医療情報システムを安全に管理するために（第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
平成 29 年５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。

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20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※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、従業者が誤ってコンピュータウイルスが仕込まれ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）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、情報端末・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）
- 不正な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（2要素認証）を採用することが推奨される。

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。

電子処方せんの取扱いについては、「電子処方せん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、「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「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」（総務省）、並びに「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」（経済産業省）の規定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。

なお、これらのリスクについては、本書の４ 章で解説をしている。

（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。

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扱うASP・SaaS型のサービスを利用する
- 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、医療機関等は保守委託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。