画像情報の確定に関するガイドライン
第2.1版

公益社団法人 日本放射線技術学会
平成26年8月18日

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，フィルムを用いた従来の概念とは異なってきていることに気付く。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，そう難しくない。しかしながら，撮影済みの画像が，時々でその情報内容を変えることに対しては，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。

この様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なったかを明確にし，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4.2版　2013年9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に記載している。

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，画質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，医療機関毎に種々のポリシーや運用手順が複数存在す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，その品質検証に相当する「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，何時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欲しい。

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）の第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」を取り扱う管理担当者は，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。

3.1. 真正性の確保

「医療情報システムの安全管理に関するガイドライン」には，電子保存の要求事項として「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が要求される」と示されている。

ここで，法的に保存義務のある文書等の電子保存の要件として，真正性，見読性及び保存性の確保の３つの基準が示されているが，真正性とは，正当な権限において作成された記録に対し，虚偽入力，書き換え，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。

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として，「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。(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 第4 条第4 項第二号，平成17 年3 月25 日)」とある。

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，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等に確定保存した場合，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，確定操作をする前の作業に関しては，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) 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スライス画像）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：「医療情報システムの安全管

理に関するガイドライン第4.2 版」に関するQ&A　Q42）。

また、3D画像関連した事項として、＜医療情報システムの安全管理に関するガイドライン第4.2 版に関するQ&A＞ 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。

(2) 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する記録のみ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。

(3) 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，装置からPACS等に画像情報が自動的に送信され保存がされており，PACS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など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，この作成責任者は〇〇〇〇とする」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。

(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，タイムサーバなど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)」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など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併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。

画像情報を電子的に保存するに当たっては，作成責任者を明確にすることと併せて，いつ確定したかということ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　ソフトウェア上で適切に記録されていることで事足ると考えられる。

4.外部の医療機関等から持ち込まれたフィルム（コピー）や画像情報の取り扱い

医療機関において画像検査を実施，確定保存して得られた画像情報等については，当該医療機関において作成責任者を定める等，適切に管理しなければならないことは先に述べたところであるが，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ってきた状況下で，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整理しておく必要がある。

4.1. 保存義務について

外部の医療機関において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記録しておくべき場合が生じる。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，その画像情報に基づくより高度な専門性を要する診断を求める場合や，治療指針に関する意見を照会しようとするものである等，画像情報を持ち込む側に何らかの目的を有するものである。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，現下，こういった「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（Health Information and Communication Standards Board；「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。

4.2.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必ずしもない。なお，持ち込まれた可搬型媒体等を破棄する場合には，厚生労働省ガイドライン：6.7「情報の破棄」に準拠しなければならない。

4.3.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，責任の所在を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。

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厚生労働省のガイドライン第9章：「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

フィルムをデジタイズする場合で，もっとも多く考えられるのが，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が，フィルムをそのまま保存する場合である。この場合は，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。しかし

ながら，個人情報保護上の配慮は保存義務のある内容と同等に行う必要がある。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。なお，スキャン精度については，日本医学放射線学会(JRS)-電子情報委員会で「デジタル画像取り扱いガイドラインv.2.0」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共に，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い，責任を明確にしなければならない。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: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」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きたさない期間とする。

(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。敢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，患者等の事前の同意を得，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：9.3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，付帯情報が正しく入っていることなどである。また，必要に応じて修正すべき内容として，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　ソフトウェア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良く見極めた上で，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　ソフトウェア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のViewerソフト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　ソフトウェアの有無に関わらず，作業がモダリティ上で

おこなわれる。検像が終わった画像は電子保存のため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　ソフトウェアを用いる

撮影装置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アプリケーション　ソフトウェアを用いて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保管装置に伝送する。

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

撮影装置からPACS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　ソフトウェアの有無に関わらず，作業が画像Viewer上でおこなわれる。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

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。なお、クラウドコンピューティングについてもNIST（National Institute of Standards and Technology）に定義されているものを参考として付録に添付した。

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に対しての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、施設の内部に電子保存の3原則の要件を満たした状態で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、「医療情報システムの安全管理に関するガイドライン第4.2 版」に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。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と記載されている。

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、保存性が要求されるわけではないが、リストアの際に診療録と同等の要件が求められることは当然である。なお、リストアする場合には、それがリストア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。

一方で災害時バックアップには、このような法的要請はない。そもそも収載され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、本来は相当程度煩雑な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り、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、データがそこにあるからといって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。

地域連携に用いるとすれば、たとえば、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（厚生労働省発行の「安全管理に関するガイドライン　付録」の記載を参考にすると良い）。

また、画像情報に関していうならば、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：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。

さらに，本書は画像情報システムに関する管理規程の例示であり，その前提として，各医療機関における組織全体の運用管理規程，組織全体にわたる機器（Ex.ネットワーク）の管理規程，災害時の事業継続計画（BCP），監査規程，従事者の守秘義務規程などが別途存在するものとしている。

途中にある“枠内部分”は別途存在する規約類の想定内容である。本サンプルにある記載項目が上位規程に存在する場合は本規定から省略することができる。

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，個別情報毎に，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，具体的対象を別表に記入し本システム関係者に開示する。

法的保存義務のある画像情報の保存（以下，「電子保存」という）に関しては，10 章に記してある。

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。

システム管理者は本章下記のシステム構築，運用体制の整備，ならびに本規定の５章以降に記載された個別事項の実行管理を行う。

システム管理者は，

① 本システム全般の構築・運用に関して，以下に挙げる通知・ガイドラインおよび標準規格についての更新状況を適宜確認し，本システムの変更・改造時の対象とすること。

・医療情報システムの安全管理に関するガイドライン（厚生労働省第 5 章に列挙の規格類
・DICOM
・HL7
・IHE
・HELICS 指針

② 使用する機器・システムが標準規格を満たしていることを確認すること。
満たしていない場合は，システムベンダからその理由・標準化に対する基本スタンス・今後の対応方針・将来のシステム更新や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，等について説明を受ける等して一定の理解を等しくしておくこと。
③ システムの設計時，運用開始時に技術的対策と運用による対策を，基準適合チェックリストに記載し，必要時には第三者への説明に使える状態で保存すること。
④ 業務上の情報漏えいなどのリスク分析を行い，結果に対して予防措置を立てること。
⑤ システムの機能要件に挙げられている機能が支障なく運用される環境を整備すると共に，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で，適宜，業務において規程通りの運用がなされていることを確認すること。
⑥ 本システムの取扱いについて手順書を整備し，利用者に周知の上，常に利用可能な状態におくこと。
⑦ この規定に定められた本システムの管理に関する行為の記録を作成し，これを保存する。
⑧ 利用者に対して研修を行い，研修時のテキスト，出席者リストを保存すること。
⑨ システム改造時は，最新の基準適合チェックリストに従って，技術的対策と運用による対策の分担を見直すこと。
⑩ 機器やソフトウェアの変更にあたっては，保存された情報が継続的に使用できることを確認すること。

３．利用者の責務

利用者は以下の責務を負う。

①自身の認証番号やパスワードを管理し，これを他者へ利用させないこと。

②本システムの情報の参照や入力（以下「アクセス」という。）に際して，認証番号やパスワード等によって，システムに利用者自身を認識させること。

③与えられたアクセス権限を越えた操作を行わないこと。

④参照した情報を，目的外に利用しないこと。
⑤患者のプライバシーを侵害しないこと。
⑥システムの異常を発見した場合，速やかにシステム管理者に連絡し，その指示に従うこと。
⑦不正アクセスを発見した場合，速やかにシステム管理者に連絡し，その指示に従うこと。
⑧保管，バックアップの作業に当たる者は，手順に従い行い，その作業の記録を残し，システム管理者の承認をうること。
⑨利用者は，作業終了あるいは離席する際は，必ずログアウト操作を行うこと。
⑩盗難，紛失は管理者への速やかな報告を行うこと。
⑪その他，手順書等で指定された操作を守ること。

４．システムの機能要件

本システムに用いる機器及びソフトウェアを導入するに当たっては，機器・システムの機能が「医療情報システムの安全管理に関するガイドライン（厚生労働省）」に示される各項目の技術的要件を満たし，運用項目にも対応可能な機能を持つものであること。
具体的には，本システムは次の機能を備えるものとする。
①情報にアクセスしようとする者の識別と認証機能
②情報の機密度に応じた利用者のアクセス権限の設定と不正なアクセスを排除する機能
③自動ログアウト機能，スクリーンセーブ後の再認証機能
④画像情報に関して，電子保存 3 原則に対応可能であること
⑤電子保存に関して利用者が入力した情報について確定操作を行うことができる機能
⑥電子保存に関して利用者が確定操作を行った情報を正確に保存する機能
⑦電子保存に関して情報の確定／未確定状態が判別できる機能
⑧電子保存に関して確定後の情報及びその更新（消去，変更，修正）に際しその内容の記録と共に実施者を特定し，関連づけて記録する機能，必要に応じて更新前の情報を参照できる機能
⑨ 管理上又は診療上の必要がある場合，記録されている情報を速やかに出力する機能
⑩ 情報の利用範囲，更新履歴，機密度等に応じた管理区分を設定できる機能
⑪ 利用者が情報にアクセスした記録(ログ)を保存し，これを追跡調査できる(監査証跡)機能
⑫ 記録された情報の複製（バックアップ）を作成する機能
⑬ 非常時用機能（ブレークグラス機能）
⑭ 無線 LAN を用いる場合は，ステルスモード，ANY 接続拒否設定，不正アクセス対策，暗

号化が出来る機能

⑭ 電子証明書による電子署名機能，タイムスタンプ付与機能，電子署名の検証機能

⑮ 保守要員のアカウントを設定する機能

⑯ 保守作業のログ取得機能

⑰ 持ち出し用の情報機器に対しての起動パスワード，情報には暗号化やアクセスパスワードの設定が可能な機能

５．機器・システムの管理

（１）設置場所

本システムの記録媒体を含む主要機器は管理者によって入退室管理された場所に設置する。

システムの設置場所には常時施錠し，システム管理者の指示がない限り，他の職員や外部の者が操作できないよう管理する。

情報が保管されている機器の設置場所及び記録媒体の保存場所への入退出記録を残すとともに，入退出の記録の内容についてシステム管理者は定期的にチェックを行う。

設置場所には火災，災害等にも対応可能な無水消火装置，漏電防止装置，無停電電源装置等を備える。

システム管理者は，設置機器を定期的に点検し，保存された情報の安全性を確保し，常に利用可能な状態に置いておくこと。

（２）機器・ソフトウェアの管理

システム管理者はシステムで使用される機器・ソフトウェアを，使用の前に審査を行い，情報の安全性に支障がないことを確認する。また，定期的にソフトウェアに異常がないかを検査する。

システム管理者は，ネットワークや可搬型媒体によって情報を受け取る機器について必要に応じてこれを限定する。

システム管理者は，定期的にソフトウェアのウィルスチェックを行い，感染の防止に努めること。

システム管理者は障害時の対応体制が最新のものであるように管理すること。

システム管理者はデータバックアップ作業が適切に行われている事を確認すること。

無線 LAN を用いる場合には，システム管理者は，無線 LAN アクセスポイントの設定状態を適宜確認し，無線 LAN 利用規則を院内関係者および利用可能性のある入院患者へ説明をすること。

６．情報の安全管理

（１）記録媒体の管理

記録媒体は，記録された情報が保護されるよう，別の媒体にも補助的に記録する。

品質の劣化が予想される記録媒体は，あらかじめ別の媒体に複写する。

（２）アクセス管理

システム管理者は，

システムの利用者の登録を管理し，職務により定められた範囲によるアクセス権限を規定し，不正な利用を防止すること。

そのため，必要に応じてハードウェア・ソフトウェアの設定を行うこと。

また，疑義が生じた場合には，アクセス状況の確認を行い，監査責任者に報告をすること。

業務上において情報漏えいなどのリスクが予想されるものに対し，規程類の見直しを行うこと。また，事故発生に対しては，速やかに責任者に報告し利用者に周知すること。

パスワードの最低文字数，有効期間等を別表に定める。

認証の有効回数，超過した場合の対処を別表に定める。

（３）業務者の外部からのアクセス

外部からアクセスを許容する機器については別途定めるものに限定する。

（４）外部への持ち出し

①システム管理者は，持ち出し対象となる情報および情報機器を別表にまとめ，管理方法と共に利用者に周知し，その機器が許可された際の状態を保持していることを定期的に確認すること。

これ以外の情報および情報機器の持ち出しを禁止する。

②システム管理者は，情報および情報機器の持ち出しに関しリスク分析を行う。

③情報および情報機器を持ち出す場合は，所属，氏名，連絡先，持ち出す情報の内容，格納する媒体，持ち出す目的，期間を別途定める書式でシステム管理者に届け出て，承認を得ること。

④システム管理者は，情報が格納された可搬媒体および情報機器の所在について台帳を用いる等で定期的にチェックし，所在状況を把握すること。

⑤持ち出す情報機器について起動パスワードを設定すること。そのパスワードは推定しやすいものは避け，また定期的に変更すること。

⑥持ち出す情報機器について，ウイルス対策ソフトをインストールしておくこと。

⑦持ち出した情報を，別途定められているアプリケーション以外がインストールされた情報機器で取り扱わないこと。

⑧持ち出した情報機器には，別途定められている以外のアプリケーションをインストールしないこと。
⑨持ち出した情報および情報機器の盗難，紛失時には，直ちにシステム管理者に届け出ること。
⑩届け出を受け付けたシステム管理者は，その情報および情報機器の重要度にしたがって，対応すること。

（５）外部とのネットワークを通じた情報交換
外部の機関と医療情報を交換する場合，「ＸＸ管理規程」の規定に従い，相手の医療機関等，通信事業者やシステムインテグレータ，運用委託業者等との間で，責任分界点や責任の所在を契約書等で明確にすること。
・システム管理者は，リスク分析を行い，上記契約状態が適切に維持管理されているか定期的に監査を行って確認し，安全に運用されるように技術的および運用的対策を講じること。
・システム管理者は，技術的対策が適切に実施され問題がないかを定期的に監査を行って確認すること。
（６）情報破棄
個人情報を記した媒体の廃棄に当たっては，安全かつ確実に行われることを，システム管理者が作業前後に確認し，結果を記録に残すこと。
（７）電子署名
電子署名が必要な文書に関して，システム管理者は，
・電子署名，タイムスタンプに関する作業手順を定めること。
・電子的に受領した文書に電子署名が有る場合の，署名検証手順を定めること。

７．ネットワークの管理
　システム管理者は，「ＸＸ管理規程」の定めに従い，本システムの定期的に利用履歴やネットワーク負荷等を検査し，通信環境の効率的な運用を維持するとともに不正に利用された形跡がないか確認する。
　システム管理者は，ネットワークの不正な利用を発見した場合，直ちにその原因を追求し対策を実施する。

８．災害等の非常時対策
　災害，サイバー攻撃等により一部医療行為の停止等医療サービス提供体制に支障が発生

する非常時の場合を考慮し，当院の定める事業継続計画(BCP)にしたがって運用を行う。
　非常時と見なす判断は，「ＸＸ管理規程」に従って責任者が行い，発生した場合，「ＸＸ管理規程」に定める連絡先に当院の担当責任者を通じて連絡する。
・非常時においても縮退したシステムで参照できるような媒体にデータを保存し保管する。
・システム管理者は，本システムの縮退運用時や非常時の運用，復旧体制並びに回復手順に関しての手順書を作成し，利用者に周知の上，常に利用可能な状態におくこと。

９．教育と訓練
システム管理者はシステムを正しく利用させるため，定期的に本システムの取扱い及びプライバシー保護に関する研修を行い，研修時のテキスト，出席者リストを残す。
新規の業務担当者には，操作前に教育を行うこと。
また，未研修者にはシステムの利用を制限することもある。

１０．電子保存に関す事項：画像情報の確定と電子保存 3 原則
（１）確定
・利用者は，電子保存システムへの情報入力に際して，定められた確定操作（入力情報が正しい事を確認する操作）を行って，入力情報に対する責任を明示すること。
詳細については，付録 2（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）を参考。

・確定後に追記，変更，消去の必要性が生じた場合は，部門システム管理者に報告し，その内容と共に操作者，時刻を記録すること。
（２）真正性
　５，６章による。
（３）見読性
電子保存に用いる機器及びソフトウェアを導入するに当たって，見読性の維持要件を明確化し，保存義務のある情報として電子保存された情報毎に見読用機器を常に利用可能な状態に置いておくこと。
・システム管理者は，応答時間の劣化がないように維持に努め，必要な対策をとること。
・システム管理者は定期的に情報の所在確認を行うこと。
（４）保存性
・機器・媒体やソフトウェアの変更に当たっては，データ移行のための業務計画を作ること。

・データのバックアップをとること
・保存場所の管理（環境，入退室）を行うこと
・記録媒体の劣化対策を行うこと
・マスタ更新時の過去情報の変更が起こらない様にすること
・標準形式でのデータ入出力機能を持つこと

１１．画像情報の保存期間と画像圧縮

保存義務期間中の画像情報は非圧縮または可逆圧縮で保存し，保存義務期間以降は廃棄または非可逆圧縮の画像情報の保存を可とする。

１２．外部委託

業務を当院外の事業者または個人に委託する場合は，守秘事項を含む業務委託契約を結ぶこと。契約の署名者は，当部門の長とする。また，各担当者は委託作業内容が個人情報保護の観点から適正に且つ安全に行われていることを確認すること。

外部の保守会社から機器・ソフトウェアに対してリモートメンテナンスを受ける場合，相手の保守会社，通信事業者，運用委託業者等関係者との間で，責任分界点や責任の所在を契約書等で明確にすること。

・業務委託の契約書には，再委託での安全管理に関する事項を含むこと
・システム管理者は，保守会社における保守作業に関し，その作業者および作業内容につき報告を求め適切であることを確認すること。必要と認めた場合は適時監査を行うこと。
・システム管理者は，上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。

準拠することを推奨する参考項目
・セキュリティ機能に関しては，JIRA 作成の「製造業者による医療情報セキュリティ開示説明書」書式による適合宣言を参考にして評価する。
・外部委託にあたってのサービス選定には，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）の評価を参考にする。
・JIRA/JAHIS「リモートサービスセキュリティガイドライン」準拠を求める。

１３．施行

この規定は。xxxx 年 xx 月 xx 日より施行する。

付録 2：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。

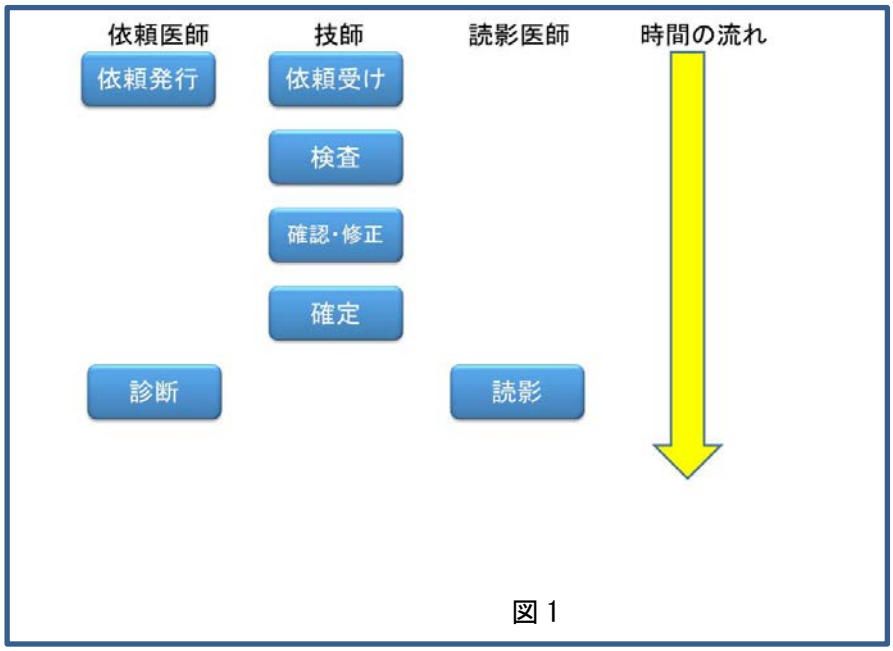

図 1

（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。

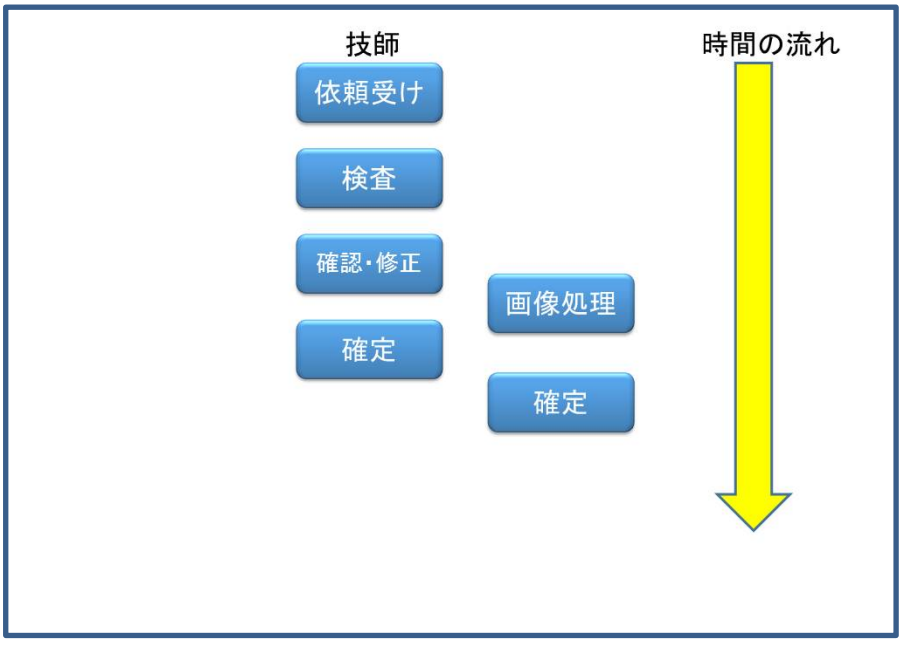

図 2

（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3：クラウドとは

以下にNIST（National Institute of Standards and Technology）に示されているクラウドに関する定義の概略を示す。

＜原文：http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf#search=%27NIST+800145%27＞

＜独立行政法人　情報処理推進機構による日本語訳サイト：http://www.ipa.go.jp/files/000025366.pdf#search=%27NIST+800145%27＞

（1） クラウドの性質

- On-demand self-service

  必要なときに必要なサービスを必要な分だけ利用可能

  ＜原文＞

  A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

- Broad network access

  種々な端末からいつでもアクセスして利用可能

  ＜原文＞

  Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

- Resource pooling

  利用者が実際にどのコンピュータを利用しているのかを意識する必要がない

  ＜原文＞

  The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- Rapid elasticity

  必要とする処理能力や状況に応じて柔軟に使える計算機資源を増減することが可能

  ＜原文＞

  Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- Measured Service

  計算機資源の利用状態をコントロールしたり最適化を行うことが可能

  ＜原文＞

  Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

（２） クラウドのサービスモデル

- Cloud Software as a Service (SaaS)

  インターネット経由のソフトウエアパッケージの提供

  ＜原文＞

  The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- Cloud Platform as a Service (PaaS)

  インターネット経由のアプリケーション実行用プラットフォームの提供

＜原文＞

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- Cloud Infrastructure as a Service (IaaS)
  インターネット経由のハードウエアやインフラの提供
  ＜原文＞
  The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

（３） クラウドのデプロイメントモデル

- Private cloud
  このクラウド・インフラストラクチャは、特定の組織のために単独で運用される。
  ＜原文＞
  The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

- Community cloud
  このクラウド・インフラストラクチャは、いくつかの組織により共有され、また、関心事（ミッション／セキュリティ要件／ポリシー／コンプライアンス）を共有する特定のコミュニティをサポートする。

＜原文＞

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public

- Public cloud

  このクラウド・インフラストラクチャは、いくつかの組織により共有され、また、関心事（ミッション／セキュリティ要件／ポリシー／コンプライアンス）を共有する特定のコミュニティをサポートする。

  ＜原文＞

  The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

- Hybrid cloud

  このクラウド・インフラストラクチャは、複数のクラウド定義（private／community／public）から、2つ以上を組み合わせたものとなる。それぞれに固有の実体は保持するが、標準あるいや個別のテクノロジーによりバインドされ、データとアプリケーションのポータビリティ（クラウド間でのロード・バランシングのためのクラウド・バーストなど）を実現する。

  ＜原文＞

  The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

資料１：医療情報システムの安全管理に関するガイドライン　第 4.2 版　（抜粋）

7　電子保存の要求事項について

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が要求される。誤った診療情報は，患者の生死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は各種の法令に規定されており，所定の期間において安全に保存されていなくてはならない。

これら法的に保存義務のある文書等の電子保存の要件として，真正性，見読性及び保存性の確保の３つの基準が示されている。それらの要件に対する対応は運用面と技術面の両方で行う必要がある。運用面，技術面のどちらかに偏重すると，高コストの割に要求事項が充分満たされなかったり，煩わしさばかりが募ったりすることが想定され，両者のバランスが取れた総合的な対策が重要である。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良く見極めた上で，最も効果的に要求を満たす運用面と技術面の対応を検討されたい。

7.1真正性の確保について

A.制度上の要求事項
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。 （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 第4 条第4 項第二号，平成17 年3 月25 日） 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。 （施行通知 第2 条　(3)）

「診療録等の記録の真正性，見読性及び保存性の確保の基準を満たさなければならないこと。」（外部保存改正通知 第2 1 (1)）

B.考え方

真正性とは，正当な権限において作成された記録に対し，虚偽入力，書き換え，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。

また，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，診療録等が書き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。

従って，ネットワークを通じて医療機関の外部に保存する場合は，医療機関等に保存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。

B-1. 虚偽入力，書換え，消去及び混同を防止すること

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システム管理者は，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，書き換え・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る。また，作成責任者（情報を作成，書き換え，消去しようとする者）は，情報の保存を行う前に情報が正しく入力されており，過失による書き換え・消去及び混同がないことを確認する義務がある。故意または過失による虚偽入力，書き換え，消去及び混同に関しては，入力者等のシステムの操作者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る。

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，あるいは，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る。

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る。

これらの虚偽入力，書き換え，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る。

(1) 故意または過失による虚偽入力，書き換え，消去及び混同の防止

故意による虚偽入力，書き換え，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らない。

1.情報の作成責任者が明確で，いつでも確認できること。

2.作成責任者の識別・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。

3.操作者の権限に応じてアクセスできる情報を制限すること。

4.入力や確定作業の手順等を運用管理規程に記載すること。

5.作成責任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，操作記録に対して適正な利用であることが監査されること。

6.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。

7.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，「6.8 情報システムの改造と保守」に記載された手続きに従う必要がある。

過失による虚偽入力，書き換え，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る。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る。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・ハット事例をもとに誤操作の発生しやすい個所を色分け表示する等の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。

(2) 使用する機器，ソフトウェアに起因する虚偽入力，書き換え，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，書き換え，消去及び混同とは，作成責任者が正当に入力したにもかかわらず，利用しているシステム自体に起因する問題により，結果が作成責任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る。

1.　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）

2.　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

3.　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

4.　ウイルス等の不正なソフトウェアに感染し，データの不正な書き換え，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，医療機関等自らがシステムの品質管理を率先して行う姿勢が重要である。具体的な方策については，C 項の記述を参照すること。

B-2.作成の責任の所在を明確にすること

電子保存の対象となる情報は，記録を作成するごとに責任者が明確になっている必要がある。また，一旦記録された情報を追記・訂正・消去することもごく日常的に行われるものと考えられるが，追記・訂正・消去するごとに責任者が明確になっている必要がある。医療機関等の規模や管理運営形態により，作成・追記・訂正等の責任者が自明となる場合も考えられるが，その場合，作成責任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何らかの記録を残した運用を実施すること。

入力は診療行為の実施者である作成責任者自らが行うことが原則であるが，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，本来の作成責任者である執刀医による入力が物理的に不可能であって，代行者による入力が必要となる場合も想定される。このような場合は，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らない。

（1）　作成責任者の識別と認証

（2）　記録の確定

（3）　識別情報の記録

（4）　更新履歴の保存

（1）作成責任者の識別及び認証

本指針6 章の「6.5 技術的安全対策　（1）利用者の識別及び認証」を参照すること。

＜代行入力を行う場合の留意点＞

医療機関等の運用上，代行入力を容認する場合には，必ず入力を実施する個人毎にID を発行し，そのID でシステムにアクセスしなければならない。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，禁止しなくてはならない。

(2) 記録の確定

記録の確定とは，作成責任者による入力の完了や，検査，測定機器による出力結果の取り込みが完了することをいう。これは，この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・誰によって作成されたかを明確にし，その保存情報自体にはいかなる追記，変更及び消去も存在しないことを保証しなければならない。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づ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。

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）により作成される記録では，作成責任者は過失による誤入力や混同の無いことを確認し，それ以降の情報の追記，書き換え及び消去等との区別を明確にするために「確定操作」が行われること。また，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もしく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，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こと。

なお，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，その作業の責任者による確定操作が行われることが必要である。

また，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，管理責任者の元で適正に管理された特定の装置もしく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を確定情報として扱い，運用される場合もある。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る。

(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・誰が作成したものかが，明確になっている必要がある。作成責任者の識別情報には，氏名及び作成された時刻を含む事が必要であり，また，作成責任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る。

識別情報は，作成者が責任を持つ個別の行為毎に個々の患者の診療録等に対して記録または記載されることを原則とする。初回の診療録等の作成時に作成責任者の識別情報が必要であるが，確定され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作成責任者の識別情報が必要である。

また，グループ診療及びグループ看護においても，作成責任者は個人とし，複数責任者

が存在する場合は複数の個人を責任者として記録する。

(4) 更新履歴の保存

例えば，診療情報を例に取ると，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，確定済で保存してある記録に対して追記や修正を行うことは少なくない。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らない。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，更新内容の確定責任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らない。

C.最低限のガイドライン

(1) 作成者の識別及び認証

b. 臨床検査システム，医用画像ファイリングシステム等，特定の装置もしくはシステムにより記録が作成される場合

1. 装置の管理責任者や操作者が運用管理規程で明確にされ，管理責任者，操作者以外による機器の操作が運用上防止されていること。

2. 当該装置による記録は，いつ・誰が行っ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こと。

(2) 記録の確定手順の確立と，作成責任者の識別情報の記録

b. 臨床検査システム，医用画像ファイリングシステム等，特定の装置もしくはシステムにより記録が作成される場合

1. 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が定義されていること。その際，作成責任者の氏名等の識別情報（または装置の識別情報），信頼できる時刻源を用いた作成日時が記録に含まれること。

2. 確定された記録が，故意による虚偽入力，書き換え，消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。

9 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

本章は法令等で作成または保存を義務付けられている診療録等をいったん紙等の媒体で作成されたものを受領または保存または運用したのちに，スキャナ等で電子化し，保存または運用する場合の取扱いについて記載している。電子カルテ等へシェーマを入力する際に，紙に描画しスキャナやデジタルカメラで入力する場合等は本章の対象ではなく，7 章の真正性の確保の項を参照すること。

9.1　共通の要件

B.考え方

スキャナ等による電子化を行う具体的事例は，次の2つの場面を想定することができる。

（1）　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。
調剤済み処方箋(薬剤師法第28条第2項に基づき調剤録への記入が不要とされた場合の調剤済み処方箋を含む）も、これに相当する。

（2）　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，及び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。

この項ではこの上記のいずれにも該当する，つまり「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」,「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」に共通の対策を記載する。

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。従って，いったん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きわめて有効であり，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。このような場合の対策に関しては,「9.4（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」で述べる。

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たりすることで，スキャンによる電子化で情報が欠落することがないことを確認すること。

・ 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。
・ 放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン2.0 版　（平成18 年4 月)」を公表しており，参考にされたい。なお，このガイドラインではマンモグラフィは対象とされていないが，同委員会で検討される予定である。
・ 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，さまざま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が必要であり，その点に十分配慮すること。
・ 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い精度であること，及び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範囲であることを念頭に行う必要がある。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。

2.　改ざんを防止するため，医療機関等の管理責任者は以下の措置を講じること

・ スキャナによる読み取りに係る運用管理規程を定めること
・ スキャナにより読み取った電子情報ともと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。
・ スキャナで読み取った際は，作業責任者(実施者または管理者)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い，責任を明確にすること。

　なお，電子署名については「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」を参照すること。

3.　情報作成管理者は，上記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。

資料2：デジタル画像取り扱いガイドライン v.2.0（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