産情発 0531 第１号
令和５年５月 31 日

各 都道府県知事
保健所設置市長
特　別　区　長 殿

厚生労働省大臣官房
医薬産業振興・医療情報審議官
（　公　印　省　略　）

「医療情報システムの安全管理に関するガイドライン　第 6.0 版」の
策定について

「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）については、直近では令和４年３月に第 5.2 版を策定し、医療情報システムの適切な取扱い等についてお示ししてきたところです。

今般、ガイドラインの見直しを行い、別添１～４のとおり「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」を策定するとともに、別添５～12 のとおり参考資料を作成しました。

ガイドラインの改定の趣旨や概要等については下記のとおりですので、貴職におかれては、御了知の上、関係団体、関係機関等に周知徹底を図るとともに、その実施に遺漏なきよう御配慮願います。

記

第１　改定の趣旨

保険医療機関･薬局においては令和５年４月からオンライン資格確認の導入が原則義務化されており､今後はガイドラインに記載されているネットワーク関連のセキュリティ対策がより多くの医療機関等に共通して求められることとなる。よって、医療機関等にガイドラインの内容の理解を促し、医療情報システムの安全管理の実効性を高めるため、構成の見直しを行う。

また､医療等分野及び医療情報システムに対するサイバー攻撃の一層の多様化･巧妙化が進み、医療機関等における診療業務等に大きな影響が生じていること等を踏まえ､医療機関等に求められる安全管理措置を中心に内容の見直しを行う。

第２　改定の概要

１．全体構成の見直し

本文を、概説編、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等において現状で選択可能な具体的な技術にも言及するなど、構成の見直しを行う。

２．外部委託、外部サービスの利用に関する整理

クラウドサービスの特徴を踏まえたリスクや対策の考え方を整理するとともに、医療機関等のシステム類型別に責任分界の考え方等を整理する。

３．情報セキュリティに関する考え方の整理

ネットワークの安全性の考え方や認証のあり方を踏まえて、ゼロトラスト思考に則した対策の考え方を示すほか、サイバー攻撃を含む非常時に対する具体的な対応について整理する。

４．新技術、制度・規格の変更への対応

オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置等について整理する。

そのほか、所要の改定を行う。

第３　留意事項

ガイドライン及び参考資料については厚生労働省ホームページに掲載する予定。

以上

医療情報システムの安全管理に関するガイドライン

第 6.0 版

概説編

[Overview]

目次

１．はじめに ..... - 1 -

２．本ガイドラインの対象 ..... - 1 -

２．１　医療機関等の範囲 ..... - 1 -

２．２　医療情報・文書の範囲 ..... - 1 -

２．３　医療情報システムの範囲 ..... - 2 -

３．本ガイドラインの構成、読み方 ..... - 2 -

３．１　各編の目的・概要 ..... - 3 -

３．１．１　概説編（Overview） ..... - 3 -
３．１．２　経営管理編（Governance） ..... - 3 -
３．１．３　企画管理編（Management） ..... - 3 -
３．１．４　システム運用編（Control） ..... - 3 -

３．２．医療機関等の特性に応じた読み方 ..... - 4 -

３．２．１　医療機関等の特性についての考え方 ..... - 4 -
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 ..... - 4 -

３．３　第 5.2 版との関係 ..... - 6 -

４．　本ガイドラインの前提 ..... - 6 -

４．１　医療情報システムの安全管理の目的 ..... - 6 -

４．１．１　医療情報システムで取り扱う医療情報の重要性 ..... - 6 -
４．１．２　医療情報システムの有用性 ..... - 6 -
４．１．３　医療情報システムの安全管理の必要性 ..... - 6 -

４．２　医療情報システムの安全管理に必要な要素 ..... - 7 -

４．３　医療情報システムの安全管理に関連する法令 ..... - 7 -

４．４　医療情報システムに関する統制 ..... - 8 -

４．５　リスク評価とリスク管理 ..... - 8 -

４．６　医療情報システムにおける認証・認可 ..... - 9 -

４．７　医療情報の外部保存 ..... - 10 -

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）。

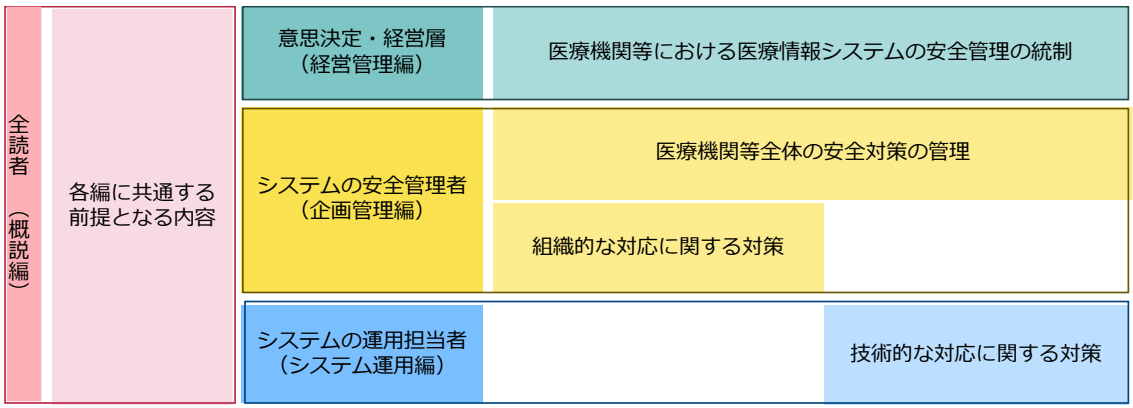


図３－１　ガイドライン第 6.0 版を構成する各編

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】 ..... - 1 -

1．安全管理に関する責任・責務 ..... - 3 -

1．1　安全管理に関する法令の遵守 ..... - 3 -

1．1．1　医療情報システムに対する医療機関等の責任 ..... - 3 -

1．1．2　医療機関等における法令上の責任 ..... - 3 -

1．2　医療機関等における責任 ..... - 3 -

1．2．1　通常時における責任 ..... - 4 -

1．2．2　非常時における責任 ..... - 5 -

1．3　委託における責任 ..... - 6 -

1．3．1　委託（第三者委託）における責任 ..... - 6 -

1．3．2　委託（第三者委託）における責任分界 ..... - 7 -

1．4　第三者提供における責任 ..... - 8 -

2．リスク評価を踏まえた管理 ..... - 9 -

2．1　医療情報システムにおけるリスク評価の実施 ..... - 9 -

2．2　リスク評価を踏まえた判断 ..... - 10 -

2．2．1　リスク評価を踏まえたリスク管理 ..... - 10 -

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 ..... - 10 -

2．2．3　リスク分析を踏まえた要求仕様適合性の管理 ..... - 11 -

3．安全管理全般（統制、設計、管理等） ..... - 12 -

3．1　統制 ..... - 12 -

3．1．1　情報セキュリティ対策のための統制 ..... - 12 -

3．1．2　医療情報システムにおける統制上の留意点 ..... - 13 -

３．２　設計 - 14 -
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 - 14 -
３．２．２　情報セキュリティ対策を踏まえた訓練・教育 - 14 -
３．３　安全管理対策の管理 - 15 -
３．３．１　安全管理状況の自己点検 - 15 -
３．３．２　情報セキュリティ監査 - 15 -
３．４　情報セキュリティインシデントへの対策と対応 - 16 -
３．４．１　事業継続計画（BCP：Business Continuity Plan）の整備と訓練 - 16 -
３．４．２　情報共有・支援、情報収集 - 17 -
３．４．３　情報セキュリティインシデントへの対応体制 - 18 -
４．安全管理に必要な対策全般 - 19 -
４．１　必要な対策項目の概要 - 19 -
４．２　必要な措置 - 20 -
５．医療情報システム・サービス事業者との協働 - 21 -
５．１　事業者選定 - 21 -
５．１．１　事業者選定 - 21 -
５．１．２　事業者選定の基準 - 21 -
５．２　事業者管理 - 22 -
５．２．１　契約管理 - 22 -
５．２．２　体制管理 - 22 -
５．３　責任分界管理 - 23 -

【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

<table>
<tr><td rowspan="5">全ての医療機関等における責任</td><td rowspan="3">通常時における責任</td><td>管理方法・体制等に関する説明責任</td></tr>
<tr><td>管理及び監査を実施する責任</td></tr>
<tr><td>定期的に見直し、必要な改善を行う責任</td></tr>
<tr><td rowspan="2">非常時における責任</td><td>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</td></tr>
<tr><td>再発防止策等の善後策を講じる責任</td></tr>
<tr><td colspan="2">第三者に業務を委託する場合</td><td>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</td></tr>
<tr><td colspan="2">第三者に医療情報を提供する場合</td><td>第三者提供が適切に実施されたかに対する責任</td></tr>
</table>

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】 ..... - 1 -

1．管理体系 ..... - 3 -

1．1　安全管理に関連する法制度等 ..... - 3 -

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 ..... - 3 -
1．1．2　医療情報システムに関係する法令 ..... - 4 -

1．2　医療情報システムの安全管理に関する方針の策定 ..... - 9 -

1．2．1　情報セキュリティ方針（ポリシー）等の策定 ..... - 9 -
1．2．2　個人情報保護に関する方針の策定 ..... - 9 -

2．責任分界 ..... - 10 -

2．1　運用管理における責任分界 ..... - 10 -

2．1．1　医療機関等における責任と責任分界 ..... - 10 -
2．1．2　通常時における責任 ..... - 11 -
2．1．3　非常時における責任 ..... - 12 -
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 ..... - 13 -

2．2　責任分界の決め方 ..... - 13 -

2．2．1　委託と第三者提供における責任分界 ..... - 13 -
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） ..... - 13 -
2．2．3　第三者提供における責任分界 ..... - 16 -

3．安全管理のための体制と責任・権限 ..... - 17 -

3．1　医療情報システムの安全管理体制の構築 ..... - 17 -

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 ..... - 17 -
3．1．2　企画管理者の業務範囲と権限 ..... - 17 -
3．1．3　情報システム管理委員会の業務範囲と権限 ..... - 18 -
3．1．4　担当者の任命、業務範囲、権限 ..... - 18 -
3．1．5　非常時の体制・CSIRT 等の整備 ..... - 18 -

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 ..... - 19 -
３．１．７　委託等における安全管理の体制 ..... - 19 -
３．１．８　監査体制の整備と監査責任者の設置 ..... - 19 -
３．１．９　患者等からの苦情・質問の受付体制 ..... - 19 -
３．１．10　体制整備の可視化 ..... - 19 -

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 ..... - 20 -

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） ..... - 20 -

４．２　規程の整備（運用管理規程ほか） ..... - 20 -

４．３　規則等の整備 ..... - 21 -

４．４　マニュアル等及び各種資料の整備 ..... - 21 -

５．安全管理におけるエビデンス ..... - 22 -

５．１　証跡の整備の目的 ..... - 22 -

５．２　整備する証跡の種類 ..... - 22 -

５．３　証跡のレビュー ..... - 23 -

５．４　証跡の管理 ..... - 23 -

６．リスクマネジメント（リスク管理） ..... - 24 -

６．１　運用管理におけるリスクマネジメント ..... - 24 -

６．１．１　リスクマネジメントの役割 ..... - 24 -
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 ..... - 25 -

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） ..... - 25 -

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）..... - 27 -

７．１　職員管理..... - 29 -

７．２　委託先事業者管理..... - 29 -

７．３　教育・訓練..... - 29 -

７．４　委託先事業者選定..... - 30 -

７．５　外部保存・外部委託の終了..... - 30 -

７．６　患者への説明等..... - 31 -

８．情報管理（管理、持ち出し、破棄等）..... - 32 -

８．１　情報管理..... - 33 -

８．１．１　情報管理方針の整備..... - 33 -
８．１．２　情報管理の手順..... - 33 -
８．１．３　情報の安全管理状況の報告..... - 33 -

８．２　医療情報の持ち出し..... - 33 -

８．２．１　医療情報の持ち出し手順等の策定..... - 33 -
８．２．２　記録媒体・情報機器等による持ち出し..... - 34 -
８．２．３　ネットワークサービスを用いた持ち出し..... - 34 -
８．２．４　外部からのアクセスによる持ち出し..... - 34 -
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..... - 35 -
８．２．６　持ち出し状況のレビュー..... - 35 -

８．３　医療情報の破棄..... - 35 -

８．３．１　破棄の手順等の策定..... - 35 -
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..... - 35 -

９．医療情報システムに用いる情報機器等の資産管理 - 37 -

９．１　情報機器等の台帳管理 - 37 -

９．２　情報機器等の安全性の確認 - 38 -

９．３　情報機器等の資産管理状況の報告 - 38 -

１０．運用に対する点検・監査 - 39 -

１０．１　運用に対する点検 - 39 -

１０．２　運用に対する監査 - 39 -

１１．非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定 - 40 -

１１．１　非常時における対応方針の策定 - 40 -

１１．２　非常時に備えた通常時からの対応 - 41 -

１１．３　非常時の事象が生じた際の対応 - 43 -

１２．サイバーセキュリティ - 45 -

１２．１　サイバーセキュリティ対応計画の策定 - 45 -

１２．２　サイバーセキュリティ対応計画の実践 - 46 -

１２．３　サイバー攻撃被害時の対応 - 46 -

１３．医療情報システムの利用者に関する認証等及び権限 - 47 -

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 - 48 -

１３．１．１　医療情報システムの利用者 - 48 -

１３．１．２　医療情報システムの利用者の登録と認証 - 48 -

１３．１．３　医療情報システムの利用者の権限設定 - 49 -

１３．２　電子カルテにおける記録の確定 - 49 -

１４．法令で定められた記名・押印のための電子署名 - 50 -

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 - 52 -

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 - 54 -

１５．技術的な安全管理対策の管理 - 55 -

１５．１　技術的な対応の管理 - 56 -

１６．紙媒体等で作成した医療情報の電子化 - 57 -

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 - 58 -

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 - 58 -

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 - 58 -

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 - 58 -

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 - 59 -

【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。

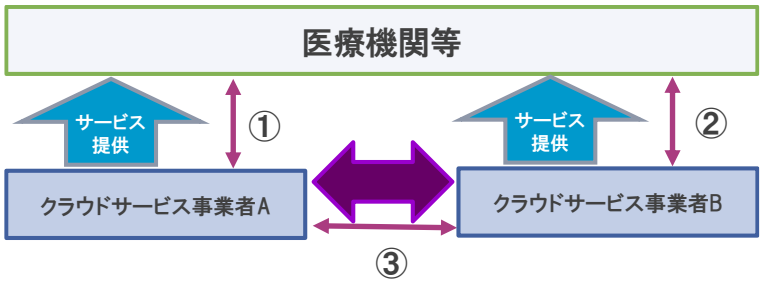
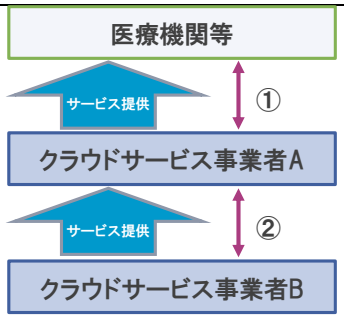
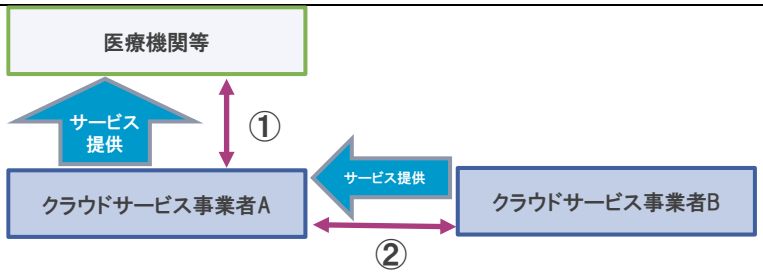
前者の場合は、基本的には医療機関等が各事業者と責任分界を取り決めることになるが、複数のシステム関連事業者のサービスの連携部分についても併せて取決めを行うことが求められる。これには、技術的な仕様等に関する取決めだけではなく、非常時におけるシステム関連事業者間での対応なども含めて取り決めることが求められる。

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〇〇年」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】 ..... - 1 -

1．情報セキュリティの基本的な考え方　［Ⅰ～Ⅳ］ ..... - 3 -

1．1　安全管理に関する法制度等による要求事項 ..... - 3 -

2．システム設計・運用に必要な規程類と文書体系　［Ⅰ～Ⅳ］ ..... - 4 -

2．1　システム運用担当者において作成すべき文書類 ..... - 4 -

3．責任分界　［Ⅰ～Ⅳ］ ..... - 5 -

3．1　技術的な対応における責任分界決定の考慮事項 ..... - 5 -

3．2　要求仕様適合性の確認を踏まえた調整 ..... - 5 -

3．3　医療機関等が負う責任に関する責任分界 ..... - 6 -

3．3．1　通常時の運用における責任分界 ..... - 6 -

3．3．2　非常時の運用における責任分界 ..... - 6 -

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 ..... - 6 -

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 ..... - 6 -

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 ..... - 7 -

3．5　第三者提供における責任分界 ..... - 9 -

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］ ..... - 10 -

4．1　情報資産の種別に応じた安全管理の設計 ..... - 10 -

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 ..... - 10 -

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］.. - 12 -

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.....- 12 -

５．２　標準化対応、データ形式・プロトコルの互換性の確保 .....- 13 -

６．安全管理を実現するための技術的対策の体系　　［Ⅰ～Ⅳ］..... - 14 -

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） .....- 14 -

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 .....- 15 -

７．情報管理（管理・持出し・破棄等）　　［Ⅰ～Ⅳ］..... - 16 -

７．１　外部へ持ち出す医療情報の管理対策 .....- 17 -

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 .....- 17 -

７．２．１　医療機関等の職員による外部からのアクセス .....- 18 -

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 .....- 19 -

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ｋ等を行う場合.....- 19 -

７．３　医療情報の破棄 .....- 19 -

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 ....- 20 -

８．利用機器・サービスに対する安全管理措置　　［Ⅰ～Ⅳ］..... - 21 -

８．１　不正ソフトウェア対策.....- 22 -

８．２　情報機器等の脆弱性への対策.....- 22 -

８．３　端末やサーバの安全な利用の管理.....- 23 -

８．４　情報機器等の棚卸 - 24 -

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 - 24 -

９．ソフトウェア・サービスに対する要求事項　［Ⅰ、Ⅲ］ - 25 -

９．１　ソフトウェアの構成管理 - 25 -

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 - 25 -

１０．医療情報ステム・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］ - 26 -

１０．１　保守時の安全管理対策 - 26 -

１１．システム運用管理（通常時・非常時等）　［Ⅰ～Ⅳ］ - 28 -

１１．１　通常時における運用対策 - 28 -

１１．２　非常時における対応 - 30 -

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］ - 31 -

１２．１　サーバルーム等の物理的要件 - 31 -

１２．２　バックアップの管理 - 32 -

１２．３　その他 - 32 -

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 - 32 -

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 - 33 -

１３．ネットワークに関する安全管理措置　［Ⅰ、Ⅲ］..... - 34 -

１３．１　ネットワークに対する安全管理..... - 35 -

１３．１．１　セキュアなネットワークの構築..... - 36 -
１３．１．２　選択すべきネットワークのセキュリティ..... - 37 -

１３．２　不正な通信の検知や遮断、監視..... - 37 -

１３．３　通信の暗号化・盗聴等の防止..... - 39 -

１３．３．１　ネットワーク回線の暗号化..... - 39 -
１３．３．２　情報に対する暗号化..... - 39 -
１３．３．３　盗聴防止等..... - 39 -

１３．４　無線 LAN の利用における対策..... - 40 -

１４．認証・認可に関する安全管理措置　［Ⅰ～Ⅳ］..... - 41 -

１４．１　利用者認証..... - 42 -

１４．１．１　利用者の識別・認証..... - 42 -
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..... - 43 -

１４．２　アクセス権限の管理..... - 44 -

１４．３　電子カルテデータの確定..... - 44 -

１５．電子署名、タイムスタンプ　［Ⅰ～Ⅳ］..... - 45 -

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..... - 45 -

１６．紙媒体等で作成した医療情報の電子化　［Ⅰ～Ⅳ］..... - 46 -

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..... - 46 -

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..... - 46 -

１７．証跡のレビュー・システム監査　　［Ⅰ、Ⅲ］..... - 47 -

１７．１　証跡のレビュー.....- 47 -

１７．２　監査の実施の支援.....- 47 -

１８．外部からの攻撃に対する安全管理措置　　［Ⅰ～Ⅳ］..... - 48 -

１８．１　サイバーセキュリティ対応.....- 48 -

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）..... - 50 -

【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。

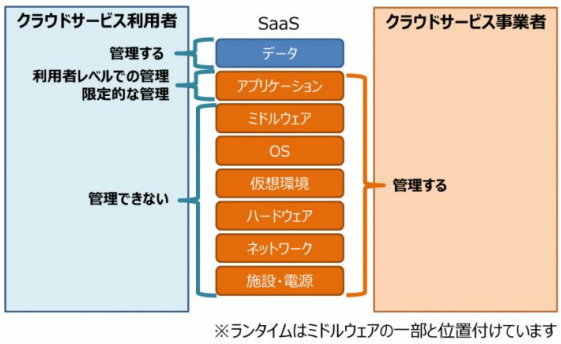
SaaS では、医療情報システムのアプリケーション部分、PaaS では、医療情報システムが利用するミドルウェアの部分、IaaS では医療情報システムが利用するインフラの部分をサービスとして提供することになる。

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。

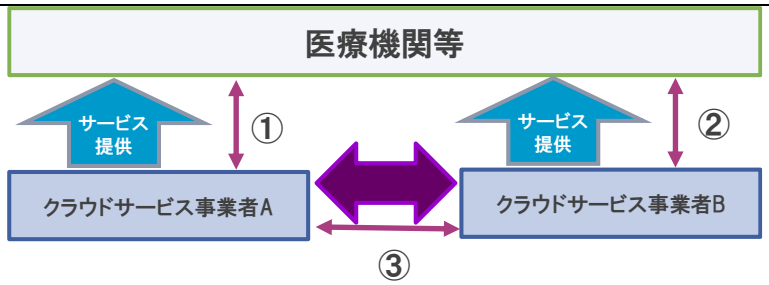
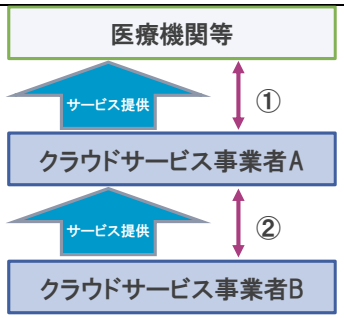
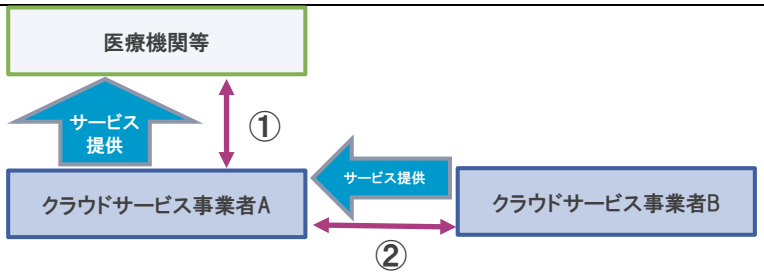
医療機関等が複数の情報システム・サービスのサービスを組み合わせて利用するような場合と、事業者が複数のサービスを組み合わせて、医療機関等に提供する場合などが想定される（表３－２参照）。

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	 ・　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。

<table>
<tr><td>クライアント側</td><td rowspan="3">セキュリティ</td></tr>
<tr><td>サーバ側</td></tr>
<tr><td>インフラ</td></tr>
</table>

－　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。

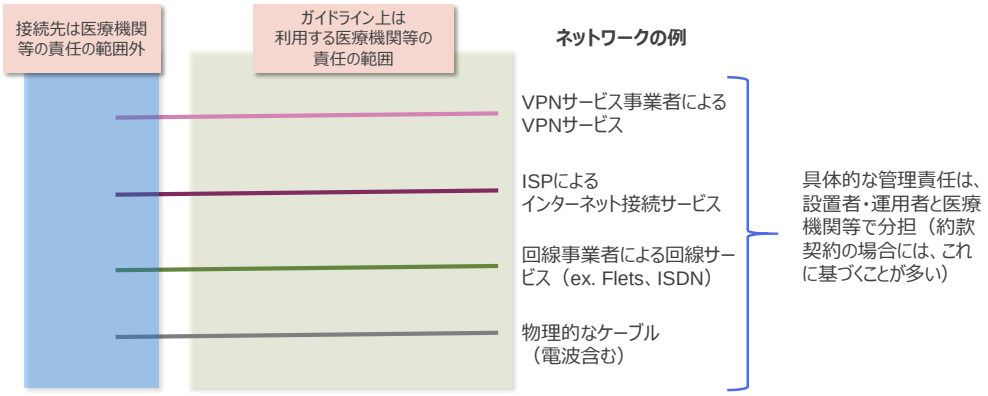


図１２－１　ネットワークの管理に対する考え方

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。

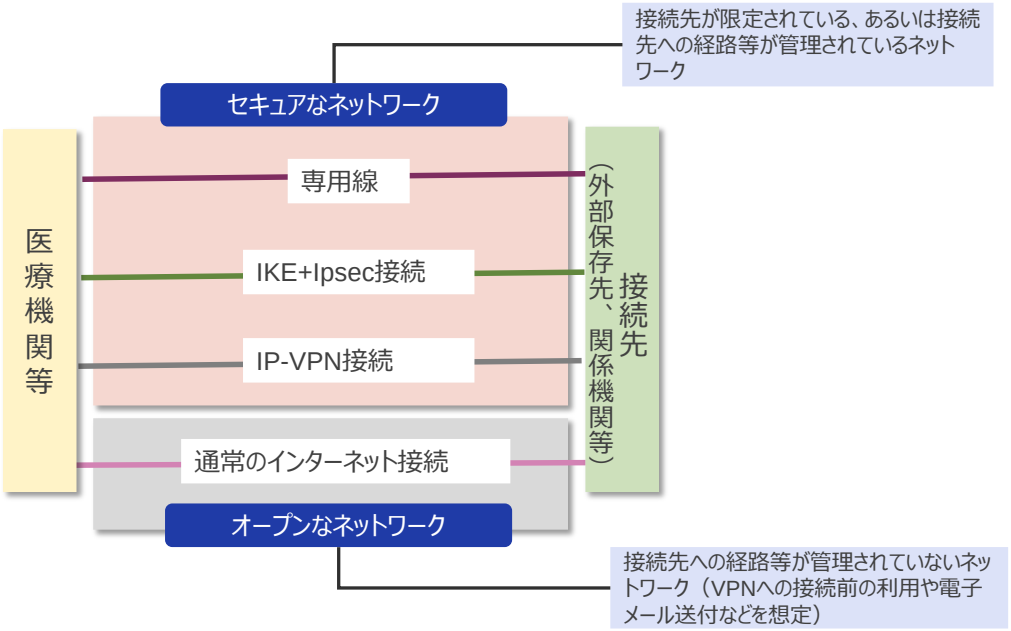


図１２－２　本ガイドラインにおけるネットワークの整理

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。

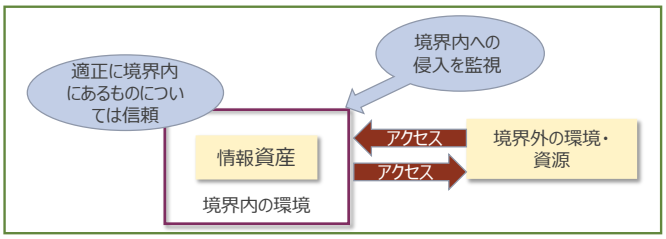
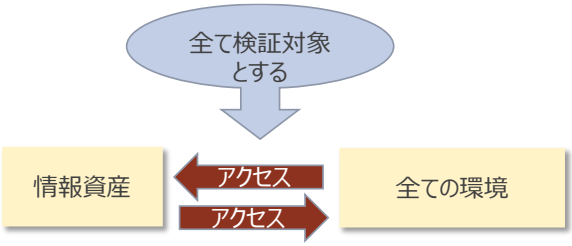
なお、システム運用担当者は医療情報システムが利用するネットワークを選定した際に、ネットワークの管理や非常時の対応など、具体的な技術的な対応に関する内容について、ネットワークを提供する電気通信事業者や、情報システム・サービスを提供する事業者との間での責任分界の範囲を明らかにしたうえで、企画管理者に報告することが求められる。

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

令和５年５月

「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」

に関するＱ＆Ａ

本 Q&A の参照箇所の使い方

企[1] ２章第[2]①条

[1] 各編の名称　概…概説編　経…経営管理編　企…企画管理編　シス…システム管理編

[2] 本編【遵守事項】の「条」です。

目次

概説編 10

概Ｑ－１　①このガイドラインは、医療機関等の関係者が読むもので、医療情報システムに関係するベンダや事業者は読む必要はないのか。②ベンダや事業者が遵守すべきガイドラインにはどのようなものがあるのか。 10

概Ｑ－２　どのような場合に、介護事業者は本ガイドラインの内容を遵守する必要があるか。 10

概Ｑ－３　他の医療機関等から提供された電子化された情報の取扱いは、このガイドラインの対象となるのか。 11

概Ｑ－４　電子保存が認められている文書とは具体的に何か。 11

概 Q－５　「医療情報システム」とは具体的に何を示すのか。 12

概Ｑ－６　オンライン資格確認や電子処方箋の導入において、どのような留意事項があるか。 12

概Ｑ－７　医療情報を電子的に保存するに当たって定められた要件は何か。また、情報セキュリティの３要素（機密性・完全性・可用性）との違いはあるか。 13

概Ｑ－８　SNS 等の Web サービスを利用して医療情報をやり取りする場合、考慮するべきことはあるか。 14

概Ｑ－９　第５．２版では、付表で小規模病院、診療所などの対応について示されていたが、小規模の基準は病床数や職員数で決められているのか。また第６．０版では、小規模病院等の対応について、同様の対応などが示されているのか。 14

概Ｑ－10　旧版のガイドラインの本編や別冊や別添等、全て読む必要があるか。 15

概Ｑ－11　このガイドラインの説明会や研修会等は実施されていないのか。 15

経営管理編 17

経Ｑ－１　電子的な医療情報を扱う責任を果たすうえで、どのようなことを理解すればいいか 17

経Ｑ－２　医療情報の取扱いに際し、令和２年改正・令和３年改正個人情報保護法も含めて、医療機関等にはどのような責任が生じるか。 18

経Ｑ－３　このガイドラインに従いシステム構築等をしていたにも関わらず起こった情報セキュリティインシデントについて、責任のあり方をどのように考えるべきか。 19

経Ｑ－４　このガイドラインを遵守しなかった場合、課せられる罰則等や e-文書法以外に抵触する法令はあるのか。 19

経Ｑ－５　通常運用時において説明責任を果たす際、患者にどのような説明をすべきか。 19

経Ｑ－６　委託している事業者において、情報漏えい等の情報セキュリティインシデントが発生した場合、事業者に対応をさせればよいのか。 20

経Ｑ－７　委託先の事業者の対応にあたり、「個人情報保護の責任者」を選定する要件や考慮すべきこと（「個人情報の保護について一定の知識」など）はあるか。 20

経Ｑ－８　委託と第三者提供の情報管理責任上の違いは何か。 20

経Ｑ－９　外部監査はどのような機関に依頼すべきか。 21

企画管理編 23

企Ｑ－１　部門系で発生し、部門システムに保管する記録等は、ガイドラインでいう診療録、診療諸

記録等としての適用を受けるのか。 23
企Ｑ－２　「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）や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」とあるが、具体的にはどのようなものが想定されているのか。 24
企Ｑ－３　医療情報システム導入に際して規程等を作成したいが、どのようなものが望ましいのか。 25
企Ｑ－４　医療機関等がこのガイドラインに基づき、診療録等の電子保存に係る運用管理規程を作成し、その規定に沿って運用している場合、医療機関等の特性に応じた対象となる項目が本ガイドラインを満足していない項目があった場合、問題となるのか。 26
企Ｑ－５　委託したクラウド型の電子カルテサービス業者から自院の患者に関するデータが漏えいした場合、自院にはどのような責任が問われるのか。 27
企Ｑ－６　第三者提供における責任分界をどのように考えればよいか。 27
企Ｑ－７　第三者提供は、どの時点で成立するか。 28
企Ｑ－８　企画管理編２．２．３では第三者提供で責任分界を定める例が示されている。地域医療連携において、医療機関間での第三者提供の責任分界を定める際、どのような留意事項があるか。 28
企Ｑ－９　地域連携のための医療情報システムとして、医療情報の所在だけを管理するレジストリと、各医療機関等が共有のために確保するリポジトリを設置する形態をとっている。利用者は、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE　XDS 統合プロファイル※）。この場合、各医療機関等は互いに保管された医療情報を共有する形となるので、共同利用という形と考えてよいか。 29
企Ｑ－10　医療情報の共同利用において、どのような留意事項があるか。 30
企Ｑ－11　医療情報連携ネットワークにおける情報連携に際して、共同利用型の場合、どのような留意事項があるか。 30
企Ｑ－12　地域医療連携で暗号化を用いて第三者提供等を行う際、これに係る医療機関等と医療情報システム・サービス事業者における責任分界において、どのような留意事項があるか。 31
企Ｑ－13　医療機関等の施設外から医療情報システムにアクセスする場合に、接続する者と医療機関等との間での責任分界において、どのような留意事項があるか。 31
企Ｑ－14　地域医療連携における第三者提供等で、外部保存を受託する事業者が介在する場合、これに係る医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。 32
企Ｑ－15　レセプトのオンライン請求のように、第三者提供が法令に定められている場合、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。 33
企Ｑ－16　外部保存を委託する際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。 33
企Ｑ－17　医療機関等の業務の一部を委託することに伴い情報が外部に保存される際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。 34
企Ｑ－18　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）として「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。」とあ

るが、どのように患者へ説明を行うべきか。 35
企Q－19　リスク分析で想定する脅威について、どのようなものがあるか。 36
企Q－20　「 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、管理することが重要である」とあるが、医療情報の場合にはどのような考え方に基づいて行う必要があるか。 38
企Q－21　医療情報システムで扱う情報の重要度の分類、確認方法、リスク分析結果はどのようにまとめるべきか。 39
企Q－22　電子化された診療情報を外部保存できるか。できる場合、求められる要件は何か。 40
企Q－23　クラウド型の電子カルテサービスを行う業者に認定制度のようなものはあるのか。もしなければ、業者を選定する際に３省のガイドライン※に準拠していることは、どうやって確認すればよいのか。 40
企Q－24　医療情報の外部保存を行う際、どのような留意事項があるか。 41
企Q－25　医療機関等や委託事業者に外部保存を委託する場合、保存する情報の取り扱いに関して、どのような留意事項があるか。 42
企Q－26　外部保存を委託する事業者の選定において、どのような留意事項があるか。 44
企Q－27　ISMS 認証を取得している事業者に対して、根拠資料を求めることはできるのか。 44
企Q－28　７．安全管理のための人的管理⑥ｇの「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」とは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」や「JASA クラウドセキュリティ推進協議 会 CS ゴールドマーク」等で公開されたサービスリストやマーク取得サービス一覧などに掲載されていることを確認することでよいか。 44
企 Q－29　外部保存を委託する場合のデータ閲覧権限はどうするといいか。 46
企 Q－30　個人識別に係る情報を適切に保管するために、外部保存を委託する事業者にどのような対策を求めればいいか。 46
企 Q－31　外部保存の委託を終了する際、どのような留意事項があるか。 46
企Q－32　医療情報の外部保存に関して、院内掲示以外の患者等への周知方法はどのようなものがあるか。 47
企 Q－33　病態、病歴等を含めた個人情報の外部保存を行う場合、患者等にどのような説明を行うべきか。 47
企 Q－34　個人情報が保存されている機器が設置されている区画への入退管理の方法として、どのようなものが挙げられるか。 48
企 Q－35　情報及び情報機器の持ち出しを認める場合、どのような留意事項があるか。 48
企 Q－36　「リスク評価に基づいて、医療情報の持ち出しに関する方針や、持ち出す情報、持ち出し方法に関する手順や管理方法を情報管理に関する規程で定める。」とあるが、具体的にどのような基準で判断をすればよいか。 49
企 Q－37　患者等に診療情報等を提供する場合、どのような留意事項があるか。 50
企 Q－38　「確実に情報の破棄されたことを確認すること」とは立ち会いを前提としているのか。 50
企 Q－39　情報及び情報機器の持ち出し並びに外部利用をする場合にどのような対応が必要か。 51
企 Q－40　事前の確認時と状況が変わり、請負事業者が倒産する等してソフトウェアの保証がなくなった場合、見読性は確保されていないことになるのか。 51
企 Q－41　医療情報システムに関する BCP（Business Continuity Plan：事業継続計画）の作成は、

医療機関にとってどのような場面を想定するといいか。 52
企 Q－42　BCP（Business Continuity Plan：事業継続計画）の内容を検討する上で、参考になる内容はあるか。 52
企 Q－43　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは、真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか。）。 54
企 Q－44　「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」にするために、どのようなリスクを想定すればよいか。 55
企 Q－45　本人確認の方法として eKYC を採用する場合、どのような留意事項があるか。 56
企 Q－46　法令で定められた記名・押印を電子署名で行うことについて、どのような経緯があるか。 57
企 Q－47　通常閉域ネットワークを構築することが多い医療機関等において、一枚一枚の文書にリアルタイムにタイムスタンプを付与することは、実装が困難ではないか。 58
企 Q－48　クラウド型の電子カルテサービスを行う場合、利用者によるトランザクションごとに電子署名が必須となるのか。 58
企 Q－49　１４．法令で定められた記名・押印のための電子署名①１⑵の「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署名等を用いること」とあるが、要件を満たす具体的な手段は何か。 59
企 Q－50　１４．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電子署名の要件のうち、①1(2)（ｂ）にある「医療機関等の管理者」とは、具体的には組織単位で考えればよいか。 59
企 Q－51　１４．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電子署名の要件①１（２）（ｂ）において、身分証明書や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）」とあるが、この「署名」と「押印」は同等と考えてよいか。 60
企 Q－52　タイムスタンプはパソコンの時間と同じでよいか。 60
企 Q－53　暗号化を行うための適切な鍵管理を行うために、どのような対応が考えられるか。 ... 60
企 Q－54　「８．情報管理（管理、持出し持ち出し、破棄等）③において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。」とあるが、例えば外来やナースステーション等では、それらの措置は困難ではないか。 62
企 Q－55　「２．１．１　医療機関等における責任と責任分界の運用管理においては、医療機関等と情報システム・サービス事業者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うえで、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。」とあるが、契約書の記載方法を教えてほしい。 62
企 Q－56　外部の医療機関等から持ち込まれた X 線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか。 62
企 Q－57　保守要員の専用アカウントの不正使用を防止するためにどのような方法があるか。また保守作業にあたってどのような作業を求めるといいか。 63

企Q－58　「スキャナによる読み取りの際の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・タイムスタンプ等を遅滞なく行うこと。」とあるが、これは取り込み責任者を明確にすることか。 64
企 Q－59　「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。」とあるが、一定期間以内とはどれ位をいうか。外来診療の場合、１日の診療が終わった後にまとめて行う等の運用でもよいか。 64
企Q－60　どの程度の期間内でスキャナ等により電子化して保存すべきか。 64
企 Q－61　電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。 65
企Q－62　①　診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。②　電子化された場合、法定保存年限を経過した文書も保存すべきと考えるべきか。 65
企Q－63　「「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」とあるが、電子保存した内容を再度プリントアウトして、訂正後に再度電子化して保存するといった運用でもよいか。 66
企Q－64　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度がいいか。 67

システム運用編 69

シＱ－１　「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）」は具体的に何を遵守すればよいのか。 69
シＱ－２　①相互運用性と標準化を行うことのメリットは何か。②基本データセットや標準的な用語集、コードセットを実装しなかった場合、どのような不利益が想像されるか。 69
シＱ－３　「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、標準項目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こと」とあるが、標準形式は正式に定められたものがあるのか。 70
シＱ－４　基本データセットを利用し、一般財団法人医療情報システム開発センター（MEDIS-DC）の標準マスタを組み合わせた場合、医療情報システムのリプレイス時の相互運用性は保証されるか。 73
シＱ－５　データ交換のための国際的な標準規格については、どのようなものがあるか。 73
シＱ－６　外字の使用について注意すべき点は何か。 74
シＱ－７　診療情報等が復元できなくなることなどが生じないように、どのような対応をすべきか。 74
シＱ－８　見読性を確保するために、どのような対応が必要か。 75
シＱ－９　汎用性が高く、見読するソフトウェアに困らない形式にはどのようなものがあるのか。 75
シＱ－10　X 線 CT の検査で、オリジナルの画像のほかに、オリジナル画像から生成した３Ｄ画像も使って診断している。電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３Ｄ画像は消去してしまっても構わないか。 76
シＱ－11　3D 画像処理を行った場合、処理を行う元となった画像は保存しなければならないか。 76

シＱ－12　確定保存された画像に関し、診断や患者説明のために一時的に医師が表示方法（濃度の変更、拡大など）のみを修正した場合、この画像を保存する必要があるか。 76
シＱ－13　検像において、検像前の画像情報、検像後の画像情報のいずれを保存対象とすべきか。 77
シＱ－14　「職員による外部からのアクセスを行う場合は、利用する PC 等の端末の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術の導入を検討するなどの対応が求められる。」とあるが、どのような留意事項があるか。 78
シＱ－15　医療情報システム・サービス事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合はどのような対応をすべきか。 78
シＱ－16　情報機器の持ち出し又は外部利用をする場合どのような対策をすべきか。 78
シＱ－17　情報の破壊及び混同等を防ぐために、どのような対策が挙げられるか。 79
シＱ－18　不正ソフトウェア対策等が大変なので、外部と遮断した環境を設定する方が望ましいのか。 79
シＱ－19　医療等分野における IoT 機器に対する安全対策を行う上で、どのような留意事項があるか。 80
シＱ－20　「８．５　医療機関等が管理する以外の機器情報機器の利用に対する対策」について、適切な技術的対策や運用による対策はどのようなものがあるか。特に BYOD を行う場合に、どのような安全対策が必要か。 81
シＱ－21　IoT 機器を含む医療情報システムの接続状況や異常発生を把握するためにはどのような方法あるか。 81
シＱ－22　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度であればいいか。 82
シＱ－23　医療情報システム・サービス事業者による保守対応が行われた場合に、診療録にアクセスした証跡を確認する方法はどのようなものがあるか。 83
シＱ－24　医療情報システム・サービス事業者と保守契約を締結する際に、情報流出を防ぐためにどのような対応をすべきか。 83
シＱ－25　保守要員が外部機器を持ち込む場合、何を確認すべきか。 83
シＱ－26　「１１．１　通常時における運用対策表１１－１　平常通常時に対応すべき技術的対応の例の広域災害対策（遠隔地バックアップ等）とあるが」とあるが、「遠隔地」の定義はあるのか。 84
シＱ－27　システムが停止した場合の診療継続に備え、見読性を確保するために、医療情報システムにどのような対策を講じるべきか。 84
シＱ－28　大規模災害の発生により、サーバ等が使用できなくなった場合に備えてバックアップ体制はどのように構築すべきか。 84
シＱ－29　非常時における利用に備えて、診療録等をどのように保存すべきか。 85
シＱ－30　障害等によるデータ保存時の不整合に備えて、どのような対応をすればいいか。 85
シＱ－31　不適切な保管・取扱いによる情報の滅失、破壊を防止するために、どのような対応が考えられるか。 86
シＱ－32　診療録等のデータを保存するサーバ等を保管する区画において、不正な行動による破壊の防止するために、どのような方法があるか。 86
シＱ－33　診療録等のデータのバックアップの管理や方法に関して、どのような留意事項があるか。 87

シＱ－34　記録媒体、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に、どのような対応が考えられるか。 87
シＱ－35　医療情報の入力や閲覧に際して、情報の漏えいを防ぐために具体的にどのような対策をすべきか。 87
シＱ－36　専用線以外の回線サービスを利用する場合、どのような留意事項があるか。 88
シＱ－37　医療機関等におけるネットワークに対する不正アクセスへの対策を講じる際、どのような留意事項があるか。 91
シＱ－38　「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すること。」とあるが、どのようなものが安全性が確認できる機器として考えられるのか。 92
シＱ－39　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）とは、具体的にどのような事象を指すものか。 92
シＱ－40　「１３．ネットワークに関する安全管理措置 」⑥に「 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」とあるが、具体的にはどのように利用するのか。 93
シＱ－41　無線 LAN の利用において、どのような留意事項があるか。 94
シＱ－42　「なりすまし」に対しては、具体的にどのような対応をとればいいか。 94
シＱ－43　「盗聴」に対しては、具体的にどのような対応をとればいいか。 94
シＱ－44　「改ざん」への対応として、どのような留意事項があるか。 95
シＱ－45　ネットワークを介して送信元と相手先の当事者間でやりとりする情報に対する暗号化等のセキュリティ対策を実施するためにはどのような技術があるか 95
シＱ－46　許可された者以外の無線 LAN の利用を防止するためにはどのような対策が必要か。 . 96
シＱ－47　医療機関等におけるローカル５Ｇの利用について、具体的な事例等はあるか。 96
シＱ－48　認証方法が安全な利用者の識別・認証方法を選定する際、どのような留意事項があるか。 97
シＱ－49　利用者の識別・認証に IC カード等のセキュリティ・デバイスを配布する場合、どのような留意事項があるか。 98
シＱ－50　「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」とあるが、類推を防ぐために定期的な変更を求めることは有効か。 98
シＱ－51　利用者の識別・認証で二要素認証を採用する際、指紋、虹彩等のバイオメトリクスを利用する場合、どのような留意事項があるか。 100
シＱ－52　FIDO 認証（※１）に関して、どのような留意事項があるか。 101
シＱ－53　ネットワーク上からの不正アクセスを防止するためにどのような対策が必要か。 101
シＱ－54　パスワードを用いた利用者認証に関して、不正な攻撃への対応としてどのようなことが挙げられるか。 102
シＱ－55　認証を伴う情報機器を通じた不正アクセスを防止するためにどのような対策が必要か。 104
シＱ－56　「虚偽入力、書換え、消去及び混同を防止する」ために、はどのように、どのような対応が求められるのか。 104
シＱ－57　「作成の責任の所在を明確する」ために、はどのように、どのような対応が求められるのか。 106
シＱ－58　医療情報システムの認証において、真正性の確保を求める場合について、記載されている

情報と確定者には具体的にどのような組み合わせがあるか。 108
シＱ－59　「１４．認証・認可に関する安全管理措置」 ⑧ｆにおいて、「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」とあるが、具体的にどのような場合を指すか。 109
シＱ－60　代行入力を行う場合、代行を許可した証拠はどのように残しておけばいいのか。 109
シＱ－61　記録を確定する方法として、①入力者が情報を入力画面を見ながら入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるが、それぞれどのように対応すべきか。 109
シＱ－62　画像の確定に当たっては明示的な確定操作が必要か。 110
シＱ－63　情報の重要度に応じでセキュリティ対策を講じたい場合どのように整理すべきか。 . 110
シＱ－64　法令で定められた記名・押印のための電子署名における要件として暗号に関するものがあるが、具体的にはどのようなものを採用する必要があるか。 111
シＱ－65　共通鍵、秘密鍵を使用して情報を管理する場合どの程度のレベルのものが必要か。 ..111
シＱ－66　「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にある「また、スキャンにより、保存できない有用な情報」とは、どのようなものがあるか。 ... 112
シＱ－67　診療録等をスキャナ等により電子化して保存する場合に、診療の用途に差し支えない精度の基準はあるか。 112
シＱ－68　「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、保存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。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。 112
シＱ－69　「１８．外部からの攻撃に対する安全管理措置」①の４つ目の「－」において、「重要なファイルは数世代バックアップを複数の方式で取得し、」とあるが、外部からの攻撃を受けた場合の復旧のための対応としては、どのような点を考慮して、バックアップを取得する必要があるか。 113

概説編

概説編

概Q－１　①このガイドラインは、医療機関等の関係者が読むもので、医療情報システムに関係するベンダや事業者は読む必要はないのか。②ベンダや事業者が遵守すべきガイドラインにはどのようなものがあるのか。

Ａ　医療情報システムの管理上の一次責任は医療機関側にありますので、医療機関等の関係者は、このガイドラインの内容をよく理解し、遵守していただく必要があります。

ただし、情報システムの安全管理は運用と技術とが相まって一定のレベルを達成するものです。特に、情報化が進み、多様なシステムが導入され、利用されている医療機関等においては、システムの構築はじめ安全管理を医療機関等の関係者のみで実施することは少なく、システムに関係するベンダや事業者の協力を得て、情報システムの安全管理を実施することが多いです。そのため、医療情報システムを安全に管理・運用するのは、医療機関側の責任ですが、システムに関係するベンダや事業者にも本ガイドラインを読んでいただき、医療機関等側が負う責任や遵守すべき内容について理解を深め、より安全な情報システムの管理・運用が果たされるような協働を働きかけることは有用です。

協働するベンダや事業者には、医療情報システムの安全管理の観点ではこのガイドラインを、医療情報システムで取り扱う個人情報の保護の観点では「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」を理解していただくことが望ましいです。

なお、ベンダや事業者といった医療情報システム・サービスに関係する事業者に対しては、総務省・経済産業省が「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」を策定しています。ベンダや事業者はそのガイドラインの内容をよく理解していただく必要があります。

概２．１章

概Q－２　どのような場合に、介護事業者は本ガイドラインの内容を遵守する必要があるか。

Ａ　下記のような事例等が想定されます。

介護事業者が取り扱う e-文書法の対象範囲となる文書に、医師等から提供を受けた患者の医療情報を記入し、電子保存を行う場合。

上記のほか、医師等が作成した患者の医療情報を情報システムにより取り扱う場合。

概２．２章

概Ｑ－３　他の医療機関等から提供された電子化された情報の取扱いは、このガイドラインの対象となるのか。

Ａ　このガイドラインは、医療に関わる情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人又は組織が対象となっています。

そのため、このガイドラインの対象情報は、前文の情報システムや人又は組織の中で扱われる情報のうち、①「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。）に含まれている文書、②施行通知には含まれていないものの、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。）の対象範囲で、かつ、患者の医療情報が含まれている文書等（麻薬帳簿等)、③法定保存年限を経過した文書等、④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像、⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等が対象です。

したがって、他の医療機関から提供された電子化された情報についても、電子化された状態で利用・保存する限りはこのガイドラインの対象となります。

なお、個人情報の取扱いについては、個人情報の保護に関する法律（平成１５年法律第５７号。以下「個人情報保護法」という。)、「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」等を参照してください。

概２．２章

概Ｑ－４　電子保存が認められている文書とは具体的に何か。

Ａ　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。以下「e-文書法省令」という。)、施行通知で定められた文書です。

概２．３章

概Ｑ－５　「医療情報システム」とは具体的に何を示すのか。

Ａ　医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末も範ちゅうとして想定しています。また、医療情報が通信される院内・院外ネットワークも含まれます。

概説３．２章

概Ｑ－６　オンライン資格確認や電子処方箋の導入において、どのような留意事項があるか。

Ａ　オンライン資格確認や電子処方箋の導入については、厚生労働省のホームページや医療機関等向けポータルサイトに資料が掲載されています。

［オンライン資格確認］
- 厚生労働省 オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）
  https://www.mhlw.go.jp/stf/newpage_08280.html
- オンライン資格確認・医療情報化支援基金関係医療機関等向けポータルサイト
  https://www.iryohokenjyoho-portalsite.jp/

［電子処方箋］
- 厚生労働省 電子処方箋
  https://www.mhlw.go.jp/stf/denshishohousen.html
- 電子処方箋ポータルサイト
  https://iryohokenjyoho.service-now.com/csm?id=csm_index

本ガイドラインを踏まえた留意事項としては、
- 「オンライン資格確認導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」
- 「ネットワーク整備を含むオンライン資格確認導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」
- 「電子処方箋導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」

に掲載されている「システム事業者へ発注」「導入・運用準備」のステップにおいて、「オンライン資格確認の機器」「医療機関等が利用するシステム（レセプトコンピュータ、電子カルテシステム/薬局システム）」「オンライン請求ネットワーク」「ルーターなどのネットワーク機器」の購入・設置・設定・保守に関係するシステム事業者との間で、役割分担や責任分界を明確にし、契約や体制、ネットワーク構成図、機器設定を適切に管理することが求められます。

概４．３章

概Ｑ－７　医療情報を電子的に保存するに当たって定められた要件は何か。また、情報セキュリティの３要素（機密性・完全性・可用性）との違いはあるか。

Ａ

電子保存の３要件は、「書面の保存等に関し、電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法」[3]に必要とされる要件で、

- 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」
- 見読性とは「電子媒体に保存された内容を、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で、肉眼で見読可能な状態にできること」
- 保存性とは、「記録された情報が法令等で定められた期間にわたって真正性を保ち、見読可能にできる状態で保存されること」

と定義されています。

これは、e-文書法令第４条第４項の第１号から第３号までを具体化したものと言えます。

一方、情報セキュリティの３要素（機密性・完全性・可用性）は、情報資産の安全かつ信頼できる利用において求められる、情報セキュリティにおける要素です。これらについては、概説編「４．２　医療情報システムの安全管理に必要な要素」で詳述しています。

電子保存の３要件と、情報セキュリティの３要素が総じて満たすことは、多くの部分で重なります。例えば、文書を電子化したファイルが、完全性と可用性を満たすことにより、見読性の要件の大半を満たすと評価することができます。また、機密性を満たすことにより、真正性の要件の多くを満たしていると評価することもできます。さらには、機密性、完全性、可用性を満たすことで保存性の要件の多くを満たすことが可能であると考えられます。

[3] 「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号）第 1 条

本ガイドライン第６．０版ではこのような関係を踏まえて、電子保存３要件のうち、情報セキュリティ３要素と重なる部分については、e-文書法令の対象だけではなく、医療情報を取り扱う情報システム全般に適用し、情報セキュリティの３要素から、遵守事項等を整理しました。

その上で、情報セキュリティ３要素だけでは満たせない内容については、別途遵守事項として定め、システム運用編の別添に示しています。

概Q－８　SNS 等の Web サービスを利用して医療情報をやり取りする場合、考慮するべきことはあるか。

Ａ　SNS（Social Networking Service）等の Web サービスを利用して患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要があります。

特に、SNS の場合、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNS を利用する際に気を付けるべき事項」[4]を参考に、適切な対策を講じてください。

概Q－９　第５．２版では、付表で小規模病院、診療所などの対応について示されていたが、小規模の基準は病床数や職員数で決められているのか。また第６．０版では、小規模病院等の対応について、同様の対応などが示されているのか。

Ａ　「小規模」に、明確な数値基準はありません。

医療情報システムの安全対策におけるリスクを考える上で、医療機関等の規模は一つの視点となりますが、必ずしも規模だけでリスクやその対策が決まるわけではありません。例えば小規模医療機関等であっても、医療情報を取り扱うシステムを、医療機関等自らがアプリケーションを使って開発し、運用している場合には、システム開発や運用に関するリスクは必ずしも低くはなく、したがって適切な対策が求められます。

医療機関等においては、専任の情報システム運用担当がいない場合や、医療情報システムを外部のクラウドサービスにするなどで、医療機関等の直接的な負担を軽減し、安全な医療情報の取り扱いを図るため、外部の医療情報システム・サービス事業者に運用等を委ねる場合があり、小規模医療機関等において、特にみられる傾向と言えます。

第６．０版では、このように医療機関等の規模の大小ではなく、医療機関等における体制や、医療情報システムの構成に着目し、医療機関等に専任のシステム運用担当者が存在しない場合や、利用する医療情報システムがクラウドサービスだけの場合には、本ガイドラインの一部については、参照を簡略化できることとしています。

[4] https://hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf
f

このように小規模医療機関等における対策の負担軽減を直接示す内容は含まれていないものの、実質的には外部委託の活用等の対応が図れるようにしています。

また、診療所や薬局等の小規模医療機関等向けの特集も、補足資料として用意していますので、適宜、ご参照ください。

概Q－10　旧版のガイドラインの本編や別冊や別添等、全て読む必要があるか。

Ａ　旧版は読む必要はありません。旧版の内容は、最新版で変更又は削除等されている場合があるため、最新版をお読みください。

概Q－11　このガイドラインの説明会や研修会等は実施されていないのか。

Ａ　厚生労働省として実施しているものはありませんが、一般社団法人日本医療情報学会や一般社団法人保健医療福祉情報システム工業会等による講演会等で、解説が行われることがあります。

なお、厚生労働省では、医療機関等向けサイバーセキュリティ研修用動画、教材を提供しております[5]ので、こちらも参考にしてください。

[5] https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

経営管理編

経営管理編

１．安全管理に関する責任・責務

経１．１章

経Ｑ－１　電子的な医療情報を扱う責任を果たすうえで、どのようなことを理解すればいいか

Ａ　医療に関わる全ての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、医療情報の取扱いも同様です。このことから、医療機関等の管理者には、収集、保管、破棄を通じて刑法（明治 40 年法律第 45 号）等に定められている守秘義務、個人情報保護に関する諸法及び指針のほか、医療情報の扱いに関わる法令、厚生労働省通知、他の指針等により定められている要求事項を満たすために適切な措置を講じることが求められます。平成 29 年５月に施行された平成 27 年度改正個人情報保護法では、個人情報の定義が明確化されるとともに、取扱いに特に配慮を要する「要配慮個人情報」や、特定の個人を識別することができないように加工した「匿名加工情報」等について、新たに規定が設けられた。このことを受けて、個人情報保護委員会が個人情報保護法についてのガイドラインを公表し、医療・介護分野においては「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」（平成 29 年 4 月 14 日、個人情報保護委員会・厚生労働省）等が定められているため、関連する規定を遵守し、適切な措置を講じてください。

故意に医療情報を漏えいさせた場合、刑法上の秘密漏示罪として犯罪行為となることがありますが、医療情報については過失による漏えいや目的外利用でも、故意の漏えいと同様に大きな問題となり得ます。そのため、医療機関等の管理者には、そのような事態が生じないよう、善良なる管理者の注意義務（善管注意義務）を果たすことが求められます。本来、医療情報の価値と重要性はその保存方法によって変化するものではないため、医療情報を電子化して保存する場合でも、医療機関等の管理者には、紙やフィルムにより院内に保存する場合と、少なくとも同等の善管注意義務を負うと考えられます。

ただし、電子化された医療情報には、次のような固有の特殊性もあります。

- 紙の媒体やフィルム等に比べて、その動きが一般の人にとって分かりにくい側面がある
- 漏えい等の事態が生じた場合に、一瞬にして大量に情報が漏えいする可能性がある
- 医療従事者が電子化された情報の取扱いの専門家とは限らないため、その安全の確保に慣れていないケースが多い

したがって、それぞれの医療機関等がその事情によりメリット・デメリットを勘案して電子化の実施範囲及びその方法を検討し、導入する医療情報システムの機能や運用方法を選択して、それに対して求められる安全基準等への対応を決める必要があります。

また、電子化された医療情報が医療機関等の施設内にとどまって存在するのではなく、ネットワークを用いた交換、共有、委託等が考えられる状況下では、その管理責任は、医療機関等だけでなく、医療情報システム・サービス事業者等にもまたがるようになります。

経１．１．２章

経Q－２　医療情報の取扱いに際し、令和２年改正・令和３年改正個人情報保護法も含めて、医療機関等にはどのような責任が生じるか。

Ａ　医療情報の取扱いにおいては、まず医師法、医療法等において適正な管理が求められており、例えば医療法では診療記録を適切に備えることが求められています（第 21 条第１項第９号等）。

また医療情報は患者に関する個人情報であることから、個人情報保護法の適用対象になることは言うまでもありません。令和２年改正個人情報保護法では個人情報取扱事業者（医療機関等も含む）が医療情報のような要配慮個人情報を流出させた場合には、個人情報保護委員会に報告し、本人にも通知することが義務づけられました（法第 26 条、規則第６条の２、第６条の３）。

そのような報告義務・通知義務や、その前提である個人情報の安全管理のための措置を講じる義務（法第 23 条）等に違反しており、個人の権利利益を保護するため必要があると認められた場合には、個人情報保護委員会から当該医療機関等に対して是正勧告がなされることになります（法第 145 条第１項）。さらに是正勧告に正当な理由なく対応しない、違反行為がなされる等により、個人の重大な権利利益の侵害が切迫していると認められた場合には、個人情報保護委員会から違反行為の中止や是正措置実施の命令がなされます。（法第 145 条第２項、第３項）

令和２年改正個人情報保護法では、個人情報保護法に対する重大な違反行為に対する罰則も強化されています。例えば、上記の個人情報保護委員会から医療機関等に対する命令違反が生じた場合、命令違反をした場合の代表者や従業員が属する法人に対する罰金刑は従来の 30 万円以下から１億円以下に大きく強化されています。医療情報などの個人情報データベースを、不正に提供等を行った場合も同様の罰金刑となっています（法 179 条第１項）。

このように個人情報保護法では医療情報が漏洩した場合の報告義務等や、これに関連して必要な対応を行わずに命令違反を行った場合の医療機関等に対する罰則などが強化されていることを十分理解する必要があります。

なお、令和３年改正法では、医療機関等における責任に直接関係する内容の改正はありませんが、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用することとしています。

経１．２章

経Ｑ－３　このガイドラインに従いシステム構築等をしていたにも関わらず起こった情報セキュリティインシデントについて、責任のあり方をどのように考えるべきか。

Ａ　このガイドラインは、医療情報システムの安全管理及び e-文書法への適切な対応に関し、厚生労働大臣が法を執行する際の基準となるものの一つです。技術的なことだけではなく、運用を含めた安全対策を示したものであり、ガイドラインを遵守していたと認められる状況下で起こった情報セキュリティインシデントについては、一定程度の法的責任を果たしていたということが可能だと考えられます。

　しかしながら、その情報セキュリティインシデントによって患者等の第三者が不利益を被った場合に全て免責されない可能性もあります。医療情報システム運用時の責任についての考え方を「企画管理編　２．責任分界」に記していますので、適宜、ご参照ください。

経１．１．２章

経Ｑ－４　このガイドラインを遵守しなかった場合、課せられる罰則等や e-文書法以外に抵触する法令はあるのか。

Ａ　本ガイドラインは、e-文書法が医療分野において執行される際の指針となります。ガイドライン自体に罰則はありませんが、ガイドラインに違背した状態は、法令を遵守していないとみなされる可能性があります。

　本ガイドラインには、法令により要求されている事項等が列挙されています。したがって、これに違背することにより、e-文書法に求められる要件を満たすことができていないと認められる場合には、医療に関係する多くの法令等に違反したとみなされ、その罰則が適用されるおそれがあります。

経１．２．１章

経Ｑ－５　通常運用時において説明責任を果たす際、患者にどのような説明をすべきか。

Ａ　「診療情報を適正に保存するとともに、適正に利用すること」を医療情報システムの安全管理に関する方針の中に盛り込み公表する必要があります。また、詳細は、苦情・質問を受け付ける窓口を設け、「１．２．１　通常時における責任の【説明責任】」の項目の問い合わせに回答できるように、準備しておく必要があります。

経１．３章

経Ｑ－６　委託している事業者において、情報漏えい等の情報セキュリティインシデントが発生した場合、事業者に対応をさせればよいのか。

Ａ　情報漏えい等の情報セキュリティインシデントに際しては、当該情報を一次管理している医療機関等側に、説明責任及び善後策を講ずる責任が発生します。もちろん情報セキュリティインシデントを起こした事業者側も責任を免れるものではなく、両者が協力して説明及び善後策を講じる必要があります。

経１．２．１章

経Ｑ－７　委託先の事業者の対応にあたり、「個人情報保護の責任者」を選定する要件や考慮すべきこと（「個人情報の保護について一定の知識」など）はあるか。

Ａ　具体的な要件が定められているものではありませんが、医療に関わる全ての行為は、医療法等で医療機関等の管理者の責任で行うことが求められています。そのため、結果的には、個々の医療機関等の管理者が、権限を一部委譲するに適当と考える者を「個人情報保護の責任者」として選任することになると考えられます。

電子化された「個人情報の保護についての一定の知識」についても、具体的な条件は示されていませんが、電子化された情報は、紙媒体の情報に比べ容易に大量の情報が漏洩する可能性がある特徴を持つことから、それらの特徴と扱い方について理解していることが重要です。

経１．３．２章、１．４章

経Ｑ－８　委託と第三者提供の情報管理責任上の違いは何か。

Ａ　委託とは、契約書等に基づき、業務の一部（例えば臨床検査）を外部に託すものであり、その情報の管理責任は一義的には委託元にあります。したがって、委託元は委託先の情報管理を監督しなければなりません。

それに対し、第三者提供（例えば紹介状による治療情報の提供）とは、患者等の同意の下に情報を他の事業者等に提供することです。第三者提供では、情報提供が確実に行われた時点で提供された情報の管理責任は提供先に移動します。

ただし、電子化された情報は提供が行われた場合でも提供元にも同じ情報が残ることが多く、残った情報の管理責任がなくなるわけではありません。

経３．３．２章

経Ｑ－９　外部監査はどのような機関に依頼すべきか。

Ａ　医療機関等が少人数の職員により運営されている等、内部監査の体制を構築できない場合には、第三者に外部監査を依頼することが考えられます。「第三者」の選定に際しては、依頼する監査の内容に応じて、医療情報システムに関する知見やシステムに求められる特性への理解を有していることが必要な場合もあれば、医療情報システムに関する知見や理解は持たず、一般的な情報セキュリティや情報システムに関する知見を有していることが重要な場合もあり、特定または専門の監査機関等に限られるものではありません。医療機関等として外部監査の目的や意義を踏まえて依頼する機関の選定を行ってください。

企画管理編

企画管理編

１．管理体系

企１章①第①条、１６章

企Q－１　部門系で発生し、部門システムに保管する記録等は、ガイドラインでいう診療録、診療諸記録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果等、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記のないものについては、スキャンして電子化した情報を原本として、元の紙を廃棄してよいか。

※　スキャンする際、どの患者の結果で、誰が、いつ記録したか、は登録することを前提とする。

※　紹介状や同意書等、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則である。

上記の場合、診療録等として確定することになるのは、どの行為の時点になるのか。

スキャン時の作業責任者と情報作成管理者は、どのようになるのか。

また、情報作成管理者は、有資格者等である必要があるのか。

手書きの付記等がある場合は、どのように行えばよいのか。

Ａ　診断の根拠となる記録や診療方針に影響を与える記録等は、定められた期間保存する必要があります。紙等の物理媒体の保存義務がある記録をスキャナ等により電子化して保存する場合は、「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」を参照してください。

確定については、紙等の記録が作成された時点で記録は確定しており、確定された記録を電子化しているため、「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」に規定されるように、電子化された情報を保存義務の対象として扱うことができます。

作業責任者と情報作成管理者は運用管理規程等で定め、適正に運営されていることを監査すること等が求められますが、有資格者である必要はありません。

企１章第⑤条

企Q－２　「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）や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」とあるが、具体的にはどのようなものが想定されているのか。

Ａ　関係する個人情報保護方針や医療情報システムの安全管理に関する方針について解説します。

【個人情報保護方針】

個人情報保護に関する方針に盛り込むべき具体的内容等について、「JIS Q 15001:2017（個人情報保護マネジメントシステム-要求事項）」では、下記のように定めています。

A.3.2.1　内部向け個人情報保護方針

トップマネジメントは，5.2.1 e）に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない。

a）事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること［特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下，“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。］。

b）個人情報の取扱いに関する法令，国が定める指針その他の規範を遵守すること。

c）個人情報の漏えい，滅失又は毀損の防止及び是正に関すること。

d）苦情及び相談への対応に関すること。

e）個人情報保護マネジメントシステムの継続的改善に関すること。

f）トップマネジメントの氏名

トップマネジメントは，内部向け個人情報保護方針を文書化した情報を，組織内に伝達し，必要に応じて，利害関係者が入手可能にするための措置を講じなければならない。

A.3.2.2　外部向け個人情報保護方針

トップマネジメントは，外部向け個人情報保護方針を文書化した情報には，A.3.2.1 に規定する内部向け個人情報保護方針の事項に加えて，次の事項も明記しなければならない。

a）制定年月日及び最終改正年月日

b）外部向け個人情報保護方針の内容についての問合せ先

トップマネジメントは，外部向け個人情報保護方針を文書化した情報について，一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。

【情報システムの安全管理に関する方針】

情報システムの安全管理に関する方針に盛り込むべき具体的内容等について、「JIS Q 27001:2014（情報セキュリティマネジメントシステム-要求事項）」では、下記のように定めています。

5.2 方針

トップマネジメントは、次の事項を満たす情報セキュリティ方針を確立しなければならない。

a) 組織の目的に対して適切である。

b) 情報セキュリティ目的（6.2 参照）を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。

d) ISMS の継続的改善へのコミットメントを含む。

情報セキュリティ方針は、次に示す事項を満たさなければならない。

e) 文書化した情報として利用可能である。

f) 組織内に伝達する。

g) 必要に応じて利害関係者が入手可能である。

企１章第⑥条

企Q－３　医療情報システム導入に際して規程等を作成したいが、どのようなものが望ましいのか。

Ａ　個人情報保護方針については、「４．２　規程の整備（運用管理規程ほか）」において個人情報保護対策の制定について説明があります。また、「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、「Ⅰ　本ガイダンスの趣旨、目的、基本的考え方」「６．医療・介護関係事業者が行う措置の透明性の確保と対外的明確化」に要求事項が記載されているため、参照してください。

運用管理規程については、「４．２　規程の整備（運用管理規程ほか）」において、運用管理規程についての説明があります。

企１章第⑥条

企Q－４　医療機関等がこのガイドラインに基づき、診療録等の電子保存に係る運用管理規程を作成し、その規定に沿って運用している場合、医療機関等の特性に応じた対象となる項目が本ガイドラインを満足していない項目があった場合、問題となるのか。

Ａ　たとえ手段が異なっていても、ガイドラインの趣旨を踏まえて、同様の効果を発揮するように実施することが求められます。「医療機関等の特性に応じた対象となる項目」が本ガイドラインを満足していない状態で何らかの問題が発生した場合は、医療機関等の特性に応じた対象となる項目本ガイドラインに沿った対応を行っていないことについて、理由や代替的にとっている措置に関する説明が求められます。

２．責任分界

企２章第①条

企Q－５　委託したクラウド型の電子カルテサービス業者から自院の患者に関するデータが漏えいした場合、自院にはどのような責任が問われるのか。

Ａ　本ガイドラインの「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）」の記述が適用されます。

管理責任は委託を行った医療機関等の責任者にあり、万一事故が起きた際には、受託する医療情報システム・サービス事業者と連携しながら本ガイドライン「経営管理編　１．２．２　非常時における責任」項の「説明責任」と「善後策を講ずる責任」を果たす必要があります。

企２章第⑥条

企Q－６　第三者提供における責任分界をどのように考えればよいか。

Ａ　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、医療機関等の管理者にとっては、原則として、提供先との責任分界に基づく範囲で責任を有しています。適切な第三者提供がなされる限り、提供された後の情報保護責任は、提供した医療機関等の管理者ではなく、提供を受けた第三者が負うことになります。

ただし、例外的に、提供先で適切に扱われないことを知りながら情報提供をしたような場合は、提供元の医療機関等の責任が追及される可能性があります。

一方、電子化された情報の特性に着目すると、医療情報が第三者提供されても、医療機関等の側で当該情報を削除しない限り、当該医療情報を引き続き保存し続けることになります。したがって、その情報について情報保護責任がなお残ることはいうまでもありません。

医療情報が電子化され、ネットワーク等を通じて情報が提供される場合、第三者提供の際にも、医療機関等から提供を受ける第三者に直接情報が提供されるのではなく、医療情報システム・サービス事業者が介在することがあります。この場合、いつの時点で、第三者提供が成立するのか、すなわち医療情報システム・サービス事業者との責任分界というべき概念が発生します。

一旦、適切・適法に提供された医療情報については、提供元の医療機関等に送付先での情報保護責任がないことは先に述べたとおりですが、第三者提供の主体は提供元の医療機関等であることから、患者等に対する関係では、少なくとも情報が提供先の第三者に到達するまで、原則として、提供元の医療機関等に責任があると考えることができます。その上で、医療機関等と医療情報システム・サービス事業者との間の内部的な意味での「善後策を講ずる責任」をいかに分担するかは、医療情報システム・サービス事業者と医療機関等の間で、あらかじめ協議して明確にしておくことが望まれます。医療情報システム・サービス事業者の選任・監督義務を果たしており、特に責任が明記されていない場合に、医療情報システム・サービス事業者の過失で何らかの不都合な事態が生じた場合は、医療情報システム・サービス事業者が全ての責任を負うのが原則です。

企２章第⑥条

企Ｑ－７　第三者提供は、どの時点で成立するか。

Ａ　第三者提供では、原則本人の同意の下に情報が第三者に提供され、説明責任を含む管理責任が第三者に生じます。

第三者が明確に自己の管理範囲に情報が存在することを確認した時点が、第三者提供の成立した時点になります。したがって、何らかの方法で受領確認を行う必要があり、受領確認がなされた時点と考えることができます。

オンラインで情報を送付する場合も同様であり、例えば相手のデータベースに格納されたことを電子的に確認する手続きを明確にした上で、その確認をもって第三者提供が成立することを、契約等で合意することが必要です。送り手は送付したと考えているものの、受け手が受領したと認識していない等、責任の空白ができないようにする必要があります。

企２章第⑥条

企Ｑ－８　企画管理編２．２．３では第三者提供で責任分界を定める例が示されている。地域医療連携において、医療機関間での第三者提供の責任分界を定める際、どのような留意事項があるか。

Ａ　医療機関間での第三者提供の責任分界を定める場合として、以下の場面について解説します。

【「医療情報システム・サービス事業者の提供するネットワーク」を通じて医療情報の提供元医療機関等と提供先医療機関等で医療情報を交換する場合の責任分界】

ここでいう「医療情報システム・サービス事業者の提供するネットワーク」とは、医療情報システム・サービス事業者の責任でネットワーク経路上のセキュリティを担保する場合をいいます。

提供元医療機関等と提供先医療機関等は、ネットワーク経路における責任分界点を定め、不通時や事故発生時の対処を含め、契約等で合意してください。

その上で、自らの責任範囲において、医療情報システム・サービス事業者との管理責任の分担について責任分界点を定め、医療情報システム・サービス事業者の管理責任の範囲及びサービスに何らかの障害が起こった際の対処主体を明らかにしてください。

ただし、通常運用における責任及び事後責任は、委託の場合、原則として提供元医療機関等にあり、第三者提供の場合、適切に情報が提供される限り原則として提供先医療機関等にある。医療情報システム・サービス事業者に過失がない場合、医療情報システム・サービス事業者に生じるのは、あくまで管理責任の一部に留まることに留意する必要があります。

【提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界】

ここでいう「独自に接続」とは、接続しようとする医療機関等同士がルータ等の接続機器を自ら設定して１対１や１対Ｎで相互に接続する場合や電話回線等の公衆網を使う場合を言います。

そのうち、あらかじめ提供先又は提供先となる可能性がある医療機関等を特定できる場合は、委託又は第三者提供の要件に従って両医療機関等が責務を果たすこととなります。

このような場合、医療情報システム・サービス事業者には管理責任は発生せず、通信の品質確保の責任は発生するとしても、医療情報システム・サービス事業者が提示する約款に示されるような一般的な責任に限られます。

一方、提供先又は提供先となる可能性がある医療機関等が特定できない場合は、法令で定められている場合等の例外を除いて、原則として医療情報を提供できません。

【共同利用により他の医療機関等が収集した医療情報を利用する場合の責任分界】

地域医療連携で医療情報を交換する際、個人情報保護法上の共同利用により他の医療機関等が収集した情報を利用できます。この場合、医療機関等の間での責任分界などを規約や契約などで明確にすることが必要です。

企２章第⑥条

企Ｑ－９　地域連携のための医療情報システムとして、医療情報の所在だけを管理するレジストリと、各医療機関等が共有のために確保するリポジトリを設置する形態をとっている。利用者は、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE　XDS 統合プロファイル※）。この場合、各医療機関等は互いに保管された医療情報を共有する形となるので、共同利用という形と考えてよいか。

※　https://www.ihe.net/

また、レジストリは民間事業者等のデータセンターを利用することが適当と考えられるが、各医療機関等はデータセンターに所在情報の管理を委託してもよいか。

Ａ　診療情報を「共同利用」するためには、個人データを特定の者との間で共同して利用することを明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等を、あらかじめ本人に通知等している必要があります（詳細は「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」を参照してください。）。本ケースの場合は、これらの要件が不明確ですので、共同利用の要件を満たしていない可能性があります。共同利用の要件を満たしてない場合、他の施設での診療情報の利用は第三者提供に当たります。また、レジストリについて医療機関等以外の外部の事業者のデータセンターを利用する際には、医療情報を外部保存する場合と同等の要件を満足する必要があります。

企２章第⑥条

企Q－10　医療情報の共同利用において、どのような留意事項があるか。

Ａ　共同利用は、個人データの第三者提供の例外として個人情報保護法上認められている個人データの利用形態です（個人情報保護法第 27 条第５項第３号）。これは、形式的には個人データを直接の提供先とは別の組織が利用するものの、本人からみて、直接個人データを提供した相手先と一体的な利用であると合理的に考えられるため、共同利用する者は第三者には含まれないという趣旨に基づくものです。例えば地域医療連携や共同研究などの場合に、このような利用が認められる場合があります。共同利用は無限定になされると、本人（患者等）の利益を損なうことから、共同利用者の範囲や利用目的などが、「本人が通常予期し得ると客観的に認められる範囲内である必要」があります（「個人情報の保護に関する法律についてのガイドライン（通則編））3-6-3（個人情報保護委員会））。共同利用の考え方については、上記ガイドラインを参照ください）。

なお、共同利用については、令和２年改正個人情報保護法により、本人への通知等の義務が強化され、共同利用の事実、共同利用の対象となるデータ項目、利用者の範囲、利用目的、管理責任者の指名等の通知等のほか、管理責任者の住所、法人代表者の氏名も併せて本人への通知等の対象となりました。

企２章第⑥条

企Q－11　医療情報連携ネットワークにおける情報連携に際して、共同利用型の場合、どのような留意事項があるか。

Ａ　医療情報連携ネットワークにおける情報連携において、個人情報保護法が求める要件を具備した場合には、共同利用として利用することが可能です。ガイダンスでは、「病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人データを特定の者との間で共同して利用することが予定されている場合、㈠共同して利用される個人データの項目、㈡共同利用者の範囲（個別列挙されているか、本人から見てその範囲が明確となるように特定されている必要がある）、㈢利用する者の利用目的、㈣当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名をあらかじめ本人に通知し、又は本人が容易に知り得る状態においておくとともに、共同して利用することを明らかにしている場合には」、共同利用として利用できるものとしています。

なお、上記、㈠、㈡ については変更することができず、㈢、㈣については、本人が想定することが困難でない範囲内で変更することができ、変更する場合は、本人に通知又は本人の容易に知り得る状態におかなければならない、とされます。

企２章第⑥条

企Q－12　地域医療連携で暗号化を用いて第三者提供等を行う際、これに係る医療機関等と医療情報システム・サービス事業者における責任分界において、どのような留意事項があるか。

Ａ　【医療情報が提供元／提供先で暗号化／復号される場合の責任分界】

提供元医療機関等の医療情報システムにおいて、送信前に医療情報が暗号化され、提供先医療機関等の医療情報システムにおいて医療情報が復号される場合、医療情報システム・サービス事業者の責任は限定的になります。

しかし、この場合でも、医療情報システム・サービス事業者の管理責任は存在するため、ネットワーク上の情報の改ざんや侵入、妨害の脅威に対する医療情報システム・サービス事業者の管理責任の範囲について契約で明らかにしておく必要があります。

【医療情報が医療情報システム・サービス事業者の管理範囲で暗号化される場合の責任分界】

医療情報システム・サービス事業者の中には、例えば暗号化された安全なネットワーク回線の提供を主たるサービスとしている事業者も存在します。

そのようなネットワーク回線を使う場合、事業者が提供するネットワーク回線上における情報保護責任やサービスの可用性等の品質確保責任は事業者に発生します。したがって、それらの責任について契約で明らかにしておきます。

ただし、医療情報システム・サービス事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、医療機関間での責任分界に沿った考え方の整理が必要です。

企２章第⑥条

企Q－13　医療機関等の施設外から医療情報システムにアクセスする場合に、接続する者と医療機関等との間での責任分界において、どのような留意事項があるか。

Ａ　外部から医療情報システムにアクセスする場合に、接続者と医療機関等の責任分界を定める場合として、以下の場面について解説します。

【施設外から自らの機関の医療情報システムにアクセスし業務を行う、いわゆるテレワークする場合の責任分界】

昨今、医療機関等においても、医療機関等の施設外から自らの機関の医療情報システムにアクセスし業務を行う、いわゆるテレワークが一般的になってきました。

テレワークは、責任分界の観点では自組織に閉じていますが、医療情報システム・サービス事業者が管理するネットワークを利用することになります。また、通信回線として、公衆回線や施設内のＷｉ-Fi 等の多様なものが利用されることとなるため、個人情報保護について広範な対応が求められることになります。

特に、医療機関等の企画管理者やシステム運用担当者でない医療機関等の職員につい

ても管理責任が問われることに注意を払う必要があります。

【第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス】

医療機関等の施設外から医療情報システムにアクセスする場合として、リモートログインを用いた医療情報システム・サービス事業者による遠隔保守（リモートメンテナンス）が考えられます。この場合、適切な情報管理やアクセス制御がなされていないと、医療情報の不正な読み取りや改ざんが行われるリスクがあります。他方、リモートメンテナンスを全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要するコストが増大します。

したがって、保守の利便性と情報保護との兼ね合いを見極めつつ、リモートメンテナンスを認めるかどうか整理する必要があります。

また、リモートメンテナンスの場合でも、当然、医療機関等に「通常運用における責任」、「事後責任」が存在するため、医療情報システム・サービス事業者の報告を定期的に受け、必要な監督を行い、管理責任を果たす必要があります。

企２章第⑥条

企Ｑ－14　地域医療連携における第三者提供等で、外部保存を受託する事業者が介在する場合、これに係る医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　地域医療連携で第三者提供等を行う際に、外部保存を受託する事業者が介在する場合、情報の保存を、外部保存を受託する事業者に委託することになるため、通常運用における責任、事後責任は医療機関等にあります。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等において管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要があります。併せて、地域医療連携における規約等において、提供側及び利用側の責任なども明らかにすることが求められます。

また、外部保存を受託する事業者とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておくことが求められます。

企２章第⑥条

企Q－15　レセプトのオンライン請求のように、第三者提供が法令に定められている場合、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　法令で定められている場合等の特別な事情により、医療情報システム・サービス事業者に暗号化されていない医療情報が送信される場合は、医療情報システム・サービス事業者及びネットワーク事業者等において盗聴の脅威に対する対策を施す必要があります。

そのため、ネットワークの管理責任を負っている医療機関等は、医療情報システム・サービス事業者と医療情報の管理責任についての明確化を行わなくてはなりません。

また、医療情報システム・サービス事業者に対して管理責任の一部又は全部を委託する場合は、それぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければなりません。

企２章第⑤条

企Q－16　外部保存を委託する際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　本ガイドラインの「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）」を十分理解して委託先の選定と適切な契約を結ぶ必要があります。患者等に対する責任の主体は委託を行う医療機関等であるため、医療機関等が説明責任を果たすための資料や説明の提供を受託する事業者との契約で定め、受託する事業者における情報の取扱いを医療機関等としても理解する努力が必要です。さらに、例えば電子カルテを提供する医療情報システム・サービス事業者と、そのデータの外部保存のための資源を提供する事業者は異なることがあります。この場合、例えば障害が起こった際の対処の責任範囲について両事業者間で明確に定めた上で、医療機関等が理解しておく必要があります。

下図は、医療機関等が複数の事業者と外部保存に関する契約を行う例ですが、障害等が発生した非常時の場合に、最初に原因調査の範囲を決める責任を負う主体や、原因調査に必要な調査協力義務などについての役割、範囲等をそれぞれの事業者と取り決めておくことが求められます。複数事業者の提供サービス内容や契約内容を合わせて、本ガイドラインの要求に漏れなく適合していることの確認が必要です。

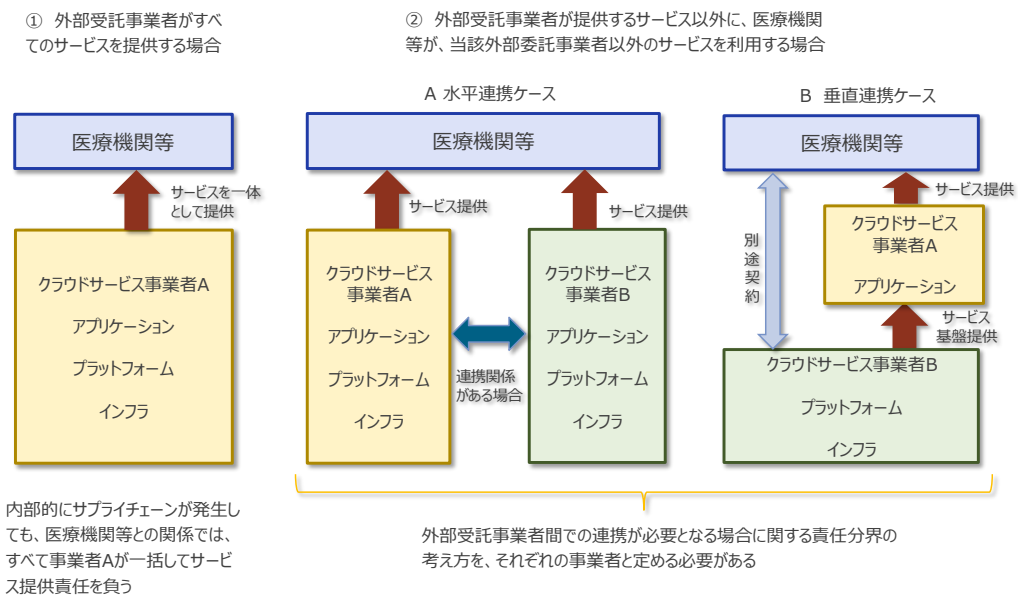


図　外部保存に関する委託例

企２章第①条

企Q－17　医療機関等の業務の一部を委託することに伴い情報が外部に保存される際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　遠隔画像診断、臨床検査等、診療等を目的とした業務の委託に伴い一時的にせよ情報を受託する事業者が保管する場合、医療機関等においては、受託する事業者の選定に関する責任やセキュリティ等の改善指示を含めた管理責任があるため、受託する事業者を適切に管理監督する必要があります。受託する事業者においても保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然ですが、感染症情報や遺伝子情報等の機微な情報の取扱い方法や保存期間等については、双方協議して整理しておく必要があります。

なお、治験のように、上記のようないわゆる業務委託ではなくとも、医療情報が外部の事業者に提供される場合は、これに準じてあらかじめ外部の事業者との間で双方の責任及び情報の取扱いについて取り決めることが必要です。

３．安全管理のための体制と責任・権限

企３章第⑨条、７章第⑦条

企 Q－18　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）として「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。」とあるが、どのように患者へ説明を行うべきか。

Ａ　外部保存実施に関する患者への説明 診療録等の外部保存を委託する医療機関等は、あらかじめ患者に対して、必要に応じて 患者の個人情報が特定の受託機関に送られ、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、理解を得る必要があります。

診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始してください。

患者本人に説明をすることが困難であるが、診療上の緊急性がある場合意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としません。意識が回復した場合には事後に説明を行い、理解を得る必要があります。

患者本人に説明し理解を得ることが困難であるが、診療上の緊急性が特にない場合乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要があります。親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に説明が 困難な理由を明記しておくことが望まれます。

６．リスクマネジメント（リスク管理）

企６章第⑤条

企Q－19　リスク分析で想定する脅威について、どのようなものがあるか。

Ａ　医療情報システムにおいては、システムに格納されている電子データの保護だけでなく、覗き見等の脅威にさらされるおそれのある、個人情報の入出力の際の保護方策についても考える必要があるなど、様々な脅威が想定されます。以下に様々な状況で想定される脅威を列挙します。なお「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」表 5-1 及びその別紙２（対策項目で対応できるリスクシナリオ例）も参考になります。

①　医療情報システムに格納されている電子データ
（a）権限のない者による不正アクセス、改ざん、毀損、滅失、漏えい
（b）権限のある者による不当な目的でのアクセス、改ざん、毀損、滅失、漏えい
（c）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（以下「不正ソフトウェア」という。）や標的型メール等を用いたサイバー攻撃等による不正アクセス、改ざん、毀損、滅失、漏えい

②　入力の際に用いたメモ・原稿・検査データ等
（a）メモ・原稿・検査データ等の覗き見
（b）メモ・原稿・検査データ等の持ち出し
（c）メモ・原稿・検査データ等のコピー
（d）メモ・原稿・検査データの不適切な廃棄

③　個人情報等のデータを格納したノートパソコン等の情報端末
（a）情報端末の持ち出し
（b）ネットワーク接続による不正ソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい
（c）情報端末に格納されたデータの漏えい
（d）情報端末の盗難、紛失
（e）情報端末の不適切な破棄

④　データを格納した可搬媒体等
（a）可搬媒体の持ち出し
（b）可搬媒体のコピー
（c）可搬媒体の不適切な廃棄
（d）可搬媒体の盗難、紛失
（e）可搬媒体接続による不正ソフトウェア感染

⑤　参照表示した端末画面等
（a）端末画面の覗き見

⑥　データを印刷した紙やフィルム等
（a）紙やフィルム等の覗き見
（b）紙やフィルム等の持ち出し
（c）紙やフィルム等のコピー
（d）紙やフィルム等の不適切な廃棄

⑦　医療情報システム
（a）サイバー攻撃によるIT障害
- 不正侵入、不正操作
- 改ざん、毀損
- 不正ソフトウェアによる攻撃
- サービス不能（DoS：Denial of Service）攻撃 等

（b）非意図的要因によるIT障害等
- システムの仕様やソフトウェア上の欠陥（バグ）
- 操作ミス
- 故障外部サービスの利用に伴う、システムポリシー等の意図しない変更等

（c）災害によるIT障害
- 地震、水害、落雷、火災等の災害による電力供給の途絶
- 地震、水害、落雷、火災等の災害による通信の途絶
- 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- 地震、水害、落雷、火災等の災害による重要インフラ事業者等におけるITの機能不全

（d）許可されていない医療情報システムの利用
- 許可されていない機器、ソフトウェア、サービスの業務利用
- 管理されている機器、ソフトウェア、サービスの目的外利用

医療機関等には、受託する事業者の選定に関する責任やセキュリティ等の改善指示を含めた管理責任があるため、受託する事業者を適切に管理監督する必要があります。受託する事業者においても保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然ですが、感染症情報や遺伝子情報等の機微な情報の取扱い方法や保存期間等については、双方協議して整理しておく必要があります。

企６章第⑨条

企Q－20　「 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、管理することが重要である」とあるが、医療情報の場合にはどのような考え方に基づいて行う必要があるか。

A　PDCA（Plan-Do-Check-Act）のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのように行われているかについて、一般財団法人日本情報経済社会推進協会（JIPDEC））の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されています。

【医療の安全管理の流れ】

事故やミスの発見と報告（Do）
「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析（Check）
・「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
（例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
・作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。

↓

予防／是正策（Act）
・再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底等）

上記を見ると、主に D→C→A が中心になっています。これは医療等分野においては診察、診断、治療、看護等の手順が過去からの蓄積によって既に確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みができ上がっているためといえます。

反面、情報セキュリティではIT技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在する可能性があります。そのため情報セキュリティ独自の管理方法が必要であり、ISMS はそのために考え出されたものです。ISMSは医療の安全管理と同様PDCAサイクルで構築し、維持していくことになります。

逆に言えば、医療関係者にとってISMS 構築はPのステップを適切に実践し、ISMSの骨格となる文書体系や手順等を確立すれば、あとは自然にISMS が構築されていく土壌があるといえます。

企６章第⑦条

企Q－21　医療情報システムで扱う情報の重要度の分類、確認方法、リスク分析結果はどのようにまとめるべきか。

Ａ　遵守事項①から⑧までの結果を系統的に文書化して管理してください。

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）

企７章第⑤条

企Ｑ－22　電子化された診療情報を外部保存できるか。できる場合、求められる要件は何か。

Ａ　電子媒体による外部保存を、ネットワークを通じて行う場合は「８．２．３ ネットワークサービスを用いた持ち出し」に、可搬媒体を用いて行う場合は「８．２．２　記録媒体・機器情報機器等による持ち出し」に、それぞれ要件が記載されているため、そちらを参照してください。

企７章第⑤条

企Ｑ－23　クラウド型の電子カルテサービスを行う業者に認定制度のようなものはあるのか。もしなければ、業者を選定する際に３省のガイドライン※に準拠していることは、どうやって確認すればよいのか。

Ａ　認定制度は現在のところ存在しません。なお、厚生労働省のガイドラインは、サービス提供業者ではなく、サービスを委託する医療機関等が遵守すべきものです。

サービス業者の選定に当たっては、「「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に準拠している旨」をサービス業者に確認させるとともに、契約を結ぶ際に、その旨を条項に盛り込んでおくとよいでしょう。

また、サービスを委託する医療機関は、当該サービスを利用した運用形態が、厚生労働省のガイドラインに準拠していることを、自ら確認してください。

※ ３省のガイドラインとは以下のガイドラインを指します。

- 厚生労働省「医療情報システムの安全管理に関するガイドライン」
- 総務省、経済産業省「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」

企７章第⑤条

企Q－24　医療情報の外部保存を行う際、どのような留意事項があるか。

Ａ　現在の技術を十分活用し、かつ注意深く運用すれば、ネットワークを通じて、診療録等を医療機関等の外部に保存することが可能です。診療録等の外部保存を受託する事業者が、真正性を確保し、安全管理を適切に行うことにより、医療機関等の経費節減やセキュリティ上の運用が容易になる可能性があります。

ネットワークを通じて外部保存を行う方法は利点が多いが、情報の漏えいや診療に差し支えるような事故に繋がるおそれがあるため、セキュリティや通信技術及びその運用方法に十分な注意が必要です。仮にこのような事故が発生し、社会的な不信を招いた場合は、結果的に医療の情報化を後退させ、ひいては国民の利益に反することになりかねないため、慎重かつ着実に進めるべきです。

ネットワークを通じて医療機関等以外の場所に診療録等を保存することができれば、システム堅牢性の高い安全な情報の保存場所の確保によるセキュリティ対策の向上や災害時の危機管理の推進、保存コストの削減等により医療機関等において診療録等の電子保存が推進されることが期待できます。しかし、外部保存には保存機関の不適切な情報の取扱いにより患者等の情報が瞬時に大量に漏えいする危険性も存在し、その場合、漏えいした場所や責任者の特定が困難になる可能性があります。そのため、常にリスク分析を行いつつ万全の対策を講じなければならず、医療機関等の責任が相対的に大きくなります。

さらには、情報の保存を受託する事業者又は職員による、利益を目的とした不当利用の危惧があるのも事実です。その一方で金融情報、信用情報、通信情報は実態として保存・管理を当該事業者以外の外部事業者に委託しており、合理的に運用されています。金融・信用・通信に関わる情報と医療に関わる情報を一概に同様に扱うことはできないが、一般に実績あるデータセンター等の情報の保存・管理を受託する事業者は慎重で十分な安全対策を講じており、医療機関等が自ら管理することに比べても厳重に管理されていることが多いです。

本来、医療に関連した個人情報の漏えいや不当な利用等により、個人の権利利益が侵害された場合には、被害者の苦痛や権利回復が困難であることが多く、医療機関等や関係各者に対し、法律や各種ガイドライン等により格別の安全管理措置を講じることが求められています。したがって、診療録等のネットワークを通じた医療機関等以外の場所での外部保存については、通常求められる安全管理上の体制と同等以上の体制を確保した上で、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることが原則です。

企７章第⑤条

企Q－25　医療機関等や委託事業者に外部保存を委託する場合、保存する情報の取り扱いに関して、どのような留意事項があるか。

Ａ　外部保存を委託する先を医療機関等と委託事業者それぞれに分けて、留意していただきたいことをまとめます。

【医療機関等に外部保存する場合】

情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所、医療法人等は適切なアクセス権限を規定し、情報漏えいや、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してください。

また、それら情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されるものであり、情報の保存を受託した病院、診療所、医療法人等が患者から何らの同意も得ずに実施してはなりません。

病院、診療所等であっても、保存を受託した診療録等について分析等を行おうとする場合は、委託した病院、診療所及び患者の同意を得た上で、不当な利益を目的としない場合に限ります。

また、実施に当たっては院内に検証のための組織等を作り客観的な評価を行う必要があります。

匿名化された情報を取り扱う場合においても、地域や委託した医療機関等の規模によっては容易に個人が特定される可能性もあることから、匿名化の妥当性の検証を検証組織で検討したり、取扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮する必要があります。

【事業者に外部保存する場合】

いかなる形態であっても、保存された情報の外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供しないでください。匿名化された情報であっても同様です。なお医療機関等が管理する端末等を用いて、医療機関等又は患者が患者情報に関するサービスを利用する場合に、受託する事業者においてCookieを取得することがあります。Cookieは直ちに個人を特定するものではないため、患者情報には当たらないとされうるものの、第三者提供することにより、患者等が特定されるリスクがあるため、受託する事業者において第三者に提供することは許されません。

外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関等以外にも提供する場合は、あくまで医療機関等同士の合意で実施されなくてはならず、当然、個人情報保護法に則り、患者の同意も得た上で実施する必要があります。

このような場合において、外部保存を受託する事業者がアクセス権の設定を受託しているときは、医療機関等又は医療機関等に対して同意した患者の求めに応じて適切な権限を設定する等して、情報漏えいや、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しなくてはなりません。

したがって、このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定しなくてはなりません。

外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、不当な利益追求を目的として情報を閲覧、分析等を行うことはあってはならず、許されません。したがって、外部保存を受託する事業者を選定する場合、医療機関等はそれらが実施されないことの確認、又は実施させないことを明記した契約書等を取り交わす必要があります。

外部保存の技術的な方法としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられます。

さらに、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、あるいは医療情報システム・サービス事業者の管理者といえどもアクセスできない制御機構をもつことも考えられます。具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられます。この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならなりません。

医療機関等が自ら暗号化を行って暗号鍵を保管している場合、火災や事故等で暗号鍵が利用不可能になった場合、全ての保存委託を行っている医療情報が利用不可能になる可能性があります。これを避けるためには暗号鍵を、外部保存を受託する事業者に預託する、複数の信頼できる他の医療機関等に預託する等が考えられます。分散保管においても同様の可用性の保証が必要です。

ただし、外部保存を受託する事業者に暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要です。

外部保存を受託する事業者による暗号鍵の不正利用を防止するため、暗号鍵の使用について運用管理規程を策定し、使用を非常時に限定しなければなりません。また、実行時に暗号鍵を使用した証跡が残る暗号手法等を利用し、医療情報システムにおける証跡管理等を適切に実施することで、暗号鍵が不正利用されていないかを確認する必要があります。

企７章第⑥条

企Q－26　外部保存を委託する事業者の選定において、どのような留意事項があるか。

Ａ　法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要があります。

また、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」の要求事項も満たす必要があります。

なお、選定にあたっては、外部委託事業者のセキュリティ対策状況を確認することが必要です。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」や「『製造業者/サービス事業者によるによる医療情報セキュリティ開示書』ガイド」によって、外部保存を受託する事業者におけるセキュリティ対応状況の概要を確認することができるため、サービスの性質等、必要に応じてその提供を求めることなどが有効です。

外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、所管する行政機関の調査等に供するため、提出等を行う必要が生じうることから、これを円滑に実現できることが求められます。そのため外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められます。

企７章第⑥条

企Q－27　ISMS 認証を取得している事業者に対して、根拠資料を求めることはできるのか。

Ａ　例えば、ISMS 認証を取得している事業者の選定に際して、選定対象となる事業者が管理しているリスクに応じて、適合性を示す資料の提供を求めてください。なお、これらの認証は、医療機関等に限らず、個人情報の取扱いに関し、適切な体制を整備していることを示すものであり、あくまで事業者として最低限の適格性を医療機関等へ示す手段として捉えています。

企７章第⑥条

企Q－28　７．安全管理のための人的管理⑥ｇの「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」とは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」や「JASA クラウドセキュリティ推進協議 会 CS ゴールドマーク」等で公開されたサービスリストやマーク取得サービス一覧などに掲載されていることを確認することでよいか。

Ａ　サービスリストやマーク取得サービス一覧に掲載されたクラウドサービス であることだけをもって適切な外部保存に求められる技術及び運用管理能力 があるとはいえず、

ISMAP や CS ゴールドマーク取得サービスでの評価、取得に際し、審査対象を定めた「言明書」が公開されているので、当該言明書を確認の上、事業者を決定してください。

企７章第⑦条

企 Q－29　外部保存を委託する場合のデータ閲覧権限はどうするといいか。

Ａ　医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託元の医療機関等のみがデータ内容を閲覧できることを担保するよう求めてください。

企７章第⑦条

企 Q－30　個人識別に係る情報を適切に保管するために、外部保存を委託する事業者にどのような対策を求めればいいか。

Ａ　外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつようにしてください。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられます。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を備えるよう求めてください。

企７章第⑨条

企 Q－31　外部保存の委託を終了する際、どのような留意事項があるか。

Ａ　診療録等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には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはなりません。

　診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査しなくてはなりません。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要があります。

　これらの廃棄・返却に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要があります。また、実際の廃棄・返却に備えて、事前にソフトウェア等の廃棄・返却の手順を明確化した規定を作成しておくべきであります。

　これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければなりません。

　ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければなりません。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要です。

また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想されます。したがって、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはなりません。

企７章第⑩条

企Q－32　医療情報の外部保存に関して、院内掲示以外の患者等への周知方法はどのようなものがあるか。

Ａ　院内掲示以外の周知方法としては、パンフレットの配布、問診表への記載、医師・看護師等による口頭説明等があります。さらに、インターネット上の医療機関等のホームページ上での公表を加えることもできます。

企７章第⑩条

企 Q－33　病態、病歴等を含めた個人情報の外部保存を行う場合、患者等にどのような説明を行うべきか。

Ａ　診療開始前の説明

患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始してください。

患者本人に説明をすることが困難であるが、診療上の緊急性がある場合

意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。

患者本人に説明することが困難であるが、診療上の緊急性が特にない場合

乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

８．情報管理（管理、持ち出し、破棄等）

企８章第③条

企 Q－34　個人情報が保存されている機器が設置されている区画への入退管理の方法として、どのようなものが挙げられるか。

Ａ　個人情報が保存されている機器が設置されている区画への入退管理を実施してください。

例えば、次に掲げる対策を実施してください。

- 入退者に名札等の着用を義務付ける。
- 台帳等によって入退者を記録する。
- 入退者の記録を定期的にチェックし、妥当性を確認する。

企８章第⑥条

企 Q－35　情報及び情報機器の持ち出しを認める場合、どのような留意事項があるか。

Ａ　昨今、医療機関等において医療機関等の職員や医療情報システム・サービス事業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生しています。

一方で、在宅医療、訪問診療等の増加、モバイル端末の発展により医療情報を持ち出すニーズや機会が増加しています。

情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末や CD-R、USB メモリのような可搬媒体が考えられます。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられます。さらにネットワークを通じてクラウドサービスを利用して持ち出すケースも想定されます。

まず重要なことは、「６．リスクマネジメント（リスク管理）」で述べていますように、取り扱う情報を適切に把握した上で、その情報についてリスク分析を実施することです。

その上で、医療機関等において把握している情報又は情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要であります。切り分けを行った後、持ち出してよいとした情報又は情報機器に対して対策を立てなくてはなりません。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器をどのように管理すべきかが明確になります。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等の対策も管理を明確にし、状況を把握するための方策となります。

一方、医療機関等の管理外のパソコン等の情報機器で、可搬媒体に格納して持ち出した情報を取り扱う時に、不正ソフトウェアの混入や不適切な設定のされたソフトウェアやサービスの利用、外部からの不正アクセスによって情報が漏えいすることも考えられます。この場合、情報機器が基本的には個人の所有物となりますが、そのような機器等の利用や情報の取扱いについては医療機関等の企画管理者の責任において把握する必要があります。

スマートフォンを利用する際の安全対策については、「スマートフォン・クラウドセキュリティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～」（総務省；平成 24 年６月）が参考になります。

企８章第⑤条

企 Q－36　「リスク評価に基づいて、医療情報の持ち出しに関する方針や、持ち出す情報、持ち出し方法に関する手順や管理方法を情報管理に関する規程で定める。」とあるが、具体的にどのような基準で判断をすればよいか。

Ａ　当該情報機器が医療情報を記録しているか否かで取扱いが異なります。

医療情報を記録している機器や媒体であれば、持ち出しには細心の注意が必要です。このような機器や媒体は、原則として持ち出すべきではないという基準にすべきです。その上で、やむを得ず持ち出す際には、情報機器を持ち出す必要性や漏えいのリスクを総合的に判断した上で、運用管理規程等に機器持ち出しの許諾ルールと判断基準を策定することが求められます。また、持ち出す機器については、システム運用編「７．情報管理（管理・持出し・破棄等）」に示す適切な防護措置を施すことが必要です。

リモートサービス等により医療機関等の情報にアクセスできる機器の場合、医療情報を機器に記録していなくても、機器そのものの盗難や置き忘れが情報漏えいのリスクになります。このような場合、機器に対する防護措置に加え、リモートサービスそのものでの防護措置が必要であり、システム運用編「７．情報管理（管理・持出し・破棄等）」に示された安全管理対策を実施していることが条件になります。

上記以外の情報機器については、機密情報の有無やその他の要件を考慮し、医療機関等における管理ルールを策定してください。

企８章第⑨条、シス７章⑧条、⑭条

企 Q－37　患者等に診療情報等を提供する場合、どのような留意事項があるか。

Ａ　まず原則として、医療機関等が患者等との同意の上で、自ら実施して患者等に診療情報等を提供する場合であることが想定されます。診療録及び診療諸記録の外部保存を受託する事業者が独自に診療情報等の提供を行うことはあってはなりません。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、診療情報等を閲覧する患者等のセキュリティ知識と環境に大きな差があるということです。また、一旦診療情報等を提供すれば、その情報保護の責任は医療機関等ではなく、患者等にも発生します。しかし、診療情報等を提供する医療機関等が患者等に十分に患者がセキュリティ対策の必要性や管理の責任を負うこと等の理解すべき事項を説明し、その提供の目的を明確にする責任があります。また、説明が不足している中で万一情報漏えい等の事故が起きた場合は、その責任を負う可能性があることを認識しなくてはなりません。

提供に用いるネットワークとしては、一般的にはオープンなネットワークを介することが現実的です。この場合、盗聴等の危険性は極めて高くなります。そのため利活用と安全確保の両面を考慮したセキュリティ対策が必須でとなります。特に、患者等に情報を公開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しておく必要があります。そのため、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 個人認証等の技術を用いるなどが求められます。

また、患者の委託先に診療情報等を送付する(クラウドサービスへのアップロード含む)際、外部の事業者に対して送付するよう、患者から依頼を受ける場合も想定されます。この場合、患者の委託先への送付であることから、第三者提供には当たらないものの、診療情報等の流出などに対する留意が求められる。送信先／アップロード先についての安全性等について疑義が生じた場合に患者からの依頼を断るなどのほか、送信等を行うに当たっては、患者との関係で責任分界についても取り決めておくことが求められます。

企８章⑫条

企 Q－38　「確実に情報の破棄されたことを確認すること」とは立ち会いを前提としているのか。

Ａ　立ち会いを前提とはしていません。破棄を行った証票を受け取る等、「７．安全管理のための人的管理（職員管理、委託先事業者管理、教育・訓練、委託先事業者選定・契約）」の内容を遵守し、確実に確認していただければ問題ありません。

９．医療情報システムに用いる情報機器等の資産管理

企９章②条関係

企 Q－39　情報及び情報機器の持ち出し並びに外部利用をする場合にどのような対応が必要か。

Ａ　情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止してください。

企９章④条関係、シス９章④条

企 Q－40　事前の確認時と状況が変わり、請負事業者が倒産する等してソフトウェアの保証がなくなった場合、見読性は確保されていないことになるのか。

Ａ　倒産ではなく、請負事業者がソフトウェア事業を廃止する場合は、見読性を確保する条項等を契約書に明記することで、見読性を確保できます。

しかし、倒産の場合、使用継続は保証されるものの、長期の見読性は保証されないこととなり、使用者がこれを担保する必要があります。診療等に差し支えない期間内に見読性が保証される対策を講じなければならず、この対策を容易にするためにも標準化や相互運用性の確保は重要です。

11．システム運用管理（通常時・非常時等）

企１１章②条

企 Q－41　医療情報システムに関する BCP（Business Continuity Plan：事業継続計画）の作成は、医療機関にとってどのような場面を想定するといいか。

Ａ　我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため医療情報システムが通常の状態で使用ができない事態に陥った場合における適切な BCP の作成と訓練は可能であり、必須の事項と考えられます。

「通常の状態で使用できない」とは、使用環境が非定常状態になる場合と、システム自体が異常動作又は停止になる場合とがあります。

前者は、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合です。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられます。

後者は、医療情報システムが自然災害やサイバー攻撃等により、システム的に損傷を被ることにより、システムの縮退運用又は全面停止に至り、医療サービス提供に支障発生が想定される場合です。

企１１章②条

企 Q－42　BCP（Business Continuity Plan：事業継続計画）の内容を検討する上で、参考になる内容はあるか。

Ａ　以下に、BCP として策定すべき項目と運用に関する一般項目を参考に示します。

①　BCP として事前に周知しておく必要がある事項

事前に関係者に対応策の周知を行い、信頼を得ておく必要がある。

- ポリシーと計画：何が「非常事態」なのかを理解し、定義すべきである。
- 非常事態検知手段：災害や故障の検知機能と発生情報の確認手段
- 非常時対応チームの連絡先リスト、連絡手段及び対策ツール
- 非常時に公にすべき文書及び情報

② BCP 実行フェーズ

災害、事故やサイバー攻撃等の発生（あるいは発生の可能性）を検知してから、BCP 実行か通常の障害対策かの判断を行い、BCP 実行と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡・協力依頼を行い、システムの切り替え／縮退等の準備を行う。例えば、ネットワークから切り離したスタンドアロンでの使用や、紙での運用等が考えられる。

業務を受託する事業者との間の連絡体制や受託する事業者と一体となったトラブル対処方法等が明示されるべきである。また、医療情報システムに障害が発生した場合は、必要に応じて所管官庁への連絡を行うべきである。

具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」、「関係先への連絡」及び「影響度の確認」である。

③ 業務再開フェーズ

BCP を発動してから、バックアップサイト・手作業等の代替手段により業務を再開し、軌道に乗せるまでのフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員等の人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。

最も緊急度の高い業務（基幹業務）から再開する。

具体的項目は「人的資源の確保」、「代替施設及び設備の確保」、「再開／復旧活動の両立」及び「リスク対策によって新たに生じるリスクへの対策」である。

④ 業務回復フェーズ

最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイントとなる。

具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」及び「制限の確認」である。

⑤ 全面復旧フェーズ

代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。

具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」及び「総括」である。

⑥ BCP の見直し

正常な状態に復帰した後に、BCP に関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCP の見直しを行い、次の非常時に備えることが重要である。

企１１．３章、シス１１．２章

企 Q－43　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは、真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか。）。

Ａ　適切な安全管理が実施されていれば、問題ありません。「１１．非常時（災害、インシデント、サイバー攻撃被害、システム障害）対応と BCP 策定」において要求事項が記載されているため、そちらを参照してください。

　また、紙データを電子システムに反映させる際に、紙データをオリジナルとして保存する必要が生じると考えられます。オリジナルの紙データをスキャナ等により電子化して保存する場合は、「１６．紙媒体等で作成した医療情報の電子化」を参照してください。

　電子カルテ等に転記した場合、転記した情報で診療等を実施することに問題はありません。ただし、オリジナルとしての紙又はスキャナ等で電子化したデータは、別途適切な安全管理を実施した上で、定められた期間保存する必要があります。

13. 医療情報システムの利用者に関する認証等及び権限

企１３章第②条

企 Q－44　「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」にするために、どのようなリスクを想定すればよいか。

Ａ　利用者の識別・認証に用いられる情報が第三者に漏れがないように以下のようなリスクに対処することが想定されます。

- ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- 初期設定のパスワードが変更されておらず、利用者以外の者でもシステムにログインできてしまう。
- 代行作業等のために ID・パスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- 一つの ID を複数の利用者が使用している。
- 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- 安全性が高くないパスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- 認証用の個人識別情報を格納するセキュリティ・デバイス（IC カード、USB キー等）を他人に貸与する、又は持ち主に無断で借用することにより、利用者が特定できない。
- 退職した職員の ID が有効になったままで、ログインができてしまう。
- 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- 不正ソフトウェアにより、ID やパスワードが盗まれ、悪用される。

企１３章第②条

企 Q－45　本人確認の方法として eKYC を採用する場合、どのような留意事項があるか。

A　eKYC （electronic Know Your Customer）は、従来、書面が使われていた利用者の身元確認のための資料を、電子的に対応するための仕組みになります。例えば金融機関における口座開設などで、本人の実在性を確認するために、従来は住民票等で身元確認を行ってきましたが、これに代わり、例えばマイナンバーカードを利用した公的個人認証サービスを利用するなど、オンラインで対応できるようになっています。

eKYC では、身元確認を行う際に、利用者が本人であることが前提となるため、これを利用者の認証方法とすることが考えられます。

ただし eKYC にも多様な方法があり、それに応じて本人認証に対する信頼性などが異なります。本人確認の方法として eKYC を採用するには、認証の信頼度が非常に高い IAL３（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 IAL２）が求められます。

また、eKYC はもともと身元確認を行うための手段なので、身元確認に必要な情報のやり取りが発生することもあります。そのため、単なるシステムの利用には不要な、利用者の個人情報が流通することもあり、その管理などを適切に行う必要なども生じます。

従って eKYC を採用する場合には、採用する eKYC の内容等を踏まえて、適切に行うことが求められます。

14. 法令で定められた記名・押印のための電子署名

企１４章第①条

企 Q－46　法令で定められた記名・押印を電子署名で行うことについて、どのような経緯があるか。

Ａ　平成 11 年４月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」においては、法令で署名又は記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていました。

しかし、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、「A. 制度上の要求事項」に示した電子署名によって、記名・押印に代わり電子署名を施すことで、作成・保存が可能となりました。

なお電子署名立会人型電子署名については、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）」において、解説されていますが、これを解説するものとして「主務三省（電子署名法第３条関係）Q&A に関する解説」（電子認証局会議・トラスト・サービス推進フォーラム））があります（同解説は以下の URL から入手できます）。

https://safe.menlosecurity.com/doc/docview/viewer/docNF1554846371E25d7bbdb9d4b0592598e59364e0a6dd04b35a948b5f7ce0fe45e0550e15e9a00

企１４章第①条の２

企 Q－47　通常閉域ネットワークを構築することが多い医療機関等において、一枚一枚の文書にリアルタイムにタイムスタンプを付与することは、実装が困難ではないか。

Ａ　「１４．法令で定められた記名・押印のための電子署名」は、診療情報提供書や診断書等の法令で記名・押印することが定められた文書等を対象としています。これら以外の文書等に一枚一枚タイムスタンプを付加することは必須ではありません。

しかしながら複数のスキャン画像ファイルなどにまとめてタイムスタンプを付す場合、方式によっては個々のファイルを個別に検証することができなくなるので留意が必要です。例えば、複数ファイルを ZIP ファイルに格納してタイムスタンプを付与した場合、タイムスタンプの検証時に ZIP ファイル全体を読み込む必要があり、ファイル個別に検証することができません。係争時等の外部提出を想定した場合に、関係のないファイルも提出する必要があるため適切な方法とはいえません。

そのため個別のファイルごとにタイムスタンプを検証することができる標準技術を使用すれば、適切にタイムスタンプを付すことができます。標準技術の例として、個々のファイルのハッシュ値を束ねて階層化した上で、頂点のハッシュにタイムスタンプを付す ERS（Evidence Record System）等があります。

なお、タイムスタンプを付与するにはセキュアなタイムスタンプ環境を構築する必要があります。

企１４章第①条

企 Q－48　クラウド型の電子カルテサービスを行う場合、利用者によるトランザクションごとに電子署名が必須となるのか。

Ａ　電子署名の付与に関する記述への対応として、個々のトランザクションを「ファイル」と考えれば、各々の情報単位で電子署名が必要になると解釈できないことはありません。しかし、ここではそれほど厳密な解釈を適用せず、トランザクション単位での電子署名の付与は不要だと考えられます。

本質問にある電子署名の付与には、２つの目的があると考えられます。１つは外部のネットワークを経由する際のメッセージの真正性の担保、もう１つはサービス側で情報を保存する際の真正性の担保（改ざん防止等の完全性の観点、否認防止の観点等）です。

これらを同時に満足するための技術的手法として、電子署名の付与は有効な方法です。しかし、これを個々のトランザクション・メッセージに適用することは必須ではありません。例えば、通信経路上の改ざん防止には、メッセージに電子署名を付与しないでも、TLS 等の適用で十分な場合があります。また、メッセージを保存する際に逐次電子署名を付与しなくても、それよりも大括りな情報単位（例えば一日単位）で電子署名を付与すること、あるいは本ガイドラインに例示された他の技術的手法・運用方法を適用することも可能です。

企１４章第①条の１⑵

企 Q－49　１４．法令で定められた記名・押印のための電子署名①１⑵の「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署名等を用いること」とあるが、要件を満たす具体的な手段は何か。

Ａ　２０２２（令和４）年 ３ 月 31 日時点で存在している、「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」に対し、医師等の国家資格の確認が電子的に検証できる電子署名としては、１４．法令で定められた記名・押印のための電子署名①⑵)の⒜の「保健医療福祉分野 PKI 認証局の発行する電子証明書」

- 日本医師会 電子認証センターが発行する「医師資格証」
- 日本薬剤師会 認証局が発行する「薬剤師資格証」
- 医療情報システム開発センター(MEDIS-DC) 電子認証局が発行する「HPKI 電子証明書」

があります。

なお、今後、⒜の「監査基準」を満たす新たな「保健医療福祉分野 PKI 認証局」や、（ｂ）の「適切な外部からの評価」を受けた事業者、電子的な資格確認に対応した（ｃ）の「公的個人認証サービス」による電子証明書が発行された場合、適宜、追加も考えられます。

企１４章第①条の１⑵

企 Q－50　１４．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電子署名の要件のうち、①1(2)（ｂ）にある「医療機関等の管理者」とは、具体的には組織単位で考えればよいか。

Ａ　本ガイドラインにおける医療機関等とは「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」を指します。従ってここでも医療機関等ごとに管理者を設置することを想定しています。例えば、同一法人に複数の病院や診療所、薬局等が属している場合でも、それぞれの病院や診療所、薬局等の単位で管理者を設置することになります。

企１４章第①条の１⑵

企 Q－51　１４．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電子署名の要件①１（２）（ｂ）において、身分証明書や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）」とあるが、この「署名」と「押印」は同等と考えてよいか。

Ａ　郵送の場合、押印（実印が捺印され、印鑑登録証明書が添えてあること）　に対して、署名が自署であることの確認を行うことが難しいため、署名をも　って確認するには、医療分野の特性を踏まえ、十分に注意すること。

企１４章第①条の２

企 Q－52　タイムスタンプはパソコンの時間と同じでよいか。

Ａ　タイムスタンプは電子署名を含む文書全体の真正性等を担保するために必要なものであることから、このガイドラインでは「時刻認証業務の認定に関する規程」（令和３年４月１日、総務省告示第 146 号）に基づき認定された事業者（認定事業者）が提供するものを利用することを求めています。※

※ 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、上記の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ありません。

企１４章第②条

企 Q－53　暗号化を行うための適切な鍵管理を行うために、どのような対応が考えられるか。

Ａ　経路の暗号化や、電子署名・電子認証によるなりすましの防止や情報の改ざん防止を図る場合には、暗号／復号、デジタル署名に用いる鍵の管理を適切に行うことが重要である。特に共通鍵や、秘密鍵の管理を適切に行うことは、暗号化、デジタル署名の安全性を保証するために必要です。

鍵管理に求められる具体的な対応は、暗号鍵の利用目的に応じて異なる。すなわち、SSL/TLS、電子署名、その他外部との情報交換の際の暗号化、通信機器の認証などに応じて異なるため、それぞれにおいて必要な共通鍵、秘密鍵を保護する機能を具備することが求められます。本ガイドラインでは、電子署名や電子証明書を利用した本人認証などでは、電子証明書の認証を行う認証局が定める「証明書ポリシー」（Certificate Policy）に従って、管理することを求めています。

また、共通鍵や暗号鍵を格納する機器や媒体についても、一定の安全性が求められます。暗号モジュールに関するセキュリティ要件の仕様を規定するものとしては、米国連邦標準規格であるFIPS 140-2 (Federal Information Processing Standardization 140-2)※が定められています。機器等の安全性を担保するためには、この基準の最低限のレベルで求められる要件を具備することが望まれます。

※ FIPS140-2 では、製品に求めるセキュリティ要件として、Level1 から Level4 の 4 段階のレベルのものを定めている。このうち最も低い Level1 では、「製品レベルのコンポーネントの基本要件を満たす物理的セキュリティメカニズムが存在すればよい」とされる。(”SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES” P4 （NIST、2002.3.12）

15．技術的な安全管理対策の管理

企１５章第②条

企 Q－54　「８．情報管理（管理、持出し持ち出し、破棄等）③において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。」とあるが、例えば外来やナースステーション等では、それらの措置は困難ではないか。

Ａ　外来やナースステーションでは患者や家族の入退がありますが、医療情報システムを導入していない場合にも行われているように、その事実をカルテ等に記録することにより、来訪を記録できます。

企１５章第⑧条

企 Q－55　「２．１．１　医療機関等における責任と責任分界の運用管理においては、医療機関等と情報システム・サービス事業者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うえで、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。」とあるが、契約書の記載方法を教えてほしい。

Ａ　「２．責任分界」に掲げている事項に関し、個別に責任範囲及び共同対応範囲を定めて、誰が何をどのタイミングで行うかを文書化してください。

　また、通信サービスを提供する事業者等に対しては、SLA（Service Level Agreement）を確認し、SLA に記載されていない若しくは不足する部分があれば、その部分について SLA の修正を要請する又は個別契約を結ぶことで対応してください。

企１５章第⑬条

企 Q－56　外部の医療機関等から持ち込まれた **X** 線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか。

Ａ　原本の保存義務は元の医療機関等にありますが、持ち込まれた診療情報を診療に利用した場合は、当該医療機関等においても保存義務が発生します。

企１５章第⑧条

企 Q－57　保守要員の専用アカウントの不正使用を防止するためにどのような方法があるか。また保守作業にあたってどのような作業を求めるといいか。

Ａ　保守要員の専用アカウントについて、外部流出等による不正使用の防止の観点から適切に管理することを求めてください。

保守要員の離職や担当替え等に応じて速やかに保守要員の専用アカウントを削除できるよう、医療情報システム・サービス事業者に報告を義務付けるとともに、それに対応できるアカウント管理体制を整備してください。

医療情報システム・サービス事業者がメンテナンスを実施する際には、日単位で作業申請書を事前提出させるとともに、終了時に速やかに作業報告書を提出させてください。提出された書類は、医療情報システム安全管理責任者が承認すること。なお、作業申請書の承認は、原則として保守作業の実施前に行う必要があるが、事前に承認を得ずに実施可能なものとして医療情報システム・サービス事業者と合意したメンテナンスについては、事後承認とすることができます。

16. 紙媒体等で作成した医療情報の電子化

企１６章第③条

企 Q－58　「スキャナによる読み取りの際の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・タイムスタンプ等を遅滞なく行うこと。」とあるが、これは取り込み責任者を明確にすることか。

Ａ　取り込み責任者を明確にする目的だけでなく、改ざんやなりすましを防止するために、また、作業内容の正確性についての説明責任を果たすために実施するものです。

企１６章第③条

企 Q－59　「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。」とあるが、一定期間以内とはどれ位をいうか。外来診療の場合、１日の診療が終わった後にまとめて行う等の運用でもよいか。

Ａ　原則は１日以内です。ただし、深夜に来院し、次の日が休診である場合等は営業日として１日以内となります。

企１６章第⑤条

企 Q－60　どの程度の期間内でスキャナ等により電子化して保存すべきか。

Ａ　運用管理規程において、改ざんの動機が生じないと考えられる期間（長くとも１～２日程度以内）を定めるとともに、その期間内に遅滞なくスキャンを行わなければならない。時間外診療等で機器の使用ができない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行う必要があります。

企１６章第⑥条

企 Q－61　電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。

Ａ　紙の診療録の法定保存年限は医師法で一連の診療の終了後５年とされています。ただし、電子カルテの導入により、以前の紙の診療録がスキャナ等で適切に電子化されており、管理責任者によって保存義務の対象が電子化された診療録であると認められていれば、紙の診療録に法定上の保存義務はありません。このような処理を行わない場合は、法定の保存義務があります。

　なお、情報の真正性、保存性の確保の観点から、スキャナ等で電子化して運用する場合でも、元の媒体である紙の診療録を併せて保存することは有効であり、法定期限に限らず保存することが望ましいです。ただし、この場合も電子化及び保存に関しては、「16.紙媒体等で作成した医療情報の電子化」等を参照の上、適切に実施する必要があります。

企１６章第⑥条

企 Q－62　①　診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。②　電子化された場合、法定保存年限を経過した文書も保存すべきと考えるべきか。

Ａ　「16.1　共通の要件」の記載に従って電子化し、電子化されたものを保存義務のある対象とする場合は、スキャンされた原本は個人情報保護の観点に注意して廃棄しても構いません。しかし、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きわめて有効であり、破棄を義務付けるものではありません。また、法定保存年限を経過した文書の保存期限は、各医療機関等で規定することとなります。

企１６章第⑦条

企 Q－63　「「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」とあるが、電子保存した内容を再度プリントアウトして、訂正後に再度電子化して保存するといった運用でもよいか。

Ａ　調剤済み処方箋をスキャナ等により電子化し、電子化した情報を原本とした後に修正を行う場合、真正性の確保の観点から、過去の電子署名の検証が可能な状態を維持する形で電子的に修正し、薬剤師の電子署名を付す必要があります。

そのため、プリントアウトしたものに訂正を行い、再度スキャナ等により電子化して保存することは、真正性の確保の観点から適切ではないと考えます。

スキャナ等による電子化は、１６．紙媒体等で作成した医療情報の電子化 に規定されているように、医療機関等において運用管理規程を適切に定めて実施されるものです。

例えば、事後修正が生じる可能性が十分低くなってから、スキャン等により電子保存する、又はスキャンした紙の調剤済み処方箋を一定期間バックアップとして保存すること等が考えられます。このような対応を講じることで、当該処方箋に修正の必要が生じた際に、スキャン等により電子化した情報を破棄した上で、その紙媒体を原本として修正を行い、改めてスキャン等により電子保存することができます。

企１６章第⑧条、シス１６章第①条

企 Q－64　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度がいいか。

Ａ　診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンしてください。これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからです。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできます。

放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン 3.0 版 （平成 27 年 4 月）」を参考にしてください。

このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮してください。

一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存してください。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要があります。放射線フィルム等の医用画像情報をスキャンした情報は DICOM 等の適切な形式で保存してください。

システム運用編

システム運用編

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）

シス５章

シＱ－１　「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）」は具体的に何を遵守すればよいのか。

Ａ　「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）」では、相互運用性の重要性と、それを実現するために医療機関等がシステムベンダに要求すべき内容が記述されています。具体的には、医療機関等はシステムベンダの標準化に対する基本スタンス、（標準に対応していないならば、その理由や対応案）についてシステムベンダから説明を受け、一定の理解を等しくしておくことが求められます。さらに、現在導入しているシステムの更新やシステムの新規導入の際に、システム間でのデータ互換性やシステム接続性が確保されるように、医療機関等においても相互運用性に係る中長期的なビジョンを持ち、計画的にベンダへ要求していくことが望まれます。

シス５．１章

シＱ－２　①相互運用性と標準化を行うことのメリットは何か。②基本データセットや標準的な用語集、コードセットを実装しなかった場合、どのような不利益が想像されるか。

Ａ　標準化のメリットには、システム間の相互運用性、データの長期的可用性等の確保があります。患者紹介や地域医療情報連携等で外部の医療機関等と医療情報をやり取りする場合、使用されているコードや用語が標準的でないと、適切な情報交換が難しくなります。また、システムをリプレイスする場合も、データ変換等が必要になってしまいます。これらの場合に、コードや用語が標準化されていれば、データ変換の手間や、変換機能の実装のための費用と時間の節約が期待できます。

　このような表受な対応を行わず、基本データセットや標準的な用語集、コードセットを実装しなかった場合、システム更新時のデータ移行に伴う作業によって、見読性、真正性の責任が果たせなくなることがあります。

シス５章第①条

シQ－３　「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、標準項目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こと」とあるが、標準形式は正式に定められたものがあるのか。

Ａ　標準化については、既に一定のレベルで確立された標準の情報項目等を利用することにより、以下の診療情報については高いデータ互換性を確保することが可能となりつつあります。これらは医療情報システムとして最も高いレベルの相互運用性が必要とされます。

- 医療機関情報
- 当該医療機関での受診歴
- 患者基本情報病名
- 保険情報
- 処方指示（含む用法）
- 検体検査（指示及び結果）
- 放射線画像情報
- 生理検査図形情報
- 内視鏡画像情報
- 注射
- 手術術式

これらの情報の相互運用性を確保するために必要とされ、これまでに確立された各種標準について、以下に示します。

【厚生労働省標準規格】

厚生労働省では通知「保健医療情報分野の標準規格として認めるべき規格について」で、厚生労働省における保健医療情報分野の標準規格（「厚生労働省標準規格」）を定め、その実装を推奨しています。

これは民間団体であるHELICS協議会によって制定された「医療情報標準化指針」で採択された規格等について、厚生労働省の保健医療情報標準化会議で審議され、その結果として出された提言に基づいて定められたものです。

令和５年３月現在、以下の規格等が厚生労働省標準規格に採択されています。

- HS001 医薬品HOTコードマスター
- HS005 ICD10対応標準病名マスター
- HS007 患者診療情報提供書及び電子診療データ提供書（患者への情報提供）
- HS008 診療情報提供書（電子紹介状）
- HS009 IHE統合プロファイル「可搬型医用画像」およびその運用指針
- HS011 医療におけるデジタル画像と通信（DICOM）
- HS012 JAHIS臨床検査データ交換規約

- HS013 標準歯科病名マスター
- HS014 臨床検査マスター
- HS016 JAHIS 放射線データ交換規約
- HS017 HIS,RIS,PACS,モダリティ間予約,会計,照射録情報連携指針（JJ1017 指針）
- HS022 JAHIS 処方データ交換規約
- HS024 看護実践用語標準マスター
- HS026 SS-MIX2 ストレージ仕様書および構築ガイドライン
- HS027 処方・注射オーダ標準用法規格
- HS028 ISO 22077-1:2015 保健医療情報ー医用波形フォーマットーパート 1：符号化規則
- HS030 データ入力用書式取得・提出に関する仕様（RFD）
- HS031 地域医療連携における情報連携基盤技術仕様
- HS032 HL7 CDA に基づく退院時サマリー規約
- HS033 標準歯式コード仕様
- HS034 口腔審査情報標準コード仕様
- HS035 医療放射線被ばく管理統合プロファイル
- HS036 処方情報 HL7 FHIR 記述仕様
- HS037 健康診断結果報告書 HL7 FHIR 記述仕様
- HS038 診療情報提供書 HL7 FHIR 記述仕様
- HS039 退院時サマリーHL7 FHIR 記述仕様

なお厚生労働省標準規格は、今後も保健医療情報標準化会議の提言等を踏まえ、適宜更新される方針ですので、必要に応じ、適宜最新版を参照する必要があります。最新版は、下記の URL から参照可能です。
https://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html

【基本データセット】
経済産業省は、平成 20 年に「医療情報システムにおける相互運用性の実証事業（相互運用性実証事業）」において、一般社団法人保健医療福祉情報システム工業会（JAHIS）等に委託し、基本データセットとそれらを用いたシステム間でのデータのエクスポート・インポートのためのガイドラインを整備しました。
この基本データセットには以下が含まれます。
- 利用者情報
- 医療情報（基本情報）
- 医療情報（感染症、アレルギー情報、入退院歴、受診歴）
- オーダ情報（処方、検体検査、放射線）
- 検査結果情報（検体検査）
- 病名情報
- 注射に関わる指示、実施情報等

・　処置・手術

最新の基本データセットは JAHIS においてメンテナンスされています。データの互換性を確保するために、以下のガイドラインを参照する必要があります。

・　JAHIS 基本データセット適用ガイドライン（第３版）
　　https://www.jahis.jp/standard/contents_type=33

【用語集・コードセット】

前述の厚生労働省標準規格の制定に先立ち、厚生労働省は一般財団法人医療情報システム開発センター（MEDIS-DC）への委託事業により、以下の標準マスターを作成し、その後も維持管理を継続しています。これらの標準マスター類の一部は厚生労働省標準規格にも採択されています。

・　病　　名：病名マスター（ICD10 対応標準病名マスター）
・　手術・処置：手術・処置マスター
・　臨 床 検 査：臨床検査マスター（生理機能検査を含む）
・　医　薬　品：医薬品 HOT コードマスター
・　医 療 機 器：医療機器データベース
・　看 護 用 語：看護実践用語標準マスター
・　症 状 所 見：症状所見マスター＜身体所見編＞
・　歯 科 病 名：歯科病名マスター
・　歯科手術等：歯科手術・処置マスター
・　画 像 検 査：画像検査マスター

・　J－MIX：電子保存された診療録情報の交換のためのデータ項目セット
・　MEDIS 標準マスター類
　　https://www.medis.or.jp/4_hyojyun/medis-master/index.html

MEDIS-DC では、前述の相互運用性実証事業において医薬品と臨床検査については、各医療機関が定める独自の用語・コードから標準的な用語、コードにマッピングするためのツールを開発しました。

シス５．１章

シＱ－４　基本データセットを利用し、一般財団法人医療情報システム開発センター（MEDIS-DC）の標準マスタを組み合わせた場合、医療情報システムのリプレイス時の相互運用性は保証されるか。

Ａ　基本データセット及び標準マスタを活用することは、相互運用性の確保を容易にしますが、保証はされません。なお、基本データセットに含まれない項目や標準が定められていない用語・コードも存在します。

基本データセットや標準マスタは、概ね重要あるいは実装頻度の高いものを対象にしており、採用することによって、相互運用性を確保するためのコストを大幅に下げることができます。

シス５．１章

シＱ－５　データ交換のための国際的な標準規格については、どのようなものがあるか。

Ａ　医療情報に関する国際的な標準である HL7（Health Level Seven）や DICOM（Digital Imaging and Communications in Medicine）については、我が国において利用可能なように、JAHIS により標準規約化されています。

主要なものとしては以下が挙げられます（一部は厚生労働省標準規格にも採択されています）。これらの規約は以下の URL で取得できます。

https://www.jahis.jp/standard/contents_type=33

- JAHIS 病理・臨床細胞 DICOM 画像データ規約
- JAHIS 病理診断レポート構造化記述規約
- JAHIS 処方データ交換規約
- JAHIS 生理検査データ交換規約
- JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格
- JAHIS 内視鏡データ交換規約
- JAHIS 内視鏡 DICOM 画像データ規約
- JAHIS 病理・臨床細胞データ交換規約
- JAHIS 放射線データ交換規約
- JAHIS 放射線治療データ交換規約
- JAHIS 臨床検査データ交換規約
- JAHIS 生理機能検査レポート構造化記述規約
- JAHIS 病名情報データ交換規約
- JAHIS 注射データ交換規約
- JAHIS ヘルスケア分野における監査証跡のメッセージ標準規約
- JAHIS 介護標準メッセージ仕様
- 健康診断結果報告書規格

- リモートサービスセキュリティガイドライン
- JAHIS シングルサインオンにおけるセキュリティガイドラン
- JAHIS 心臓カテーテル検査レポート構造化記述規約
- JAHIS 診療文書構造化記述規約共通編
- JAHIS データ交換規約（共通編）
- JAHIS 保存が義務付けられた診療録等の電子保存ガイドライン
- JAHIS HPKI 電子認証ガイドライン
- HPKI 対応 IC カードガイドライン
- JAHIS 内視鏡検査レポート構造化記述規約

また医療情報システムの相互接続性を推進する国際的なプロジェクトの IHE（Integrating the Healthcare Enterprise）では、標準規格の使い方が定まっていないことに起因する問題を解決するために、標準規格の使い方の「ガイドライン」として Technical Framework を提案しています。これは、分野ごとに実際の医療現場での一般的なワークフロー調査を行い、その上でシステム連携を実現するために必要となる標準規格の使い方を示したガイドラインです。詳細は以下の URL から得られます。

https://www.ihe-j.org/

なお、日本 IHE 協会が IHE Technical Framework を参照した「地域医療連携における情報連携基盤技術仕様」を策定しており、厚生労働省標準規格として採択されています。

シス５．１章

シＱ－６　外字の使用について注意すべき点は何か。

Ａ　外字を使用したシステムでは、あらかじめ使用した外字のリストを管理しておき、システムを変更した場合又は他のシステムと情報を交換する場合に、表記に齟齬のないよう対策する必要があります。

シス５章第④条

シＱ－７　診療情報等が復元できなくなることなどが生じないように、どのような対応をすべきか。

Ａ　媒体・機器・ソフトウェアの不整合により、電子的に保存されている診療録等の情報が復元できなくなることがあります。具体的には、システム移行時にマスタデータベース、インデックスデータベースに不整合が生じること、機器・媒体の互換性がないことにより情報の復元が不完全となる又は読み取りができなくなること等です。このようなことが起こらないように、システム変更・移行時の業務計画を適切に作成する必要があります。

シス５章第④条

シＱ－８　見読性を確保するために、どのような対応が必要か。

Ａ　電子媒体に保存された情報は、紙に記録された情報と違い、以下の理由によりそのままでは見読できない場合があります。

- 電子媒体に格納された情報を見読可能なように画面に呼び出すために、何らかのアプリケーションが必要である。
- 記録が、他のデータベースやマスター等を参照する形で作成されることが多く、データの作成時点で採用したマスター等に依存しなければ、正しい記録として見読できない。
- 複数に分かれて記録された情報の相互関係が、そのままでは一瞥して分かりにくい。

そのため、紙の記録と同等といえる見読性を確保するためには、電子媒体に保存された情報は、これらのことに適切に対応する必要があります。

また、ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の事業者におけるシステムやサービス等により見読性が損なわれることを考慮し、十分な配慮が求められます。その際には、あらかじめ事業者との間で責任を明確化しておき、速やかな復旧が図られるように配慮しておく必要もあります。

シス５章第④条

シＱ－９　汎用性が高く、見読するソフトウェアに困らない形式にはどのようなものがあるのか。

Ａ　医療情報には様々な形態の情報があり、画像、図形、波形、テキスト、数値、グラフ等の形式のデータから構成されています。これらのデータを一様に見ようとするならば、画像化することが、おそらく最も汎用性の高い見読化手段になるでしょう。デジタル情報を画像化するには、PDF（Portable Document Format）が一般的な形式だと考えられます。紙やフィルムの形で存在する場合には、スキャナ等を用いて画像化することで見読可能にできますが、この場合には JPEG（Joint Photographic Experts Group）、PNG（Portable Network Graphics）等の形式を利用することができます。

これらのフォーマットは、PC やスマートフォンなどの情報機器で容易に取得できるソフトウェアによって見読可能な状態にすることができます。

シス５章第④条

シＱ－10　X 線 CT の検査で、オリジナルの画像のほかに、オリジナル画像から生成した３Ｄ画像も使って診断している。電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３Ｄ画像は消去してしまっても構わないか。

３D 画像作成時のパラメータは保存されていないため、診断の際に生成した３Ｄ画像を完全に再現することが難しい状況である。

Ａ　オリジナル画像から当該画像を生成することが原理的に可能であれば、直接診療に使用した処理画像データを保存しておく必要はありません。しかし、この例では、３Ｄ画像作成のパラメータがないと診断に用いた画像を完全に再現することが困難であるということなので、3D 画像を消去することはできません。

シス５章第④条

シＱ－11　3D 画像処理を行った場合、処理を行う元となった画像は保存しなければならないか。

Ａ　3D 画像処理を行う元となった画像を、3D を作成することのみに用い、診断に用いないならば保存する必要はありません。診断用に作成した 3D 画像は保存する必要があります。

シス５章第④条

シＱ－12　確定保存された画像に関し、診断や患者説明のために一時的に医師が表示方法（濃度の変更、拡大など）のみを修正した場合、この画像を保存する必要があるか。

Ａ　濃度の変更、拡大といった程度の処理ならば、改めて保存する必要はありません。

シス５章第④条

シＱ－13　検像において、検像前の画像情報、検像後の画像情報のいずれを保存対象とすべきか。

Ａ　「検像」とは、ここでは医師の診断や読影のために、診療放射線技師等が画像の確定前に当該画像を確認し、必要に応じて画像の付帯情報の修正や不必要な画像の削除を行うことを指すものとします。保存義務の対象とすべき画像については、検像の後に診断に用いるのであり、検像後の画像を対象とすべきと考えられます。ただし、検像において情報の修正・削除といった行為により、照射記録と検像の後の画像情報が一致しない等のことが生じる場合には、修正履歴を保存しておく等、所定の措置が必要となります。また、これらの行為に対する責任の所在を組織として説明できるようにしておく必要があります。

（※）「検像」の定義は公益社団法人日本放射線技術学会が公表している「画像情報の確定に関するガイドライン Ver.2.1」を参照すること。

７．情報管理（管理・持出し・破棄等）

シス７章第⑬条

シＱ－14　「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。」とあるが、どのような留意事項があるか。

Ａ　利用者による外部からのアクセスで問題になることは、利用するＰＣや通信経路等の状態、及び周囲から盗み見されるおそれがある等、職員の作業環境が管理できないことなどが挙げられます。例えば、ＰＣにキーボードロガーのような不正ソフトウェアがインストールされているリスクや、空港や喫茶店等でアクセスすれば周囲の人に覗かれるリスクがあります。

仮想デスクトップは、不正ソフトウェアの作用を避け、ＰＣ上に情報が残留することを防ぐ目的で使用されます。また、通信経路の安全性を確保するため、ＶＰＮの成立と連動して稼働することが望まれます。運用としては、周囲の環境に十分注意して盗み見を防止するとともに、過去のログイン時間の確認を確実に行うこと等を通じて、不正アクセスの検出に努める必要があります。また、不正アクセス等のリスクを回避するために、VPN 接続時には仮想デスクトップ以外のアプリケーションが起動できないようにするなど、VPN 接続と仮想デスクトップとの連携についても留意することが望ましいです。

シス７章第②条

シＱ－15　医療情報システム・サービス事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合はどのような対応をすべきか。

Ａ　例えば、保守に際して医療情報システム・サービス事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合、詳細な持出に関する記録や作業記録を残すよう求めてください。また、必要に応じて、医療機関等の監査に応じるよう求めてください。

シス７章第③条

シＱ－16　情報機器の持ち出し又は外部利用をする場合どのような対策をすべきか。

Ａ　ノートパソコン、スマートフォン、タブレット等を持ち出して使用する場合、次に掲げる対策を実施してください。

紛失、盗難の可能性を十分考慮し、可能な限り端末内に医療情報を置かないでください。やむを得ず医療情報が端末内に存在する場合や、当該端末を利用すれば容易に医療情報にアクセスできる場合は、一定回数パスワード入力を誤った場合に端末を初期化する等の対策を行ってください。

８．利用機器・サービスに対する安全管理措置

シス８章第①項

シＱ－17　情報の破壊及び混同等を防ぐために、どのような対策が挙げられるか。

Ａ　不正ソフトウェア又は不具合等によるソフトウェアの不適切な動作により、電子的に保存された診療録等の情報が破壊されるおそれがあります。このため、不正ソフトウェアによる情報の破壊及び混同等を防ぐためには、不正ソフトウェアによるこれらの情報へのアクセス防止対策を講じることが求められます。

また、医療情報を取り扱うソフトウェアが改ざんされていないこと、及び仕様のとおりに動作していることを、適宜、確認しなければなりません。

さらに、保存されている情報が、改ざんされていない情報であることを確認できる仕組みを設けることが望ましいです。

シス８章第③項

シＱ－18　不正ソフトウェア対策等が大変なので、外部と遮断した環境を設定する方が望ましいのか。

Ａ　不正ソフトウェア混入等の脅威であり、しっかりとした対応が必要です。ただし、サイバー攻撃が巧妙化する中で、外部と遮断した環境とするだけで不正ソフトウェアの侵入を完全に防ぐことはできません。例えば、職員が不用意に USB ポートなどを利用する場合等でも、不正ソフトウェアが混入することがあります。よって、外部と遮断されている環境であっても、不正ソフトウェア対策ソフトの導入、ぜい弱性の対策を行ったソフトウェアの利用等の対策が必要です。

また、外部と遮断することによって、不正ソフトウェア混入のリスクを低減できることは事実ですが、一方で医療情報の有効な利用を図るために、外部との接続を行うことも広く行われるようになっています。この場合でも、効果的な対策を行うことで、リスクを許容範囲に収めることが可能です。

なお、不正ソフトウェア対策ソフトやぜい弱性の対策等については、外部との接続を断つことによって、最新のソフトウェア検知パターンファイルの取得、対策ソフトウェアの緊急アップデート等を、可搬記憶媒体を介して手作業により行うことになるため、作業が遅れたり、可搬記憶媒体が不正ソフトウェアの混入源となったりするリスクがあります。一方で、外部との接続を遮断しつつ、管理者が安全な形で外部から取得した最新の内部サーバから配信するという手段もありますので、利便性とリスクを踏まえて対応することになります。

また端末やサーバ装置の活動を監視し、不正プログラム等の検知や対処を行う EDR（Endpoint Detection And Response）ソフトウェア等の利用や、主体の操作に対する常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等）を用いて内部ネットワーク、外部ネットワーク問わずに対策を講じることも有効な手段として挙げられています。

シス８章第⑥項

シQ－19　医療等分野における IoT 機器に対する安全対策を行う上で、どのような留意事項があるか。

A　近年、様々なモノがネットワークに繋がることで新たなサービス等を実現する「IoT（Internet of Things）」が普及しつつあり、医療等分野での活用も進んでいます。具体的には、医療機関等の内外で用いられる医療機器やバイタルを測定するウェアラブル端末等から患者のデータを収集し、医師の診療支援や経過観察等に活用することや、医療機関等内における職員の位置情報や動線を分析し、病床や人員の配置等を改善すること等が行われています。

このような仕組みやサービスにより、患者の状態をリアルタイムで捕捉できるようになる等、IoT の導入は医療機関等と患者の双方に利益をもたらす可能性があります。ただし、情報セキュリティの観点から、これまで想定されなかったリスクが顕在化するおそれもあります。

IoT 機器により医療情報を取り扱う場合は、医療機器か非医療機器かを問わず、製造販売業者からの情報提供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必要があります。

特に、ウェアラブル端末や在宅設置の IoT 機器を患者等へ貸し出す場合には、機器によって、セキュリティが十分に確保されないおそれがあります。そこで、ウェアラブル端末や在宅設置の機器を貸し出す際は、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事前に患者等へ説明し、同意を得ることが必要です。また、IoT 機器に異常や不都合が発生した場合の問合せ方法等について、患者等に説明する必要があります。

IoT 機器には、機器やサービスの導入後に脆弱性が発見されることがありますので、サービスへの提供に支障が生じないよう適切な時期・方法により対策を講じる必要があります。脆弱性に関しては、IoT 機器が用いる通信規格（例:Bluetooth、NFC 等）の脆弱性についても、併せて対応することが望まれます。

また、IoT の活用状況によって、大量の IoT 機器が同時に接続している環境が想定されますが、この場合、機器の接続状況や異常の発生を正確に把握することが難しいとされます。IoT 機器を含むシステムについて単独でそれぞれの状態を把握できることが望まれますが、機器・システムの中には、大量のログを管理したり、ログの暗号化を行う等の対策を講じることが難しい場合があります。この場合、IoT 機器に関連する他のシステムに監視装置を設置する等、システムやサービス全体での対策が検討することが求められます。

このほか、IoT 機器のリスクとして、使用を終えた又は停止した機器をネットワークに接続した状態のままにしておくと、利用者さえ気付かない間に当該機器が不正に接続される場合がある。さらに、機器の利用状況に関する情報を収集し、不正に利用者を特定される等のリスクも想定されます。

IoT の更なる普及によって、活用方法の多様化や安全性に対する脅威やその対策に係る技術的変化が進み、医療等分野のセキュリティに大きな影響を及ぼす可能性があります。医療機関等においても、今後の動向に注意を払う必要があります。

シス８章第⑧条、第⑨条、企９章第⑥条

シＱ－20　「８．５　医療機関等が管理する以外の機器情報機器の利用に対する対策」について、適切な技術的対策や運用による対策はどのようなものがあるか。特に BYOD を行う場合に、どのような安全対策が必要か。

Ａ　下記の対策等が挙げられます。

医療機関等が管理しているもの以外の機器情報機器の利用、特に BYOD を行う場合における技術的対策としては、職員のモバイル端末で、他のアプリケーション等からの影響を遮断しつつ、仮想デスクトップのような技術を活用して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すること等が考えられます。この場合、OS レベルで業務利用領域（仮想デスクトップ）と個人利用領域を切り分け、管理領域を分離する必要があります。また、サービスや製品によっては十分な安全性が確保されない場合があるため、十分な知見を有する者が判断する必要があります。

さらに、上記の対策に加え、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し、管理する端末と同等の安全性を確保するための、セキュリティ対策の徹底を図ることが期待されます。

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（例えば、「設定」用のアプリケーションにより、医療情報システムへの接続に使用するアプリケーションに対して、他のアプリケーションが自動的にアクセスできるようにする等）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が想定されます。BYOD を行うに当たって、運用管理規程に記載すべき事項の例を下記に示します。

【BYOD に係る運用管理規程への記載事項（例）】

BYOD を認める場合、管理者は下記を遵守すること。

- 利用者に対し、端末や OS 等に応じて推奨されている適切な方法により、アプリケーションをインストールするよう指導すること。
- アプリケーション等の脆弱性に関する情報を収集し、利用者が脆弱性の明らかになったアプリケーションを使用していないか、定期的に確認すること。

シス８章第⑥条

シＱ－21　IoT 機器を含む医療情報システムの接続状況や異常発生を把握するためにはどのような方法あるか。

Ａ　IoT 機器・医療情報システムそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録してください。

９．ソフトウェア・サービスに対する要求事項

シス９章第③条、企１６章第⑧条

シＱ－22　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度であればいいか。

Ａ　診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンしてください。これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからです。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできます。

放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン 3.0 版 （平成 27 年 4 月）」（※）を参考にしてください。

※　http://www.radiology.jp/content/files/20150417.pdf

このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮してください。

一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存してください。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要があります。放射線フィルム等の医用画像情報をスキャンした情報は DICOM 等の適切な形式で保存してください。

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

シス１０章第④条

シＱ－23　医療情報システム・サービス事業者による保守対応が行われた場合に、診療録にアクセスした証跡を確認する方法はどのようなものがあるか。

Ａ　保守作業に関わるログの確認の際に、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者の診療録等に何回アクセスされたか確認できる仕組みを備えてください。

保守作業は、原則、医療機関等の関係者の立会いの下で行わせてください。また詳細なオペレーション記録を保守操作ログとして記録してください。

シス１０章第④条、企７章③条

シＱ－24　医療情報システム・サービス事業者と保守契約を締結する際に、情報流出を防ぐためにどのような対応をすべきか。

Ａ　保守を行う医療情報システム・サービス事業者と保守要員者との間で守秘義務契約があることを求めてください。

シス１０章第⑤

シＱ－25　保守要員が外部機器を持ち込む場合、何を確認すべきか。

Ａ　保守要員の持ち込む機器や記憶媒体に対して、不正ソフトウェアが混入していないことを確認してください。

１１．システム運用管理（通常時・非常時等）

シス１１．１章

シＱ－26　「１１．１　通常時における運用対策表１１－１　平常通常時に対応すべき技術的対応の例の広域災害対策（遠隔地バックアップ等）とあるが」とあるが、「遠隔地」の定義はあるのか。

Ａ　具体的な定義はありませんが、当該医療機関等が地震等の大災害に見舞われた場合でも、それらの被害を受けず、安全に保存できると考えられる地域と考えられます。

シス１１．１章、企１５章第④

シＱ－27　システムが停止した場合の診療継続に備え、見読性を確保するために、医療情報システムにどのような対策を講じるべきか。

Ａ　システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにしてください。

　またシステムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力できるようにしてください。

シス１１．１章、企１５章第④条

シＱ－28　大規模災害の発生により、サーバ等が使用できなくなった場合に備えてバックアップ体制はどのように構築すべきか。

Ａ　大規模火災等の災害対策として、遠隔地のデータバックアップを使用した見読機能を確保する必要があります。電子保存記録のバックアップを遠隔地に保存するとともに、そのバックアップデータ等と汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにしてください。

シス１１．１章、企１５章第④条

シＱ－29　非常時における利用に備えて、診療録等をどのように保存すべきか。

Ａ　非常時に必要になることが予測される診療録等の見読性の確保するため、非常時に必要になることが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持してください。

　またその分量等ですが、各医療機関等の機能により判断すべきですが、診療録等の参照が迅速に行えないことで、患者の生命や身体に重大な影響を及ぼすおそれがあることが想定されるものが対象となります。例えば、これから手術を行う方や入院されている方の診療録等が想定されます。通常１週間程度のデータ、あるいは前回の診療データも目安になります。

シス１１．２章

シＱ－30　障害等によるデータ保存時の不整合に備えて、どのような対応をすればいいか。

Ａ　ネットワークを通じて外部に保存する場合、診療録等を転送している途中でシステムが停止したり、ネットワークに障害が発生することなどにより、正しいデータが外部の委託先に保存されないことも起こり得ます。その際は、再度、外部保存を委託する医療機関等からデータを転送する必要が生じる場合があります。

　そのため、委託する医療機関等は、医療機関等内部のデータを消去する等の場合には、外部保存を受託する事業者において、当該データが保存されたことを確認してから行う必要があります。

12. 物理的安全管理措置

シス１２章第①条

シＱ－31　不適切な保管・取扱いによる情報の滅失、破壊を防止するために、どのような対応が考えられるか。

Ａ　電子的な情報を保存している媒体が不適切に保管されている、あるいは情報を保存している機器が不適切な取扱いを受けているために情報が滅失してしまうか、破壊されてしまうことがあります。このようなことが起こらないように、情報が保存されている媒体及び機器の適切な保管・取扱いが行われるように、技術面及び運用面での対策を施さなければなりません。

使用する記録媒体や記録機器の環境条件を把握し、電子的な情報を保存している媒体や機器が置かれているサーバ室等の温度、湿度等の環境を適切に保持する必要があります。また、サーバ室等への入室は、許可された者以外が行うことができないような対策を施す必要があります。

また、万一、滅失であるか改ざん又は破壊であるかを問わず、情報が失われるような場合に備えて、定期的に診療録等の情報のバックアップを作成し、そのバックアップを履歴とともに管理し、復元できる仕組みを備える必要があります。この際に、バックアップから情報を復元する際の手順と、復元した情報を診療に用い、保存義務を満たす情報とする際の手順を明確にしておくことが望ましいです。

シス１２章第②条

シＱ－32　診療録等のデータを保存するサーバ等を保管する区画において、不正な行動による破壊の防止するために、どのような方法があるか。

Ａ　診療録等のデータを保存するサーバや記録媒体、記録機器を保管する区画において、不正な行動による破壊等を防止するために、サーバ等は、許可された者しか入ることができない区画に保管するとともに、サーバ室等には、許可された者以外が入室できないよう、施錠等の物理的な対策を施してください。

また、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存してください。さらにサーバ室等の安全管理上重要な場所では、モニタリング等により職員の行動を管理してください。

シス１２章第④条

シＱ－33　診療録等のデータのバックアップの管理や方法に関して、どのような留意事項があるか。

Ａ　診療録等のデータのバックアップについては、定期的に取得するとともに、その内容に対する改ざん等が行われていないことを検査する機能を備えてください。

　また、障害などに備えて診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 又は RAID-6 相当以上のディスク障害に対する対策を行ってください。

シス１２章第⑤条

シＱ－34　記録媒体、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に、どのような対応が考えられるか。

Ａ　記録媒体、記録機器の劣化による読み取り不能又は不完全な読み取りにより、電子的に保存されている診療録等の情報が滅失してしまうか、破壊されてしまうことがあります。これを防止するために、記録媒体や記録機器の劣化特性を考慮して、劣化が起こる前に新たな記録媒体や記録機器に複写する必要があります。

シス１２章第⑥条

シＱ－35　医療情報の入力や閲覧に際して、情報の漏えいを防ぐために具体的にどのような対策をすべきか。

Ａ　外部での情報機器の覗き見による情報の漏えいを避けるため、ディスプレイに覗き見防止フィルタ等を張ってください。

　また　個人情報を入力・参照できる端末から離席する場合、クローズ処理等（クリアスクリーン、ログオフ、パスワード付きスクリーンセーバーの起動等）を実施してください。

13．ネットワークに関する安全管理措置

シス１３章第②条

シQ－36　専用線以外の回線サービスを利用する場合、どのような留意事項があるか。

A　過去には、重要な情報システムの利用に際しては、専用線などを用いることが多かったのですが、現在のブロードバンドの普及状況やセキュリティ技術の向上から、公衆回線等を活用した回線サービスを用いて医療情報システムで利用するネットワークを構築することで導入コストを削減したり、地域医療情報連携の仕組みを構築したりする等、その利用範囲が拡大していくことが考えられます。この場合、セキュアなネットワークを用いて、安全な通信を行うことが求められます。

その際、OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書」（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム：HEASNET；平成 19 年３月）が参考になります。

※　OSI 階層モデル（Open Systems Interconnection）：開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコル。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択ための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電気的、物理的に変換。機器の形状・特性を規定している層

表　OSI 階層モデル

接続先や経路先を管理することによりセキュアなネットワークの構築が期待されますが、OSI 階層に応じてこのリスクとそれを踏まえた対策が異なってきます。

例えば、SSL-VPN を用いる場合、５階層目の「セッション層」といわれる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ありませんが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在します。また、偽サーバへの対策が不十分なものが多いという指摘があります。一方、IPsec を用いる場合は、２階層目の「データリンク層」又は３階層目の「ネットワーク層」といわれる部分で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低くなっています。そのため、SSL-VPN を使用する場合には、適切な手法の選択及び必要な対策を行う必要があります。ただし、この場合でも、経路を暗号化するための暗号鍵の取り交わしに IKE（Internet Key Exchange）といわれる標準的手順を組み合わせる等により、確実にその安全性を確保する必要があります。

また、IPsec を用いた VPN 接続等によるセキュリティの担保を行わず、インターネット等のオープンなネットワークを介し、他の医療機関や患者等が医療情報システムへ接続する場合（下図）は、少なくとも TLS による暗号化を用いた HTTPS の利用が求められます。

図　オープンネットワークで接続されている場合

しかし、昨今 TLS においてプロトコルやソフトウェアの脆弱性を突いた攻撃の報告が相次いでおり、TLS を適切に利用しなければ接続に HTTPS を用いても、必ずしも安全性を確保することができません。TLS を利用する上での適切な設定方法は、CRYPTREC が作成し独立行政法人情報処理推進機構によって発行された「TLS 暗号設定ガイドライン」にて指針が示されている。「TLS 暗号設定ガイドライン」にて示される設定をすることで、TLS への既知の攻撃から、一定の安全性を確保することができます。なお現時点で最新の「TLS 暗号設定ガイドライン 3.0.1 版」では 3 段階の設定基準が定められているところ、医療情報システムで利用する場合は、そのうち最も安全性水準の高い「高セキュリティ型」の設定を反映することで TLS への攻撃リスクを低減する必要があります。「高セキュリティ型」の設定の一つとして、利用可能なプロトコルバージョンを TLS1.3 に設定するものの、システムやサービス等の対応上、これによることが難しい場合には、TLS1.2 以上に限定して設定する必要があります。そのため、サーバ・クライアントともに TLS1.2 以上をサポートしていることが必須となることに注意することが必要です（TLS1.2、TLS1.3 のいずれかの利用に限定している場合には、それぞれのプロトコルをサポートしていることが求められる）。加えて、オープンなネットワークの場合、不特定の端末から接続されるリスクがあるため、対策の一つとして TLS クライアント認証を行う必要があります。

さらに、オープンネットワークで接続する場合には、IPsec や TLS によるセッションが安全でも、他セッションが同居できるため、ネットワークに接続している機器やシステムが標的型メール等の攻撃にさらされるリスクがある。仮に、このような攻撃によってネットワークに接続する端末等に不正ソフトウェアが混入し、遠隔操作が可能になると、IPsec や TLS1.2 以上によるセッションへの正規のアクセスが発生する可能性があります。

IPsec や TLS による接続は、適切な経路設定を行うことで、セッション間の回り込みを回避することが可能である。一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公開している「レセプト・オンライン請求用チェックシート項目集」（※）が参考になります。

※　「レセプト・オンライン請求用チェックシート項目集」
https://hispro.or.jp/open/pdf/200909OnRece%20koumoku.pdf

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要があります。なお、日頃からセキュリティインシデントの報道や事業者からの情報提供等を通じて、TLS 等の脆弱性リスクについて注意、認識しておくことが求められます。また、多くの場合、ネットワーク導入時に事業者等に委託をすることになるが、その際、リスクの説明を求め、理解しておくことも必要です。

なお、オープンネットワークを通じて外部から情報を取り込む際に、取り込む情報の安全性を確認する必要があり、そのため例えば取り込むデータ等についての無害化を図るなど、標的型攻撃等によるリスクを減少する対応を図ることが求められます。

また、外部との接続については、医療機関等がクラウドサービスを利用し、医療情報システム・サービス事業者等のサーバからデータを取得する場合も、同様のリスクを想定する必要があります。特にクラウドサービスの場合には、利用するサービスによって、取り扱う情報の機密性等が異なるため、事業者によってセキュリティの水準が異なることがあります。したがって、医療情報を取り扱う場合には、利用する各クラウドサービスにおけるリスク等を鑑みた対応をとることが求められます。必要に応じて、ネットワークの論理制御（例えばメールシステムと医療情報システムの情報が混在しないようにすること等）や、これを踏まえた情報交換のルールに基づく管理を行うことが望まれます。

シス１３章第②条

シＱ－37　医療機関等におけるネットワークに対する不正アクセスへの対策を講じる際、どのような留意事項があるか。

Ａ　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りますが、これに加えて、不正な攻撃を検知するシステムファイアウォールは、「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式があります。また、その設定によっても動作機能が異なるので、単にファイアウォールを導入すれば安心というものではありません。単純な「パケットフィルタリング」で十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望まれます。医療情報システム安全管理責任者は、その方式が何をどのように守っているかを認識する必要があります。このことは、医療機関等の外部から医療機関等の医療情報システムに接続する場合も同様です（「７．情報管理（管理・持出し・破棄等）」参照）。

部外者により物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、不正ソフトウェアが混入したり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS：Denial of Service 等）を行ったりすることや、不正にネットワーク上のデータを傍受したり改ざんしたりすることが可能となります。

不正なコンピュータの物理的な接続に対する対策を行う場合、一般的に MAC アドレスを用いてコンピュータを識別する場合が多いが、MAC アドレスは改ざん可能なため、そのことを念頭に置いた上で対策を行う必要です。不正アクセスの防止は、いかにアクセス先の識別を確実に実施するかが重要であり、特に、“なりすまし”の防止は確実に行う必要があります。無線 LAN のアクセスポイントを複数設置して運用する場合等、マネジメントの複雑さが増し、侵入の危険が高まるような設置をする場合には、一層留意が必要であります。

また、ネットワーク上を流れる情報の盗聴を防止するために、暗号化等による“情報漏えい”への対策も必要となります。

シス１３章第⑤条

シＱ－38　「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すること。」とあるが、どのようなものが安全性が確認できる機器として考えられるのか。

Ａ　安全性が確認できる機器としては、ISO/IEC 15408 で規定されるセキュリティターゲット又はそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものなどが挙げられますが、この規格で認証された機器を導入することは必須ではありません。このガイドラインが求める安全対策のための要求事項を、導入を検討している機器ベンダに示して、回答を求めてください。満足する回答が得られれば、安全性が確認された機器と判断していただいて結構です。

　また、「ルータ等のネットワーク機器の機能をソフトウェアで実現しているもの」については、その当該ソフトウェアに対して安全性が確認できる必要があります。「ルータ等のネットワーク機器」を「当該ソフトウェア」に読み替えてご対応ください。

シス１３章第⑥条

シＱ－39　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）とは、具体的にどのような事象を指すものか。

Ａ　例えば、下図のように、医療情報連携ネットワークの Web サーバへのアクセス等のために、医療機関等の専用端末がソフトウェア型の IPsec や TLS1.2 以上によりオープンネットワークに接続している場合、攻撃者は開放された当該端末のポートを標的として、何らかの攻撃（典型的には標的型メール攻撃等）を試みることが想定されます。

　この攻撃により、当該専用端末が遠隔操作型のマルウェア等に感染すると、攻撃者は本人になりすまして医療情報連携ネットワークの Web サーバとのセッションの立上げを試みることが可能になります。セッションの立上げに成功すると、外観上は正規の権限によるアクセスが発生することになり、IPsec や TLS1.2 以上により適切に暗号化していても、攻撃者は医療情報連携ネットワークの Web サーバにアクセスできるようになります。

　ガイドラインでは、この一連の攻撃を「セッション間の回り込み」と称しています。対策として、適切な経路設定を実施することに加え、医療情報連携ネットワークへのアクセスに当たって、二要素認証により利用者の識別・認証を行うことで、遠隔操作を防ぐこと等が考えられます。

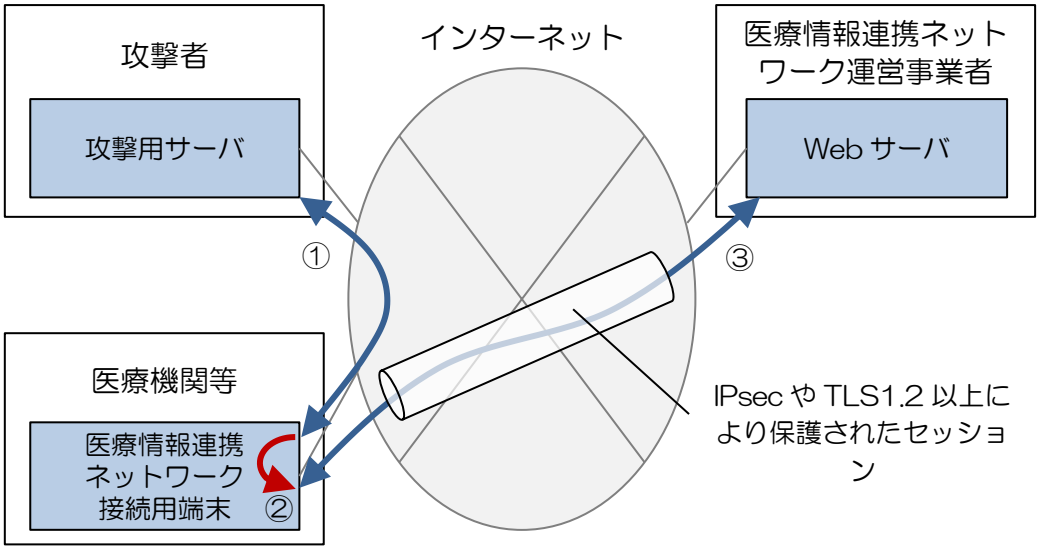


図　セッション間の回り込み（イメージ）

シス１３章第⑥条

シQ－40　「１３．ネットワークに関する安全管理措置 」⑥に「 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」とあるが、具体的にはどのように利用するのか。

A　安全管理ガイドラインでは、偽サーバへの対策が不十分なものが多いため、医療情報システムでは原則として使用するべきではないとしています。しかし SSL-VPN についてもクライアント型と呼ばれるものについては、「専用のクライアントソフトがインストールされた端末との間でのみアクセスする。つまり、誤って偽サーバに接続することがなく、また内部サーバにアクセスできる端末も厳格に制限できるため、端末に IPsec-VPN ソフトをインストールして構成するモバイル型の IPsec-VPN に近い形での運用形態」が可能とされています（「TLS 暗号設定ガイドライン 3.01 版」IPA）。

従って、SSL-VPN を利用する場合には、１３．ネットワークに関する安全管理措置⑥に記載されているクライアント証明書を利用した TLS クライアント認証や「高セキュリティ型」に準じた適切な設定を行った上で例外的にクライアント型の SSL-VPN などの利用によることが考えられます。

シス１３章第⑬条

シＱ－41　無線 LAN の利用において、どのような留意事項があるか。

Ａ　無線 LAN は、看護師等が情報端末を利用し患者のベッドサイドで作業する場合等において利便性が高い反面、通信の遮断等も起こる危惧があります。そのため、情報の可用性が阻害されないように留意する必要があります。また、無線電波により重大な影響を被るおそれのある機器等の周辺での利用には注意が必要です。

無線 LAN の運用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考に対策を実施する必要があります。

シス１３章第⑪条

シＱ－42　「なりすまし」に対しては、具体的にどのような対応をとればいいか。

Ａ　ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の機関が確かに意図した相手であるかを確認しなければなりません。逆に、情報の受け手となる送信先の機関は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られてきた情報が確かに送信元の医療機関等の情報であるかを確認する必要があります。これは、ネットワークが非対面による情報伝達手段であることに起因するものです。

そのため、例えば通信の起点と終点の機関を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられます。また、改ざん防止と併せて、送信元が正当な送信元であることを確認するために、医療情報等に対して電子署名を組み合わせることも考えられます。

シス１３章第⑪条

シＱ－43　「盗聴」に対しては、具体的にどのような対応をとればいいか。

Ａ　ネットワークを通じて情報を伝送する場合には、盗聴に最も留意しなくてはなりません。盗聴は様々な局面で発生します。例えば、何者かがネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取ったりする等、必ずしも医療機関等の責任といえない明らかな犯罪行為も想定されます。一方、ネットワーク機材の不適切な設定による意図しない情報漏えいや誤送信等、医療機関等が責任を負うべき事例も考えられます。

このように様々な事例が考えられる中で、医療機関等においては、万一、伝送途中で情報が盗み取られたり、意図しない情報漏えいや誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要があります。その一つの方法として医療情報の暗号化が考えられます。ここでいう暗号化とは、先に例示した情報そのものの暗号化（オブジェクト・セキュリティ）のことを指しています。

どのような暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密性や医療機関等で構築している医療情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ですが、少なくとも情報を伝送し、医療機関等の設備から情報が送出される段階においては暗号化されていることが望まれます。

この盗聴防止については、例えばリモートログインによる保守を実施する時も同様です。その場合、医療機関等は上記のような留意点について、保守作業を受託する事業者等に確認し、監督する責任を負うことになります。

シス１３章第⑪条

シQ－44　「改ざん」への対応として、どのような留意事項があるか。

Ａ　ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えなければなりません。情報を暗号化して伝送する場合には改ざんの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要があります。また、ネットワークの構成によっては、ネットワーク自体に情報の秘匿化機能が不十分な場合もあるので、改ざんに対する対処は確実に実施しておく必要があります。

なお、改ざんを検知するための方法としては、例えば、電子署名を用いる等が想定されます。

シス１３章第⑪条

シQ－45　ネットワークを介して送信元と相手先の当事者間でやりとりする情報に対する暗号化等のセキュリティ対策を実施するためにはどのような技術があるか

Ａ　例えば、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用してください。

シス１３章第⑪条

シQ－46　許可された者以外の無線 LAN の利用を防止するためにはどのような対策が必要か。

A　許可された者以外の無線 LAN の利用を防止するため、例えば 802.1x や電子証明書を組み合わせるなどして、無線 LAN のセキュリティを強化してください。

シス１３章第⑬条

シQ－47　医療機関等におけるローカル５Gの利用について、具体的な事例等はあるか。

A　医療分野でのローカル5G の利用については、現時点では実証段階のケースが多く、具体的な事例は多くはありません。今後具体的な導入実態を踏まえて導入の検討を図ることが望まれます。

14. 認証・認可に関する安全管理措置

シス１４章第①条

シQ－48　認証方法が安全な利用者の識別・認証方法を選定する際、どのような留意事項があるか。

A　利用者の識別・認証方法を選定する際には、認証の安全性を考慮する必要がありますが、その際に、認証強度が高い利用者の識別・認証を採用することが求められます。

これまで使われてきた ID・パスワードの組み合わせは、これまで広く用いられてきた方法ですが、ID・パスワードによる認証ではその運用によっては、リスクが大きくなります。認証強度を維持するためには、交付時の初期パスワードの利用者本人による変更や定期的なパスワード変更を義務付ける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要があります。

ただし、このような対策を徹底することは一般に困難であると考えられるため、その実現可能性の観点からは必ずしも推奨されません。

認証に用いる手段としては、ID・パスワードの組み合わせのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体情報」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的です。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難です。そこで、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように、認証の３要素である「記憶」、「生体情報」、「物理媒体」のうち、２ つの独立した要素を組み合わせて認証を行う方式（二要素認証）を採用することが望ましいとされます。

なお、認証に際して、二段階で認証を行う二段階認証と呼ばれる方法がありますが、この場合には利用される認証要素が同一となることもあるため、実質的にリスク低下につながらないこともあります。そのため、二段階認証を選択するだけでは二要素認証の要求を満たさないと考えるべきでしょう。

また、シングルサインオン方式を用いて、一度の認証により複数のアプリケーションを操作する場合であっても、最初のログイン時に二要素認証を行っていれば、セキュリティは確保されていると考えられます。ただし、ログイン状態のまま長時間放置したり、特定の端末でログインしただけで院内の複数の端末にログイン可能となるような運用は認められません。また利用者が端末から長時間離席する場合には、正当な利用者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきでしょう。

シス１４章第③条

シＱ－49　利用者の識別・認証に IC カード等のセキュリティ・デバイスを配布する場合、どのような留意事項があるか。

Ａ　利用者の識別、認証、署名等を目的として、IC カード等のセキュリティ・デバイスに個人識別符号のうち指紋等の生体情報に関するデータや暗号化鍵、電子証明書等を格納して配布する場合は、これらのセキュリティ・デバイスが誤って本人以外の第三者の手に渡ることのないよう対策を講じる必要があります。また、万一そのセキュリティ・デバイスが第三者によって不正に入手された場合でも、簡単に利用されないようにすることが重要です。

したがって、利用者の識別、認証、署名等が、これらセキュリティ・デバイス単独で可能となるような運用はリスクが大きいため、必ず利用者本人しか知り得ない情報との組み合わせによってのみ有効になるようなメカニズム、運用方法を採用しなければなりません。

また、IC カードの破損等、本人の識別情報が利用できない時を想定し、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しておく必要があります。その際、安全管理のレベルを安易に下げることがないよう、本人確認を十分に行った上で代替手段の使用を許し、さらにログ等を残して、後日再発行された本人の正規の識別情報により、上記緊急時の操作のログ等の確認操作をすることが望まれます。

シス１４章第⑥条

シＱ－50　「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」とあるが、類推を防ぐために定期的な変更を求めることは有効か。

また、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、導入または更新する場合、原則として二要素認証を採用する趣旨は何か。

Ａ　医療情報システムにおいては、医療情報を預かる医療従事者による職務上の安全確保という観点から、推定困難なパスワードを設定することが求められます。

パスワードの要件による安全性については、日々研究が進められています。近年では、定期的な変更を行うことで利用者が推定可能なパスワードを設定することで、むしろ脆弱になってしまうという報告もあります。

米国国立標準技術研究所（以下、「NIST」）から 2017 年６月に公表された「SP 800-63-3（Digital Identity Guidelines（デジタルアイデンティに関するガイドライン））第３版」においては、パスワードの定期的な変更を強制することにより、「類推されやすいパスワードを使用しない」という要件を満たさないことになるリスクが指摘されています。

他方、「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）（内閣官房 内閣サイバーセキュリティセンター（以下「NISC」））」においては、利用者にパスワードの定期的な変更を求めるか否かは、その効果と逆効果を勘案して判断する必要がある旨を指摘しています。例えば「オフライン攻撃を許す旧式の認証プロトコルが用いられている場合であって、13 文字といった十分に長いパスワードを設定できない旧式の情報システムを用いている場合には、パスワードの定期的な変更は必要である。この場合には、オフライン攻撃によってパスワードを復元されるまでにかかる時間を踏まえて、必要な周期での定期的な変更を求める必要がある」としています。

医療情報を取り扱う医療情報システムの性格や構成を鑑みると、原則として、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが求められる。ただし、利用するパスワードが 13 文字以上のランダムな設定がなされており、パスワード管理の安全性などが担保されているシステムを用いている場合には、パスワードの定期的変更は必ずしも求められない（※１）。なお、これらのパスワード変更に関するルールは、ＩＤとパスワードのみによる認証を用いている場合に該当するものです。

なお二要素認証を採用している場合、必ずしもパスワードの定期的な変更は求められない。）。

また、医療情報システムのシステム上の制約等で 13 文字以上の文字列を設定できない又は適切な管理を行うことができない環境においては、推定困難なパスワードを、脆弱にならない形（※２）で定期的に変更させることにより、安全性を担保することができると考えられます。この場合、英数字、記号を混在させた８文字以上の推定困難な文字列のパスワードでもよいとしております。

しかしながら、ID とパスワードによる認証では、安全性の確保に限度があります。前述の報告においても、医療情報のような個人情報へのアクセスは二要素以上の認証を組み合わせる認証方式（二要素認証）とすることが示されています。そのため、できるだけ早く二要素認証を導入することが求められます。本ガイドラインでは、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、導入または更新する場合、原則として二要素認証を採用することを求めています。導入または更新に際して、対象となる製品・サービスがベンダ等から提供されていないなどの理由で二要素認証対応が困難な場合にも、対象となる医療情報システムの利用に供する部屋の入室管理を個人ごとに特定できるようにする等の措置を講じて、全体として二要素認証に相当する安全性の確保を行う必要があります。

（※１）例えば、漏えいしたことのある及び推定可能な脆弱なパスワードを設定できない技術的な制約を課すことや、設定しようとするパスワードの強度が確認できること等の管理が挙げられています。（実装に関係される方は“Digital Identity Guidelines から Authentication and Lifecycle Management”（NIST Special Publication 800-63B ）https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf を参照してください）。

（※２）例えば、以前のパスワードから推定可能なパスワードといった解析のヒントを与えないような形が想定されます。

シス１４章第③条

シQ－51　利用者の識別・認証で二要素認証を採用する際、指紋、虹彩等のバイオメトリクスを利用する場合、どのような留意事項があるか。

Ａ　利用者識別・認証に指紋や虹彩、声紋等のバイオメトリクスを用いる場合の留意点として、その測定精度にも注意を払うことが挙げられます。医療情報システムで一般的に利用可能と思われる各種のバイオメトリクス機器の測定精度は、現状では、１対Ｎ照合（入力された 1 つのサンプルが、登録されている複数のサンプルのどれに一致するか）には十分とはいえないため、１対１照合（入力されたサンプルが、特定の１つのサンプルと一致するか）での利用が妥当であると考えられます。

したがって、バイオメトリクスを用いる場合は、単独での識別・認証を行わず、必ずユーザ ID 等個人を識別できるものと組み合わせて利用するべきです。

また、生体情報を基に認証するに当たって、以下のような生体情報特有の問題があります。

- 事故や疾病等による認証に用いる部位の損失等
- 成長等による認証に用いる部位の変化
- 一卵性の双子の場合における特徴値の近似
- 赤外線写真等による“なりすまし”（IC カード等の偽造に相当）

上記のことを考慮の上、生体情報の特徴を吟味し適切な手法を用いる必要があります。欠損への対処としては異なる手法や異なる部位の生体情報を用いること、なりすましへの対処としては二要素認証（IC カードやパスワードとバイオメトリクスの組み合わせ等）を用いることが求められます。これらのことを踏まえ、実際の採用が想定される二要素認証の方式として、下記の例が挙げられます。

二要素認証の採用例

- ユーザ ID＋パスワード＋指紋認証
- IC カード＋パスワード
- IC カード＋静脈認証等

シス１４章第③項

シQ－52　FIDO 認証（※１）に関して、どのような留意事項があるか。

A　FIDO 認証を使用し、医療情報システムの利用者の識別・認証を行う場合には、求められる当人認証の頑強性として、「Digital Identity Guidelines」（NIST　SP800-63）で定められている AAL（Authentication Assurance Level）の強度：Level２以上の技術を採用することが望ましいです（※２）。

例えば、FIDO―U2F（Universal 2nd Factor）は、２要素認証による技術であるため、安全性が高く、AAL3 に位置付けられますが、２要素認証によらない場合には、AAL３を満たさないこともあります。

FIDO 認証のメリットとしては、既存のスマートフォンの機能などを活用することが可能であるため、導入しやすいなどが挙げられます。他方で、デメリットとしてはパスワード認証との併用、利用者の使用デバイスの登録などによる認証フローが複雑になりやすいなどがあります。

（※１）FIDO（Fast IDentity Online）認証とは、オンラインの認証サーバを通じてパスワード不要で利用者を認証する仕組みです。具体的な利用方法は、FIDO 認証対応のスマートフォンで利用者に対する使用デバイスの登録を行い、本人認証を行うなどが挙げられます。なお、FIDO 認証では生体認証機能を利用することでパスワードに代わる認証が行われることが多いとされますが、生体認証に限らず他の方式の技術によることも可能とされています。

（※２）「企画管理編　１３．医療情報システムの利用者に関する認証等及び権限」参照

シス１４章第①条

シQ－53　ネットワーク上からの不正アクセスを防止するためにどのような対策が必要か。

A　外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分には、ファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定してください。

シス１４章第⑥条

シＱ－54　パスワードを用いた利用者認証に関して、不正な攻撃への対応としてどのようなことが挙げられるか。

Ａ　不正な攻撃に対応するために、類推されにくいパスワードや辞書攻撃を受けにくいパスワード等が求められます。

例えば以下のような例が挙げられます。なお、類推されやすいパスワードには、利用者の氏名や生年月日、辞書に記載されている単語等が含まれるものがあります。

a. 英数字、記号を混在させた 13 文字以上の推定困難な文字列
b. 英数字、記号を混在させた 8 文字以上の推定困難な文字列を定期的に変更させる（最長でも２ヶ月以内）
c. 二要素以上の認証の場合、英数字、記号を混在させた 8 文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用に PIN 等が設定されている場合には、この限りではない。
いずれのパスワードを設定した場合でも、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏えい対策が講じられていることを確認すること。

このうち c.の場合、二要素認証となり、ＩＤ／パスワードのみの認証よりも安全性が高いことから、二要素認証におけるパスワードについては、同項 a.、b.の要件とは異なり、8 文字以上の推定困難な文字列であっても定期的な変更は求めないこととしています。

パスワード長については、原則として英数字、記号を混在させた８文字以上としていますが、例外として二要素認証のもう片方の認証要素を使う際に、ＰＩＮなどが設定されているなどの安全管理が施されている場合には、上記のパスワード長のルールは求めないこととしています。この理由は、IC カードに格納されている電子証明書等の認証要素（知識以外の要素）を使うために設定されている場合のＰＩＮは、ＩＤ／パスワード（知識）におけるＩＤに紐づくものではなく、厳密に言えばパスワードとは異なるためです。このようなケースでは利用者認証全体を勘案すると、ＩＤ／パスワードのほかに、ＩＣカード（所有）や指紋認証（生体）などの知識ではない認証要素、さらに追加の認証要素（知識）を利用するＰＩＮなどが設定されていることになるため、十分な安全性が確保されるものと評価されると考えられます。そのため、このような場合には、英数字、記号を混在させた８文字以上というパスワードの要件は求めないこととしています。具体的には下図の通りなります。

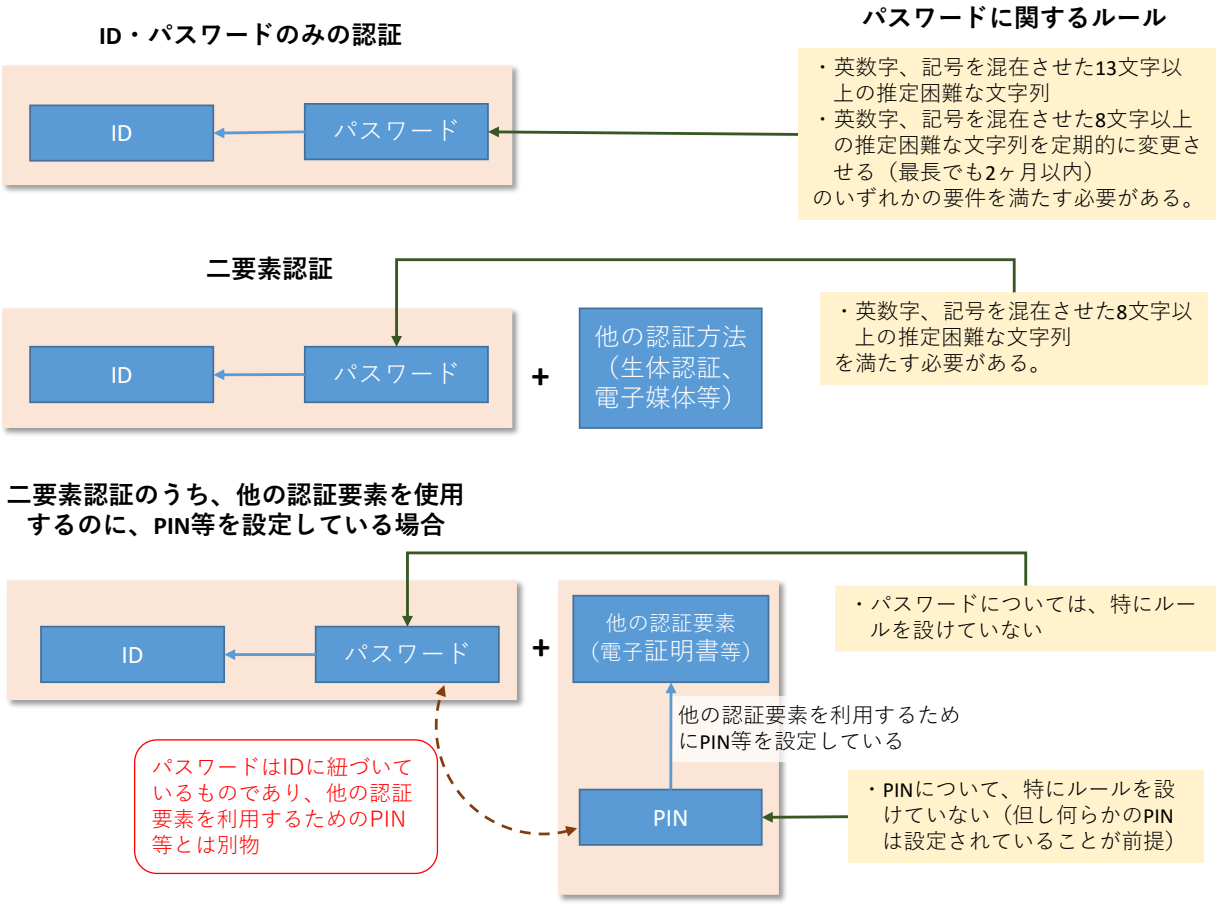


図　パスワードを用いた利用者認証

また不正な攻撃に対して、連続する攻撃を避けるため、次に掲げる対策を実施してください。

- パスワード入力が不成功に終わった場合、再入力に対して一定の不応時間を設定すること
- パスワード再入力の失敗が一定回数を超えた場合、再入力を一定期間受け付けない仕組みとすること

シス１４章第⑤条、企１５章第⑥条

シＱ－55　認証を伴う情報機器を通じた不正アクセスを防止するためにどのような対策が必要か。

Ａ　まず、情報機器やソフトウェアに関しては、出荷時の初期パスワード、可能であればＩＤも含めて変更することが求められます。そのうえで、情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いてください。

シス１４章第⑧条

シＱ－56　「虚偽入力、書換え、消去及び混同を防止する」ために、はどのように、どのような対応が求められるのか。

Ａ　保存義務のある文書等の電子保存に際して、電子保存を実施する医療情報システム安全管理責任者は、正当な手続を経ずに、あるいは過失により、電子化した診療情報等が誤入力、書換え・消去及び混同されたりすることを防止する対策を講じる必要があります。また、システムで診療録等の情報の作成、書換え、消去等の作業をする入力者（以下「入力者」という。）、記録の確定（※）を実施する権限を有する確定者（以下「確定者」という。）は、情報の保存を行う前に情報が正しく入力されており、過失による書換え、消去及び混同がないことを確認する義務があります。

※　記録の確定とは、入力者により入力された情報に対して、確定を実施する権限を有する確定者によって入力の完了が確認されることや、検査、測定機器による出力結果の取込みが完了することです。

虚偽入力、書換え、消去及び混同に関しては、入力者等の故意又は過失に起因するものと、使用する機器、ソフトウェアに起因するものの２つに分けることができます。

前者は、例えば、入力者が故意に診療録等の情報を改ざんする場合や、入力ミス等の過失により誤った情報が入力されてしまう場合等が考えられます。

後者は、例えば、入力者は正しく情報を操作しているが、使用している機器やソフトウェアの誤動作やバグ等により、入力者の入力した情報が正しくシステムに保存されない場合等が考えられます。

これらの虚偽入力、書換え、消去及び混同の防止は、機器やソフトウェアにおける技術的な対策だけで防止することが困難なため、運用的な対策も含めて防止策を検討する必要があります。

①　故意又は過失による虚偽入力、書換え、消去及び混同の防止

故意による虚偽入力、書換え、消去及び混同はそもそも違法行為であるが、それを防止するためには、以下が守られなければなりません。

- 情報の入力や記録の確定に係る作業の手順等を運用管理規程に記載すること。
- 情報の入力者、及び入力者と確定者が異なる場合はその両者（以下「入力者及び確定者」という。）が明確で、いつでも確認できること。

- 入力者及び確定者の識別・認証を確実に行うこと。すなわち、なりすまし等が行えないような運用操作環境を整備すること。
- 入力者やシステムを操作できる者の権限に応じてアクセスできる情報を制限すること。
- 入力者及び確定者が行った操作に関して、いつ、誰が、どこで、どの情報に対して、どんな操作を行ったのかが記録され、必要に応じて、操作記録に対して医療機関等が定めた運用管理規程に準拠した適正な利用であることが監査されること。
- 確定された情報は、確定者によって確定操作が実施されたことが医療機関等で定めた運用管理規程に準拠して監査できること。
- 確定され保存された情報は、運用管理規程で定めた保存期間内は履歴を残さないで改変、消去ができないようにすること。
- システムの改造や保守等で診療録等にアクセスされる可能性がある場合には、真正性確保に留意し、システム運用編 10 に記載された手続きに従うこと。

過失による虚偽入力、書換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じます。誤入力等を問題ないレベルにまで低減する技術的方法は存在しないため、入力ミス等は必ず発生するとの認識の下、運用上の対策と技術的対策の両面から誤入力等を防止する対策を講じることが求められます。例えば、情報の確定を行う前に十分に内容の確認を行うことを運用管理規程に定めるとともに十分な教育訓練を行う、あるいは、ヒヤリ・ハット事例に基づき誤操作の発生しやすい箇所を色分け表示する等、操作者に注意喚起を行う技術的対策を施すことが望ましいです。

② 使用する機器、ソフトウェアに起因する虚偽入力、書換え、消去及び混同の防止

使用する機器、ソフトウェアに起因する虚偽入力、書換え、消去及び混同とは、入力者が正当に入力したにも関わらず、利用しているシステム自体に起因する問題により、結果が入力者の意図したものと異なる状況となるリスクを指す。このような状況が発生する原因として下記のケース等が考えられます。

- システムを構成する機器、ソフトウェア自体に問題がある場合（故障、熱暴走、ソフトウェアのバグ、バージョン不整合等）
- 機器、ソフトウェアに問題はないが、正しく設定されていないために所定の機能動作をしない状態になっている場合
- 正当な機器、ソフトウェアが悪意ある第三者により別のものに置き換えられている場合
- 不正ソフトウェアが混入し、データの不正な書換え、消去や、ソフトウェアの誤動作が発生している場合

これらの脅威は、システムの導入時に入念な検証を行うとともに、システムの維持と管理を適切に行うことで防止できると考えられるため、医療機関等においてシステムの品質管理を十分に行う姿勢が重要です。具体的な方策については、【遵守事項】の記述を参照してください。

シQ－57　「作成の責任の所在を明確する」ために、はどのように、どのような対応が求められるのか。

Ａ　電子保存の対象となる情報は、記録を作成するごとに入力者及び確定者が明確になり、作成の責任の所在が明らかになっている必要があります。また、一旦記録された情報を追記・訂正・消去することも日常的に行われるものと考えられるため、追記・訂正・消去するごとに入力者及び確定者が明確になっている必要があります。

医療機関等の規模や管理運営形態により、作成・追記・訂正等の確定者が自明となる場合も考えられます。その場合、確定者が明確になるよう運用方法を定め、運用管理規程等に明記した上で、入力者が作成や追記・訂正・消去した内容について確定者が確定した旨の何らかの記録を残した形で運用を実施する必要があります。電子保存の対象となる情報の入力は、診療行為等の実施者が行うことが原則です。しかし、例えば外科手術時の経過をカルテに記録する際のように、本来の診療行為の実施者である執刀医による入力が物理的に不可能であるため、代行者が入力する場合も想定される。また、医師事務作業補助者が、医師の指示の下で電子カルテに入力をすることも考えられます。このように、診療行為等の実施者でない者が、その者に代わって入力を行う場合は、代行入力に関する規定の策定と、その実施に関して記録を残さなければなりません。

ここでは次の４つを要件として取り上げ、それぞれについての考え方を示します。

- 入力者及び確定者の識別と認証
- 記録の確定
- 識別情報の記録
- 更新履歴の保存

①　入力者及び確定者の識別・認証

真正性を確保する上で、何らアクセス権限を持たない者がシステムを利用することを排除し、自身の ID を持つ適正な入力者に利用を限定しなければなりません。よって、入力者の識別・認証は必須となります。また、入力者と確定者が異なる場合は、確定者の識別・認証も必要となります。

具体的な対策については、１４．認証・認可に関する安全管理措置の利用者の識別・認証に係る記述を参照してください。

代行入力を行う場合の留意点

医療機関等の運用上、代行入力を実施する場合には、必ず入力を実施する個人ごとに ID を発行し、その ID でシステムにアクセスしてください。また、日々の運用においても ID、パスワード等を他人に教えたり、他人の ID でシステムにアクセスしたりすることは、システムで保存される作業履歴から作業者が特定できなくなるため、禁止しなければなりません。

② 記録の確定

記録の確定は、当然、その記録の確定を実施できる権限を持つ確定者によって実施されなければなりません。多くの場合は、入力者にその権限があることが想定されるが、入力者にその権限がない場合は、権限を持つ確定者が記録の確定を実施する必要があります。

記録の確定は、確定された時点から真正性を確保して保存することを明確にするもので、いつ・誰によって入力され、また確定されたかを明確にして、その保存情報自体にはいかなる追記、変更及び消去も行われてないことを保証することを目的とします。なお、確定以降に追記、変更、消去の必要性が生じた場合は、その内容を確定済みの情報に関連付けた新たな記録として作成し、別途、確定保存しなければなりません。

手入力（スキャナやデジタルカメラ等の周辺機器からの情報取込操作を含む。）により記録が作成される場合は、入力者は過失による誤入力や混同のないことを確認する必要があります。また、それ以降の情報の追記、書換え及び消去等との区別を明確にするために、確定者により確定操作が行われなければなりません。

なお、明示的な確定操作が行われなくとも、最終入力から一定時間経過又は特定時刻通過により記録が確定されるとみなして運用される場合においては、入力者及び確定者を特定する方法とともに運用方法を定め、運用管理規程に明記する必要があります。

手入力以外に外部機器システムからの情報登録が行われる場合は、取込みや登録の時点で目的とする情報の精度や正確さが達成されていることを確認して、確定者による確定操作が行われる必要があります。

臨床検査システム、医用画像の撮影装置（モダリティ）やファイリングシステム（PACS）等の特定の装置又はシステムにより作成される記録では、当該装置からの出力結果を当該装置の管理者の責任において確定情報として扱い、運用される場合もあります。この場合、確定情報は、どの記録が・いつ・誰によって作成されたかが、システム機能と運用の組み合わせにより、明確になっている必要があります。

③ 識別情報の記録

確定された記録は、第三者から見て、いつ・誰が入力し、また確定したものであるかが明確になっている必要があります。入力者及び確定者の識別情報には、氏名及び作成された時刻を含むことが必要である。また、入力者及び確定者の識別情報が記録情報に関連付けられ、通常の手段では誤った関連付けができないこと、及びその関連付けの分離・変更又は改ざんができないことが保証されている必要があります。

識別情報は、入力者及び確定者が責任を持つ個別の行為ごとに、個々の患者の診療録等に対して記録又は記載されることを原則とします。初回の診療録等の作成時に入力者及び確定者の識別情報が必要であるが、確定の上で保存された後の追記、修正、削除等を行う場合も、該当する診療録等に対してその情報に係る入力者及び確定者の識別情報が必要です。

また、グループ診療のように、入力者が複数存在する場合でも、情報を入力する者は個々人であり、その複数の個人をそれぞれ入力者として記録する。かつ、その記録の確定は「②記録の確定」に従って実施しなければなりません。

④　更新履歴の保存

例えば、診療情報は診療の遂行に伴い増加し、その際、新たな知見を得たことにより、確定済みで保存してある記録に対して追記や修正を行うことが少なくないです。このような診療行為等に基づく記録の更新と、不正な記録の改ざんは容易に判別されなければなりません。そのためには記録の更新内容、更新日時を記録するとともに、権限に基づき更新内容の確定を行った確定者の識別情報を関連付けて保存し、それらの改ざんを防止でき、万一改ざんが起こった場合にもそれが検証可能な環境で保存しなければなりません。

シス１４章第⑧条

シＱ－58　医療情報システムの認証において、真正性の確保を求める場合について、記載されている情報と確定者には具体的にどのような組み合わせがあるか。

Ａ　情報と確定者の組み合わせとしては下記のような例があります。

例 1）　医師が患者の診察時にカルテに所見を記述する。

情報　：所見

確定者　：実際に診察を行った医師

例 2）　看護師が医師の指示に基づく処置を行った際に、実施状況を看護記録に記述する。

情報　：処置実施記録

確定者　：実際に処置を行った看護師

例 3）　読影担当医が放射線画像の読影レポートを作成する。

情報　：読影レポート

確定者　：読影を行った放射線科医師

例 4）　検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。

情報　：検査結果

確定者　：バリデーションと取り込み操作を行った検査技師

例 5）　夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。

情報　：投薬指示

確定者　：実際にオーダを実施した当直医

シス１４章第⑧条ｆ

シＱ－59　「１４．認証・認可に関する安全管理措置」⑧ｆにおいて、「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」とあるが、具体的にどのような場合を指すか。

Ａ　例えば、在宅で治療を行っている患者の様態が急変した等、緊急で対応すべき事由が発生したため、確定操作を行う時間的余裕もなく、担当医が外出せざるを得なくなった等の事例が考えられます。

シス１４章第⑧条

シＱ－60　代行入力を行う場合、代行を許可した証拠はどのように残しておけばいいのか。

Ａ　代行入力を実施する場合には、必ず入力を実施する個人ごとに ID を発行し、代行入力を行う者はその ID でシステムにアクセスしなければなりません。その際、入力者のログ、あるいは作業報告等の台帳を作成し、記録を残す必要があります。

　また、誰の意思決定に基づいて代行入力を実施したかが説明できるように、上記の内容を含めた代行入力に関する運用管理規程等の策定が必要です。

シス１４章第⑧条

シＱ－61　記録を確定する方法として、①入力者が情報を入力画面を見ながら入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるが、それぞれどのように対応すべきか。

Ａ　確定操作は、文書の責任者が誰かを明らかにし、操作の時点で対象とする文書の記述に誤入力や改ざん等がないことを保証し、記載に対して責任を持つという意味合いがあります。そのため、上記①～③の対応について下記のように考えられます。

①　「入力者が情報を入力画面を見ながら入力し記録する場合」

　この場合には、確定するという操作を行うことで、内容を確定者が保証することになります。「確定者が」としたのは、文書の入力を確定者が自ら行う場合や代行入力による場合があるからです。いずれの場合も、運用管理規程等によって決められた確定者が確定したということになります。また、処理としては署名を施す等になります。

　代行入力の場合には、確定者が必ず確認を行った上で、確定を実施しなければなりません。

②　「外部機器等から確定されていない情報を取り込み記録する場合」

この場合には入力者が、記述の改ざんや誤入力等がないことを確認した上で、スキャナ等による読み込みを行い、誰の記録であるかを関連付けして、①の確定操作を行うことになります。

③　「外部システムで確定された情報を取り込み記録する場合」

改めて受け取り側で確定操作を行う必要はありませんが、外部システムで確定されていることを確認することが必要です。ただし、確定された情報しか取り込まれないようにシステムが構築されている場合、その限りではありません。

シス１４章第⑧条

シQ－62　画像の確定に当たっては明示的な確定操作が必要か。

Ａ　必ずしも必要ではありません。例えば、①PACS が受信した時点、②PACS で受信してから一定時間経過した時点、③PACS で受信してから一定時刻を過ぎた時点をもって確定とすること等が考えられます。これらについては、各医療機関等において、運用管理規程に明記することが必要です。

シス１４章、シス１２章

シQ－63　情報の重要度に応じでセキュリティ対策を講じたい場合どのように整理すべきか。

Ａ　情報の区分管理を実施し、区分単位でアクセス管理を実施してください。

15. 電子署名、タイムスタンプ

シス１５章第①条

シＱ－64　法令で定められた記名・押印のための電子署名における要件として暗号に関するものがあるが、具体的にはどのようなものを採用する必要があるか。

Ａ　ガイドラインにおいては、電子署名法における特定認証業務に係る電子署名等が要件を満たすものとして挙げられています。電子署名法における特定認証業務に係る電子署名の基準として、電子署名法施行規則第２条及び電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成十三年四月二十七日総務省・法務省・経済産業省告示第二号）第３条では、RSA 方式であって、ハッシュ関数として SHA-256 を使用するもの、SHA-384 を使用するもの又は SHA-512 を使用するもののうち、モジュラスとなる合成数が 2048bit 以上のもの、RSA-PSS 方式であって、SHA-256、SHA-384 又は SHA-512 を使用するもののうち、モジュラスとなる合成数が 2048bit 以上のもの、ECDSA 方式であって、ハッシュ関数として SHA-256 を使用するもの、SHA-384 を使用するもの又は SHA-512 を使用するもののうち、楕円曲線の定義体及び位数が 224bit 以上のもの、DSA 方式であって、ハッシュ関数として SHA-256 を使用するものであり、かつ、モジュラスとなる素数が 2048bit 以上のものが定められています。

シス１５章第①条

シＱ－65　共通鍵、秘密鍵を使用して情報を管理する場合どの程度のレベルのものが必要か。

Ａ　共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-2 レベル１相当以上の対応を図ってください。

16．紙媒体等で作成した医療情報の電子化

シス１６章第①条、同章第②条

シＱ－66　「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にある「また、スキャンにより、保存できない有用な情報」とは、どのようなものがあるか。

Ａ　現在のスキャナの機能は向上しており、高い解像度での読み取りや筆圧などを記録できるものもあります。一方、紙媒体においては、例えば、患者が疾患・症状から書面作成時に用紙をペン先で突き破ってしまったり、用紙の固定がうまくできず、不規則な折れ目（しわ）が付くこともあります。

　このような変化はスキャナで必ずしも正確に記録できないことがあるため、このような場合の記録を電子的に行う際は、スキャナで電子化するのではなく、適切に動画撮影をする方が正確な記録となる可能性があります。

　このようにスキャナで直接記録される文字情報等以外に、紙媒体の物理的な状態などの有用な情報があることについて、示したものです。

シス１６章第②条、企１６．２章

シＱ－67　診療録等をスキャナ等により電子化して保存する場合に、診療の用途に差し支えない精度の基準はあるか。

Ａ　画一的な基準はありません。手書き文書、ワープロ印刷文書、インスタント写真等、対象ごとに診断等の診療目的の利用に十分な精度を満たしていることをあらかじめ確認した上で、運用管理規程等で定めてください。

　なお、第３版までは 300dpi、RGB 各８ビット以上としていましたが、一般に販売されている汎用のスキャナでもこれ以上の性能を持つものが大多数を占めるために、記載を改めたものです。不用意に精度を下げることを推奨しているものではありません。

シス１６章第②条

シＱ－68　「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、保存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。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。

Ａ　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、電子化した情報はあくまでも参照情報です。

　緊急時とは、例えばシステムダウン等が想定できます。また、一般に「診療のために直ちに特定の診療情報が必要な場合」とは継続して診療を行っている場合であり、患者の診療情報が緊急に必要になることが予測されるときは、診療に差し支えない範囲で原本である紙媒体を閲覧可能な状態にしておくことが必要です。

18．外部からの攻撃に対する安全管理措置

シス１８省第①条

シQ－69　「１８．外部からの攻撃に対する安全管理措置」①の４つ目の「－」において、「重要なファイルは数世代バックアップを複数の方式で取得し、」とあるが、外部からの攻撃を受けた場合の復旧のための対応としては、どのような点を考慮して、バックアップを取得する必要があるか。

A　バックアップ取得のポリシーは、医療の社会的な影響度を鑑みて、医療機関等における診療業務の継続性を確保するため、できる限り診療に影響に及ぼさないよう、計画を立てることが求められます。この部分は一般企業におけるバックアップに対する考え方との大きな違いになります。

但し具体的なバックアップ取得の計画については、取扱うデータの利用頻度やシステムが停止した場合に復元すべき時点、システムの特性などを考慮して、総合的に決定されるため、一意に決まるわけではありません。

例えばバックアップの取得範囲として、通常、フルバックアップ、差分バックアップ、増分バックアップなどがあり、適切に組み合わせて、対応することになります。

そのうえでさらに具体的な例として、日次で差分バックアップ、週次でフルバックアップを行う場合、前々週以前のフルバックアップ及びその週以前の日時の差分バックアップは、ネットワークから切り離した記録媒体で保管すること（磁気テープ、DVD、Blu-Ray 等）あるいは論理的に書き込み禁止（磁気ディスク等）の状態にする等の対策が必要となります。

最近ではクラウドサービスを利用したバックアップを行うことも考えられます。例えば、原本データ以外にクラウド上でバックアップを取得する場合、バックアップデータを追記できない設定としたり、複数のバックアップデータを取得したりするなどの方式で、複数方式によるバックアップを行うことが想定されます。

また電子カルテ、医事システム、LIS、RIS（PACS 含む）等のサブシステムがそれぞれデータベースを持つ場合、それぞれについてシステム特性やデータの影響度を鑑みて、バックアップ取得の計画を策定することになります。

具体的な例としては、電子カルテ、LIS 等保存データがあまり大きくないサブシステムについては、日次でバックアップを確保し、電子カルテは５世代、その他のシステムは３世代保存するなどにより、前週までのデータを回復することが想定されます。この場合、ランサムウェア等の攻撃への対策という観点から、電子カルテで３世代以降のバックアップデータについては、ネットワーク的あるいは論理的に書き込み禁止属性とし、その他のシステムは３世代目をネットワーク的あるいは論理的に書き込み禁止とするなどが求められます。

一方、PACS を含む RIS のような大量のデータを扱う場合はバックアップそのものが困難な場合もありえます。この場合には、サイバーセキュリティを考慮すると、確定されたデータについては書き込み禁止に設定するべきです。そのうえで、運用上可能であれば、例えばキー画像の指定がされた画像データ等は電子カルテと同様の対策するなどにより、医療の継続性の確保において極めて有用な対応になると考えられます。

バックアップ計画の策定に際しては、利用する医療情報システムやサービスを提供する事業者からの情報提供等を踏まえて検討することが重要です。例えば「「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド」[6]では、「医療機関等には、情報を保存する場所や、その場所ごとの保存可能容量、リスク、レスポンス、バックアップ頻度、バックアップ方法等を運用管理規程にまとめ、関係者に周知することが求められます。」（P24）とし、事業者によるバックアップに関する情報提供の有無が確認できることとなっています。事業者から情報提供されている場合には、その内容などを参考に、計画の策定を行うことが考えられます。また医療機関等が自らシステム構築を行う場合には、「非機能要求グレード 2018」（独立行政法人情報処理推進機構）などを参考に、バックアップ計画を策定するなども一案です。

なお別冊「[特集] 医療機関等におけるサイバーセキュリティ」も併せてご活用ください。

[6] 一般社団法人保健医療福祉情報システム工業会、一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会

令和５年５月

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　**用語集**

用語		説明	概 O	経 G	企 M	シ C
あ	アプリケーション（アプリ）	コンピュータの OS 上で動作するソフトウェアのこと。ファイル管理やネットワーク管理、ハードウェア管理、ユーザー管理といった基本的な機能を持つ OS に対して、ワープロソフトや表計算ソフトといったソフトウェアのことをアプリケーションと呼ぶ。スマートフォンの場合は、ゲームを初め、辞書機能や動画再生、文書作成等、様々な目的に応じたアプリケーションがあり、「アプリ」と略されて使われる場合もある。			○	○
あ	暗号アルゴリズム	暗号化の手順のこと。主な暗号アルゴリズムは、鍵の扱い方によって共通鍵暗号方式（暗号化と復号とで共通の鍵を使用する方式）と公開鍵暗号方式（暗号化と復号とで別々の鍵を使用する方式）の二つに大別される。			○	
あ	暗号化	データを見てもその内容が分からないように定められた処理手順でデータを変えること。また、暗号化されたデータは、復号という処理によって元のデータに戻すことができる。			○	○
あ	安全管理措置	医療情報を安全に管理する（例えば、医療情報の漏えい、滅失又は毀損を防止する）ために必要かつ適切な内容で、講ずるべきこととされている措置。 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。）により、これを講ずることが法的な責務として求められている。	○	○	○	○
い	委託	医療機関等が外部の事業者との間で業務委託契約（契約の形態・種類は問わない）を締結し、外部の事業者に医療情報の取り扱いや、医療情報を取り扱う情報システム・サービスの管理・運用を行わせること。	○	○	○	○
い	医療情報	医療に関する患者情報（個人識別情報）を含む情報。 具体的には、	○	○	○	○

用語		説明	概 O	経 G	企 M	シ C
		①「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。）に含まれている文書 ②施行通知には含まれていないものの、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。）の対象範囲で、かつ、患者の医療情報が含まれている文書等（麻薬帳簿等） ③法定保存年限を経過した文書等 ④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像 ⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等が対象となる。				
い	医療情報システム	医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステム。 例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定される。また、患者情報の通信が行われる院内・院外ネットワークも含む。	○	○	○	○
い	医療情報連携ネットワーク	情報通信技術（ICT）を活用して関係医療機関等の間で効率的に患者の医療情報を共有することを目的とした、患者の同意のもと、医療機関等の間で、診療上必要な医療情報（患者の基本情報、処方データ、検査データ、画像データ等）を電子的に共有・閲覧できることを可能とする仕組みのこと。	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
い	インタフェース	コンピュータ等と他のコンピュータ・周辺機器等を接続するための規格や仕様。				○
い	インフォームド・コンセント	医療の場合では、医療行為を受ける前に、医師および看護師から医療行為について、わかりやすく十分な説明を受け、それに対して患者さんは疑問があれば解消し、内容について十分納得した上で、その医療行為に同意すること。すべての医療行為について必要な手続き。もともとは米国で生まれた言葉で、「十分な説明と同意」と訳される場合もある。	○			
う	ウイルススキャン	コンピュータがウイルスに感染していないかどうかを検査すること。 一般のウイルス対策ソフトは、通常の動作では、電子メールやファイルのコピー等で送受信されるデータについて、ウイルス感染を調査するようになっている。そのため、既にコンピュータに感染してしまったウイルスを検出するには、ウイルススキャンを実行する必要がある。				○
う	ウェアラブル端末	腕や頭部等の身体に装着して利用する ICT 端末のこと。				○
お	オンプレミス型	医療機関等自身が保有・管理する機材にソフトウェアを配備し、データを保管する形で情報システムを利用する形態のこと。 「クラウドサービス型」と対比されて用いられることが多い用語である。	○		○	○
か	仮想デスクトップ	サーバやパソコン等で複数の OS を動かし、ネットワーク経由で個々のデスクトップ端末へ割り当てて通常のデスクトップパソコン同様の機能を実現する技術のこと。端末側には、記憶装置を持たない「シンクライアント」を使うことが多い。ネットワークにさえ繋がっていれば、利用する環境の違いに関係なく同じ作業環境を提供できる。				○
か	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○	○	○
か	監視装置	ネットワークの処理能力低下や障害の発生を定期的または常時監視する機器や				○

用語		説明	概 O	経 G	企 M	シ C
		システム。				
か	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity)。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○		
き	機微性	個人の生命・身体・健康等に関わる情報をはじめとした、漏えいすることによって深刻なプライバシー侵害につながる危険性がある情報の特性。	○	○		
き	基本４情報	氏名、生年月日、性別、住所を指す。			○	
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality)。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○	○	○
き	脅威	情報の盗難や不正利用など、情報セキュリティリスクを発生、または、顕在化させる要因のことを指す。 脅威は、人に起因するものと作業環境に起因するものの２つに大別され、人に起因するものは、意図的脅威と偶発的脅威に分類される。 意図的脅威としては、標的型攻撃やマルウェア感染、Web サイトの改ざんなど、外部の人間による悪意ある行為や機密データを持ち出し、悪用するといった内部不正などが該当します。	○			
き	共通鍵	暗号化と復号に同じ暗号鍵を用いる暗号方式である共通鍵暗号方式において、暗号文の送信者と受信者の間で共有する暗号鍵。				○
く	クライアント	ネットワーク上で情報やサービスを利用するコンピュータのこと。 通常は、一般利用者が使用するコンピュータがクライアントになる。なお、クライアントが要求した情報やサービスを提供するコンピュータは、サーバと呼ばれる。		○		○
く	クラウドサービス型	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービ	○	○		○

用語		説明	概 O	経 G	企 M	シ C
		スであって、情報セキュリティに関する十分な条件設定の余地があるもの。提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及びSaaS（Software as a Service）に分かれる。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。 「オンプレミス型」と対比されて用いられることが多い用語である。				
く	クラッカー	コンピュータネットワークに不正に侵入するなど、破壊・改竄などの悪意を持った行為を行う者。				○
く	クリアスクリーン	情報セキュリティに関する対策の一つで、自席のコンピュータを意図せず第三者に操作されたり画面を盗み見されたりしないことを求めるもの。				○
こ	公衆無線 LAN	駅や街中等、公共の場所で利用できるように設定された無線 LAN の施設やサービスのこと。				○
こ	公的個人認証サービス（JPKI）	インターネット上での行政手続等に際して本人確認を行う場合に必要となる電子証明書を個人・法人が利用できるサービス。地方公共団体情報システム機構（J-LIS）が提供している。 作成・送信した電子文書が、利用者本人が作成した真正なものであり、利用者が送信したものであることを証明する署名用電子証明書と、インターネットサイト等にログインした者が利用者本人であることを証明する利用者証明用電子証明書の 2 種類の電子証明書をマイナンバーカードに搭載することでサービス提供がなされている。			○	
こ	互換性	部品や構成要素を置き換えても、従来通り使用できる性能を互換性という。IT分野では、特に、特定の製品向けのハードウェアやソフトウェア等を他のものに置き換えても利用できることをいう。			○	○
こ	コンピュータウイルス	他のコンピュータに勝手に入り込んで、意図的に何らかの被害を及ぼすように				○

用語		説明	概 O	経 G	企 M	シ C
		作られたプログラムのこと。ディスクに保存されているファイルを破壊したり、個人情報等を盗むこともある。また、感染経路として、ウイルスは、インターネットからダウンロードしたファイルや、他人から借りた CD メディアや、USB メモリ、電子メールの添付ファイル、ホームページの閲覧等を媒介して感染する。ウイルスにはウイルス対策ソフトでは検出・駆除できないものもあり、ウイルスに感染したことに気付かずにコンピュータを使用し続けるとウイルス自身が自分を複製する仕組みを持っていた場合には、他のコンピュータにウイルスを感染させてしまう危険性もある。				
さ	サーバ	ネットワーク上で情報やサービスを提供するコンピュータのこと。サーバに対して、情報やサービスを要求するコンピュータをクライアントという。		○	○	○
さ	サイバー攻撃	コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。	○			
し	死活監視／死活管理	機器やシステム、ソフトウェアなどの対象が動作しているかどうか外部から定期的・継続的に調べること。特に、専用の装置やソフトウェアなどによって自動的に調べ続けること。				○
し	実在性	対象の個人・組織等が間違いなく実在していること。			○	
し	証跡	情報システムが行った処理内容や処理対象、処理過程のデータ、利用者が行った操作などを時系列にそのまま電子的に記録したデータのこと。 「証跡管理」とは、不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争の発生時における原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称を指す。		○	○	○
し	冗長化	システムの構成要素や機能の実現手段を複数用意することにより、一部に故障が発生しても上位系の障害に至らないよう配慮した設計を行うこと。			○	○

用語		説明	概 O	経 G	企 M	シ C
し	情報セキュリティインシデント	望まない又は予期しない、単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。		○	○	○
し	情報セキュリティ監査	情報システムについて、セキュリティ対策を正しく実施し、機能させることができているかを実際に検証・評価することで、組織が保有する情報資産を守るために正しく対策がとれているかを第三者の目線で確認すること。 組織内で監査人を立てる内部監査、組織外から監査人を呼ぶ外部監査の二通りの実施方法がある。		○		
し	情報セキュリティマネジメントシステム	個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。	○	○	○	
し	証明書ポリシー（CP：Certificate Policy）	証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるもの。			○	
す	スマートフォン	従来の携帯電話に比べてパソコンに近い性質を持った情報機器。大きな画面でパソコン向けの Web サイトや動画を閲覧できたり、アプリケーションを追加することによって機能を自由に追加したりすることができる。また、タッチパネルを使い、画面の拡大やスクロールなど直感的な操作が可能。				○
せ	脆弱性	コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生したサイバーセキュリティ上の欠陥のこと。セキュリティ・ホール（security hole）と呼ばれることもある。 セキュリティ上の設定に不備がある状態を指して、脆弱性があるといわれることもある。		○	○	○
せ	政府情報システムのためのセキュリティ評価制度（ISMAP）	政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とし			○	

用語		説明	概 O	経 G	企 M	シ C
		た制度。				
せ	責任分界	協働や提携、委託等する関係者間でそれぞれの責任の範囲を明確にして分けること。責任を分けて、責任の移行する点のことを責任分界点という。	○	○	○	○
せ	セキュリティ・デバイス	IC カード、USB キー等の認証用の個人識別情報を格納するデバイス。				○
せ	セキュリティ・パッチ	セキュリティ上の脆弱性・機能的不適合等を解消するためのプログラム。単に「パッチ」ともいう。				○
せ	セッション	コンピュータシステムやネットワーク通信において、接続/ログインしてから、切断/ログオフするまでの、一連の操作や通信のこと。				○
せ	セッション乗っ取り	ホームページの閲覧等、パソコンと Web サーバとの間で通信を行っている際に、その通信を利用者以外の者が乗っ取る攻撃のこと。通信が乗っ取られると、本来の利用者になり代わって通信が行われてしまう。「セッションハイジャック」と呼ばれることもある。				○
そ	ソフトウェア	コンピュータを構成する電子回路や装置などの物理的実体を指す「ハードウェア」と対比して、それ自体は形を持たないプログラムや付随するデータなどを指す言葉。 ソフトウェアは、コンピュータの中でファイル管理やネットワーク管理、ハードウェア管理、ユーザー管理といった基本的な機能を持つ OS と、その OS の上で動作する、ワープロソフトや表計算ソフト等に代表されるアプリケーションの 2 種類に大別される。	○	○	○	○
た	タイムスタンプ	電子文書がタイムスタンプが付与された時点で存在することを証明する技術。作成された電子文書がその時点で存在したことだけではなく、その時点からいかなる人にも改ざんされていないことを証明するもの。		○	○	○
た	台帳管理	情報機器等（医療情報システムにおいて利用する物理的な資産、サービス、ライセンス等）や ID・パスワード、医療情報そのものといった、医療機関等におい			○	○

用語		説明	概 O	経 G	企 M	シ C
		て管理する情報資産を洗い出した上で、保存先や利用者範囲、保存期限等を台帳に記録して管理する方法のこと。				
た	立会人型電子署名	利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス。			○	
た	タブレット PC	薄い板状（タブレット）の本体に、タッチして操作が可能な液晶画面が組み込まれたパソコン。				○
ち	チャネル・セキュリティ	ネットワーク回線を通って情報が伝送される途中で情報が盗み見られることのないよう、ネットワーク回線の経路を暗号化する等の措置をとること。				○
て	データ形式	プログラム上でデータを保存する形式をいう。また、補助記憶にデータを保存する形式、転送でデータを送る形式等を指す場合を含む。ファイルとして保存する場合はファイル形式という。代表的なものとして CSV 等が挙げられる。				○
て	データセンタ	サーバやネットワーク機器などの IT 機器を設置、運用する施設・建物の総称。			○	
て	データベース	複数の主体で情報を共有若しくは利用し、又は用途に応じ加工、再利用ができるように、一定の法則に基づき、作成、管理されたデータの集合をいう。				○
て	電子証明書	暗号化やデジタル署名に用いる公開鍵暗号の公開鍵が配送される際に添付され、受信者が鍵の所有者を確認するために利用する一連のデータセットのこと。信頼できる第三者（認証局）によって、間違いなく所有者本人であることを電子的に証明するために発行される。			○	○
て	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。	○	○	○	○
と	統制	一般的には、多くの物事を一つにまとめておさめることや国家などが一定の計画や方針に従って指導・制限することを指す。 情報セキュリティにおける統制としては、内部統制や情報セキュリティガバナンスとして用いられ、情報資産に係るリスクの管理を狙いとして、情報セキュリ	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
		ティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築・運用することを指す。 （参照）経済産業省「情報セキュリティガバナンスの概念・定義」 https://www.meti.go.jp/policy/netsecurity/secgov-concept.html				
と	トラフィック	通信回線やネットワーク上で送受信される信号やデータ、およびその量や密度のこと。				○
に	二要素認証	情報システムの利用者を認証する方式のうち、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように、認証の 3 要素である「記憶」、「生体情報」、「物理媒体」のうち、2 つの独立した要素を組み合わせて認証を行う方式のこと。				○
ね	ネットワーク機器	ルータ、スイッチ、HUB 等の情報通信ネットワークを構築する際に用いられる機器。				○
は	パーソナルファイアウォール	個人向けファイアウォール製品。				○
は	パターンファイル	ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。 ウイルスは日々新しいものが出現しているため、最新のウイルスに対応するためには、パターンファイルを常に最新のものに更新しておく必要がある。 ウイルス対策ソフトによっては、「ウイルス定義ファイル」や「ウイルス検知用データ」、「シグネチャ」等と呼び名が異なる。				○
は	バックドア	外部からコンピュータに侵入しやすいように、“裏口”を開ける行為、またはそれを実現するプログラムのこと。このプログラムが実行されると、攻撃者によってインターネットを通じてコンピュータを遠隔操作されてしまう可能性がある。 一部のウイルスでは、感染時にバックドアを埋め込むことがある。				○
は	パブリッククラウド	情報システムのインフラをサービスとして遠隔から利用できるようにしたクラウドコンピューティング環境のうち、インターネットを通じて事業者から一般				○

用語		説明	概 O	経 G	企 M	シ C
		の法人や個人に広く提供されているもの。Web サービス運営などによく用いられる。 限られた環境からのみアクセス可能なクラウドコンピューティング環境である「プライベートクラウド」と対をなす言葉である。				
ひ	秘密鍵	公開鍵暗号で使用される一対の暗号鍵の組のうち、相手方に渡したり、一般に公開したりせず、所有者が管理下に置いて秘匿する必要がある鍵。公開鍵暗号では一対の対応関係にある暗号鍵のペアを用い、公開鍵で暗号化した暗号文は秘密鍵でしか復号できないという仕組みになっている。			○	
ひ	標準時刻	国立研究開発法人情報通信研究機構の原子時計で生成・供給される協定世界時（UTC）をベースに定められた時刻。日本国内では、英国の標準時であるグリニッジ標準時（GMT）に対して 9 時間を加えた日本標準時（JST）が用いられる。				○
ふ	ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器。 ファイアウォールには防火壁の意味があり、火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。				○
ふ	ファームウェア	ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。パソコンや周辺機器、家電製品等に搭載されており、機器に内蔵された ROM やフラッシュメモリに記憶されている。			○	○
ふ	フェイルセーフ	システムが故障した場合において、安全性が確保された状態で機能を停止させることで、被害を最小限に留めることを目指す考え方のこと。			○	
ふ	不可逆変換	ある文字列を他の文字列に変換する方法の一つで、変換後の文字列を使って変換前の文字列を特定することができないように変換する方法のこと。				○
ふ	不正アクセス	利用する権限を与えられていないコンピュータに対して、不正に接続しようと	○		○	○

用語		説明	概 O	経 G	企 M	シ C
		すること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。				
ふ	不正ソフトウェア	利用者の予期していない不利益をもたらす不正な活動を実行する、悪意を持ったソフトウェアのこと。マルウェアとも呼ばれる。 コンピュータウイルス、ワーム等、様々な形態がある。		○	○	○
ふ	振る舞い検知	ウイルス対策の方法の一つで、検査対象のプログラムを仮想環境で実行したり、実際の環境で監視したりするなどして、不審な挙動が行われていないかを確認し、それによってウイルスかどうか判断する方法。				○
ふ	プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順等の国際標準規則のこと。通信プロトコルとも呼ばれる。				○
ほ	ポート	外部とデータを入出力するための、ソフトウェアやハードウェアの末端部分（インタフェース）のこと。多くのパソコンは、周辺機器を接続するインタフェースとしての USB ポート、LAN ポート等を備えている。				○
ほ	保健医療福祉分野 PKI（HPKI）	「保健医療福祉分野の公開鍵基盤（Healthcare Public Key Infrastructure）」の略。医療現場において、本人確認だけでなく、公的資格の確認機能を有する電子署名や電子認証を行うための基盤。基盤の設置要件等は厚生労働省において策定されている。 現在は日本医師会、日本薬剤師会、医療情報システム開発センターにおいて、医師等の資格確認を行うための HPKI カードを発行している。			○	
ほ	本人性	申請等が行われる場面において、当該申請等の内容が、間違いなく当該申請等の対象者本人が作成した真正なものであること。			○	
ま	マイナンバーカード	マイナンバー制度導入により、平成 28 年 1 月から交付が開始された IC カードで、基本 4 情報と顔写真、電子証明書機能等が付されている。本人の申請に			○	

用語		説明	概 O	経 G	企 M	シ C
		より交付され、個人番号を証明する書類や本人確認の際の公的な本人確認書類として利用できる。				
ま	マクロ	アプリケーションソフトの操作を自動化する機能の一つで、利用者が関連する複数の操作や手順、命令を一連の手続きとして記録し、必要に応じて簡単な操作で繰り返し呼び出して実行することができる機能。表計算ソフトでよく利用される。				○
ま	マスターデータベース	情報システムにおいて、複数のデータベースで共通で用いられる情報群。医療分野では、医薬品や病名等に関するマスターが厚生労働省標準規格として、広く用いられている。				○
ま	マルウェア	「不正ソフトウェア」参照				○
む	無害化	無害化とは、攻撃者からの悪意のあるファイルの送付やファイル・データ等の利用に対して、利用者の PC 等の利用環境にマルウェア等が混入しないように行われる対策。これにより送付された悪意のあるマクロやコード等を削除し、送付先のシステム等の障害や情報漏えいを防止することが期待される。				○
む	無線 LAN	ケーブル線の代わりに無線通信を利用してデータ送受信を行う LAN システム。				○
ら	ランサムウェア	感染することにより PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正ソフトウェアをいう。				○
り	リスク	医療の場合でのリスクとは、健康や生命に被害や悪影響、危険を与える可能性のことを指す。 情報セキュリティにおけるリスクは、情報セキュリティを損ねる要因のことを指し、脅威と脆弱性の要素で構成される。 （参照）日本ネットワークセキュリティ協会（JNSA） https://www.jnsa.org/ikusei/01/02-03.html	○	○	○	○

用語		説明	概 O	経 G	企 M	シ C
り	リスクアセスメント	現実に自組織が持つ情報資産（経営情報や預かり情報と、それを扱う情報システムや、紙を含む記録媒体）について、どのようなリスクが存在するのか、調査して洗い出し、そのインパクトを評価して、対応を決める必要があり、この一連の作業をリスクアセスメントという。 （参照）日本ネットワークセキュリティ協会（JNSA） https://www.jnsa.org/ikusei/01/02-04.html				○
り	リモート署名	クラウド上のサーバに利用者自身の署名鍵を格納し、利用者が当該サーバにリモートでログインした上で行う電子署名。			○	
り	リモートログイン	遠隔地から公衆回線網やインターネット等を利用して施設内のネットワークシステム（LAN）に接続し、ネットワーク上の情報資源を活用すること。				○
る	ルータ	ネットワーク上を流れるデータを他のネットワークに中継する機器。				○
ろ	ローカル署名	IC カードやパソコン等の媒体に格納された、本人が管理する鍵で署名するもの。			○	
わ	ワーム	ネットワークを通じてほかのコンピュータに拡散することを目的としたマルウェアのこと。他のファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行う。				○
わ	ワンタイムパスワード	接続する度に入力するパスワードが毎回変わり、一度使用されたパスワードは次回からは使用できないような方式のこと。実装にあたっては専用プログラムやハードウェアを利用するため、パスワードの盗み見等に対するリスクも軽減できる。				○
A	ANY 接続拒否	無線 LAN アクセスポイントの設定において ESSID が「ANY」や空欄の設定になっている無線 LAN クライアントを拒否する対策のこと。この対策により、不特定多数の無線 LAN 端末からの接続を防ぐことが可能となる。				○
A	ASP	「Application Service Provider」の略。ネットワークを通じて、アプリケーショ				○

用語		説明	概 O	経 G	企 M	シ C
		ン・ソフトウェア及びそれに付随するサービスを利用させることを指す。SaaS（Software as a Service）もほとんど同様であるため、「ASP・SaaS」と連ねて呼称する。				
B	BCP	「Business Continuity Plan」の略。災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関等の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。 このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（Business Continuity Plan）と呼ぶ。		○		
B	BYOD	「Bring Your Own Device」の略。個人の所有する、あるいは個人の管理下にある端末の業務利用。			○	○
C	CISO	「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す。			○	
C	CSIRT	「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。		○	○	
E	EDR	「Endpoint Detection and Response」の略。情報システムのネットワーク末端（エンドポイント）の端末に導入し、そこに存在する脅威を監視・検知することで、インシデント対応等を支援するセキュリティ対策システム・対策手法のこと。				○
H	HTTPS	「HTTP Security」の略。インターネット接続における情報通信プロトコル（HTTP：Hyper Text Transfer Protocol）に、TLS 技術による暗号化プロトコ				○

用語		説明	概 O	経 G	企 M	シ C
		ルを付加した通信プロトコル。				
I	IaaS	「Infrastructure as a Service」の略。CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
I	IDS	「Intrusion Detection System」の略。不正な攻撃を検知するシステム。ネットワークやサーバを監視し、不正なアクセスを検知する役割を担う。ファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組みであり、不正な通信を検知した場合、管理者に通知する機能を提供する。				○
I	IKE	「Internet Key Exchange」の略。ネットワーク上の機器や端末間で暗号鍵の交換及び管理を行うためのプロトコル。				○
I	Internet-VPN	「Internet-Virtual Private Network」の略。各事業所の LAN をインターネット経由で接続しながら、VPN 技術を使うことで盗聴や改ざんを未然に防止し、インターネット経由でも安全に情報を伝送することができる技術。インターネット VPN を提供するための選択肢としては、IPsec、SSL-VPN が代表的である。				○
I	IoT 機器	IoT は「Internet of Things」の略。物理的または仮想的なモノに通信機能を持たせ、インターネットに接続したり相互に通信したりすることにより、自動認識や自動制御、遠隔計測等の高度なサービスを実現するために配置する機器。				○
I	IPS	「Intrusion Prevention System」の略。不正な攻撃を遮断するシステム。不正な通信を検知した場合,管理者への通知に加え、その通信を遮断する機能を提供する。				○
I	IPsec	IP レイヤー（ネットワーク層）において暗号に基づくセキュリティサービスを提供する機能。インターネット規格の RFC 4301 で規定されている。				○
I	IP-VPN	「IP-Virtual Private Network」の略。電気通信事業者の閉域 IP 通信網を経由して構築された仮想私設通信網。IP-VPN を利用することにより、遠隔地のネット				○

用語		説明	概 O	経 G	企 M	シ C
		ワーク同士を LAN 同様に運用することが可能になる。				
I	IP アドレス	インターネット等の TCP/IP 環境に接続されているネットワーク関連機器の識別番号。				○
I	ISMS	「Information Security Management System」の略。「情報セキュリティマネジメントシステム」参照	○	○	○	
K	Kerberos	利用者のコンピュータ（クライアント）からネットワークを通じてサーバにアクセスする際に利用者の認証を行う方式の一つで、パスワードから一定の手順により生成した暗号鍵により、クライアントとサーバ間の通信経路を暗号化することで、認証情報を安全に送受信する仕組み。 複数のサーバにアクセスする際、共通に認証情報を利用することができる利点もある。				○
L	LAN	「Local Area Network」の略。企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。				○
M	MAC アドレス	「Media Access Control アドレス」の略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、全く同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。				○
M	MDM	「Mobile Device Management」の略。組織内の従業者に支給する携帯情報端末のシステム設定等を統合的・効率的に管理する手法、あるいはそれを実現するシステム。 利用できる機能、導入できるソフトウェアやデータに制限を加えたり、端末の紛失時に遠隔制御によってデータの消去や操作のロックを行ったりすることが可				○

用語		説明	概 O	経 G	企 M	シ C
		能となるものもある。				
N	Nonrepudiation（否認防止）	送信元（あるいは受信者）が、あとになってその送信事実（受信事実）またはその内容を否定する主張をすることができないように証拠を残すこと。			○	
O	OS	「Operating System」の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。例えば、メモリやディスク等のハードウェアの制御、キーボードやマウスといったユーザーインタフェースの処理、画面への表示とウィンドウの制御等、コンピュータが動作するための数多くの基本処理を行う。さらに、コンピュータシステムを管理するための数多くのツールが用意されている。				○
P	PaaS	「Platform as a Service」の略。オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
P	PKI	「Public Key Infrastructure」の略。信用の起点となる最上位の認証局（ルート認証局）が自らの秘密鍵で署名した電子証明書に基づいて、他の認証局が提供する公開鍵を利用する形で、インターネットによる通信のみによって公開鍵暗号とデジタル署名サービスが運用される仕組みのこと。			○	○
R	REST-API	「Representational State Transfer Application Programming Interface」の略。Web システムを外部から利用するためのプログラムの呼び出し規約（API）の種類の一つで、「REST」（レスト）と呼ばれる設計原則に従って策定されたもの。				○
S	SaaS	「Software as a Service」の略。ソフトウェアをインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
S	SLA	「Service Level Agreement」の略。書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書（JIS Q 20000-1:2020）。	○		○	○

用語		説明	概 O	経 G	企 M	シ C
S	SSL-VPN	「Secure Socket Layer-Virtual Private Network」の略。リモートアクセスでの通信経路上を TLS（SSL の後継技術）で保護する技術。IPsec を用いた VPN のような特定端末間だけで VPN を構成する、いわゆる拠点間 VPN とは異なる。				○
T	TLS	「Transport Layer Security」の略。インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルのこと。利用者は、認証機関により発行されたサーバ証明書によって、サーバの真正性を確認する。				○
V	VPN	「Virtual Private Network」の略。公衆回線網等の上に仮想的に構築された閉域網（イントラネットのように外部に対して非公開であるネットワーク。				○
W	WPA2-AES、WPA2-TKIP	WPA2 は、無線 LAN 上で通信を暗号化して保護するための技術規格である WPA（Wi-Fi Protected Access）のセキュリティを向上させた技術規格であり、そのうち WPA2-AES は、共通鍵暗号方式として AES と呼ばれるアルゴリズムを用いた CCMP と呼ばれる暗号化方式を、WPA2-TKIP は、共通鍵暗号方式として RC4 と呼ばれるアルゴリズムを用いた TKIP と呼ばれる暗号化方式を、それぞれ採用している。				○

［特集］小規模医療機関等向けガイダンス

目次

１．はじめに ..... - 1 -

２．医療情報システムの安全管理 ..... - 1 -

２．１　小規模医療機関等における安全管理 ..... - 2 -

２．２　小規模医療機関等における安全管理ガイドライン ..... - 2 -

３．安全管理ガイドラインに基づく留意点 ..... - 3 -

３．１　安全管理に関する責任・責務 ..... - 3 -

３．１．１　法令上の遵守事項や義務 ..... - 3 -

３．１．２　通常時や非常時における説明責任や管理責任 ..... - 5 -

３．１．３　委託における責任 ..... - 6 -

３．１．４　第三者提供における責任 ..... - 6 -

３．２　リスク評価を踏まえた管理 ..... - 6 -

３．２．１　リスク分析・評価 ..... - 7 -

３．２．２　リスク管理 ..... - 7 -

３．３　安全管理全般（統制、設計、管理等） ..... - 7 -

３．３．１　統制（Governance） ..... - 7 -

３．３．２　設計 ..... - 8 -

３．３．３　管理（Management） ..... - 9 -

３．３．４　情報セキュリティインシデントへの対策と対応 ..... - 9 -

３．４　安全管理に必要な対策全般 ..... - 10 -

３．５　医療情報システム・サービス事業者との協働 ..... - 10 -

３．５．１　事業者選定 ..... - 10 -

３．５．２　事業者管理 ..... - 10 -

３．５．３　責任分界管理 ..... - 11 -

医療情報システム・サービス事業者との協働事項 ..... - 12 -

１．はじめに

オンライン資格確認が医療機関等に導入される中で、医療情報システムに関する安全管理や情報セキュリティ対策は、今日、すべての医療機関等において必須の事項となっています。また、サイバー攻撃は巧妙化が進み、適切な対策を講じることが求められています。

一方で、具体的な安全管理対策は導入している医療情報システムの特性により異なります。例えば電子カルテをはじめとした多数の医療情報システムを医療情報システム・サービス事業者（以下「システム関連事業者」という。）に依頼して導入し、その運用を医療機関等のシステム運用担当者が自ら行っている場合と、主だった医療情報システムとしては電子カルテや医事会計システムほどで、かつ、医療機関等内にシステムのサーバ等主要な機器を設置するオンプレミス型とは異なり、システム利用者が使用する端末のみ医療機関等に設置、もしくは利用者自身の PC 等を利用し、システムは医療機関等の外部クラウドサービス上で稼働しており、サービスを利用しているクラウド型で、情報技術やシステム運用に関する知見のある担当者も特に登用しておらず、基本的にシステム関連事業者にシステムの導入や保守等の管理のかなりの部分を委ねている場合とでは、具体的な安全管理対策の内容は異なります。

特に、診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する職員が不在で、医療機関等の経営層（院長や事務長等）が、医療情報システムの安全管理に関する企画管理を兼任することも多くみられます。このような医療機関等では、「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）のすべてを詳細に理解し、自施設に関係する事項を選出して対策を講じることは難しく、システム関連事業者から多くの支援を受けながら安全管理対策を講じることも多いです。

本ガイダンスでは、このような観点から、小規模医療機関等において、安全管理ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示すことを目的とします。

２．医療情報システムの安全管理

医療情報システムは、医療機関等において、患者に対する診療行為をはじめとする各種医療行為を円滑かつ効率的に行うために利用されるため、

・医療情報システムで保管する医療情報（患者に関する診療情報等）を適切に管理すること

・医療機関等の診療業務等に支障が生じないようにすること

・医療情報の取扱いや医療情報システムの管理に関係する各種法令等を遵守すること

などが医療情報システムの安全管理として求められます。

具体的に実施される安全管理対策として、適切な管理を実施するための組織運営やシステム運用に関する観点から医療機関等に課せられた責任を果たすために必要となる対策と、情報システムに関する技術的な観点に基づき、管理責任を適切に果たすために実装される技術的な対策が主に考えられます。

２．１　小規模医療機関等における安全管理

小規模医療機関等では、院長や事務長等の特定の職員が安全管理ガイドラインの各編で想定する役割のすべてまたは大半を担うことも少なくありません。この場合には、例えば組織図のようなものを作成する意義は低く、むしろ属人的な管理に関するリスクへの対策（緊急時に代理的に執行する体制を用意するなど）の方が重要となります。

管理責任を適切に果たすために求められる技術的な対策は、専門的な知見を有する者に委ねざるを得ないと厳しい状況であることが多いが、専門的な知見を有する外部のシステム関連事業者に安全管理ガイドラインを踏まえた対策を委ね、適切に当該事業者との関係を管理する方が、契約書類等によりサービス内容が技術的対策に関して具体的に安全管理対策の内容を把握でき、結果的に効果的な対策を講ずることが可能となることが期待されます。

２．２　小規模医療機関等における安全管理ガイドライン

安全管理ガイドラインに示す安全管理対策は、「概説編　３．２　医療機関等の特性に応じた読み方」にまとめているとおり、医療情報システムが稼働しているすべての医療機関等を対象としており、病床数や職員数、情報システム関連機器数などの医療機関等の規模ではなく、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に応じて、参照パターンを例示しています。

なお、医療情報の取扱いや医療情報システムの安全管理対策は、個々の医療機関等の実状に合わせて検討するものですが、医療機関等の規模等に応じて一律の組織運営やシステム運用、医療情報システム形態ではないことから、一概に規模別に分類して一律に安全管理対策を講じることは困難です。また、医療情報の機微性を考えると、保管する医療情報の多寡で、医療情報システムに関する安全管理対策の重要度合いや内容が変わるわけでもありません。

３．安全管理ガイドラインに基づく留意点

小規模医療機関等が、安全管理ガイドラインの「経営管理編」「企画管理編」「システム運用編」を通して、留意すべき事項の概要を以下に簡略的に示します。詳細は各編を参照してください。

３．１　安全管理に関する責任・責務

安全管理に関する責任・責務としては、

- 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

があります。

３．１．１　法令上の遵守事項や義務

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ます。（表１）

表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

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ます。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が求められています。

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ています。

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。）に従うことが求められ、施行通知第二の 2（3）に掲げる 3 条件を満たす必要があります。

（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ています。

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ます。

３．１．２　通常時や非常時における説明責任や管理責任

医療機関等には、通常時においては、説明責任や管理責任、定期的な見直し、必要に応じた改善を行う責任があり、医療情報システムの安全管理上、情報漏洩や情報システム障害等の望ましくない事象、いわゆる、情報セキュリティインシデントが生じた非常時においては、説明責任や善後策を講じる責任があります。

通常時の責任を果たすためには、以下の取組が重要です。

【説明責任】

医療情報システムの機能や運用を、必要に応じて患者等に説明ができるように、システム機能仕様やシステム運用手順等について、システム関連事業者の協力を得ながら文書化し、管理しておく。

【管理責任】

個人情報保護法第 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。」と規定されているとおり、医療機関等は、個人情報取扱事業者として、医療情報システムの管理実態や責任の所在を明確にする必要があり、システム関連事業者の協力を得ながら、システムの管理や運用が適切に行われているかどうかを監督する。

【定期的な見直し、必要に応じた改善を行う責任】

医療機関等で利用している医療情報システムを提供するシステム関連事業者の協力を得ながら、医療機関等として安全管理の改善に必要な情報を収集し、必要に応じて、文書化して管理しているシステム運用手順等を改善する。

また、非常時においては、以下の取組が重要となります。

【説明責任】

情報セキュリティインシデントの事態やその原因、影響、対応方針や対処方法等を、インシデントの事態に応じて、システム関連事業者の協力を得ながら、患者等への説明、ならびに、所管官庁への報告等を実施する。

【善後策を講じる責任】

情報セキュリティインシデントが生じた場合に、システム関連事業者や外部有識者の協力を得ながら、原因を究明し、再発防止策を講じる。

３．１．３　委託における責任

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。個人情報取扱事業者である医療機関等は委託先の事業者を監督する責任を負い、委託先のシステム関連事業者によ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ています。

利用する医療情報システム・サービスはじめネットワーク回線や情報機器設備など医療情報システムに関する導入や保守などについて、システム関連事業者などの委託先の事業者との間で締結する契約において、委託する内容や非常時も含めた役割分担、責任の所在を明確にして、委託先事業者との間で適切な協働体制を構築する必要があります。

双方の役割を分担し、責任の所在を明確にする、いわゆる責任分界には、

・法律上の責任の範囲を明確にする。

・具体的な運用及び対応の範囲を明確にする。

等の設定効果が期待されますので、システム関連事業者との間で認識の齟齬等が生じないよう、詳細に確認をし、書面等により可視化して、適切な契約等の取決めを実施することが重要です。

３．１．４　第三者提供における責任

医療機関等が外部の第三者に医療情報を提供する場合、医療機関等は、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」に留意し、安全に医療情報を提供する責任を負っています。

医療機関等は、医療情報を提供する先の第三者との間で、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が必要です。

３．２　リスク評価を踏まえた管理

医療機関等は、医療情報システムの安全管理対策を講じるために、リスク分析・評価を実施し、リスク管理方針（リスクの回避・低減・移転・受容）を決定することが必要です。

３．２．１　リスク分析・評価

リスク分析・評価、いわゆるリスクアセスメントを実施するには、専門的な知見などが求められることがあるため、医療情報システム・サービス事業者に対して、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』ガイド」で示されているチェックリスト等を参考に、資料や情報の提供を依頼し、協働してリスクアセスメントを実施するようシステム関連事業者へ相談することは有意義です。

なお、リスクアセスメントを行うに当たっては、下記の資料等が参考になります。

「中小企業の情報セキュリティ対策ガイドライン」（独立行政法人情報処理推進機構：IPA）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ならびに、上記の付録

「付録 3：5 分でできる！情報セキュリティ自社診断」

「付録 7：リスク分析シート」

３．２．２　リスク管理

リスク分析・評価を踏まえ、各リスクに対して「回避・低減・移転・受容」のいずれのリスク管理方針をとるか決定します。

リスク管理方針の検討を行う際には、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)」のバランスを考慮しながら、医療機関等に求められる医療の提供の維持・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などの判断が求められます。

リスク管理方針を決定し、リスク管理対策を講じるに際しては、医療情報システム・サービス事業者とも協議を行い、助言を求めるなどしながら、認識の齟齬等が生じないようにすることは重要です。

３．３　安全管理全般（統制、設計、管理等）

３．３．１　統制（Governance）

医療機関等での医療情報システムの安全管理において、安全管理に関する経営層の意識や方針が、組織全体にしっかり浸透し、これに基づいて適切に運用され、その状況や改善すべき課題を経営層が管理できるように、統制が効いている状態となっていることが重要です。

小規模医療機関等では、限られた人数と医療情報システム・サービス事業者で手分けをして、適切な安全管理に行うこともあるかと思われます。

そのため、統制の効いた体制づくりとして、個々の職員やシステム関連事業者の役割分担を明確にすることが求められます。例えば、

・医療情報システムが利用できる機器の施錠管理を誰が行うのか

・医療情報システムに異常が生じた場合に誰がどのような連絡体制で対応するのか

・職員の情報セキュリティなどに関する教育や訓練の担当は誰がどのように行うのか　等

役割を明確にし、遂行した上で、病院長など経営層が管理できるようにすることが求められます。

なお、技術的な対応などは、医療情報システム・サービス提供事業者に委ねることも考えられるため、体制づくりに際してこうした事業者も組み込むことは重要です。

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、医療情報システムの運営や利用をする場合、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、安全管理ガイドラインに加えて、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、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をして選定し、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必要で、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ます。

３．３．２　設計

リスク分析・評価、そして、リスク管理方針の決定を踏まえ、医療情報システムの安全管理に関する情報セキュリティ方針を定め、具体的な情報セキュリティ対策を整備・実装する、医療情報システムの安全管理における設計を行います。

情報セキュリティ対策の整備に当たっては、運用ルールを定め、規程類を整備しますが、適宜、自医療機関等と同規模、同様の医療サービス提供形態、同じ医療情報システム・サービスを利用しているなどの条件に適合する他の医療機関等の運用ルールや規程類を参考にして、自医療機関等の実態と照らし合わせて策定することも効率的で効果的な進め方と考えられます。

医療情報システム・サービスを利用する上で講じた情報セキュリティ対策や適切なシステム運用のルール等を、医療情報システム・サービスを利用する職員などのすべての関係者が理解して、実践できる必要があるため、定期的に教育・訓練を行うこと必要があります。適切なシステム運用の周知などに際しては、医療情報システム・サービス事業者にも協力を得ながら実施すると有効だと考えられます。

３．３．３　管理（Management）

設計された医療情報システムの安全管理の対策が適切に行われていることを定期的に確認し、必要があれば更なる対策を講じることが求められており、点検や監査を行うことは必要です。

３．３．４　情報セキュリティインシデントへの対策と対応

災害、サイバー攻撃、システム障害といった情報セキュリティインシデントが発生したことによる非常時において、医療機関等としての事業継続計画等（以下「BCP 等」という。）に基づいて行動し、医療情報システムに関する対応も的確に実施できることが必要です。

医療機関等は、地域における医療の継続と、医療機関等の要員等の状況などを踏まえて、各医療機関等が自ら BCP 等を策定し、この BCP に基づいて非常時における医療情報システムの運用や通常時における対策等を整理する必要があります。例えば医療情報システムを構成する機器等の一部が損傷するなどにより機能しなくなった場合に、診療等の医療業務をどうするのか、損傷したものをどのように復旧させるのか、復旧した後に、機能しなくなった間に講じた措置をどのように反映させるのか、などをあらかじめ整理する必要があります。

BCP 等は策定するだけでなく、通常時でも訓練などを通じて、周知だけでなく、BCP 等の改善の要否を確認することが必要です。例えば非常時を想定して、連絡や対応の方法や手順、非常時に使用する機器等が適切に機能するかの確認などを定期的に行うことが求められます。

また、技術的な対応の多くを医療情報システム・サービス事業者に委ねることが多いことから、非常時における対応についても、当該事業者に十分に確認しておく必要があります。特に非常時のうち、サイバー攻撃などへの対応では、通常のシステム・サービス事業者だけでは対応できないこともあるので、通常のシステム関連事業者以外の事業者に関する情報収集や協力体制の構築なども重要です。

最後に、サイバー攻撃やそのおそれがある場合を含めて、非常時となった場合には、行政機関等に対する速やかな報告や警察等への連絡が必要となることがありますので、関係する官庁の連絡先や非常時に相談や依頼するシステム関連事業者や外部有識者についても、通常時から確認しておく必要があります。

３．４　安全管理に必要な対策全般

医療機関等は、利用している医療情報システム・サービスのシステム関連事業者に、利用しているシステム特性を踏まえた医療機関等として実施すべき安全管理対策に関する提案や情報提供を、前述のリスク分析・評価の際と同様に依頼し、協力を得ながら対策を講じることは有効です。

３．５　医療情報システム・サービス事業者との協働

３．５．１　事業者選定

小規模医療機関等では、医療情報システムの安全管理を実現するために、的確で専門的な知見を有する医療情報システム・サービス事業者と協働することが重要です。

当該事業者の選定に際して、費用面や機能面などを重視して選定することも多いとされますが、患者等の機微な情報である医療情報を適切に管理することが医療機関等の信頼にも直結することを考えると、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をして、情報セキュリティにおいて十分な対応をしていると確認できる事業者を選定することは重要です。

３．５．２　事業者管理

医療情報システム・サービス事業者との契約や当該事業者との協働体制の管理は、医療機関等の規模を問わず重要です。システム関連事業者との契約や協働体制の管理では、特に非常時における対応や、契約の更新・終了などの場面が重要となります。

医療機関等においては、

- 医療機関等で導入している医療情報システム・サービスについて、どの事業者と、どのシステム・サービスについて、どのような契約を締結しているかいつでも確認できるようにすること。
- 医療情報システム・サービス事業者の体制、連絡先などを整理し、非常時の対応内容や非常時の連絡体制や連絡手順もいつでも確認できるようにしておくこと。
- 契約の更新時、特に継続する場合に、自動契約とされていることも多いですが、契約の詳細内容が変更となっていることもあります。契約内容（特に医療情報システムの運用に関する内容）の変更時などは、システム関連事業者が変更内容について医療機関等に丁寧に説明することを定め、医療機関等はその内容を十分に確認すること。

・契約の終了時、システム関連事業者におけるデータの取扱い（返却、削除など）や手順について確認すること。

等は少なくとも実施することが求められます。

３．５．３　責任分界管理

医療情報システム・サービス事業者との責任分界を、当該事業者による業務内容や利用する医療情報システム・サービスの特性に応じて、具体的なセキュリティに関する責任の範囲を明確にする必要があります。また、通常時に加えて、非常時における対応内容などについても、それぞれ整理することが必要です。

複数の医療情報システム・サービスを導入している場合には、医療機関等のみでは、医療情報システムに不具合があった場合に、適切な対応ができないなどの事態も想定されますので、医療機関等が利用する医療情報システム全体について整理し、助言を受けられるような体制を整備することも重要です。

【別添】

医療情報システム・サービス事業者との協働事項

小規模医療機関等が本ガイダンスに基づいて医療情報システムの安全管理を実施する上で、専門的な知見を有し、技術的な対応を委ねることが多いシステム関連事業者からの協力を得ることが望ましいと考えられる事項を以下に示します。

○医療機関等として、管理責任を果たすために求められる技術的な対策の具体的な内容

○説明責任を果たすためのシステム機能仕様やシステム運用手順等の文書化及び当該資料の管理

○管理責任を果たすためのシステムの管理実態や責任の所在に関する情報や資料の提供

○医療情報システムの安全管理の改善に必要な、文書化し管理しているシステム運用手順等に関する情報や資料の提供

○利用する医療情報システム・サービスはじめネットワーク回線や情報機器設備など医療情報システムに関する導入や保守などにおいて、非常時も含めた役割分担、責任の所在、協働体制をまとめた情報や資料の提供

○医療情報システムに関するリスク分析・評価・管理を実施するために必要な情報や資料の提供（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したもの。）

［特集］医療機関等におけるサイバーセキュリティ

目次

１．はじめに ..... - 1 -

２．サイバーセキュリティとは ..... - 1 -

３．サイバーインシデント ..... - 2 -

３．１　代表的な起因例 ..... - 2 -

３．２　サイバー攻撃の典型例 ..... - 2 -

３．３　必要最小限の対策：バックアップ（システム・データ） ..... - 3 -

４．対策 ..... - 5 -

４．１　ガバナンス ..... - 5 -

４．１．１　構成管理 ..... - 5 -

４．１．２　アカウント管理 ..... - 6 -

４．１．３　監視 ..... - 7 -

４．２　バックアップ ..... - 7 -

４．２．１　BCP（Business Continuity Plan：事業継続計画） ..... - 7 -

４．２．２　システム・データ ..... - 7 -

１．はじめに

診療情報等の機微な情報を扱う電子カルテをはじめとする医療情報システムは、情報の利用性を高めて連携を容易にし、質の高い医療の提供に極めて有用ですが、短時間で大量の情報を処理できることが可能であるために、何かセキュリティ上の問題が起こると被害や業務影響が大きくなる可能性があります。セキュリティ上の問題としては、例えば、システム利用終了時にログアウトし忘れるといった運用上の問題から、停電や機器の故障、さらにはマルウェア（コンピュータウイルス）と呼ばれる悪意のある不正ソフトウェアの混入など様々な事象があります。「医療情報システムの安全管理に関するガイドライン」は、これらすべてに対応するためのガイドラインで、どうしても扱う項目が多くなります。一方でサイバー攻撃と呼ばれる外部からの不正ソフトウェアの混入による被害が昨今増えてきており、最悪の場合は診療機能停止に至るなど、社会的にも問題になっています。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 項では、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順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ます。そこで、「医療情報システムの安全管理に関するガイドライン」の中で、サイバーセキュリティに関係する部分を要約し、できるだけ具体的な例などにも触れてまとめたものがこの特集です。一読いただいて、ご自身の所属する医療機関の対策に役立てていただければ幸いです。

最初に述べなければならないことは、サイバーセキュリティは導入している医療情報システムによって異なるということです。例えば、フルクラウドの電子カルテサービスを導入している診療所など小規模医療機関等の場合は、サイバーセキュリティを踏まえたシステムやデータ、サービスが用意された適切なシステム関連事業者のサービスを採用していれば、医療機関等が主に取り組むことは医療情報システムの利用者認証を適切に行うことと想定されますので、当該事業者にサイバーセキュリティに関して医療機関等側が取り組むべきことを確認し、認識の齟齬や漏れがないようにして、適切に医療情報システムを利用してください。

これ以降の記載はオンプレミス型の医療情報システムや、オンプレミス型とクラウド型の混在した医療情報システムを導入・利用している医療機関等を想定しており、地域において地域医療の基幹を担う医療機関は必要最小限の対策に留まることなく、地域で担っている役割を維持できるよう各種対策に注力してください。

２．サイバーセキュリティとは

不正ソフトウェアによる感染被害や、外部から不法に医療情報システムに侵入し、データを盗み取ったり、または破壊したりするような被害を受けるか、または被害には至らなくとも対応が必要になる事象をサイバーインシデントと呼び、これに対応する対策がサイバーセキュリティです。

外部からネットワーク等を介して、侵入または不正ソフトウェアの送り込みをサイバー攻撃と呼びますが、例えばユーザや保守事業者の自宅のパソコンが不正ソフトウェアに感染し、USB メモリや CD/DVD、外付け HDD 等の可搬媒体を介して医療情報システムに不正ソフトウェアが入り込むこともあります。

３．サイバーインシデント

３．１　代表的な起因例

サイバーインシデントの代表的な起因例を以下に示します。

（１）USB メモリ、CD/DVD、業務に使っているスマートフォンなどを介して不正ソフトウェアに感染する。（媒体感染）

（２）送られてきた電子メールに添付されたファイルやソフトウェアを、不用意にダブルクリック等を行い、開封または起動する、あるいはメール本文中にあるリンク情報（URL）をクリックし、不正ソフトウェアを呼び込んでしまう。（メール攻撃）

（３）地域医療連携、オンライン保守作業（リモートメンテナンス）、インターネット利用などの外部に接続する部分を攻撃されて、侵入または不正ソフトウェアを送り込まれる。（サイバー攻撃）

上記以外にもありますが、本特集では代表的なものにとどめます。しかし、サイバーセキュリティの観点から、基本的に講ずるべき対策などに変わりはません。

３．２　サイバー攻撃の典型例

サイバー攻撃被害と対応の典型的な例として、ランサムウェア*と呼ばれる不正ソフトウェアが保守回線から医療情報システムに侵入した場合をあげます。

＊ランサムウェア：　身代金要求（Ransom）型の不正ソフトウェアで、典型的な場合はデータを暗号化し、復号するために暗号資産などで身代金を要求してきます。

[攻撃被害]

１．最初に侵入するのはランサムウェアそのものではないことが多いです。最初に侵入した不正ソフトウェアは、医療情報システムを静かに観察します。どのファイルが良く使われて、システムがどのような構成になっているか調査し、急所となる部分に外部からランサムウェアを呼び込む不正ソフトウェアを配置します。この時点で検出することは不可能ではありませんが、比較的難しいです。

２．ランサムウェアを外部から呼び込みます。呼び込まれたランサムウェアは一斉に重要なファイルを暗号化します。さらに脅迫文書をプリンタから打ち出したり、画面に脅迫文などを表示したりします。この時点で正常な業務はできなくなります。最初の不正ソフトウェアの侵入から被害が表面化するまでに数日～数週間かかることが多いようです。

[被害対応]

３．自機関の BCP（Business Continuity Plan：事業継続計画）に基づき、非常時における緊急的な情報アクセスを開始します。現状が BCP に記載されているどのフェイズにあるのかを確認することが重要です。

４．被害を把握した場合、被害届けを警察に提出します。警察では、被害防止対策に必要な情報の提供・助言や被害の復旧への貢献が行われています。また、こうした対応や捜査に当たって

は、被害医療機関の意向が最大限尊重され、業務への影響が最小限となるよう早期被害復旧等に配慮されます。

5．侵入経路に関係する通信ログの保全が完了すれば、医療情報システムの復旧に着手します。バックアップデータはすでに不正ソフトウェアが侵入している可能性があり、検出と適切な対応を行いながら復旧します。復旧が完了した医療情報システムの動作が確認できれば、必要に応じて緊急対応中のデータ復旧を行い、終了した時点で平常運用に戻り、BCP を終了します。

6．それまでの経過をレビューし、BCP の点検・検証・評価を行い、必要があれば改善し、すべての対応プロセスが完了します。

上記は比較的大規模な医療機関で最近見られた典型的な例を記載したもので、攻撃の種類や医療機関の規模によって被害や対応方法は変わってきます。

３．３　必要最小限の対策：バックアップ（システム・データ）

媒体感染、メール攻撃、サイバー攻撃等のサイバーインシデントの被害に遭ったとしても、被害や業務影響を少しでも小さくし、業務や情報システムの復旧が少しでも早くなるための必要最小限の基本的な対策として、システムやデータのバックアップがあります。

医療情報システムを利用して、診療等の患者に対する医療サービスを行っている医療機関等においては、自施設が提供している医療サービスの特性を踏まえ、利用する医療情報システムや取り扱う医療情報の重要性に鑑み、対象とするシステムの範囲やデータの期間を定め、地域医療に与える影響や業務の復旧に要するコストが許容できる最小限に留まるよう、システム関連事業者とも協議をし、バックアップを整える必要があります。

システムやデータのバックアップの目的は下記の２つがあります。

1．最低限の業務が継続できるように、最低限必要な情報へのアクセスをすばやく復旧させる。

2．医療情報システムになにかあった場合に、元の正常な状態に戻し、復旧させる。

１．は、診療等の最低限の業務を継続するために最低限必要なデータへのアクセスをできるだけ早く回復させるためのものです。何が最低限必要であるかは医療機関等によって異なります。またデータが利用可能でもシステムの機能が回復できず、アクセスできないこともありますので、非常時における緊急のデータへの代替アクセス方法も考えておく必要があります。

また、このバックアップは毎営業日に行うべきです。典型的なサイバー攻撃の例で述べたように、不正ソフトウェアは観察してから暗号化していきますので、バックアップも狙われます。したがってバックアップを一つ用意するだけでは、対応できないこともあります。これを防ぐためには複数世代のバックアップを用意し、少なくともその一つは暗号化などのデータの変更ができないように既に書き込まれたデータに対する追加の書き込みを禁止にする必要があります。

対策の例としては、テープカートリッジにバックアップし、次の日には前の日のバックアップをさらにコピーバックアップし、このバックアップカートリッジを外します。カートリッジを５セット用意してローテーションで使うと、常に３世代分は書き込みされる恐れのないバックアップが確保できます。

テープバックアップが利用できない場合は、複数世代のバックアップをディスク領域に保存した上で、OS の機能で書き込み禁止にしますが、不正ソフトウェアによって管理者権限が奪取されると、書き込み禁止の状態を解除される恐れがあります。完全に防止することは難しいですが、少なくとも医療情報システムの運用系とバックアップ系は管理者のパスワードを異なるものにするか、利用者の管理ドメインを変えるなどの措置を施すことで、リスクの軽減を講じることはできます。

２．におけるシステムの復旧には、データだけでなくシステムを動作させるためのプログラムや設定もバックアップしておく必要があります。フルバックアップと言ってもいいでしょう。一般的に医療機関等の判断と作業で実施できうるものではなく、医療情報システムを導入するシステム関連事業者がセットアップするものです。医療機関等はシステムを導入するときに、フルバックアップを適切に行うことを仕様に含め、検収の際に確認することになります。医療機関等の判断で、医療情報システムを複数のシステム関連事業者が構成することもあります。例えば放射線画像システムと電子カルテが異なる事業者が導入する場合で、LAN などのネットワークインフラは別事業者という場合もあります。複数のシステム関連事業者が関与する場合は、バックアップに抜け漏れや隙間があってはいけません。またシステムの稼働や利用に必要なサーバやクライアントＰＣ等の機器に障害が発生した場合で、同じ機器が手配・調達できない場合もあります。機器の設定等は、単純なバックアップと同時に、論理的な設定の記録も必要です。これがあるとないとでは復旧に要する時間や作業効率に差が出ます。

プログラムや設定のバックアップは変更した時に取ればいいですが、データはやはり毎日バックアップされると思います。こちらも１．の場合と同じで、バックアップも不正ソフトウェアに狙われますので、１．と同様の対策を取る必要があります。また、被害の範囲や性格等によっては、ソフトウェアやデータばかりでなく、医療情報システムで利用する機器（ハードウェア）のバックアップが求められることがあります。例えばサイバー攻撃による刑事事件とされるような場合には、警察による捜査のため、サーバや端末、機器等について証拠として提供を求められることがあります。また機器等のファームウェア等が書き換えられているリスクが認められる場合には、交換等の対応も必要となります。このように犯罪による被害やその範囲・内容によっては、既存のシステムと互換性を保つことが可能なハードウェアを準備しておくことが必要なこともあります。

診療の継続性をできる限り早く回復させるためのバックアップについては、医療機関によって何が必要か異なりますので、事前によく検討しておく必要があります。一般的に言って、情報が生成されてから時間が経てば経つほど、利用される頻度は低下します。もちろん過去の情報との比較は必要ですが、一般的な医療機関では、緊急事態である非常時では直近１年程度の期間の情報が比較できれば、緊急の診療としては可能なことが多いと思われます。したがって、バックアップ対象期間については、１年を少し超える期間をバックアップ対象とすることが推奨されます。なお、放射線画像診断検査結果データのようにデータサイズが大きい画像情報については、バックアップの環境にかけられるコストの都合から、このような目的でのバックアップが難しい場合は、読影レポートを保存するか、カルテ自体に所見を記載するようにしておくといいでしょう。検査結果や処方データなどは、厚生労働省標準規格である SS-MIX２標準化ストレージの形式で保存されていれば必要なバックアップデータを容易に作成することができます。また、HL7 FHIR 化が進んでいる場合は SS-MIX２標準のデータを HL7 FHIR 化した HL7 FHIR 規格準拠サーバでも同じことが言えます。

また、システム機能が回復できないためにバックアップデータがあってもアクセスできなくなる可能性もあります。一年程度のデータであれば CD-R や DVD-R にコピーすることも可能ですので、非常用

のノート PC を用意して、SS-MIX2 ビューアや HL7 FHIR クライアントを用意することも考えられます。システム関連事業者と事前によく相談しておくことが必要です。

非常時における緊急用のデータアクセスで過去の記録まで用意することは一般的には難しく、対応も複雑になり経費もかかります。非常時はインシデント発生以前のデータは閲覧のみと割り切って、紙ベースで運用することも一つの方法です。その際、非常時の真っ只中や非常時からの復旧を急いで対応している中、データの事後入力や再入力が必要になりますが、非常時においては、診療の継続性の確保が優先すべき状況であるため、やむを得ないことだと考えられます。

４．対策

サイバーセキュリティを確保するために医療情報システムの稼働を支えるサーバや端末、ネットワーク等の機器、様々なシステム群の構成管理、そして、システムを利用・管理する利用者・管理者をシステム関連事業者の担当者も含めてリストアップし、かつ、複数のシステムが互いに連携したり、制御し合ったりして稼働しているためシステム自体も管理対象としてリストアップして、医療情報システムの稼働に接するすべてのアカウントの管理を行うことが重要である。そして、これらの多数の構成とアカウントが正常な動作をしていることをモニタリングし、正常ではない動き等をすることがないように制御、または、異常な動き等を検知した際には、予防的措置を発動する、というような監視を含め、ガバナンスを働かせる必要がある。

次に、ガバナンスを働かせていたとしてもサイバーインシデントの被害に遭う、という非常時を想定して、システムとの共存環境において、非常時における運用面の方針や判断基準や手順等を BCP（Business Continuity Plan：事業継続計画）として定め、業務継続に必要なシステムやデータの冗長化や複製などの保管を行い、運用面からシステム面までトータルでのバックアップを策定しておく必要がある。

４．１　ガバナンス

現在の医療情報システムは複雑で、外部サービスを利用することもありますし、機器やシステムの保守を外部からオンラインで行うこともあります。このような場合、外部接続するためのルータなどの機器や回線自体も外部事業者が管理している場合があります。この回線や通信機器あるいは外部事業者のシステムに脆弱性があると、ここが攻撃され、医療情報システム全体に被害が及びます。ガバナンスと言っても外部事業者を直接管理することはできませんので、医療機関としては接続の状況を把握し、契約等で、脆弱性が生じないように縛る必要があります。例えば、部門システムの保守は部門が業者と交渉し、契約も担当し、医療機関としては把握が不十分なことがありえます。このような状況では患者に対して責任あるセキュリティ対策を行うことは不可能です。医療機関として接続状況を把握し、コントロールすることが必須です。

４．１．１　構成管理

医療情報システムの構成や利用するサービスの形態に応じて、システムやサービスを構成する機器や利用するネットワーク構成を一覧化し、システムが稼働するためのネットワークに接続する機器やネッ

トワーク経路を掌握し、不正な機器が接続されたり、不正なソフトウェアやデータが混入されたり、異常なデータ通信が発生したりすることがないよう、管理する必要があります。

特に、セキュアなネットワークを整備する観点からは、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を実施し、セキュリティを確保することが重要です。

４．１．２　アカウント管理

医療情報システムを利用・管理する関係者をリストアップし、それぞれがどのような権限でどのようなシステムを操作するのかを掌握しておく必要があります。

特に、システム関連事業者を含めて、システムの管理を行う関係者のアカウントの管理は厳重に行う必要があります。

３．３の項でも少し触れましたが、不正ソフトウェアはシステムを解析し、管理者権限を奪取し、防御を無力化します。管理者権限を奪取されると、アクティブディレクトリや LDAP のような利用者認証のコントロールは奪われますが、運用系とバックアップ系などのセキュリティ系の認証を分離しておくと、時間稼ぎにはなりますし、うまく行けばバックアアップ系やセキュリティ系を守ることができます。

また、昨今の情報システムは複雑で、様々なシステムが互いに自動的に連携したり、支援・制御していたりします。アカウント管理に、システムやアプリケーション等のソフトウェアも含めて管理することが重要です。

Windows のような PC の OS でもサーバ系の Linux 系の OS でも極めて多機能で、様々なプロセスがインストールされており、必要に応じて、あるいは自動的に起動されています。医療情報システムで利用しない機能は起動する必要はありません。起動していると、そのプロセスに脆弱性があればサイバー攻撃の侵入口になります。不要なプロセスやプログラムは削除あるいは起動しないようにシステム関連事業者に要求してください。また、実際に不要なプロセスが起動されていないかの監視も重要です。削除や起動静止していたプロセスが、セキュリティパッチによって再生することもあります。

４．１．３　監視

機器構成やアカウントを管理することで、システムやネットワークに対する不正な侵入が検知でき、不正アクセスを防止することが可能となり、さらには、不正な侵入等がなされた際においても、不正なソフトウェアやデータによる正常とは異なる振る舞いを検知する、監視の仕組みを整え、その効果を発揮することが可能となります。

不正侵入の検知や不正アクセスの防止を支援するシステムとしては、IDS（Intrusion Detection System：不正侵入検知システム）/IPS（Intrusion Prevention System：不正侵入防御システム）と称したセキュリティサービスが提供されています。

不正なソフトウェアやデータによる振る舞い検知によるセキュリティサービスとして、EDR（Endpoint Detective and Response）があります。最近の不正ソフトウェアの被害を見ると、従来のパターンマッチングによる不正ソフトウェア検出をすり抜ける不正ソフトウェアが多いと言えます（ゼロ・デイ攻撃)。100%検出できるわけではありませんが、不正ソフトウェアの異常な動きを検出して、被害が出る前に報告します。最近のコンピュータウイルス対策ソフトウェアには EDR 機能も持つものが増えていますが、ライセンス契約によっては活性化していないこともあります。EDR が導入されていればリスクを低下させることが可能です。

４．２　バックアップ

ガバナンスを補完し、少しでもサイバーインシデントが発生した際に、混乱を最小限にとどめ、業務影響、復旧に要する時間等を最小限にするために、システムも含んだ運用面での方針等を定めた BCP の策定及びシステムやデータのバックアップの整備は重要です。

４．２．１　BCP（Business Continuity Plan：事業継続計画）

サイバーインシデントを 100%防止することは不可能ですし、大規模災害もないとは言えません。地域に一定の役割を担う医療機関としては BCP の策定と、BCP に基づく訓練、さらに BCP の持続的な見直しは必須です。昨今の状況を踏まえると、サイバーインシデントも BCP の重要なテーマです。大規模災害の BCP も重要ですが、サイバーインシデントも主要なテーマに入れて BCP を策定し運用してください。非常時には最悪の場合は紙運用や地域の他の医療機関等による支援も視野に含めることも必要です。

４．２．２　システム・データ

医療機関等の担う特性に応じて、「３．３　必要最小限の対策：バックアップ（システム・データ)」を参照し、継続できる業務の範囲を広げ、サイバー攻撃による影響が少しでも軽減されるように、システムやデータのバックアップを策定する必要がある。

第5.2 版→第6.0 版 項目移行対応表

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
			記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無
1. はじめに	ー	（略）	レ	1、2.1							
2. 本ガイドラインの読み方	ー	（略）	レ	3							
3. 本ガイドラインの対象システム及び対象情報	ー	（略）	レ	2.2、2.3、4.7	レ	16					
4. 電子的な医療情報を扱う際の責任のあり方	ー	（略）	レ	4.1	レ	1.1～1.4、5.3					
5. 情報の相互運用性と標準化について	ー	（略）							レ	5	
6.1. 方針の制定と公表	C.最低限のガイドライン	1. 個人情報保護に関する方針を策定し、公開すること。	レ	4.4	レ	1.1	レ	１．２．２			
		2. 医療情報システムの安全管理に関する方針を策定すること。その方針には、次に掲げる事項を定めること。 ・ 理念（基本方針と管理目的の表明） ・ 医療情報システムで扱う情報の範囲 ・ 情報の取扱いや保存の方法及び期間 ・ 不要・不法なアクセスを防止するための利用者識別の方法 ・ 医療情報システム安全管理責任者 ・ 苦情・質問の窓口	レ	4.4	レ	1.1	レ	1．④			
6.2 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践	B.考え方	（略）	レ	4.2							
6.2.1 ISMS構築の手順	B.考え方	（略）			レ	2.2	レ	6.2			
6.2.2 取扱い情報の把握	B.考え方	（略）					レ	6.1.2			
6.2.3. リスク分析	C.最低限のガイドライン	1. 医療情報システムで扱う情報を全てリストアップすること。	レ	4.5	レ	2.2	レ	6．②			
		2. リストアップした情報を、安全管理上の重要度に応じて分類し、常に最新の状態を維持すること。			レ	2.2	レ	6．②			
		3. リストアップした情報は、医療情報システム安全管理責任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。			レ	2.2	レ	6．１．２			
		4. リストアップした情報に対してリスク分析を実施すること。脅威に関してはリスク分析に関する解説（別冊）を参照	レ	4.5	レ	2.2	レ	6．⑤			
		5. 医療情報システムベンダ及び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。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」（総務省・経済産業省　令和2年8月21日）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。	レ	4.5	レ	2.2	レ	6．⑥	レ	4②	
		6. 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一覧（設置事業者等含む）を作成し、常に最新の状態を維持すること。例えば、前述の「サービス仕様適合開示書」を利用することが考えられる。	レ	4.5	レ	2.2	レ	6．⑥	レ	2②	
		7. リスク分析により得られたリスクに対して、6.3章～6.12章に示す対策を実施すること。			レ	2.2	レ	6．⑧			
	D.推奨されるガイドライン	1. 上記1から7の結果を系統的に文書化して管理すること。			レ	2.2	レ	6．⑦			
6.3 組織的安全管理対策（体制、運用管理規程）	B.考え方	（略）			レ	3.2					
	C.最低限のガイドライン	1. 医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定すること。ただし、小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。			レ	3.2	レ	3① 3③			
		2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めること。			レ	3.2	レ	8③			
		3. 医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	レ	4.4	レ	3.2	レ	8①			
		4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	レ	4.4	レ	3.2	レ	7⑤			
		5. 運用管理規程等において次の内容を定めること。 ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	レ	4.4	レ	3.2	レ				
6.4 物理的安全対策	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。					レ	8③			
		2. 個人情報を入力・参照できる端末が設置されている区画は、業務時間帯以外は施錠するなど、運用管理規程等に基づき許可された者以外の者が立ち入ることができないようにするための対策を実施すること。ただし、上記の対策と同等レベルの他の対策がある場合はこの限りではない。					レ	15②			
		3. 個人情報が保存されている機器が設置されている区画への入退管理を実施すること。例えば、次に掲げる対策を実施すること。 ・ 入退者に名札等の着用を義務付ける。 ・ 台帳等によって入退者を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。					レ	15②			レ
		4. 個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。					レ	8③	レ	12.3.1	
		5. 個人情報が入力・参照できる端末の覗き見防止対策を実施すること。							レ	１２.3.2	
	D.推奨されるガイドライン	1. 情報管理上重要な区画に防犯カメラ、自動侵入監視装置等を設置すること。							レ	12②	レ
6.5 技術的安全対策	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 医療情報システムへのアクセスにおける利用者の識別・認証を行うこと。	レ	4.6	レ	4.1	レ	13①	レ	14①	
		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。	レ	4.6			レ	13②	レ	14②	
		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。							レ	14③	
		4. 利用者が個人情報を入力・参照でき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させること。					レ	8③	レ	12.3.2	
		5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	レ	4.4			レ	15⑨	レ	10①	
		6. 利用者の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行うこと。また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、アクセス権限の変更を行うことを、運用管理規程で定めること。なお、複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことでアクセス管理を実施する必要がある。			レ	4.2	レ	13③	レ	14.2	
		7. 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。			レ	4.2	レ	5③	レ	17①	
		8. 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。	レ	4.4	レ	4.2	レ	5②	レ	17②	
		9. 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。					レ	5①	レ	17③	
		10. 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。					レ	9⑥	レ	8①	
		11. 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。	レ	4.4	レ	4.2	レ	15⑥	レ	8②	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 （Overview）		経営管理編 （Governance）		企画管理編 （Management）		システム運用編 （Control）		Q&A
		12. 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付等を行う場合、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 。					レ	15⑥	レ	8④	
		13. 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。					レ	15②	レ	14⑤	
		14. パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。 (1) 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。また、利用者識別にICカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者のパスワードの失念や、パスワード漏えいのおそれなどにより、医療情報システムの運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏えいのおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。 (3) 医療情報システムの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記載される等があってはならない）。 (4) パスワードは以下のいずれかを要件とする。 a. 英数字、記号を混在させた13文字以上の推定困難な文字列 b. 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更させる（最長でも2ヶ月以内） c. 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用にPIN等が設定されている場合には、この限りではない。 いずれのパスワードを設定した場合でも、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏えい対策が講じられていることを確認すること。 (5) 類推されやすいパスワードを使用させないこと。また、類似のパスワードを繰り返し使用させないこと。なお、類推されやすいパスワードには、利用者の氏名や生年月日、辞書に記載されている単語等が含まれるものがある。					レ	15②	レ	14⑥	レ
		15. 無線LANを利用する場合、次に掲げる対策を実施すること。 (1) 適切な利用者以外に無線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。 (2) 不正アクセス対策を実施すること。少なくともMACアドレスによるアクセス制限を実施すること。 (3) 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。 (4) 電波を発する機器（携帯ゲーム機等）による電波干渉に留意すること。			レ	4.2	レ	15⑦	レ	13⑬	
		16. 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) 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。 (3) 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。 (4) 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。			レ	4.2	レ	9④	レ	8⑥	
	D.推奨されるガイドライン	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	レ	4.6	レ	4.2	レ		レ	14.2	レ
		2. 個人情報を入力・参照できる端末から離席する場合、クローズ処理等（クリアスクリーン、ログオフ、パスワード付きスクリーンセーバーの起動等）を実施させること。					レ		レ		レ
		3. 外部のネットワークとの接続点やDBサーバ等の安全管理上の重要部分には、ファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。					レ		レ		レ
		4. パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。 (1) パスワード入力が不成功に終わった場合、再入力に対して一定の不応時間を設定すること。 (2) パスワード再入力の失敗が一定回数を超えた場合、再入力を一定期間受け付けない仕組みとすること。					レ		レ		レ
		5. 利用者認証には、ID・パスワード＋バイオメトリクス又はICカード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように、2つの独立した要素を用いて行う方式（二要素認証）等、より認証強度が高い方式を採用すること。ただし、医療情報システムを利用する端末に二要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・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れば、二要素認証に相当すると考えてよい。					レ	13②	レ	14②	レ
		6. 許可された者以外の無線LANの利用を防止するため、例えば802.1xや電子証明書を組み合わせるなどして、無線LANのセキュリティを強化すること。	レ	4.6			レ	13.4	レ		レ
		7. IoT機器を含む医療情報システムの接続状況や異常発生を把握するため、IoT機器・医療情報システムそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。			レ	4,2	レ	13.4	レ		レ
6.6 人的安全対策	B.考え方	（略）			レ	3.2					
	C.最低限のガイドライン	1. 従業者に対する人的安全管理措置 (1) 法令上の守秘義務のある者以外の者を従業者等として採用するに当たって、雇用契約に守秘・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。	レ	4.4	レ	3.2	レ	7①			
		1. 従業者に対する人的安全管理措置 (2) 従業者に対し個人情報の安全管理に関する教育訓練を定期的に実施すること。	レ	4.4	レ	3.2	レ	7②			
		1. 従業者に対する人的安全管理措置 (3) 従業者の退職後の個人情報保護規程を定めること。	レ	4.4	レ	3.2	レ	7①			
		2. 事務取扱委託業者の監督及び守秘義務契約 (1) 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、個人情報保護のため、次に掲げる対策を実施すること。 a　受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。 b　保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認すること。 c　清掃等の直接医療情報システムにアクセスしない作業の場合でも、作業結果を定期的に確認すること。 d　受託する事業者が再委託を行うか否かを明確にすること。受託する事業者が再委託を行う場合は、受託する事業者と同等の個人情報保護に関する対策及び契約がなされることを条件とすること。			レ	3.2	レ	1② 7③④			
		2. 事務取扱委託業者の監督及び守秘義務契約 (2) ソフトウェアの異常等でデータを救済する必要があるとき等、やむを得ない事情で受託する事業者の保守要員が医療情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。			レ	3.2	レ	7③④			
	D.推奨されるガイドライン	1. サーバ室等の安全管理上重要な場所では、モニタリング等により従業者の行動を管理すること。					レ	8③	レ	12	レ
6.7 情報の破棄	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	3. 6.2章C.1で把握した情報種別ごとに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従業者、具体的な破棄方法を含めること。					レ	8①	レ	7⑨	
		2. 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、読み出し可能な情報がないことを確認すること。					レ	8⑨	レ	7⑩	
		3. 外部保存を受託する事業者等に破棄を委託した場合は、6.6章C.2に従うとともに、確実に情報が破棄されたことを確認すること。					レ	8⑩	レ	7⑪	
		4. 運用管理規程において、不要になった個人情報を含む媒体の破棄に関する規定を定めること。					レ	8⑨			
6.8 情報システムの改造と保守	B.考え方	（略）			レ	4.1					
	C.最低限のガイドライン	1. 動作確認で個人情報を含むデータを使用するときは、明確に守秘義務を設定するとともに、終了後は確実にデータを消去させること。					レ	15⑨	レ	10①	
		2. メンテナンスを実施するためにサーバに保守事業者の作業員（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。					レ	13⑤	レ	10③	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		3. 保守要員の専用アカウントについて、外部流出等による不正使用の防止の観点から適切に管理することを求めること。					レ	13⑤			レ
		4. 保守要員の離職や担当替え等に応じて速やかに保守要員の専用アカウントを削除できるよう、保守事業者に報告を義務付けるとともに、それに対応できるアカウント管理体制を整備すること。			レ	4.1	レ	13⑤⑦	レ	10③	レ
		5. 保守事業者がメンテナンスを実施する際には、日単位で作業申請書を事前提出させるとともに、終了時に速やかに作業報告書を提出させること。提出された書類は、医療情報システム安全管理責任者が承認すること。なお、作業申請書の承認は、原則として保守作業の実施前に行う必要があるが、事前に承認を得ずに実施可能なものとして保守事業者と合意したメンテナンスについては、事後承認とすることができる。					レ	15⑧	レ	10.1	レ
		6. 保守事業者と守秘義務契約を締結し、これを遵守させること。			レ	4.1	レ	7③			
		7. 原則として、保守事業者に個人情報を含むデータを医療機関等外等に持ち出させないこと。やむを得ず医療機関等外に持ち出さなければならない場合は、置き忘れ等に対する十分な対策を含む運用管理規程を定めることを求め、医療情報システム安全管理責任者がそれを承認すること。					レ	8⑤	レ	7.1	
		8. リモートメンテナンスによるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに医療機関等の責任者が確認すること。					レ	15⑧	レ	10④	
		9. リモートメンテナンス において、やむを得ずファイルを医療機関等へ送付等を行う場合、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。					レ	15⑧	レ	10⑤	
		10. 再委託が行われる場合は、再委託を受ける事業者に対しても、保守事業者の責任で同等の義務を課させること。	レ	4.4	レ	5	レ	1②	レ	3.3	
	D.推奨されるガイドライン	1. 詳細なオペレーション記録を保守操作ログとして記録すること。									レ
		2. 保守作業は医療機関等の関係者の立会いの下で行わせること。									レ
		3. 保守要員と保守事業者との守秘義務契約を求めること。									レ
		4. 保守要員の持ち込む機器や記憶媒体に対して、不正ソフトウェアがないことを確認すること。									レ
		5. 保守事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合には、詳細な作業記録を残すよう求めること。また、必要に応じて、医療機関等の監査に応じるよう求めること。									レ
		6. 保守作業に関わるログの確認の際に、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者の診療録等に何回アクセスされたか確認できる仕組みを備えること。									レ
6.9 情報及び情報機器の持ち出し並びに外部利用について	B.考え方	（略）			レ	2.2、3、4					
	C.最低限のガイドライン	1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しや、BYODの実施に関する方針を運用管理規程で定めること。	レ	4.4	レ	3.2	レ	9⑥	レ	7.1 8.4	
		2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。					レ	8①			
		3. 情報を格納した可搬媒体又は情報機器の盗難、紛失時の対応を運用管理規程に定めること。					レ	8⑦			
		4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底するとともに、教育を実施すること。					レ	7②			
		5. 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こと。					レ	9①②	レ	7⑦	
		6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けるとともに、定期的なパスワードの変更等の対策を実施すること。	レ	4.6	レ	3.2	レ	13⑥	レ	8⑤	
		7. 盗難、置き忘れ等に対応する措置として、情報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。					レ	8⑤	レ	7③	
		8. 持ち出した情報機器について、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、コンピュータウイルス対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施すること。なお、ネットワークに接続する場合は6.11章の規定を遵守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは6.5章C.15.の基準を満たさないことがあるため、利用できない。ただし、非常時等でやむを得ず公衆無線LANしか利用できない環境である場合に限り、利用を認める。利用する場合は6.11章で述べている基準を満たした通信手段を選択すること。					レ	8⑤	レ	7④	
		9. 持ち出した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。					レ	8⑤	レ	7⑥	
		10. 個人保有の情報機器（ノートパソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、医療情報システム安全管理責任者は1～5の対策を行うとともに、医療情報システム安全管理責任者の責任において上記の6、7、8、9と同様の要件を遵守させること。			レ	3.2	レ	9⑥	レ	8.4	
	D.推奨されるガイドライン	1. 外部での情報機器の覗き見による情報の漏えいを避けるため、ディスプレイに覗き見防止フィルタ等を張ること。							レ	12⑥	レ
		2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。							レ		レ
		3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	レ	4.4	レ	3	レ	9⑥	レ	8⑨	レ
		4. ノートパソコン、スマートフォン、タブレット等を持ち出して使用する場合、次に掲げる対策を実施すること。 (1) 紛失、盗難の可能性を十分考慮し、可能な限り端末内に医療情報を置かないこと。やむを得ず医療情報が端末内に存在する場合や、当該端末を利用すれば容易に医療情報にアクセスできる場合は、一定回数パスワード入力を誤った場合に端末を初期化する等の対策を行うこと。 (2) BYODを行う場合は、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等、適切な技術的対策や運用による対策を選択・採用し、十分な安全性が確保された上で行うこと。					レ	9⑥	レ	8⑨	レ
6.10 災害、サイバー攻撃等の非常時の対応	B.考え方	（略）			レ	3.4					
	C.最低限のガイドライン	1. 医療サービスを提供し続けるためのBCPの一環として、“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めておくこと。	レ	4.4	レ	3.4	レ	11①			
		2. 非常時における対応に関する教育及び訓練を従業者に対して行うこと。なお、医療情報システムの障害時の対応についても同様に行うこと。	レ	4.4	レ	3.4	レ	11⑥			
		3. 正常復帰後に、代替手段で運用した間のデータ整合性を図るための規約を用意すること。					レ	11①			
		4. 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。 (1) 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 (2) 非常時機能が定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。 (3) 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。 (4) 医療情報システムに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。 (5) 重要なファイルは数世代バックアップを複数の方式で取得し、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。					レ	11④⑤	レ	11①	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		5. 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」（医政総発1029 第１号　医政地発1029 第３号　医政研発1029 第１号　平成30年10月29日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための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。 厚生労働省連絡先 https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html ※ 独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、5. 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。標的型メールを受信した、Webサイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先　情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	レ	4.4	レ	3.4	レ	11⑧			
6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	B.考え方	（略）			レ	4					
	C.最低限のガイドライン	1. 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。 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。 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対策を実施すること。 上記を満たす対策としては、①クローズドなネットワークを選択する、又は②オープンなネットワークを選択する場合、例えばIPsecとIKEを利用する等してセキュアな通信路を確保すること又は、IPsecによるVPN接続等を利用せず医療情報システムへ接続する場合は、後述の11.に示す方法等により実施すること。 チャネル・セキュリティの確保を閉域ネットワークに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閉域性の範囲を電気通信事業者に確認すること。							レ	13⑨	
		2. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、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た必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、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。					レ	15⑦	レ	13④	
		3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を実施すること。これに関しては、6.5章で包括的に述べているので、それを参照すること。					レ				
		4. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。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。安全性が確認できる機器とは、例えば、ISO 15408で規定されるセキュリティターゲット又はそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。					レ	15⑦	レ	13⑤	
		5. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても 、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。例えば、S/MIMEの利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。							レ	13⑦	レ
		6. 医療機関等の間の情報通信には、医療機関等だけでなく、電気通信事業者やシステムインテグレータ、運用を受託する事業者、遠隔保守を行う機器保守事業者等の多くの組織が関連する。そのため、次に掲げる事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・ 診療録等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・ 送信元の医療機関等がネットワークに接続できない場合の対処 ・ 送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ ネットワークの経路途中が不通の場合又は著しい遅延が発生している場合の対処 ・ 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・ 伝送情報の暗号化に不具合があった場合の対処 ・ 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・ 障害が起こった場合に障害部位を切り分ける責任 ・ 送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関等内においても、次に掲げる事項を契約や運用管理規程等で定めておくこと。 ・ 通信機器、暗号化装置、認証装置等の管理責任（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・ 患者等に対する説明責任 ・ 事故発生時における復旧作業・他施設やシステムベンダ及びサービス事業者との連絡に当たる専任の管理者の設置 ・ 交換した医療情報等に対する管理責任及び事後責任（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）			レ	4	レ	2①	レ	13①	
		7. 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。			レ	4	レ	7⑥	レ	13⑪	
		8. リモートメンテナンスを実施する場合は、必要に応じて、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等、不必要なログインを防止するための対策を実施すること。 また、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をはじめとする6.5章及び6.6章に記載されている内容や、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。メンテナンス自体は6.8章を参照すること。			レ	4	レ	12⑤	レ	10.1 18.1	
		9.電気通信事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質を確認すること。また、上記1及び4を満たしていることを電気通信事業者やオンラインサービス提供事業者に確認すること。			レ	4	レ	15⑩	レ	10.1	
		10.患者等に情報を閲覧させる場合、情報を公開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個人認証等の対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、ITに係る以外の法令等の遵守の体制等も含めた幅広い対策を立て、それぞれの責任を明確にすること。					レ	8⑧	レ	7⑭	
		11.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。					レ	15⑦	レ	13⑥	
		12. クローズドなネットワークで接続する場合でも、内部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。					レ	15⑦	レ	13③	
		13. 電子署名に用いる秘密鍵の管理は、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うこと。					レ	14②	レ	15.1	
	D.推奨されるガイドライン	1. やむを得ず従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。 2. 共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-2レベル１相当以上の対応を図ること。					レ	8⑧	レ	7.2.1	レ
6.12 法令で定められた記名・押印を電子署名で行うことについて	B.考え方	（略）			レ	4					
	C.最低限のガイドライン	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必要がある。			レ	4	レ	14①			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 （Overview）		経営管理編 （Governance）		企画管理編 （Management）		システム運用編 （Control）		Q&A
		1. 以下の電子証明書を用いて電子署名を施すこと (1) A項の要件を満たす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署名等を用いること。 (a) 厚生労働省の定める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6.12.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）。					レ	14①			
		・ 事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、オンラインの場合、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）第3条第1項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ（いずれも本項と同等の電子署名（資格確認を除く）を施すこと）により確認を行うこと。郵送の場合は、身分証明書のコピー（署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること ））、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用すること 。 ※　身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか1種類により、又はその他の身分証明書であれば2種類以上により行うこと。 ・ 事業者による利用者の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					レ	14①			
		－　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。					レ	14①			
		2. 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、「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－」（総務省、平成16年11月）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。 (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。					レ	14①			
		2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること (1) タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）に基づき認定された事業者（認定事業者）が提供するものを使用すること。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」（総務省、平成16年11月）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。 当然ではあるが、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。					レ	14①			
7.1 真正性の確保について	B.考え方	（略）			レ	1.1					
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 入力者及び確定者の識別・認証 (1) 電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合 a　入力者及び確定者を正しく識別し、認証を行うこと。 b　システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。 c　業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。 (2) 臨床検査システム、医用画像ファイリングシステム等、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　装置の操作者を運用管理規程で明確にするとともに操作者以外のものによる機器の操作を運用上防止すること。 b　当該装置による記録をいつ・誰が行ったか、システム機能と運用の組み合わせにより明確にすること。			レ	1.1	レ	13.⑧ 15⑬			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 （Overview）		経営管理編 （Governance）		企画管理編 （Management）		システム運用編 （Control）		Q&A
		2. 記録の確定手順の確立と、識別情報の記録 (1) 電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合 a　診療録等の作成・保存を行おうとする場合、確定された情報を登録できる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。 (2) 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　確定された記録が、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。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		3. 更新履歴の保存 (1) 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。 (2) 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。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		4. 代行入力の承認機能 (1) 代行入力を実施する場合、具体的にどの業務等に代行入力を認めるか、誰が誰を代行してよいかを運用管理規程で定めること。 (2) 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。 (3) 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。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		5. 機器・ソフトウェアの品質管理 (1) システムがどのような機器、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、システムの仕様を明確に定義すること。 (2) 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) 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程で定めるとともに、従業者等への教育を実施すること。 (4) 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。			レ	1.1	レ	15⑬	レ	9.2	
	C.最低限のガイドライン 【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】	6. 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 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が必要である。					レ	15⑦	レ	13⑫	
		7. 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 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。					レ	15⑦ 15⑬	レ	13⑧	
		8. リモートログイン機能を制限すること 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。					レ	8⑧ 15⑬	レ	7⑫	
7.2 見読性の確保について	B.考え方	（略）			レ	1.1					
	C.最低限のガイドライン	1. 情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの全ての情報の所在が日常的に管理されていること。					レ	8④ 15⑬	レ	4①	
		2. 見読化手段の管理 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。					レ	15⑬	レ	5④	
		3. 見読目的に応じた応答時間 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にすること。					レ	15⑬	レ	9④	
		4. システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするため、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。			レ	1.1	レ	15⑬	レ	11.2	
	D.推奨されるガイドライン 【医療機関等に保存する場合】	1. バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		2. 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力できるようにすること。									レ
		3. 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップするとともに、そのバックアップデータ等と汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		4. 緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持すること。									レ
		5. 緊急に必要になるとまではいえない診療録等の見読性の確保 緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する事業者の障害等に対応できるような対策を実施しておくこと。									レ
7.3 保存性の確保について	B.考え方	（略）			レ	3、4					
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 不正ソフトウェアによる情報の破壊、混同等の防止 (1) 不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。	レ	4.4	レ	3、4	レ	15⑥ 15⑬	レ	8.1	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 （Overview）		経営管理編 （Governance）		企画管理編 （Management）		システム運用編 （Control）		Q&A
		2. 不適切な保管・取扱いによる情報の滅失、破壊の防止 (1) 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。 (2) 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、バックアップ頻度、バックアップ方法等を明確にすること。これらを運用管理規程に定めて、その運用を関係者全員に周知徹底すること。 (3) 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を実施すること。 (4) 電子的に保存された診療録等の情報に対するアクセス履歴を残すとともに、その履歴を適切に管理すること。 (5) 各保存場所における情報が毀損したときに、バックアップされたデータ等を用いて毀損前の状態に戻せるようにすること。もし、毀損前と同じ状態に戻せない場合には、毀損された範囲が容易に分かるようにしておくこと。			レ	3、4	レ	15②③ 15⑬	レ	12.2 18.1	
		3. 記録媒体、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 (1) 記録媒体が劣化する前に、当該記録媒体に保存されている情報を新たな記録媒体又は記録機器に複写すること。記録媒体及び機器ごとに劣化が起こらずに正常に保存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、月に一回程度の頻度でチェックを行うこと。使用終了予定日が近づいた記録媒体又は記録機器は、そのデータを新しい記録媒体又は記録機器に複写すること。これら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。					レ	15⑬	レ	12.2	
		4. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 (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。					レ	15⑬	レ	5①	
	C.最低限のガイドライン 【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】	5. 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しなくてはならない。			レ	3、4	レ	15⑬	レ	5③	
		6. ネットワークや外部保存を受託する事業者に設備の劣化対策の実施を求めること ネットワークや外部保存を受託する事業者の設備の条件を考慮し、回線や設備が劣化した際にそれらを更新する等の対策を実施するよう求めること。			レ	3、4	レ	15⑬	レ	12.2	
	D. 推奨されるガイドライン 【医療機関等に保存する場合】	1. 不適切な保管・取扱いによる情報の滅失・破壊の防止 (1) 記録媒体、記録機器及びサーバは、許可された者しか入ることができない部屋に保管するとともに、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。 (2) サーバ室には、許可された者以外が入室できないよう、鍵等の物理的な対策を施すこと。 (3) 診療録等のデータのバックアップを定期的に取得するとともに、その内容に対する改ざん等が行われていないことを検査する機能を備えること。					レ	8③	レ	12②	レ
		2. 記録媒体、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 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1又はRAID-6相当以上のディスク障害に対する対策を行うこと。									レ
8 診療録及び診療諸記録を外部に保存する際の基準	ー						レ	7			
8.1 電子保存の３基準の遵守							レ	1.1.2			
8.2 運用管理規程	B.考え方	（略）			レ	3.2	レ	16			
8.3. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン	1. 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (1) 病院や診療所、医療法人等が適切に管理する場所に診療録等を保存すること。 (2) 委託した医療機関等及び患者等の許可なく、保存を受託した診療録等を分析等の目的で取り扱わせないこと。 (3) 保存を受託した診療録等の分析等は、不当な利益を目的としない場合に限って許可すること。 (4) 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わせること。 (5) 保存を受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、外部保存を受託する事業者に適切なアクセス権を設定し、情報漏えいや、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よう求めること。 (6) 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間の同意に基づいて実施すること。			レ	5	レ	7⑦			
		2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合 (1) 保存した情報の取扱いに関して監督できるようにするため、外部保存を受託する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。 (2) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線に関しては6.11章を遵守させること。 (3) 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で確認をすること。 (4) 外部保存を受託する事業者の選定に当たっては、事業者のセキュリティ対策状況を示す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。 (5) 外部保存を受託する事業者に、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。なお保守に関しては、6.8章を遵守すること。 (6) 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するとともに、外部保存を受託する事業者に遵守させること。 (7) 保存した情報を、外部保存を受託する事業者が独自に提供しないように、契約書等で情報提供について定めること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏えいや、誤った閲覧（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させること。 (8) 保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。			レ	5	レ	7⑤			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 （Overview）		経営管理編 （Governance）		企画管理編 （Management）		システム運用編 （Control）		Q&A
		(9) 外部保存を受託する事業者を選定する際は、(1)から(8)のほか、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認証を取得していること 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機器が設置されている場所(地域、国) i　受託事業者に対する国外法の適用可能性			レ	5	レ	7⑥			
	D. 推奨されるガイドライン	1. ISMS認証を取得している事業者の選定に際しては、選定対象となる事業者に管理しているリスクに応じて、適合性を示す資料の提供を求めること。					レ				レ
		2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保するよう求めること。									レ
		3. 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を備えるよう求めること。									レ
8.4. 個人情報の保護	B.考え方	（略）			レ	4					
	C.最低限のガイドライン	1. 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 (1) 委託先を適切に監督すること 診療録等の外部保存を受託する事業者内の個人情報保護については、本ガイドライン6章を参照し、適切な管理を行わせる必要がある。			レ	5	レ	7⑧			
		2. 外部保存実施に関する患者への説明 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、理解を得る必要がある。 (1) 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。 (2) 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。 (3) 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。			レ	1.1、1.2	レ	7⑨			
9.1. 共通の要件	C.最低限のガイドライン	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。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンを行うこと。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版 （平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるため、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像をスキャンした情報はDICOM等の適切な形式で保存すること。					レ	16①	レ	16①	レ
		2. 改ざんを防止するため、次に掲げる対策を実施すること。 (1) スキャナによる読み取りについて運用管理規程に定めること。 (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) スキャナによる読み取りの際の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こと。なお、電子署名については6.12章を参照すること。			レ	4.1	レ	16①②③			
		3. 情報作成管理者は、運用管理規程に基づき、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こと。					レ	16④			
9.2. 診療等の都度スキャナ等で電子化して保存する場合	C.最低限のガイドライン	1. 9.1章の対策に加えて、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。 (1) 運用管理規程において、改ざんの動機が生じないと考えられる期間（長くとも1～2日程度以内）を定めるとともに、その期間内に遅滞なくスキャンを行わなければならない。時間外診療等で機器の使用ができない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行う必要がある。			レ	4.1	レ	16⑤			
9.3. 過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合	C.最低限のガイドライン	1. 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すること。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。			レ	4.1	レ	16⑥			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説（Overview）		経営管理編（Governance）		企画管理編（Management）		システム運用編（Control）		Q&A
		2. 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。 (1) 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）） (2) 作業責任者 (3) 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 (4) 相互監視を含む実施体制 (5) 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） (6) 事後の監査人と監査項目 (7) 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			レ	4.1	レ	16⑥			
		3. 医療機関等の保有するスキャナ等で電子化を行う場合、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。					レ	16⑥			
		4. 外部事業者に委託する場合は、9.1章の対策と同等以上の安全性を満たすことができる適切な事業者を選定すること。適切な事業者とみなすためには、少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認する必要がある。また、実施に際しては、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の監査を受けることを含め、安全管理に関する条項を契約書等に具体的に明記すること。			レ	4.1	レ	16⑥			
9.4. 紙の調剤済み処方箋をスキャナ等で電子化し保存する場合について	C.最低限のガイドライン	1. 紙の調剤済み処方箋の電子化のタイミングに応じて、9.2章又は9.3章の対策を実施すること。					レ	16⑦			
		2. 「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。					レ	16⑦	レ	16.1	
9.5（補足）　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	C.最低限のガイドライン	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ぐため、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。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンすること。これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからである。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできる。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版 （平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像情報をスキャンした情報はDICOM等の適切な形式で保存すること。					レ	16⑧	レ	16②	
		2. 情報作成管理者は、運用管理規程を定めて、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こと。					レ	16⑧			
		3. 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、保存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。					レ	16⑧			
		4. 電子化後の元の紙媒体やフィルムの安全管理を行うこと。					レ	16⑧			
10. 運用管理について	C.最低限のガイドライン	以下の項目を運用管理規程に含めること。本ガイドラインの 4 章から 9 章において「D. 推奨されるガイドライン」に記されている項目は省略しても差し支えない。 1. 一般管理事項			レ	4.1	レ	4.2、8.2.5など			
		2. 電子保存のための運用管理事項			レ	4.1	レ	15③～⑤			
		3. ネットワークによる外部保存に当たっての「医療機関等としての管理事項」 可搬媒体による外部保存、紙媒体による外部保存に当たっては、本項を参照して管理事項を作成すること。			レ	4.1	レ	15④			
		4. スキャナ等により電子化して保存する場合			レ	4.1	レ	16①、③～⑥			
		5. 運用管理規程の作成に当たって			レ	4.1	レ	4.2			

各編間相関表

経営管理編					企画管理編						システム運用編						
記載箇所			遵守事項			記載箇所			遵守事項			備考	記載箇所			遵守事項			備考
1．安全管理に関する責任・責務	1.1安全管理に関する法令の遵守		① 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。	–	5.2版のA項に関する前提を対策として新設														
			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。	–	5.2版のA項に関する前提を対策として新設	1．管理体系			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。				1．情報セキュリティの基本的な考え方			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。	10C2-4		
						1．管理体系			② 委託先の医療情報システム・サービス事業者等に対しても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。										
						1．管理体系			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。										
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
						14．法令で定められた記名・押印のための電子署名			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）～（e）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。【以下略】 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。												
	1.2 医療機関等における責任	通常時における責任																	
		【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。	–	5.2版第4の趣旨を踏まえて新設	4．医療情報の安全管理において必要な規程・文書類の整備			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。										
						4．医療情報の安全管理において必要な規程・文書類の整備			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。										
						4．医療情報の安全管理において必要な規程・文書類の整備			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。				2．システム設計・運用に必要な規程類と文書体系			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。	10C1-4		
													2．システム設計・運用に必要な規程類と文書体系			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。	10C1		
						4．医療情報の安全管理において必要な規程・文書類の整備			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。				2．システム設計・運用に必要な規程類と文書体系			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。	6.2C4 6.9C5		
													2．システム設計・運用に必要な規程類と文書体系			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。	6.2C4		
			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。	–	5.2版第4の趣旨を踏まえて新設	1．管理体系			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。										
						3．医療機関等における安全管理のための体制と責任・権限			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。										
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
						8．情報管理（管理、持出し、破棄等）			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。										
		【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。	6.3C1-5 第10章	–	1．管理体系			① 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。										
			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。	6.3C1-5 第10章	–	3．医療機関等における安全管理のための体制と責任・権限			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。										
		【定期的に見直し必要に応じて改善を行う責任】	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。	–	5.2版第5章の趣旨を踏まえて新設	10．運用に対する点検・監査			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、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。										
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
						12．サイバー攻撃対策			⑤ 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。										
			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。	–	5.2版6.2の趣旨を踏まえて新設	4．医療情報の安全管理において必要な規程・文書類の整備			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。										
						10．運用に対する点検・監査			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、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。										
						12．サイバー攻撃対策			⑤ 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。										
						15．技術的な対策の管理			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。										
		1．2．2 非常時における責任																	
		【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。	6.10C5	5.2版4.1B(2)①の趣旨を加味	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
						12．サイバー攻撃対策			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。										
						12．サイバー攻撃対策			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また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」（医政総発1029 第１号　医政地発1029 第３号　医政研発1029 第１号　平成30 年10 月29 日）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。										
			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。	–	5.2版6.10B(4)の趣旨を踏まえて新設	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										

		【善後策を講ずる責任】				12．サイバー攻撃対策			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。）											
			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。	–	5.2版4.1B(2)②の趣旨を踏まえて新設	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			⑨　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。											
		1.3.2　委託（第三者委託）における責任分界	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。	–	5.2版8.3の趣旨を踏まえて新設	1．管理体系			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。											
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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											
	1.3.1　委託（第三者委託）における責任					7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。）を勝手で分析、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。											
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。											
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。											
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。											
		1.3.2　委託（第三者委託）における責任分界	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及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。	6.11C6 10C1(7)	5.2版4.2の趣旨を加味	1．管理体系			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。											
	1.4　第三者提供における責任		①　医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。	–	5.2版4.2.2の趣旨を踏まえて新設	2．責任分界			①　医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。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。											
						5．安全管理におけるエビデンスの考え方			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　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。	–	5.2版4.2.2の趣旨を踏まえて新設	2．責任分界			④　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。				3．責任分界		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。		6．安全管理を実現するための技術的対策の体系	①　システム運用管	
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		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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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　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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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。											
						6．リスクマネジメント			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．リスクアセスメントを踏まえた安全対策の設計		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。				
						6．リスクマネジメント			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。											
						6．リスクマネジメント			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。				4．リスクアセスメントを踏まえた安全対策の設計		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。				
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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．システム設計・運用に必要な規程類と文書体系		③　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。				
													11．システム運用管理（通常時・非常時）		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。				

						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		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　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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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。										
					6．リスクマネジメント			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各安全管理対策を講じること。			4．リスクアセスメントを踏まえた安全対策の設計			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。			
											4．リスクアセスメントを踏まえた安全対策の設計			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。			
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	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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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各安全管理対策を講じること。			4．リスクアセスメントを踏まえた安全対策の設計			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。			
											4．リスクアセスメントを踏まえた安全対策の設計			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。			
		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。	6.2C4	リスク分析を踏まえた対応について新設	6．リスクマネジメント			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。										
	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	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。	－	5.2節(6.2.1の趣旨を踏まえて新設	6．リスクマネジメント			⑨　PDCA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。										
	2．2．3　リスク分析を踏まえた要求仕様適合性の管理	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。	6.2.3C4	－	6．リスクマネジメント			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各安全管理対策を講じること。										
					6．リスクマネジメント			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。										
3.1.統制	3．1．1　情報セキュリティ対策のための統制	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、適切に統制が機能されているかを確認すること。	6.3C5 第10章	統制についての記述は新設	1．管理体系			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。										
					1．管理体系			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。										
					1．管理体系			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。										
					3．医療機関等における安全管理のための体制と責任・権限			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。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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。										
					4．医療情報の安全管理において必要な規程・文書類の整備			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．医療情報の安全管理において必要な規程・文書類の整備			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。										
	3．1．2　医療情報システムにおける統制上の留意点	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。	6.3C1 付表	－														
		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。	6.3C1		3．医療機関等における安全管理のための体制と責任・権限			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。										
					3．医療機関等における安全管理のための体制と責任・権限			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．医療機関等における安全管理のための体制と責任・権限			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。										
					3．医療機関等における安全管理のための体制と責任・権限			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。										
					3．医療機関等における安全管理のための体制と責任・権限			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。										
		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。	－	統制の趣旨を踏まえ新設														
		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。	－	統制と6.6の趣旨を踏まえ新設	7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
3．2　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	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。	10C1(1)a	－	1．管理体系			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。										
		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。	－	6.3の趣旨を踏まえ新設	7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
	3．2．2　情報セキュリティ対策を踏まえた訓練・教育	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。	6.6C1(2) 6.10C2	－	3．医療機関等における安全管理のための体制と責任・権限			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．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
3．3　安全管理対策の管理	3．3．1　安全管理状況の自己点検	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。	１０C1(2)c	－	5．安全管理におけるエビデンスの考え方			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。			１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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。			
					5．安全管理におけるエビデンスの考え方			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。			１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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。			
											１７．証跡のレビュー・システム監査			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。			
					5．安全管理におけるエビデンスの考え方			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。										
					5．安全管理におけるエビデンスの考え方			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。										
					8．情報管理（管理、持出し、破棄等）			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。										
		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。	－	4.1(1)の趣旨を踏まえて新設	3．医療機関等における安全管理のための体制と責任・権限			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。										

						10．運用に対する点検・監査		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。										
		３．３．２　情報セキュリティ監査				10．運用に対する点検・監査		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。										
						10．運用に対する点検・監査		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。										
						10．運用に対する点検・監査		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、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。				１７．証跡のレビュー・システム監査			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。			
			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。	－	4.1(1)の趣旨を踏まえて新設	10．運用に対する点検・監査		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、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。				１７．証跡のレビュー・システム監査			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。			
３．安全管理全般（統制、設計、管理等）			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、BCP等を整備すること。	6.10C1	－	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		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。										
						11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		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。										
						12．サイバー攻撃対策		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。）										
						12．サイバー攻撃対策		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」（医政総発1029第１号　医政地発1029第３号　医政研発1029第１号　平成30年10月29日）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。										
			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。	6.10C2-4	－	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		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。				１１．システム運用管理（通常時・非常時等）			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。			
													１１．システム運用管理（通常時・非常時等）			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。			
		３．４．１　事業継続計画（BCP：Business Continuity Plan）の整備と訓練	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。	－	6.10の趣旨を踏まえて新設	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		⑦　非常時への対応状況を定期的に確認し、経営層に報告のうえ、承認を得ること。										
						12．サイバー攻撃対策		④　サイバーセキュリティ対応計画を踏まえ、対応状況を確認する。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。				１１．システム運用管理（通常時・非常時等）			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。 －　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。			
													１８．外部からの攻撃に対する安全管理措置			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）			
													１１．システム運用管理（通常時・非常時等）			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。			
						12．サイバー攻撃対策		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。										
						12．サイバー攻撃対策		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。										
		３．４　情報セキュリティインシデントへの対策と対応	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。	－	6.10B(4)の趣旨を踏まえて新設	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定		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。				１１．システム運用管理（通常時・非常時等）			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。			
													１８．外部からの攻撃に対する安全管理措置			①　医療情報システムに対する不正ソフトウェア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）			

					11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
					11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。										
３．４．２　情報共有・支援、情報収集					11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			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。				１１．システム運用管理（通常時・非常時等）			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。			
					12．サイバー攻撃対策			②　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、経営層に報告し、承認を得ること。				１８．外部からの攻撃に対する安全管理措置			①　医療情報システムに対する不正ソフトウェア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）			
					12．サイバー攻撃対策			③　サイバーセキュリティ対応計画を踏まえ、その内容を各規程や手順等に反映すること。										
		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。		6.2.3C5の趣旨から新設	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			④　非常時の事象発生への対応等に関して、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。				１１．システム運用管理（通常時・非常時等）			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。			
					12．サイバー攻撃対策			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・見直しも実施し、必要に応じて対応計画等の改善を行うこと。										
３．４．３　情報セキュリティインシデントへの対応体制		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や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。	6.10C5	－	12．サイバー攻撃対策			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。）										
					12．サイバー攻撃対策			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」（医政総発1029 第１号　医政地発1029 第３号　医政研発1029 第１号　平成30 年10 月29 日）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。										
		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、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。	6.10C5	－	11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定			⑧　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。										
		①　医療情報システムの安全管理に必要な対策項目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。	6-7章	－	８．情報管理（管理、持出し、破棄等）			①　医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順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。				７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
					８．情報管理（管理、持出し、破棄等）			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。				７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
					８．情報管理（管理、持出し、破棄等）			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。				１２．物理的安全管理措置			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。			
												１２．物理的安全管理措置			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。			
					８．情報管理（管理、持出し、破棄等）			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。				４．リスクアセスメントを踏まえた安全対策の設計			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。			
												７．情報の持出し・管理・破棄等			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に関する手順を作成し、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．情報管理（管理、持出し、破棄等）			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。				７．情報の持出し・管理・破棄等			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。			
					８．情報管理（管理、持出し、破棄等）			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．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			
												７．情報の持出し・管理・破棄等			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。			

														7．情報の持出し・管理・破棄等			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．情報の持出し・管理・破棄等			⑦　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。			
														7．情報の持出し・管理・破棄等			⑧　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。			
					8．情報管理（管理、持出し、破棄等）			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。				7．情報の持出し・管理・破棄等			⑨　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。			
														7．情報の持出し・管理・破棄等			⑩　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。			
					8．情報管理（管理、持出し、破棄等）			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。				7．情報の持出し・管理・破棄等			⑦　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。			
														7．情報の持出し・管理・破棄等			⑧　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。			
														7．情報の持出し・管理・破棄等			⑨　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。			
					8．情報管理（管理、持出し、破棄等）			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。				7．情報の持出し・管理・破棄等			⑤　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。			
														7．情報の持出し・管理・破棄等			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。			
														7．情報の持出し・管理・破棄等			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。			
					8．情報管理（管理、持出し、破棄等）			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。				7．情報の持出し・管理・破棄等			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。			
					9．医療情報システムに用いる機器等の資産管理			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。）											
					9．医療情報システムに用いる機器等の資産管理			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。											
					9．医療情報システムに用いる機器等の資産管理			③　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。				8．利用機器・サービスに対する安全管理措置			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併せて確認すること。			
					9．医療情報システムに用いる機器等の資産管理			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。				8．利用機器・サービスに対する安全管理措置			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。			
					9．医療情報システムに用いる機器等の資産管理			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。											
					9．医療情報システムに用いる機器等の資産管理			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。				8．利用機器・サービスに対する安全管理措置			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。			
												8．利用機器・サービスに対する安全管理措置			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。			
					9．医療情報システムに用いる機器等の資産管理			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。				8．利用機器・サービスに対する安全管理措置			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。			
					13．医療情報システムの利用者に関する認証等及び権限			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。											
					13．医療情報システムの利用者に関する認証等及び権限			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。				14．認証・認可に関する安全管理措置			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。			
												14．認証・認可に関する安全管理措置			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。			
												14．認証・認可に関する安全管理措置			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。。			
												14．認証・認可に関する安全管理措置			④　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策を行うこと。			
												14．認証・認可に関する安全管理措置			⑤　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て等があってはならない）。			
					13．医療情報システムの利用者に関する認証等及び権限			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。				14．認証・認可に関する安全管理措置			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。			

					13．医療情報システムの利用者に関する認証等及び権限			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知識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。				１４．認証・認可に関する安全管理措置			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。			
																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。			
					13．医療情報システムの利用者に関する認証等及び権限			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。				１４．認証・認可に関する安全管理措置			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。			
																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。			
					13．医療情報システムの利用者に関する認証等及び権限			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。				１４．認証・認可に関する安全管理措置			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。			
																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。			
					13．医療情報システムの利用者に関する認証等及び権限			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。				１４．認証・認可に関する安全管理措置			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。			
												１４．認証・認可に関する安全管理措置			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。			
					13．医療情報システムの利用者に関する認証等及び権限			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				１４．認証・認可に関する安全管理措置			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。			
												１４．認証・認可に関する安全管理措置			⑧　電子カルテにおける記録の確定手順の確定と、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者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。			
					14．法令で定められた記名・押印のための電子署名			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。【以下略】 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、関係省資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。				１５．電子署名、タイムスタンプ			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。			
					14．法令で定められた記名・押印のための電子署名			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。										
					15．技術的な対策の管理			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。				１２．物理的安全管理措置			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。			
					15．技術的な対策の管理			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。医療機関等の施設外からの入力・参照等が可能な端末等についても同様である。				１２．物理的安全管理措置			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を設置されていることを確認すること。			
												１２．物理的安全管理措置			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。			
					15．技術的な対策の管理			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。										
					15．技術的な対策の管理			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。				１１．システム運用管理（通常時・非常時等）			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。			
												１２．物理的安全管理措置			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。			

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													１８．外部からの攻撃に対する安全管理措置			①　医療情報システムに対する不正ソフトウェア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）			
					15．技術的な対策の管理		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。					１２．物理的安全管理措置			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。			
					15．技術的な対策の管理		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。					８．利用機器・サービスに対する安全管理措置			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。			
												８．利用機器・サービスに対する安全管理措置			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。			
												８．利用機器・サービスに対する安全管理措置			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。			
												８．利用機器・サービスに対する安全管理措置			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。			
												８．利用機器・サービスに対する安全管理措置			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。			
												８．利用機器・サービスに対する安全管理措置			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。			
												１８．外部からの攻撃に対する安全管理措置			①　医療情報システムに対する不正ソフトウェア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）			
					15．技術的な対策の管理		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。					１３．ネットワークに関する安全管理措置 【遵守事項】			①　ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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、erberos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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
												１３．ネットワークに関する安全管理措置 【遵守事項】			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。			

														１３．ネットワークに関する安全管理措置 【遵守事項】			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。			
														１３．ネットワークに関する安全管理措置 【遵守事項】			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．ネットワークに関する安全管理措置 【遵守事項】			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。 － 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。			
														１８．外部からの攻撃に対する安全管理措置			①　医療情報システムに対する不正ソフトウェア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）			
				15．技術的な対策の管理				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。						７．情報の持出し・管理・破棄等			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。			
														７．情報の持出し・管理・破棄等			③　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。			
														８．利用機器・サービスに対する安全管理措置			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。			
														９．ソフトウェア・サービスに対する要求事項			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。			
														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			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。			
														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			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。			
														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			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。			
														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			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。			
														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			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。			
														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			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。			
					15．技術的な対策の管理			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．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			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。			
														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			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。			
														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			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。			
				15．技術的な対策の管理				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。						９．ソフトウェア・サービスに対する要求事項			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。			
														９．ソフトウェア・サービスに対する要求事項			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。			
				15．技術的な対策の管理				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。						９．ソフトウェア・サービスに対する要求事項			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。			
														９．ソフトウェア・サービスに対する要求事項			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。			
				15．技術的な対策の管理				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。						９．ソフトウェア・サービスに対する要求事項			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。			
														９．ソフトウェア・サービスに対する要求事項			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。			
				15．技術的な対策の管理				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。						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）			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。			
														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）			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。			
														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）			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継持すること。			
														５．システム設計の見直し（標準化対応、新規技術導入のための評価等）			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。			
														９．ソフトウェア・サービスに対する要求事項			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。			

																修　電子カルテシステム等における記録の確定手順の確立と一連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。			
					16.　紙媒体等で作成した医療情報の電子化		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。				14．認証・認可に関する安全管理措置			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。			
					16.　紙媒体等で作成した医療情報の電子化		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。				16．紙媒体等で作成した医療情報の電子化			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。			
					16.　紙媒体等で作成した医療情報の電子化		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。													
					16.　紙媒体等で作成した医療情報の電子化		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。				16．紙媒体等で作成した医療情報の電子化			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。			
					16.　紙媒体等で作成した医療情報の電子化		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。												
					16.　紙媒体等で作成した医療情報の電子化		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。												
					16.　紙媒体等で作成した医療情報の電子化		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。				16．紙媒体等で作成した医療情報の電子化			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、以下の措置を講じること。 ・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ぐため、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。 ・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.　紙媒体等で作成した医療情報の電子化		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管を行う場合、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。												
			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。	－	6.2.1の趣旨から新設	15.　技術的な対策の管理			14　①～⑧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。										
4．2　必要な措置			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。	6.2.3C7	－	1．管理体系			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。										
5.1　事業者選定			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システム関連事業者を選定するよう指示すること。	8.3C2	－														
			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。	8.3C2(9)f	2者ガイドラインとの整合性確保														
			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。	－	4.2の趣旨から新設	7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。										
	5．2．1　契約管理					7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）			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。				7．情報の持出し・管理・破棄等			⑨　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。			
5．2　事業者管理											7．情報の持出し・管理・破棄等			⑩　患者等に医療情報を閲覧させる場合、医療情報を公開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。			

5．医療情報システム・サービス事業者との協働						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）		②　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委託した医療情報を分析等の目的で取り扱わないこと。 －　保存を委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アクセス権を設定し、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。				7．情報の持出し・管理・破棄等			③　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。			
													7．情報の持出し・管理・破棄等			④　患者等に医療情報を閲覧させる場合、医療情報を公開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。			
						7．安全管理のための人的管理（従業者管理、委託先管理、教育・訓練、委託先選定・契約）		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。										
		5．2．2　体制管理	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。	6.6C2(1)d 10C1(5)b		3．医療機関等における安全管理のための体制と責任・権限		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。										
	5.3　責任分界管理		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。	－	4.2.1の題旨から新設	2．責任分界		①　医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。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．責任分界		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			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．責任分界		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。				3．責任分界			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。			
						2．責任分界		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。				3．責任分界			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。			
												3．責任分界			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。			
						2．責任分界		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。				3．責任分界			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。			
												3．責任分界			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。			

参照文書リンク集

	文書名	制定・公表	主体	最新	参照先リンク①	参照先リンク②	参照先リンク③
1	個人情報の保護に関する法律	平成15年法律第57号	法律	令和3年法	https://elaws.e-gov.go.jp/document?lawid=415AC0000000057		
2	行政機関の保有する個人情報の保護に関する法律	平成15年法律第58号	法律	令和3年法律第37号による廃止	https://elaws.e-gov.go.jp/document?lawid=415AC0000000058		
3	独立行政法人等の保有する個人情報の保護に関する法律	平成15年法律第59号	法律	令和3年法律第37号による廃止	https://elaws.e-gov.go.jp/document?lawid=415AC0000000059		
4	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	法律	令和3年法律第36号による改正	https://elaws.e-gov.go.jp/document?lawid=416AC0000000149		
5	電子署名及び認証業務に関する法律	平成12年5月	法律	令和4年法律第68号による改正	https://elaws.e-gov.go.jp/document?lawid=412AC0000000102		
6	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	法律	令和4年法律第68号による改正	https://elaws.e-gov.go.jp/document?lawid=414AC0000000153		
7	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律	昭和35年法律第145号	法律	令和4年法律第47号による改正	https://elaws.e-gov.go.jp/document?lawid=335AC0000000145		
8	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日発出	厚生労働大臣	令和4年厚生労働省令第75号による改正	https://elaws.e-gov.go.jp/document?lawid=417M60000100044		
9	政府情報システムにおけるクラウドサービスの利用に係る基本方針	令和4年9月30日初版決定	デジタル社会推進会議幹事会決定	令和4年12月28日最終改定	https://www.digital.go.jp/resources/standard_guidelines/	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/17ef852e/2022	
10	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日発出	厚生労働省	平成19年3月30日発出	https://www.mhlw.go.jp/web/t_doc?dataId=00tb3561&dataType=1&page		
11	「診療録等の保存を行う場所について」の一部改正について	平成25年3月25日発出	厚生労働省	平成25年3月25日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html		
12	「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」の一部改正について	平成28年3月31日発出	厚生労働省	平成28年3月31日発出	https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000120128.pdf		
13	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	平成27年4月28日発出	厚生労働省	平成27年4月28日発出	https://www.pmda.go.jp/files/000204891.pdf		
14	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日発出	厚生労働省	平成30年10月29日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html	https://www.mhlw.go.jp/content/10808000/001011697.pdf	
15	ランサムウエアによるサイバー攻撃に関する注意喚起	令和3年4月30日発出	内閣官房内閣サイバーセキュリティセンター（NISC）	令和3年4月30日発出	https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf		
16	時刻認証業務の認定に関する規程	令和3年4月1日制定	総務省	令和3年4月1日制定	https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html	https://www.soumu.go.jp/main_content/000742664.pdf	
17	個人情報の保護に関する法律についてのガイドライン（通則編）	平成29年5月公表	個人情報保護委員会	令和4年9月改正	https://www.ppc.go.jp/personalinfo/legal/guidelines_administrative/		

18	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	平成29年4月14日	個人情報保護委員会 厚生労働省	令和4年3月一部改正	https://www.mhlw.go.jp/content/000909511.pdf	https://www.ppc.go.jp/personalinfo/legal/iryoukaigo_guidance/	
19	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	令和2年8月21日策定	経済産業省 総務省	令和3年8月31日改定	https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html		
20	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）	令和3年7月7日策定	内閣官房内閣サイバーセキュリティセンター（NISC）	令和4年12月12日一部改定	https://www.nisc.go.jp/policy/group/general/kijun.html		
21	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）	令和2年7月17日公表	総務省 法務省 経済産業省	令和2年7月17日公表	https://www.meti.go.jp/covid-19/denshishomei_qa.html	https://www.moj.go.jp/MINJI/denshishomeihou.html	
22	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）	令和2年9月4日公表	総務省 法務省 経済産業省	令和2年9月4日公表	https://www.meti.go.jp/covid-19/denshishomei3_qa.html		
23	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－	平成16年11月5日公表	総務省	平成16年11月5日公表	https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html	https://www.soumu.go.jp/main_content/000485112.pdf	
24	医療機器のサイバーセキュリティの確保に関するガイダンス	平成30年7月24日発出	厚生労働省	平成30年7月24日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html	https://www.mhlw.go.jp/content/10808000/001011666.pdf	
25	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）	平成26年に初版公表	総務省	令和3年9月公表	https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html	https://www.soumu.go.jp/main_content/000771516.pdf	
26	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	令和4年10月策定	総務省	令和4年10月策定	https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00149.html	https://www.soumu.go.jp/main_content/000843318.pdf	
27	厚生労働省標準規格	平成22年3月31日医政発0331第1号	厚生労働省	令和4年3月24日改正	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html	http://helics.umin.ac.jp/helicsStdList.html	
28	JIS Q 27001（情報セキュリティマネジメントシステム）	平成18年5月20日制定	経済産業大臣	平成26年3月20日最終改正	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?toGnrJISStandardDetailList		
29	ISO14533-1：2014CMS利用電子署名(CAdES)の長期署名プロファイル	平成26年12月策定	ISO/TC154	ISO 14533-1:2022が最新（令和4年6月策定）	https://www.iso.org/standard/64756.html	https://www.iso.org/standard/81814.html	
30	ISO14533-2:2021XML署名利用電子署名(XAdES)の長期署名プロファイル	令和3年8月策定	ISO/TC154	令和3年8月策定	https://www.iso.org/standard/79129.html		
31	ISO14533-3:2017PDF長期署名プロファイル(PAdES)	平成29年9月策定	ISO/TC154	平成29年9月策定	https://www.iso.org/standard/67937.html		
32	JIS Q 15001（個人情報保護マネジメントシステム）	平成11年3月20日制定	（原案作成）一般財団法人日本情報経済社会推進協会（JIPDEC）	2017年12月20日改正	https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+Q+15001%3A2017		
33	「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書	平成19年2月公表	保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム（HEASNET）	平成19年2月公表	http://www.heasnet.jp/open/report.php?data=report_docs		
34	TLS暗号設定ガイドライン3.0.1版	平成27年5月8日初版発行	独立行政法人情報処理推進機構	令和2年7月8日改定	https://www.cryptrec.go.jp/op_guidelines.html		
35	『製造業者・サービス事業者による医療情報セキュリティ開示書』ガイド	令和3年3月公表	一般社団法人保健医療福祉情報システム工業会（JAHIS）	令和3年3月公表	https://www.jahis.jp/standard/detail/id=779		

36	IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省；平成 28 年 7 月）	平成28年7月5日公表	IoT 推進コンソーシアム 総務省 経済産業省	平成28年7月5日公表	https://www.ipa.go.jp/security/iot/	http://www.iotac.jp/wg/security/	
37	標的型攻撃メールへの対処について	平成28年4月28日公表	日本医療情報学会	平成28年4月28日公表	https://www.jami.jp/medicalFields/	https://www.jami.jp/medicalFields/Documents/targetedmailattack.pdf	
38	IPA対策のしおりシリーズ	平成24年1月30日第1版策定	情報処理推進機構（IPA）	令和2年9月4日最終更新	https://www.ipa.go.jp/security/antivirus/shiori.html		
39	デジタル画像の取り扱いに関するガイドライン 3.0 版（平成 27 年 4 月）	平成11年4月公表	日本医学放射線学会電子情報委員会	平成27年4月改定	http://www.radiology.jp/member_info/guideline/20150417.html	http://www.radiology.jp/content/files/20150417.pdf	http://www.radiology.jp/member_info/guideline/20060402.html
40	個人情報保護に役立つ監査証跡ガイド～あなたの病院の個人情報を守るために～（医療情報システム開発センター）	平成19年3月発行	一般財団法人医療情報システム開発センター（MEDIS）	平成19年3月発行	https://www.medis.or.jp/7_kikaku/hanbai/hanbai.html		

安全管理ガイドラインの改定の経緯に関する年表

個人情報保護法及びその関連法令等
e-文書法及びその関連法令等
総務省・経済産業省ガイドライン（3省4ガイドライン→3省3ガイドライン→3省2ガイドライン）
外部保存通知

	年度	法改正・政府の動き等			安全管理ガイドライン策定のための会議体での検討	医療情報システムの安全管理に関するガイドライン（安全管理ガイドライン）の改定
		個人情報関係	e-文書法及びその関連法令等	その他		
作成以前	1988（昭和63）年		1988（昭和63）年　診療録等の記載方法等について			
	1994（平成6）年		1994（平成6）年4月　エックス線写真等の光磁気ディスク等への保存について			
	1999（平成11）年		1999（平成11）4月 厚生省通知「診療録等の電子媒体による保存について」及び「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」			
	2002（平成14）年		2002（平成14）年3月 厚生労働省通知「診療録等の保存を行う場所について」（**外部保存通知**）			
			2002（平成14）年5月 厚生労働省「診療録等の外部保存に関するガイドライン」 →診療録等の電子保存及び保存場所に関する要件等が明確化			
	2004（平成16）年		2004（平成16）年11月 「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」（**e-文書法**）			
		2004（平成16）年 **個人情報保護法成立**				
		2004（平成16）年12月 **「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ドライン」**				
	2005（平成17）年		2005（平成17）年3月 厚生労働省令「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」（**e-文書法省令**）			
		2005（平成17）年4月 「個人情報の保護に関する法律」施行（**個人情報保護法**）				
第1版						**2005（平成17）年3月　第1版公開** **e-文書法・省令、個人情報保護法への対応としてガイドラインを新設** （e-文書法令の別添として） 「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」及び「診療録等の外部保存に関するガイドライン」を見直し、さらに、個人情 報保護に資する情報システムの運用管理に関わる指針と e-文書法への適切な対応を行うた めの指針を統合して作成
第2版				2005（平成17）年9月 情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る基本的考え方」発表 →医療を「重要インフラ」として位置づけ	2006（平成18）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療機関等で用いるのに適した**ネットワークに関するセキュリティ**要件定義 （2）**自然災害・サイバー攻撃**による IT 障害対策等	
	2006（平成18）年			2006（平成18）年1月 高度情報通信技術戦略本部（IT 戦略本部）から、「IT 新改革戦略」が発表 →「安全なネットワーク基盤の確立」を掲げる		
	2007（平成19）年					**2007（平成19）年3月　第2版公開** ネットワーク基盤の安全性、災害・サイバー攻撃への対応を追加 ●ネットワークの要件を定義し、「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」を新設 ●医療における災害、サイバー攻撃対策に対する指針として「6.9災害等の非常時の対応」を新設 ●「6.2 医療機関における情報セキュリティマネジメント（ISMS）の実 践」でISMSの概念を導入 ・その他関連する箇所の修正
第3版		2007（平成19）年3月 「IT 新改革戦略評価専門調査会 2006 年度報告書」公表 →処方箋の電子化について言及			2007（平成19）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療情報の取扱に関する事項 **→医療従事者とそれ以外の事業者等との責任分界** （2）処方箋の電子化に関する事項 →医療情報ネットワーク基盤検討会提言「処方せんの電子化について」（第4.2版でガイドラインに対応） （3）**無線・モバイル**を利用する際の技術的要件に関する事項	
	2008（平成20）年					**2008（平成20）3月　第3版公開** **責任分界の追加** **●医療従事者とその他の関係者が医療・健康情報を取り扱う際の責任のあり方を定め「4 電子的な医療情報を扱う際の責任のあり方」を取りまとめ** **→「8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」を改定** **無線・モバイルといった新技術への対応** **●無線・モバイルを利用する際の脅威や技術的要件について6章を加筆** **→特にネットワークのあり方については「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」に取りまとめ** **→盗難や紛失といった新たなリスクについて、「6.9 情報及び情報機器の持ち出しについて」を新設**
第4版					2008（平成20）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療分野における電子化された情報管理の在り方に関する事項 **→体系的な見直し** （2）個人が自らの医療情報を管理・活用するための方策等に関する事項	**2009（平成21）年3月　第4版公開** **体系的な見直し** ●本ガイドラインに準じて取り扱うものとして、「3.3 取扱いに注意を要する文書等」を新設 ●「5 情報の相互運用性と標準化について」を全面改定 ●「6.1 方針の制定と公表」について、JIS Q 15001:2006をもとに説明し C 項を新設 ●「6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」においてC、D項を新設 ●「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」においてB、D項に従業者による外部からのアクセスに関する事項を追加 ●7章の大幅改定 「7.1 真正性の確保について」：B項簡略化、C項見直し、D項削除 「7.2 見読性の確保について」：B項簡略化、C項・D項の整理 「7.3 保存性の確保について」：C項、D項で大幅な見直し ●8章「診療録及び診療諸記録を外部の保存する際の基準」：2省ガイドラインとの整合を明確化
第4.1版		2008（平成20）年 1 月 総務省「ASP･SaaSにおける情報セキュリティ対策ガイドライン」（「**ASP･SaaSセキュリティガイドライン**」）			2009年11月 医療情報ネットワーク基盤検討会提言 「診療録等の保存を行う場所に関する提言」	
		2008（平成20）年 7 月 経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（「**情報処理事業者ガイドライン**」）				
	2009（平成21）年	2009（平成21）7月 総務省「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（「**ASP･SaaS 事業者ガイドライン**」）策定 →外部保存に対する対応方法が明確化			2009年11月 医療情報ネットワーク基盤検討会提言 「診療録等の保存を行う場所に関する提言」	
					2009（平成21）年度 医療情報ネットワーク基盤検討会検討事項 ・診療録等の保存を行う場所について ・「医療情報システムの安全管理に関するガイドライン」等の改正について	
	2010（平成22）年	2010（平成22）年2月 厚生労働省**外部保存通知の一部改正**（民間事業者が設置するデータセンターへの保存を解禁）				**2010（平成22）年2月　第4.1版公開** **総務省・経済産業省ガイドラインの策定と外部保存通知の改正に合わせた対応** **●「4.3 例示による責任分界点の考え方の整理」：（4）オンライン外部保存を委託する場合」を追加** **●「8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」** **●10章：4章、8章に合わせて修正**
第4.2版		**処方箋の電子化・電磁交付に向けた動き** 2010（平成22）年6月　「規制・制度改革に係る対処方針」「「国民の声集中受付月間（第１回）」において提出された提案等への対処方針について」閣議決定 2010（平成22）年6月　「新たな情報通信技術戦略工程表」IT 戦略本部決定 2011（平成 23）年8月　「情報通信技術利活用のための規制・制度改革に係る対処方針」IT 戦略本部決定				**2013（平成25）年10月　第4.2版公開** **調剤済み処方箋及び調剤録等の外部保存への対応** **●3章：調剤録の外部保存に関する事項を追加、「3.3 調剤済み処方箋と調剤録の電子化・外部保存について」追加** **●9章：紙の処方箋を電子化する方法について追加** **大規模災害時の対応** **●「6.10 災害等の非常時の対応」：大規模災害時を想定した事業継続計画（BCP）の作成等の考え方を追加** **●上記に合わせ、その他の章を適宜修正**
	2011（平成 23）					
	2012（平成24）年				2012（平成24）年4月 医療情報ネットワーク基盤検討会提言 「処方箋の電子化に向けて」	
					2012（平成24）年度 医療情報ネットワーク基盤検討会検討事項 ・処方箋の電子化について	
	2013（平成25）年	2013（平成25）年3月 厚生労働省**外部保存通知の一部改正**（調剤済み処方箋及び調剤録等の外部保存を解禁）			2013（平成25）年3月 医療情報ネットワーク基盤検討会提言 「電子処方箋の実現について」	
					2013（平成25）年9月 医療情報ネットワーク基盤検討会提言 「電子処方箋の実現に向けた工程表」	
第4.3版	2015（平成27）年				2015（平成27）年度 医療情報ネットワーク基盤検討会検討事項 （１）電子処方せんの運用ガイドライン（案）について	
	2016（平成28）年	2016（平成28）3月 厚生労働省**e-文書法省令の一部改正**			2016（平成28）年3月 電子処方せんの運用ガイドラインの策定	**2016（平成28）年3月　第4.3版公開** **処方箋の電磁的記録による取扱いの運用は「電子処方せんの運用ガイドライン」を参照するものとする** ●関連する３，８，９省の一部を修正

個人情報保護法及びその関連法令等
e-文書法及びその関連法令等
総務省・経済産業省ガイドライン（3省4ガイドライン→3省3ガイドライン→3省2ガイドライン）
外部保存通知

	年度	法改正・政府の動き等			安全管理ガイドライン策定のための会議体での検討	医療情報システムの安全管理に関するガイドライン（安全管理ガイドライン）の改定
第5版	2017（平成29）年	2017（平成29）年 **改正個人情報保護法施行**			2017（平成29）年度 医療情報ネットワーク基盤検討会検討事項 （１）「医療情報システムの安全管理に関するガイドライン」の改定について	**2017（平成29）年5月　第5版公開** **改正個人情報保護法等への対応** ●1章：本ガイドラインの対象に、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における電子的な医療情報の取扱いに係る責任者が含まれることを明確化 ●3章：1章を踏まえて、介護事業者が取り扱う文書で7章及び9章の対象となる文書を列挙 ●4章「4.2.2 第三者提供における責任分界」：改正個人情報保護法で新たに規定された義務について関係資料を参照 **4.2版公表以降に追加された標準規格等への対応** ●5章：厚生労働省標準規格・JAHIS標準規約を追加。日本 IHE 協会の「地域医療連携における情報連携基盤技術仕様」について記述を新設 ●6章：「6.1 方針の制定と公表」及び「6.2 医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」において所要の改定 **新たなセキュリティリスクへの対応** ●6章 ・6.2 章：「『製造業者による医療情報セキュリティ開示書』ガイド」に関する記述の追加 ・「6.5 技術的安全対策」：できるだけ早期に二要素認証を実装することを求め、かつパスワード要件について追記、「（6）医療等分野における IoT 機器の利用」を新設 ・「6.6 人的安全対策」及び「6.10 災害、サイバー攻撃等の非常時の対応（改題）」：サイバー攻撃等への事前及び事後の対応や連絡先等について規定を新設 ・「6.9 情報及び情報機器の持ち出しについて」：公衆無線LAN、BYODについて追記 ・「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」：オープンなネットワークを介した SSL/TLS 接続における遵守事項や留意点を追記 **その他** ●「6.12 法令で定められた記名・押印を電子署名で行うことについて」：国家資格の証明が求められる文書に対する考え方や取扱いについて追記 ●「7.1 真正性の確保について」：電子カルテ等の入力における関係者の役割や責任をより明確にするとともに、代行入力を行う場合の記録確定に当たって遵守すべき事項を追記 ●「7.3 保存性の確保について」において、医療機関等が文書を保存する際の将来の互換性の確保について、規定を設けた。 ●10章他、上記に合わせた修正
		2017（平成29）年 「個人情報の保護に関する法律についてのガイドライン（通則編）」（**通則ガイドライン**）施行				
		2017（平成29）年4月 「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」				
		2017（平成29）年5月 平成27年**改正個人情報保護法施行**				
第5.1版	2018（平成30年）年	2018（平成30年）年7月 総務省「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2版）」改定 （初版策定は2014年（平成26）年4月）				
		2018（平成30年）年7月 総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」 （**「クラウド事業者ガイドライン」**）（**総務省の2ガイドラインを統合**） ASP･SaaS セキュリティガイドラインにおける医療情報に関する内容と ASP･SaaS 事業者ガイドラインの内容を１つのガイドラインに統合するとともに、ガイドラインの対象を ASP･SaaS 事業者だけではなく PaaS や IaaS 等のクラウドサービス事業者も対象とする				
	2019(平成31年／令和元年)				健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ 検討事項 ・保健医療情報を全国の医療機関等で確認できる仕組み及び標準的な医療情報システムについて ・電子処方箋について ・医療情報システムの安全管理に関するガイドライン改定素案について	
	2020（令和2）年	2020（令和2）年8月 総務省・経済産業省「医療等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」（**2省ガイドライン**）策定				
	2021（令和3）年					**令和3年1月　第5.1版公開** **サイバー攻撃の多様化・巧妙化への対応** **●6章：以下の追記** ・「6.2.3 リスク分析」（管理されていない機器やソフトウェア、サービス等の利用等のリスク） ・「6.5 技術的安全対策」及び「6. 11 外部と個人情報を含む医療情報を交換する場合の安全管理」（ネットワークの監視等の措置やネットワークの構築のあり方、外部からのデータ取り込みにおける対応措置等の必要性） ・「6.5 技術的安全対策」（二要素認証導入を促す方針をさらに進めるため、B、 C 項の改定、暗号鍵の管理に関する内容も新規に規定） ・「6.10 災害、サイバー攻撃等の非常時の対応」（非常時の体制構築） **新技術への対応（スマホの普及、クラウドサービス、ネットワークサービス）** ●4章：クラウドサービスの概要を示すとともに、「4.3 例示による責任分界点の考え方の整理」に追記 ●「8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」：行政機関等又は民間事業者が設置するデータセンターに関する選定の在り方、受託事業者の選定（Cookie 等の取扱いに関する事項、受託事業者に対する国内法の適用、求められる認証や提供すべきセキュリティ情報）について追記 **関連ガイドライン等との整合** ●関連法規の改正に伴う部分の修正
第5.2版	2022（令和4）年	2021（令和3）年4月 総務省告示「時刻認証業務の認定に関する規程（令和3年総務省告示第146号）」 **→タイムスタンプ認定制度開始**			健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ 検討事項 ・データヘルス集中改革プラン等の主な論点と検討の方向性について ・データヘルス改革に関する工程表について ・医療情報ネットワークの基盤に関するワーキンググループの設置について ・医療情報システムの安全管理に関するガイドラインについて ・電子処方箋の仕組みの構築について ・民間PHR事業者による健診等情報の取扱いに関する基本的指針について	
		2022（令和4）年3月 「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」一部改正				**2022（令和4）年3月　第5.2版公開** **本編と別冊編に分離** ●本ガイドラインについての理解をより促す観点から、安全対策として実施すべき内容に直接関係する部分と、安全対策を行う上での背景となる考え方や例示などの部分を分けて記述 **ランサムウェアに代表される攻撃への対策** ●6.2章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一覧（設置事業者等含む）を整備する旨追記 ●6.10 章：サイバー攻撃対応としてのバックアップのあり方等の対策を示す **関連する制度等の状況の反映** ●6.12章：電子署名が求められる文書の長期保存に必要なタイムスタンプについて、総務大臣の認定制度が創設されたことに伴う修正、JIS から ISO に参照規格を変更、リモート署名や立会人型電子署名など新たな利用形態が普及しつつあることを踏まえて、電子署名に関する 6.12 章の記載を整理 ●8.3章：2省ガイドラインとの整合（外部保存を行う際の事業者の選定） **その他** ●6.9章：BYOD利用時の安全な環境について追記 ●全体的な表現の修正
		2022（令和4）年4月 改正個人情報保護法施行				