医政発 0331 第 56 号
令和４年３月３１日

公益社団法人日本精神科病院協会会長　殿

厚生労働省医政局長
（ 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 5.2 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。）は、平成 17 年 3 月 31 日「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」（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・厚生労働省医薬食品局長・厚生労働省保険局長連名通知）の別添として、個人情報保護に資する情報システムの運用管理、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。）への適切な対応等について示したところである。

その後所要の改定を行い、令和３年１月にガイドライン第 5.1 版が策定されたところであるが、ガイドライン第 5.1 版の公表以降、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被害が見られる。

そのため、本ガイドラインについて利用用途に応じて閲覧しやすいように本編と別冊とに分冊化を行うとともに、制度的な動向、技術的な動向、「規制改革実施計画（令和３年６月 18 日閣議決定）」等への対応として、外部アプリケーションとの連携における利用者の認証・認可に関する記述を示す、ランサムウェアによる攻撃への対応としてのバックアップのあり方等の対策を示す、電子署名に関する 6.12 章の記載を整理するなどの所要の改定を行い、別添１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 5.2 版」を策定したので、貴職におかれては、御了知の上、貴会員等関係者に周知方願いたい。

また、すべての医療機関等の管理者にガイドラインの内容をご理解頂けるよう、別添 2 のとおり、「医療情報を安全に管理するために」（「「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版」の策定について」（政統発第 0530 第１号厚生労働省政策統括官（統計・情報政策担当）通知）の別添 2）を第 2.2 版として改定するとともに、別添 3 のとおり、ガイドラインの別冊用語集（「「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 版」の策定について」（政統発第

0530 第 1 号厚生労働省政策統括官（統計・情報政策担当）通知）の別添 3）を改定したため、併せて周知方願いたい。

なお、令和４年１月 27 日から全国の病院に対し実施した「病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査」について、対象となった 8,252 施設中 6,216 施設からご回答をいただいた。本調査の御周知など、ご協力いただいたことについて感謝申し上げる。結果については、第 10 回健康・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にて公表（別添４）を行ったところだが、医療機関がアンケートの項目と本ガイドラインの対応箇所が把握できるよう追記した別添５を作成したので、こちらについても医療機関に活用いただけるよう周知方願いたい。

このガイドライン等については厚生労働省ホームページへの掲載も予定しているので、念のため申し添える。

医療情報システムの安全管理に関するガイドライン

第 5.2 版

本編

令和 4 年 3 月

厚生労働省

改定履歴

版数	日付
第 1 版	平成 17 年 3 月
第 2 版	平成 19 年 3 月
第 3 版	平成 20 年 3 月
第 4 版	平成 21 年 3 月
第 4.1 版	平成 22 年 2 月
第 4.2 版	平成 25 年 10 月
第 4.3 版	平成 28 年 3 月
第 5 版	平成 29 年 5 月
第 5.1 版	令和 3 年 1 月
第 5.2 版	令和 4 年 3 月

【目次】

1. はじめに

本ガイドラインは、医療情報システムの安全管理や「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号。以下「e-文書法」という。）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。ただし、医療情報の適切な取扱いの観点からは、医療情報システムに関わる対策のみを実施するだけで十分な措置が講じられているとは言い難い。したがって、本ガイドラインを使用する場合、医療情報システムの担当者であっても、「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」を十分理解し、医療情報システムに関わらない部分でも医療情報の適切な取扱いのための措置が講じられていることを確認することが必要である。

本ガイドラインは、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（以下「医療機関等」という。）における電子的な医療情報の取扱いに係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及した。したがって、本ガイドラインは技術的な記載の陳腐化を避けるために定期的に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。

第 2 版から第 5.1 版までの改定概要については別冊に掲載。

改定概要

【第 5.2 版】

本ガイドライン第 5.1 版の公表以降、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が一層、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る被害も見られる。特にランサムウェアに代表される攻撃への対策は、喫緊の課題となっている。そのほか本ガイドラインを踏まえた対策を医療機関等が行う重要性が高まっている。

そのため、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した。具体的には、利用用途に応じて閲覧しやすいように本編と別冊とに分冊化を行った。

ランサムウェア対策との関係では、6.10 章において、ランサムウェアによる攻撃への対応としてのバックアップのあり方等の対策を示した。また適切なリスク分析を行い、被害に遭った際の対策を速やかに講じられるよう、6.2 章において、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）を整備する旨について示した。

医療機関等が利用する医療情報システムにおいて外部サービスとの連携が進む中で、アプリケーション間の安全性を確保する観点から、6.5 章において外部アプリケーションとの連携における利用者の認証・認可に関する記述を示した。

本ガイドラインにおいて、従来から利用が認められているシステムやサービスの利用形態に関して、これらの利用が安全に管理されている状況下で利用が可能であることを、改めて示すよう、一部記述の追記等を行った。具体的には、BYOD については安全に管理されている環境下での利用について、6.9 章において具体的な記述を行った。また外部ネットワークを利用する上で医療機関等が負うべき管理内容を明示した。

電子署名については、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 章の記載を整理した。具体的には、文書の作成者に資格が必要な場合に求められる署名についての要件等について示した。

その他関係制度の変更等に伴う修正を行った。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を 6.12 章において行った。併せて、電子署名に用いる暗号アルゴリズムの参照規格について、実務の状況を勘案して、JIS から ISO に参照規格を変更する旨を 6.12 章に示した。また外部保存を行う際の事業者の選定に関して、「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」（総務省・経済産業省　令和 2 年 8 月 21 日）における基準に揃えて 8.3 章の変更を行った。

その他、分かりやすさや表現の平仄を合わせる観点から、一部構成を修正した。

2. 本ガイドラインの読み方

本ガイドラインは本編において、医療機関等において実施すべき内容を示し、別冊でその考え方や、具体的な対応例などを示す形としている。医療機関等において、医療情報システムの安全対策上、求められる内容は本編において確認し、具体的な対策を検討するに際して、本編で述べた内容の考え方や具体例などを別冊において確認すること。本編においては次のような構成になっている。医療機関等の管理者、医療情報システム安全管理責任者及び医療機関等から業務を受託する事業者が、それぞれ関連する箇所を理解した上で、必要な対策を実施することを期待する。

なお、本ガイドラインでは、医療情報、医療情報システムという用語を用いているが、これは医療に関する患者情報（個人識別情報）を含む情報及びその情報を扱うシステムという意味で用いている。

【1 章～6 章及び 10 章】

医療情報を扱う全ての医療機関等が参照すべき内容を含んでいる。

【7 章】

保存義務のある診療録等を電子的に保存する場合に参照すべき内容を含んでいる。

【8 章】

保存義務のある診療録等を電子媒体により外部保存する場合に参照すべき内容を含んでいる。

【9 章】

e-文書法に基づいてスキャナ等により電子化して保存する場合の指針を含んでいる。

なお、本ガイドラインの大部分は法律、厚生労働省通知、他の指針等の要求事項に対応する対策を示すことを目的としており、そのような部分では概ね、以下の項に分けて説明している。

A. 制度上の要求事項

法律、厚生労働省通知、他の指針等の要求事項を記載している。

B. 考え方

要求事項の解説及び原則的な対策方針について記載している。

C. 最低限のガイドライン

A 項の要求事項を満たすために必ず実施しなければならない対策を記載している。ただし、医療機関等の規模により実際に必要な対策が異なる場合や、幾つかの対策の中の一つを選択する場合もあるため、付表の運用管理表を活用し、適切な対策を採用して、実施しなければならない。

D. 推奨されるガイドライン

実施しなくても A 項の要求事項を満たすことが可能であるが、説明責任の観点から実施した方が理解を得やすい対策を記載している。

また、最低限のシステムには使用されていない技術を使用する上で一定の留意が必要な事項の記載も含んでいる。

なお、別紙の 3 つの付表は、安全管理上要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされて初めて有効なものとなるが、技術的対策には複数の選択肢があることが多いため、付表を活用して、採用した技術的対策に相応した運用的な対策を実施すること。なお、付表は以下の項目で構成している。

1. 運用管理項目：安全管理上の要求事項で多少とも運用的対策が必要な項目
2. 実施項目：上記管理項目を実施レベルに細分化したもの
3. 対象：医療機関等の規模の目安
4. 技術的対策：技術的に可能な対策（一つの実施項目に対して選択可能な対策を列挙した）
5. 運用的対策：上記 4. の技術的対策を行った場合に必要な運用的対策の要約
6. 運用管理規程文例：運用的対策を規程に記載する場合の文例

各医療機関等は、実施項目に対して採用した技術的対策に応じ、必要な運用的対策を運用管理規程に含め、実際に規程が遵守されていることを確認することで、実施項目を達成することが可能となる。また、技術的対策を選択する前に、それぞれの運用的対策を検討することで、各医療機関等で運用可能な範囲の技術的対策を選択することも可能となる。一般に運用的対策の比重を大きくすれば医療情報システムの導入コストは下がるが、技術的対策の比重を大きくすれば利用者の運用的な負担は軽くなる。運用的対策と技術的対策について適切なバランスを求めることは非常に重要なので、運用的対策及び技術的対策の選択に、これらの付表が活用されることを期待する。

3. 本ガイドラインの対象システム及び対象情報

本ガイドライン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及び組織を対象としている。ただし、「7　電子保存の要求事項について」、「8　診療録及び診療諸記録を外部に保存する際の基準」、及び「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」は対象となる医療情報が、一部の文書等に限定されている。

3.1. 7章及び9章の対象となる文書について

医療情報を含む文書は、法令等によって保存、作成、交付等が定められている文書と、そうでない文書に大別できる。7章及び9章は、法令等によって保存、作成、交付等が定められている文書の一部であり、具体的には、e-文書法の対象範囲となる医療関係文書等として、「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。以下「e-文書法省令」という。）、「「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律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日付け医政発0331第30号・薬生発0331第10号・保発0331第26号・政社発0331第1号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下「施行通知」という。）で定められた文書等（別冊参照）を取り扱う場合を対象としている。

また、介護事業者が取り扱う文書等のうち、一部の文書等（別冊参照）は、e-文書法の対象範囲でかつ当該文書の内容に医療情報が含まれることがある。この場合、この文書等に限らず、介護事業者は、7章及び9章の規定を遵守する必要がある。

3.2. 8章の対象となる文書等について

8章は、「「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日付け医政発0325第15号・薬食発0325第9号・保発0325第5号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下「外部保存改正通知」という。）で定められた文書等（別冊参照）を取り扱う場合を対象としている。

なお、調剤録の保存については、薬局開設者の責任とされており、外部保存を行う場合についても従前と同様に薬局開設者の責任で行う必要がある。また、調剤録は当該薬局に備えることとされているため、当該薬局の調剤録を外部保存する場合には、他の薬局の調剤録と明確に区分し、薬局ごとに個別に管理する必要がある。

3.3. 紙の調剤済み処方箋と調剤録の電子化・外部保存について

紙の調剤済み処方箋の電子化は、紙の処方箋に法令で定められた事項を記入した後、記名押印又は署名を行い調剤済みとしたものを 9 章に示す方法により実施することとなる。

薬局で紙の処方箋を受け取った場合、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）。

なお、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。

この場合、既に電子化された紙の調剤済み処方箋に対して、過去の電子署名の検証が可能な状態を維持する形で、電子的に修正を実施し、薬剤師の電子署名を付すことが必要となる。

なお、電子処方箋を（電子的な）調剤済み処方箋とした場合には 7 章を、さらにそれを外部保存する場合には、8 章を参照すること。

3.4. 取扱いに注意を要する文書等

3.1 章に示した文書等のほか、医療関係文書等のうち個人情報の保護について留意しなければならないものには、①施行通知には含まれていないものの、e-文書法の対象範囲で、かつ患者の個人情報が含まれている文書等（麻薬帳簿等）、②法定保存年限を経過した文書等、③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、④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）等がある。

これら①～④に示した文書等については、個人情報保護関連各法の趣旨を十分理解した上で、各種指針及び本ガイドライン 6 章の対策事項を実施するとともに、情報管理体制確保の観点から、バックアップ情報等を含め、それらを破棄せず保存している限り、3.1 章に示す文書等に準じて取り扱う必要がある。

なお、「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」も、適宜参照すること。

また、3.2 章に示す文書等がその法定保存年限を経過する等の事由によって、施行通知や外部保存改正通知の対象外となった後においても、外部保存を実施（継続）する場合には、3.2 章に示す文書等に準じて取り扱わなければならない。

4. 電子的な医療情報を扱う際の責任のあり方

本章では、医療機関等、情報処理事業者、電気通信事業者等の関係者間での電子的な医療情報の取扱いにおける責任の在り方について、「医療機関等の管理者の情報保護責任の内容と範囲」及び「他の医療機関等や事業者に情報処理の委託や他の業務の委託に付随して医療情報を委託する場合と第三者提供した場合」に分けて、責任分界という概念を用いて整理した（具体的な内容は別冊「4.電子的な医療情報を扱う際の責任のあり方」参照)。

4.1. 医療機関等の管理者の情報保護責任について

医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、通常の運用時における医療情報保護の体制を構築し管理する責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に対処をすべき責任とがある。便宜上、本ガイドラインでは前者を「通常運用における責任」、後者を「事後責任」と呼ぶこととする。

(1) 通常運用における責任について

ここでいう通常運用における責任とは、医療情報の保護のための適切な情報管理ということになるが、適切な情報管理を行うことが全てではなく、以下に示す 3 つの責任を含む必要がある。

① 説明責任

医療情報システムの機能や運用方法の取扱いに関する基準を満たしていることを患者等に説明できるようにする責任である。この責任を果たすためには、以下のことが必要である。

- 医療情報システムの仕様や運用方法を明確に文書化すること
- 仕様や運用方法が文書化した方針のとおりに機能しているかどうかを定期的に監査すること
- 監査結果をあいまいさのない形で文書化すること
- 監査の結果問題があった場合は、真摯に対応すること
- 対応の記録を文書化し、第三者が検証可能な状況にすること

② 管理責任

医療情報システムの運用管理を行う責任である。医療情報システムの管理を受託する事業者に任せきりにしているだけでは、これを果たしたことにはならないため、医療機関等においては、以下のことが必要である。

- 管理状況の報告を定期的に受けること

・　管理に関する最終的な責任の所在を明確にすること
・　受託する事業者を監督すること

さらに、「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。）上は、受託する事業者との対応に当たり、以下のことが必要である。

・　個人情報保護の責任者を定めること
・　電子化された個人情報の保護について一定の知識を有する責任者を決めること

③ 定期的に見直し必要に応じて改善を行う責任

情報保護に関する技術は日進月歩であり、情報保護体制が陳腐化するおそれがあるため、医療情報保護の仕組みの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う責任がある。この責任を果たすためには、以下のことが必要である。

・　医療情報システムの運用管理の状況を定期的に監査すること
・　問題点を洗い出し、改善すべき点があれば改善すること

⑵ 事後責任について

医療情報について何らかの不都合な事態（典型的には漏えい）が生じた場合、医療機関等の管理者には、以下の責任がある。

なお、「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 Ⅳ 8.」では、漏えい等の報告等について規定していることから、参照すること。

① 説明責任

特に医療機関等は一定の公共性を有するため、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明・公表も求められる。そのため、医療情報について何らかの不都合な事態が生じた場合、以下のことが必要である。

・　その事態の発生を公表すること
・　原因及びそれに対する対処方法について説明すること

②　善後策を講ずる責任

また、医療情報について何らかの不都合な事態が生じた場合、善後策を講ずる責任として、以下のことが必要である。

・　原因を追及し明らかにすること
・　損害を生じさせた場合にはその損害を填補すること
・　再発防止策を講ずること

4.2. 委託と第三者提供における責任分界

医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託（第三者委託）と第三者提供の 2 種類がある。本節では、それぞれの形態における医療機関等の管理者の情報保護責任のあり方を、前節で挙げた責任の分類に従って整理して示す。

4.2.1. 委託における責任分界

委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は、患者に対する関係では、受託する事業者の助けを借りながら、前節に掲げた「説明責任」、「管理責任」及び「定期的に見直し必要に応じて改善を行う責任」を果たす義務を負う。

万一、何らかの不都合な事態が生じた場合にも同様に、受託する事業者と連携しながら「説明責任」及び「善後策を講ずる責任」を果たす必要があるため、受託する事業者との契約において、受託する事業者の義務を明記すべきである。

また受託する事業者の責任によって不都合な事態が生じた場合に、受託する事業者との間で「善後策を講ずる責任」をどのように分担するかについても、受託する事業者との契約で明記すべきである。

そのため、「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」に示す「サービス仕様適合開示書」、「サービスレベルアグリーメント」において、その内容を明記させる必要がある。

4.2.2. 第三者提供における責任分界

医療機関等が医療情報の第三者提供を行う場合、個人情報保護法、関連するガイドライン、「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」等を遵守する必要がある。

4.3. 例示による責任分界点の考え方の整理

責任分界点について検討する際に、いくつか例が想定される。各例において、医療情報システムや外部接続時のネットワークの安全管理の考え方、保存義務のある書類の保存、外部保存を受託することが可能な機関の選定基準等を検討する際には、それぞれ 6 章、7 章、8 章を参照する必要がある。具体的な例としては、

- 地域医療連携で「患者情報を交換」する場合（第三者提供による場合、共同利用による場合等）
- 業務の必要に応じて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
- 医療機関等の業務の一部を委託することに伴い、情報が「一時的に外部に保存」される場合
- オンライン外部保存を委託する場合

などが挙げられる。特にオンライン外部保存を委託する場合については、医療情報システムにおいて、オンプレミスばかりではなく、クラウドサービスを利用するケースも増えていることから留意点を示す。

クラウドサービスを利用する際の医療情報システムの新規導入・更新や運用は、受託事業者経由で行うことになるほか、サービスの性格上、サービスに用いている機器等を共同利用することとなる。そのため、医療情報システムの管理監督や責任分界においても、このような特性を踏まえた管理方法による取決めを行う必要がある。

各例における具体的な考え方は、別冊において示す。

4.4. 技術的対策と運用による対策における責任分界点

医療情報システムの安全を担保するためには、「技術的な対応（対策）」と「組織的な対応（運用による対策）」を総合的に組み合わせる必要がある。

特に、技術的な対応（対策）は、医療機関等の総合的な判断の下、主にシステム提供側（システムベンダ及びサービス事業者）を中心に医療機関等と協働で対策を行うことが求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。

5. 情報の相互運用性と標準化について

医療機関等では、業務上様々な情報のやりとりが行われ、それらによる指示、報告、連絡等の意思の共有によって一連の業務が成立する。

これらのやりとりを単に電子化するだけであれば、これまでの業務に情報入力という業務を付加してしまうだけである。しかし、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が可能となる。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。

事実、医療機関等において電子化された情報を扱うシステムの導入は、当初、事務処理の合理化を目的としたものであったが、現在では情報共有の推進や、医療安全、ひいては医療の質の向上に資することを目的としたものになっている。

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。このことは、7.2 章及び 7.3 章で述べるように、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存することが望ましい。よって、本章ではそれらについて記した。

医療情報における標準規格に関する民間主導の取組みとして、各種の標準化団体・規格制定団体等が会員となっている一般社団法人医療情報標準化推進協議会（Health Information and Communication Standards Organization ： HELICS 協議会）がある。HELICS 協議会が利用目的ごとに採択すべき標準規格を推奨し、その利用のための医療情報標準化指針を示している。

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、HELICS 協議会が指針として掲げた標準規格のうち、我が国で必要不可欠と考えられるものについては、厚生労働省の保健医療情報標準化会議での審議を経て「厚生労働省標

準規格」とし、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（具体的な内容は別冊「5.情報の相互運用性と標準化について」参照)。

医療機関等において、自らこれらの用語・コードの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。

したがって、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システムベンダ及びサービス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

さらに、現在導入している医療情報システムの更新や医療情報システムの新規導入の際に、医療機関等においても相互運用性について中長期的なビジョンを持ち、計画を策定していくことが望ましい。

6. 医療情報システムの基本的な安全管理

医療情報システムの安全管理は、個人情報保護関連各法（個人情報保護法、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）及び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））に規定された安全管理・確保に関する条文によって法的な責務として求められている。安全管理を疎かにすることは上記法律に違反することになるが、医療において最も重要なことは患者等との信頼関係であり、単に違反事象が起こっていないことを示すだけでなく、安全管理が十分であることを説明できるようにすること、つまり説明責任を果たせるようにすることが求められる。この章での制度上の要求事項として、個人情報保護法の条文を例示する。

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（従業者の監督）

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業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。

（委託先の監督）

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。

（個人情報保護法　第 23 条　第 24 条　第 25 条）

6.1. 方針の制定と公表

B. 考え方

「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」において、個人情報保護に関する方針を定め公表することが求められている。本ガイドラインが対象とする医療情報システムの安全管理も、個人情報保護対策の一部として考えることができるため、この方針の中で、医療情報システムの安全管理についても言及する必要がある。

個人情報を取り扱う医療情報システムを運用する組織は、これらの要求事項を勘案して組織の実情に合った基本的な方針を策定し、適切な方法で公開することが重要である。

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。
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

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

安全管理を適切に行うための標準的なマネジメントシステムが ISO（ISO/IEC 27001:2013）及び JIS（JIS Q 27001:2014）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。

なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、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が重要である。その際には、「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」（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」や、保健医療福祉情報システム工業会の JAHIS 標準及び日本画像医療システム工業会規格（JESRA）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が参考になる。

「『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」は以下の URL から取得できる。

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

https://www.jira-net.or.jp/publishing/jesra_public.html

6.2.1. ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006（※）では PDCA の各ステップを次の様に規定している。

※ 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。そのモデルとして PDCA サイクルが理解しやすいので旧版を引用している。

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－実施 （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
Action－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（Action）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（具体的な内容は別冊「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」参照)。

6.2.2. 取扱い情報の把握

医療情報システムで扱う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を行い、常に最新の状態を維持する必要がある。このリスト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されなければならない。

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。

個人を識別可能な医療に係る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。

6.2.3. リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等の脅威を列挙する。医療機関等では一般に他の職員等への信頼に基づいて業務を進めているため、利用者の悪意や過誤を想定することに抵抗があると思われる。しかし、情報の安全管理を達成して説明責任を果たすためには、例え起こり得る可能性は低くても、万一に備えて対策する必要がある。また、説明責任を果たすため、これらのリスク分析の結果は文書化して管理する必要がある。この分析により得られた脅威に対して、6.3 章から6.12章の対策を行うことになる。

また、情報の安全管理や、個人情報保護法で原則禁止されている目的外利用の防止は、システム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保証することであり、これが限界である。したがって、人の行為も含めた脅威を想定し、運用を含めた対策を講じることが重要である。加えて、この観点から、組織が管理しない機器やソフトウェア、サービスの利用を禁止することが求められる。

リスク分析で明らかとなった脅威について対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要である。

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。
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。
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。
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
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。
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。
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。

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。

6.3. 組織的安全管理対策（体制、運用管理規程）

B. 考え方

安全管理について、従業者の責任と権限を明確に定め、規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で医療情報システムを利用するかどうかに関わらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

① 安全管理対策を講じるための組織体制の整備
② 安全管理対策を定める規程等の整備と規程等に従った運用
③ 医療情報の取扱い台帳の整備
④ 医療情報の安全管理対策の評価、見直し及び改善
⑤ 情報や端末の外部持ち出しに関する規則等の整備
⑥ 端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その端末等の管理規程
⑦ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程は極めて重要であり、必ず定めなければならない。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

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。
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。
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。
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。
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

6.4. 物理的安全対策

B. 考え方

物理的安全対策とは、医療情報システムにおいて個人情報が入力、参照又は格納される端末や情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義した上で、以下の事項を考慮して、適切に管理する必要がある。

- 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
- 盗難、覗き見等の防止
- 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

また、医療情報システムを格納するデータセンター等の場所については、6.2.3 章のリスク分析を踏まえて、適切に選定することが重要である。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

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。
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。
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。
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。
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。

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。

6.5. 技術的安全対策

B. 考え方

技術的な対策のみで全ての脅威に対抗できる保証はないため、運用管理による対策との併用は必須である。

しかし、その有効範囲を認識し適切な適用を行えば、技術的な対策は強力な安全管理の手段となり得る。ここでは 6.2.3 章のリスク分析で列挙した脅威[1]に対抗するために利用できる技術的な対策として下記の項目について解説する。

(1) 利用者の識別・認証
(2) 情報の区分管理とアクセス権限の管理
(3) 外部のアプリケーションとの連携における認証・認可
(4) アクセスの記録（以降、アクセスログという。）
(5) 不正ソフトウェア対策
(6) ネットワーク上からの不正アクセス
(7) 医療等分野における IoT 機器の利用

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

(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。

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は、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、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、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。

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

[1] 具体的な脅威については、別冊 6.2 を参照。

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。

(2) 情報の区分管理と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。ここで重要なことは、付与する利用権限を必要最小限にすることである。

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、その運用方法について組織の規程で定めなければならない。

また、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付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。

(3) 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。このことは、HL7 FHIR の規格を用いた API ごとの連携促進の観点からも重要な問題となる。

API 連携のセキュリティ確保のためには、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ー・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

(4) アクセスログ

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、さらにはセキュリティ事故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。したがって、アクセスログへのアクセス制限を行い、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なければならない。このためにログサーバで統合して管理し、ログサーバのアクセス制限を講じることも有効である。

また、アクセスログの証拠性確保のため、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。

加えて、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事業者に委託している場合には、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）を管理する必要がある。

(5) 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（以下「不正ソフトウェア」という。）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、情報の漏えいや改ざん、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。そして、何らかの問題が発生して初めて、不正ソフトウェアの侵入に気付くことになる。

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最も効果的であ

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。また、このことは医療機関等の外部で利用する端末や PC 等についても同様であるが、その考え方と対策については、6.9 章を参照すること。

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や検索エンジンを常に最新のものに更新しておく必要がある。

また、たとえ優れた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、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。

(6) ネットワーク上からの不正アクセス

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。

また、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）もあるため、医療情報システムと外部ネットワークとの関係に応じて、IDS、IPS の採用も検討すべきである。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。

さらに、近時のサイバー攻撃の高度化・多様化に鑑みると、上記対策等に加えて、不正ソフトウェアが侵入した場合を想定した内部脅威監視などのモニタリングを講じることも、有効な対策として挙げられる。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) 医療等分野における IoT 機器の利用

本節では、IoT 機器（センサ等で自動的に情報を取得し、又は他の機器が自動的に取得した情報を中継し、ネットワークを通じて他の医療情報システムに送信する機器）によって医療に関する個人の情報を取得し、ネットワークを介して収集する仕組みを利用する場合に遵守すべき事項を規定する。

なお、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」（昭和 35 年 8 月 10 日法律第 145 号）において定める医療機器のサイバーセキュリティの保全については、厚生労働省医薬・生活衛生局から発出されている「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 日付け薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号）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。

施設外からネットワークに接続する場合の基準については、6.11 章の規定を参照すること。

IoT セキュリティに関しては「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）が取りまとめられており、参考になる。

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。
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. 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。
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。
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。
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。
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。

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。
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、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。
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。
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。
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。
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、パスワード漏えい流出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。

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。

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やアップデートが困難な場合に代替措置を講じる方法を検討し、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。

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。

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。

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。
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。
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。
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。
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。

6.6. 人的安全対策

B. 考え方

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。

医療情報システムに関連する者として、次の 5 種類を想定する。

(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
(c) システムの保守事業者等、医療機関等とは雇用契約を結ばずに医療機関等の業務に携わる者
(d) 見舞い客等の医療情報にアクセスする権限を有しない第三者
(e) 診療録等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a)、(b)に対する人的安全対策は、医療機関等の従業者に対する人的安全管理措置、(c)に対する人的安全対策は、事務取扱受託業者の監督及び守秘義務契約として説明する。

(d)については、そもそも医療機関等の医療情報システムに触れてはならない者であるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万一、第三者によるサイバー攻撃等によってシステム内の情報漏えい等が発生した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、「外部保存」を受託する事業者等に該当するが、これに関しては詳細を 8 章に記述する。

また、近年、医療機関等を標的としたサイバー攻撃のリスクが高まっていることから、日本医療情報学会が公表している「標的型攻撃メールへの対処について」や情報処理推進機構の「対策のしおりシリーズ」等を参考に、標的型メール等のサイバー攻撃の対応について、従業者への教育を実施する必要がある。

C. 最低限のガイドライン

医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督するため、以下の措置をとること。

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。

(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。

(3) 従業者の退職後の個人情報保護規程を定めること。

2. 事務取扱受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。

(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。

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。

6.7. 情報の破棄

B. 考え方

医療に係る電子情報は、破棄を確実に行うことにより、破棄に際しても安全性を確保する必要がある。しかし、例えば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、注意しなくてはならない。

実際に破棄する場合に備えて、事前に破棄の手順を明確化しておくべきである。

C. 最低限のガイドライン

1. 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。
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。
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。
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。

6.8. 医療情報システムの改造と保守

B. 考え方

医療情報システムの可用性を維持するためには、定期的なメンテナンスが必要である。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、システムのメンテナンス要員が管理者モード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。

リスク分析で明らかとなった改造と保守において想定される脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。そのためには、①保守事業者との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の医療機関等の関係者による監督等の運用面を中心とする対策が必要である。

保守作業によっては保守事業者からさらに外部の事業者に再委託されることが考えられる。そのため、保守事業者との契約の締結に当たっては、再委託する事業者への個人情報保護の徹底等について医療機関等と保守事業者の契約と同等の契約を求めることも重要である。

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。
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。
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。
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。
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。
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。
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。

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。
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。
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。

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。
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。
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。
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。
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。
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。

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

情報又は情報機器の持ち出しについては組織的な対策が必要となり、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という方針が必要である。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた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、対策を検討しておくことが必要である。

この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、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、過誤のリスクの方が、医療機関等に設置されている医療情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

したがって、情報又は情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策を施す必要がある。

ノートパソコンや、タブレット、スマートフォン等を用いて医療情報システムにログインする場合においても、二要素認証を用いることが望ましい。利用者の識別・認証に係る説明や留意点については、6.5 章の記載を参照すること。

また、以降のガイドラインと内容は重複するが、タブレット PC 及びスマートフォンを用いる場合の守るべき事項をまとめると以下のようになる。

- 機器自体の管理を、運用管理規程を定めて実施すること。盗難・紛失を早期に発見することはもちろんのこと、不要なアプリの存在や、パスワードの設定が適切であること等を定期的に確認しなければならない。
- 端末自体の起動パスワード等の設定は必須であり、パスワードを用いる場合、パスワードは容易に推定されることがないものとし、かつ定期的な変更を行わなければならない。
- 端末内に患者等の情報が保存されている場合、あるいはアクセス先に存在する患者等の情報を表示や編集できる場合は、その機能を持つアプリ自体にもパスワードを設定し、端末内に情報が存在する場合は暗号化しなければならない。
- 業務に用いる機能に影響を与えないために、必要最小限のアプリ以外はインストールしないこと。OS のメモリ管理機能で、メモリを隔離して他のアプリの影響を受けないアプリが構築可能な場合は、確実にメモリ隔離ができることを確認することが必要である。
- ネットワークは 6.11 章の基準を満たしたもの以外は利用しないこと。特に公衆無線 LAN はリスクが大きいため、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、6.11 章の基準に則った利用を認める。また、自動的に公衆無線 LAN に接続してしまう端末も存在するので、業務アプリ起

動時に VPN 接続を確立しない場合は、公衆無線 LAN への自動接続機能を切る必要がある。

- 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（以下「BYOD」(Bring Your Own Device）という。）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えい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。
- 覗き見防止対策の実施が望ましい。

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。
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。
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。
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。
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。
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。
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。
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、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。

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。
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。

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。
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。
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。
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。

6.10. 災害、サイバー攻撃等の非常時の対応

B. 考え方

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。また、サイバー攻撃の場合は、自医療機関の診療等への影響だけでなく、他医療機関へ影響が波及することもあり、適切な対応が求められる。このような事態に可能な限り対応するためには、普段から想定されるあらゆるレベルの異常時について、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（BCP：Business Continuity Plan）と呼ぶ。

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る。

医療機関等全体の BCP は本ガイドラインの範疇を超えるため、ここでは自然災害やサイバー攻撃による IT 障害等の非常時に、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医療情報システムの BCP や留意事項について述べる。ただし、医療機関等全体の BCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならなければならないことはいうまでもない。

(1) 非常時における事業継続計画

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り下記の事項・フェーズごとに計画内容を事前演習等で検証することが望ましい。

① BCP として事前に周知しておく必要がある事項
② BCP 実行フェーズ
③ 業務再開フェーズ
④ 業務回復フェーズ
⑤ 全面復旧フェーズ
⑥ BCP の見直し

(2) 医療情報システムの非常時使用への対応

① 非常時用ユーザアカウントの用意

停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、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なくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データ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して

いる。ブレークグラスでは、非常時用ユーザアカウントの通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更することを基本としている。

② 非常時の運用に対応する機能の実装

災害時は、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。

上記のような非常時使用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る必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

(3) サイバー攻撃を受けた際の対応

医療情報システムに不正ソフトウェアが混入するなどによるサイバー攻撃を受けた場合、以下の対応等を行う必要が生じる場合がある。これらに備え、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。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、7.2 章及び 7.3 章も参照すること。

- 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
- 他の機器への混入拡大の防止や情報漏えいの抑止のための当該混入機器の隔離
- 他の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媒体と追記不能設定がなされた媒体の組み合わせ、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）で取得することが重要である）

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。

(4) 非常時に備えたセキュリティ体制の整備

非常時やサイバー攻撃などに対して、的確に対応できるためにセキュリティ体制を医療機関等においても構築することが求められる。非常時等において必要な原因関係の調査、必要なセキュリティ対応等に関する指揮、所管官庁等への報告などの体制については、医療の継続を確保する観点からも平常時から明確にする必要がある。

また、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、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなどが強く求められる。

また、日頃から脆弱性情報を収集し、速やかに対策を行える体制を整えておくことが

必要である。

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。
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。
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。
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。
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、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）

6.11. 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

B. 考え方

本章では、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。医療機関等において外部と個人情報を含む医療情報を交換する場合、医療情報システムを医療機関等が管理する内部ネットワークを通じて外部のネットワークに接続して利用することが考えられる。

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、「送付すべき相手に」、「正しい内容を」、「内容を盗み見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、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」等の脅威から守らなければならない。

医療機関はこれらの脅威に留意したうえで、医療情報システムに接続するネットワーク、機器、サービス等を適切に選定し、6.2.3 章のリスク分析を行い、6.2 章の情報セキュリティマネジメントシステム（ISMS）を実践することが必要である。

なお、可搬媒体や紙を用いて情報を搬送する場合は、付則 1 及び 2 を参照すること。

(1) 医療機関等における留意事項

医療機関等において、ネットワークを利用して医療情報を外部と交換する際の留意事項としては、

・「盗聴」の危険性に対する対応
・「改ざん」の危険性への対応
・「なりすまし」の危険性への対応
・適切な暗号鍵の管理

などが挙げられる。

(2) 選択すべきネットワークのセキュリティの考え方

医療情報を内部ネットワークと外部ネットワークを接続して交換する際、ネットワークの接続形態により選択すべきセキュリティの考え方が異なる。

・クローズドなネットワークで接続する場合
・オープンなネットワークで接続する場合
・モバイル端末等を使って医療機関等の外部から接続する場合

の 3 つの場合について、それぞれ接続先の医療機関等のネットワーク構成や経路設計によって、意図しない情報漏えいが起こる可能性について留意し、確認する責務がある。

①クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、インターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」等の危険性は比較的低い。ただし、「(1)医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、複数拠点の接続により内部ネットワークが拡張する場合、内部トラフィックにおける脅威の拡散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・パッチ等を適切に適用する等を行うことが求められる。

②オープンなネットワークで接続する場合

インターネットによる接続形態である。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を行わなければならない。すなわち、オブジェクト・セキュリティの考え方に沿った対策を施す必要がある。

オープンなネットワークで接続する場合であっても、電気通信事業者とクラウドサービス事業者が、これらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の判断で導入する必要がある。技術的な安全性についても自ら責任を持って担保できるよう、これら脅威に対する十分なセキュリティ対策を実施する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI（Open Systems Interconnection）階層モデル※」で定義される 7 階層のうち、どの階層でセキュリティを担保するかによって異なってくる。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 2 月）が参考になる。

※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

IPsec もしくは新たな技術によりそれと同等以上の安全性が担保されている VPN 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 の利用が求められる。

IPsec や TLS を採用する場合でも、その端末にオープンネットワークに対する開放されたポートがある場合には、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）等による攻撃からの防護について、適切な対策を実施する必要がある。

③モバイル端末等を使って医療機関等の外部から接続する場合

ここでは、携帯電話・PHS やノートパソコン、スマートフォン、タブレット等の、モバイル端末を用いて、医療機関等の外部から医療機関等内部のネットワークに接続する場合のセキュリティ要件を整理しておく。

外部からの接続については、6.8 章で述べた保守用途でのアクセス、医療機関等の職員による業務上のアクセス、さらには本節「(4)　患者等に診療情報等を提供する場合のネットワークに関する考え方」で述べた患者等からのアクセス等、様々なケースが想定される。

したがって、実際の接続において利用されるモバイル端末とネットワークの接続サービス及びそれらの組み合わせが、本章で説明する接続形態のどれに該当するかを明確に識別することが重要になる。具体的な接続方法との関係では以下の対応が必要である。

携帯電話・PHS 網を経由して、電気通信事業者の提供するサービスを利用してインターネットへ接続するケースでは、「②オープンなネットワークで接続されている場合」に相当する。したがって、セキュリティ上の要件は、そこでの記述を適用する必要がある。オープンなネットワークを経由するので、「(1)医療機関等における留意事項」で述べたオブジェクト・セキュリティとチャネル・セキュリティを担保するための対策が必要である。

オープンなネットワークを通じて閉域ネットワークへ接続するケースでは、「Ⅰ．クローズドなネットワークで接続する場合」における「③閉域 IP 通信網で接続されている場合」に相当するため、セキュリティ上の要件は、そこでの記述を適用する必要がある。クローズ

なネットワークを経由するため、比較的安全性は高い。

閉域ネットワークに到達するまでにオープンなネットワーク（インターネット）を経由する場合、サービス提供者によってはこの間でのチャネル・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、事前にサービス提供者との契約をよく確認して、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、ここで述べたようなモバイル接続形態に関連するセキュリティ要件に加え、医療機関等の外部で情報にアクセスするという行為自体に特有のリスクが存在する。

例えば、機密情報が格納されたモバイル端末の盗難や紛失等の管理面のリスク、さらには公共の場所で情報を閲覧することによる他者からの覗き見等による機密漏えいのリスク等である。

(3) 従業者による外部からのアクセスに関する考え方

医療機関等の職員がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可することもあり得る。このような場合のネットワークに関わる安全管理の要件は既に述べたが、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。加えて、外部からのアクセスに用いる機器の安全管理を運用管理規程で定めることが重要ではあるが、その場合に考慮すべき点が 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、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、医療機関等の管理下にある機器を必要に応じて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、医師不足等に伴う医療従事者の過剰労働等に対応するために、従業者による外部からのアクセスを行う場合は、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の導入を検討するとともに、運用等の要件にも相当な厳しさが求められる。

(4) 患者等に診療情報等を提供する場合のネットワークに関する考え方

診療情報等の開示が進む中、ネットワークを介して患者（又は家族等）に診療情報等を提供したり、医療機関内の診療情報等を閲覧させる可能性も出てきた。本ガイドラインは、医療機関等の間における医療情報の交換を想定しているが、患者等に対する診療情報等の提供も十分想定される状況にある。患者等に診療情報等を提供する場合には、ネットワークのセキュリティ対策のみならず、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、診療情報等の主体者となる患者等へ危険性や提供目的の納得できる説明、また非 IT に関わる各種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した上で実施しなくてはならない。

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。
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。
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。
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。

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。
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）
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。
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。

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。
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。
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。
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。
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。

D. 推奨されるガイドライン

1. 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。

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

A. 制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　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。

二　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。

（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）

B. 考え方

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・保存が可能となった。

近年、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）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、A 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、7 章及び 9 章の対象となる文書は、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、「A. 制度上の要求事項」の一、二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（ISO 14533-1:2014 CMS利用電子署名(CAdES)の長期署名プロファイル、ISO 14533-2:2021 XML 署名利用電子署名(XAdES)の長期署名プロファイル、ISO 14533-3:2017 PDF長期署名プロファイル(PAdES)、ISO 14533-4:2019 proof of existence objects)。

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。

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。

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）。

- 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」（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。

7. 電子保存の要求事項について

本章の規定は、3.1 章において、7 章及び 9 章の対象として挙げられている文書等を電子保存する場合に適用される。

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、煩わしさばかりが大きくなったりすることが想定されるため、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よう、運用面と技術面の対応を検討すること。

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。

（e-文書法省令　第 4 条第 4 項第 2 号）

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　2（3）②）

「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。

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、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。

具体的には、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。

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、更新履歴の保存において、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）。

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。
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。

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。

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。

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。

【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最低限のガイドラインに加え、次の事項が必要となる。

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。

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。

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。

なお、これらの具体的要件については、6.11 章「外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理」を参照すること。

7.2. 見読性の確保について

A. 制度上の要求事項

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。

（e-文書法省令　第4条第4項第1号）

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。

（施行通知　第2　2（3）①）

「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

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である。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に表示できることが求められることもあるため、必要に応じてこれに対応することを考慮する必要がある。

また、何らかのシステム障害が発生した場合においても、診療に重大な支障がない最低限の見読性を確保する対策も考慮に含める必要がある。特に、災害等の非常時には、システムが完全に停止してしまうおそれもあるため、定期的なバックアップを実施して、診療録等に記載された患者情報を確認できるようにしておくことが望ましい。

保存していた情報が毀損した場合等は、可能な限り速やかな復旧に努め、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応える見読性の確保を図らなければならない。

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。

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。

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。

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。

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。

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。

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。

【ネットワークを通じて外部に保存する場合】

医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。

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。

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。

7.3. 保存性の確保について

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。

（e-文書法省令　第4条第4項第3号）

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。

（施行通知　第2　2（3）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

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をいう。

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、例えば下記のものが考えられる。

・コンピュータ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
・不適切な保管・取扱いによる情報の滅失、破壊
・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
・媒体・機器・ソフトウェアの不整合による情報の復元不能
・障害等によるデータ保存時の不整合

保存性の確保に対するこれらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

具体的には、不正ソフトウェアによる情報の破壊及び混同等、不適切な保管・取扱いによる情報の滅失、破壊、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、媒体・機器・ソフトウェアの不整合による情報の復元不能、障害等によるデータ保存時の不整合など原因に対する技術面及び運用面での対策が求められる。

なおサイバー攻撃等については、6.10章を参照すること。

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。
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。
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。
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。

【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最低限のガイドラインに加え、次の事項が必要となる。

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。

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。

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。

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。

8. 診療録及び診療諸記録を外部に保存する際の基準

※ 本章の規定は、3.2 章において、8 章の対象として挙げられている文書等を電子保存する場合に適用される。

診療録等の保存場所に関する基準は、2 つの場合に分けて考える必要がある。一つは電子媒体により外部保存を行う場合で、もう一つは紙媒体のままで外部保存を行う場合である。さらに、電子媒体の場合、ネットワークを通じて外部保存を行う場合が特に規定されていることから、実際には次の 3 つに分けて考える必要がある。

(1) 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
(2) 電子媒体による外部保存を磁気テープ、CD-R、DVD-R 等の可搬媒体で行う場合
(3) 紙やフィルム等の媒体で外部保存を行う場合

このうち電子媒体による外部保存を、可搬媒体を用いて行う場合については、付則 1 へ移動したのでそちらを参照すること。

また紙媒体のままで外部保存を行う場合については、付則 2 へ移動したのでそちらを参照すること。

ネットワークを経由して診療録等を電子媒体によって外部に保存する場合は、6.11 章を参照し、安全管理に関して医療機関等が主体的に責任を負い適切に推進することが求められる。

8.1. 電子保存の 3 基準の遵守

3 基準の記載については、7.1 章、7.2 章及び 7.3 章にそれぞれ統合したので、そちらを参照すること

8.2. 運用管理規程

A. 制度上の要求事項

外部保存を行う病院､診療所等の管理者は､運用管理規程を定め､これに従い実施すること。

（外部保存改正通知　第３　1）

B. 考え方

外部保存に係る運用管理規程を定めることが求められており、考え方及び具体的なガイドラインは、6.3 章の項を参照すること。

また、その際の責任のあり方については、4 章を参照すること。

なお､既に電子保存の運用管理規程を定めている場合には､外部保存に対する項目を適宜修正・追加等すれば足りると考えられる。

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

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（個人情報保護法　第 23 条）

電気通信回線を通じて外部保存を行う場合にあっては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第 1 条の 5 第 1 項に規定する病院又は同条第 2 項に規定する診療所その他これに準ずるものとして医療法人等が適切に管理する場所、行政機関等が開設したデータセンター等、及び医療機関等が民間事業者等との契約に基づいて確保した安全な場所に置かれるものであること。

（外部保存改正通知　第２　１　(2)）

B. 考え方

特に「２　医療機関等が外部の事業者に対して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」には、データセンター等の情報処理を受託する事業者が総務省・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、契約等でその遵守状況を明らかにしなくてはならない。なお、データセンターについては、個人情報保護法の改正により、民間事業者においても安全管理に関する法律上の義務が生じるようになったことから、行政機関等が開設したデータセンター等と契約に基づいて確保した安全な場所である民間事業者が開設したデータセンターとは区別せず、同一の要求事項が求められる。

外部保存を受託する事業者の選定基準や情報の扱い、情報の提供にあたっては、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、又は医療機関等が外部の事業者等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のそれぞれにおいて、適切に対応する必要がある。

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。

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。

(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

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。
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。
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。

8.4. 個人情報の保護

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（委託先の監督）

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。

（個人情報保護法　第 23 条、第 25 条）

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。

（外部保存改正通知　第２　１（3））

B. 考え方

ネットワークを通じて外部に保存する場合、医療機関等の管理者の権限や責任の範囲が、自機関等の施設とは異なる施設や電気通信事業者にも及ぶために、より一層、個人情報の保護に配慮することが必要となる。

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。

ネットワークを通過する際の個人情報保護は、通信手段の種類によって個別に考える必要がある。通信手段の違いによる情報の秘匿性確保に関しては 6.11 章「 (2)選択すべきネットワークのセキュリティの考え方」で触れているので、そちらを参照すること。

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。

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。

8.5. 責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　１（4））

本項の記載は、4 章及び 6.11 章に考え方を集約したため、それらを参照すること。

8.5.1. 留意事項

ネットワークを通じて外部保存を行い、これを外部保存を受託する事業者において可搬媒体に保存する場合にあっては、付則 1 に掲げる事項についても十分留意すること。

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

※ 本章の規定は、「3.1　7 章及び 9 章の対象となる文書について」において、7 章及び 9 章の対象として挙げられている文書等をスキャナ等により電子化して保存する場合に適用される。

本章は法令等で作成又は保存を義務付けられている診療録等を一旦紙等の媒体で作成されたものを受領又は保存又は運用した後に、スキャナ等で電子化し、保存又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（人体図）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いため、7 章の真正性の確保を参照すること。

A. 制度上の要求事項

民間事業者等が、法第三条第一項の規定に基づき、別表第一の一及び二の表の上欄に掲げる法令のこれらの表の下欄に掲げる書面の保存に代えて当該書面に係る電磁的記録の保存を行う場合並びに別表第一の四の表の上欄に掲げる法令の同表の下欄に掲げる電磁的記録による保存を行う場合は、次に掲げる方法のいずれかにより行わなければならない。

一　（略）

二　書面に記載されている事項をスキャナ（これに準ずる画像読取装置を含む。）により読み取ってできた電磁的記録を民間事業者等の使用に係る電子計算機に備えられたファイル又は磁気ディスク等をもって調製するファイルにより保存する方法

（e-文書法省令　第 4 条）

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**

紙の調剤済み処方箋も、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、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**

この節では、この上記のいずれにも該当する、つまり「診療等の都度スキャナ等で電子化して保存する場合」及び「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。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。このような場合の対策に関しては、9.5 章で述べる。

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。
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。

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。

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

B. 考え方

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。

この場合、「9.1　共通の要件」を満たした上で、さらに改ざん動機が生じないと考えられる時間内に、適切に電子化が行われることが求められる。

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。

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

B. 考え方

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。このような場合、改ざん動機の生じる可能性の低い、9.2 章の「診療等の都度スキャナ等で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、9.1 章の要求を全て満たした上で、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。

C. 最低限のガイドライン

9.1 章の対策に加えて、以下の対策を実施すること。

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。
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
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。
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。

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

B. 考え方

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。

なお、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）。

なお、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。

C. 最低限のガイドライン

9.1 章の対策に加えて、次に掲げる対策を実施すること。

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。
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。

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

B. 考え方

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。

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。

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。
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。

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。

10. 運用管理について

「運用管理」において運用管理規程は管理責任や説明責任を果たすために極めて重要であり、運用管理規程は必ず定めなければならない。

A. 制度上の要求事項

(1) 「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」

Ⅰ　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

ーーー個人情報の取扱いに関する明確かつ適正な規則を策定し、それらを対外的に公表することが求められる。

ーーー個人情報の取扱いに関する規則においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続き、第三者提供の取扱い、苦情への対応等について具体的に定めることが考えられる。

Ⅳ　7（2）①個人情報保護に関する規程の整備、公表

ーーー個人情報保護に関する規程を整備し、ーーー。

個人データを取り扱う情報システムの安全管理措置に関する規程等についても同様に整備を行うこと。

(2) その他の要求事項

診療録等の電子保存を行う場合の留意事項

1　施設の管理者は診療録等の電子保存に係る運用管理規程を定め、これに従い実施すること。

2　運用管理規程には以下の事項を定めること。

(1) 運用管理を総括する組織・体制・設備に関する事項

(2) 患者のプライバシー保護に関する事項

(3) その他適正な運用管理を行うために必要な事項

（施行通知　第 3）

電子媒体により外部保存を行う際の留意事項

1　外部保存を行う病院、診療所等の管理者は運用管理規程を定め、これに従い実施すること。なお、既に診療録等の電子保存に係る運用管理規程を定めている場合は、適宜これを修正すること。

2　1 の運用管理規程の策定にあたっては、診療録等の電子保存に係る運用管理規程で必要とされている事項を定めること。

（外部保存改正通知　第 3）

B. 考え方

医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の 4 章から 9 章の記載に従い、定めるべき管理項目を記載している。1.に電子保存する・しないに拘らず必要な一般管理事項を、2.に電子保存のための運用管理事項を、3.に外部保存のための運用管理事項を、4.にスキャナ等を利用した電子化、5.に運用管理規程の作成に当たっての手順を記載している。

電子保存を行う医療機関等は 1.、2.及び 4.の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに 3.の管理事項を合わせて採用する必要がある。

運用管理規程等の作成に際しては、以下の文書を参照することが有用である。

- 監査証跡の取り組み方については、「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）を参考にすること。
- 技術的対応の検討のための情報収集には、6.2 章 B で紹介している「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　チェックリスト」を参考にすること。

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

(1)　総則

a　理念（基本方針と管理目的の表明）

b　対象情報

(a) 医療情報システムで扱う全ての情報のリストアップ

(b) 安全管理上の重要度に応じた分類

(c) 医療リスク分析

c　医療情報システムにおいて採用し変更をフォローすべき標準規格

(2)　管理体制

a　システム管理者、機器管理者、運用責任者、安全管理者、個人情報保護責任者等

b　マニュアル・契約書等の文書の管理体制

c　監査体制と監査責任者

d　患者及びシステム利用者からの苦情・質問の受け付け体制

e　事故対策時の責任体制

f　システム利用者への教育・訓練等の周知体制

(3)　管理者及び利用者の責務

a　システム管理者や機器管理者、運用責任者の責務

b　監査責任者の責務

c　利用者の責務

(a) 監査証跡の取り組み方については、「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）を参考にすること。

(4)　一般管理における運用管理事項

a　来訪者の記録・識別、入退の制限等の入退管理規程

b　情報保存装置、アクセス機器の設置区画の管理・監視規程

c　情報へのアクセス権限の決定方針

d　個人情報を含む記録媒体の管理（保管・授受等）規程

e　個人情報を含む媒体の廃棄の規程

f　リスクに対する予防措置、発生時の対応方法

g　医療情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理規程

h　システムの導入に際して、技術的に対応するか、運用によって対応するかを判定し、その内容を文書化し管理する旨の規程

(a) 技術的対応の検討のための情報収集には、6.2 章 B で紹介している「『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』ガイドチェックリスト」を参考にすること。

i　技術的安全対策規程

(a) 利用者識別と認証の方法

(b) IC カード等セキュリティ・デバイス配布の方法

(c) 情報区分とアクセス権限管理及び人事異動等に伴う見直し

(d) アクセスログ取得と監査の手順

(e) 時刻同期の方法

(f) 不正ソフトウェア対策

(g) ネットワークからの不正アクセス対策

(h) パスワードの管理

j　IoT 機器の利用に関する事項

(a) IoT 機器の貸し出しに関するリスク受容の合意

(b) 異常時の患者及び医療機関等の役割、連絡先

(c) 異常の検知方法

(d) セキュリティ上重要なアップデートの方法

(e) 使用終了後又は停止中の不正接続対策

k　無線 LAN に関する事項

(a) 無線 LAN 設定（アクセス制限、暗号化等）

(b) 電波障害のおそれがある機器の使用制限

l 電子署名・タイムスタンプに関する規程

(a) 対象となる発行文書、電子署名付き受領文書の取扱規程、日常的運用管理規程

(5) 業務委託（システムの運用・保守・改造）の安全管理措置

a 業務委託契約における安全管理・守秘条項

b 再委託の場合の安全管理措置事項

c システム改造及び保守での医療機関等関係者による作業管理・監督、作業報告確認

(a) 保守要員専用のアカウントの作成及び運用管理

(b) 作業時のデータアクセス範囲の確認

(c) アクセスログの採取と確認

※ リモートメンテナンスには下記(7)も参照。

(6) 情報及び情報機器の持ち出しについて

a 持ち出し対象となる情報及び情報機器の規程

b 持ち出した情報及び情報機器の運用管理規程

c 持ち出した情報及び情報機器への安全管理措置

d 盗難、紛失時の対応策

e 利用者への周知徹底方法

(7) 外部の機関と医療情報を提供・委託・交換する場合

a 安全を技術的、運用的面から確認する規程

b リスク対策の検討文書の管理規程

c 情報処理を受託する事業者等との通常運用時、事故対処時それぞれでの責任分界点を定めた契約文書の管理と契約状態の維持管理規程

d リモートメンテナンスの基本方針

(a) 保守事業者によるリモートメンテナンス体制の安全性確認

e 従業者による医療機関等の外部からアクセスする場合の運用管理規程

(a) アクセスに用いる機器の安全管理

(8) 災害、サイバー攻撃等の非常時の対応

a BCP の規程における医療情報システムの項

b システムの縮退運用管理規程

c 非常時の機能と運用管理規程

d 報告先と内容一覧

(9) 教育と訓練

a マニュアルの整備

b　定期又は不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修

c　従業者に対する人的安全管理措置

(a) 医療従事者以外との守秘契約

(b) 従事者退職後の個人情報保護規程

(10) 監査

a　監査の内容

b　監査責任者の任務

c　アクセスログの監査

(11) 規程の見直し

a　運用管理規程の定期的見直し手順

2.　電子保存のための運用管理事項

(1)　真正性確保

a　入力者及び確定者の識別・認証

b　記録の確定手順と、識別情報の記録

c　更新履歴の保存

d　代行入力の承認記録

e　機器・ソフトウェアの品質管理、動作状況の内部監査規程

(2)　見読性確保

a　情報の所在管理

b　見読化手段の管理

c　見読目的に応じた応答時間とスループット

d　システム障害対策

(a) 冗長性

(b) バックアップ

(c) 緊急対応

(3)　保存性確保

a　ソフトウェア・機器・媒体の管理（例えば、設置場所、施錠管理、定期点検、不正ソフトウェアチェック等）

(a) 不正ソフトウェアによる情報の破壊及び混同等の防止策

b　不適切な保管・取扱いによる情報の滅失、破壊の防止策

(a) バックアップ、作業履歴管理

c　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策

d　媒体・機器・ソフトウェアの不整合による復元不能の防止策

(a) システムの移行時のデータベースの不整合、機器・媒体の互換性不備に備えたシステム変更・移行時の業務計画の作成規約

(4)　相互運用性確保

a システムの改修に当たっての、データ互換性の確保策

b システムの更新に当たっての、データ互換性の確保策

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。

(1)　管理体制と責任

a　委託する事業者選定規約、選定時に「適合」と判断した根拠記載の規程

(a) 受託事業者が医療機関等以外の場合には、8.1.2 章に記された要件を参照すること。

(b) 医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合には、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」に準拠していることを確認する規程

b　医療機関等における管理責任者

c　受託事業者への監査体制

d　受託事業者、回線事業者等との責任分界点

e　受託事業者、回線事業者等の管理責任、説明責任、定期的に見直し必要に応じて改善を行う責任の範囲を明文化した契約書等の文書作成と保管

f　不都合な事態が発生した場合における対処責任、障害部位を切り分ける責任所在を明文化した契約書等の文書作成と保管

(a) 受託事業者が医療機関等以外の場合には、「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」に記された要件を参照すること。

g　外部に保存を委託する文書の選定基準

(2)　外部保存契約終了時の処理

a　受託事業者に診療録等が残ることがない処理方法の規程

(a) 受託事業者に診療録等が残ることがないことの契約、管理者による確認

(3)　真正性確保

a　相互認証機能の採用

b　電気通信回線上で「改ざん」されていないことの保証機能

(4)　見読性確保

a　施設内保存と同項目 2（2）の確認

b　緊急に必要になることが予測される医療情報の見読性の確保手段（推奨）

c　緊急に必要になるとまではいえない医療情報の見読性の確保手段（推奨）

(5)　保存性確保

a　外部保存を受託する事業者での保存確認機能

b　施設内保存と同項目 2（3）（4）の確認

c　標準的なデータ形式及び転送プロトコルの採用（推奨）

d　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確保

(6)　診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護

a　秘匿性の確保のための適切な暗号化

b　通信の起点・終点識別のための認証

(7)　診療録等の外部保存を受託する事業者内での個人情報の保護

a　外部保存を受託する事業者における個人情報保護

b　外部保存を受託する事業者における診療録等へのアクセス禁止

受託する事業者が医療機関等以外の場合には、8.3 章に記された要件を参照すること。

c　障害対策時のアクセス通知

d　アクセスログの完全性とアクセス禁止

(8)　患者への説明

a　診療開始前の説明方法

b　患者本人の理解を得ることが困難であるが診療上の緊急性がある場合の説明方法

c　患者本人の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の説明方法

(9)　受託事業者に対する監査項目

a　保存記録（内容、期間等）

b　受託事業者における管理策とその実施状況監査

4.　スキャナ等により電子化して保存する場合

(1)　スキャナ読み取りの対象文書の規程

(2)　スキャナ読み取り電子情報と原本と同等であることを担保する情報作成管理者の任命

(3)　スキャナ読み取り電子情報への作業責任者（実施者又は情報作成管理者）の電子署名法に適合した電子署名

(4)　診療等の都度、スキャンするタイミングに関する規程

(5)　過去に蓄積された文書を電子化する場合の、実施手順規程

5.　運用管理規程の作成に当たって

運用管理規程は、システムの運用を適正に行うためにその医療機関等ごとに策定されるものである。すなわち、各々の医療機関等の状況に応じて自主的な判断の下に策定されるものである。もちろん、独自に一から作成することも可能であるが、記載すべき事項の網羅性を確保することが困難なことが予想されるため、付表 1～付表 3 に運用管理規程文案

を添付する。

付表 1 は電子保存する・しないに拘らず一般的な運用管理の実施項目例、付表 2 は電子保存における運用管理の実施項目例であり、付表 3 はさらに外部保存の場合において追加すべき運用管理の実施項目例である。

したがって、外部保存の場合は、付表 1 から付表 3 の項目を運用管理規程に盛り込むことが必要となる。

「運用管理規程」が 1 冊の独立した文書である必要性はない。実際の運用に当たって使用される管理規程を定めた文書類の中に、本ガイドラインで記載され本章にまとめられた内容が記載されていれば良い。しかし、日常運用及び見直し・改定のことを考慮し、業務単位に分かりやすくまとまっていることが大事である。

運用管理規程書を作成する場合の推奨手順は以下のとおりである。

ステップ 1：全体の構成及び目次の作成

全体の章立てと節の構成を決める場合に、本章の項目と付表の「運用管理項目」、「実施項目」を参照し、医療機関等ごとの独自性を考慮する方法で全体の構成を作成する。

この際、電子保存及び外部保存のシステムに関する運用管理規程だけではなく、医療情報システム全体の総合的な運用管理規程の構成とすることが重要である。

ステップ 2：運用管理規程文の作成

運用管理規程文の作成には、付表の「運用管理規程文例」を参考にして作成する。

特に、大規模／中規模病院用と小規模病院／診療所用では、運用管理規程文の表現が大きく異なることを想定して、付表に「対象区分」欄を設けている。大規模／中規模病院の場合は、対象区分の A と B の運用管理規程文例を選択し、小規模病院／診療所の場合は、対象区分の A と C の運用管理規程文例を選択することを推奨する。

ステップ 3：全体の見直し及び確認評価

運用管理規程の全体が作成された段階で、医療機関等の内部の関係者等にレビューを行い、総合的視点で実施運用が可能か評価し改善する。

なお、運用管理規程は単に策定すれば良いというものではなく、策定（Plan）された管理規程に基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Action）していかねばならない。この PDCA サイクルを適切に廻しながら、改善活動を伴う継続的な運用を行うことが重要である。

付則１　電子媒体による外部保存を可搬媒体を用いて行う場合

電子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えいや大幅な書換え等の危険性は少なく、注意深く運用すれば真正性の確保が容易になる可能性がある。

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。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媒体を用いればさらに機密性は増す。

したがって、一般的には付則 2 の紙媒体による外部保存の基準に準拠していれば大きな問題はないと考えられる。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、一媒体あたりに保存される情報量が極めて多いことから、媒体を遺失した際に紛失、漏えい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。

なお、診療録等のバックアップ等、法令で定められている保存義務を伴わない文書を外部に保存する場合についても、個人情報保護の観点から保存義務のある文書と同等に扱うべきである。

付則 1.1　電子保存の 3 基準の遵守

A. 制度上の要求事項

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

診療録等を医療機関等の内部に電子的に保存する場合に必要とされる真正性、見読性、保存性を確保することで概ね対応が可能と考えられるが、これに加え、搬送時や外部保存を受託する事業者における取扱いに注意する必要がある。

具体的には、以下について対応が求められる。

(1) 搬送時や外部保存を受託する事業者の障害等に対する真正性の確保
(2) 搬送時や外部保存を受託する事業者の障害等に対する見読性の確保
(3) 搬送時や外部保存を受託する事業者の障害等に対する保存性の確保

C. 最低限のガイドライン

1. 搬送時や外部保存を受託する事業者の障害等に対する真正性の確保

(1) 可搬媒体を授受する際に、明確な記録を行うこと。

可搬媒体の授受及び保存状況を確実に記録し、事故､紛失や窃盗を防止することが必要である。また、他の保存文書等との区別を行うことにより、混同を防止しなければならない。

(2)　媒体を変更したり､更新したりする際に、明確な記録を行うこと

2.　搬送時や外部保存を受託する事業者の障害等に対する見読性の確保

(1)　診療に支障が生じないようにすること

患者の情報を可搬媒体で外部に保存する場合、情報のアクセスに一定の搬送時間が必要であるが、患者の病態の急変や救急対応等に備え、緊急に診療録等の情報が必要になる場合も想定しておく必要がある。

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ることから、患者の診療情報が緊急に必要になることが予測され、搬送に要する時間が問題になるような診療に関する情報は、内部に保存するか、外部に保存するとしても、保存情報の複製又はそれと実質的に同等の内容を持つ情報を、委託する医療機関等の内部に保存しておかなければならない。

(2)　監査等に差し支えないようにすること

監査等は概ね事前に予定が判明しており、緊急性を求められるものではないことから､搬送に著しく時間を要する遠方に外部保存しない限り､問題がないと考えられる。

3.　搬送時や外部保存を受託する事業者の障害等における保存性の確保

(1)　標準的なデータ形式の採用

システムの更新等に伴う相互運用性を確保するために、データの移行が確実にできるように、標準的なデータ形式を用いることが望ましい。

(2)　媒体の劣化対策

媒体の保存条件を考慮し、例えば、磁気テープの場合、定期的な読み書きを行う等の劣化対策が必要である。

(3)　媒体及び機器の陳腐化対策

媒体や機器が陳腐化した場合、記録された情報を読み出すことに支障が生じるおそれがある。したがって、媒体や機器の陳腐化に対応して、新たな媒体又は機器に移行することが望ましい。

付則 1.2　個人情報の保護

A. 制度上の要求事項

(安全管理措置)

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

(委託先の監督)

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。
（個人情報保護法　第 23 条、第 25 条）

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。
（外部保存改正通知　第 2　1（3））

B. 考え方

平成 27 年度改正個人情報保護法が成立し、医療等分野において「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」が策定された。医療において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイダンスを参照し、十分な安全管理策を実施することが必要である。

診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者の統括によって、個人情報が保護されている。

しかし、可搬媒体を用いて外部に保存する場合、委託する医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶため、より一層の個人情報保護への配慮が必要である。

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、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

C. 最低限のガイドライン

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

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に注意する必要がある。

(1) 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によって、遺失の危険性を軽減すること。

(2) 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たり、同時に搬送しないことによって、その危険性を軽減すること。

(3)　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するとともに、守秘義務に関する事項等を契約上明記すること。

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

外部保存を受託する事業者が、委託する医療機関等からの求めに応じて、保存を受託した診療録等における個人情報を検索し、その結果等を返送するサービスを行う場合や、診療録等の記録された可搬媒体の授受を記録する場合、受託する事業者に障害の発生した場合等に、診療録等にアクセスをする必要が発生する可能性がある。このような場合には、次の事項に注意する必要がある。

(1)　外部保存を受託する事業者における医療情報へのアクセスの禁止

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。

(2)　障害発生時のアクセス通知

診療録等を保存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。

(3)　外部保存を受託する事業者との守秘義務に関する契約

診療録等の外部保存を受託する事業者は、法令上の守秘義務を負っていることからも、委託する医療機関等と受託する事業者、搬送業者との間での責任分担を明確化するとともに、守秘義務に関する事項等を契約に明記する必要がある。

(4)　外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関しては、最終的に診療録等の保存義務のある医療機関等が責任を負わなければならない。したがって、委託する医療機関等は、受託する事業者における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

「C. 最低限のガイドライン」に加えて以下の対策を行うことが推奨される。

1.　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、診療を開始する必要がある。

(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の同意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る。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。

付則 1.3　責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　１（4））

B. 考え方

診療録等を電子的に記録した可搬媒体で外部の機関に保存する場合であっても、責任に対する考え方は 4.1 章や 4.2 章と同様に整理する必要がある。

これらの考え方に則れば、実際の管理や部分的な説明の一部を委託先の機関や搬送業者との間で分担して問題がないと考えられる。

また、万一事故が起きた場合に、患者に対する責任は、4.1 章における事後責任となり、説明責任は委託する医療機関等が負うものである。ただし、適切に善後策を講ずる責任を果たし、あらかじめ 4.2 章の責任分界点を明確にしておけば、受託する事業者や搬送業者等は、委託する医療機関等に対して契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 通常運用における責任の明確化
(2) 事後責任の明確化

C. 最低限のガイドライン

1. 通常運用における責任の明確化

(1) 説明責任

利用者を含めた保存システムの管理運用体制について、患者や社会に対して十分に説明する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託する事業者にさせることは問題がない。

(2) 管理責任

媒体への記録や保存等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託する事業者に行わせることは問題がない。

(3) 定期的に見直し必要に応じて改善を行う責任

可搬媒体で搬送し、外部に保存したままにするのではなく、運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していかなくてはならない。

したがって、医療機関等の管理者は、現行の運用管理全般の再評価・再検討を常にこころがけておく必要がある。

2. 事後責任の明確化

診療録等の外部保存に関して、委託する医療機関等、受託する事業者及び搬送業者の間で「4.2 委託と第三者提供における責任分界」を参照しつつ、管理・責任体制を明確に規定して、次に掲げる事項を契約等で交わすこと。

(1) 委託する医療機関等で発生した診療録等を、外部に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
(2) 委託する医療機関等と搬送（業）者で可搬媒体を授受する場合の方法と管理方法
(3) 事故等で可搬媒体の搬送に支障が生じた場合の対処方法
(4) 搬送中に情報漏えいがあった場合の対処方法
(5) 受託する事業者と搬送（業）者で可搬媒体を授受する場合の方法と管理方法
(6) 受託する事業者で個人情報を用いた検索サービスを行う場合、作業記録と監査方法、取扱い従業者等の退職後も含めた秘密保持に関する規定、情報漏えいに関して患者からの照会があった場合の責任関係
(7) 受託する事業者が、委託する医療機関等の求めに応じて可搬媒体を返送すること

ができなくなった場合の対処方法

(8) 外部保存を受託する事業者に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

付則 1.4　外部保存契約終了時の処理について

診療録等が高度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、委託する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らない。

外部保存の開始には何らかの期限が示されているはずであり、外部保存の終了もこの前提に基づいて行わ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り得るし、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こともあり得る。

いずれにしても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、処理が厳正に執り行われたかを監査しなくてはならない。また、受託する事業者も、委託する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、処理を行った旨を委託する医療機関等に明確に示す必要がある。

当然のことであるが、これらの廃棄に関わる規定は、外部保存を開始する前に委託する医療機関等と受託する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、実際の廃棄に備えて、事前にソフトウェアの廃棄等の手順を明確化したものを作成しておくべきである。

委託する医療機関等及び受託する事業者双方に厳正な取扱いを求めるのは、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、そのことに十分なことに留意しなければならない。

また、患者の個人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、及び検索記録も機密保持できる状態で廃棄しなければならない。

さらに、委託する医療機関等及び受託する事業者が負う責任は、先に述べたとおりであり、可搬媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことに十分留意する必要がある。

付則２　紙媒体のままで外部保存を行う場合

紙媒体とは、紙だけを指すのではなく、X線フィルム等の電子媒体ではない物理媒体も含む。検査技術の進歩等によって、医療機関等では保存しなければならない診療録等が増加しており、その保存場所の確保が困難な場合も多い。本来、法令に定められた診療録等の保存は、証拠性と同時に、有効に活用されることを目指すものであり、整然と保存されるべきものである。

一定の条件の下では、従来の紙媒体のままの診療録等を当該医療機関等以外の場所に保存することが可能になっているが、この場合の保存場所も可搬媒体による保存と同様、医療機関等に限定されていない。

しかしながら、診療録等は機密性の高い個人情報を含んでおり、また必要な時に遅滞なく利用できる必要がある。保存場所が当該医療機関等以外になることは、個人情報が存在する場所が拡大することになり、外部保存に係る運用管理体制を明確にしておく必要がある。また、保存場所が離れるほど、診療録等を搬送して利用可能な状態にするのに時間がかかるのは当然であり、診療に差し障りのないように配慮しなければならない。

さらに、紙やフィルムの搬送は注意深く行う必要がある。可搬媒体は内容を見るために何らかの装置を必要とするが、紙やフィルムは単に露出するだけで、個人情報が容易に漏出するからである。

付則 2.1　利用性の確保

A. 制度上の要求事項

診療録等の記録が診療の用に供するものであることにかんがみ、必要に応じて直ちに利用できる体制を確保しておくこと。

（外部保存改正通知　第２　２（1））

B. 考え方

一般に、診療録等は、患者の診療や説明、監査、訴訟等のために利用するが、あらゆる場合を想定して、診療録等をいつでも直ちに利用できるようにすると解釈すれば、事実上、外部保存は不可能となる。

診療の用に供するという観点から考えれば、直ちに特定の診療録等が必要な場合としては、継続して診療を行っている患者等、緊急に必要になることが容易に予測される場合が挙げられる。具体的には、以下について対応が求められる。

(1) 診療録等の搬送時間
(2) 保存方法及び環境

C. 最低限のガイドライン

1. 診療録等の搬送時間

外部保存された診療録等を診療に用いる場合、搬送の遅れによって診療に支障が生じないようにする対策が必要である。

(1) 外部保存の場所

搬送に長時間を要する機関に外部保存を行わないこと。

(2) 複製や要約の保存

継続して診療を行っている場合等で、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、外部に保存する場合でも、診療に支障が生じないようコピーや要約等を内部で利用可能にしておくこと。

また、継続して診療している場合であっても、例えば入院加療が終了し、適切な退院時要約が作成され、それが利用可能であれば、入院時の診療録等自体が緊急に必要になる可能性は低下する。ある程度時間が経過すれば外部に保存しても診療に支障をきたすことはないと考えられる。

2. 保存方法及び環境

(1) 診療録等の他の保存文書等との混同防止

診療録等を必要な利用単位で選択できるよう、他の保存文書等と区別して保存し、管理しなければならない。

(2) 適切な保存環境の構築

診療録等の劣化、損傷、紛失、窃盗等を防止するために、適切な保存環境・条件を構築・維持しなくてはならない。

付則 2.2 個人情報の保護

A. 制度上の要求事項

(安全管理措置)

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

(委託先の監督)

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。

(個人情報保護法　第 23 条、第 25 条)

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。

(外部保存改正通知　第 2　2 (2))

B. 考え方

平成 27 年度改正個人情報保護法が成立し、医療等分野において「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」が策定された。医療において扱われる健康情報は極めて機微なプライバシー情報であるため、上記ガイダンスを参照し、十分な安全管理対策を実施することが必要である。

診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、紙やフィルム等の媒体のままで外部に保存する場合、委託する医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶため、より一層の個人情報保護への配慮が必要である。

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、以下についての対応が求められる。

(1) 診療録等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

C. 最低限のガイドライン

1. 診療録等が搬送される際の個人情報保護

診療録等の搬送は遺失や他の搬送物との混同について、注意する必要がある。

(1) 診療録等の封印と遺失防止

診療録等は、目視による情報の漏出を防ぐため、運搬用車両を施錠する等、搬送用ケースを封印すること。また、診療録等の授受の記録を取る等の処置を取ることによって、その危険性を軽減すること。

(2) 診療録等の搬送物との混同の防止

他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、混同の危険性を軽減すること。

(3) 搬送業者との守秘義務に関する契約

診療録等を搬送する業者は、個人情報保護法上の守秘義務を負うことからも、委託する医療機関等と受託する事業者、搬送業者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上、明記すること。

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

診療録等の外部保存を受託する事業者においては、委託する医療機関等からの求めに応じて、診療録等の検索を行い、必要な情報を返送するサービスを実施する場合、また、診療録等の授受の記録を取る場合等に、診療録等の内容を確認したり、患者の個人情報を閲覧する可能性が生じる。

(1)　外部保存を受託する事業者内で、患者の個人情報を閲覧する可能性のある場合

診療録等の外部保存を受託し、検索サービス等を行う機関は、サービスの実施に最小限必要な情報の閲覧にとどめ、その他の情報は、閲覧してはならない。また、情報を閲覧する者は特定の担当者に限ることとし、その他の者が閲覧してはならない。

さらに、外部保存を受託する事業者は、個人情報保護法による安全管理義務の面から、委託する医療機関等と搬送業者との間で、守秘義務に関する事項や、支障があった場合の責任体制等について、契約を結ぶ必要がある。

(2)　外部保存を受託する事業者内で、患者の個人情報を閲覧する可能性のない場合

診療録等の外部保存を受託する事業者は、専ら搬送ケースや保管ケースの管理のみを実施すべきであり、診療録等の内容を確認したり、患者の個人情報を閲覧してはならない。また、これらの事項について、委託する医療機関等と搬送業者との間で契約を結ぶ必要がある。

(3)　外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関しては、最終的に診療録等の保存義務のある医療機関等が責任を負わなければならない。したがって、委託する医療機関等は、受託する事業者における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

1.　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る。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。

付則 2.3　責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　２（3））

B. 考え方

診療録等を外部の機関に保存する場合であっても、責任に対する考え方は 4.1 章や 4.2 章と同様に整理する必要がある。

これらの考え方に則れば、実際の管理や部分的な説明の一部を委託先の機関や搬送業者との間で分担して問題がないと考えられる。

また、万一事故が起きた場合に、患者に対する責任は、4.1 章における事後責任となり、説明責任は委託する医療機関等が負うものである。ただし、適切に善後策を講ずる責任を果たし、あらかじめ 4.2 章の責任分界点を明確にしておけば、受託する事業者や搬送業者等は、委託する医療機関等に対して契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 通常運用における責任の明確化

(2) 事後責任の明確化

C. 最低限のガイドライン

1.　通常運用における責任の明確化

(1)　説明責任

利用者を含めた管理運用体制について、患者や社会に対して十分に説明する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や委託先の機関にさせることは問題がない。

(2)　管理責任

診療録等の外部保存の運用及び管理等に関する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託する事業者に行わせることは問題がない。

(3)　定期的に見直し必要に応じて改善を行う責任

診療録等を搬送し、外部に保存したままにするのではなく、運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していかなくてはならない。

したがって、医療機関等の管理者は、現行の運用管理全般の再評価・再検討を常にこころがけておく必要がある。

2.　事後責任の明確化

診療録等の外部保存に関して、委託する医療機関等、受託する事業者及び搬送業者の間で、「4.2　委託と第三者提供における責任分界」を参照しつつ、管理・責任体制を明確に規定して、次に掲げる事項を契約等で交わすこと。

(1)　委託する医療機関等で発生した診療録等を、外部に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
(2)　委託する医療機関等と搬送（業）者で診療録等を授受する場合の方法と管理方法
(3)　事故等で診療録等の搬送に支障が生じた場合の対処方法
(4)　搬送中に情報漏えいがあった場合の対処方法
(5)　受託する事業者と搬送（業）者で診療録等を授受する場合の方法と管理方法。
(6)　受託する事業者で個人情報を用いた検索サービスを行う場合、作業記録と監査方法
(7)　取扱い従業者等の退職後も含めた秘密保持に関する規定、情報漏えいに関して患者から照会があった場合の責任関係
(8)　受託する事業者が、委託する医療機関等の求めに応じて診療録等を返送することができなくなった場合の対処方法
(9)　外部保存を受託する事業者に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

付則 2.4　外部保存契約終了時の処理について

診療録等が高度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、委託する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らない。

外部保存の開始には何らかの期限が示されているはずであり、外部保存の終了もこの前提に基づいて行わ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り得るし、一連の診療の終了後○○年といった一定の条件が示されていることもあり得る。

いずれにしても、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、処理が厳正に執り行われたかを監査しなくてはならない。また、受託する事業者も、委託する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、処理を行った旨を委託する医療機関等に明確に示す必要がある。

当然のことであるが、これらの廃棄に関わる規定は、外部保存を開始する前に委託する医療機関等と受託する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、実際の廃棄に備えて、事前にソフトウェアの廃棄等の手順を明確化したものを作成しておくべきである。

委託する医療機関等及び受託する事業者双方に厳正な取扱いを求めるのは、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、そのことに十分なことに留意しなければならない。

また、患者の個人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、及び検索記録も機密保持できる状態で廃棄しなければならない。

さらに、委託する医療機関等及び受託する事業者が負う責任は、先に述べたとおりであり、紙媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことに十分留意する必要がある。

医療情報システムの安全管理に関するガイドライン

第 5.2 版

別冊編

令和４年３月

厚生労働省

【目次】

1. はじめに

医療情報システムの安全管理に関するガイドラインの経緯

平成 11 年 4 月の通知「診療録等の電子媒体による保存について」（平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知）、平成 14 年 3 月通知「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 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 17 年 3 月 31 日改正、医政発第 0331010 号、保発第 0331006 号）により、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された。その後、情報技術の進歩は目覚しく、社会的にも e-Japan 戦略・計画を始めとする情報化の要請はさらに高まりつつある。平成 16 年 11 月に成立した「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」（平成 16 年法律第 149 号。以下「e-文書法」という。）によって原則として法令等で作成又は保存が義務付けられている書面は電子的に取り扱うことが可能となった。医療情報においても「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。以下「e-文書法省令」という。）が発出された。

平成 15 年 6 月より厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」においては、医療情報の電子化についてその技術的側面及び運用管理上の課題解決や推進のための制度基盤について検討を行い、平成 16 年 9 月最終報告が取りまとめられた。

上記のような情勢に対応するために、これまでの「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ガイドライン」（平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付。）、「診療録等の外部保存に関するガイドライン」（平成 14 年 5 月 31 日付け医政発第 0531005 号厚生労働省医政局長通知）を見直し、さらに、個人情報保護に資する医療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的に作成することとした。平成 16 年 12 月には「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ドライン」が公表され、平成 17 年 4 月の「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。）の全面実施に際しての指針が示された。これらの事情を踏まえ、本ガイドライン初版が平成 17 年 3 月に公開された。

また、平成 29 年 5 月に、平成 27 年度改正個人情報保護法が全面施行されることとなり、これに伴って個人情報保護委員会が「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 28 年個人情報保護委員会告示第 6 号。以下「通則ガイドライン」という。）を公表した。この通則ガイドラインを踏まえ、医療・介護分野における個人情報の取扱いに係る具体的な留意点や事例等が「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（個人情報保護委員会、厚生労働省；平成 29 年 4 月 14 日）にお

いて示された。同ガイダンスでは、医療情報システムの導入及びそれに伴う外部保存を行う場合の取扱いにおいては本ガイドラインによることとされている。(本ガイドラインの 6 章、8 章、付則 1、及び付則 2 が該当)

医療情報システムの安全管理に関するガイドライン　第 2 版から第 5.1 版までの改定概要

【第 2 版】

本ガイドライン初版公開（平成 17 年 3 月）後の平成 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」が発表された。IT 新改革戦略では、「e-Japan 戦略」に比べて医療情報の活用が重視されている。様々な医療情報による連携がメリットをもたらすものと謳い、連携の手法、またその要素技術について種々の提言がなされており、その一つに「安全なネットワーク基盤の確立」が掲げられている。

他方、平成 17 年 9 月に情報セキュリティ政策会議により決定された「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」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められた。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では、「(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」の検討を行い、本ガイドラインの改定を実施した。

「(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」では、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適した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」として取りまとめている。さらには、関連箇所として「8　診療録及び診療諸記録を外部に保存する際の基準」の中のネットワーク関連の要件について 6.10 章を参照すること、医療機関等における当該ネットワークの運用の指針となる「10　運用管理について」の一部改定を実施している。

また、「(2) 自然災害・サイバー攻撃による IT 障害対策等」では、医療の IT への依存度等も適切に評価しながら、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」を新設して取りまとめ、情報セキュリティを実践的に運用していくための考え方として「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」の概念を取り入れ、「10　運用管理について」も該当箇所の一部追記を行った。

なお、本ガイドライン公開後に発出、改正等がなされた省令・通知等についても制度上の要求事項として置き換えを実施している。基本的要件について変更はないが、制度上要求される法令等が変更されている点に注意すること。

【第 3 版】

本ガイドライン第 2 版の公開により、ネットワーク基盤における安全性確保のための指標は示されたが、その後、さらに医療に関連する個人情報を取り扱う種々の施策等の議論が進行している。このような状況下においては、従来のように医療従事者のみが限定的に情報に触れるとは限らない事態も想定される。例えば、ネットワークを通じて医療情報を交換する際に、一時的に情報を蓄積するような情報処理事業者等が想定される。このような事業者が関係する際には明確な情報の取扱いルールが必要となる。

また、業務体系の多様化により、医療機関等の施設内だけでなく、ネットワークを通じて医療機関等の外部で業務を行うシーンも現実的なものとなってきている。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では「(1) 医療情報の取扱に関する事項」、「(2) 処方箋の電子化に関する事項」、「(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」の検討を行い、(1) 及び (3) の検討結果をガイドライン第 3 版として盛り込んだ。

「(1) 医療情報の取扱に関する事項」では、従来、免許資格等に則り守秘義務を科せられていた医療従事者が取り扱っていた医療・健康情報が、情報技術の進展により必ずしもそれら資格保有者が取り扱うとは限らない状況が生まれてきていることに対し、取扱いのルールを策定するための検討を実施した。

もちろん、医療・健康情報を本人や取扱いが許されている医師等以外の者が分析等を実施することは許されるものではないが、情報化によって様々な関係者が関わる以上、各関係者の責任を明確にして、その責任の分岐点となる責任分界点を明確にする必要がある。

今般の検討では、その責任のあり方についての検討結果を「4　電子的な医療情報を扱う際の責任のあり方」に取りまとめた。また、この考え方の整理に基づき「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」を改定している。

一方、昨今の業務体系の多様化にも対応ができるように「(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」も併せて検討を実施している。

無線 LAN は電波を用いてネットワークに接続し場所の縛られることなく利用できる半面、利用の仕方によっては盗聴や不正アクセス、電波干渉による通信障害等の脅威が存在する。また、モバイルネットワークは施設外から自施設の医療情報システムに接続ができ、施設外で業務を遂行できる等、利便性が高まる。しかし、モバイルアクセスで利用できるネットワークは様々存在するため、それらの接続形態ごとの脅威を分析した。

これらの検討を踏まえた対応指針を 6 章の関連する箇所に追記し、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」に取りまとめを行った。

さらに、モバイル端末や可搬媒体に情報を格納して外部に持ち出すと、盗難や紛失といった新たなリスクも想定されるため「6.9　情報及び情報機器の持ち出しについて」を新設し、その留意点を述べている。

【第 4 版】

本ガイドライン第 3 版においては、医療情報を取り扱う様々な職種や事業者に対する明確な情報の取扱いルールを規定し、特に責任分界点を明確化にした。このことにより情報化の更なる進展は期待できるが、一方で医療機関や医療従事者等にとって、医療情報の安全管理には、情報技術に関する専門的知識が必要であり、さらに多大な設備投資等の経済的な負担も伴うこと、昨今の厳しい医療提供体制を鑑みれば、限りある人的・経済的医療資源は、医療機関及び医療従事者の本来業務である良質な医療の提供のために費やされるべきであり、情報化に対して過大な労力や資源が費やされるべきではないこと、他方、近年の医療の情報化の進展に伴い、個人自らが医療情報を閲覧・収集・提示することによって、自らの健康増進へ役立てることが期待されていること等の指摘がなされ、医療情報ネットワーク基盤検討会では、より適切な医療等分野の情報基盤構築のために、「(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」、「(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」について検討を行った。

このうち、(1) の「各所より医療情報に関するガイドラインの整合を図ることが求められていること、また、技術進歩に合わせた医療情報の取扱い方策について、物理的所在のみならず医療情報を基軸とした安全管理及び運用方策等をさらに体系的に検討し、読みやすさにも配慮した医療情報ガイドラインの改定を行う」事項についての検討結果をガイドライン第 4 版に盛り込んだ。概略は次のとおりである。

体系的な見直しの一環として、3 章において従前の記載では明確ではなかった「①施行通知には含まれていないものの e-文書法の対象範囲で、かつ、患者の個人情報が含まれている文書等（麻薬帳簿等)」、「②法定保存年限を経過した文書等」、「③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」「④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)」等について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」を新設している。

また、医療情報の相互運用性や標準化の重要性に鑑み、体系的な見直し及び最新の技術等への対応として従来の 5 章を全面的に見直し「5　情報の相互運用性と標準化について」として全面的な改定を加えた。

6 章では、「6.1　方針の制定と公表」において JIS Q 15001:2006 の引用によって公表すべき基本方針の項目を明示し、JIS Q 27001:2006 の引用によって安全管理方針を具体的に説明した上で「C　最低限のガイドライン」を新設した。同様に、「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」においても「C　最低限のガイドライン」及び「D　推奨されるガイドライン」を新設している。「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」においては、B 項及び 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している。

7 章では、電子保存に前文を追加し、要件と対策の原則を述べ、7 章全体の A 項において厚生労働省令と通知の関係を明確にした。「7.1　真正性の確保について」では、B 項の記載

を大幅に簡略化､C項の見直しを実施しD項を全て削除した｡｢7.2　見読性の確保について」でもB項を簡略し、C項の保存場所の区分による記載を取りやめ、整理の上、D項に緊急に必要となることが予想される場合を追加している｡｢7.3　保存性の確保について」も同様にC項、D項で大幅な見直しを実施している。このように7章については、C項、D項において、見直し、修正が数多くなされているため注意願いたい。

また、各所より医療情報に関するガイドラインの整合を図ることが求められていることに対しては、医療情報の外部保存に関して民間事業者が実施する場合において、危機管理上の目的でという要件に変更はないが、情報受託者の事業者に対して8章の「診療録及び診療諸記録を外部の保存する際の基準」の中に、経済産業省及び総務省から発出されているガイドラインに準拠することを条件にして、運用と情報管理のあり方を明確化している。

その他、9章のスキャナの要件を変更する等、全体的に技術進歩に合わせた改定、読みやすさに配慮した記述にする等して第4版としている。

【第4.1版】

本ガイドライン第4版の公開後、平成21年7月に総務省が「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」を策定した。加えて、平成20年7月に経済産業省が告示した「医療情報を受託管理する情報処理事業者向けガイドライン」（平成20年7月24日経済産業省告示第167号）の整備等により、外部保存に対する対応方法が明確になったとの指摘がなされ、医療情報ネットワーク基盤検討会で外部保存先の基準に関する検討を行った。

検討の結果、各ガイドラインの要求事項の遵守を前提として｢「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする「診療録等の保存を行う場所に関する提言」を取りまとめた。

これを受けて、外部保存通知の改正を行い、本ガイドラインにおいても関連する4章、8章、10章の一部を中心に改定を実施した。

4章では「4.3　例示による責任分界点の考え方の整理」に「(4) オンライン外部保存を委託する場合」を追加し、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の資料や説明の提供を委託契約で定め、医療機関等としても理解する努力が必要であること、監督が必須であること、定期的に安全管理に関する状況の報告を受ける必要があることを記載した。

8章では､｢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」の「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」を「③医療機関等が民間事業者等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」とし、内容を通知に合わせて改定した。

10章は、これらの改定に合わせて所要の改定を行った。

今般の改定は、軽微なものであるため、第5版とはせず第4.1版とした。

【第 4.2 版】

本ガイドライン第 4.1 版の公開後、平成 25 年 3 月に「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）の一部改正がなされ、調剤済み処方箋及び調剤録等の外部保存が認められたことから、これを踏まえ、本ガイドラインにおいても、関連する 3 章、8 章、9 章の一部を改正した。

また、モバイル端末の普及に鑑み、機器の取扱いについて明確化するとともに、災害等の非常時の対応について大規模災害時を想定した考え方について追記するため 6 章の一部を改定し、さらに、医療情報の相互運用性と標準化について、最新の技術等への対応として、5 章の一部を改定した。

3 章では、調剤録（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。）を外部保存する場合においても、従前と同様に薬局開設者の責任において行うことや、他薬局の調剤録と明確に区分し、薬局ごと、個別に管理する必要がある旨を記載した。

また、「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」の事項を追加し、現在、処方箋の電子的な発行は認められていないことから、調剤済み処方箋の電子化については、必然的に、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、9 章に示すスキャナ等により電子化して保存する方法となることを明確化した。

さらに、電子保存の対象が「調剤済み処方箋」のみであることから、紙の処方箋を薬局で受け取った後においても、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ことを明確化した。

なお、調剤終了後に修正が発生した場合、既に電子化された調剤済み処方箋に対して、過去の電子署名の検証が可能な状態で、電子的に修正し、薬剤師の電子署名を付すことが必要となることを明確化した。

5 章では、最新の技術等へ対応するため「5.1.1　厚生労働省標準規格」の事項を追加し、厚生労働省標準規格について追記するほか、所要の改定を行った。

6 章では「6.9　情報及び情報機器の持ち出しについて」の事項に、スマートフォンやタブレットのようなモバイル端末の普及を鑑み、機器を取り扱う際の要件を明確化する記述を追加するとともに「6.10　災害等の非常時の対応」の事項に、大規模災害時を想定した事業継続計画（BCP：Business Continuity Plan）の作成等の考え方について記述した。

8 章では、現在、処方箋の電子的な発行は認められていないことから、調剤済み処方箋を紙媒体のままで外部保存する場合のほか、9 章に示すスキャナ等により電子化して保存する場合は、電子媒体による外部保存が可能となる旨を記述した。

9 章では、「9.4　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」の事項を追加し、3 章の改定に合わせて所要の記述を追記した。

今般の改定は、軽微なものであるため、第 5 版とはせず第 4.2 版とした。

【第 4.3 版】

平成 28 年 3 月「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）の一部を改正し、処方箋の電磁的記録による保存、作成及び交付を可能とするとともに、電子処方箋の運用や地域医療連携の取組みを進め、できるだけ早く国民がそのメリットを享受できるように「電子処方せんの運用ガイドライン」を策定した。

これを踏まえ、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」を参照するものとし、本ガイドラインで処方箋に関連する記述がある 3 章、8 章、9 章の一部を改正した。

3 章では、これまで処方箋の電子的発行は認められていない旨、記述していたが、省令の改正に合わせて該当部分を削除した。これに伴い、調剤済み処方箋の取扱いを定めた 3.3 章を「紙」の調剤済み処方箋の扱いとして明確にした。また、電子化された調剤済み処方箋の外部保存は 8 章で、紙媒体をスキャンして保存する場合は 9.4 章での取扱いとなるため、一部記載を改定の上、その旨を追記している。

今般の改定は、処方箋の電磁的記録による保存、作成及び交付等が可能となったことに伴う限定的な改定であるため、第 5 版とはせず第 4.3 版とした。

【第 5 版】

本ガイドライン第 4 版の公表以降、医療等分野及び医療情報システムを取り巻く環境は大きく変化している。個人や組織に関する情報や金銭等の窃取を目的としたサイバー攻撃が多様化・巧妙化し、医療機関等がその標的となる事例も現れるようになった。また、地域医療連携や医療介護連携等の推進を背景に、これまで医療情報に触れる機会の少なかった組織や団体が電子的な医療情報を日常的に取り扱うようになっている。「IoT（モノのインターネット）」と称される新技術やサービス等の普及も著しく、今後の技術の進展が期待されるものの、医療等分野は新たなセキュリティリスクに直面している。

こうした動向を踏まえ、このたび本ガイドラインにおいても、関連する 1 章や 6 章を改定するとともに、第 4.2 版の公表以降に追加された標準規格等への対応を行った。

また、平成 27 年度改正個人情報保護法及びその関連法令等が平成 29 年 5 月に全面施行されることを踏まえ、本ガイドラインにおける参照記述を修正する等、上記法令等や「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」への対応を行った。

1 章では、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した。また、平成 27 年度改正個人情報保護法及びその関連法令等並びに「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」踏まえた改定を行う。

3 章では、1 章の改定を踏まえ、介護事業者が取り扱う文書が e-文書法の対象範囲でかつ当該文書の内容に医療情報が含まれる場合には、7 章及び 9 章の対象となる旨を追記し、該当し得る文書等を列挙した。

4 章では、平成 27 年度改正個人情報保護法で新たに規定された事項について、関係資料を参照する。また、「4.2.2　第三者提供における責任分界」において、平成 27 年度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する。

5 章では、新たに加わった厚生労働省標準規格や JAHIS 標準規約等を追記した。「5.3　標準規格の適用に関わるその他の事項」では、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」について記述を設けた。

6 章では、規格の更新を受け、「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を行った。併せて、6.2 章ではリスク分析等の参考として「『製造業者による医療情報セキュリティ開示書』ガイド」に関する記述を加えた。また、「6.5　技術的安全対策」では、攻撃手法の高度化により、ID・パスワードのみの組み合わせによる認証では十分な安全性を確保できない現状に鑑みて、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したほか、上述の IoT について「(6) 医療等分野における IoT 機器の利用」を設け、情報セキュリティの観点から医療機関等が遵守すべき事項を規定した。

「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」では、医療機関等を対象とするサイバー攻撃のリスクが顕在化していることへの対応として、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設けた。このことに併せて、6.10 章の章題も改定している。

在宅医療や訪問看護等、医療機関等の職員が業務にモバイル端末を用いる機会が増加していることを踏まえ、「6.9　情報及び情報機器の持ち出しについて」において、公衆無線 LAN、個人所有又は個人の管理下にある端末の業務利用（BYOD）の取扱い等、モバイル端末の使用時における遵守事項を明確化した。

「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」では、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示した。

「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」では、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を行った。

7 章では、「7.1　真正性の確保について」において、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した。また、「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 章は、これらの改定に合わせて所要の改定を行った。

このほか、分かりやすさの観点から、全般的な表現の修正を行った。

【第 5.1 版】

本ガイドライン第 5 版の公表以降、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が一層、多様化・巧妙化が進み、さらなるセキュリティ上の対応が求められるようになった。このような状況を踏まえ、医療機関等を対象とするサイバー攻撃の多様化・巧妙化、スマートフォンや各種クラウドサービス等の医療現場での普及、各種ネットワークサービスの動向への対応として、関連する 4 章、6 章等の改定を行った。

また、各種ガイドラインとの整合性の確保や近時の個人情報に関する状況等への対応として、6 章、8 章の改定を行った。

4 章では、クラウドサービスの概要を示すとともに、これを利用した場合の責任分界の考え方や、複数の事業者を利用する場合の責任分界の考え方を示すため、「4.3　例示による責任分界点の考え方の整理」に追記等を行った。

6 章では、リスク分析を行う際に、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を考慮するために、「6.2.3 リスク分析」に追記等を行った。

また、近時のサイバー攻撃などへの対応に求められる措置として、ネットワークの監視等の管理に関する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について、「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」に追記を行った。

医療情報システムにおける利用者認証について、第 5 版において示した二要素認証導入を促す方針をさらに進めるため、「6.5　技術的安全対策」の B 項及び C 項の改定を行った。

また、暗号鍵の管理に関する内容も新規に規定し、「6.5　技術的安全対策」に追記を行った。

サイバー攻撃を含む非常時の体制整備の観点から、非常時の体制構築に関する内容や、平常時における教育・訓練、サイバー攻撃等が生じた場合の通報等を示すため、「6.10　災害、サイバー攻撃等の非常時の対応」に追記等を行った。

8 章では、外部保存における受託事業者に関して、行政機関等が設置するデータセンターと、民間事業者が設置するデータセンターに関する選定のあり方について、考え方及び要求事項を統合するために、「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」の改定を行った。併せて、受託事業者の選定に関して、Cookie 等の取扱いに関する事項や、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などに関する内容を示すため、「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」に追記を行った。

その他、関連法規の改正に伴う部分の修正を行うとともに、分かりやすさの観点から、全般的な表現の修正を行った。

2. 本ガイドラインの読み方

本ガイドラインは本編において、医療機関等において実施すべき内容を示し、別冊でその考え方や、具体的な対応例などを示す形としている。医療機関等において、医療情報システムの安全対策上、求められる内容は本編において確認し、具体的な対策を検討するに際しての参考として、本編で述べた内容の考え方や具体例などを別冊において確認すること。

3. 本ガイドラインの対象システム及び対象情報

3.1. 7章及び9章の対象となる文書についての解説

「施行通知」で定められた文書等を下記に示す。

なお、次に掲げる文書等のうち、「※」を付した処方箋については、施行通知第二　2 (4) の要件を充足する必要がある。

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 2 第 1 項及び第 2 項の規定による事業報告書等及び監事の監査報告書の備置き
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 17 条及び歯科医師法第 17 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（昭和 23 年法律第 205 号）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（昭和 35 年法律第 146 号）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（昭和 32 年厚生省令第 16 号）第 6 条の処方せん※

16. 医療法（昭和 23 年法律第 205 号）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（昭和 23 年法律第 201 号）第 22 条の処方せん※
20. 歯科医師法（昭和 23 年法律第 202 号）第 21 条の処方せん※
21. 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 23 条第 1 項の処方せん※
22. 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

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かつ当該文書の内容に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（平成 11 年厚生省令第 37 号）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（平成 11 年厚生省令第 37 号）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（平成 18 年厚生労働省令第 35 号）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（平成 18 年厚生労働省令第 35 号）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（平成 18 年厚生労働省令第 34 号）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（平成 18 年厚生労働省令第 34 号）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（平成 18 年厚生労働省令第 34 号）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（平成 18 年厚生労働省令第 34 号）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、別途作成・保存が必要となる。

3.2. 8章の対象となる文書等についての解説

「外部保存改正通知」で定められた下記の文書等を取り扱う場合を対象としている。

1. 医師法（昭和 23 年法律第 201 号）第 24 条に規定されている診療録
2. 歯科医師法（昭和 23 年法律第 202 号）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（昭和 23 年法律 203 号）第 42 条に規定されている助産録
4. 医療法（昭和 23 年法律第 205 号）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（昭和 23 年法律第 205 号）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（昭和 26 年法律第 226 号）第 28 条に規定されている照射録
7. 歯科技工士法(昭和 30 年法律第 168 号)第 19 条に規定されている指示書
8. 薬剤師法（昭和 35 年法律第 146 号）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（平成 3 年法律第 36 号）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（昭和 23 年厚生省令第 50 号）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（昭和 32 年厚生省令第 15 号）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（昭和 32 年厚生省令第 16 号）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（昭和 33 年厚生省令第 24 号）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（平成元年厚生省令第 46 号）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

なお、調剤録の保存については、薬局開設者の責任とされており、外部保存を行う場合についても従前と同様に薬局開設者の責任で行う必要がある。また、調剤録は当該薬局に備えることとされているため、当該薬局の調剤録を外部保存する場合には、他の薬局の調剤録と明確に区分し、薬局ごとに個別に管理する必要がある。

3.3. 紙の調剤済み処方箋と調剤録の電子化・外部保存について

別冊における解説はない。

3.4. 取扱いに注意を要する文書等

別冊における解説はない。

4. 電子的な医療情報を扱う際の責任のあり方

電子的な医療情報を扱う際の責任における全般に関する解説

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ある。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る。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、適切な措置を講じられたい。

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る。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る。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る。

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る。

- 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る。

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、情報処理事業者、電気通信事業者等にもまたがるようになる。

4.1. 医療機関等の管理者の情報保護責任について

別冊における解説はない。

4.2. 委託と第三者提供における責任分界

4.2.1. 委託における責任分界に関する解説

以下に、医療機関等の管理者が責任を果たすために必要な、受託する事業者との契約の原則を掲げる。

(1) 通常運用における責任について

① 説明責任

患者等に対し、どのような医療情報保護の仕組みが構築され、どのように機能しているかということを説明する責任は、いうまでもなく医療機関等の管理者にある。

ただし、医療機関等の管理者が説明責任を果たすためには、受託する事業者による情報提供が不可欠の場合があるため、受託する事業者には、医療機関等の管理者に対する説明責任を果たさせる必要がある。

したがって、受託する事業者との契約において、適切な情報提供義務・説明義務を含め、医療機関等の管理者に対する説明の履行を確保しておく必要がある。

② 管理責任

管理責任も、やはり医療機関等の管理者にある。しかし、現実に医療情報システムの保守作業等を行うのは、受託する事業者である場面が多いと考えられる。医療機関等の管理者としては、受託する事業者の管理の実態を把握し、その監督を適切に行う仕組みを作る必要があり、そのために必要な事項を契約に含めるべきである。

③ 定期的に見直し必要に応じて改善を行う責任

医療情報システムの運用管理の状況の定期的な監査や、問題点の洗い出し、改善すべき点の改善の分担情報保護に関する技術進展に配慮した定期的な再評価・再検討の結果に基づき対策を行う際の医療機関等との協議に関する事項について、契約に含めるべきである。

(2) 事後責任について

① 説明責任

前節で述べたように、医療情報について何らかの不都合な事態が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明することが求められる。

しかし、情報に関する事故は、説明に際して受託する事業者による情報提供や分析が

不可欠な場合が多いと考えられる。そのため、あらかじめ可能な限りの事態を予想し、説明責任の分担に関する事項について、契約に含めるべきである。

② 善後策を講ずる責任

医療情報について何らかの不都合な事態が生じた場合、医療機関等の管理者に「善後策を講ずる責任」が発生することについて前節で述べた。しかし、医療情報の取扱いを受託する事業者の責任によってそのような事態が生じた場合、適切な委託契約に基づき、受託する事業者の選任・監督に適切な注意を払っていれば、法律上、医療機関等の管理者の善管注意義務は果たされていると解される。

しかしながら、本章の冒頭に述べたように、情報の管理は、医療機関等の管理者の責任において行うことが求められている。そのため、医療情報について何らかの不都合な事態が生じた場合の原因究明、被害者への損害填補、再発防止について、患者等との関係においては、医療機関等の管理者が責任を負わなければならない。また、現実的にも、受託する事業者が医療情報の全てを管理しているとは限らないため、再発防止のために医療情報保護の仕組み全体について善後策を講ずる責任は、医療機関等の管理者が負わざるを得ない。

上記のように、医療機関等の管理者は、受託する事業者の責任によって何等かの不都合が生じた場合であっても、患者等に対して、「原因を追及し明らかにすること」、「損害を生じさせた場合にはその損害を填補すること」、「再発防止策を講ずること」等の善後策を講ずる責任を免れるものではない。

ただし、患者等に対する責任が免ぜられることはないとしても、受託する事業者との間での責任分担は別の問題である。特に、受託する事業者の責任で不都合な事態が生じた場合、医療機関等の管理者が全ての責任を負うことは、原則としてあり得ない。

しかし、医療情報について何らかの不都合な事態が生じた場合、医療機関等と受託する事業者の間で責任の分担について争うことよりも、まず原因を追及し明らかにし、再発防止策を講ずることを優先させる必要がある。

そのため、受託する事業者との契約において、医療情報について何らかの不都合な事態が生じた場合、原因追及と再発防止策の実施を優先させることを明記しておく必要がある。

委託内容によっては、より具体的に、受託する事業者の負う原因追及責任と再発防止策の提案義務を明記することも考えられる。

損害填補責任の分担については、事故の原因が受託する事業者にある場合、最終的には受託する事業者が負うのが原則である。ただし、この点は、原因の種類や複雑さによっては原因究明が困難な場合があること、及び損害填補責任の分担の定め方によっては原因究明の妨げになるおそれがあることや、保険による損害分散の可能性等、考慮すべき様々な要素がある。それらを考慮した上で、受託する事業者との契約において損害填補

責任の分担を明記することが必要である。

4.2.2. 第三者提供における責任分界に関する解説

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あり、医療機関等の管理者にとっては、原則としてその正当性だけが問題となる。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、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る。

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る。

一方、電子化された情報の特殊性に着目すると、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となる。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ない。

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、情報処理関連事業者が介在することがある。この場合、いつの時点で、第三者提供が成立するのか、すなわち情報処理関連事業者との責任分界というべき概念が発生する。

一旦適切・適法に提供された医療情報の情報保護について、提供元の医療機関等に責任がないことは先に述べたとおりであるが、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る。その上で、前節で示した「善後策を講ずる責任」をいかに分担するかは、情報処理関連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しい。情報処理関連事業者の選任・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、情報処理関連事業者の過失で何らかの不都合な事態が生じた場合は、情報処理関連事業者が全ての責任を負うのが原則である。

4.3. 例示による責任分界点の考え方の整理における具体的な責任分界例の解説

(1) 地域医療連携で「患者情報を交換」する場合

(a) 医療機関等における考え方

① 「情報処理関連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患者情報を交換する場合の責任分界点

ここでいう「情報処理関連事業者の提供するネットワーク」とは、情報処理関連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う。

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、契約等で合意しておく。

その上で、自らの責任範囲において、情報処理関連事業者との管理責任の分担につい

て責任分界点を定め、情報処理関連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おく。

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。情報処理関連事業者に過失がない場合、情報処理関連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る。

② 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点

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う。

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る。

このような場合、情報処理関連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、情報処理関連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る。

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ない。

③ 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点

地域医療連携で患者情報を交換する際、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の利用が可能である。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ある。

(b) 情報処理関連事業者に対する考え方

① 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点

提供元医療機関等の医療情報システムにおいて、送信前に患者情報が暗号化され、提供先医療機関等の医療情報システムにおいて患者情報が復号される場合、情報処理関連事業者の責任は限定的になる。

しかしながら、この場合でも、情報処理関連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情報処理関連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。

なお、暗号化等のネットワークに係る考え方や最低限のガイドラインについては、6.11 章を参照すること。

② 医療情報が情報処理関連事業者の管理範囲で暗号化される場合の責任分界点

情報処理関連事業者の中には、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する。

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する。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く。

ただし、情報処理関連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、(a)①に沿った考え方の整理が必要である。

なお、ネットワーク回線を流れる情報に対する考え方や最低限のガイドラインについては、6.11 章を参照すること。

(c) 外部保存を受託する事業者が介在する場合に対する考え方

この場合、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る。

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る。

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。

なお、医療機関等が外部保存を受託する事業者を通じて患者情報を交換する場合の医療機関等及び外部保存を受託する事業者に対する考え方は本編 8.3 章を参照すること。

(2) 業務の必要に応じて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

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のネットワーク全般の考え方については、6.11 章 B 項、特に「B-2. 選択すべきネットワークのセキュリティの考え方 Ⅲ. モバイル端末等を使って医療機関等の外部から接続する場合」を参照すること。ここでは特に責任分界点の考え方について述べる。

(a) 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

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た。

テレワークは、責任分界の観点では自施設に閉じているが、情報処理関連事業者が管理する通信回線を利用することになる。また、通信回線として、インターネットだけでなく、携帯電話網、公衆回線等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る。

特に、医療機関等の管理者や医療情報システム安全管理責任者でない医療機関等の従業者についても管理責任が問われる事態も発生することに注意を払う必要がある。

この例の場合、責任分界点としては基本的に自施設に閉じているため、責任のあり方の原則としては、4.1 章を参照すべきことに留意しなくてはならない。

(b) 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保守事業者による遠隔保守（リモートメンテナンス）が考えられる。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、一時保存しているディスク上の個人情報を含む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る。他方、リモートログイン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する。

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る。

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、保守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る。

なお、リモートメンテナンスも含めた保守の考え方については、6.8 章を参照すること。

(3) 医療機関等の業務の一部を委託することに伴い情報が「一時的に外部に保存」される場合

ここでいう委託とは遠隔画像診断、臨床検査等、診療等を目的とした業務の委託であり、これに伴い一時的にせよ情報を受託する事業者が保管することとなる。

医療機関等の管理者は、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る。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あるが、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る。

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ある。

(4) オンライン外部保存を委託する場合

本ガイドラインの 8.3 章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る。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ある。さらに、情報処

理関連事業者と外部保存を受託する事業者は異なることが多いため、障害が起こった際の対処の責任範囲について明確に定めた上で、医療機関等が理解しておく必要がある。

さらに、委託先に対する監督も必須であり、定期的に安全管理に関する状況の報告を受ける必要がある。

クラウドサービスは、受託事業者等によって提供されるサービスで、利用者が医療情報システム及びこれに必要な機器を保有することなく、ネットワーク経由で事業者が提供する医療情報システムにアクセスし、必要な処理や、データ保管等の管理を行うものである。医療情報においても、外部保存を行うほか、必要な情報処理を行うのに用いることができる。

外部保存を受託事業者が 1 社ではなく複数の事業者を通じて行われることもある。この場合には障害や情報漏洩等の事故が生じた場合に、責任分界を明瞭にしておかないと、原因の特定や対策などが遅滞する危険性がある。

図 4-1 の②の場合は、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あるが、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る。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ある。

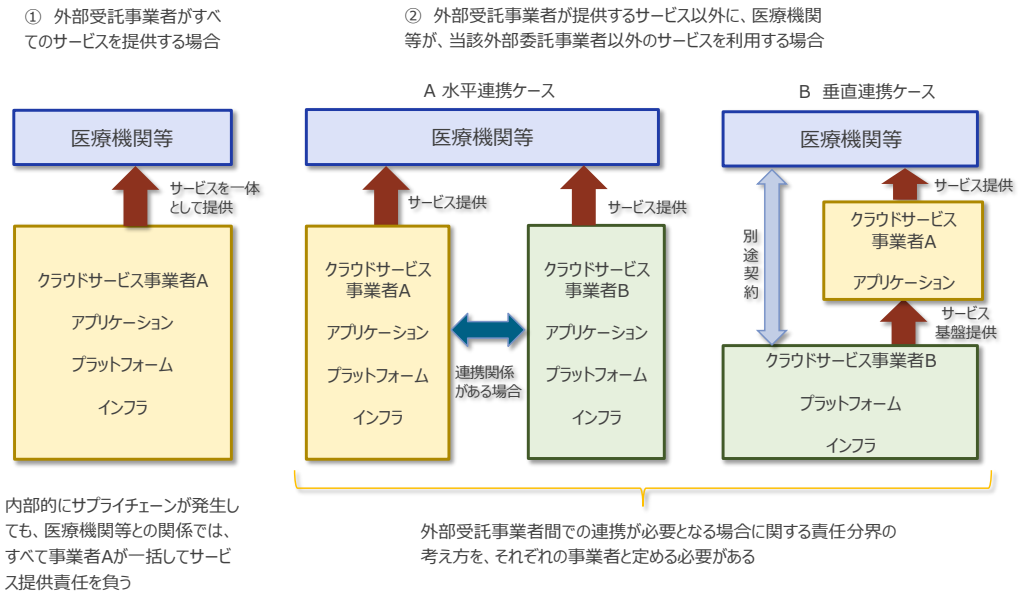


図 4-1　1 者又は複数の事業者が受託する場合の責任分界の考え方

(5) 法令で定められている場合

法令で定められている場合等の特別な事情により、情報処理関連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、情報処理関連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る。

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、情報処理関連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らない。

また、情報処理関連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、監督しなければならない。

4.4. 技術的対策と運用による対策における責任分界点

総合的な判断では、リスク分析に基づき、経済性も加味して、装置仕様、システム要件と運用管理規程について決定する必要がある。この決定は、安全性に対する脅威、その対策に関する技術的変化、医療機関等の組織の変化を含めた社会的環境変化等により異なってくるので、その動向に注意を払う必要がある。

総合的な判断を下し、医療機関等が責任を果たすためには、ベンダに要求する技術要件とベンダが要求する運用条件を明確にして、ベンダとの責任分界点を明確にする必要がある。

運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として、10 章と付表を参考にして、「基準適合チェックリスト」等を作成して整理しておく必要がある。このようなチェックリストは第三者へ説明責任を果たす際の参考資料として利用できる。

5. 情報の相互運用性と標準化について

5.1. 基本データセットや標準的な用語集、コードセットの利用

本編第 5 章で記述したように標準化に向けた取組みは進捗中であるが、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る。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る。

- 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を以下に示す。

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る。

前述のように、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ある。

令和 4 年 1 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る。

- 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－医用波形フォーマット－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

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あるので、必要に応じ、適宜最新版を参照すること。最新版は、下記の URL から参照可能である。

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た。

この基本データセットには以下が含まれる。

- 利用者情報
- 患者情報（基本情報）
- 患者情報（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る。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こと。

・　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る。

なお、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る。

・　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ているので、適宜利用すること。

5.2. データ交換のための国際的な標準規格への準拠

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、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る。

主要なものとしては以下が挙げられる（一部は厚生労働省標準規格にも採択されている）。

・　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

これらの規約は以下の URL で取得できる。

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

5.3. 標準規格の適用に関わるその他の事項

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 を提案している。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ある。詳細は以下の URL から得られる。

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る。

また、注意しなければならない点として外字の問題がある。外字とは個別のシステムにおいて独自に定義した表記文字であるが、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、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要がある。

6. 医療情報システムの基本的な安全管理

6.1. 方針の制定と公表に関する解説

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る。

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。

また、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る。

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。

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

ISMS 構築の手順

ISMS 構築の手順に関する解説

PDCA 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る。

【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（Action）

・ 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が中心になっている。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る。

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し得る。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。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。

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る。

取扱い情報の把握

別冊における解説はない。

リスク分析に関する解説

医療情報システムとして上記の観点で留意すべき点として、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。以下に様々な状況で想定される脅威を列挙する。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）も参考になる。

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

6.3. 組織的安全管理対策（体制、運用管理規程）

別冊における解説はない

6.4. 物理的安全対策

別冊における解説はない

6.5. 技術的安全対策

(1) 利用者の識別・認証に関する解説

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しなければならない。

- 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。

① 利用者の識別・認証における認証強度の考え方に関する解説

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ある。しかし、ID・パスワードによる認証ではその運用によっては、上記に列挙したようなリスクが大きくなる。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る。

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推奨されない。

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ある。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ある。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。

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るが、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る。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ある。

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る。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ない。

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ある。

なお、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、「C. 最低限のガイドライン」における「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る。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る。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」としている。

患者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。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あり、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。

② 利用者の識別・認証における IC カード等のセキュリティ・デバイスを配布する場合の留意点に関する解説

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情報や暗号化鍵、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る。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ある。

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らない。

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べきである。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しい。

③ 利用者の識別・認証におけるバイオメトリクスを利用する場合の留意点に関する解説

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は、その測定精度にも注意を払う必要がある。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る。

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ある。

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る。

- 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る。

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る。

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る。

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

(2)～(5)での別冊における解説はない

(6) ネットワーク上からの不正アクセスに関する解説

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」等の各種方式がある。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ない。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しい。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べきである。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 PC 等の情報端末に対しても同様であるが、その考え方と対策については、6.9 章を参照すること。

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る。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であるため、そのことを念頭に置いた上で対策を行う必要がある。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”の防止は確実に行わなければならない。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る。

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る。

(7) 医療等分野における IoT 機器の利用に関する解説

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る。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る。

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るが、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る。

IoT 機器により患者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る。

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、機器の機能・性能によって、セキュリティが十分に確保されないおそれがある。よって、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、同意を得る必要がある。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る。

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るので、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る。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しい。

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るが、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。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しいが、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る。この場合、上位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される。

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る。

IoT 機器が通信で用いる PAN（Personal Area Network）※と呼ばれる Bluetooth や Zigbee などの 802.15.XX の標準による規格、NFC（Near Field Communication）、赤外線通信などを用いた規格においては、必ずしも十分通信の暗号化対策が取られているわけではないため、技術的な対応に限界があるとされる。IoT 機器のネットワーク接続状況を監視する等の対策も考えられるが、使用を終えた又は停止した機器は電源を切り、接

続を遮断する、不要な接続は行わない等、運用面での対策も可能である。

※ 人体表面や周辺においてデータをやり取りする通信距離の極めて短いワイヤレスネットワークである BAN（Body Area Network）を含めた広義の意味で、PAN という表現が用いられることもある。

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る。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る。

(8) その他

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るので、情報の可用性が阻害されないように留意する必要がある。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ある。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る。

また、電力線搬送通信（PLC：Power Line Communication）を利用する場合、医療機器に対する安全性が確認されておらず、厚生労働省医薬食品局から「広帯域電力線搬送通信機器による医療機器への影響に関する医療関係者等からの照会に対する対応について」（平成 18 年 11 月 9 日付け薬食安発第 1109002 号）の通知が出されているため、可用性の確保と他の医療機器への影響の双方に留意する必要がある。

6.6. 人的安全対策

別冊における解説はない。

6.7. 情報の破棄

別冊における解説はない。

6.8. 医療情報システムの改造と保守に関する解説

医療情報システムの改造と保守において想定される脅威に対する十分な対策が必要になるが、具体的には以下の脅威が存在する。

- 機密性の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
- 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
- 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
- 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等

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の解説

昨今、医療機関等において医療機関等の従業者や保守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る。

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ることも事実である。

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る。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る。

まず重要なことは、6.2章で述べているように、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ある。

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る。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らない。

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が明確になる。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る。

一方、医療機関等の管轄外のパソコン（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、不正ソフトウェアや不適切な設定のされたソフトウェア（Winny 等）、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る。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取扱いについての把握や規制は難しくなるが、情報の取扱いについては医療機関等の情報の管理者の責任において把握しなければならない。

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）が参考になる。

6.10. 災害、サイバー攻撃等の非常時の対応に関する解説

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る。

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

前者としては、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ある。

後者としては、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ある。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る。

(1) 非常時における事業継続計画

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掲げる。

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。

(2) 医療情報システムの非常時使用への対応

別冊における解説はない。

(3) サイバー攻撃を受けた際の対応

ランサムウェアを考慮した対策を検討するに際しては、NISC の「ランサムウエアによるサイバー攻撃に関する注意喚起」（2021 年 4 月 30 日）などが参考になる。

(4) 非常時に備えたセキュリティ体制の整備

別冊における解説はない。

6.11. 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

B. 考え方

外部と診療情報等を交換（双方向だけではなく、一方向の伝送も含む）するケースとしては、地域医療連携で医療機関等や検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS 型のサービスを利用する、医療機関等の従事者がノートパソコンのようなモバイル型の端末を用いて業務上の必要に応じて医療機関等の医療情報システムに接続する、患者等による外部からのアクセスを許可する等が考えられる。

本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して、いくつかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

(1) 医療機関等における留意事項に関する解説

4.2 章で述べた責任のうち、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は、送信元の医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が電気通信事業者の提供するネットワークを通じ、適切に送信先の機関に受け渡されるまでの一連の流れにおいて適用される。

ただし、誤解のないように整理すると、ここでいう管理責任とは電子的に記載されている情報の内容に対して負うべきものであり、その記載内容や記載者の正当性の保持（真正性の確保）を指す。つまり、後述する「(2)選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても、第三者がその情報を判読できないようにしておく処置を指す。また、改ざん検知を行うために電子署名を付与することも対策の一つである。このように情報の内容に対するセキュリティをオブジェクト・セキュリティと呼ぶことがある。一方、「(2)選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。このような回線上の情報に対するセキュリティをチャネル・セキュリティと呼ぶことがある。

このような視点から、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生するため、次のような点に留意する必要がある。

①　「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。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る。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る。

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る。その一つの方法として医療情報の暗号化が考えられる。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）のことを指している。

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はあるが、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しい。

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ある。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。

②　「改ざん」の危険性への対応

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らない。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る。また、後述する「(2)選択すべきネットワークセキュリティの考え方」の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り、改ざんに対する対処は確実に実施しておく必要がある。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る。

③　「なりすまし」の危険性への対応

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くてはならない。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

しなくてはならない。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ある。

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る。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る。

なお、上記の危険性がサイバー攻撃による場合の対応は 6.10 章を参照すること。

④ 暗号化を行うための適切な鍵管理

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な対応である。

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る。例えば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、管理することが求められる。

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る。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)※が定められている。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しい。

※ 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)

⑵選択すべきネットワークのセキュリティの考え方に関する解説

医療情報を内部ネットワークと外部ネットワークを接続して交換する際、ネットワークの接続形態により選択すべきセキュリティの考え方が異なる。

・クローズドなネットワークで接続する場合
・オープンなネットワークで接続する場合

・モバイル端末等を使って医療機関等の外部から接続する場合

の 3 つの場合について、それぞれ接続先の医療機関等のネットワーク構成や経路設計によって、意図しない情報漏えいが起こる可能性について留意し、確認する責務がある。

医療機関等になるか又は双方の分担となるかを契約等で明らかにする必要がある。その際の考え方としては「(1)医療機関等における留意事項」では主に情報内容が脅威に対応するオブジェクト・セキュリティについて解説したが、ここでは通信経路上での脅威への対応であるチャネル・セキュリティについて解説する。

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から情報を受信する機関の外部ネットワーク接続点までや、業務の必要性から従業員に外部からのアクセスを許可した場合、患者等からのアクセスを許可した場合等における外部から医療機関等の医療情報システムにアクセスする接続点までのことを指し、医療機関等の内部で構成される LAN は対象としていない。ただし、4.2 章でも触れたとおり、医療機関等には、接続先の医療機関等のネットワーク構成や経路設計によって、意図しない情報漏えいが起こる可能性について留意し、確認する責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等は交換しようとする情報の機密性の整理をする必要がある。基本的に医療情報をやり取りする場合、確実なセキュリティ対策が必須であるが、例えば、予約システムが扱う再診予約情報のように機密性の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対するリスク分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任の所在が、電気通信事業者又は情報処理事業者となるか、医療機関等になるか又は双方の分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

- **<u>電気通信事業者とクラウドサービス事業者がネットワーク経路上のセキュリティを担保する場合</u>**

  電気通信事業者とクラウドサービス事業者が提供するネットワークサービスのうち、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPN サービスのような通信経路が暗号化されるネットワークとして電気通信事業者が提供するサービスも存在する。

  このようなネットワークの場合、医療機関等は、通信経路上におけるセキュリティに関する管理責任の大部分をこれらの事業者に委託できる。もちろん自機関等においては、善管注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り、自機関

等のシステムの安全管理を確認しなくてはならない。

- **電気通信事業者とクラウドサービス事業者がネットワーク経路上のセキュリティを担保しない場合**

  例えば、インターネットを用いて、医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して電気通信事業者とクラウドサービス事業者は責任を負わない。そのため、上述の安全管理に加え、導入したネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識を持たない者が安易にネットワークを構築して医療情報等を脅威にさらさないように、万全の対策を実施する必要がある。

  そのため、情報の送信元・送信先に導入されるネットワーク接続機器に加え、医療機関等内に設置されている情報端末、当該端末に導入されている機能及び端末の利用者等を確実に確認する手段を確立する必要がある。また、情報をやり取りする機関同士での情報の取扱いに関する契約の締結、(脅威が発生した際に備えて) 電気通信事業者にネットワーク経路上のセキュリティを委託する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等も考慮しなくてはならない。

このように、医療機関等においてネットワークを通じて医療情報を交換しようとする場合には、利用するサービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークサービスの形態は様々存在するため、以降ではいくつかのケースを想定して留意点を述べる。

また、想定するケースの中でも、スマートフォン、タブレット等の可搬型コンピュータ、いわゆるモバイル端末等を使って医療機関等の外部から接続する場合は、利用するモバイル端末とネットワークの接続サービス及びその組み合わせによって複数の接続形態が存在するため、特に「Ⅲ　モバイル端末等を使って医療機関等の外部から接続する場合」を設けて考え方を整理している。

①クローズドなネットワークで接続する場合に関する解説

以下、それぞれの接続方式について特徴を述べる。

1) 専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契

約機関専用のネットワーク接続である（図①）。電気通信事業者によってネットワークの品質と通信速度（以下「帯域」という。）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入に当たってやり取りされる情報の重要性と情報の量等との兼ね合いを見極める必要がある。

図①　専用線で接続されている場合

2)公衆網で接続されている場合

公衆網とはISDN（Integrated Services Digital Network）※やダイアルアップ接続等、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続はインターネットサービスプロバイダ(以下「ISP」という。)に接続する方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続（図②）となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイアルしてネットワーク接続を確立するため、ネットワーク接続を確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続や誤送信のリスクがあること、専用線と同様に拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報又は画像等の容量の大きな情報の送信には不向きであることから、適用範囲を適切に見定める必要がある。

図②　公衆網で接続されている場合

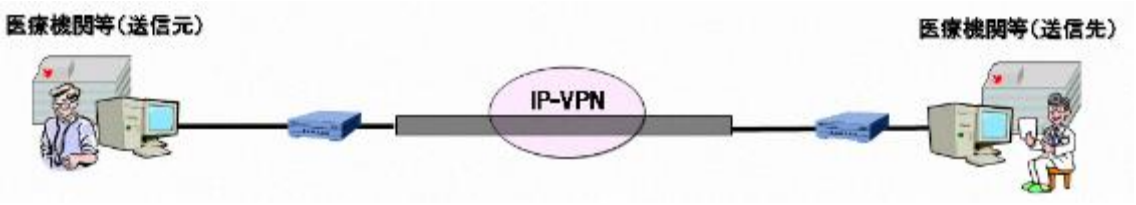
※　なおISDNは2024年1月にサービスの終了がアナウンスされていることから、現在同サービスを利用している場合には、代替策を講じることが求められる。ISDNの代

替策としては、現在のネットワーク機器に INS から IP-VPN に変換するアダプタを装着する方法等や、閉域モバイル網を利用するサービス等による例がある。

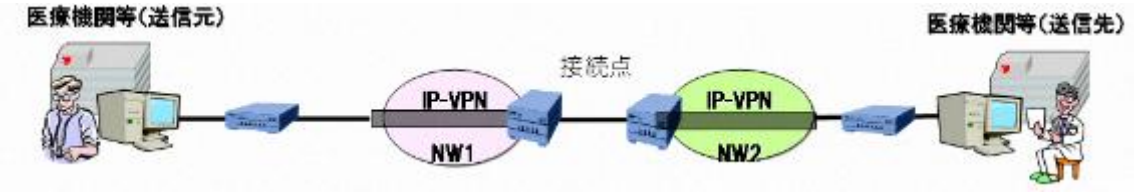
3)閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、電気通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式をいう。このような接続サービスを本ガイドラインでは IP-VPN（Internet Protocol-Virtual Private Network）と呼び、クローズドなネットワークとして取り扱う（図③-a、図③-b）。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。



図③-a　単一の電気通信事業者が提供する閉域ネットワークで接続されている場合



図③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

以上の 3 つのクローズドなネットワークの接続では、クローズドなネットワーク内に外部から侵入される可能性はなく、その意味では安全性は高い。しかし、異なる電気通信事業者のクローズドなネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとはいえない。電気通信事業法（昭和 59 年法律第 86 号）があり、万一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からはこうした事態への対応策をあらかじめ検討しておく必

要がある。その他、医療機関等から閉域 IP 通信網に接続する点等、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

これらの接続サービスでは、一般的に送られる情報そのものに対する暗号化は施されていない。そのため、クローズドなネットワークを選択した場合であっても、「(1)医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにして、改ざんを検知可能な仕組みを導入する等の措置を取る必要がある。

②オープンなネットワークで接続する場合に関する解説

現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療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る。

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 2 月)が参考になる。

※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

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ないが、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する。また、偽サーバへの対策が不十分なものが多い。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 よりは危険度が低い。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る。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して、確実にその安全性を確保する必要がある。

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 (図④) は、少なくとも TLS による暗号化を用いた HTTPS の利用が求められる。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 を用いても安全性を確保することができな

い。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る。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る。なお、「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 に設定するが、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る。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（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る。

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し得る。

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」（※）が参考になる。

※　「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/2009090nRece%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る。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る。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ある。

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る。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る。

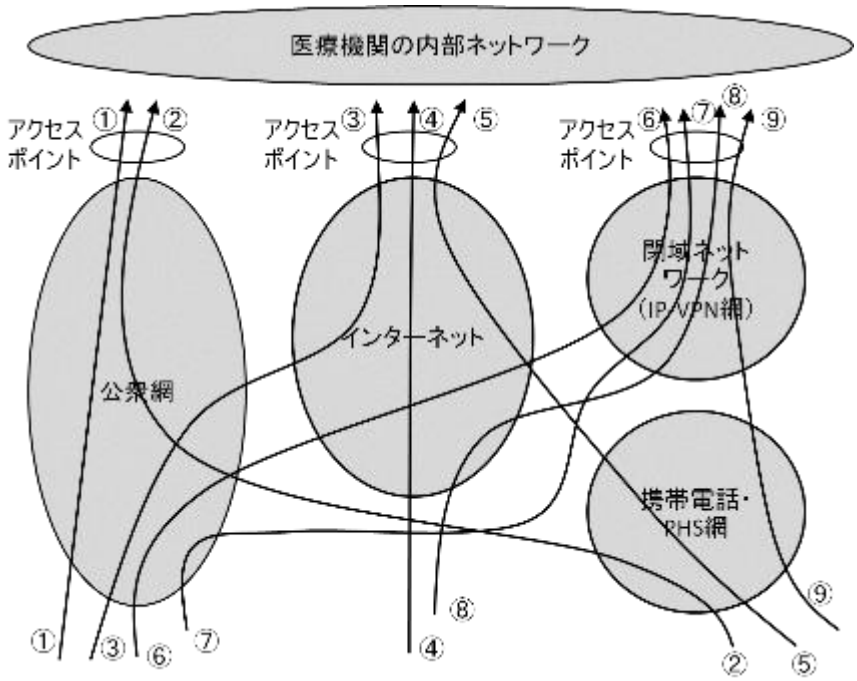
また、外部との接続については、医療機関等がクラウドサービスを利用し、受託事業者等

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る。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る。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る。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しい。

図④　オープンネットワークで接続されている場合

③モバイル端末等を使って医療機関等の外部から接続する場合に関する解説

外部から医療機関等の内部ネットワークに接続する場合、現状で利用可能な接続形態の俯瞰図を図⑤に示す。



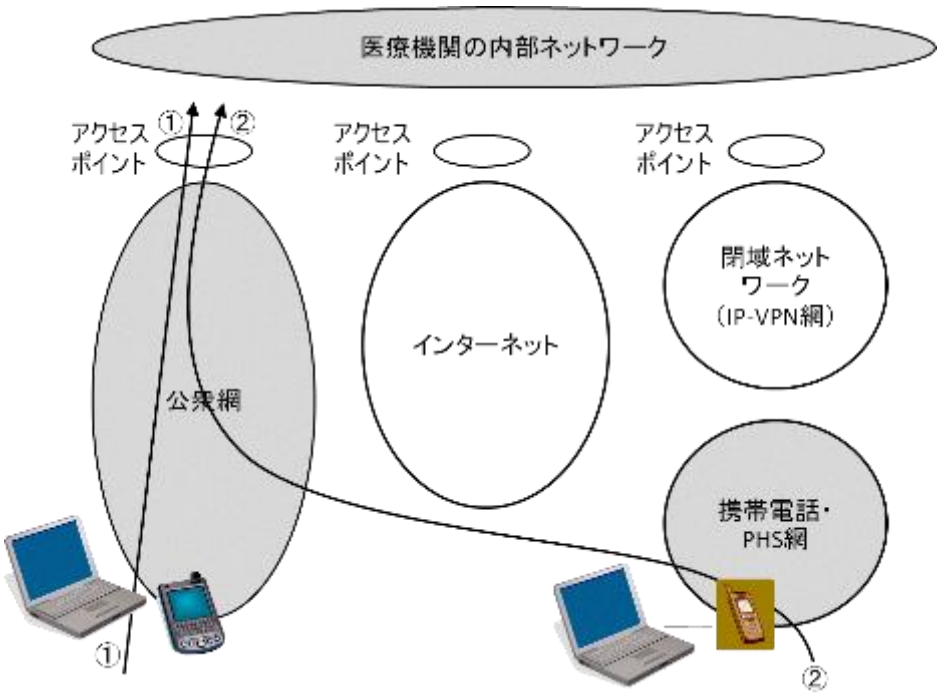
図⑤　モバイル環境における接続形態

図⑤に示したように、接続形態は下記の 3 つの系統に類型化できる。（括弧内の丸数字はそれぞれ図⑤と対応する）

1）公衆網（電話網）を経由して直接ダイアルアップする場合（①、②）
2）インターネットを経由して接続する場合（③、④、⑤）
3）閉域ネットワーク（IP-VPN 網）を経由して接続する場合（⑥、⑦、⑧、⑨）

ここでは、本章の「Ⅰ．クローズドなネットワークで接続する場合」と「Ⅱ．オープンなネットワークで接続する場合」で説明したどのケースに該当するかを示し、それぞれのケースにおけるセキュリティ上の留意点をまとめる。

1）公衆網（電話網）を経由して直接ダイアルアップする場合（図⑥）



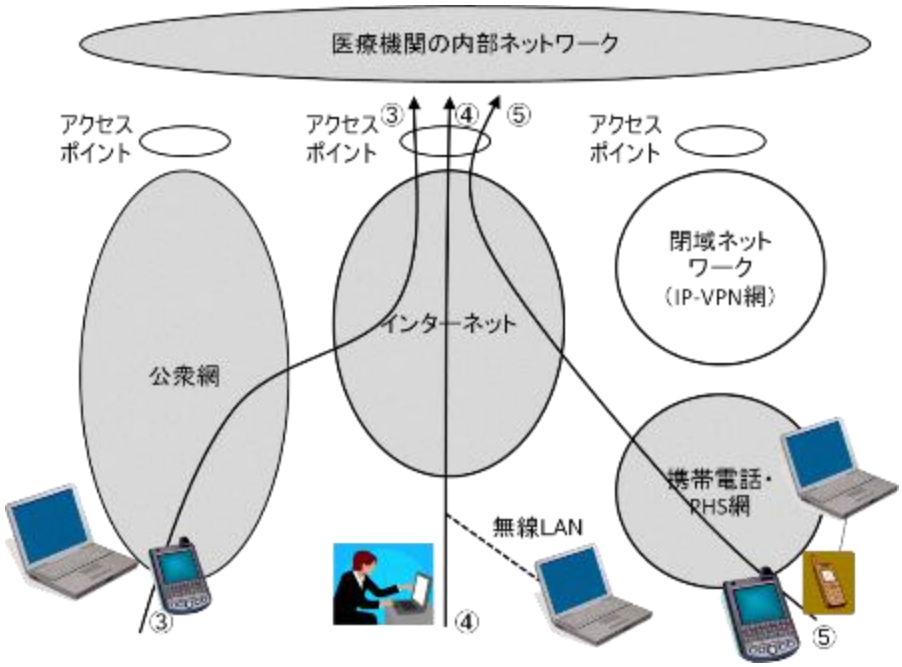
図⑥　モバイル環境における接続形態（公衆網経由）

①は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続し、医療機関等内に設けられたアクセスポイントに直接ダイアルアップするケースである。

②は①における電話回線の代わりに、携帯電話・PHS やその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS 網に接続するケースである。①と②は携帯電話・PHS 網を経由するかどうかの違いがある。

いずれも「Ⅰ．クローズドなネットワークで接続する場合」における「②公衆網で接続されている場合」に相当するため、セキュリティ上の要件は、そこでの記述を適用する必要がある。全てクローズなネットワークを経由するため、比較的安全性は高い。

2）インターネットを経由して接続する場合（図⑦）



図⑦　モバイル環境における接続形態（インターネット経由）

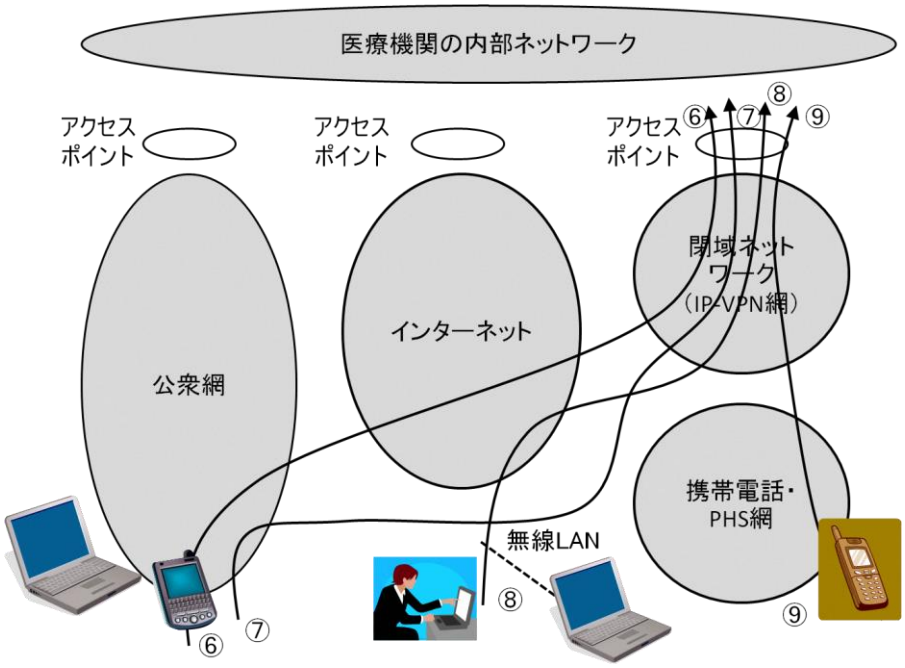
③は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続してインターネットのサービスプロバイダのアクセスポイントにダイアルアップし、インターネット経由で医療機関等のアクセスポイントに接続するケースである。

④は③における電話回線の代わりに、自宅やホテル等インターネットへの接続インタフェースのあるところで LAN を使って接続するケースである。LAN として有線の LAN の代わりに無線 LAN を利用するケースもある。いわゆる公衆無線 LAN を利用した接続もこの形態に含まれる。

⑤は携帯電話・PHS 網を経由して、電気通信事業者の提供するサービスを利用してインターネットへ接続するケースではある。

③から⑤のいずれのケースも「②　オープンなネットワークで接続されている場合」に相当する。したがって、セキュリティ上の要件は、そこでの記述を適用する必要がある。オープンなネットワークを経由するので、「(1)　医療機関等における留意事項」で述べたオブジェクト・セキュリティとチャネル・セキュリティを担保するための対策が必要である。

3）閉域ネットワークを経由して接続する場合（図⑧）に関する解説



図⑧　モバイル環境における接続形態（閉域ネットワーク経由）

⑥と⑦はいずれも自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続して閉域ネットワークのサービスプロバイダのアクセスポイントにダイアルアップし、閉域ネットワーク経由で医療機関等のアクセスポイントに接続するケースである。

⑥は⑦とよく似ているが、⑥がダイアルアップする際に一度オープンなネットワーク（インターネット）を提供するプロバイダを経由するのに対して、⑦では閉域ネットワークを提供するプロバイダに直接ダイアルアップするという違いがある。

⑧は⑥における電話回線の代わりに、自宅やホテル等インターネットへの接続インタフェースのあるところで LAN を使って接続するケースである。このケースのバリエーションとして、LAN として有線の LAN の代わりに無線 LAN を利用するケースもあり、いわゆる公衆無線 LAN 等もこのケースに含まれる。

⑨は携帯電話・PHS 網を経由して、オープンなネットワークを通じて閉域ネットワークへ接続するケースである。この場合の携帯電話・PHS 網から閉域ネットワークへの接続は、電気通信事業者によって提供されるサービスである。

④患者等に診療情報等を提供する場合のネットワークに関する考え方に関する解説

ここでの考え方の原則は、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り、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らない。

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ある。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、患者等にも発生する。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る。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らない。

今まで述べてきたような専用線等のネットワーク接続形態で患者等に診療情報等を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、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になる。この場合、盗聴等の危険性は極めて高い。医療機関等における基本的な留意事項は、既に 4 章や(1)で述べているが、オープンなネットワーク接続であるため、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ある。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る。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必要がある。

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る。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る。

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

法令で定められた記名・押印を電子署名で行うことの経緯に関する解説

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・保存が可能となった。

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、解説されているが、これを解説する者として「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)) がある（同解説は以下の URL から入手できる)。

https://www.dekyo.or.jp/tsf/wp-content/uploads/2021/02/%E9%9B%BB%E5%AD%90%E7%BD%B2%E5%90%8D%E6%B3%95Q%EF%BC%86A%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E8%A7%A3%E8%AA%AC.pdf

電子署名で用いられる暗号に関する解説

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る。

長期署名方式に関する解説

長期署名方式では、下記により、署名検証の継続を可能としている。

- 署名に付与するタイムスタンプにより署名時刻を担保する（署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること）。
- 署名当時の検証情報（関連する証明書や失効情報等）を保管する。
- 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。

7. 電子保存の要求事項について

7.1. 真正性の確保に関する解説

(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る。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る。

※ 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をいう。

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らない。

- 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、6.8 章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。

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る。

- 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ある。具体的な方策については、「C. 最低限のガイドライン」

の記述を参照すること。

(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る。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・訂正等の確定者が自明となる場合も考えられる。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る。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ある。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る。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らない。

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す。

(1) 入力者及び確定者の識別と認証
(2) 記録の確定
(3) 識別情報の記録
(4) 更新履歴の保存

① 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らない。よって、入力者の識別・認証は必須となる。また、入力者と確定者が異なる場合は、確定者の識別・認証も必要となる。

具体的な対策については、6.5 章の利用者の識別・認証に係る記述を参照すること。

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くてはならない。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る。

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する。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る。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らない。

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る。

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ことが必要である。

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る。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る。

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する。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ある。

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らない。

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。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、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らない。

7.2.　見読性の確保に関する解説

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る。

- 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。
- 複数媒体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、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ことにより、紙の記録と同等といえる見読性を確保しなければならない。

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、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、「4.2　委託と第三者提供における責任分界」を参考にしつつ、あらかじめ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る。

7.3. 保存性の確保に関する解説

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、例えば下記のものが考えられる。

(1) 不正ソフトウェアによる情報の破壊及び混同等
(2) 不適切な保管・取扱いによる情報の滅失、破壊
(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
(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
(5) 障害等によるデータ保存時の不整合

様々な原因に対する技術面及び運用面での各種対策を施す必要がある。具体的には、不正ソフトウェアによる情報の破壊及び混同等、不適切な保管・取扱いによる情報の滅失、破壊、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、媒体・機器・ソフトウェアの不整合による情報の復元不能、障害等によるデータ保存時の不整合など原因に対する技術面及び運用面での対策が求められる。

また(1)～(5)の原因によってもバックアップが論理的又は物理的に改ざんされない仕組みも求められる。具体的な対応については、本編 6.10 章を参照。

これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

(1) 不正ソフトウェア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

不正ソフトウェア又はバグ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る。このため、不正ソフトウェアによるこれらの情報へのアクセスを防止しなければならない。

また、情報を操作する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確認しなければならない。

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。

(2) 不適切な保管・取扱いによる情報の滅失、破壊

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る。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らない。

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る。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る。

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る。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。

(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

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る。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る。

(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

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る。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ある。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る。

(5) 障害等によるデータ保存時の不整合

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にシステムが停止したり、ネットワークに障害が発生したりして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る。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。

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る。

8. 診療録及び診療諸記録を外部に保存する際の基準

調剤済み処方箋は、そのままの形式（紙又は電子）での外部保存のほか、紙媒体を 9 章に示す方法により電子化した上で外部保存することが可能である。紙の調剤済み処方箋の電子化については 3 章及び 9 章に、調剤録の外部保存については 3 章に記載があるので参照すること。

8. 診療録及び診療諸記録を外部に保存する際の基準のうち、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に関する解説

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ある。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る。

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ある。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ある。

8.1. 電子保存の 3 基準の遵守

別冊における解説はない。

8.2. 運用管理規程

別冊における解説はない。

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に関する解説

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る。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る。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る。

さらには、情報の保存を受託する事業者又は従業者による、利益を目的とした不当利用の危惧があるのも事実である。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る。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。

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る。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ある。

本項では「1. 外部保存を受託する事業者の選定基準」、「2. 情報の取扱い」、「3. 情報の提供」に分けて考え方を整理する。

4 章及び 6.11 章と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。

1. 外部保存を受託する事業者の選定基準

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

病院、診療所が自ら堅牢性の高い設備環境を用意し、近隣の病院、診療所の診療録等を保存する、ASP・SaaS 型のサービスを提供するような場合が該当する。

また、病院、診療所に準ずるものとして医療法人等が適切に管理する場所としては、公益法人である医師会の事務所で複数の医療機関等の管理者が共同責任で管理する場所等がある。

② 医療機関等が外部の事業者等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以外の機関が医療機関等の委託を受けて情報を保存するデータセンター等が該当する。

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る。

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る。

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ある。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ある。

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る。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る。

2. 情報の取扱い

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

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る。

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る。

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る。

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

本項で定める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、許されない。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る。

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る。

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、あるいは情報処理関連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る。

具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられる。

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い。

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る。

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る。分散保管においても同様の可用性の

保証が必要である。

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ある。

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らない。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る。

3. 情報の提供

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

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なくてはならない。

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らない。

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

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てはならない｡匿名化された情報であっても同様である。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る。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ない。

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る。

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らない。

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

てはならない。

8.4. 個人情報の保護

別冊における解説はない。

8.5. 責任の明確化

別冊における解説はない。

旧 8.4　外部保存全般の留意事項について

旧 8.4.2　外部保存契約終了時の処理に関する解説

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らない。

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らない。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る。

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る。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る。

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らない。

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らない。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ある。

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る。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らない。

旧 8.4.3　保存義務のない診療録等の外部保存について

3.4 章を参照すること。

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

別冊における解説はない。

10. 運用管理について

別冊における解説はない。

医療情報システムの安全管理に関するガイドライン　第 1 版から第 5.1 版までの改定履歴

版数	日付	内容
第 1 版	平成 17 年 3 月	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」、及び平成 14 年 3 月通知「診療録等の保存を行う場所について」に基づき作成された各ガイドラインを統合。 新規に、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（紙等の媒体による外部保存を含む。）及び医療・介護関連機関における個人情報保護のための医療情報システム運用管理ガイドラインを含んだガイドラインとして作成。
第 2 版	平成 19 年 3 月	平成 18 年 1 月の高度情報通信技術戦略本部（IT 戦略本部）から発表された「IT 新改革戦略」（平成 18 年 1 月）において、「安全なネットワーク基盤の確立」が掲げられたこと、及び平成 17 年 9 月に情報セキュリティ政策会議により決定された「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」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められたことを踏まえ、 (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について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適した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」として取りまとめる等の改定を実施。 (2) 自然災害・サイバー攻撃による IT 障害対策等について、医療の IT への依存度等も適切に評価しながら、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」を新設して取りまとめる等の改定を実施。

第3版	平成20年3月	第2版改定後、さらに医療に関連する個人情報を取り扱う種々の施策等の議論が進行している状況を踏まえ、 (1)「医療情報の取扱に関する事項」について、医療・健康情報を取り扱う際の責任のあり方とルールを策定し、「4　電子的な医療情報を扱う際の責任のあり方」に取りまとめる等の改定を実施。また、この考え方の整理に基づき「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」を改定。 (2)「無線・モバイルを利用する際の技術的要件に関する事項」について、無線LANを扱う際の留意点及びモバイルアクセスで利用するネットワークの接続形態毎の脅威分析に基づき、対応指針を6章と10章の関連する箇所に追記。特にモバイルで用いるネットワークについては、「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」に要件を追加。さらに、情報を格納して外部に持ち出す際の新たなリスクに対して「6.9　情報及び情報機器の持ち出しについて」を新設し、留意点を記載。
第4版	平成21年3月	第3版改定後、「医療機関や医療従事者等にとって、医療情報の安全管理には、情報技術に関する専門的知識が必要であり、さらに多大な設備投資等の経済的な負担も伴う」、「昨今の厳しい医療提供体制を鑑みれば、限りある人的・経済的医療資源は、医療機関及び医療従事者の本来業務である良質な医療の提供のために費やされるべきであり、情報化に対して過大な労力や資源が費やされるべきではない」、「他方、近年の医療の情報化の進展に伴い、個人自らが医療情報を閲覧・収集・提示することによって、自らの健康増進へ役立てることが期待されている」等の指摘がなされたことを踏まえ、より適切な医療等分野の情報基盤構築のため、 ・　「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」について、各所より医療情報に関するガイドラインの整合を図ることが求められていること、また、技術進歩に合わせた医療情報の取扱い方策について、物理的所在のみならず医療情

		報を基軸とした安全管理及び運用方策等をさらに体系的に検討し、読みやすさにも配慮することとして、「3.3　取扱いに注意を要する文書等」を新設し留意点を明記、5 章を全般的に見直し「5　情報の相互運用性と標準化について」として全面改定、「6.1　方針の制定を公表」、「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 C 項及び D 項を設置、「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」に外部からのアクセスに関する事項を追加、「7　電子保存の要求事項について」の B 項、C 項及び D 項を 7 章全体で大幅に見直し、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」に情報受託者が民間事業者である場合には、経済産業省及び総務省が発出しているガイドラインに準拠することを明記、その他、技術的要件の見直し、各種省令・通知等と A 項の関係性整理等、全般的な改定を実施。
第4.1版	平成 22 年 2 月	平成 21 年 11 月の医療情報ネットワーク基盤検討会において、診療録等の保存を行う場所について、各ガイドラインの要求事項の遵守を前提として「「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする提言が取りまとめられたことを受けて、外部保存通知の改正を行い、本ガイドラインにおいても関連する 4 章、8 章、10 章の一部を中心に改定を実施した。 4 章では「4.3　例示による責任分界点の考え方の整理」に「(4) オンライン外部保存を委託する場合」を追加した。 8 章では、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」の「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」を「③医療機関等が民間事業者等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」とし、内容を通知に合わせて改定した。 10 章は、これらの改定に合わせて内容の整合性を図っている。
第4.2版	平成 25 年 10 月	平成 25 年 3 月に外部保存通知の一部改正が行われ、調

		剤済み処方箋及び調剤録等の外部保存が認められたことから、本ガイドラインにおいても関連する 3 章、8 章、9 章の一部を改定。 　また、モバイル端末の普及に鑑み、機器の取扱いについて明確化するとともに、災害等の非常時の対応について、大規模災害時を想定した考え方について追記するため 6 章の一部を改定。 　さらに、医療情報の相互運用性と標準化について、最新の技術等への対応として、5 章を改定。 　3 章では、「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」を追加した。 　5 章では、「5.1.1　厚生労働省標準規格」を追加した。 　6 章では、「6.9　情報及び情報機器の持ち出しについて」を明確化するとともに「6.10　災害等の非常時の対応」に大規模災害時を想定した考え方を追加した。 　8 章では、調剤済み処方箋の外部保存に関する記述を追加した。 　9 章では、「9.4　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」を追加した。
第 4.3 版	平成 28 年 3 月	平成 28 年 3 月に「電子処方せんの運用ガイドライン」が発出されたことを踏まえ、本ガイドラインで関連する 3 章、8 章、9 章の一部を改正した。
第 5 版	平成 29 年 5 月	医療機関等を対象とするサイバー攻撃の多様化・巧妙化、地域医療連携や医療介護連携等の推進、IoT 等の新技術やサービス等の普及への対応として、関連する 1 章、6 章等を改定するとともに、第 4.2 版の公表以降に追加された標準規格等への対応を行った。 　また、平成 27 年度改正個人情報保護法や「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」等への対応を行った。（本ガイドライン 6 章、8 章、付則 1 及び付則 2 の記載事項については、「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」Ⅲの 4 の（4）「医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取扱い」において、本ガイドラインによることとされている。） 　1 章では、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旨を明確化した。また、平成 27 年度改正個人情報保護法や「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」等を踏まえた修正を行った。 3 章では、1 章の改定を踏まえ、7 章及び 9 章の対象になり得る介護事業者の文書等について追記した。 4 章では、関連する平成 27 年度改正個人情報保護法や「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」等の規定を参照した。 5 章では、厚生労働省標準規格や JAHIS 標準規約等を追加し、所要の改定を行った。 6 章では、規格の更新を受け、「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を行った。6.2 章では、「『製造業者による医療情報セキュリティ開示書』ガイド」に係る追記を行った。また、「6.5　技術的安全対策」では、利用者の識別・認証について B 項、C 項、D 項の内容を改定するとともに、上述の IoT について「(6) 医療等分野における IoT 機器の利用」を設け、C 項及び D 項を追加した。「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」では、サイバー攻撃に事前・事後の対応について、改定を行った。このことに併せて、6.10 章の章題も改定している。「6.9　情報及び情報機器の持ち出しについて」では、公衆無線 LAN や個人所有又は個人の管理下にある端末の業務利用 (BYOD) の取扱い等、モバイル端末の使用時における規定を改定した。「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」では、オープンなネットワークを介した SSL/TLS 接続について C 項を追加した。「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」では、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を行った。 7 章では、電子カルテ等の入力における関係者の役割や責任を明確化するとともに、代行入力に係る取扱いについ

		て、「7.1　真正性の確保について」を改定した。また、将来における互換性の確保について、「7.3　保存性の確保について」を改定した。 10 章は、これらの改定に合わせて所要の改定を行った。 分かりやすさの観点から、全般的な表現の修正を行った。
第5.1版	令和 3 年 1 月	医療機関等を対象とするサイバー攻撃の多様化・巧妙化、スマートフォンや各種クラウドサービス等の医療現場での普及、各種ネットワークサービスの動向への対応として、関連する 4 章、6 章等の改定を行った。 また、各種ガイドラインとの整合性の確保や近時の個人情報に関する状況等への対応として、6 章、8 章の改定を行った。 4 章では、クラウドサービスの概要を示すとともに、これを利用した場合の責任分界の考え方や、複数の事業者を利用する場合の責任分界の考え方を示すため、「4.3　例示による責任分界点の考え方の整理」に追記等を行った。 6 章では、リスク分析を行う際に、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を考慮するために、「6.2.3 リスク分析」に追記等を行った。 また、近時のサイバー攻撃などへの対応に求められる措置として、ネットワークの監視等の管理に関する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込みにおける対応措置等の必要性について、「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」に追記を行った。 医療情報システムにおける利用者認証について、第 5 版において示した二要素認証導入を促す方針をさらに進めるため、「6.5　技術的安全対策」の B 項及び C 項の改定を行った。 また、暗号鍵の管理に関する内容も新規に規定し、「6.5 技術的安全対策」に追記を行った。 サイバー攻撃を含む非常時の体制整備の観点から、非常時の体制構築に関する内容や、平常時における教育・訓練、サイバー攻撃等が生じた場合の通報等を示すため、「6.10 災害、サイバー攻撃等の非常時の対応」に追記等を行った。

		8章では、外部保存における受託事業者に関して、行政機関等が設置するデータセンターと、民間事業者が設置するデータセンターに関する選定のあり方について、考え方及び要求事項を統合するために、「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」の改定を行った。併せて、受託事業者の選定に関して、Cookie等の取扱いに関する事項や、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などに関する内容を示すため、「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」に追記を行った。 その他、関連法規の改正に伴う部分の修正を行うとともに、分かりやすさの観点から、全般的な表現の修正を行った。

別紙

付表1　一般管理における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	総則	理念（基本方針と管理目的の表明）	A		・情報システムの安全管理に関する方針に基づき、本規程の目的を述べる	・この規程は、〇〇病院（以下「当院」という。）において、情報システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当院において、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に資することを目的とする。
		対象情報	A		・対象システム、対象情報を定める ・対象システム、対象情報を安全管理上の重要度に応じて分類し、リスク分析を行う	・対象システムは、電子カルテシステム、オーダエントリシステム、画像管理システム、・・・である。 ・対象システムの扱う情報については、そのシステムごとに別途定義と安全管理上の重要度の分類を行い、リスク分析の結果を表に記入し保管すること。
		標準規格	B		・医療機関等側でフォローすべき標準規格の列挙を行い、標準規格の改訂への対応をシステム改定時に変更の対象とする	・システム管理者は、別表に挙げる標準規格についての変更状況を確認し、システムの変更・改造時の対象とすること。
			C		・ベンダに対しシステムで使われている標準規格に関する情報提供を求め、標準規格の改訂への対応をシステム改訂時に変更の対象とする	・システム管理者は、情報システムで使われている標準規格についてベンダへ情報提供を要求し、標準規格の改訂への対応をシステムの変更・改造時の対象とすること。
②	管理体制	運用責任者、個人情報保護責任者、システム管理者	B		・運用責任者、個人情報保護責任者、システム管理者、機器管理者、安全管理者等の任命規程	・当院に運用責任者及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、情報システムに関する運用を担当する管理者（以下「システム管理者」という。）を置くこと。 ・システム管理者は病院長が指名すること。 ・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、病院長の下に情報システム管理委員会を置くこと。 ・情報システム管理委員会の運営については、別途定めること。 ・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。
			C		・院長が運用責任者、個人情報保護責任者とシステム管理者を兼ねる場合、その旨を明記する	・当クリニックに運用責任者、個人情報保護責任者及びシステム管理者を置き、院長をもってそれに充てること。 ・院長は、必要な場合、システム管理者を別に指名すること。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		マニュアル・契約書等の文書管理体制	A		・別途定めてある文書管理規程に従うことを規定する	・契約書、マニュアル等の文書の管理については、別途規程を定めること。 ・システム管理者は、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。
		監査体制と監査責任者	B		・監査体制（監査の周期、監査結果の評価・対応等）を規定する ・監査責任者の任命規程	・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。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・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、病院長がこれを定めること。 ・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。
			C		・院内で監査体制を整えることができない場合、第三者への監査依頼を規定する	・情報システムの監査を XX との契約により毎年 X 回行い、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。
		患者及びシステム利用者からの苦情・質問の受付体制	A		・患者及びシステム利用者からの苦情・質問受付窓口の設置 ・受付後の処置を規定する	・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。
		事故対策	A		・緊急時あるいは災害時の連絡、復旧体制並びに回復手段を規定する	・システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め文書化し、利用者に周知の上、常に利用可能な状態におくこと。
		システム利用者への教育・訓練等周知体制	A		・各種規程書、指示書、取扱説明書等の作成 ・定期的な利用者への教育、訓練	・システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・システム管理者は、情報システムの利用者に対し、定期的に情報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うこと。
③	管理者及び利用者の責務 ※監査責任者に係る記述を削除する	システム管理者や運用責任者の責務	A		・機器、ソフトウェア導入時の機能確認 ・運用環境の整備と維持 ・情報の安全性の確保と利用可能な状況の維持 ・情報の継続的利用の維持 ・不正利用の防止 ・利用者への教育、訓練 ・患者又は利用者からの問い合わせ・苦情窓口設置	・情報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、システムの機能を確認すること。 ・情報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こと。 ・診療情報の安全性を確保し、常に利用可能な状態におくこと。 ・機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持すること。 ・システム管理者は情報システムの利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
					・外部のサービス事業の利用に当たっては、必要なガイドラインへの適合性を、サービス事業者からの文書等により確認する	・情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行うこと。 ・患者及び利用者から、情報システムについての問い合わせや苦情を受け付ける窓口を設けること。 ・外部のサービス事業の利用に当たっては、必要なガイドラインへの適合性を、サービス事業者からの文書等により確認し、文書の保存を行うこと。
		利用者の責務	B		・自身の認証番号やパスワードあるいはICカード等の管理 ・利用時にシステム認証を必ず受ける ・確定操作の実施による入力情報への責任の明示 ・権限を超えたアクセスの禁止 ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常、不正アクセスを発見した場合の速やかな運用管理者へ通知 ・離席対策	・利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。 ・利用者は、情報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、システムに自身を認識させること。 ・利用者は、情報システムへの情報入力に際して、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。 ・利用者は、与えられたアクセス権限を超えた操作を行わないこと。 ・利用者は、参照した情報を、目的外に利用しないこと。 ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、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。 ・利用者は、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。 ・利用者は、離席する際は、ログアウトすること。
			C		・利用者が限定される運用の場合、その旨を明記し、責任の所在を明確にする ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常時の対応を規定する	・利用者は、XXX、XXX、XXX である。 ・利用者は、参照した情報を、目的外に利用しないこと ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、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。 ・利用者は、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。
④	一般管理における運用管理事項	来訪者の記録・識別・入退の制限等の入退管理規程	B	・IDカード利用による入退者の制限、名札着用の実施 ・PCの盗難防止チェーンの設置 ・防犯カメラの設置 ・施錠	・入退者の名簿記録と妥当性チェック等の定期的チェック	・個人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者は名簿に記録を残すこと。 ・入退出の記録の内容について定期的にチェックを行うこと。
			C	・施錠	・スタッフの常駐	・個人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は、スタッフの常駐又は施錠できる部屋に設置すること。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		情報システムへのアクセス制限の決定方針及び記録、点検等のアクセス管理	B	・ID・パスワード、IC カード、生体認証等により診療録データへのアクセスにおける識別と認証を行う ・監査ログサーバを設置し、アクセスログの収集を行う	・管理規則に則ったハードウェア・ソフトウェアの設定を行う ・認証方法等に応じた適切なパスワード設定・運用を行う ・情報区分とアクセス権限に基づくアクセスできる診療録等の範囲を定め、アクセス管理を行う ・誰が、いつ、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行う	・ID・パスワードに用いるパスワードについて、認証方法に応じて適切に設定・運用すること。 ・システム管理者は、職務により定められた権限によるデータアクセス範囲を定め、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、その内容に沿って、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。
			C	（上記技術的対策が行えない場合）	・システム操作業務日誌を備え、システムを操作するものはシステム操作業務日誌に操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象を記載する ・システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を確認する	・システム管理者はシステム操作業務日誌を設置すること。 ・利用者は、操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象をシステム操作業務日誌に記載すること。 ・システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を評価すること。
		個人情報を含む記録媒体の管理（保管・授受等）規程	A		・保管、バックアップ作業を的確に行う	・保管、バックアップの作業に当たる者は、手順に従って行い、その作業の記録を残し、システム管理者の承認を得ること。
		個人情報を含む媒体の廃棄の規程	A	・技術的に安全（再生不可）な方式で破棄を行う	・情報種別ごとに破棄の手順を定める・手順には破棄を行う条件、破棄を行うことができる従事者の特定、具体的な破棄の方法を含める	・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。
		リスクに対する予防、発生時の対応方法	A		・情報に対する脅威を洗い出し、そのリスク分析の結果に対し予防対策を行う ・リスク発生時の連絡網、対応、代替手段等を規定する	・システム管理者は、業務上において情報漏えい等のリスクが予想されるものに対し、運用管理規程の見直しを行うこと。また、事故発生に対しては、速やかに運用責任者に報告し利用者に周知すること。
		技術的と運用的対策の分担を定めた文書の管理規程	A	・6 章全般に基づいて取られる技術的対策 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	・左記の項と対応する、運用事項 ・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」別紙に示す「サービス仕様適合開示書」に基づ	・各システムは、その設計時及び運用開始時に、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。 ・システムの保守時には、基準適合チェックリスト記載に従っていることを確認すること。 ・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。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
				ィ開示書（JIRA/ JAHIS による）」技術的対策項目	き、運用的対策が必要な事項への対応の実施。なお具体化のために、「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（ JIRA/JAHIS）」が参考になる。	・技術的対策内容は「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」別紙に示す「サービス仕様適合開示書」等で確認をすること。
		IoT 機器利用に関する事項		・サイバーセキュリティに関して製造販売事業者の情報提供文書を、組み込んだ実施 ・購入後に発見された脆弱性対策に実施 ・機器・システムの動作状態の監視を実施	・患者への機器貸し出しに関して、リスク等の注意事項、不具合時の連絡先等の情報を提供する ・機器の管理台帳の作成により、使用終了機器・不具合未対応機器の再利用を防止する	・IoT 機器の利用において、サイバーセキュリティに関して対策を行うこと。 ・製造販売事業者提供の文書を運用実施手順書に含めること。 ・購入後に発見された脆弱性対策に実施においても同様とすること。 ・患者への機器貸し出しに関して、リスク等の注意事項、不具合時の連絡等の情報を提供すること。 ・機器の管理台帳により、使用終了機器・不具合未対応機器の再利用を防止すること。 ・機器・システムの状態や通信状態を収集・把握し、ログを適切に記録すること。
		無線 LAN に関する事項	A	・ステルスモード、ANY 接続拒否設定、不正アクセス対策、暗号化を行う	・利用者への規則の説明を行う ・電波発生機器の利用に当たっての規則を定める	・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すること。 ・システム管理者は、無線 LAN 利用規則を院内関係者及び利用可能性のある入院患者へ説明をすること。
		電子署名・タイムスタンプに関する規程	A	・電子証明書による電子署名環境 ・タイムスタンプ付与環境 ・電子署名の検証環境	・利用する電子証明書が、ガイドラインが求める信用性を有していることを記載した文書の作成 ・署名が必要な文書に電子署名があることの確認手順の作成 ・タイムスタンプを付与する作業手順の作成 ・電子的な受領文書の電子署名検証手順の作成	・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。 ・システム管理者は、電子的に受領した文書に電子署名がある場合の、署名検証手順を定めること。
⑤	業務委託の安全管理措置	委託契約における安全管理・守秘条項	A		・包括的な委託先の罰則を定めた就業規則等で裏付けられた守秘契約を締結する	・業務を当院外の所属者に委託する場合は、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、その部門の長とする。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、かつ安全に行われていることを確認すること。
		再委託の場合の安全管理措置事項	A		・委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とする	・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。
		システム改造及び保守での医療機関等関係	A	・保守要員用のアカウントを設定する	・保守要員用のアカウントを確認する ・保守作業等の情報システムに直接ア	・システム管理者は、保守会社における保守作業に関し、その作業者及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。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		者による作業管理・監督、作業報告確認		・保守作業におけるログの取得と保存	クセスする作業の際には、作業者・作業内容・作業結果の確認を行う ・清掃等直接情報システムにアクセスしない作業の場合、定期的なチェックを行う ・保守契約における個人情報保護の徹底 ・保守作業の安全性についてログによる確認	
⑥	情報及び情報機器の持ち出しについて	持ち出し対象となる情報及び情報機器の規程	A		・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に関する方針を運用管理規程で定める	・システム管理者は、情報及び情報機器の持ち出しに関しリスク分析を行い、持ち出し対象となる情報及び情報機器を規定し、それ以外の情報および情報機器の持ち出しを禁止すること。 ・持ち出し対象となる情報若しくは情報機器は別表としてまとめ、利用者に公開すること。 ・個人保有又は個人管理下の情報機器の業務利用（BYOD）は、管理者による安全管理措置を施すものとする。
		持ち出した情報及び情報機器の運用管理規程	A		・持ち出した情報及び情報機器の管理方法を定める ・情報が格納された可搬媒体及び情報機器の所在を、台帳を用いる等して把握する	・情報及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。 ・システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録すること。その内容を定期的にチェックし、所在状況を把握すること。
		持ち出した情報及び情報機器への安全管理措置	A	・情報機器に対して起動パスワード等を設定する ・持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続したりする場合は、コンピュータ不正ソフトウェア対策ソフトの導入やパーソナルファイアウォールを用いる等して、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施す ・公衆無線 LAN は使用せず、公衆無線 LAN しか使用できない環境にある場合は、6.11 章の基準に則り使用する	・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等、適切なパスワードの設定・運用を行う ・持ち出した情報を、承認されていないソフトウェアがインストールされた（あるいは承認されていないサービスが利用できる）情報機器で取り扱わない ・医療機関等が管理する情報機器の場合は、このようなアプリケーションをインストールしない	・持ち出す情報機器について起動パスワード等を設定すること。推定しやすいパスワード等の利用を避ける等、適切なパスワードの設定・運用を行うこと。 ・持ち出す情報機器について、不正ソフトウェア対策ソフトをインストールしておくこと。 ・公衆無線 LAN を使用しないこと。公衆無線 LAN しか使用できない環境にある場合には「医療情報システムの安全管理に関するガイドライン」で定める基準に則り使用すること。 ・持ち出した情報を、別途定められている以外のアプリケーションがインストールされた（あるいは承認されていないサービスが利用できる）情報機器で取り扱わないこと。 ・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、あるいは承認されていないサービスが利用しないこと。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		盗難、紛失時の対応策	A	・情報に対して暗号化したりアクセスパスワードを設定したりする等、容易に内容を読み取られないようにする	・情報を格納した可搬媒体及び情報機器の盗難、紛失時の対応	・持ち出した情報及び情報機器の盗難、紛失時には、直ちにシステム管理者に届け出ること。 ・届出を受け付けたシステム管理者は、その情報及び情報機器の重要度にしたがって、別途定めるとおり対応すること。
		利用者への周知徹底方法	A		・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し、教育を行う	・システム管理者は、情報及び情報機器の持ち出しについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・システム管理者は、利用者に対し、情報及び情報機器の持ち出しについて研修を行うこと。また、研修時のテキスト、出席者リストを残すこと。
⑦	外部の機関と医療情報を交換する場合	安全を技術的、運用的面から確認する規程	A	・6.11 章に基づいて行われる技術的対策	・左記の項と対応する、運用事項	・システム管理者は、外部の機関と医療情報を交換する場合、リスク分析を行い、安全に運用されるように別途定める技術的及び運用的対策を講じること。 ・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。
		リスク対策の検討文書の管理規程	A		・上記のリスク対策の検討文書を作成し管理する	
		情報処理関連事業者との通常運用時、事故処理時それぞれで責任分界点を定めた契約文書の管理と契約状態の維持管理規程	A		・医療機関等の間の情報通信に関連する医療機関等、電気通信事業者やシステムインテグレータ、クラウドサービス事業者、運用委託事業者等、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 ・またその契約状態を維持管理する規程を定めている	・外部の機関と医療情報を交換する場合、相手の医療機関等、電気通信事業者、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。 ・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。
		リモートメンテナンスの基本方針	A	・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を行って不必要なログインを防止する	・遠隔保守を行う事業者との間で、責任分界点、責任の所在を契約書等で明確にすること	・外部の保守会社からリモートメンテナンスを受ける場合、相手の保守事業者等、電気通信事業者、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。 ・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。
		従業者による医療機関等の外部からアクセスする場合の運用管理規程	A	・医療機関等の内部のシステムに不正な侵入等を防止する技術的対策	・外部からアクセスを許容する機器及びその状態を規定する ・外部からアクセスを許容した機器が、その許容状態を保持しているのかを確認する	・外部からアクセスを許容する機器については、別途定める規程に従ったものに限定すること。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。
⑧	自然災害やサイバー攻撃等による非常時の対策	BCP の規程における医療情報システムの項	A		・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”と判断する仕組み、正常復帰時の手順を設ける	・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、別途定める事業継続計画（BCP）に従って運用を行うこと。 ・どのような状態を非常時とみなすかについては、別途定める基準、手順に従って運用責任者が判断すること。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
					・すなわち、判断するための基準、手順、判断者、をあらかじめ決めておく	
		システムの縮退運用管理規程	A	・技術的な縮退運用時機能	・システムが縮退運用を行っている際の、運用管理規程	・システムの縮退運用時や非常時の運用に関して運用管理規程を作成し、利用者に周知の上、常に利用可能な状態におくこと。
		非常時の機能と運用規程	A	・技術的な非常時用機能	・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規約 ・「非常時のユーザアカウントや非常時用機能」の管理手順	
		サイバー攻撃対策のためのバックアップ取得	A	・技術的な平常時のバックアップ対策	・サイバー攻撃に備えたバックアップ取得規則（取得対象、取得方法等） ・サイバー攻撃に備えたバックアップ取得手順	・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
		報告先と内容一覧	A		・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を行う	・災害、 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、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した等の場合には、別途定める一覧の連絡先に連絡すること。 ・所管官庁への連絡については、「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）に基づき行うこと。
⑨	教育と訓練	マニュアルの整備	A		・マニュアルの整備	・システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。
		定期又は不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修	A		・定期又は不定期な電子保存システムの取扱い及びプライバシー保護に関する教育、研修	・システム管理者は、利用者に対し、定期的に情報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うこと。また、研修時のテキスト、出席者リストを残すこと。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		従事者に対する人的安全管理措置	A		・守秘契約、業務規程 ・退職後の守秘規程 ・規程遵守の監査	・当院の業務従事者は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負う。
⑩	監査		B		・定期的な監査の実施 ・監査責任者の任命、役割、責任、権限を規定 ・監査結果の検討、規程見直しといった手順の規定	・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。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・監査責任者は病院長が指名すること。 ・システム管理者は、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、病院長がこれを定めること。 ・システム管理者は、必要な場合、臨時の監査を監査責任者に命ずること。
			C		・第三者に監査を委託している場合、その旨を記載する ・監査内容と実施規程の提供を受け保管する ・監査結果に対する対応を規定する	・情報システムの監査を XX との契約により毎年 X 回行い、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。
⑪	その他		A		・運用管理規程の公開について規定する ・運用管理規程の改定の規程	

付表2　電子保存における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	真正性確保	入力者及び確定者の識別及び認証	B	・利用者識別子、パスワード等による識別と認証	・利用者識別子とパスワードの発行、管理 ・パスワードの最低文字数、有効期間等の規定 ・パスワード以外の認証要素の発行・登録・利用・変更・削除等の規定 ・認証の有効回数、超過した場合の対処 ・入力者及び確定者への認証操作の義務付け ・識別子、パスワードの他人への漏えいや、パスワード方法以外の認証に必要な情報・機器等の他人への貸出し、メモ書きの禁止 ・入力者及び確定者への教育 ・緊急時認証の手順規程	・システム管理者は、電子保存システムの入力者及び確定者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。 ・パスワードの最低文字数、有効期間等を別途規定すること。 ・パスワード以外の認証要素に関し、採用した認証方法（例：指紋認証、IC カードによる認証等）の発行・登録・利用・変更・削除等について、別途規定すること。 ・認証の有効回数、超過した場合の対処を別途規定すること。 ・入力者及び確定者は、自身の認証番号やパスワード、その他認証に係る情報等を管理し、これを他者に利用させないこと。 ・入力者及び確定者は、電子保存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、システムに自身を認識させること。 ・システム管理者は、電子保存システムを正しく利用させるため、入力者及び確定者の教育と訓練を行うこと。
				・ログアウト操作、自動ログアウト機能、スクリーンセーブ後の再認証等	・入力者及び確定者への終了操作義務付け ・離席時の対処の規程と周知	・入力者及び確定者は、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。
			A	・運用状況において確定者が自明の場合は、技術的対策なし	・確定者を明記する ・定期的な実施状況の監査	・電子保存システムにおいて保存されている情報の確定者は XX である。
		情報の確定手順と、識別情報の記録	B	・技術的に入力した情報の確定操作を行う機能	・確定者への確定操作法の周知・教育 ・確定者が、何らかの理由で確定操作ができない場合の対応を明記する ・代行入力の場合、確定者による確定を義務付け	・確定者は、電子保存システムへの情報入力に際して、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。 ・確定者が何らかの理由で確定操作ができない場合には、管理責任者が自身の責任において確定操作を行うこと。 ・代行入力の場合、確定者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			B	・技術的に情報に確定者の識別情報を記録する機能	・確定者への確定操作法の周知・教育	・確定者は、電子保存システムへの情報入力に際して、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。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
						・代行入力の場合、確定者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			A	・運用において確定の状況が自明の場合は、「確定」操作はない	・「確定」を定義する状況を運用管理規程に明記する	・本規程が対象とする情報システムの作成データの「確定」については、付表に記す。[付表として、各システムの操作における「確定」の定義を行う。“xx機器のyyボタン操作の時点”、“確定操作”等]
		更新履歴の保存	B	・技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・確定者への確定操作法の周知・教育 ・確定後の記録の追記・訂正・消去に係る手順の周知・教育	・確定者は、電子保存システムへの情報入力に際して、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。 ・代行入力の場合、確定者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
		代行入力の承認記録	B	・技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・代行入力を依頼する可能性のある担当者に、確定者による確定操作を徹底すると同時に、適宜履歴の監査を行う	・代行入力の場合、確定者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
		機器・ソフトウェアの品質管理、動作状況の内部監査規程	A		・定期的な機器、ソフトウェアの動作確認 ・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の規定	・システム管理者は、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。
②	見読性確保	情報の所在管理	A	・技術的に情報の論理的所在確認を行う	・情報機器・媒体のリストを作成し、物理的所在場所の確認を行う	・システム管理者は定期的に情報の所在確認を行うこと。
		見読化手段の管理	A	・見読に必要な機器（モニタ、プリンタ等）の整備を行う	・見読化手段の維持、管理（例えば、モニタ・プリンタの管理やネットワークの管理）要件を明記する	・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、保存義務のある情報として電子保存された情報ごとに、見読用機器を常に利用可能な状態におくこと。
		見読目的に応じた応答時間とスループット	A	・応答時間の確保ができるシステム構成、機器の選定	・システム利用における見読目的の定義と、システム管理により業務上から要請される応答時間の確保を行う	・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、必要な対策を行うこと。
		システム障害対策	A	・システムの冗長化	・システム障害時に備えた機器・システムの維持体制を定める ・データのバックアップ	・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。データバックアップ作業が適切に行われていることを確認すること。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
③	保存性確保	ソフトウェア・機器・媒体の管理	A		・定期的な機器、ソフトウェアの動作確認 ・媒体の保存場所、その場所の環境、入退出管理	・システム管理者は、電子保存システムで使用されるソフトウェアを、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こと。 ・電子保存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こと。 ・システム管理者は、定期的にソフトウェアの不正ソフトウェアチェックを行い、感染の防止に努めること。 ・設置場所には無水消火装置、漏電防止装置、無停電電源装置等を備えること。 ・設置機器は定期的に点検を行うこと。
		不適切な保管・取扱いによる情報の滅失、破壊の防止策	A		・作業の管理を行う ・データのバックアップを行う ・業務担当者の変更に当たって教育を行う	・システム管理者は新規の業務担当者には、操作前に教育を行うこと。
		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策	A		・記録媒体劣化以前の情報の複写を規程	・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こと。 ・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こと。
		媒体・機器・ソフトウェアの不整合による復元不能の防止策	A	・マスタ DB 変更時に過去の情報に対する内容変更が起こらない機能 ・標準形式でのデータ入出力機能	・システムの移行時のデータベースの不整合、機器 ・媒体の互換性不備に備えたシステム変更・移行時の業務計画の作成 ・定期的なバグフィックスや不正ソフトウェア対策の実施	・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。
④	相互運用性確保	システムの改修に当たっての、データ互換性の確保策	A	・標準的な規約（例えば、HL7、DICOM、HELICS、IHE 等）に従った情報形式を持つシステム構築	・システム更新時の継続性確保策 ・異なる施設間の場合、契約により責任範囲を明確にすることを規定する	・機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用できるよう維持すること。
		システム更新に当たっての、データ互換性の確保策	A			
⑤	スキャナ読み取り書類の運用	スキャナ読み取りの対象にする文書の規程	A		・対象文書を定める	・システム管理者は、適宜、業務において規程に則った運用がなされていることを確認すること。
		スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	A	・適切な精度のスキャナの使用	・スキャナ読み取りに係る運用管理規程を設け、対象文書ごとに、情報作成管理者、作業責任者、スキャン精度、電子証明・タイムスタンプ、スキャン後	

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		スキャナ読み取り電子情報への作業責任者の電子署名及び認証業務に関する法律に適合した電子署名・タイムスタンプ	A	・電子署名・タイムスタンプ環境の構築	の原本の取扱い等を明記する（対象文書種別によって責任者が異なる場合は、対象文書種別と責任者の関係を明確にすること）	
		診療の都度、スキャンするタイミングの規程	A	・タイムスタンプ機能	・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（1～2 日程度以内）にスキャンを行うことを運用管理規程で定め、遅滞なくスキャンを行う	

付表3　外部保存における運用管理の例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①、⑨	管理体制と責任	管理体制の構築、受託する機関の選定、責任範囲の明確化、契約	B		・管理体制の構築、受託する機関の評価・選定、契約	・この規程は、〇〇病院（以下「当院」という。）において、診療録及び診療諸記録（以下「診療記録」という。）の、ネットワークを経由して XX において保管するための仕組みと管理に関する事項を定めたものである。本規程の付表に、当院における管理体制（運用責任者、システム管理者、各作業実務者（外部の実業務委託者を含む。））、XX への監査体制（監査者）を定める。 　なお、システム管理者は、保管を委託する XX は「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する事業者の選定基準」を満たしていることを適宜確認すること。XX が民間事業者等のデータセンター等の情報処理関連事業者である場合には、「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」（総務省・経済産業省　令和 2 年 8 月 21 日）の要求事項を満たしていることを確認すること。 確認には、XX からの適合性を示す文書を持って行い、文書は保管する。
			C		・管理体制の構築、受託する機関の評価・選定、契約	・この規程は、〇〇病院（以下「当院」という。）において、診療録及び診療諸記録（以下「診療記録」という。）の、ネットワークを経由して XX において保管するための仕組みと管理に関する事項を定めたものである。運用責任者は院長とし、運用内容の管理実務及び監査は△△に委託する。また、保管を受託する XX の評価、管理・監査を受託する△△への評価を添付する。 　なお、院長は、保管を委託する XX は「医療情報システムの安全管理に関するガイドライン」が定める「外部保存を受託する事業者の選定基準」を満たしていることを△△に適宜確認すること。また、XX が民間事業者等のデータセンター等の情報処理関連事業者である場合には「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」（総務省・経済産業省　令和 2 年 8 月 21 日）要求事項を満たしていることを△△に適宜確認すること。 確認には、適合性を示す文書を持って行い、文書は保管する。
		受託する機関への監査	A		・受託する機関に対する保管記録の監査規程作成、契約	・システム管理者は、XX における「診療記録」の保管内容を示す記録を監査し、正しいことを確認する。異常の発見時には直ちに運用責任者に報告するとともに、XX と契約の責任分担に基づき対処に着手する。また、これらの確認記録を残す。
					・受託する機関での管理策の承認、実施監査規程作成、契約	・システム管理者は、XX における受信「診療記録」の管理策を精査し、承認する。その管理策の実施状況を必要時に監査する。異常の発見時には直ちに運用責任者に報告するとともに、XX に対し対処を指示し、結果を確認する。また、これらの監査記録を残す。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		責任の明確化	A		・通常運用における責任、事後責任の分界点を定める	・運用責任者は、定められた責任体制が維持されていることを確認する。
		動作の監査	B	・委託する機関での送信記録、受託する機関での受信記録の保持	・委託する機関での送信記録、受託する機関での受信記録の合致監査	・システム管理者は、XX から「診療記録」の受信記録を受け取り、送信した「診療記録」との合致を確認する。また、確認した旨の作業記録を残す。異常の発見時には直ちに運用責任者に報告するとともに、XX と契約の責任分担に基づき対処に着手する。
			C	（監査目的に耐える記録レベル、保存期間である）	・監査（上記を含む全て）を第三者へ委託した場合は、定期的報告（6 ヶ月程度）を受ける	・運用責任者は、監督を委託した△△から、『XX からの「診療記録」の受信記録、送信した「診療記録」との合致を確認した』旨の報告を受け、確認後に報告内容の保管を行う。また、異常発生時には直ちに報告を受け、△△とともに対処に着手する。
		不都合な事態への対処	A		・受託する機関との間で、不都合な事態（異常の可能性も含む。）の責任対処作業範囲を定める	・運用責任者は「診療記録」流出の危険があると判断した時には、直ちに外部保存の運用を停止する。
②	外部保存契約終了時の処理		A		・保管データの破棄契約と管理者による確認、守秘義務契約	・【契約事項として】当院と XX との契約終了時には、それまでに保管を受託した全ての「診療記録」を当院に戻す（あるいは、利用不可能な形で廃棄する）こととし、その結果について当院の監査を受けるものとする。また、XX が受託期間中に異常への対応等で「診療記録」の内容にアクセスした場合、その内容についての守秘義務は、本保管委託契約終了後も有効である。
③	真正性確保	相互認証機能の採用	A	・TLS あるいは相互認証付き VPN の使用	・認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する ・双方が合意すれば、特に独立した第三者の認証局である必要性はない	・システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方のなりすましがないことを確認する。
		通信上で「改ざんされていない」ことの保証	A	・TLS あるいはメッセージ認証付きの VPN の使用	・認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する ・双方が合意すれば、特に独立した第三者の認証局である必要性はない	・システム管理者は、記録による動作の確認において、通信上の改ざんの発見に努める。
④	見読性確保	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とスループット システム障害対策	A		・付表2の見読性確保と同じ技術的対策・運用的対策がとられていることの確認	・システム管理者は、XX における見読性対策が適切であることを確認する。監査者は必要に応じて XX の設備を監査する。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
⑤	保存性確保	外部保存を受託する事業者での保存確認機能	A	・受託する機関との間で、改ざんされることのないデータとして保存されたことを確認できる機能、例えばネットワークを介したストレージへの保管確認機能、あるいは保存を委託する機関への保管内容送信機能（1 時間～1 日単位）	・付表2の保存性確保と同じ技術的対策・運用的対策がとられていることの確認 ・受託先での保存が確認された時点まで委託元でのデータ削除を行わない旨の規定の確認	・システム管理者は、XX における保存性対策が適切であることを確認する。監査者は必要に応じて XX の設備を監査する。
		標準的なデータ形式及び転送プロトコルの採用	A	・DICOM、HL7、標準コードの使用あるいはこれらへの変換機能		
		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確保	A		・継続性の保証契約を交わす	・【契約事項として】当院と XX は、互いに各自のシステム変更に当たって、相互にデータ通信の継続性に配慮し、変更内容が外部保存の障害にならないように協議をする。
⑥	診療録等の個人情報を電気通信回線で伝送する間の個人情報保護策	秘匿性の確保のための適切な暗号化	A	・メッセージの暗号化が可能な通信手段 ・暗号の強度は、電子署名法令に準じる		
		通信の起点・終点識別のための認証	A	・TLS あるいは相互認証付き VPN の使用 ・暗号の強度は、電子署名法令に準じる	・認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する ・双方が合意すれば、特に独立した第三者の認証局である必要性はない	・システム管理者は、記録による動作の監査において、委託する機関、受託する機関双方が正当であることを確認する。
⑦	外部保存を受託する事業者内での個人情報保護策	外部保存を受託する事業者における個人情報保護	A		・受託する機関と受託する機関側における業務従事者への教育、守秘義務	・監査者は必要に応じて XX を監査する。 【契約事項として】①XX は当院から受けた保管委託を再委託してはならない。②XX は「診療記録」の保管業務に従事する従業員に対して「個人情報保護の重要性」の教育を年 1 回行う。また、その業務を離れた後も有効な守秘契約を当該従業員と交わす。
		外部保存を受託する事業者における診療情報へのアクセス禁止	A	・アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間である	・委託する機関によるアクセスログの監査	・監査者は、XX における保管された「診療記録」及びアクセスログへのアクセス記録を監査する。
		外部保存を受託する事業者における障害対策時のアクセス通知	A	・アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間である	・アクセス許可、秘密保持に関する契約と委託する機関によるアクセスログの監査	・【契約事項として】XX においては正当な理由なく、保管した「診療記録」及びアクセスログにアクセスしてはならない。できる限り事前に当院の許可を得ることとし、やむを得ない事情により許可を得ずアクセスした場合は、遅滞無く当院に報告するものとする。また、目的外に利用してはならないし、正当で明確な目的がないのに他の媒体等に保管してはならない。

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
		外部保存を受託する事業者におけるアクセスログの完全性とアクセス禁止	A	・アクセスログファイルへのアクセス制御とアクセスログ機能、監査目的に耐えるログ保存期間である	・委託する機関によるアクセスログへのアクセスの監査	
⑧	患者への説明	外部保存を行っている旨を院内掲示等を通じて周知すること	A		・外部保存を行っている旨を院内掲示等を通じて周知する	・運用責任者は、外部保存していることの患者への周知（例、掲示内容）が計られていることを適宜確認する。
						付録 1．管理体制・受託する機関との責任分担規程 2．XX に保管を委託する「診療記録」の定義 3．XX への監査事項 4．XX との契約

付録　（参考）外部機関と医療情報等を連携する場合に取り決めるべき内容

外部の機関と医療情報共有の連携等を行う場合に、連携する機関の間で取り決めるべき内容の参考として以下に記載する。

1. 組織的規約
   理念、目的
   管理と運営者の一覧、各役割と責任
   遵守すべき法令・ガイドライン等の確認
   医療機関等と情報処理事業者・クラウドサービス事業者・電気通信事業者等との責任分界点
   セキュリティ事故・大規模災害等が発生した際の報告体制・内容
   免責事項、知的財産権に関する規程
   参加機関間の規約（参加機関の資格タイプ、参加機関の状況を管理する規約)、費用負担等に係る取決め等　等

2. 運用規則
   管理組織構成、日常的運営レベルでの管理方法
   システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知等)、データ維持、保存、バックアップ、不具合の回復等

3. プライバシー管理
   患者共通ID（もし、あるならば）の管理方法
   患者情報等のアクセスと利用の一般則
   利用者とアクセス権限のある医療情報別の対応規約
   患者同意のルール
   非常時のガイド（ブレークグラス（非常時のID等の運用)、システム停止時、等の条件）　等

4. システム構造
   全体構造、システム機能を構成する要素、制約事項、採用する標準等
   連携組織外部との接続性（連携外部の組織とデータ交換方法）　等

5. 技術的セキュリティ
   リスク分析
   認証、利用者管理、利用者識別（パスワード規約、二要素認証等の識別方法）

可搬媒体のセキュリティ要件　等

6. 構成管理
ネットワーク構成、ハードウェアやソフトウェアの機能更新・構成変更等の管理方法、新機能要素の追加承認方法　等

7. 監査
監査者、監査頻度、監査結果を踏まえた対応

8. 規約の更新周期

医療情報システムを安全に管理するために（第2.2版）

「医療情報システムの安全管理に関するガイドライン」
全ての医療機関等の管理者向け読本

厚生労働省
令和４年３月

改定履歴

版数	日付	内容
第1版	平成21年3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4版を医療機関等の管理者向けポイント集としてとりまとめた。
第2版	平成29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5版の公表に合わせて、本書第1版以降における同ガイドラインの改定内容を反映させた。 また、分かりやすさの観点から全般的な表現、レイアウト等の修正を行った。
第2.1版	令和３年１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5.1版の公表に合わせて、二要素認証に関する対応方針等について反映させた。 また、分かりやすさの観点から表現、レイアウト等の修正を行った。
第2.2版	令和４年3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5.2版の公表に合わせて、脅威に応じたバックアップの取得の必要性について反映させた。 また、分かりやすさの観点から表現等の修正を行った。

目次

1　本書の位置付けと活用方法

本書の想定読者とその目的

本書は、医療情報システムの導入を検討若しくは決定する立場にある管理者、又は医療情報システムを既に導入し運用している管理者、医療機関等にあっては院長や理事長を主たる読者と想定している。

これらの管理者の方々が、本書を一読し、実際にシステムの導入や運用に携わる情報技術管理者やシステムベンダ等に指示等を出す際の手引きとなることを目的とする。

1.1　本書の位置付け

本書は、厚生労働省が策定した「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）を医療機関等の管理者に理解してもらうために、そのポイントを要約したものである。

本書の各項目の　　に、ガイドラインの参照している箇所を示しているので、ガイドラインの規定の詳細は、該当箇所を確認されたい。

本書でいう「医療情報システム」は、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。

また、ガイドラインの対象には、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の電子的な医療情報の取扱いに係る責任者が含まれる。

ガイドラインは、①法令等により求められる要件を満たすための実行指針、②医療に関わる情報を医療機関等の資産（以下「情報資産」という。）と捉え、これを継続的に保護していくためのプロセスに関する手引書という２つの性格を有する。

したがって、ガイドラインでは、遵守すべき法令等や情報資産を保護するための方策等について詳細な解説を加える必要があり、情報技術の利活用に関する留意点等を記載するに当たって内容や分量が多くなることが避けられない。

そのため、本書は、ガイドラインの趣旨をできるだけ平易に解説し、医療機関等の管理者にそれを理解してもらうことを期待して作成した。

1.2　本書の活用方法

本書は読みやすさに配慮した上で、ガイドラインで求められている医療情報システムを利用した電子的な医療情報の取扱い要件等について、ポイントを絞って解説する。

第2章　電子的な医療情報を扱う際の責任の在り方

医療機関等において電子的な医療情報を扱う際の医療機関等の管理者の責任について解説している。ガイドラインに違反した場合に訴求される管理者の責任に対する考え方も含まれる。

第3章　電子的な医療情報を扱う際の考え方

電子的な医療情報を扱う際に求められる継続的な情報資産の保護と法令等の遵守について解説している。

- 医療情報システムの機能向上と運用の見直しに関する視点から
  継続的に情報資産を保護するため必要な取組み等について解説している。

- 個人情報保護の視点から
  個人情報の保護に関する法律（平成15年5月30日法律第57号。以下「個人情報保護法」という。）で求められる安全管理措置に関連して、医療情報システムの安全管理に求められる基準について解説している。なお、医療・介護分野における個人情報の取扱いに係る具体的な留意点や事例等が「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」（以下「ガイダンス」という。）で示されているため、ガイドラインと併せて参照されたい。

- e-文書法の視点から
  主に「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号。以下「e-文書法」という。）、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成17年3月25日厚生労働省令第44号。以下「e-文書法省令」という。）及び「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。以下「外部保存通知」という。）で求められる文書の「真正性」、「見読性」、「保存性」について解説している。

第4章　電子的な医療情報を交換若しくは提供する際の考え方

医療機関等において、外部とネットワークを通じて医療情報を交換する場合の考え方について解説している。

2　電子的な医療情報を扱う際の責任の在り方

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、情報の取扱いも同様である。情報の取扱いについては、情報を適切に収集した上で、必要に応じて遅滞なく利用できるよう適切に保管し、不要になった場合には適切に廃棄する必要がある。このことにより、刑法等に定められている守秘義務、個人情報保護の関連法令等のほか、診療情報の取扱いに関わる法令、通知、指針等の要件を満たすことが求められる。

故意にこれらの要件に反する行為を行えば、刑法上の秘密漏示罪で処罰される。同時に、診療情報等については、過失による漏えいや目的外利用も大きな問題となる可能性があるため、そのような事態が生じないよう適切な管理（このような善良なる管理者の注意義務を「善管注意義務」という。）を行う必要がある。

ガイドラインは、この善管注意義務をできるだけ具体的に示しており、そこで述べられている管理者の情報保護責任を俯瞰すると、下記のように分類できる。

＜ガイドラインで述べられている管理者の情報保護責任＞

自組織内で管理する場合	通常運用時	①管理方法・体制等に関する説明責任
		②管理を実施する責任
		③定期的に見直して改善する責任
	事故発生時	①事故の原因・対策等に関する説明責任
		②善後策を講じる責任
第三者に委託する場合		受託する事業者の過失に対する責任
第三者に提供する場合		第三者提供が適切に実施されたかに対する責任

2.1　医療機関等の管理者の情報保護責任

医療機関等の管理者の情報保護責任は次の２つのケースに分けて考える必要がある。

（1）通常運用における責任

医療情報保護のための体制を構築し、管理する局面での責任を指す。「説明責任」、「管理責任」、「定期的に見直し必要に応じて改善を行う責任」に分けられる。

（2）事後責任

医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に適切な対応を取る責任を指す。「説明責任」、「善後策を講じる責任」に分けられ

る。

（1）通常運用における責任

① 説明責任

通常運用における説明責任とは、システムの機能や運用計画がガイドラインを満たしていることを、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、システムの仕様や運用計画を文書化しておき、通常運用時の仕様や計画が当初の方針に則って機能しているか、定期的に監査を行い、その結果も文書化することが求められる。監査の結果に問題があった場合は、真摯に対応した上で、対応の記録を文書化して第三者が検証可能な状況にすることが必要である。また、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設置することも必要となる。

② 管理責任

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。

システムの管理を請負事業者に任せきりにしている状況では、これを果たしたことにならない。管理に関する最終的な責任の所在を明確にするため、少なくとも管理状況の報告を定期的に受け、監督を実施する必要がある。

個人情報保護法では、個人情報保護の担当責任者を定める必要があるため、適切な担当責任者を決めて請負事業者の対応に当たる必要がある。

③ 定期的に見直し必要に応じて改善を行う責任

定期的に見直し必要に応じて改善を行う責任とは、医療情報システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任である。

情報保護に関する技術は日進月歩であり、旧態依然の情報保護体制ではすぐに時代遅れになってしまう。一方、管理者がこのような最新の技術動向を都度把握することは、管理者としての本来業務と異なることがある。したがって、管理者は、運用管理の状況を監査・確認する際、技術の進展を意識しつつ、例えば医療情報システムの技術担当者やシステムベンダに現在の動向を調査させる等して、必要な改善を実践していくことが重要になる。

（2）事後責任

① 説明責任

事後の説明責任とは、医療情報について何らかの事故（典型的には漏えい）が生じた場合に、事態の発生を公表し、その原因と対処法を説明する責任である。

個々の患者へ事故の内容並びにその原因と対策について説明することはもちろん、監督

官庁への報告や社会への公表が求められる。

② 善後策を講ずる責任

善後策を講ずる責任とは、「原因を追及し明らかにする責任」、「損害を生じさせた場合にはその損害填補責任」、「再発防止策を講ずる責任」である。

何らかの不都合な事態が生じた場合、医療機関等の管理者は善後策を講じる必要がある。

医療情報について事故が発生した場合、その事故が適切な契約に基づき医療情報の処理を委託した事業者の責任によるものであり、かつ選任監督における注意を払っていたとしても、患者に対する関係では、上記3つの善後策を講ずる責任を免れるものではない。

2.2 責任分界点について

ネットワーク及びその技術の進展から、電子化された医療情報が、医療機関等の空間的境界を越えてネットワーク上に広がって存在するようになってきた。

このような状況の下、医療情報の管理責任は、医療機関等のみならず、ネットワークを介したサービスを提供する事業者やネットワークを提供する通信事業者、伝送先の医療機関等にもまたがるようになる。その際、責任範囲の切り分けが必要となり、ガイドラインではこれを責任分界点として説明している。

医療情報を外部の医療機関等や情報処理関連事業者に伝送する場合について、個人情報保護法では、（1）委託（第三者委託）と（2）第三者提供の2つの形態が規定されている。両者では、医療機関等の管理者の責任のあり方に大きな違いがあるため、解説する。

（1）委託（第三者委託）の場合

委託（第三者委託）とは、医療機関等の管理者の業務遂行を目的として医療情報の取扱いを委託するものであり、医療情報は管理者の支配下にある。

患者に対する関係では、受託する事業者の過失による事故についても医療機関等の管理者が責任を免れるものではない。一方、委託先との間で締結する委託契約書には、双方の責任を明記し、その責任の所在を明確にしておく必要がある。

（2）第三者提供の場合

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あり、提供された情報については、第三者に適切に保護する責任が生ずる。

提供元の医療機関等の管理者にとっては、原則として適切な第三者提供がなされる限り、その後の情報保護に関する責任は医療機関等の管理者から離れる。

ただし、電子化された情報は、情報を第三者に提供しても、医療機関等の側で当該情報を削除しない限り、なお医療機関等の下に存在するため、それに関し適切な情報管理責任が残ることはいうまでもない。

さらに、レセプトの代行請求や特定健診結果の代行送信のように、情報処理関連事業者を介して情報提供が行われる場合には、どの時点で第三者に提供されたことになるかを明らかにすることが求められる。そのため、それらの事実をできる限り記録・管理して、実際に事故が起きた場合には、患者等からの記録の開示要求に応じる必要がある。

3　電子的な医療情報を扱う際の考え方

本章では、情報資産を保護していくため継続的に取り組むべき枠組み、及びガイドラインで参照されている法令等に対して、医療情報システムに求められる要件を解説する。

3.1　情報資産を保護していくための手引き

医療情報システムを導入する時又は導入した後に、継続的にシステムを活用し、システムに蓄積された情報を資産として保護していくための考え方を解説する。一般的に、情報システムやそこに蓄積された情報を保護していく手段や手続き等については、国際的に確立されたシステム構築方法や、それに基づく文書等が存在する。

中心となる概念は、「①計画を立てる（Plan）」、「②それを実行する（Do）」、「③必要に応じて見直しを行う（Check）」、「④改善する（Action）」という一連の取組みによって構成される、いわゆる「PDCAサイクル」である。これは、これらの手順を継続して繰り返すことで、情報保護のレベルを向上させていくものである。

医療機関等における情報資産保護において、この概念は決して新しいものではない。特に、医療安全に関してこの概念が顕著に示されており、「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、医療の安全に関する事項として、この概念が規定されている。

＜医療の安全を確保するための措置について（第0330010号通知より要約）＞

（1）医療に係る安全管理のための指針の作成

- 「安全管理に関する基本的考え方」、「委員会その他医療機関内の組織」、「従業者研修の基本方針」、「事故報告等、安全確保のための基本方針」、「患者からの相談対応に関する基本方針」等を盛り込んだ指針の作成。

（2）委員会の設置（ただし、無床診療所は適用除外となっている）

- 管理及び運営に関する規程の制定。
- 重要な検討内容の患者への対応状況を含めた管理者への報告。
- 重大問題発生時の原因分析・改善案の立案及び実施並びに従業者への周知。
- 改善策の実施状況の調査、見直し、等。

（3）医療に係る安全管理のための職員研修の開催

- 医療安全の基本的な考え方や具体的方策について、病院等の従事者に周知徹底を行うことで、安全に業務を遂行するための意識の向上を図るものとす

る。

（4）医療に係る安全の確保を目的とした改善のための方策

- 安全管理委員会（無床診療所においては管理者）への報告。
- 事例の収集、分析。これにより問題点を把握し改善策の企画立案及びその実施状況の評価並びに医療機関内での情報の共有。
- 改善策については、再発防止策等を含んだものであること。

つまり、医療機関等では、医療安全管理の事例にあるように、「①計画を立てる（Plan）」、委員会や職員研修を実施しながら「②それを実行する（Do）」、改善のための方策を講じるために「③必要に応じて見直しを行う（Check）」、必要に応じて「④改善する（Action）」というプロセスが既に存在している。

したがって、医療情報システムやそこに蓄積された情報を継続的に保護し、利活用していくプロセスを特殊な概念と捉えず、通常業務の枠組みの一環として検討し、確実に実行していくことが重要である。

ただし、医療情報システムの場合、現在利用しているシステムが、翌年には何らかのセキュリティ上の問題を抱えた状態になっていることも想定される。したがって、「2.1（１）通常運用における責任」でも述べたように、見直しや改善の際には情報技術の進展に留意する必要がある。その際、ガイドラインを参考にすることはたいへん有益な手段であり、積極的に活用されたい。

新たに電子カルテ等の医療情報システムを導入する際、出発点として「①計画を立てる（Plan）」ことは必須である。「①計画を立てる」際、医療機関等の管理者・責任者は、保護すべき情報をリストアップした上で、それを重要度に応じて分類し、医療機関等の業務や組織形態、人事体系等と整合性を取らなければならない。情報のリストアップやリスク分析及び対策に当たって、システムベンダからの情報収集が重要となるため、保健医療福祉情報システム工業会（JAHIS）及び日本画像医療システム工業会（JIRA）が公表しているセキュリティ情報の開示資料等が参考になる。

既に医療情報システムを導入している医療機関等においても、「③必要に応じて見直しを行う（Check）」、「④改善する（Action）」ことは不可欠である。

医療機関等の管理者・責任者は自らの資産管理を主体的に行う必要があるため、医療情報を資産と捉えることで、このことを素直な感覚で受け止めてもらえるだろう。

3.2　医療情報システムの安全管理に求められる基準

個人情報保護法第23条は、安全管理措置に関する定めである。一般に、安全管理措置とは、具体的に「組織的安全管理対策」、「物理的安全対策」、「技術的安全対策」、「人

的安全対策」により構成される。本章では、これらについて解説する。

（１）組織的安全管理対策（体制、運用管理規程）

組織的安全管理対策とは、安全管理について従業者の責任と権限を明確に定めて、安全管理に対する規程や手順書を整備・運用し、その実施状況を確認することをいう。

従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備・運用し、その実施状況を日常の自己点検等によって確認することが必要である。

これらのことを実践し、運用管理規程を定めておくことは、管理責任や説明責任を果たす上でも極めて重要である。

医療機関等の管理者は上記を踏まえて、医療情報システムを運営しなければならない。

組織的安全管理対策の詳細について⇒ガイドライン 6.3 章が参考になる。

また、医療機関等は、災害やサイバー攻撃等の非常時に備え、事業継続計画（BCP：Business Continuity Plan）を作成し、平常時から、システム停止時の代替手段及び所管官庁・関係機関への連絡手段を用意する必要がある。

昨今、医療機関等における情報の連携が進んでいることから、医療機関等がサイバー攻撃を受けるリスクは増大しつつあるといえる。標的型メール攻撃※、ランサムウェア※２等、サイバー攻撃の手法は一層高度化、多様化しており、後述の技術的安全対策を講じるだけでは被害の発生を防止できないおそれもある。万一サイバー攻撃を受けた場合には、速やかに関係官庁や相談窓口に報告し、対応について相談する必要がある。

※標的型メール攻撃とは、特定の従業者あてに業務に関連する内容を装ったメールを送付し、従業者が誤って不正ソフトウェアが混入している添付ファイルを実行等するように誘導を行う手法等をいう。

※２　ランサムウェアとは、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。

（２）物理的安全対策

物理的安全対策とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

情報の種別・重要性・利用形態、組織の規模に応じて、セキュリティ上保護すべき幾つかの区画を定義し、端末・コンピュータ・情報媒体（CD-RやUSBメモリ等）を物理的に適切な方法で管理する必要がある。

留意するポイントとして、入退館（室）の管理、機器等の盗難の防止、紛失防止等があり、それらを十分に考慮されたい。

物理的安全対策の詳細について⇒ガイドライン 6.4 章が参考になる。

（３）技術的安全対策

技術的安全対策とは、個人データ及びそれを取り扱う医療情報システムへのアクセス制御、不正ソフトウェア対策、医療情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

医療情報システムへの脅威に対する主な技術的対策として、下記の項目が挙げられる。

- 情報区分と利用者の対応付けに基づくアクセス権限の設定
- 運用時における利用者の識別と認証、アクセスの記録（アクセスログの取得）
- 不正ソフトウェアの混入やネットワークからの不正アクセス防止

これらの対策は、それぞれに対して有効範囲を適切に認識して実施すれば、強力な手段となり得る。ただし、技術的な対策のみで全ての脅威に対抗することはできないため、運用管理による対策の併用は必須である。

上記の利用者の識別と認証に当たって、これまでID・パスワードの組み合わせを入力する方式が広く用いられてきた。しかし、このように利用者の「記憶」によるものに頼る方式は、運用状況によりセキュリティ上のリスクを高めることになる。

したがって、①ID・パスワードを入力する方式、②指紋や静脈、虹彩のような利用者の生体的特徴を利用する方式、③ICカードのような物理媒体を用いる方式を組み合わせ、２つの独立した要素を用いて行う方式（二要素認証）を採用することが推奨される。なお、安全管理ガイドライン5.2版では、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、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とされている。

また、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る。ウェアラブル端末や在宅設置の医療機器等の「IoT 機器」※により、医療に関する個人の情報を取得し、ネットワークを介して収集する仕組みを利用する場合には、ガイドラインに則った適切な対策を講じる必要がある。

※IoT 機器とは、センサ等で自動的に情報を取得し、若しくは他の機器が自動的に取得した情報を中継し、ネットワークを通じて他の医療情報システムに送信する機器をいう。

技術的安全対策の詳細について⇒ガイドライン 6.5 章が参考になる。

（４）人的安全対策

人的安全対策とは、従業者等との間において、業務上秘密と指定された個人データの非開示契約を締結し、情報保護に関する教育・訓練等を行うことをいう。

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対策を講じる必要がある。

医療の現場では様々な資格者と職種が混在しており、医療情報システムの関係者はさらに多岐にわたる。法令上の守秘義務を負う者、雇用契約の下で守秘義務を負う者、保守契約に基づいてシステムを保守する者等が例に挙げられる。

したがって、これらの関係者を適切に管理するため、守秘義務と違反時の罰則に関する規程の策定、情報保護に関する教育や訓練を実施する必要がある。

また、近年は標的型メールや偽装したWebサイト等を利用した巧妙なサイバー攻撃が増加しているため、従業者にはこれらのリスクや対策について日頃から啓発・教育することが求められる。

情報の生成から破棄に至る「ライフサイクル」全体にわたって安全管理措置を講ずることが求められており、情報の破棄についても上記措置に含めることが必要である。

人的安全対策の詳細について⇒ガイドライン 6.6 章が参考になる。

3.3　電子保存する場合に求められる基準

従来は紙媒体による管理が義務付けられていた診療録等が、「診療録等の電子媒体による保存について」（平成11年4月22日付け健政発第517号・医薬発第587号・保発第82号厚生省健康政策局長・医薬安全局長・保険局長連名通知）によって規制緩和され、「電子保存」が認められた。この通知では、前述した医療情報システムの安全管理に加え、診療に供する情報を扱う医療固有の要求事項が示されている。これが「電子保存の三原則」と呼ばれるものであり、「真正性」、「見読性」、「保存性」で構成される。

ここでは、e-文書法省令及び外部保存通知に則り、ガイドラインの7章から9章で詳細に規定されている、いわゆる「電子保存の三原則」（真正性、見読性、保存性）について解説する。

電子処方箋の取扱いについては、「電子処方箋の運用ガイドライン」が公表されているため、参照されたい。

また、外国にある事業者に診療録等の8章で規定されている文書等の取扱いを委託する場合、ガイダンスとともに、「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）の内容を確認する必要があるため、参照されたい。

（1）真正性の確保について

真正性とは、正当な人が記録・確認を行った情報について、第三者にとって作成の責任の所在が明確であり、かつ、故意又は過失による虚偽入力・書換え・消去・混同※が防

止されていることである。

※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付けを誤ることをいう。

発生する各種のデータに対して、「作成の責任の所在及び記録の確定方法の明確化」が必要である。その上で、技術的対策、運用的対策等を組み合わせて、責任の所在を明確化し、情報の完全性を確保する（虚偽入力、書換え、消去及び混同の防止）必要がある。

記名・押印が必要な文書については、電子署名、タイムスタンプを付すことが必要である。特に、保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、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ことが推奨される。

一方、ネットワークを通じて外部に保存を行う場合、第三者が医療機関等になりすまして、不正な診療録等を診療録等の外部保存を受託する事業者へ転送することは、診療録等の改ざんとなるため、対策が求められる。また、ネットワークの転送途中で診療録等が改ざんされないようにも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、非対面での情報転送であることや通信経路上でのハッキングの危険性等、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。

上記リスクについて⇒ガイドライン４章が参考になる。

（2）見読性の確保について

見読性とは、電子媒体に保存された内容を、要求に基づき、必要に応じて肉眼で読み取れる状態にすることができることである。見読性とは、本来「診療に用いるため支障がないこと」と「監査等に差し支えないこと」を指し、この両方を満たすことがガイドラインで求められる実質的な見読性の確保である。

「必要に応じて」とは、診療、患者への説明、監査、訴訟等に際して、それぞれの目的に支障のない応答時間やスループット、操作方法により読み取れる状態にできることである。

また、情報の所在管理と見読化手段の管理も必要であり、患者ごとの全ての情報の所在が日常的に把握されていなければならない。このことは外部保存の場合も同様である。電子媒体に保存された情報はそのままでは見読できず、電子媒体から情報を取り出すに当たって何らかの処理を行う必要があるため、これらの見読化手段が日常的に正常に動作することが求められる。

必要な情報を必要なタイミングで情報の利用者に提供できない、又は記録時と異なる内容が表示されると、医療の提供に重大な支障となる。よって、バックアップや冗長性の確保、システム全般の保護対策を通じて、診療に重大な支障を及ぼすことのない最低限の見読性を確保することが求められる。またバックアップの取得方法や保管方法については、システム障害への対応や、災害への対応、サイバー攻撃等による被害への対応など、脅威

に応じた検討を行う必要がある。

さらに、システムを更新する場合も同様であり、新旧のシステム間で記録内容が異なることがないようにしなくてはならない。

（3）保存性の確保について

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、見読性が確保された状態で保存されることをいう。

診療録等の情報を電子的に保存する場合、保存性を脅かす原因に下記が挙げられる。

- 機器やソフトウェアの障害等により、データ保存自体がなされていない可能性
- 記録媒体、設備の劣化による不完全な読み取り
- コンピュータウイルスや不正なソフトウェアによる場合を含む、設備・記録媒体の不適切な管理による情報の喪失
- システム更新時の不完全なデータ移行

これらの脅威をなくすために、それぞれの原因に対して、技術面及び運用面での対策を講じる必要がある。外部保存を行っている場合には、保存施設においてこれらの対策が行われていることを確認することが必要である。

また、例えば保険請求に用いる診療行為や医薬品等のマスタ変更や、医療機関等の組織変更によるシステム保守等の際に、過去の記録が記録時と異なる内容で表示されることがないようにすることも、保存性確保の範囲である。

4　電子的に医療情報を交換若しくは提供する際の考え方

ここでは、ネットワークを通じて組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべきことを述べる。これには、双方向だけでなく一方向の伝送も含まれる。

外部と診療情報等を交換するケースとしては、下記のこと等が想定される。

- 地域医療連携で医療機関等や検査会社等がネットワークで診療情報等をやり取りする
- 診療報酬の請求のために審査支払機関等にネットワークで接続する
- 事業者の提供するソフトウェアをネットワーク越しにクラウドサービスにより利用する
- 医療機関等の従事者が業務上の必要に応じて、ノートPC、スマートフォン、タブレットのようなモバイル端末を用いて医療機関等の医療情報システムに接続する
- 患者等がネットワークを介して自らの診療情報を閲覧する

ネットワークを利用して外部と医療情報を交換する場合、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、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。

本章では、医療機関等の視点から、ネットワークのセキュリティを確保するために求められる対策について解説する。

なお、他の医療機関等と医療情報をやり取りする場合、情報の相互運用性を確保する観点から、広く用いられている標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）を活用することが望まれる。

モバイル端末の取扱いについて⇒ガイドライン 6.9 章が参考になる。

標準規格について⇒ガイドライン 5 章が参考になる。

4.1　医療機関等における留意事項

ここでは、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の、医療機関等における留意事項を整理する。

まず、医療機関等は、情報を伝送するまでの医療情報の管理責任は送信元の医療機関等にあることを強く意識しなければならない。これは、情報が送信元である医療機関等から、通信事業者の提供するネットワークを介して、適切に送信先の医療機関等に受け渡しされるまでの、一連の流れ全般において適用される。

医療機関等が情報を送信する場合には、情報を適切に保護する責任を全うするため、次の点に留意されたい。

（1）盗聴の危険性への対応

盗聴とは、ネットワークに特有の事象ではなく、広く第三者が意図的に会話の内容・情報を盗み聞くことである。ネットワークでは、一般的に何らかの手段で伝送中の情報（電気信号）を盗み取ることを指す。

ネットワークを通じて情報を伝送する場合、盗聴に最も注意しなくてはならない。

また、第三者が意図的に情報を盗み取る場合だけでなく、伝送途中で意図しない情報漏えいや誤送信等が発生した場合に備え、適切な処置を取る必要がある。その一つの方法に医療情報の暗号化がある。

どの程度の暗号化を、どのタイミングで施すかについては、伝送しようとする情報の機密性の高さや、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り異なる。よって、一概に規定することは困難であるが、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必須である。

盗聴防止については、リモートログインによる保守を実施する時も同様である。その場合、医療機関等は保守事業者等に対処方法を確認し、監督する責任を負う。

（2）改ざんの危険性への対応

改ざんとは、情報を不正に書き換えることである。例えば、ホームページを不正に書き換えたり、伝送途中の情報を書き換えたりする行為が挙げられる。

ネットワークを通じて情報を伝送する場合、正当な内容を送信先に伝えることも重要な要素である。情報を暗号化して伝送すれば改ざんの危険性は軽減されるが、適切な対策を講じなければ、なお通信経路上の障害等により（意図的・非意図的要因に関わらず）データが改変されてしまう可能性があることを認識する必要がある。

また、ネットワークの構成によっては、情報を暗号化せずに伝送することが想定されるため、その場合改ざんへの対応を必ず実施しなければならない。改ざんを検知する方法として、電子署名を用いること等が考えられる。

（3）なりすましの危険性への対応

なりすましとは、本人ではない第三者が、本人のふりをしてネットワーク上で活動することである。例えば、情報を受け取る人のふりをして不正に情報を取得する行為や、他人のID・パスワード等を盗み出して、本人しか確認することのできない情報を閲覧する行為が挙げられる。

ネットワークを通じて情報を送ろうとする医療機関等は、ネットワークは非対面による情報伝達手段であることを十分に認識し、送信先の医療機関等が確かに意図した相手であ

るかを確認しなくてはならない。

逆に、情報の受け手となる送信先の医療機関等は、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、送られてきた情報が送信元の医療機関等の情報であるかを確認しなくてはならない。

確認の手段には様々な方法があり、それらを適切に活用若しくは組み合わせて、なりすましの危険性に対応する必要がある。

4.2　選択すべきネットワークのセキュリティの考え方

「4.1　医療機関等における留意事項」では、主に情報の内容に対する脅威への対応方法について解説したが、ここでは情報を伝達する通信経路への脅威に対応する方法について解説する。

一言でネットワークといっても、その構成には様々なものがあるため、全てを網羅することは難しい。そこで、ガイドラインでは大きく「クローズドなネットワークで接続する場合」と「オープンなネットワークで接続されている場合」とに分けており、本書もその体系に沿って解説する。

（1）クローズドなネットワークで接続する場合

クローズドなネットワークとは、インターネットに接続されていないネットワーク網で、専用線、ISDN、閉域IP通信網のことを指す。

クローズドなネットワークは、後述のオープンなネットワークに比して安全性が高い。

ただし、複数の通信事業者のネットワークを介して接続する場合には、ネットワーク間の接続の過程で情報に何らかの処理を行うことがあり、このとき、偶発的に情報の内容が漏示してしまう可能性もある。

よって、クローズドなネットワークを利用する場合でも、「4.1 医療機関等における留意事項」を参考に、送り届ける情報の内容が判読できないよう暗号化を施し、かつ改ざんを検知できる仕組みを導入する等、適切な措置を講じる必要がある。

また、ウイルス対策ソフトの更新やOSのセキュリティパッチ等を適切な時期・方法によって適用し、システムの安全性の確保にも配慮する必要がある。

（2）オープンなネットワークで接続されている場合

オープンなネットワークとは、いわゆるインターネットによる接続である。インターネットを活用して広範な地域医療連携の仕組みを構築する等、その利用範囲が拡大していくことが考えられる。

オープンなネットワークを利用する場合、その通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在し、先述のクローズドなネットワークに比し

てセキュリティ上のリスクは大きい。よって、十分なセキュリティ対策を実施することは必須であり、かつ「4.1 医療機関等における留意事項」に従い医療情報を暗号化しなければならない。

オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者が、これらの脅威に対するネットワーク経路上のセキュリティを担保して、サービス提供することがある。

医療機関等がこのようなサービスを利用する場合、契約等で管理責任の分界点を明確にした上で、通信経路上の管理責任の大部分をこれらの事業者に委ねることができる。

一方、医療機関等が独自にオープンなネットワークを用いて外部と医療情報を交換する場合、管理責任のほとんどは医療機関等に委ねられることを考慮して、導入を判断する必要がある。また、技術的な安全性についても、自らの責任で担保しなければならない。

オープンなネットワーク接続を利用する場合、用いるセキュリティ技術やサービスの内容・特徴に応じて内在するリスクが異なる。

利用する医療機関等にあっては、導入時に十分な検討を行い、リスクの受容範囲を見定めることが求められる。

また、ネットワーク導入時に業者等に委託する際は、事前にリスクの説明を求め、理解しておくことが必要となる。

5 おわりに

この管理者向け読本では、管理者の立場にある方々に向けて、「責任」という観点からガイドラインを解説した。

ガイドラインでは、安全なシステムの構築・運用に寄与するより多くの事項が規定されている。本書が管理者の方々にもガイドライン本文に手を延ばす契機になれば幸いである。

医療情報システムの安全管理に関するガイドライン　別冊用語集

用語		説明
あ	アクセスポイント	通常は、無線 LAN アクセスポイントを指す。ノートパソコンやスマートフォン等の無線 LAN 接続機能を備えた端末を、相互に接続したり、有線 LAN 等、他のネットワークに接続するための機器。
	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。
	アプリケーションゲートウェイ	院内 LAN（企業内 LAN）から直接外部ネットワーク（インターネット）にアクセスさせず、アプリケーションが代行して接続（通信制御）する関所のようなもの。このアプリケーションは通信されるデータやコマンドに不正がないかチェックしながら接続代行するため安全にネットワークアクセスが可能となる。
	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（暗号化と複号とで別々の鍵を使用する方式）の二つに大別される。
	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。
	暗号鍵	暗号化（又は復号）する時に必要な鍵（情報）のこと。
	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。
	インデックスデータベース	テーブル（データが記録された表）に格納されているデータを高速に取り出せるよう加工したデータベース。
	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。
	オフライン攻撃	パスワードを発見するために、事前に取得した当該システムの暗号化されたパスワードファイルを基に、オフラインでなされる攻撃。辞書に登録しておいた文字列をパスワードシステムと同じ暗号化を行い、その結果と照合し一致するものを探すことにより元のパスワードを知ることができる。
	オンライン外部保存	医療情報を医療機関等外の事業者等の環境に、ネットワークを通じて保存を行うこと。
	オンラインサービス	ネットワークを介して提供されるサービスの総称。
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」を使うことが多く使われる。 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。

用語		説明
	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。
	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に若しくは常時監視する機器やシステム。
	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。
	基本４情報	氏名、生年月日、性別、住所を指す。
	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。
	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。
	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。
	クラウドサービス	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。
	クラッカー	コンピュータネットワークに不正に侵入したり、破壊・改竄などの悪意を持った行為を行う者。
	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。
	検索エンジン	インターネット上に存在する Web ページや画像ファイルなどの情報を探すための仕組み。
	堅牢性	ハードウェアやシステム等が頑丈で、壊れにくいこと。
	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。
	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。
	コンピュータウィルス	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

用語		説明
		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。
	サービス不能（DoS）攻撃	Denial of Service攻撃の略。サービス拒否攻撃のこと。攻撃者は、Webサーバやメールサーバ等に対して大量のサービス要求のパケットを送りつけ、過大な負荷をかけて相手のサーバやネットワークを使用不能にする。
	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。
	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。
	重要インフラ分野	情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、及び石油。重要インフラの情報セキュリティ対策に係る第4次行動計画において記載。
	証跡管理	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が生じた際に、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。
	冗長化	アイテム中に要求機能を遂行するための二つ以上の手段が存在し、手段の一部が故障しても故障とならない性質を冗長性という。冗長化は、システムの構成要素や機能の実現手段を複数用意した冗長性によって、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をいう。
	情報処理関連事業者	情報処理（電子計算機（計数型のものに限る。）を使用して、情報につき計算、検索その他これらに類する処理を行うこと）を業とする事業者。
	情報セキュリティポリシー	情報セキュリティに関する組織的取組についての基本的な方針及び情報セキュリティ対策における具体的な実施基準や手順等の総称。
	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。
	シンクライアント	団体・組織の情報システムで、従業者等が利用するコンピュータ（クライアント）に最低限の機能だけを持たせて、サーバ側でアプリケーションソフトやファイル等の管理を可能にするシステムの総称。また、そのようなシステムを実現するための、機能を絞ったクライアント用コンピュータのことをいう。

用語		説明
	シングルサインオン	ユーザーが一度認証を受けるだけで、許可されているすべての機能を利用できるようになるシステム。
	スキャン（ウィルススキャン）	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、ウィルススキャンを実行する必要がある。
	スタンドアロン	ネットワークに接続されていない状態のこと。
	ステートフルインスペクション	通信内容を検査して、動的にポートの閉鎖・開放を制御すること。
	ステルスモード	無線 LAN のアクセスポイントで、SSID を外部に見えなくする機能のこと。 アクセスポイントの存在を隠すことができるため、無線 LAN を利用する場合の情報セキュリティ対策の一つとして利用できる。 なお、メーカーによっては、SSID 隠蔽機能等の呼び名になっていることもある。
	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。
	スループット	一定時間内に処理できるデータ量のこと。CPU の処理性能の指標となる。
	脆弱性	情報セキュリティ分野において、通常、脆弱性とは、システム、ネットワーク、アプリケーション、又は関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在、設計若しくは実装のエラーのことをいう。オペレーティングシステムの脆弱性である場合もあれば、アプリケーションシステムの脆弱性である可能性もある。 また 、ソフトウェアの脆弱性以外に、セキュリティ上の設定が不備な状態においても、脆弱性があるといわれることがあるセキュリティ・ホール（security hole）と呼ばれることもある。
	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た制度。
	責任分界点	情報システムに係る関係者間の責任の移行点。
	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。
	セキュリティターゲット	情報処理製品や情報処理システムの、セキュリティ対策方針・セキュリティ機能等を記載した文書。情報処理製品や情報処理システムの開発や改善に際して利用されるものであり、評価対象を評価する際に必要なドキュメントでもある。

用語		説明
	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。
	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。
	セキュリティ・ホール	脆弱性の項を参照されたい。
	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。
	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。
	選任監督義務	情報処理を第三者に委託する場合に、適切な者に委託し、かつ当該第三者に対して必要かつ適切な監督を行う義務。
た	ダイアルアップ接続	電話回線や ISDN 回線等を通じてインターネットや社内 LAN に接続するサービス又はその方式のこと。
	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。
	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。
	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。
	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。
	データセット	コンピュータで処理が行われるデータのまとまり。通常は、属性によって分類され、若しくは何らかの目的で収集されたデータが記録されたファイル群を指すもの。
	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。
	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。
	デジタル署名	数学的なコンピュータ プログラムによって生成される。手書きの署名ではなく、それをコンピュータに取り込んだものでもない。公開鍵暗号技術を利用して、電子メール メッセージ、又はファイルに添付される。メッセージ又はファイルの出所は、専用のツールを使って、このデジタル署名によって検証される。
	電子証明書	信頼できる第三者（認証局）が間違いなく本人であることを電子的に証明するために発行されたデータセットをいう。

用語		説明
	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。
	電子認証	電子認証とは、電子認証局から発行される「電子証明書」を用いて、なりすましの防止や情報の改ざんを防止する技術。
	電力線搬送通信（PLC）	電力を供給する電力線を伝送路として通信を行うもの。既設の電力線を利用することにより容易にネットワークを構築することが可能。
な	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。
	熱暴走	機器の発熱を適切に制御できないこと等により、中央演算装置等のコンピュータチップ等が高熱により誤動作、停止等の状態になること。
は	バグ	ソフトウェアで設計者の認識の有無に関わらず、全ての成果物において、要件定義の誤り、仕様設計の誤り、プログラミングの誤り、システム構築の誤り等により、期待される結果」と乖離があるために、何かしらの対策・対応が必要と考えられる現象、又はその原因。
	パケットフィルタリング	フィルタリングとは、一般的な意味ではろ過することであるが、コンピュータや Web 等、インターネットの世界では「情報ろ過」を指す。パケットフィルタリングは、ネットワークを行き交うパケット（ネットワークを通して送信されるデータを分割する際に使われる単位）をポリシーに応じて制御する手法。
	バージョン不整合	プログラムの不備の修正や機能の追加等のため、バージョンの更新を行った際に、何らかの理由で特定のファイルやプログラムの更新が行われず、更新された他のシステムとの整合性が取れなくなること。その結果として、間違ったデータを参照したり、システムエラーにより停止したりする場合がある。バージョンは元々「版」を意味する。
	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。
	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。パターンファイルは、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。
	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、または裏口を開けるプログラムのこと。このプログラムが実行されると、インターネットからコンピュータを操作されてしまう可能性がある。なお、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。
	搬送波	音声や映像、データ等の情報を伝送する信号。信号は電波（無線通信）や光（光ファイバーケーブル）等によって伝達される。送信する信号に応じて搬送波に対して変調を加え、通信を行う。

用語		説明
	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。
	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。
	標的型メール	情報システムへの攻撃や機密情報の漏洩等を目的に、特定の企業や個人を対象に送りつけられる電子メールのこと。その電子メールの添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する。
	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。
	ファイル交換ソフト（ファイル共有ソフト）	複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェア。
	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。
	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。
	不正コマンド	プログラムに対して、本来期待される機能が損なわれるような処理の実行を求める命令
	不正侵入	利用する権限を与えられていないネットワークやコンピュータに侵入して、不正にネットワークやコンピュータを操作する行為のこと。
	不正ソフトウェア	コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称があるが、端末に悪影響を与えることを目的とするソフトウェアを指す。
	ブラウザ	Web サイトを閲覧するためのアプリケーションソフト。
	振る舞い検知	アンチウイルスの一種で、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、その振る舞いによってウイルスかどうか判断する方法。
	ブレークグラス	ICT システムにおいて非常時専用の ID パスワードを準備し、使った痕跡が残る運用を「ブレークグラス」という。火災を発見時、消火栓が使用できるように、消火栓設置の非常押しボタンを覆うガラスを割ってから、ボタンを押してポンプを起動し、警報を鳴らす。このとき、割れたガラスが痕跡として残ることから、このように呼ばれる。

用語		説明
	プロセスアプローチ	同じ性質の活動の集まりをプロセスとみなし（例：設計プロセス、購買プロセス、製造プロセス など）、品質マネジメントシステム（QMS）を構成するプロセス間の前後を効果的に繋げ、さらに個々のプロセスの管理を徹底することで、個々のプロセス及びプロセス全体の効率とパフォーマンス（意図した結果の達成）、を高めようとする品質管理活動手法のこと。
	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。
	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。
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。
	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。
	マッピング	AとBを関連付けること。例えば、地図上に住所を関連付けること等をいう。
	マルウェア	malicious softwareの短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。
	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。
	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。
	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。
	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社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。
	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。
	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	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タイプのウイルスのこと。

用語		説明
	ワンタイムパスワード	接続する毎に入力するパスワードが毎回変わる方式で、一度使用されたパスワードは次回からは使用できない。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	ACL（アクセス制御リスト）	情報等へのアクセスの制御を行う際に利用する、誰からのどのような操作を許可するかのリスト。
	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をいう。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。
	ASP・SaaS	ASP（Application Service Provider）は、ネットワークを通じて、アプリケーション・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	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。
	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。企業における情報セキュリティを統括する責任者を指す。
	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。
D	DICOM	Digital Imaging and Communications in Medicine の略。医用画像情報やそれらの通信に関する国際標準規格。
	DoS	サービス不能（DoS）攻撃の項を参照されたい。
F	FIPS140-2	コンピュータシステム及び電気通信システム(音声システムを含む)内の、米国の”the Information Technology Management Reform Act of 1996, Public Law 104-106”の 5131 節に定義された重要情報を保護するセキュリティシステムで利用される暗号モジュールに対するセキュリティ要求事項を規定する標準（FIPS140-1 の改定版）。
E	EDR（Endpoint Detection and Response）	端末での脅威を検知してインシデント対応等を支援する手法。
H	HL7	Health Level Seven の略。医療情報交換のための国際標準規格。
	HL7 FHIR	HL7 International によって作成された医療情報交換の次世代標準フレームワーク。HL7 International の一連の標準規格、HL7

用語		説明
		version 2 、 HL7 version 3 と CDA(Clinical Document Architecture)の優れた機能等を踏まえ、最新の Web 技術を活用し、実装性に重点を置いて策定された。
	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サービスとして提供するクラウドサービス。
	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ーを監視し、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。
	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。
	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。
	IoT	Internet of Things の略。情報社会のために、既存もしくは開発中の相互運用可能な情報通信技術により、物理的もしくは仮想的なモノを接続し、高度なサービスを実現するグローバルインフラのこと。
	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。
	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。
	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、遠隔地のネットワーク同士を LAN 同様に運用することが可能になる。
	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。
	ISDN	Integrated Services Digital Network の略。電話やファクシミリ、データ通信等を統合して扱うデジタル通信網のこと。
	ISMS	Information Security Management System の略。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。

用語		説明
	ISP	Internet Service Provider の略。インターネットに接続できるサービスを提供する事業者のこと。通常、電子メールを送ったり、ホームページを閲覧するためには、プロバイダと契約する必要がある。
K	Kerberos	オープンネットワークシステムのための認証システム。
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（メディア・アクセス・コントロール）アドレス。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。
	MO	MO（Magneto-Optical）ディスク。光磁気ディスクのこと。
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。
	OSI 階層モデル	ISO（国際標準化機構）が提唱した、異機種間通信を実現するためのネットワーク設計方針である OSI（開放型システム間相互接続）において、プロトコルを機能により 7 つの 階層に分割した概念モデル。
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）をサービスとして提供するクラウドサービス。
	PKI	Public Key Infrastructure の略。公開鍵をベースに秘匿性、アクセスコントロール、データの完全性、認証、否認防止を確実にするための公開鍵暗号とデジタル署名サービスを提供する包括的なシステム。
R	RAID	Redundant Arrays of Inexpensive Disks 若しくは Redundant Arrays of Independent Disks の略。複数のハードディスクを組み合わせ、仮想的な 1 つのハードディスクとして運用する技術。これにより冗長性の向上が期待できる。
	REST API （Representational State	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。

用語		説明
	Transfer Application Programming Interface)	
S	S/MIME	電子メールに送信内容の電子署名や暗号化の機能を付加するための規格。
	SNS	Social Networking Service（ソーシャル・ネットワーキング・サービス）の略。登録したユーザーだけが参加できるインターネットの Web サイトのこと。
	SSID	Service Set Identifier の略。無線 LAN で特定のコンピュータや通信機器で構成されるネットワークを指定して、接続するための一意の識別コードのこと。ESS ID とも呼ばれている。 無線 LAN で送信するパケットのヘッダ（先頭部）に含まれ、受信側は、SSID が一致しない場合は、そのパケットを無視するため通信ができない。
	SSL-VPN	SSL-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（バーチャル・プライベート・ネットワーク）の略。インターネット上を利用しながら、仮想的にプライベート・ネットワーク（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）を構築する技術。
W	Winny	日本で開発されたファイル共有ソフト。 インターネット上でクライアント同士が互いの保有するファイルをやり取りすることができる P2P 方式のソフトウェア。
	WPA2/AES	WPA2 は、Wi-Fi Protected Access 2 の略。無線 LAN の暗号化方式である WPA（Wi-Fi Protected Access）のセキュリティを向上させ、AES 暗号に対応した方式。AES は上記の暗号技術のこと。
	802.1x	LAN におけるユーザー認証の方式の規格。IEEE802.1x は、無線 LAN だけでなく、有線も含んだユーザー認証の方式である。クライアントが接続を要求した場合には、認証サーバである Radius サーバが認証処理を行う。クライアントが認証された場合には、セッションごとに暗号鍵が与えられる。 なお、IEEE802.1x では通常暗号化を行わないため、無線 LAN を利用する場合には暗号化する。

資料２

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

令和４年３月30日
第10回健康・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資料２

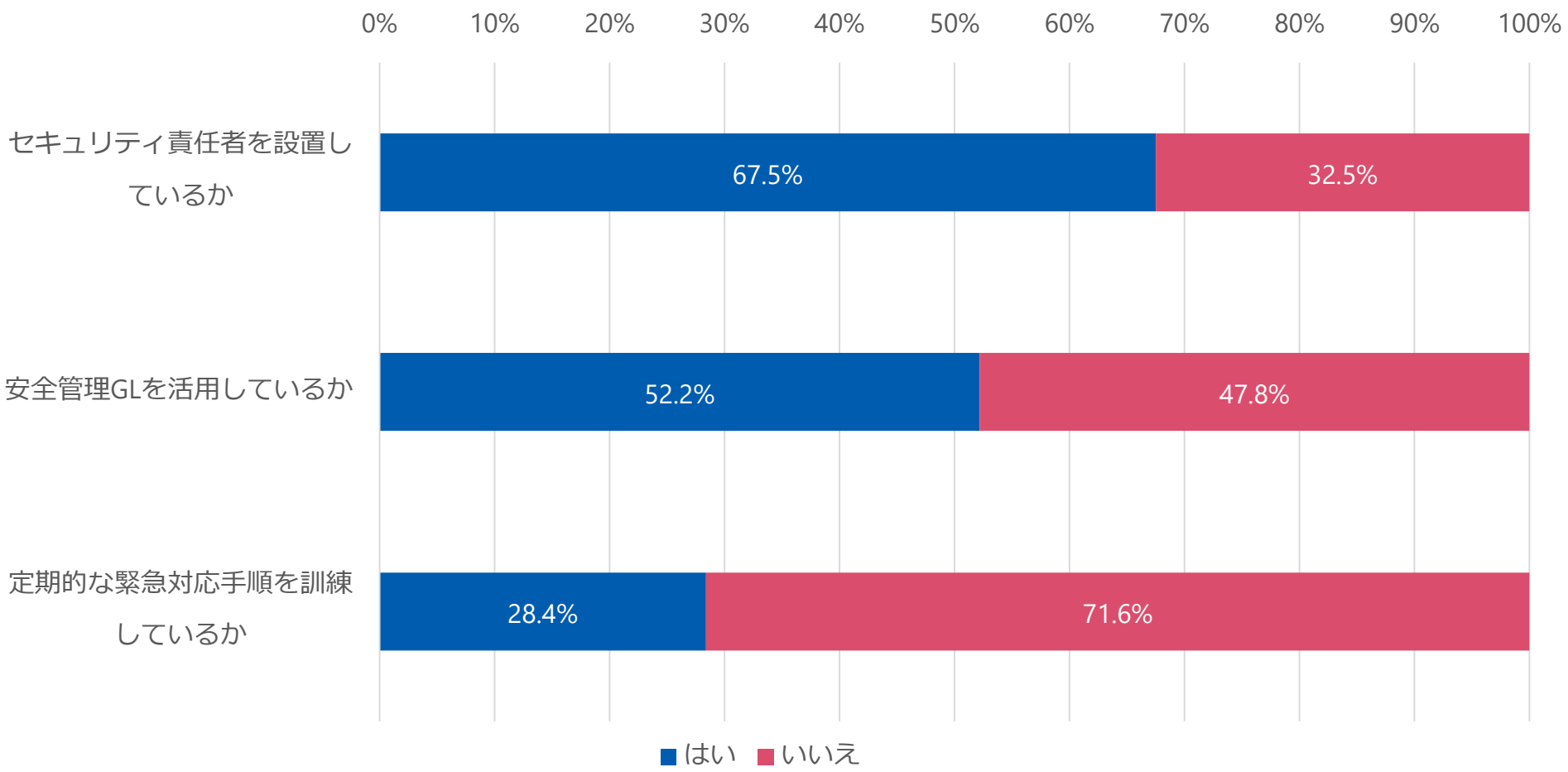
「病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査」の結果について

Ministry of Health, Labour and Welfare of Japan

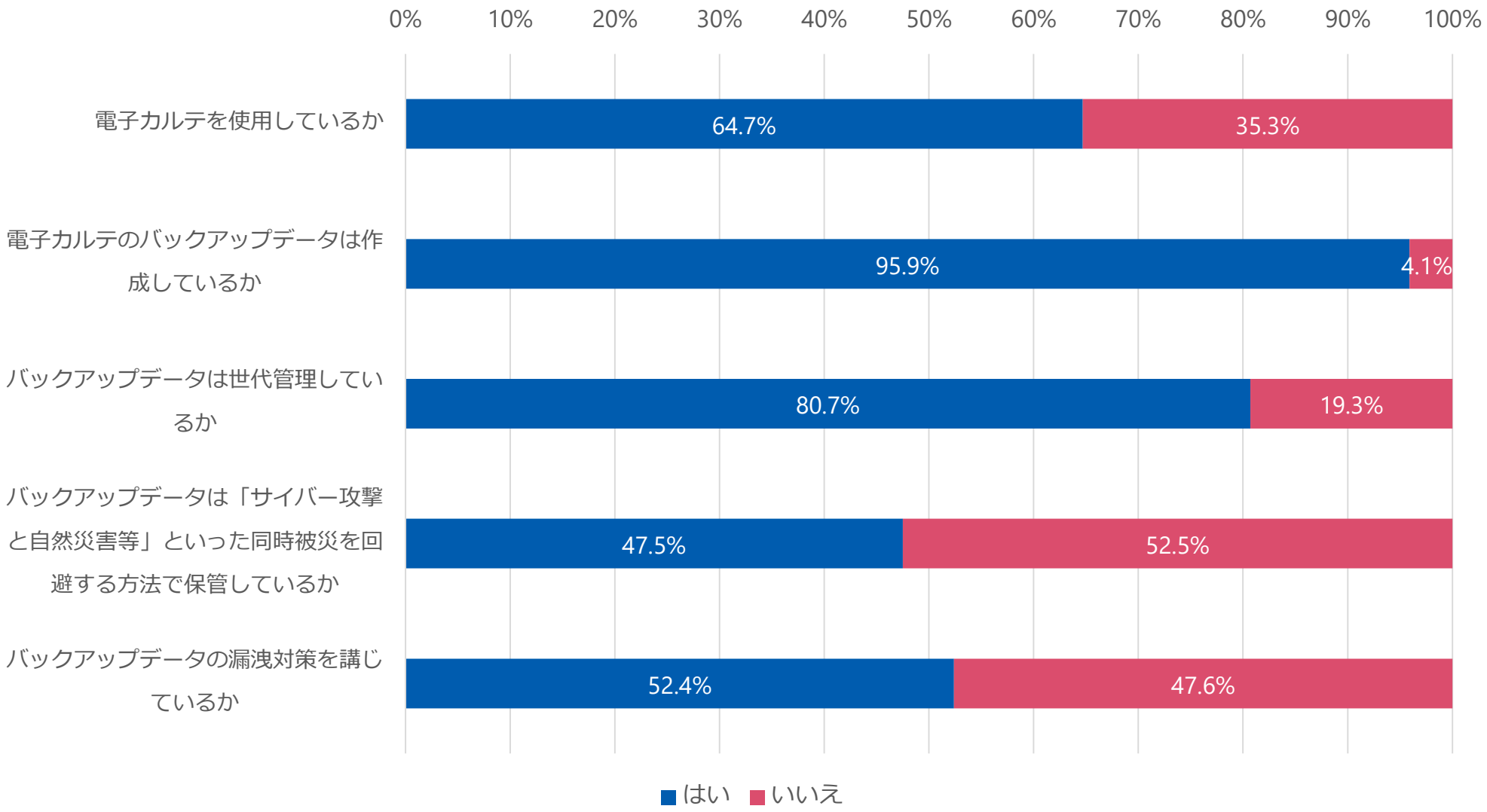
調査結果について

調査対象医療機関数：8,252施設

有効回答数　　：6,216施設（回答率：75.3%）

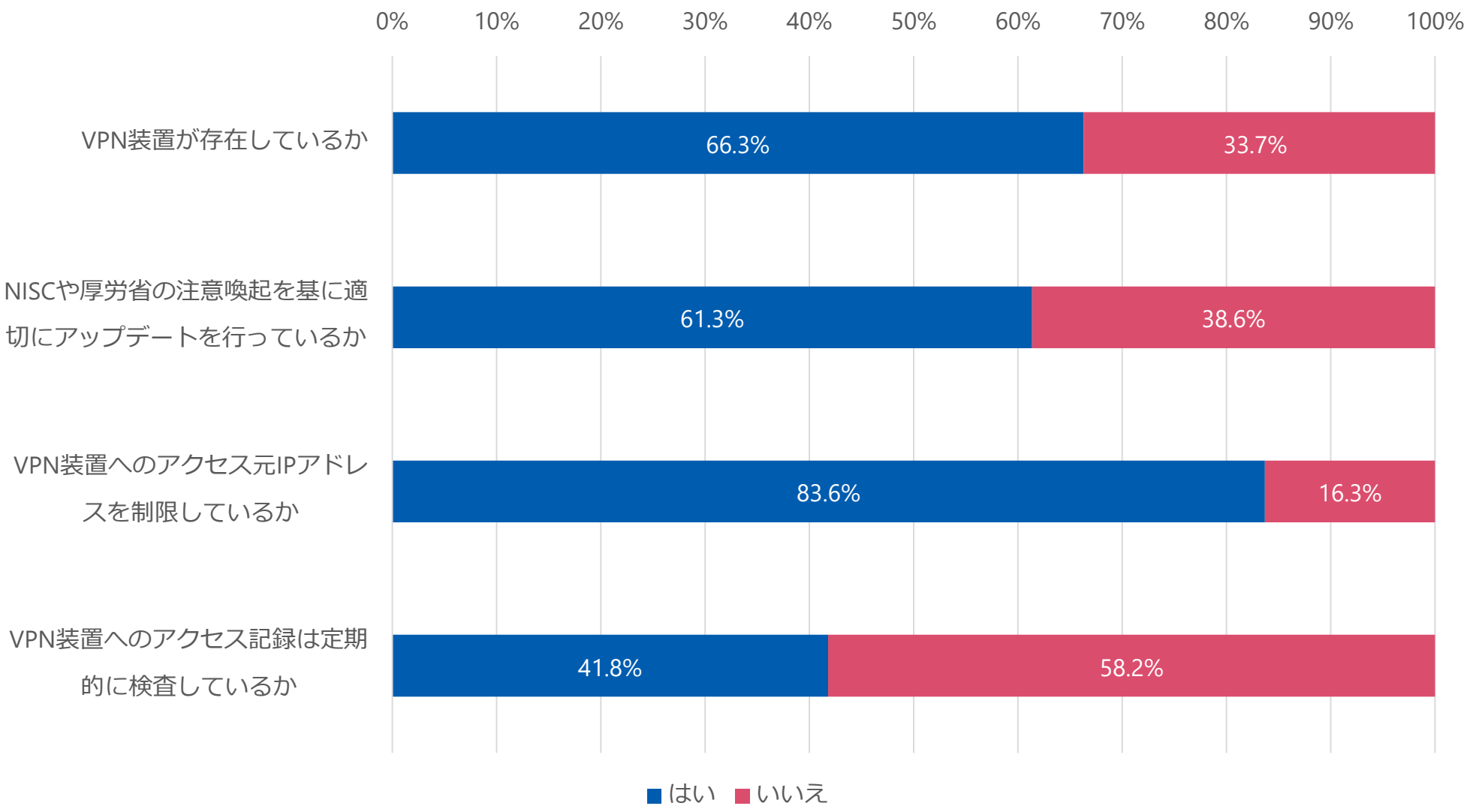


調査結果について（電子カルテシステムのバックアップについて）



※バックアップデータ作成に関する質問（2項目）以降ついては、電子カルテを導入している64.7%（4,020施設）が母数となっている。

調査結果について（リモートゲートウェイ装置について）



※VPN装置のアップデートに関する質問（2項目）以降については、VPN装置が存在する66.3%（4,120施設）が母数となっている。

病院における医療情報システムのバックアップデータおよびリモートゲートウェイ装置に係る調査（概要）

第28回重要インフラ専門調査会

厚生労働省提出資料より抜粋

目　的

医療機関に対するランサムウェアなどのサイバー攻撃が増加し、長期にわたり診療が停止した事例等が確認されていることから、病院におけるランサムウェアのリスクを把握するとともに、早急に長期に診療が停止することがないよう有効な対策の実施を促すため、病院が保有する医療情報システムの保守等に用いられるリモートゲートウェイ装置の有無とそのアップデート状況及び電子カルテシステムのバックアップ保持の実態についての調査を行う。

調査方法・対象

- G-MISを用いて、リモートゲートウェイ装置及びバックアップ保持の実態に関する調査を実施する。（問数は10～15問程度）
- 調査対象は、G-MIS IDが付与されている、約8,300の病院。

スケジュール

調査期間：令和４年１月27日～令和４年２月14日、令和４年３月８日～令和４年３月24日（予備）

それぞれ項目について、医療情報システムの安全管理に関するガイドライン第5.2版（以下、「ガイドライン」という）のどこの部分が対応するかを項目に追記しました。

病院における医療情報システムのバックアップデータ及び
リモートゲートウェイ装置に係る調査に係る回答要領

依頼事項

- 本回答要領に基づき、病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査（以下「本調査」という。）の設問に回答してください。
- 回答に当たっては、提出後の修正等作業をできるだけ防ぐだめ、必ず本回答要領を確認してください。
- 技術的な質問・用語等については、院内担当者だけでなく、システム設置事業者や保守事業者への照会等も活用して回答してください。

【電子カルテシステムのバックアップに係る質問関係】

１．回答者の情報

回答者の氏名、所属、連絡先を記載してください。なお、後日内容の確認のため、厚生労働省より回答者に対し連絡をさせていただく可能性があります。

２．セキュリティ責任者を設置しているか

システム障害時の対応や、問題発生の原因調査、セキュリティ対策訓練に関して責任がある、セキュリティ責任者を職員として配置しているか。また、セキュリティ責任者を医療情報システムの責任者とは、別に、配置しているか。回答を選択してください。

【ガイドラインにおける該当箇所と概要】
本項目における「セキュリティ責任者」とは、ガイドライン本編6.10章（P.37）おける「情報セキュリティ責任者（CISO）」を指します。現状、すべての医療機関において設置の義務はありませんが、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、CISOの設置が強く求められています。

３．医療情報システムの安全管理に関するガイドライン及びそれを基としたチェックリスト等を活用しているか。

厚生労働省が定めている、

- 医療情報システムの安全管理に関するガイドライン
- 同ガイドラインを基にした「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」

を活用しているか回答を選択してください。

（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5.1版（令和3年1月）https://www.mhlw.go.jp/stf/shingi/0000516275.html

【ガイドラインにおける該当箇所と概要】

ガイドライン本編３章（P.5）において、「本ガイドラインは医療情報を保存するシステムだけでなく、医療情報を扱うすべ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及び組織を対象としている」と記載されています。

４．システム障害発生時等において詳細な緊急対応手順を整備し、定期的に訓練しているか

システム障害時や不正アクセスが顕在化した際に、速やかに連絡するべき者（※）を院内に平時から確認・周知することが必須です。障害や不正の発生個所特定のための分析や切り分けの具体的な技術手順、代替措置のための機器や環境整備、緊急対応のための技術的措置に必要な設計資料やマニュアル、認証等の情報を常時最新化し、緊急対応が発生した際に対応が可能な状態であるか、また、それらの情報を医療情報システムの担当者と導入事業者が一体となって定期的に点検しているか、回答を選択してください。

（※）具体的には、医療情報システムの完全管理に関するガイドラインに記載されている

医政局研究機発振興課医療情報技術推進室　03-3595-2430

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

の他、必要に応じて事業者、捜査機関等にも適切に情報提供すること。

【ガイドラインにおける該当箇所と概要】

ガイドライン本編6.10章（P.37）において、システム障害発生時等の“非常時”における対応について、あらかじめ手順を定め、職員に対し教育・訓練を行うことを求めています。

５．電子カルテシステムを使用しているか

診療録の記載・保存を電子カルテシステムで行っているか回答を選択してください。なお、本問でいう電子カルテシステムとは、

- オーダリングシステム
- オーダリング機能、画像管理等の部門システム及び診療録を電子的に記録する機能を備えた統合的な医療情報システム

を指します。なお、電子カルテシステムを使用していない場合は、９．までは回答不要となります。

６．電子カルテシステムのバックアップデータは作成しているか

サイバー攻撃や災害等で電子カルテシステムのデータが消失又は使用不可能な状態（暗号化等）になった場合でも、バックアップデータを作成し、診療におおきな支障がないように復旧が可能となるように定期的にテストを行っているか回答を選択してください。

【ガイドラインにおける該当箇所と概要】

ガイドライン本編 7.2 章（P.60）、7.3 章（P.62）において、診療録等に記載された患者情報を確認できるよう、定期的なバックアップの実施を求めています。

７．バックアップデータは世代管理しているか

電子カルテシステムのバックアップデータについて、世代管理をしているか回答を選択してください。ただし、具体的な管理方法までを問うものではありません。

なお、世代管理とは最新のバックアップデータだけでなく、それ以前のバックアップデータも管理することを指します。例えば、１日１回バックアップデータを作成している環境で「３世代管理」といえば、３日前までのデータまでさかのぼれることが可能となります。

【ガイドラインにおける該当箇所と概要】

ガイドライン本編 6.10 章（P.37）において、「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。」と具体例を示し、C.最低限のガイドラインに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することを求めています。

８．バックアップデータについて、サイバー攻撃による汚損や破壊、火災や自然災害による消失等同時災害を回避する方法で管理しているか

作成しているバックアップデータについて、例えば遠隔地のサーバに保管、世代ごとにオフラインで保存するなど、不測の事態に備えた保管方法をとっているか回答を選択してください。ただし、具体的な管理方法まで問うものではありません。

【ガイドラインにおける該当箇所と概要】

上記同様に、「バックアップデータを保存した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」と具体を記載しています。

９．バックアップデータの漏洩対策を講じているか

作成しているバックアップデータが仮にサイバー攻撃等を受け漏洩する事態が起こった場合等においても、解読できないような対策（暗号化や秘密分散管理等）を講じているか回答を選択してください。ただし、具体的な管理方法まで問うものではありません。

【ガイドラインにおける該当箇所と概要】

ガイドラインにおいては、バックアップデータの暗号化等を具体的には定めていませんが、令和４年４月施行となる改正個人情報保護法において、個人情報の流出事案については、報告の義務化・罰金の増額（最大１億円）等の措置が取られるようになるため、漏洩対策についても検討を行う必要があります。

別紙

【リモートゲートウェイ装置に係る質問関係】

本項目については、回答に当たり院内のサーバ室等を確認し、リモートゲートウェイ装置（以下、「VPN 装置」という）が存在するか確認してください。

１０．VPN 装置が存在するか。

医療情報システム（※）の保守点検等を目的とし、事業者とシステムを接続するために VPN 装置を設置している場合が多々あります。

システム設置業者や保守業者などに照会し、当該機器が設置されているか回答を選択してください。設置されていない場合は、以降の設問は回答不要となります。

（※）医療情報システムとは、オーダリングシステム、電子カルテシステム、レセプト電算システム（審査請求受付も含む）、画像・検査等の各部門システム、地域医療ネットワークシステム、PHR 等、病院における診療を補助するためのシステム全般を指します。

１１．VPN 装置のメーカー名、型番、台数を全て記載すること

上記で確認した VPN 装置について記載してください。（記述方式）

１２．内閣サイバーセキュリティセンター（NISC）や厚生労働省の注意喚起を基に VPN 装置のアップデートを適切に行っているか

NISC や厚生労働省では、医療セプターや都道府県・地方厚生局宛にサイバーセキュリティ対策に係る情報を提供しています。それらの情報を基に、VPN 装置のアップデートを適切に行っているか、回答を選択してください。

（参考）

内閣サイバーセキュリティセンターランサムウェア特設ページ

https://security-portal.nisc.go.jp/stopransomware/

【ガイドラインにおける該当箇所と概要】

ガイドライン本編 6.10 章（P.37）において、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」も参照することを求めています。

１３．VPN 装置へのアクセス元 IP アドレスを保守業者等に制限しているか

VPN 装置への不正アクセスを防ぐため、アクセス元 IP アドレスを制限しているか、回答を選択してください。保守業者がアクセスするだけで機能を果たせると考えられ、それ以外のアクセスについては制限されるのが一般的です。保守事業者に照会し、現状を確認してください。

【ガイドラインにおける該当箇所と概要】

ガイドライン 6.11 章（P.42）C.最低限のガイドラインにて、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、と求めています。

１４．VPN 装置へのアクセス記録を定期的に分析・監査しているか

不正アクセス防止の観点から VPN 装置へのアクセスをログ等に記録し、かつ、記録に不正な傾向がないか定期的に（例えば年１回）分析・監査をしているか回答を選択してください。

サイバー攻撃を受けた医療機関においても、不正アクセスの記録が残っていることがあり、それらを把握することができていれば被害を防げていた可能性もあります。

【ガイドラインにおける該当箇所と概要】

ガイドライン 6.5 章（P.21）においては、VPN 装置のみならず医療情報システム全般について、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を求めています。