# 画像情報の確定に関するガイドライン

## 第 2.2 版

公益社団法人　日本放射線技術学会

令和 7 年 4 月 1 日（2025 年 4 月 1 日）

# 目次

## 1. はじめに

画像情報の電子化は、フィルムレスをはじめとする医療機関内の医用画像の取り扱いにまつわる利便性向上だけでなく、より診断に適した情報にするための追加処理や遠隔画像診断など他の医療機関との電子的な画像交換をも可能にした。

画像情報が電子化される以前は、フィルムに焼き付けられた写真の改変が非常に困難であったため、フィルムという物体自体を診断の根拠として適切に管理してさえいれば、ほぼ画像情報における履歴管理は十分といえた。しかし、情報システムの普及に伴い、医療機関において電子化された画像情報の生成や保管管理がもはや一般的になった現状を踏まえると、フィルムによる画像管理とはまったく異なる概念を持って管理する必要がある。例えば、情報価値の向上を目的に、撮影済み画像に対し追加処理を行い、そのまま従前の画像に上書き更新するといった操作も、電子化された情報に対しては、そう難しいことではない。しかしながら、画像情報を利用する度にその内容が変わってしまうことは、真正性の確保における問題が発生する。特に医師が診断の根拠として使用した(画像)情報を、その後に変更することが、臨床上どれほど危険な運用であるかは想像に難くない。

このような問題に対応し必要な情報の真正性を確保するためには、画像情報がいつ診断の根拠として使われたかを明確にし、保存義務にまつわる作成責任の所在をはっきりさせておく必要がある。

電子的な医療情報の取り扱いや医療情報システムの運用管理に関わる指針として「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、「安全管理ガイドライン」) が厚生労働省より示されている (第 6.0 版 2023 年 5 月)。

本ガイドラインは、「安全管理ガイドライン」で各医療機関に定めることが求められている運用管理規定において、「画像情報の確定を診療放射線技師の業務とした場合」を想定し、日本放射線技術学会の「電子的な画像情報の確定 (検像) に関するガイドライン作成班」が平成 21 年度に策定し、改訂班が令和 7 年 4 月に改訂したものである。画像処理など電子画像に特有な運用及び医療機関における画像情報の取り扱い状況を考慮し、特に画像情報の確定保存に関する適用を示す指針として、電子的な画像情報が確定という行為を経て保存され、画像管理が適切に行われることを目的とした。言い換えれば、本ガイドラインは、医療機関において「どのタイミングを以て情報を確定させるか」に関し、運用管理規程で明確に定義するための考え方を示している。

もちろん、「画像を確定して保存する」までの一連の流れの中には、画像情報の最適化と付帯情報を確認するためのいわゆる「検像行為」や、医師が「診断の根拠となる情報を指定するための手法」など、医療機関ごとに種々のポリシーや運用手順が異なることは言うまでもない。

本ガイドラインでは、「安全管理ガイドライン」が求める真正性の確保に必要な「記録の確定」という概念に注目し、例えば「撮影済み画像」に関する「情報の確定」という一つの「区切り」が「いつ」なのかを、運用管理規定上で明確に定義することを求めている。ここ

で、画像領域における「記録の確定」と、その品質保証に相当する「検像行為」は、成果とその過程の関係に位置付けられ、どちらも重要なステップといえるため、本ガイドラインでは双方を「便宜的に一連の流れ」として取り扱った。しかし、行為の効率化や利便性の向上を目的とした「検像システム」の導入と、いつを以て記録を確定するのかという定義は、別の次元に存在する概念であり、必ずしも「記録の確定」に検像システムといった特定用途のシステムが必要という意味ではない。また、診療の一翼を担う医療従事者の責務である検像のあり方や、最適な画像の処理手順などは、本ガイドラインとは別の議論に委ねることとする。

本ガイドラインは、記録の確定に関する重要性を認識し、運用管理規定の内容により、誰もが作成責任者になりうる状況を想定の上、診療放射線技師が職責を全うするために必要なポイントを示してしている。なお、内容については技術的な記載の陳腐化を避けるために定期的に見直すことを予定しており、本ガイドラインを利用する際には最新版であることを確認し、今後の改訂についても十分留意してほしい。

## 2. 本ガイドラインの対象及びターゲットとしている画像情報

本ガイドラインは、PACS(Picture Archiving and Communication System)だけではなく、画像情報を扱うすべての情報システムや、それらのシステムの運用、利用、保守及び廃棄に関わる担当者を対象に作成されている。

医療法（昭和 23 年 7 月 30 日法律 205 号）第 21 条、第 22 条、第 22 条の 2 に示される「診療に関する諸記録」のうち、医療法施行規則第 20 条にある「エックス線写真」と、これ以外の個人情報の保護について留意しなければならない画像情報のうち「保存義務のある画像情報」の管理担当者は、本ガイドラインの内容を十分熟知することが望ましい。

## 3. 画像情報の確定と作成責任について

診断の根拠となる画像情報の確定とその作成責任、及びそれに関わる要件について整理する。

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。

### 3.1 真正性の確保

「安全管理に関するガイドライン」には、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」と示されている。

### 3.2　確定操作と作成責任に関する考え方

作成責任に関する制度上の要求事項については、前項3.1を参照されたい。

医療機関において、画像検査を実施した結果得られる診断の根拠となるべき画像情報を管理するシステム（以下、PACS等）に保存する場合、基本的にはこの保存行為が確定操作であり、この操作を行った者が作成責任者である。例えば、診療放射線技師が画像検査を行い、ここで生成された画像情報を「保存義務のある画像情報」としてPACS等に保存した場合、作成責任者は確定保存を行った診療放射線技師である。なお、作成責任者は、情報の保存を行う前に情報が正しく入力および生成されており、過失による書き換え・消去及び混同がないことを確認する義務がある。

ただし、確定操作に至るまでの作業に関しては、作業履歴などを必ずしも残す必要はない。また、作成責任は新規に確定操作をする場合だけではなく、確定後の書き換え、消去を行う場合にも生じるが、一時的に表示方法（濃度の変更、拡大など）のみを修正しもとの画像データへの変更がないのであれば、あらためて確定し保存する必要はない。

なお、作成責任の所在を明示するには、作成責任の所在を明確にし、電磁的あるいは書面にて必要に応じて速やかに明示できる対策を講じておく必要がある。

#### （１）作成責任者の記録

当該画像情報に対する作成責任者の記録が、どこに記録されているかを運用管理規程に明記する必要がある。作成責任者の記録は、画像情報の付帯情報としての記録だけを指すものではなく、別のシステム、あるいは紙面等に記録することも可能である。例えば「CT画像に関しては、該当検査の確定操作を行った者は、放射線情報システムにある検査実施者とする」と定める等が考えられる。

#### （２）明示的な「確定操作」が行われない場合について

作成責任者を明らかにするためには、明示的な確定操作が行われなくても記録が確定されたとみなして運用する場合がある。具体的には、撮影終了などのタイミングで撮影装置等からPACS等に画像情報が自動的に送信・保存される運用でPACS等に画像情報が保存された時点で確定とする場合、またはPACS等に画像情報が保存されてから一定時間経過もしくは特定時刻通過等をもって確定とみなす場合等であり、このような場合は作成責任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る。例えば、運用管理規程に「CT装置からPACS等に自動的に送信された画像情報は、当日の24時に記録は確定され、この作成責任者は○○○○とする」と明記した場合、作成責任者は当該画像情報の保存にあたって適切に保存されたことに関する責任を負うことになる。また、その後に追記、

変更、消去の必要性が生じた際は、その内容を確定済みの画像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らない。この場合の作成責任者はこの操作を行った者である。

### （３）画像処理等を伴う場合の考え方

真正性を確保すべき画像情報は、記録の確定がなされた画像情報であり、これ以前の画像情報は対象ではない。例えば、診療放射線技師が 3D 画像作成の処理を行い、処理済みの画像情報を PACS 等に確定保存し、この画像情報を元に医師が診断を行った場合、3D 画像等を生成するために必要とした画像情報（thin slice 画像）は保存対象ではない。この時の作成責任者は、処理済みの画像情報を PACS に保存した診療放射線技師である（参考：「安全管理ガイドライン第 6.0 版」に関する Q&A　シ Q-11）。

また、3D 画像に関連した事項として、＜安全管理ガイドライン第 6.0 版に関する Q&A シ Q-10＞ に「X 線 CT の検査で、オリジナルの画像の他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かまわないか。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は難しい状況である。」という問いに対し、「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。」といった記載がある。

### （４）時刻同期について

信頼できる時刻源を用いた作成日時が記録に含まれている必要がある。信頼できる時刻源とは、標準時刻と定期的に一致させる等の手段で標準時と診療の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。少なくとも、医療機関において医用画像の撮影・検査装置（以下、モダリティ）や PACS 等の時刻同期がとれていることが最低限求められる。なお、タイムサーバ等の導入を必ずしも強要するものではない。

### （５）電子署名などについて

電子署名とは「電子署名法（電子署名及び認証業務に関する法律　令和 4 年 6 月 17 日）」の定義によれば、当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること及び当該情報について改変が行われていないかどうかを確認することができるものであることの二点を満たすことが、法的に署名（記名・押印）が求められる文書などを電子的に保存する場合に必要な要件とされる。

電子署名により文書の作成者及び文書の改ざん等がないことの証明は可能であるが、それがいつ作られたものかをあわせて証明しようとするシステムがタイムスタンプ制度であり、個別の情報システム等の内部時計とは別の、世界標準時などを基準にし、タイムスタンプを

得た時刻に、その文書がたしかに存在しており、その後の改ざんがないことを証明するものである。

電子署名にあっては認証局、タイムスタンプにはタイムスタンプ局という、信頼できる第三者機関による証明が必要であるため、証明されている事実について他者からの信頼が得られやすい反面、そこまでの対外的な証拠能力・証明能力が求められていない文書等についてまで必須としてしまうことは、日常の運用に影響を及ぼすとも考えられる。

画像情報の電子的な保存については、作成責任者を明確にするとともに、いつ確定したかについても適切に記録する必要があるが、電子署名法に定める電子署名やタイムスタンプを必須とするものではなく、画像情報システムや医療情報システム、またはそれらのアプリケーション上で適切に記録されていることが求められる。

## 4. 外部の医療機関等から持ち込まれた画像情報の取り扱い

昨今、診療情報連携や患者に対する診療情報提供が一般的になり、外部の医療機関から画像情報等が持ち込まれるケースがあり、これらの保存や管理に関する義務についても整理しておく必要がある。

### 4.1 画像情報の取り込みと作成責任者

外部の医療機関等から持ち込まれた画像情報を PACS 等に取り込みを行った場合の責任の所在についても運用管理規程に明記する必要がある。一般的には PACS 等に取り込み作業を行った者が作成責任者である。なお、付帯情報などを修正した場合は、この記録を残す必要があるが、必ずしも電子的に残す必要はない。

### 4.2 保存義務について

外部の医療機関で実施された画像検査の結果は、当該検査を実施した医療機関に適切に保存する義務が生じることは言うまでもない。持ち込まれた画像を明らかに診断や治療方針の策定に用いた場合、診療録にその旨を記載する等の際にはその根拠として画像情報を記録する必要が生じる。また、診療情報連携や患者への診療情報提供等のいずれにあっても、診断を求める、診療指針に関する意見を紹介する等、医療機関を越えた画像情報のやりとりには何かしらの目的を有している。よって、それに対して最低限の説明責任を果たしうる根拠として保存の必要が生じる場合もあると考えられる。これらの場合、診断の根拠として用いた一部の画像情報について保存の必要性が生じるものであり、持ち込まれた画像情報のすべてについて保存義務が生じるとはいえない。

画像情報が医療機関に持ち込まれる態様についても、ネットワークを経由したり可搬型媒体用いたり様々な場合があるが、「画像情報の提供形態」に関しては、既に医療情報標準化推進協議会（HealthInformationandCommunicationStandardsBoard;「HELICS Board」）により標準化指針「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」

として採択されている。

### 4.3　持ち込まれた可搬型媒体の取り扱い

持ち込まれた可搬型媒体は、本来患者の所有物であるため、紹介先医療機関などにおいて保存する必要はない。なお、持ち込まれた可搬型媒体等を破棄する場合には、安全管理ガイドライン：企画管理編 8.3・システム運用編 7.3「医療情報の破棄」に準拠しなければならない。

## 5. フィルムのデジタイズに関する要件

すでに確定した情報としてフィルム等の媒体で作成されたものを受領または保存あるいは運用したのちに、デジタイズ装置等で電子化し、保存または運用する場合の取扱いについては安全管理ガイドライン企画管理編 16・システム運用編 16：「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ついて」を遵守しなければならない。

### 5.1　フィルムを保存対象とする場合

フィルムをそのまま保存するが、運用の利便性のためにデジタイズ装置等で電子化を行う場合は、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。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るが、個人情報保護上の配慮を行うことが必要である。またデジタイズ装置等による電子化の際には、診療に差し支えない精度の確保が必要である。スキャン精度については、日本医学放射線学会電子情報委員会「デジタル画像取り扱いガイドライン v.3.0 版」において示されている（参考資料 2)。

デジタイズした画像情報は、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が必要であり、DICOM 形式で保存することが適切である。デジタイズ作業に当たっては、運用管理規程を定めて、デジタイザ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が管理者に求められる。

### 5.2　電子的な情報を保存対象とする場合

デジタイザによる電子化を行ない、その電子情報を保存対象とする具体的事例は、次の 2 つの場面を想定することができる。

●電子カルテ等の運用で、診療の大部分が電子化された状態で行われている場合で、他院からの診療情報提供書等の紙やフィルムが避けられない事情で生じる場合。つまり「診療等の都度デジタイザで電子化して保存する場合」である。

●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、更に紙等の保管場所に窮している場合。つまり「過去に蓄積されたフィルムをデジタイザで電子化保存する場合」である。

いずれの場合も、電子情報とフィルム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。

### （１）診療等の都度デジタイザで電子化して保存する場合

この場合は、5.1 項での条件に加えて、①電子化情報が元のフィルムと同等であることを担保し、作業が適正な手続きで確実に実施される措置を講じる責任者として情報作成管理者を置くとともに、②デジタイザで読み取った際の作業責任者(実施者または管理者)が必要に応じ電子署名法に適合した電子署名・タイムスタンプを遅滞なく行わなければならない。なお、電子署名については、厚生労働省の安全管理に関するガイドライン：企画管理編 14「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」を参照すること。また、③フィルムを入手してから一定期間内にデジタイズを行うことが必要である。一定期間とは１～２日程度以内の運用管理規程で定めた診療に支障を来さない期間とする。

### （２）過去に蓄積されたフィルムをデジタイザで電子化保存する場合

このケースは本ガイドラインでは推奨しない。5.１項の運用に加えて、フィルムの外部保存を行えば殆どの目的には合致すると思われる。あえて実施する場合は、説明責任を果たすために相応の対策をとることが求められる。（１）の要件をすべて満たした上で、患者等から事前の同意を得て、さらに厳格な監査を実施することが必要である。

すなわち、安全管理ガイドライン：企画管理編 16.3 に記載があるように、①事前の対象患者等への周知と同意、②実施計画書の作成と外部の有識者を含む委員会での妥当性評価、③適切な能力を持つ外部監査人の監査、が求められる。

## 6.　画像情報の保存期間と画像圧縮について

画像情報は、法的には「その他診療に関する諸記録」に該当し、医療法施行規則第 20 条では 2 年間の保存義務、保険医療機関及び保険医療養担当規則第 9 条では完結の日から 3 年の保存義務があるとされている。なお、診療録に関しては、医師法第 24 条、歯科医師法第 23 条、保険医療機関及び保険医療養担当規則第 9 条に 5 年の保存義務があるとされている。

画像情報は、読影時に利用した状態で保存する必要があり、可逆圧縮画像にて診断を行った場合は、そのままの状態で保存し、非可逆圧縮による保存を行ってはならない。ただし、法的な保存期間を過ぎたものに関しては、この限りではないが取り扱いについては運用管理規程に明記しておく必要がある。

（例）診療完結の日から 5 年を経過した画像情報は、非可逆圧縮にて保存する。ただし、これにより患者が不利益を被ることが予測される場合は、これを適用しない。

## 7.　検像

検像とは、医師の診断・読影を支援する目的で、診療放射線技師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修正や不必要な画像の削除を行う行為をさす。確定前に確認するポイントとしては、オーダに応じた画像情報が取得できていること、付帯情報が正しいことなどである。また、必要に応じて、画像の付帯情報・画像の濃度・画像の方向・画像の順序の変更などがある。

検像は特別な装置や機器およびアプリケーションなどを必須とするものではなく、技術面と運用面の両方でバランスをとり総合的に行えばよい。各医療機関等は、自らの機関の規模や各部門システム、既存システムの特性をよく見極めた上で、最も効果的な対応を検討されたい。

### 7.1　確認すべき情報の種類

検像を行うにあたり確認すべき情報のサンプルを表１に示す。

| | |
|---|---|
| **患者情報** | 患者ID |
| | 患者氏名 |
| | 年齢 |
| | 性別 |
| **依頼情報** | 依頼科 |
| | 依頼医師 |
| | 検査内容 |
| | 検査目的 |
| | 検査日時 |
| **画像情報** | モダリティ |
| | 画像枚数 |
| | シリーズ数 |
| | 画像の順序 |
| | 検査部位 |
| | 検査範囲 |
| | 画像の方向 |
| | 濃度 |
| | コントラスト |
| | 画質 |
| | マーキング |
| | 各種処理 |

※画像の方向 - 上下左右裏表

※画質 - ボケ、鮮鋭度等
※各種処理 - フィルタ、MIP、MPR、3D 等

### 7.2 運用ケース

いくつかのケースを以下に示すが、これらを複合的に用いても、モダリティごとに手法が異なっていてもよい。また、技術的に行うことは必須ではなく運用的に行っても問題はない。例えば、患者情報を照合する手法として放射線情報システムから検像アプリケーションに送信された患者情報などと画像情報に含まれる情報とを自動的に照合しても、放射線情報システムの情報あるいは紙面などに記載された患者情報などと画像 viewer 上に描出された情報とを操作者が照合してもよい。

#### （1）ケース 1：モダリティ上で検像する

モダリティにおいて撮影を実施し、そのモダリティ上で検像作業を行う場合である。検像を実施するアプリケーションの有無に関わらず、作業がモダリティ上で行われる。検像が終わった画像は電子保存のための PACS 等の保管装置に伝送される。

#### （2）ケース 2：検像を行う専用のアプリケーションを用いる

モダリティから画像を検像専用システムに伝送し、専用システム上で検像作業を行う場合である。検像が終わった画像は電子保存のための PACS 等の保管装置に伝送する。

#### （3）ケース 3：PACS 等 の機能として画像 の viewer などを用いて検像する

撮影装置から PACS 等のサーバに保管されている画像を画像 viewer などで読み出し、検像を行い、電子保存のための保管装置に伝送する。検像を実施するアプリケーションの有無に関わらず、作業が画像 viewer 上でおこなわれる。PACS 等の保管装置上に検像前の画像と検像後の画像が同時に存在する場合は、検像前後の画像を区別する対策を施し、検像後の画像を誤って消去しないようにする工夫が必要である。

## 8. 画像情報の外部保存、外部へのバックアップ、地域連携での共有について

考え方やシステム的な実装に関して混同が生じているため、本ガイドラインに関連するそれぞれの要件について解説を行う。

### 8.1 外部保存

本ガイドラインでは、医療機関において法的保存義務のある記録が電子保存の三原則を満たした状態で、情報を施設外に保管し運用することを指す。よって、見読性などが外部保存を行うことで損なわれる場合は、電子保存の 3 原則の要件を満たした状態で施設の内部にも保存することが必要となる。

なお、ネットワークを通じて外部に保存する場合の見読性の確保については、「安全管理ガイドライン第 6.0 版」に緊急に必要になることが予測される診療録等は、医療機関等に保存するか、ネットワークを通じて医療機関等の外部に保存しても複製又は同等の内容を医療機関等の内部に保持することが必要になる。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機関の障害等に対応できるような措置を行っておくことも記載されている。

### 8.2 外部へのバックアップ

データの外部へのバックアップには、主として以下の 2 つがある。

①診療録の消失に備える、いわゆる「診療録バックアップ」

② 災害時における診療の継続を目的とした、いわゆる「災害時バックアップ」

これらは目的が異なるため、データ量、データの構造、バックアップをとるタイミングなどが異なるのは当然であるとともに、要求される法的要件も異なる。

診療録バックアップでは、バックアップデータそのものには、真正性、見読性、保存性は要求されないが、リストアの際に診療録と同等の要件が求められる。なお、リストアする場合には、それがリストアした情報である事実を証跡として残すことが重要である。サービス提供事業者と契約する場合にあっては、契約条件に含めるなどの配慮が必要である。

一方、災害時バックアップには、このような法的要件はない。バックアップの対象とするデータ項目についても、目的に照らして施設、地域ごとに検討し定めるべきものである。

### 8.3 地域連携での共有

本章でいうデータは、外部保存/バックアップを目的に蓄積されたデータである。したがって、地域連携や医学研究への活用など情報を二次的に利用する場合には、別途手続きが必要である。

複数医療機関での情報共有は患者の同意を伴う行為である。一方、外部保存/バックアップは医療機関の自らの責任を果たすために行うものであり、直ちにこれが共有等に利用できると考えるのは誤りである。

地域連携に用いる際には、患者の同意取得、参加する医療機関間でのポリシーに関する合意、共有情報の定義やアクセス権限管理、各医療機関の責任範囲、相互運用性の確保などについての取決めを定めなければならない。

また、画像情報については、地域連携に際して画像情報を提供している側の「確定」と、共有された画像情報にもとづき診断した側の「診断に対する証拠保全」では概念が異なる（この場合の保存の義務については＜4.1＞を参照）

**付録１：本ガイドラインが想定する業務フローと運用管理規定の例**

本ガイドラインの範囲として想定される業務フローについて以下に例示する。

（１）一般的な業務の流れにおいて確定を行うケース

＜業務フロー＞

検査を行い、画像の修正、確認を終え、診療現場に画像情報を提供する前に診療放射線技師が確定を行う。

＜運用管理規程例＞

注）[]の中を選択し、規定文を作成する。なお、該当する項目がない場合は追加すること。

・その１

*[一般撮影・CT 検査]*の画像情報に関しては、*[検像システム・検査装置]* において、保存操作をした場合を確定とし、その操作を実施した者を作成責任者とする。

・その２

*[一般撮影・CT 検査]*の画像情報に関しては、検査終了後の*[一定時間経過後（例：当日の 24時）、検査日翌日の XX:00 時、検査後 XX 時間経過の遅い時点]*に確定するものとし、この場合の作成責任者は、*[検査実施者・技師長]*とする。

＜留意事項＞

・確定という行為が、どの時点で、どのシステムのどの操作が該当するのかを、医療機関ごとに検討し定める必要がある。

・確定の行為を行うものが検査を行った者なのか、別の者なのかについても、医療機関ごとに検討し定める必要がある。

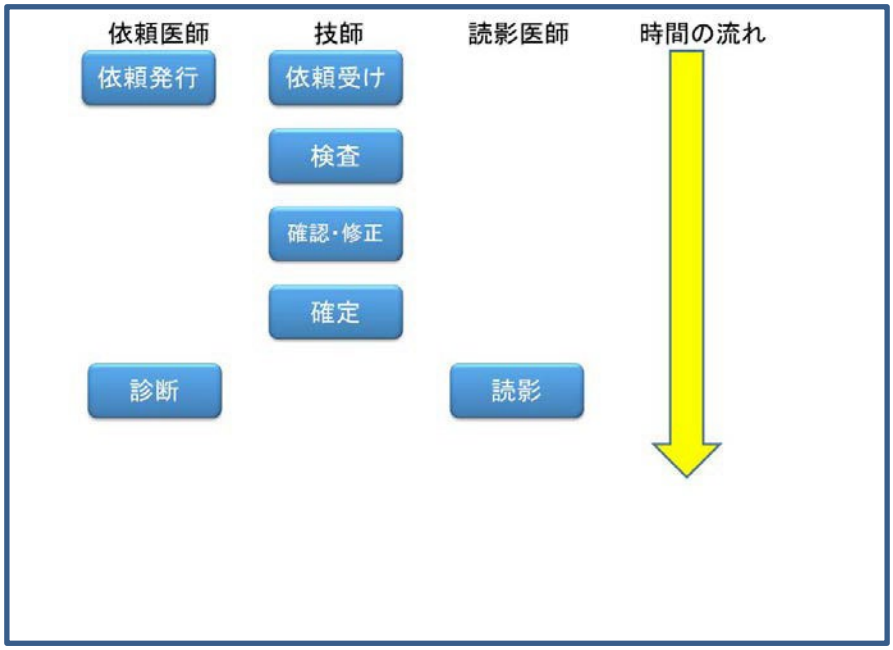



図1

(2) 画像処理を伴うケース

＜業務フロー＞

ケース（1）のフローと並行、あるいは終了後に、画像処理などを行う場合、保存対象の画像に関しては、診療現場に画像情報を提供する前に、診療放射線技師が確定を行う。

＜運用管理規程例＞

注）[]の中を選択し、規定文を作成する。なお、該当する項目がない場合は追加すること。

・その 1

後処理画像に関しては、*[検像システム・画像処理システム]*において、保存操作をした場合を確定とし、その操作を実施した者を作成責任者とする。

・その 2

後処理画像に関しては、処理終了後の*[一定時間経過後（例：当日の 24 時）、処理の翌日の XX:00 時、処理後 XX 時間経過の遅い時点]*に確定するものとし、この場合の作成責任者は、*[検査実施者・画像処理者・技師長]*とする。

＜留意事項＞

画像処理を行うためだけに必要とした画像については、特に確定および保存する必要はない。

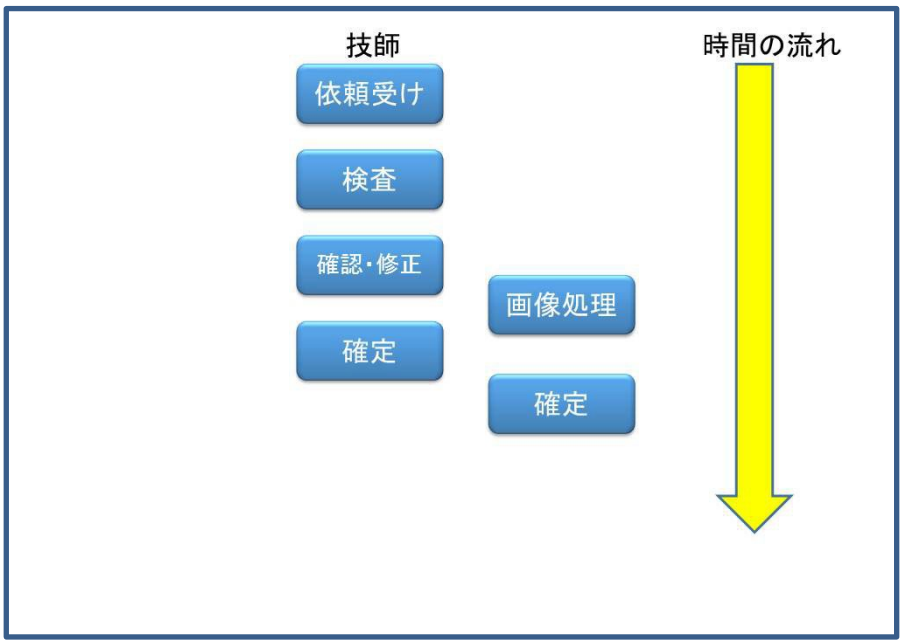



図 2

（3）外部から持ち込まれた画像情報を確定するケース

＜業務フロー＞

診療放射線技師が、外部から持ち込まれた画像情報の確定を行う。

＜運用管理規程例＞

注）[]の中を選択し、規定文を作成する。なお、該当する項目がない場合は追加すること。

・その 1

外部から持ち込まれた画像情報に関しては、*[検像システム・画像取り込み装置]*において、保存操作をした場合を確定とし、その操作を実施した者を作成責任者とする。

・その 2

外部から持ち込まれた画像情報に関しては、取り込み終了後の*[一定時間経過後（例：当日の 24 時）取り込みの翌日の XX:00 時、取り込み後 XX 時間経過の遅い時点]*に確定するものとし、この場合の作成責任者は、*[取り込み実施者・技師長]*とする。

＜留意事項＞

・取り込みを行うタイミングについて、医師が閲覧する前なのか後なのかによって、責任範囲および確定を行う画像の範囲が異なる場合が想定される。

（4）本ガイドラインでは範囲外としたケース

本ガイドラインの作成にあたって検討を行ったが、本ガイドラインの範囲には含まれないと判断されたものとして以下のものがある。これらについても、各医療機関において「確定」について検討を行う際には、十分に配慮などをされることを望む。

・診断医、読影医などが診断後に該当画像を確定する場合

・冠動脈造影検査など医師が撮影をし、都度 PACS（あるいは動画サーバ）などに医師が確定し保存する場合

・他の医療機関などから持ち込まれた画像を用い医師が診断し、該当画像を医師が確定する場合

## 付録 2：運用管理規程サンプル

本サンプルの位置付け

各医療機関で実際の運用管理規程作成においては、各組織の方針によって様々な姿があり、実施にあたっての技術と運用の組み合わせも組織の実情において決められる。従って、本書はあくまでも例示であり、実情に合わせて作成時の参考に資するものである。

### 画像情報システムに関する運用管理規程

XXX 病院
画像部門

1. 総則

（1）理念と目的

診療情報は患者の診療や病院の管理運営上必要とされるときに、信頼性のある情報を迅速に提供できるよう、環境の整備と運営が適正になされる必要があり、とりわけ患者のプライバシーへの留意が求められる。

この規程は ＸＸＸ病院（以下「当院」という）における「ＸＸ管理規程」の下位規定として、画像情報システム（以下「本システム」という）を構成する機器とソフトウェアの機能要件、及びその運用管理に関する事項を定めたものである。

これにより、当院において、画像情報の適正な保存とともに、適正な利用に資することを目的とする。

（2）対象情報

本システムの扱う情報については、情報の種類や内容ごとに、安全管理上の重要度の分類、リスク分析、法的保存義務の対象／非対象の別、必要な保存期間を検討し、具体的対象について別表を作成し本システム関係者に開示する。

２．システム管理組織

本システムには、「ＸＸ管理規程」の定めに従い院長の指名によりシステム管理者を置く。システム管理者は本システムの運用管理組織の統括を行い、文書管理・システム構築と運用に関しての責務を負う。

システム管理者は、管理範囲の部分に対して運用の代行者を指名できる。代行者名は周知されていること。

本システムの運用に必要な文書（契約書、システム構成図、各機器・ソフトウェアの説明書等）の保管管理は、別表に定める。

**このテンプレートとしては、病院全体の規定として、以下の事項が定められている**

ことが前提になっている。
・当院に運用責任者および個人情報保護責任者を置き、病院長をもってこれに充てること。
・病院長は必要な場合、運用責任者及び個人情報保護責任者を別に指名すること。
・情報システムを円滑に運用するため、全情報システムに関する運用を担当する管理者を置くこと。
・各部門システムにはシステム管理者を置き、病院長が指名すること。たとえば、システム管理者は、部門長（技師長）とする。
（組織によっては、全システムを統括するシステム管理者が存在する場合もある）
・情報システムに関する取扱い及び管理に関し必要な事項を審議するため、病院長のもとに情報システム管理委員会を置くこと。
・その他、この規程の実施に関し必要な事項がある場合については、情報システム管理委員会の審議を経て、病院長がこれを定めること。
・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。
・監査責任者は病院長が指名すること。
・運用責任者は、監査責任者に毎年 X 回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
・監査の内容については、情報システム管理委員会の審議を経て、病院長がこれを承認すること。
・運用責任者は必要な場合、臨時の監査を監査責任者に命ずること。
・患者及び利用者からの情報システムについての苦情・質問を受け付ける窓口を設けること。
・苦情・質問受け付け後は、その内容を検討し、速やかに必要な措置を講じること。

以下、安全管理ガイドライン第6.0版　企画管理編に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）及び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）に分け、システム運用専任の担当者がいる場合といない場合に参照すべき管理について遵守事項をまとめてあるので施設の実情に合わせて画像情報システムに関する運用管理規程を作成するとよい。

以下、抜粋。

| | 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<br>（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<br>（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 | すべて参照 | 基本的にすべて参照<br>※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。<br>４．４マニュアル等及び各種資料の整備<br>５．安全管理におけるエビデンス<br>１５．技術的な対策の管理<br>遵守事項：④、⑥、⑦、⑧、⑬以外 |
| システム運用専任の担当者がいない | すべて参照<br>※「担当者」という記載を「企画管理者」に置換し、参照 | 基本的にすべて参照<br>※「担当者」という記載を「企画管理者」に置換し、参照。<br>※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。<br>４．４マニュアル等及び各種資料の整備<br>５．安全管理におけるエビデンス<br>１５．技術的な対策の管理遵守事項：<br>④、⑥、⑦、⑧、⑬以外 |

## 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。
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。
⑥⑤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。

## 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。

## 3.　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。
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。
⑩①～⑨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.　医療情報システム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。
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。

## 5.　安全管理におけるエビデンス

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。

## 6.　リスクマネジメント（リスク管理）

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。
⑤②～④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。
⑨PDCA（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。
⑩PDCA 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。

## 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）

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。
④③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。

## 8. 情報管理（管理、持ち出し、破棄等）

①医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順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。

## 9. 医療情報システムに用いる情報機器等の資産管理

①医療情報システム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。

## 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。
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。

## 11.　非常時（災害、サイバー攻撃、システム障害）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。

## 12.　サイバーセキュリティ

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。

## 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。
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

## 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。
(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。

## 15.　技術的な安全管理対策の管理

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。
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。
⑭①～⑬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。

## 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。
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。

**資料1：安全管理ガイドライン第6.0版 （抜粋）**

### 概説編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。

### 企画管理編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。

7.1　見読性の確保のための対策
（１）情報の所在管理
**システム運用編 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。

（２）見読化手段の管理

**システム運用編 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

（3）見読目的に応じた応答時間

**システム運用編 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。

（4）システム障害対策としての冗長性の確保

**システム運用編 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。

7.2　真正性の確保のための対策

【医療機関に保存する場合】

（1）入力者及び確定者識別及び認証

（2）記録の確定手順の確立と、識別情報の記録

（3）更新履歴の保管

（4）代行入力の承認

**システム運用編 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）。

（５） 情報機器・ソフトウェアの品質管理

**システム運用編 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。

システム運用編 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。

**システム運用編 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。

**システム運用編 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。

【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

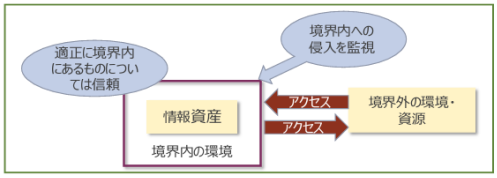
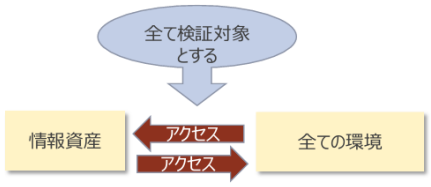
**システム運用編 13.2　不正な通信の検知や遮断、監視**

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<br>  | ・　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。<br>・　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<br>  | ・　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。<br>・　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。

（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

**システム運用編 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。

（８） リモートログイン機能を制限すること

**システム運用編 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。

7.3 保存性の確保のための対策

【医療機関等に保存する場合】

（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棟の防止

**システム運用編 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。

（２） 不適切保管・取扱いによる情報の滅失、破壊の防止

**システム運用編 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。

（ア）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

（イ）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

**システム運用編 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。
（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
**システム運用編 12.2　バックアップの管理**
【医療機関等に保存する場合】7.3　保存性の確保のための対策（２）参照
（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
**システム運用編 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。
【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】
（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行うこと
**システム運用編 5.2　標準化対応、データ形式・プロトコルの互換性の確保**
【医療機関等に保存する場合】7.3　保存性の確保のための対策（４）参照
（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行うこと
**システム運用編 12.2　バックアップの管理**
【医療機関等に保存する場合】7.3　保存性の確保のための対策（２）参照

**資料 2：デジタル画像取り扱いガイドライン v.3.0（抜粋）**

フィルムデジタイズ装置を電子保存に用いる場合には、次の特性を有すること。(但し、マンモグラフィは除く。)

(1) サンプリングピッチ：200μm以下

(2) 空間分解能：CTF（0.25）≧0.9、CTF（0.5）≧0．8、CTF（1.0）≧0.7

ここでCTF（n）は、nlp/mmのContrast Transfer Functionを示す。

(3) 濃度階調数：1024以上（10ビットグレイスケール以上）

(4) デジタイズ濃度範囲：0.0D－3.0D以上

**資料 3：サイバーセキュリティ（［特集］医療機関等におけるサイバーセキュリティより抜粋）**

1　概要

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る。

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、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おり、安全管理ガイドラインでもセキュリティに関係する記載が多く見られる。

2　サイバーセキュリティ／インシデント

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ある。

3.1　対策：バックアップ

どのようなサイバーインシデントであったとしても、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の 1 つとして、システムやデータのバックアップがあげられる。

システムやデータのバックアップの目的は下記の 2 つがある。

（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。

バックアップは毎営業日行うことが推奨され、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などの工夫もまた必要である。

あわせて、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可能となる。

LAN などのネットワークインフラを含め、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ないよう配慮する必要がある。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、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ある。

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、事前によく検討しておく必要がある。
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る。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る。しかし、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、カルテ自体に所見を記載するようにしておく、なども現実的な対応としては有効となると考えられる。

### 3.2　対策：ガバナンス

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。これら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。
また、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。
とは言っても、外部事業者を直接管理することは難しく、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る。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る。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あり、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となる。

### 3.3　対策：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、管理する必要がある。

### 3.4　対策：アカウント管理

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るが、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、時間稼ぎとしては有効であるし、うまく行けばバックアアップ系やセキュリティ系

を守ることができる。
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・制御していることもあり、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ある。
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る。

### 3.5　対策：監視

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る。また、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）がある。
近年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ないが、不正ソフトウェアの異常な動きを検出し、被害が出る前にシステムに報告させることも対策としては有効である。

### 3.6　対策：BCP

サイバーインシデントを 100%防止することは不可能であり、また大規模災害もないとは言えない。地域に一定の役割を担う医療機関としては、BCP の策定と B CP に基づく訓練、さらに BCP の持続的な見直しは必須である。昨今の状況を踏まえると、サイバーインシデントも BCP の重要なテーマである。大規模災害の BCP も重要であるが、サイバーインシデントも主要なテーマに入れて BCP を策定し運用する必要がある。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となる。