医療情報システムの安全管理に関するガイドライン

第３版

（案）

新旧対照表

改正案	現　行
【目次】	【目次】
1 ～3 （略）	1 ～3 （略）
4　電子的な医療情報を扱う際の責任のあり方	4　電子情報を扱う医療機関等における責任のあり方
4.1　医療機関等の管理者の情報保護責任について	
4.2　責任分界点について	
4.3　例示による考え方の整理	
5　（略）	5　（略）
6　（略）	6　（略）
6.1 ～6.8 （略）	6.1 ～6.8 （略）
6.9　情報および情報機器の持ち出しについて	
6.10　災害等の非常時の対応	6.9　災害等の非常時の対応
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	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
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	
7　（略）	7　（略）
7.1 ～7.3 （略）	7.1 ～7.3 （略）
	7.4　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
8　（略）	8　（略）
8.1　（略）	8.1　（略）
8.1.1　（略）	8.1.1　（略）
8.1.2　外部保存を受託する機関の選定基準および情報の取り扱いに関する基準	8.1.2　外部保存を受託する機関の限定
8.1.3 ～8.1.4 （略）	8.1.3 ～8.1.4 （略）
8.1.5　留意事項	

8.2　（略）	8.2　（略）
	8.2.1　電子保存の 3 基準の遵守
	8.2.2　個人情報の保護
	8.2.3　責任の明確化
8.3　（略）	8.3　（略）
	8.3.1　利用性の確保
	8.3.2　個人情報の保護
	8.3.3　責任の明確化
8.4　（略）	8.4　（略）
9 ～10　（略）	9 ～10　（略）
付則 1　電子媒体による外部保存を可搬型媒体を用いて行う場合	
付則 2　紙媒体のままで外部保存を行う場合	
付表 1 ～付表 3　（略）	付表 1 ～付表 3　（略）
付録　(参考)外部機関と診療情報等を連携する場合に取り決めるべき内容	

改正案	現　行
4　電子的な医療情報を扱う際の責任のあり方	**4　電子情報を扱う医療機関等における責任のあり方**
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。	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責任者の責任で行うことが求められており、情報の取扱いも同等である。媒体に関わらず情報の取扱いは本章の最後に参考 1 として添付した「証拠能力、証明力について」や、参考 2「技術的対策と運用による対策」を留意して医療機関等の自己責任で行う必要がある。
（削除）	診療録等の電子保存や外部保存に係る自己責任は、電子化を行う場合に新たに付け加えられた要件ではなく、本来、そもそも紙やフィルムによる記録を院内に保存する場合も、医療法等で、医療機関等の管理責任者の責任、すなわち自己責任で行われてきており、それと同等な要件である。 ただ、紙の媒体やフィルムはその動きが一般の人にとってわかりやすく、特段の配慮が求められてこなかったが、電子化情報は一般の人にとってわかりにくく、情報の電子化はその実施が強制されるものではなく、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外部保存を含めた電子化の実施範囲及びその方法、すなわち導入システムの機能や運用計画を選択して求められる基準等への対応を決める必要があることから、自己責任で行っていることをあらためて明示し、管理責任者等の意識を喚起するために、あえて明記されたものと考えることができる。 自己責任は、「説明責任」、「管理責任」、「結果責任」を果たすことと考えられている。説明責任とは、電子保存や外部保存に関するシステムの機能や運用計画が電子保存や外部保存の基準を満たしていることを第三者に説明する責任である。管理責任とは、当該システムの運用管理を医療機関等が行う責任である。結果責任とは当該システムにより発生した問題点や損失に対する責任である。 この中で特段の配慮が必要なものは説明責任と管理責任で、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する必要がある。また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、その結果もあいまいさのない形で文書化し、また監査の結果問題があった場合は、真摯に対応するのはもちろんのこと、その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。管理責任も、例えば電子保存や外部保存に関するシステムの管理を納入業者にまかせていては果たせない。すく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等の監督を行う必要がある。
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ことで、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場合があるが、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りうるから、いずれにしろそのような事態が生じないよう適切な管理をする必要がある。問題はいかなる管理が適切であるか否かであるが、法律的な用語では、管理者に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。その具体的内容は、扱う情報や状況によって異なるものであり、本ガイドラインは、医療情報を電子的に取り扱う際の善管注意義務をできるだけ具体的に示したものである。 医療情報を電子的に取り扱う場合といっても、本来、医療情報の価値と重要性はその媒体によって変化するものではないから、医療機関等の管理者は、そもそも紙やフィルムによる記録を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、電子化された情報は、紙の媒体やフィルムなど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こと、漏えい等の事態	（新設）

が生じた場合に一瞬かつ大量に情報が漏えいする可能性が高いこと、さらに医療者が情報取扱の専門家とは限らないためその安全な保護に慣れていないケースが多いことなど、固有の特殊性もある。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、導入するシステムの機能や運用計画を選択して、それに対し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、昨今のブロードバンドに代表されるような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施設内だけに存在するという状況から、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等にもまたがるようになる。その際、必要となる新たな概念としては責任分界点が挙げられる。 　本章では、電子的な医療情報を取り扱う際の責任のあり方として、医療機関等の管理者の責任の内容と範囲および他の医療機関等や事業者に情報処理の委託や他の業務の委託に付随して医療情報を提供する場合と第三者提供した場合の責任分界点について整理する。	
4.1　医療機関等の管理者の情報保護責任について 　医療機関等の管理者が医療情報を保護するべく善管注意義務を果たすためには、さまざまな局面で注意を払う必要がある。ここでは、医療情報保護の体制を構築し管理する局面での責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合にいかなる対処をすべきかという意味での責任とに分けて解説する。便宜上、本ガイドラインでは前者を通常運用における責任、後者を事後責任とする。 （1）通常運用における責任について	（新設）

ここでいう通常運用における責任とは、医療情報の適切な保護のために医療機関等の管理者が何をすべきかを示す概念である。それは何よりも適切な情報管理ということになるが、実際には、単に適切な情報管理を行っているばかりでなく、そういう体制がきちんととられていることを患者をはじめとする外部に示す責任（説明責任）と、定期的に情報保護システムを評価し改善を図る責任を含む必要がある。 そこで、本ガイドラインにおける医療機関等の管理者の通常運用における責任は、「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３分し、以下にそれぞれの責任内容を整理する。 ①　説明責任 電子的に医療情報を取り扱うシステムの機能や運用計画が、その取り扱いに関する基準を満たしていることを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明確に文書化する必要がある。また、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、その結果もあいまいさのない形で文書化し、また監査の結果問題があった場合は、真摯に対応するのはもちろんのこと、その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。 ②　管理責任 当該システムの運用管理を医療機関等が行う責任である。医療情報を取り扱うシステムの管理を請負事業者にまか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等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、電子情報化された個人情報の保護について一定の知識を有する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 　当該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。特に、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。 　従って、医療機関等の管理者は、医療情報保護のシステムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う必要がある。 （2）事後責任について ①　説明責任 　医療情報について何らかの事故（典型的には漏えいの事態）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責任がある。 　説明は個々の患者に対するものであると同時に、特に医療機関等は一定の公共性を有しているので、監督機関である行政機関や社会への説明・公表が求められている。 ②　善後策を講ずる責任 　医療情報について何らかの事故が生じた場合、医療機関等の管理者には善後策を講ずる責任が発生する。 　その責任は、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に分けられる。 　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、法律上、医療機関等の管理者の善管注意義務については、委託先の事業者の選任監督に適切な注意を払っていれば責任はないことになるが、本ガイドラインの下では、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上記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。	

本章冒頭に述べたように、医療機関等では医療情報の管理を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おり、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、管理者の責任を免れさせるのは不適当と考えられるからである。また、現実的にも、委託先の事業者が医療情報のすべてを管理しているとは限らないから、事故を契機として、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うほかないこともある。 ただし、事故の原因が委託先の事業者にある場合に、医療機関等と当該事業者との間の責任分担をどのようにするかはまた別の問題であり、この問題は次の責任分界点の項目で扱う。	
4.2　責任分界点について 医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託（第三者委託）と第三者提供の２種類があり、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。 委託の場合、それが第三者委託と呼ばれることがあるにしても、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、大きな意味で管理者の支配下にある。前項で述べたように、本ガイドラインでは、患者に対する関係では、委託先の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と整理したところでもある。 これに対し、医療情報の第三者提供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、提供された部分の情報については、もはや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。医療機関等の管理者にとっては、原則として、第三者提供の正当性だけが問題となり、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ことになる。 ただし、情報の特異な性格のため、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	（新設）

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、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。 A. 委託 委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は患者に対する関係では、委託先の事業者の助けを借りながら、前項に掲げた説明責任・管理責任・定期的に見直し必要に応じて改善を行う責任を果たす義務を負い、万一、何らかの事故が生じた場合にも、同様に委託先の事業者と連携しながら説明責任と善後策を講ずる責任を果たす必要がある。 ただし、これとは別に、委託先事業者の責任による事故が生じた場合については、善後策を講ずる責任を医療機関等と委託先事業者との間でいかに分担するか、委託契約で明記しておくべき事項であり、以下にその原則を掲げる。 （1）通常運用における責任について ① 説明責任 医療情報を実際に扱う委託先事業者と医療機関等の管理者との間における説明責任の分担については、次のように考えられる。 患者等に対し、いかなる内容の医療情報保護のシステムが構築されどのように機能しているかの説明責任は、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、委託先事業者による情報提供が不可欠の場合があり、委託先事業者は医療機関等の管理者に対し説明責任を負うといってよい。委託先事業者に対し適切な情報提供義務・説明義務を委託契約事項に含め、その履行を確保しておく必要がある。	

② 管理責任 同様に、管理責任の分担については、次のように考えられる。 管理責任を負う主体はやはり医療機関等の管理者にある。しかし、現実に情報処理に当たりその安全な保守作業等を行うのは、委託先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、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要がある。 ③ 定期的に見直し必要に応じて改善を行う責任 当該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の分担、また、情報保護に関する技術進展に配慮した定期的な再評価・再検討について委託先事業者との契約事項に含めるべきである。 (2) 事後責任について ① 説明責任 前項で述べたように、医療情報について何らかの事故（典型的には漏えいの事態）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責任が求められている。 しかし、情報に関する事故は、説明に際して委託先事業者の情報提供や分析が不可欠な場合が多いと考えられる。そのため予め可能な限りの事態を予想し、委託先事業者との間で、説明責任についての分担を契約事項に含めるべきである。 ② 善後策を講ずる責任 前項で述べたように、医療情報について何らかの事故が生じた場合、医療機関等の管理者には善後策を講ずる責任が発生する。 その責任は、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に分けられ	

る。 事故が委託先事業者の業務範囲と関係する場合、委託先事業者との協力と責任分担の下に上記の責任を果たす必要がある。 既に述べたように、患者に対する関係では、医療機関等の管理者は、委託先事業者の選任監督に十分な注意を払っている場合でも善後策を講ずる責任を免れることはできない。ただし、委託先事業者との間での責任分担はそれとは別の問題であり、特に、事故が委託先事業者の責任で生じた場合、医療機関等の管理者がすべ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事故が生じた場合、医療機関等と委託先事業者の間で責任の押し付け合いをするよりも、まず原因を追及し明らかにすること、そして再発防止策を講ずることが重要であるため、委託契約においては、医療機関等と委託先事業者が協力してこれらの措置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、より詳しく委託先事業者の責任での原因追及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、事故の原因が委託先事業者にある場合、最終的には委託先事業者が負うのが原則である。ただし、この点は、原因がどの程度のものかや、原因究明の困難や、責任分担の定め方によっては原因究明の妨げとなるおそれもあること、あるいは保険による損害分散の可能性など、さまざまに考慮すべき要素があり、それらを考慮した上で、委託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。 B. 第三者提供 医療機関等が医療情報について第三者提供を行う場合、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）第２３条および「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」を遵守する必要がある。 いったん適切・適法に提供された医療情報については提供元の医療機	

関等に責任はない。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するような場合は、提供元の医療機関等の責任が追及される可能性がある。 　また、医療情報が電子化され、ネットワーク等を通じて情報を提供する場合、第三者提供の際にも、医療機関等から提供先へ直接情報が提供されるわけではなく、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、言い換えれば、情報処理関連事業者の処理する段階にある時点で何らかの事故が生じた場合の責任の所在について明らかにする必要が生ずる。 　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みて、患者に対する関係では、少なくとも情報が提供先に到達するまでは、原則として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、情報処理関連事業者および提供先との間で、前項にいうところの善後策を講ずる責任をいかに分担するかは、医療機関等・情報処理関連事業者・提供先の間で予め協議し明確にしておくことが望ましい。選任監督義務を果たしており、特に明記されていない場合で情報処理関連事業者の過失によるものである場合は、情報処理関連事業者がすべての責任を負うのが原則である。	
4.3　例示による考え方の整理 　本項では「4.2　責任分界点について」について、いくつか例を挙げて解説する。ただし、本項は 4.2 の考え方を例として考えた場合であるため、医療情報システムの安全管理や接続時のネットワークの考え方、保存義務のある書類の保存、外部保存が受託可能な機関の選定基準等は、それぞれ 6 章、7 章、8 章を参照すること。 A. 地域医療連携で患者情報を交換する場合 Ⅰ　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	（新設）

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 　提供元医療機関等と提供先機関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も含めて契約などで合意しておく。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管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにしておく。 　ただし、通常運用における責任、事後責任は、委託の場合は、原則として提供元医療機関等にあり、第三者提供において適切に情報が提供された場合は、原則として提供先医療機関等にあり、情報処理関連事業者に瑕疵のない場合は、情報処理関連事業者に生じるのは管理責任の一部のみであ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 　ここでいう独自とは、情報処理関連事業者のネットワークではあるが、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について述べる。 　この場合、あらかじめ提供先または提供先となる可能性がある機関を特定できる場合は、委託または第三者提供の要件に従って両機関が責務を果たさなければならない。 　情報処理関連事業者に対しては、管理責任の分担は発生せず、通信の品質確保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一般的な責任しか存在しない。 　更に、提供元医療機関等と提供先機関が 1 対 N 通信で、提供先機関が一つでも特定できない場合は原則として医療情報を提供できない。ただし、法令で定められている場合等の例外を除く。	

Ⅱ　情報処理関連事業者に対する考え方 ①　医療情報が発信元／送信先で適切に暗号化される場合の責任分界点 　患者情報を送信しようとする医療機関等の情報システムにおいて、送信前に患者情報が暗号化され、情報を受け取った医療機関等の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は盗聴の脅威に対する個人情報保護上の責務とは無関係であり、4.2で述べた責任は限定的になる。 　この場合、情報処理関連事業者に存在するのは管理責任であり、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管理責任の範囲やネットワークの可用性等の品質に関し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　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」を参照されたい。 ②　医療情報が情報処理関連事業者の管理範囲の開始点で適切に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外部からの情報の盗聴や改ざん、侵入等やサービスの可用性等の品質については事業者に管理責任が発生する。従って、それらの責任については契約で明らかにしておく。 　ただし、事業者が提供するネットワーク回線に到達するまでの管理責任やネットワーク回線を流れる情報に対する管理責任は医療機関等に存在するため、「Ⅰ医療機関等における考え方　①医療情報の提供元医療機関等と提供先医療機関等の責任分界点」に則った考え方の整理が必要である。 　なお、ネットワーク回線上と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　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」を参照されたい。	

Ⅲ　外部保存機関が介在する場合の考え方 　この場合、保存する情報は外部保存機関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ける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、外部保存機関とは、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機関を通じて患者情報を交換する場合の医療機関等および外部保存機関に対する考え方は、「8.1.2　外部保存を受託する機関の選定基準および情報の取り扱いに関する基準」で定める保存機関毎に「2. 情報の取り扱い」および「3. 情報の提供」として別途、詳細に規定しているため 8.1.2 を参照されたい。 B. 業務の必要に応じて医療機関等の施設外から情報システムにアクセスする場合 Ⅰ　自機関の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機関の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も一般的になってきた。 　この場合、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間に入って通信回線の両端で一医療機関等の従業者が係わることになる。 　更に、この場合には通信回線がインターネットだけでなく携帯電話網、公衆回線など多彩なものが利用されることになり、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　医療機関等の管理者の情報保護責任について」となることに留意しなくてはならない。 Ⅱ　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 この例のような、リモートログインを用いた保守業者の遠隔保守のためのアクセスが考えられる。この場合、適切な情報管理や情報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可能性もある。他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。 従って、保守の利便性と情報保護との兼ね合いを見極めつつ実施する必要がある。 ただし、この場合でも、当然、医療機関等に対して「通常運用における責任」、「事後責任」が存在するため、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等の監督を行い、管理責任を果たす必要がある。 なお、リモートログインも含めた、保守の考え方については「6.8　情報システムの改造と保守」を参照されたい。 なお、「Ⅰ　自機関の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」、「Ⅱ　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」のどちらにおいても、施設外から情報システムにアクセスする場合のネットワークの考え方については、「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」の、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の外部から接続する場合」を参照されたい。 C. 診療を目的とした第三者委託の場合	

ここでいう第三者委託とは遠隔画像診断、臨床検査、治験等、診療を目的とした第三者委託であり、一時的にせよ情報を第三者が保管する。 委託元である医療機関の管理者は委託先に対して、委託先の選定や委託先への（セキュリティ等の）改善指示を含めた管理責任があるとともに、情報の保存期間の規定等の管理監督を行う必要がある。 ただし、委託先は保存した情報の漏洩防止、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など機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。 D. 法令で定められている場合 法令で定められている場合など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もしくはネットワーク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、当該医療情報の通信経路上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もしく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。	
（削除）	**【参考 1】証拠能力・証明力について** 訴訟における証拠能力・証明力については「高度情報通信社会推進本部制度見直し作業部会報告書　平成 8 年 6 月」に以下のように述べられている。 ①　刑事訴訟 電子データの存在自体を立証する場合は、非供述証拠であり、刑事訴訟法上の伝聞法則の適用はなく、したがって、要証事実との関連性が立

	証できれば証拠能力が認められる。通常、プリントアウトした書面を証拠として提出することになるため、電子データの内容が正確に出力されていることの立証が必要とされている。 　また、電子データの内容の真実性を立証する場合は、供述証拠であり、文書に準ずるものと考えられることから、証拠能力が認められるためには、要証事実との関連性に加え、刑事訴訟法上の伝聞法則の例外が認められるための要件の具備が必要とされている。この場合、商業帳簿等業務の通常の過程において作成された書面については、一般に業務の遂行に際して規則的、機械的かつ継続的に作成されるもので、作為の入り込む余地が少なく、正確に記載されるものと一般に期待されていることから、証拠能力が認められている。これ以外の書面についても特に信用すべき状況の下に作成されていることが認められれば、証拠能力が認められるが、商業帳簿等と同様に信用性の高い書面であることが必要とされている。 　さらに、証明力については裁判官の自由な判断に委ねられているが、その判断は電子データの正確性等の評価に依存するものとされている。 以上から、電子データの証拠能力及び証明力の確保については、データの入力及び出力の正確性を確保するとともに、データの改変の可能性を減殺すること等により電子データの信頼性を高め、かつこれに対する責任の所在を明かにする必要がある。 そのためには、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。 　なお、紙で作成又は受領した証票類の電子化については、紙に記録される紙質、筆跡等の情報が電子データには記録されないため、犯罪捜査・立証上問題が多いと指摘されており、電子データによる保存を認めるに当たっては、その点に十分配意する必要がある。 ②　民事訴訟 　民事訴訟においては、証拠能力についての制限はなく、また、証明力については裁判官の自由な判断に委ねられている。

	電子データによって保存された書類を証拠とする場合、その証明力の判断においては、データの入力及び出力の正確性、データの改変の可能性が問題となり、電子データの信頼性を高め、かつこれに対する責任の所在を明らかにすることが必要であるが、この点については、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。 なお、書類の電子データによる保存の認容をどの程度とするかは、そのデータにより証明しようとする事柄についての挙証責任を官と民のいずれが負担するかについても関係するので、その点も踏まえ、検討することが必要である。 さらに、上記の補足として、医療分野における各種の法令にも留意する必要がある。 例えば、医師等の資格保有者が作成した文書は、医師法、歯科医師法、薬剤師法、医療法等の各種法令により、2 年から 5 年の保存期間が設けられている。保存期間が設けられている文書は財務関係書類等にも見られるが、財務関係書類等と大きく違う点が存在し、医師法を例に挙げれば、第 33 条の 2 の条項がそれにあたる。 この条項は、医師が診療行為を行って診療録を作成しなかった、もしくは 5 年間保存していなかった場合、50 万円以下の罰金刑を科するという条項である。つまり、医師は、診療録そのものを作成・保存していない行為そのものが刑事罰の対象となる。このような厳しい規定は、健康情報を扱う医療分野の特異性といえる。 裁判等で、電子データの証拠能力、証明力を争う場合は、「高度情報通信社会推進本部制度見直し作業部会報告書　平成 8 年 6 月」の見解に加え、このような医療分野に特異な法令も踏まえた上で検討をすることが必要である。
（削除）	**【参考 2】技術的対策と運用による対策** 情報システムの安全を担保するためには、「技術的な対応」と「組織的

	な対応（運用による対策）」の総合的な組み合わせによって達成する必要がある。 技術的な対応は医療機関等の総合的な判断の下、主にシステム提供側（ベンダー）に求められるものであり、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。 総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により基準に適合させることである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化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。 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「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する際の参考資料に利用できる。
【参考】技術的対策と運用による対策 情報システムの安全を担保するためには、「技術的な対応」と「組織的な対応（運用による対策）」の総合的な組み合わせによって達成する必要がある。 技術的な対応は医療機関等の総合的な判断の下、主にシステム提供側（ベンダー）に求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。 総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により一定レベルの安全性を確保することである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化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。 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	（新設）

しているか否かを判断する目安として「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する際の参考資料に利用できる。	

改正案	現　行
5　情報の相互利用性と標準化について 本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において情報処理システムを導入する目的は当初は事務処理の合理化だけであったが、現在は平成 13 年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報の共有の推進や、医療安全、医療の質の向上に寄与できるものであることが求められている。 これらの目的を実現するためには情報の適切な標準化が必要であることは論を待たない。本ガイドラインは医療に関係する情報システムの安全な管理・運用を目的としているが、情報の安全性の重要な要素として、必要時に利用可能であることを確保する可用性を上げることができる。 可用性は情報を保持しなければならない任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い新旧のシステム間での情報の互換性を保ち旧システムで保存された医療情報を確実に読み出せるという、「新旧システムで医療情報の相互利用性」を確保することは、電子保存の見読性及び保存性原則確保の点からみても医療情報システムの必須の要件である。 医療に有用な意味のある情報を長期間にわたり読み出し可能な形で保存するためには、将来にわたりメンテナンスを継続することが期待される標準的な用語集やコードセットを出来る限り利用して保存を行うことが望ましい。 （略）	**5　情報の相互利用性と標準化について** 本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において情報処理システムを導入する目的は当初は事務処理の合理化だけであったが、現在は平成 13 年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報の共有の推進や、医療安全、医療の質の向上に寄与できるものであることが求められている。 これらの目的を実現するためには情報の適切な標準化が必要であることは論を待たない。本ガイドラインは医療に関係する情報システムの安全な管理・運用を目的としているが、情報の安全性の重要な要素として、必要時に利用可能であることを確保する可用性を上げることができる。 可用性は情報を保持しなければならない任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い新旧のシステム間での情報の互換性を保ち旧システムで保存された医療情報を確実に読み出せるという、「新旧システムで医療情報の相互利用性」を確保することは、電子保存の見読性及び保存性原則確保の点からみても医療情報システムの必須の要件である。 医療に有用な意味のある情報を長期間に渡り読み出し可能な形で保存するためには、将来に渡りメンテナンスが継続することが期待される標準的な用語集やコードセットを出来る限り利用して保存を行うことが望ましい。 （略）

改正案	現　行
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	**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**
（略）	（略）
6.2.3　リスク分析 分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、6.3～6.10 の対策を行うことになる。 特に安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障することであり、これが限界である。従って人の行為も含めた脅威を想定し、運用規程を含めた対策を講じることが重要である。 医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。 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	**6.2.3　リスク分析** 分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、6.3～6.10 の対策を行うことになる。 特に安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障するのが限界である。したがって人の行為も含めた脅威を想定し、運用規程を含めた対策を講じることが重要である。 医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。 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 (b)　権限のある者による不当な目的でのアクセス、改ざん

(c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい	(c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん
② （略）	② （略）
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コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい (c) ファイル交換ソフト（Winny 等）の不適切な取扱いによる情報漏えい (d) 情報端末の盗難、紛失 (e) 情報端末の不適切な破棄	（新設）
④ データを格納した可搬型媒体等 (a) 可搬型媒体の持ち出し (b) 可搬型媒体のコピー (c) 可搬型媒体の不適切な廃棄 (d) 可搬型媒体の盗難、紛失	③ データを格納した可搬型媒体等 (a) 可搬型媒体の持ち出し (b) 可搬型媒体のコピー (c) 可搬型媒体の不適切な廃棄 (d) 非可搬型媒体（ハードディスクを搭載したパーソナルコンピュータ等（以下、PC 等という。）の不適切な廃棄
⑤～⑦ （略）	④～⑥ （略）

改正案	現　行
6.3　組織的安全管理対策（体制、運用管理規程）	**6.3　組織的安全管理対策（体制、運用管理規程）**
B. 考え方	**B. 考え方**
安全管理について、従業者の責任と権限を明確に定め、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しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。 ① 安全管理対策を講じるための組織体制の整備 ② 安全管理対策を定める規程等の整備と規程等に従った運用 ③ 医療情報の取扱い台帳の整備 ④ 医療情報の安全管理対策の評価、見直し及び改善 ⑤ 情報や情報端末の外部持ち出しに関する規則等の整備 ⑥ 情報端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その情報端末等の管理規定 ⑦ 事故又は違反への対処 （略） なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報および情報機器の持ち出しについて」に記載しているので参照されたい。	安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。 ① 安全管理対策を講じるための組織体制の整備 ② 安全管理対策を定める規程等の整備と規程等に従った運用 ③ 医療情報取扱い台帳の整備 ④ 医療情報の安全管理対策の評価、見直し及び改善 ⑤ 事故又は違反への対処 （略）
C. 最低限のガイドライン	**C. 最低限のガイドライン**
（略）	（略）

改正案	現　行
6.4　物理的安全対策 **B. 考え方** 物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。 ① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ② 盗難、窃視等の防止 ③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護および措置 なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報および情報機器の持ち出しについて」に記載しているので参照されたい。 （略）	**6.4　物理的安全対策** **B. 考え方** 物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される、情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。 ① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ② 盗難、窃視等の防止 ③ 機器・装置・情報媒体等の物理的な保護 （略）

改正案	現　行
6.5　技術的安全対策 **B. 考え方** 技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。 しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。 (1) 利用者の識別及び認証 (2) 情報の区分管理とアクセス権限の管理 (3) アクセスの記録（アクセスログ） (4) 不正ソフトウェア対策 (5) ネットワーク上からの不正アクセス なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報および情報機器の持ち出しについて」に記載しているので参照されたい。 **(1) 利用者の識別及び認証** （略） **＜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＞** 利用者の識別や認証、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な対策を講じる必要がある。また、万一そのデバイスが第三者によって不正に入手された場合においても、簡単には利用されないようになっていることが重要である。	**6.5　技術的安全対策** **B. 考え方** 技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。 しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。 (1)　利用者の識別及び認証 (2)　情報の区分管理とアクセス権限の管理 (3)　アクセスの記録（アクセスログ） (4)　不正ソフトウェア対策 (5)　ネットワーク上からの不正アクセス **(1)　利用者の識別及び認証** （略） **＜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＞** 利用者の識別や認証、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な対策を講じる必要がある。また、万一そのデバイスが第三者によって不正に入手された場合においても、簡単には利用されないようになっていることが重要である。

従って、利用者の識別や認証、署名等が、これらデバイス単独で可能となるような運用はリスクが大きく、必ず利用者本人しか知りえない情報との組合せによってのみ有効になるようなメカニズム、運用方法を採用すること。	したがって、利用者の識別や認証、署名等が、これらデバイス単独で可能となるような運用はリスクが大きく、必ず利用者本人しか知りえない情報との組合せによってのみ有功になるようなメカニズム、運用方法を採用すること。
（略）	（略）
＜バイオメトリクスを利用する場合の留意点＞ 識別・認証に指紋や虹彩、声紋等のバイオメトリクス（生体計測情報）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現存する各種のバイオメトリクス機器の測定精度は、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）には十分とは言えず、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。 従って、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合せて利用するべきである。 また、生体情報を基に認証するために以下のような、生体情報特有の問題がある。 ・事故や疾病等により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、特徴値が近似することがある ・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)	**＜バイオメトリクスを利用する場合の留意点＞** 識別・認証に指紋や虹彩、声紋等のバイオメトリクス（生体計測情報）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現存する各種のバイオメトリクス機器の測定精度は、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）には十分とは言えず、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合せて利用するべきである。 また、生体情報を基に認証するために以下のような、生体情報特有の問題がある。 ・事故や疾病等により認証に用いる部位の損失等 ・成長等に認証に用いる部位の変化 ・一卵性の双子の場合、特徴値が近似する手法がある ・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)
(2) （略）	**(2)** （略）
(3) アクセスの記録（アクセスログ） 個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。	**(3) アクセスの記録（アクセスログ）** 個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。従って、アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対策を講じなければならない。	アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。したがって、アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対策を講じなければならない。
（略）	（略）
(4)　不正ソフトウェア対策 ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なコードは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正コードの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正コードの侵入に気づくことになる。 対策としては不正コードのスキャン用ソフトウェアの導入が最も効果的であると考えられ、このソフトウェアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正コードの検出と除去が期待できる。また、このことは医療機関等の外部で利用する情報端末や PC 等についても同様であるが、その考え方と対策については、「6.9　情報および情報端末の持ち出しについて」を参照されたい。 ただし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。 たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正コードが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。	**(4)　不正ソフトウェア対策** ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なコードは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正コードの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正コードの侵入に気づくことになる。 対策としては不正コードのスキャン用ソフトウェアの導入が最も効果的であると考えられ、このソフトウェアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正コードの検出と除去が期待できる。 しかし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。 ただし、たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正コードが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。

(5)　ネットワーク上からの不正アクセス ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。 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」および「ステートフルインスペクション」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入れれば安心ということにはならない。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護することが望ましい。システム管理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情報システムに接続される 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　情報および情報端末の持ち出しについて」を参照されたい。 また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ等の対策を講じておく事も重要である。 無線 LAN や情報コンセントが部外者により、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、ウイルス等を感染させたり、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）を行なったり、不正にネットワーク上のデータを傍受したり改ざん等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて PC 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、その事を念頭に置いた上で対策を行なう必要がある。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担保するかが問題であり、特に、“なりすまし“の問題は絶えずついて廻る。また、ネットワーク上を流れる情報の傍受を防止するために、暗号化などによる”情報漏えい“への対策も必要となる。その際、暗号化技術として、	**(5) ネットワーク上からの不正アクセス** ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。 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」および「ステートフルインスペクション」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入れれば安心ということにはならない。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護することが望ましい。システム管理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。 また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ等の対策を講じておく事も重要である。 無線 LAN や情報コンセントが部外者により、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、ウイルス等を感染させたり、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）を行なったり、不正にネットワーク上のデータを傍受したり改ざん等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて PC 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、その事を念頭に置いた上で対策を行なう必要がある。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担保するかが問題であり、特に、“なりすまし“の問題は絶えずついて廻る。

容易に解読されない手法を選択する必要がある。 昨今は無線 LAN を用いてコンピュータをネットワークに接続する構成にしている医療機関等も見受けられる。無線 LAN は、看護師などが使用する情報端末を利用し患者のベッドサイドで作業する場合などに利便性が高い反面、通信の遮断など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、それとは別に、無線電波により重大な影響を被るおそれのある機器などへの利用には注意が必要である。 また、最近では、電力線搬送通信（PLC：Power Line Communication）が利用可能になった。しかし、医療機関等において PLC 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」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。	
C. 最低限のガイドライン	**C. 最低限のガイドライン**
1. （略） 2. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。 3. ～7. （略） 8. 無線 LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否などの対策をとること。 (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えば、WPA/TKIP、WPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こ	1. （略） 2. 動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意すること。 3. ～7. （略） （新設）

り得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 適用に関しては、総務省発行の「安心して無線 LAN を利用するために」を参考にすること。	
D. 推奨されるガイドライン	**D. 推奨されるガイドライン**
1. ～4. （略）	1. ～4. （略）
5. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクション）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。	5. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクション）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。 また、無線 LAN を用いる場合はリスクの増大を慎重に考慮し、総務省発行の「安心して無線 LAN を利用するために」を参考にし、暗号化や容易に推測できない SSID を用いる等、情報資産の評価にもとづき適切な配慮をおこなうこと。
6. （略）	6. （略）
7. 認証に用いられる手段としては、ID＋バイオメトリックスあるいは IC カード等のセキュリティ・デバイス＋パスワードまたはバイオメトリックスのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用することが望ましい。 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は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化が望まれる。	7. 認証に用いられる手段としては、ID＋バイオメトリックスあるいは IC カード等のセキュリティ・デバイス＋パスワードまたはバイオメトリックスのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用することが望ましい。

改正案	現　行
6.6　人的安全対策 **B. 考え方** 医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。 医療情報システムに関連する者として、次の 5 種類を想定する。 (a) 医師、看護師等の業務で診療に係わる情報を取扱い、法令上の守秘義務のある者 (b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元に医療情報を取扱い、守秘義務を負う者 (c) システムの保守業者等の雇用契約を結ばずに診療を維持するための業務に携わる者 (d) 患者、見舞い客等の医療情報にアクセスする権限を有しない第三者 (e) 診療録等の外部保存の委託においてデータ管理業務に携わる者 このうち、(a) (b)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の２つに分けて説明する。 (d)の第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏えい等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。 (e)については、いわゆる「外部保存」の委託先の機関等に該当するが、これに関しては詳細を 8 章に記述する。 （略）	**6.6　人的安全対策** **B. 考え方** 医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。 医療情報システムに関連する者として、次の 5 種類を想定する。 (a) 医師、看護師等の業務で診療に係わる情報を取扱い、法令上の守秘義務のある者 (b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元に医療情報を取扱い、守秘義務を負う者 (c) システムの保守業者等の雇用契約を結ばずに診療を維持するための業務に携わる者 (d) 患者、見舞い客等の医療情報にアクセスする権限を有しない第三者 (e) 診療録等の外部保存の委託においてデータ管理業務に携わる者 このうち、(a) (b)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の２つに分けて説明する。 (d)の第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏洩等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。 (e)については、いわゆる「外部保存」の委託先の機関等に該当するが、これに関しては、その主旨と実施の詳細を 8 章に記述する。 （略）

改正案	現　行
6.7　情報の破棄 **B. 考え方** 医療に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もある。 実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化したものを作成しておくべきである。 外部の委託機関等に保存を委託している診療録等について、その委託の終了により診療録等を破棄する場合には、速やかに破棄を行い、処理が厳正に執り行われたかを監査する義務（または 監督する責任）を果たさなくてはならない。また、受託先の機関等も、委託元の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、処理を行った旨を明確に示す必要がある。 （略）	**6.7　情報の破棄** **B. 考え方** 医療に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報がお互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もある。 実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化したものを作成しておくべきである。 外部の委託機関等に保存を委託している診療録等について、その委託の終了により診療録等を破棄する場合には、速やかに破棄を行い、処理が厳正に執り行われたかを監査する義務（または 監督する責任）を果たさなくてはならない。また、受託先の機関等も、委託元の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、処理を行った旨を明確に示す必要がある。 （略）

改正案	現　行
6.8　情報システムの改造と保守 （略） **C. 最低限のガイドライン** 1. ～7　（略） 8. リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずアクセスログを収集すると共に、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。 （略）	**6.8　情報システムの改造と保守** （略） **C. 最低限のガイドライン** 1. ～7　（略） 8. リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること。 （略）