的な対応は難しい。但しこの場合でも、インターネット VPN のサービスを利用するなどにより、境界防御的な対応を行うことが期待できる。

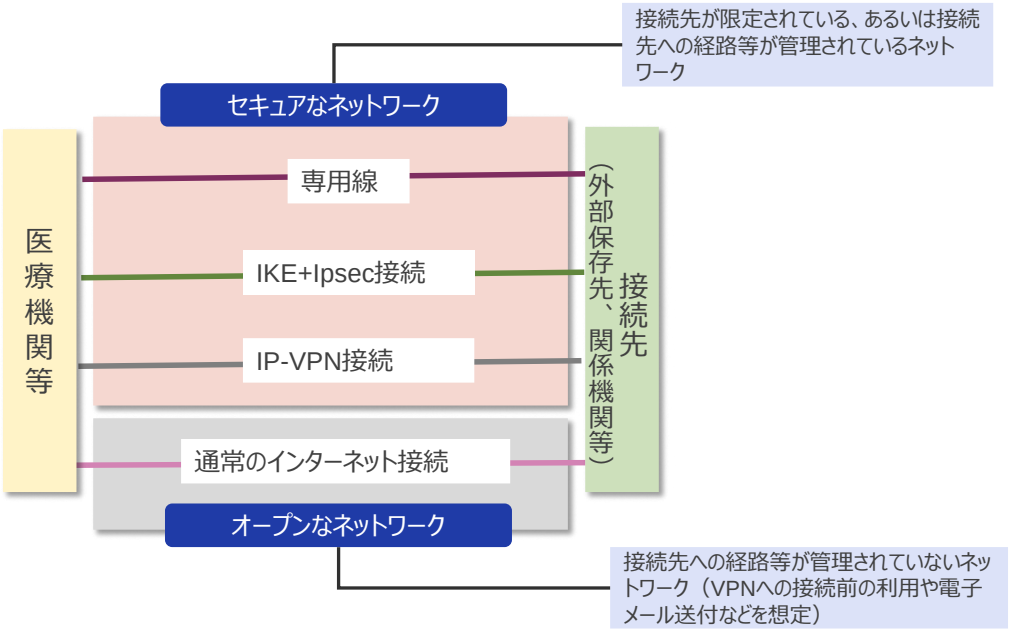


図１２－２　本ガイドラインにおけるネットワークの整理

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」と称することとし、医療情報システムでの利用は、原則として「セキュアなネットワーク」を用いることと整理する。但しオープンなネットワークも、「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用いたり、あるいは電子メールの送信時において、送信するデータ自体を暗号化して送信したりするなどで用いることが想定されるため、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は、医療情報システムの構成に応じて、安全性が確認できるネットワーク機器を利用し、不正な機器が接続したり、不正なデータやソフトウェアが混入したり、異常なデータ通信が発生したりしないよう、セキュアなネットワークを構築し、ネットワークに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の分割、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必要がある。

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、ネットワークの選定に際しては、医療情報の安全管理が確保できるもの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、独占的な回線利用となるため高コストであることや、多目的な利用にはなじみにくいなどがある。

これに対して、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り、いくつかの VPN の実装方法がある。

IP-VPN は、インターネットを用いず、通信事業者が提供するものである。このサービスの場合にも、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等があるとされる。

システム運用担当者は、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等の方針なども踏まえて、適切なものを選択することが求められる。

なお、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オープンではない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こともあり得る。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、チャネル・セキュリティが確実に確保されるようにしておく必要がある。

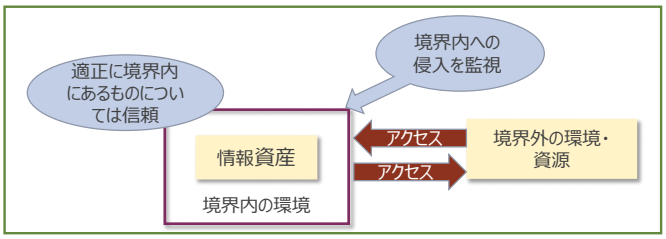
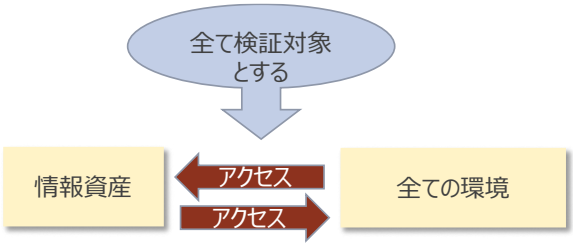
なお、システム運用担当者は医療情報システムが利用するネットワークを選定した際に、ネットワークの管理や非常時の対応など、具体的な技術的な対応に関する内容について、ネットワークを提供する電気通信事業者や、情報システム・サービスを提供する事業者との間での責任分界の範囲を明らかにしたうえで、企画管理者に報告することが求められる。

１３．２　不正な通信の検知や遮断、監視

ネットワークの選択においては、オープンではないセキュアなネットワークを選択し、境界防御的な対応を原則とするが、巧妙化するサイバー攻撃に対しては、境界防御的な対応だけでは十分ではない。例えば VPN 装置の脆弱性を攻撃することにより、ランサムウェアによる被害なども見られることから、境界防御だけでサイバー攻撃への対応を図ることは困難と言える。

近年は、境界防御の思考による安全性のみに限らず、すべ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」の概念による考え方も出てきている。ゼロトラスト思考では、利用者の行動も含めてすべて検証し、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などの仕組みで構成される。

表１２－１　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、すべ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。

ゼロトラスト思考の有効性は、認められているものの、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。また医療機関等の場合、接続先が多方面にわたっていない医療機関等が多いことから、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。

但し、境界防御ではサイバー攻撃への対応としては十分ではないことから、境界防御を採用する場合でも、トラフィックの監視等、多層防御の考え方を導入することが、医療機関等においては求められる。

クラッカーや不正ソフト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）などの採用もシステム運用担当者は、検討する必要がある。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）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が求められる。

さらに、外部からのサイバー攻撃の高度化・多様化に鑑みると、境界防御の対策を行っていたとしても、不正ソフトウェア等の攻撃や侵入があることから、このような場合を想定して、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　不正ソフトウェア対策」参照)。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。

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」等の脅威から守られるよう、対策を講じることが求められる。

１３．３．１　ネットワーク回線の暗号化

ネットワーク回線の暗号化については、特にオープンなネットワークを利用する際に求められる。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、システム運用担当者は、医療情報を医療機関等の外部とやり取りする場合には、TLS の設定を適切に行って、通信するための措置を講じ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、偽サーバの接続リスクなども鑑みて、適切な手段を選択することが求められる。

１３．３．２　情報に対する暗号化

システム運用担当者は、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こともあるため、特に留意する必要がある。

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、送信元から送信先に確実に情報を送り届ける必要があり、「送信すべき相手に」、「正しい内容を」、「内容を盗み見されない方法で」送信しなければならない。そのため、システム運用担当者は送信する情報が

- 盗聴されないこと
- 改ざんされないこと
- メッセージ挿入や不正ソフトウェアの混入等や中間者攻撃を受けないこと
- なりすまされた相手先に送信しないこと

等のための措置を講じることが求められる。そのために、ネットワークや機器、サービス等の監視などを行うほか、通信の相手先との相互認証を行うなどの措置を必要に応じて行うなどが求められる。

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、可用性などにも配慮した対策を講じることが求められる。

無線 LAN は無線を用いたネットワークであることから、適切な措置を講じないと本来利用が許されない第三者の利用が生じるほか、侵入者による攻撃などを招くリスクがある。また適切な暗号化を講じないと、盗聴や不正ソフト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。

１４．認証・認可に関する安全管理措置　［Ⅰ～Ⅳ］

【遵守事項】

① 医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証方法に関する手順等に関して、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 IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。

④ アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、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よう指示すること。

⑤ 利用者認証にパスワードを用いる場合には、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、今後、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。

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。

－ 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。

－ 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。

－ 利用者のパスワードの失念や、パスワード漏洩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、パスワード漏洩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。

－ 医療情報システムの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）。

⑦ 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、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。

⑧ 電子カルテシステムにおける記録の確定手順の確立と、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。

－ 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仕組みをシステムに備えること。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めること。

b 「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。

c 「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。

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。

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。

－　臨床検査システム、医用画像ファイリングシステム等、特定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。

－　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ようにすること。

－　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ようにすること。

－　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。

－　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

医療情報システムへのアクセスを正当な利用者のみに限定するために、医療情報システムは利用者の識別・認証を行う機能を持たなければならない。システム運用担当者は、リスク分析の結果を踏まえて、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、その運用に必要な具体的な手順の作成を行う必要がある。

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、一般的にこの機能は必須である。

認証を実施するためには、医療情報システムへのアクセスを行う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が行われなければならない。

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。なお利用者認証を 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、パスワードが第三者に推定されにくいものとするよう、安全性を考慮した機能仕様とする必要があるほか、システム側でのパスワードの管理については、システム運用担当者でもわからないようにする措置を講じることが求められる。

認証強度の考え方として、現状において、医療情報システムにアクセスする端末ごとに二要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる（※）。

※　二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、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、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が求められる。

また医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか２つ以上）の認証がなされている場合には、二要素認証に相当すると考えてよい。

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

クラウドサービスなどの普及から、外部のアプリケーションを連携して用いる場面等が多くなってきている。院内のシステムと外部アプリケーションを連携して用いる場合や、複数のクラウドサービスを連携して用いる場合には、アプリケーション間でデータの引き渡しなどを行う必要が生じる。昨今、システム間連携のインタフェースとして、Web 技術のうち、連携のしやすさから、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 ASP 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できるように、必要に応じてネットワークセキュリティを確保し、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を限定し、その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、それに沿った認証・認可に関する仕組みを設ける必要がある。

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。また付与する利用権限は必要最小限にすることが重要である。

知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。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を行う機能があれば、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行う必要があるため、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。

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危険性がある。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、意図せぬ設定の変更に関して検知できる措置を講じることが求められる。特に自動的に検知し、運用に反映できることが必要となる。

システム運用担当者は、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が求められる。

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、電子化した文書を支障なく取り扱えることが当然担保されなければならないことに加え、その内容の正確さについても訴訟等における証拠能力を有する程度のレベルを担保することが要求される。誤った診療情報は、患者の生命や身体に関わることであるので、電子化した診療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について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ていなくてはならない。

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である。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、診療録等が書換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。

したがって、システム運用担当者はネットワークを通じて医療機関等の外部に保存する場合は、医療機関等に保管する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。例えば虚偽入力、書換え、消去及び混同を防止するためには、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、運用も含めて対応することが求められる。

また作成の責任の所在を明確にすることも求められる。具体的には入力者及び確定者の識別・認証、記録の確定、識別情報の記録、更新履歴の保管において、対策を講じる必要がある（代行入力を行う場合には、確定者の識別・認証において留意が必要である）。

１５．電子署名、タイムスタンプ　［Ⅰ～Ⅳ］

【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、これが利用できるよう、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ることができるよう、技術的な対応を行うことが求められる。

１６．紙媒体等で作成した医療情報の電子化　［Ⅰ～Ⅳ］

【遵守事項】

① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、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、スキャンによる電子化で情報が欠落することがないよう、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けられていたり、スキャナ等が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 運用の利便性のために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、緊急に閲覧が必要になったときに迅速に対応できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。

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に、医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保する等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などがある場合もある。したがって、一旦紙等の媒体で運用された情報をスキャナ等で電子化することは慎重に行う必要がある。電子情報と紙等の情報が混在することで、運用上著しく障害がある場合等に限定すべきである。その一方で、電子化した上で、元の媒体も保存することは真正性・保存性の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されるべきである。

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

紙等の媒体で扱うことが著しく利便性を欠くためにスキャナ等で電子化するが、紙等の媒体の保存は継続して行う場合、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。しかしながら、個人情報保護上の配慮は同等に行う必要があり、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。

システム運用担当者は、このような観点から、運用の利便性のために電子化をスキャナ等で行う場合に、スキャナや電子化されたファイルに対して、技術的な対応を行うことが求められる。

１７．証跡のレビュー・システム監査　［Ⅰ、Ⅲ］

【遵守事項】

① 利用者のアクセスについて、アクセスログ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 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実施すること。

③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。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に、技術的な対応として、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。

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、さらには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効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、アクセスログへのアクセス制限や改ざん防止措置等を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じることが求められる。

アクセスログの正確性のため、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らなければならない。

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、明確にする必要がある。

なお、医療機関等において取り扱っている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、技術的な対応における部分の内容を作成し、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が求められる。監査結果で指摘された事項については、企画管理者と協議し、改善することも求められる。

１８．外部からの攻撃に対する安全管理措置　［Ⅰ～Ⅳ］

【遵守事項】

① 医療情報システムに対する不正ソフト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洩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（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）

１８．１　サイバーセキュリティ対応

システム運用担当者は、サイバー攻撃を受けた等、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必要が生じる場合がある。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する必要がある。

サイバー攻撃への対策については、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、NISC から示されている「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３年度版）」、2021 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」も参照することが求められる。

また、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」も参照することが求められる。

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、診療の継続や早期に業務を再開することが求められる。バックアップに関しては、全ての情報をバックアップから復元するのではなく、ある程度のリスクを許容することで運用が容易になり、確実に対応することが可能になることも多い。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が必要である。

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、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した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等を考慮して対策を講じることが強く求められる。例えば、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）確保し、遅くとも３世代目以降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、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不正ソフトウェアが混入による影響が及んでいる可能性が高く、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繰り返し、場合によっては被害を拡大することになりかねない。不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

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
- 同じ脆弱性を突かれて侵入されない
- 他の脆弱性を突かれない
- 不正に作成されたり、盗まれたりした ID・パスワード等を使われないようにする

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たりしないようにする必要がある。なお専門的な知見に関して、情報処理推進機構が、不正ソフト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を開設している。

【別添】

e-文書法対応に求められる技術的対策（見読性、真正性、保存性）

「医療情報システムの安全管理に関するガイドライン」第 5.2 版第 7 章では、施行通知に基づいて求められる安全管理対策について示している。示されている内容の中には、施行通知で対象となる文書の電子化だけではなく、医療情報システムで取り扱う医療情報全般においても求められると考えられるものを含むことから、本ガイドライン第 6.0 版においては、これらの安全管理対策については分けて記載せず、共通できる内容として記載した。

「医療情報システムの安全管理に関するガイドライン」第 5.2 版第 7 章における安全管理対策につき、本ガイドライン第 6.0 版での記載箇所との対応関係を以下に示す。

１.「見読性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、見読性の確保の安全管理対策について、

- ネットワークを通じて医療機関等の外部に保存する場合
- 医療機関等に保存する場合

の２つのケースについて、それぞれ対応策を整理している。

また、どちらの場合にも対応すべき対策として

- 情報の所在管理
- 見読化手段の管理
- 見読目的に応じた応答時間

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.2　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（１）情報の所在管理	4.1
（２）見読化手段の管理	5.1
（３）見読目的に応じた応答時間	9.2
（４）システム障害対策としての冗長性の確保	11.2

２.「真正性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、真正性の確保にかかる安全管理対策について、

- 医療機関等に保存する場合
- ネットワークを通じて医療機関等の外部に保存する場合

の２つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

- 入力者及び確定者の識別及び認証
- 記録の確定手順の確立と、作成責任者の識別情報の記録
- 更新履歴の保管
- 代行操作の承認機能
- 情報機器･ソフトウェアの品質管理

等の対策が示されている。

また、ネットワークを通じて医療機関等の外部に保存する場合については、

- 通信の相手先が正当であることを認識するための相互認証を行うこと
- 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
- リモートログイン機能を制限すること

の 3 点について対策が示されている。

本版との対象関係について、以下に示す。

【医療機関等に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.1　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（１）入力者及び確定者識別及び認証	14.3
（２）記録の確定手順の確立と、識別情報の記録	14.3
（３）更新履歴の保管	14.3
（４）代行入力の承認機能	14.3
（５）情報機器･ソフトウェアの品質管理	8.1、8.2、8.4、10.1

【ネットワークを通じて医療機関等の外部に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.1　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（１）通信の相手先が正当であることを認識するための 相互認証をおこなうこと	13.2
（２）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	13.3
（３）リモートログイン機能を制限すること	9.2

3.「保存性」確保のための対策

「医療情報システムの安全管理に関するガイドライン」第 5.2 版では、保存性の確保の安全管理対策について、

- 医療機関等に保存する場合
- ネットワークを通じて医療機関等の外部に保存する場合

の 2 つのケースについて、それぞれ対応策を整理している。

医療機関等に保存する場合では、さらに、

- ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止
- 不適切な保管･取扱いによる情報の滅失、破壊の防止
- 記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止
- 記録媒体･情報機器･ソフトウェアの整合性不備による復元不能の防止

等の対策が示されている。

具体的な対策として規定されている内容を以下に示す。

【医療機関等に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.3　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
(1) ウイルスや不適切なソフトウェア等による 情報の破壊及び混同等の防止	8.3
(2) 不適切な保管･取扱いによる情報の滅失、破壊の防止	12.2、18.1
(3) 記録媒体、設備の劣化による読み取り不能 または不完全な読み取りの防止	12.2
(4) 記録媒体･情報機器･ソフトウェアの整合性不備による 復元不能の防止	5.2

【ネットワークを通じて医療機関等の外部に保存する場合】

「医療情報システムの安全管理に関するガイドライン」 第 5.2 版の項目 7.3　　C.最低限のガイドライン	本ガイドライン 第 6.0 版での記述箇所
（1）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おこなうこと	5.2
（2）ネットワークや外部保存を受託する機関の 設備の劣化対策をおこなうこと	12.2