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年〇月

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。

⑹ 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。

⑶ 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。

⑷ 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。

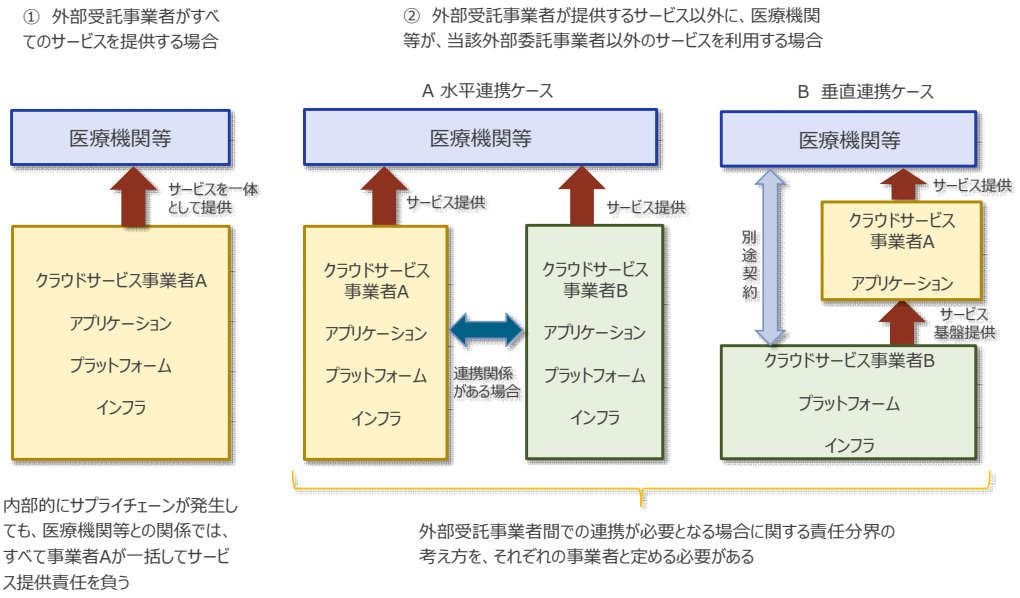


図 4-1　1 者又は複数の事業者が受託する場合の責任分界の考え方

(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

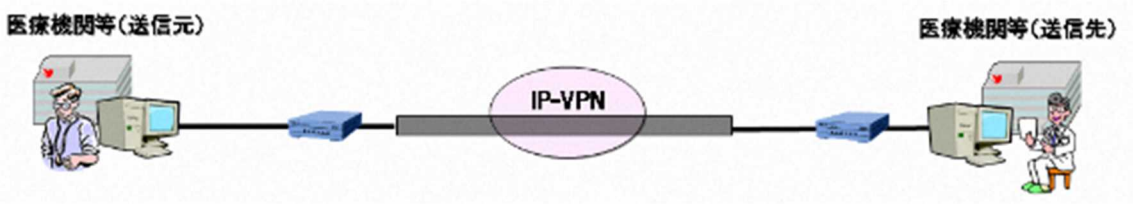
※　なおISDNは2024年1月にサービスの終了がアナウンスされていることから、現在同サービスを利用している場合には、代替策を講じることが求められる。ISDNの代

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。

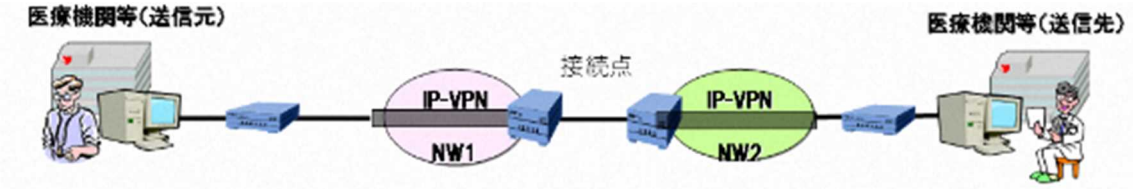
3)閉域 IP 通信網で接続されている場合

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。

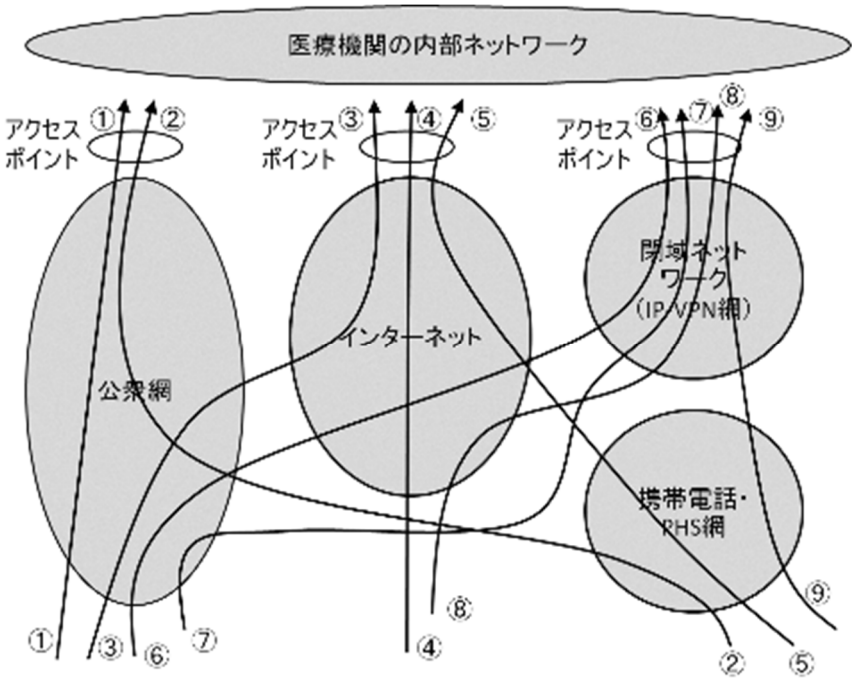
また、外部との接続については、医療機関等がクラウドサービスを利用し、受託事業者等

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。



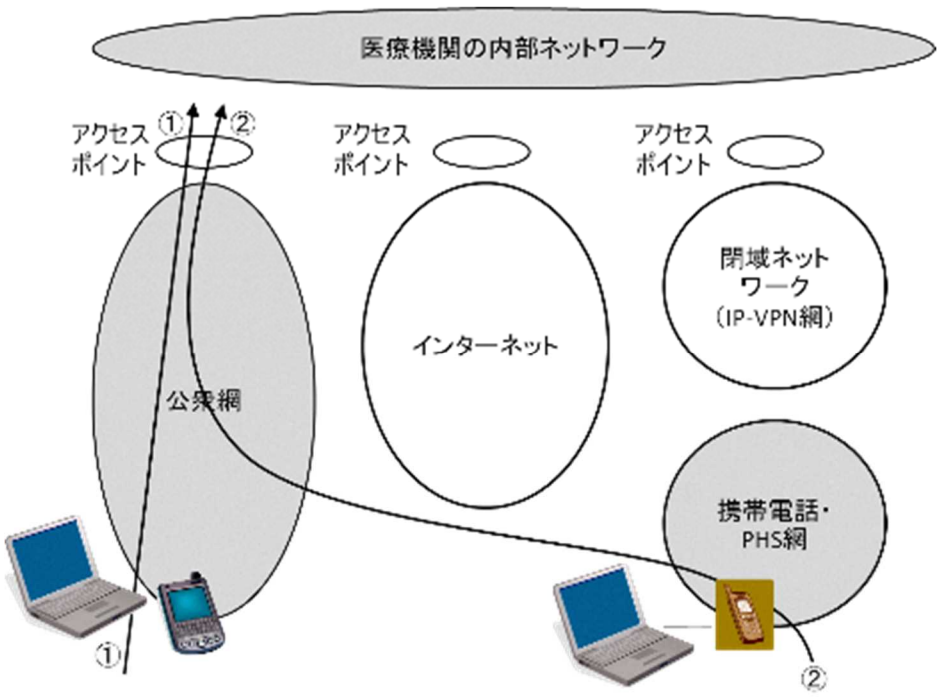
図⑤　モバイル環境における接続形態

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）



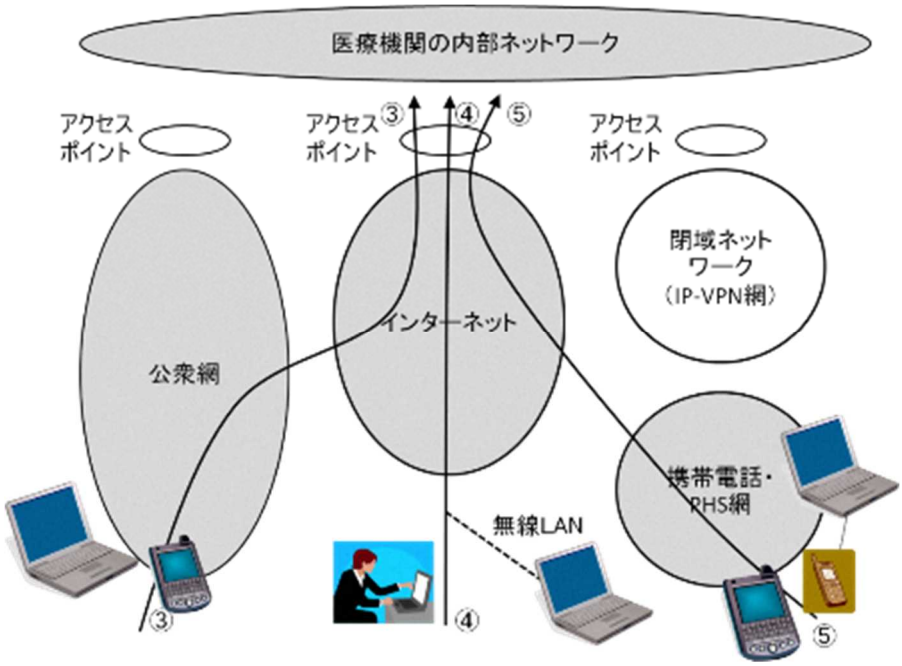
図⑥　モバイル環境における接続形態（公衆網経由）

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）

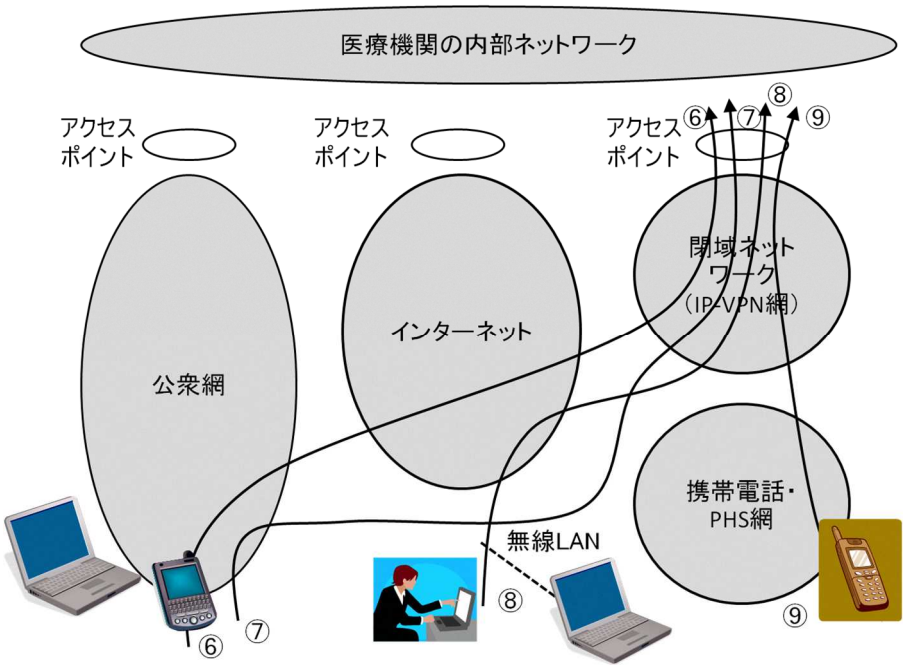
③は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続してインターネットのサービスプロバイダのアクセスポイントにダイアルアップし、インターネット経由で医療機関等のアクセスポイントに接続するケースである。

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。