医療情報システムを安全に管理するために

「医療情報システムの安全管理に関するガイドライン」

すべての医療機関等の管理者向け読本

平成 21 年3月

厚生労働省

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。

【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もしくは決定する立場にある管理者、ならびに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対象と想定している。

また、これら管理者の方々が、本書を一読して実際にシステムを導入する情報技術管理者や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している。

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。

本書でいう「医療情報システム」とは、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・取得するようなコンピュータや携帯端末も範疇として想定している。また、患者情報が通信される院内・院外ネットワークも含まれる。

ガイドラインは、①各種の法令等で求められるもしくは規定される要件を満たす実行指針、②医療に係わる情報を医療機関等の資産（以下、本書では「情報資産」という）と捉え、継続的に保護して行くためのプロセスに関する手引書、の２つの性格を有している。

従って、ガイドラインでは情報技術を利用・活用する場合の留意点等を記載するに当たって、遵守すべき法令等への言及、情報資産の保護のための方策等に対して詳細に渡って解説を加える必要があることから、内容や頁数が多くなる傾向が避けられず、平易に読めるものにはなっていない。

そのため本書は、ガイドラインの概要をできるだけ平易に示し、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、ポイントを絞って整理し解説を加えている。

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に際して、医療機関等の管理者に求められる責任について解説をしている。これには、ガイドラインに違反していた場合に訴求され

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必要な、継続的な情報資産の保護と法令等に対する解説をしている。

・　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に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
　個人情報保護法で求められる安全管理措置について解説している。

・　e-文書法の視点から
　主に e-文書法の厚生労働省省令及び外部保存通知で求められる「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もしくは提供する際の考え方

医療機関等で外部とネットワークを通じて個人情報を含む医療情報を交換する場合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

医療に関わるすべ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、情報が適切に収集され、必要に応じて遅滞なく利用できるように適切に保管され、不要になった場合に適切に廃棄される必要がある。これにより、刑法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および指針の他、診療情報の扱いに係わる法令、通知、指針等により定められている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犯罪として処罰される。しかし、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同様に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のことを「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たものであり、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なる。

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

医療情報保護の体制を構築し、管理する局面での責任。「①説明責任」、「②管理責任」、「③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。「①説明責任」、「②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。

ポイント

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明確に文書化し、仕様や計画が当初の方針の通りに機能しているかどうかを定期的に監査し、その結果も文書化し、監査の結果問題があった場合は、真摯に対応し、対応の記録も文書化し、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、患者等に説明するため、患者窓口を設置することも必要となる。

② 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。

ポイント

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

個人情報保護法上は個人情報保護の担当責任者を定める必要があり、適切な担当責任者を決めて、請負事業者との対応にあたる必要がある。

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。

ポイント

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る可能性がある。ただし、このような最新の技術動向を管理者が都度、把握して行くことは、管理者としての本来業務と異なることもある。従って、管理者は、運用管理の状況を監査・確認する際には、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などして、必要な改善を実践して行くことが重要な役割となる。

(2)　事後責任

① 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、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、対処法を説明する責任である。

ポイント

個々の患者へ事故の内容ならびにその原因と対策についての説明責任はもちろんのこと、監督機関である行政機関や社会への説明・公表が求められる。

② 善後策を講ずる責任とは？

1）原因を追及し明らかにする責任、2）損害を生じさせた場合にはその損害填補責任、3）再発防止策を講ずる責任である。

ポイント

何らかの不都合な事態が生じた場合には、医療機関等の管理者は善後策を講じなくてはならない。

その責任は、事故が、適切な委託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場合でも、患者に対する関係では、選任監督の注意を払っていてもなお、これら 3 つの意味で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

ネットワークおよ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ことも現実のものとなってきた。

このような状況の下では、医療情報の管理責任が医療機関等の管理ばかりでなく、ネットワーク上の空間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、さらには伝送先の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で、ガイドラインでは責任分界点として説明されている。

医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には「(1) 委託（第三者委託)」と「(2) 第三者提供」の 2 種類があり、医療機関等の管理者の責任のあり方には大きな違いがある。

(1) 委託（第三者委託）の場合

医療情報は医療機関等の管理者の業務遂行目的のために委託されるのであり、管理者の支配下にある。

ポイント

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、提供された部分の情報については、もはや提供元の管理者ではなく第三者に情報を適切に保護する責任が生ずる。

ポイント

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、電子化情報は、医療機関等の側で当該情報を削除しない限り、情報が第三者提供されたからといってなお医療機関等のもとにも残るため、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の手を経て情報提供が行われる場合には、いかなる時点で、第三者に提供されたことになるかということを明らかにすべきである。そのためには、それらの事実を可能な限り記録管理し、事故が起きた場合に記録の開示要求があれば、それに応じる必要もある。

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行くための継続的に取組む枠組みについて、及びガイドラインで言及されている各種法令等に対して、医療情報システムで必要な要件について解説する。

3.1　情報資産を保護して行くための手引き

医療情報システムを導入する時、また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行くために必要な取組みについて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行く手段や手続き等については、国際的にも確立されたシステム構築方法やそれに伴う文書等がある。中心となる概念としては、「①計画を立てる」、「②それを実行する」、「③必要に応じて見直しを行う」、「④改善をする」である。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行くというものである。しかし、医療機関等の情報資産保護においてはこの概念が新しいものであるかと言えば、そうではない。

特に、医療安全に関してはこの概念が顕著であり、平成 18 年の「良質な医療を提供する体制の確立を図るための医療法等の一部を改正する法律」（法律第 84 号）の施行に伴い通知された「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）においては、医療の安全に関する事項として、この概念が以下の様に規定されている。

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（※但し、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、医療機関等においては医療安全管理の例の様に「①計画を立てる」、委員会や職員研修を実施しながら「②それを実行する」、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」、必要に応じて「④改善をする」というプロセスが既に存在している。従って、医療情報システムやそこに蓄積された情報の継続的な保護、利用・活用のプロセスも特殊な概念と捉えずに通常の業務の枠組みの一環として検討をした上で、確実に実行して行くことが重要であるといえる。

ただし、医療情報システムの場合、現在活用しているシステムが翌年にはセキュリティ上の問題を抱えたシステムになっていることもあり得る。従って、見直しや改善の際には、通常運用における責任でも述べたように、情報技術の進展にも留意する必要がある。その際には、ガイドラインを参考にすることが有益な手段となるので、積極的に活用してもらいたい。

新たに電子カルテなどの医療情報システムを導入する際には、出発点となる「①計画を立てる」ことが必須である。「①計画を立てる」際には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、それを重要度に応じて分類し、業務や組織形態、人事体系等との整合性を図らなければならない。既に医療情報システムを導入している場合においても、「③必要に応じて見直しを行う」において適切な見直しを行い改善につなげていく必要がある。

医療情報を資産として捉えた場合、医療機関等の管理者・責任者は、資産管理に対して主体的に行う必要があり、これは情報技術を使う、使わない以前の問題として素直な感覚として捉えてもらえると思われる。

3.2 医療情報システムの安全管理に求められる基準

個人情報保護法では、第 20 条に安全管理措置の定めがある。安全管理措置とは、具体的には「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」で構成されている。本章では、これらについて解説をする。

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、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。

ポイント

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重要である。

また、これらのことを実践し、管理責任や説明責任を果たすために運用管理規程を定めることはきわめて重要である。

医療機関等の管理者は上記の事項を踏まえて、医療情報システムを運営して行かなくてはならない。

物理的安全対策

物理的安全対策とは？

物理的安全管理措置とは、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。

ポイント

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

留意するポイントとしては、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してもらいたい。

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。

ポイント

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は、下記の項目が挙げられる。

（1） 情報区分と利用者の対応付けを行い、アクセス権限を設定すること
（2） 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)
（3） 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できる保証はなく、一般的には運用管理による対策との併用は必須である。

人的安全対策

人的安全対策とは？

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

ポイント

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はかるため、人による誤りの防止を目的とした対策を施す必要がある。これには、守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項を含む必要がある。

医療分野は様々な資格者と職種が混在しており、医療情報システムに関連する関係者は更に多岐に渡る。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。従って、これらの関係者を適切に管理する規程の策定と教育、訓練を実施する必要がある。

また、求められていることは医療情報システムが対象にしている情報の生成から廃棄に至るまでの情報のライフサイクルに渡る安全管理であるので、廃棄についても上記措置に含めて考えることが必要である。

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、平成 11 年 4 月の厚生省通知「診療録等の電子媒体による保存について」によって規制緩和され、いわゆる「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て、診療に供する情報を扱うが故の医療固有の要求事項が示されている。これがいわゆる「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」の３つの要件で構成されている。

ここでは、e-文書法の厚生労働省令である「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」及び「診療録の保存を行う場所（通知）」に則ってガイドライン第３版の７章から９章の中で詳細に記述され、実現を求められる「真正性」、「見読性」、「保存性」について解説する。

真正性の確保について

真正性とは？

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。

ポイント

発生する各種のデータに対して、「作成責任の所在と、内容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の明確化と完全性の確保（虚偽入力、書き換え、消去、及び混同の防止）を行う必要がある。

また、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。

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。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ので参照してもらいたい。

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、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできることである。 ただし、見読性とは本来「診療に用いるのに支障が無いこと」と「監査等に差し支えないようにすること」であり、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。

ポイント

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と操作方法でということである。

情報の所在管理と見読化手段の管理も必要である。患者毎の情報全ての所在が日常的に把握されていなければならない。外部保存していたとしても同様である。また、電子媒体に保存された情報は、そのままでは見読できず、その電子媒体から情報を取り出すには何らかのアプリケーションが必要であり、表示のための編集前提となるマスタ、利用者テーブル等が別に存在したりする可能性がある。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。

また、必要な情報を必要なタイミングで正当な情報利用者に提供できなかったり、記録時と異なる内容で表示されたりすることは、重大な支障となるので、それを防ぐためのバックアップや冗長性の確保などのシステム全般の保護対策が必要である。何らかのシステム障害が発生した場合においても診療に重大な支障が無い最低限の見読性を確保するための対策が必要である。

更には、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ようなことがないようにしなくてはならない。

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渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

ポイント

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、下記のものが考えられる。

（1） データ保存自体が機器やソフトウエァの障害等によりなされていない可能性
（2） 記録媒体、設備の劣化による不完全な読取

（3） コンピュータウイルスや不正なソフトウェアを含む設備・記録媒体の不適切は管理による情報の喪失

（4） 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する技術面及び運用面での各種対策を施す必要がある。

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ことが対策されていることを確認することが必要である。

また、マスタ変更の際に、過去の記録が記録時と異なる内容で表示されたりすることが無い様にする事も保存性確保の範囲である。

4　電子的に医療情報を交換も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、個人情報保護およびネットワークのセキュリティに関して特に留意すべき項目について述べる。これには、双方向だけではなく、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、地域医療連携で医療機関、薬局、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、事業者が提供するソフトウェアをネットワーク越しに動かす ASP・SaaS（Application Service Provider・Software as a Service）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様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場合等が考えられる。

医療情報を、ネットワークを利用して外部と交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を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、これらについて医療機関等の視点から、「4.1　医療機関等における留意点」、「4.2　選択すべきネットワークセキュリティの考え方」について解説をする。

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。

医療機関等において情報を送信しようとする場合には、情報を適切に保護する責任を意識しつつ、次のような点に留意してもらいたい。

盗聴の危険性に対する対応

盗聴とは？

ネットワークに特異な事象ではなく、広く一般的に、意図的に第三者が会話や情報を盗み聞いたり、盗み取る行為。ネットワークでは、一般的には何らかの手段で伝送中の情報（電気信号）を盗み取る行為を指す。

ポイント

ネットワークを通じて情報を伝送する場合には、盗聴に最も留意しなくてはならない。

医療機関等においては、万が一、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。そのひとつの方法として医療情報の暗号化が考えられる。

どの程度の暗号化を施すか、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って異なるため、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必須である。

盗聴防止については、例えば ID とパスワードを用いたリモートログインによる保守を実施するような時も同様である。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。

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行為のこと。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を指す。

ポイント

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ることも重要な要素である。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、適切な対策を講じなければ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、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可能性も否定できず、その場合には改ざんに対する対処は必ず実施しておく必要がある。改ざんを検知するための方法としては、電子署名を用いる等が想定される。

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。例えば、本来情報を受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 やパスワードを盗み出して、本人しか見ることができない情報を見たりする行為を指す。

ポイント

ネットワークを通じて情報を伝送する場合、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た上で、情報を送ろうとする医療機関等は、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、また、送られて来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。

確認の手段は様々な方法があり、それらを適切に活用もしくは組み合わせて、なりすましに対する危険性へ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しての脅威に対応する方法の考え方について解説したが、ここでは、情報を伝達する通信経路上に対しての脅威に対応する方法の考え方について解説する。

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、医療機関等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。

一言でネットワークといっても、その構成は様々なものがあるため、全てを網羅して行くことは難しい。そこで、ガイドラインでは大きく「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されている場合」とに分けて考えており、本書もその体系に合わせて解説をする。

Ⅰ．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。

ポイント

クローズドなネットワークは安全性は高いものの、例えば、異なる通信事業者の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。この場合、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言えないため、クローズドなネットワークを利用する場合であっても、「4.1　医療機関等における留意事項」を参考に、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入するなどの措置を考慮する必要がある。

また、ウイルス対策ソフトのウイルス定義ファイルや OS のセキュリティパッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

Ⅱ．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形態である。現在のブロードバンドの普及状況から、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したりする等、その利用範囲が拡大して行くことが考えられる。

ポイント

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する。従って、十分なセキュリティ対策を実施することは必須である。また、「4.1　医療機関等における留意事項」に従って、医療情報に対して暗号化の措置を講じなければならない。

ただし、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、これらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。

医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の判断で導入する必要がある。また、技術的な安全性について、自らの責任において担保しなくてはならないことも意味する。

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やサービスが存在し、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。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。

5　おわりに

この管理者向け読本において、管理者としての立場のある方々に向けて、「責任」という面から、ガイドラインの解説をした。

ガイドラインは、システム構築のために本書で述べた事柄以上の多くの項目が記載されている。従って、本書が管理者の方々もガイドライン本文にも手を延ばす契機になれば幸いである。