4　電子的な医療情報を扱う際の責任のあり方

医療従事者等には刑法の規定及び関係法令が定める秘密保持義務に関する規定に基づいて守秘義務が課されている。図 7 に示されるように、患者との信頼に基づいて知りえた医療情報を受託管理する情報処理事業者では、医療機関等の負う重い責任に配慮し、十分に安全性、信頼性の確保に努めること。

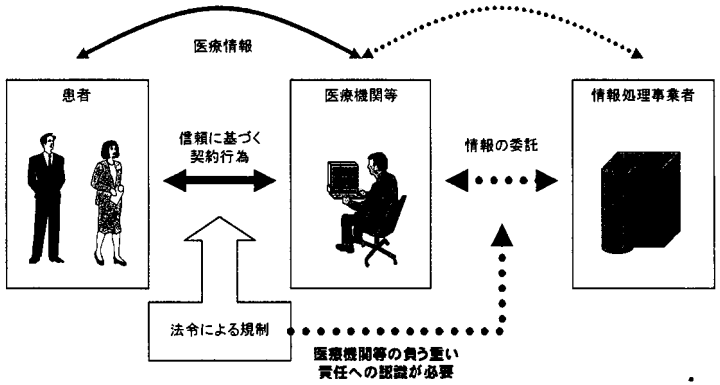

図 7 患者と医療従事者と情報処理事業者の責任関係

医療情報安全管理ガイドラインには「外部保存を委託する医療機関等は保存を受託する機関、搬送業者に対して個人情報保護法を順守させる管理義務を負う。したがって、両者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上明記すること。」とある。ここでは情報保護に関する情報処理事業者の責任と、医療機関と情報処理事業者との責任分界点の考えについて示す。

4.1　情報処理事業者の管理者における情報保護責任について

本ガイドラインで対象とする情報処理業務は、医療機関等から医療情報の保存及び運用管理を委託される場合のみである。この場合においては情報の提供者である患者等に対する医療情報の管理責任は一義的には医療機関等にあり、情報処理事業者との委託契約と監督責任を通じてこの責任を果たす責務があると考えられる。しかし、情報処理事業者においても、医療情報という機微性の高い情報を扱うことから、医療機関等の負う責任の一端を共有していると考えるべきであり、扱う個々の情報の価値、リスク、責任について受託元の医療機関等と考えを共通した上で、システム仕様、運用計画、事業継続計画等に合意することが重要である。

医療情報安全管理ガイドラインでは、医療機関における管理者の善管注意義務[29]を果たすための責任を「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」とに分けて記述している[30]。

「不都合な事態」により損害が発生した場合には損害填補責任が生じる。委託契約においては医療機関等と情報処理事業者との責任分担を予め考慮しておく必要があることから、本ガイドラインにおいては、責任分界点に関する考えとともに、上記の分類で、情報処理事業者にとって善管注意義務を果たすための責任を記述する。

4.2　通常運用における責任について

医療情報の適切な保護のために情報処理事業者側の管理者が実施すべき安全管理策は「通常運用における責任」である。医療情報安全管理ガイドラインでは、この責任を「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」の三つであるとしている。医療機関等の管理者が担うそれぞれの責任に対応して、情報処理事業者が配慮すべき事項について述べる。

(1) 説明責任

医療機関等の管理者においては「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、その取扱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。（医療情報安全管理ガイドライン）」とされている。情報処理事業者にとっても医療機関等に対して同様の責任があると考え、医療情報処理に関わるシステム文書として、ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと、定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果

[29] 社会通念上、善良なる管理者として果たすべき注意義務
[30] 情報漏洩の他にもサービス不能攻撃、コンピュータウイルスの感染等が想定される

及び是正措置報告についても提出可能な状態におくこと等を委託契約事項に含め、履行する必要がある。

(2) 管理責任

医療機関等の管理者においては「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。(医療情報安全管理ガイドライン)」とされている。情報処理事業者は医療機関等から委託を受けてシステムの運用管理を行うことから、運用状況及び管理状況について定期的に報告し、医療機関等から意見又は指摘を受けることが求められる。

(3) 定期的に見直し必要に応じて改善を行う責任

医療機関等の管理者においては「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。(医療情報安全管理ガイドライン)」とされている。情報処理事業者は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った上で医療機関に報告し、医療機関等から意見又は指摘を受けることが求められる。

4.3 事後責任について

ここでは情報処理事業者の責任範囲において「何らかの不都合な事態」が生じた際の対応に関わる責任について述べる。

(1) 説明責任

医療機関等の管理者においては「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。(医療情報安全管理ガイドライン)」とされている。情報処理事業者においては、事態の発生を認識次第、ただちに医療機関等に通知し、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために、協力して情報収集を図ることが求められる。加えて、発生しうる事態を想定した説明責任の分担を契約事項として含める必要がある。

(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、速やかに善後策を講じなければならない。そのためには、前もって発生しうる事故と考えられる原因を洗い出して対応手順を策定しておくことが必要である。また、事故に対する緊急対応が完了した後で原因を確定するために、事故発生時の状況を保存あるいは記録する手順、対応過程で行われた作業を記録する手順等も策定しておくことが求められる。加えて、確定された原因に基づき再発防止策を講じることも求められる。

(3) 再委託先に対する責任

外部データセンター、バックアップ施設の運用管理等、一部の情報処理業務を再委託している場合、再委託先あるいは再委託している情報処理業務において発生した事態に関する責任については、医療機関との契約において第一義に委託先である情報処理事業者が負うべきであると考えられるが、再委託先の事業者においても責任は発生していると考えられる。互いの責任の範囲について合意し、再委託先との契約で明記しておくことが求められる。

4.4　ネットワーク利用時における回線事業者との責任分界点について

情報処理にネットワークを利用する際には、医療機関等と情報処理事業者を接続する回線事業者が介在し、回線上に発生した障害等については回線事業者にも責任が生じる場合があると考えられる。

医療機関等と情報処理事業者の間をインターネット上に構築した VPN で接続する場合、VPN を構成する装置の管理を医療機関等あるいは情報処理事業者が行う場合には、回線上の安全管理は VPN 装置で担保されるものであるから、回線事業者は安全管理上の責任を負わないと考えられる。また、インターネット VPN は複数の回線事業者が構成するもので、品質保証を行うことができないことから、直接の契約関係にない回線事業者で発生したインターネット VPN 上の障害についての責任を誰かに負わせることはできない。インターネット VPN を利用する場合には、このようなリスクもあることを考慮すること。ただし、回線事業者がインターネット VPN を提供する場合には、VPN 装置含め、回線に起因する障害の責任は回線事業者が負うべきものである。

医療機関等と情報処理事業者の間を、閉域網 VPN 又は専用線で接続する場合には、回線の品質、帯域、稼働率等に一定の保証があることから、回線上の障害の責任は回線事業者が負うべきである（一般には接続用ルータなどの終端機器までが責任範囲となる）。

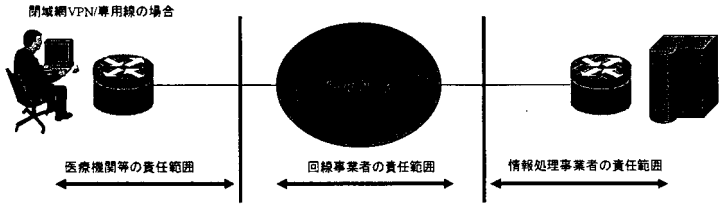

図 8 閉域網/専用線利用時の責任分界点

いずれの形態においても、医療機関等と情報処理事業者、回線事業者の責任について、想定される障害等のそれぞれについて契約に明示するなどの対策を行うこと。

5　医療情報の取扱に関する知識

診療録等の医療情報の取扱については医師法、歯科医師法、薬剤師法等の法令によって定められている。昭和 63 年 5 月通知「診療録等の記載方法について[31]」により「作成した医師、歯科医師又は薬剤師の責任が明白であれば、ワードプロセッサ等所謂 OA 機器により作成することができる」こととされた。この段階では紙文書を OA 機器で作成することについて規定されているのみで、電磁的記録として保管することについては規定されていなかった。

その後、平成 11 年 4 月通知「診療録等の電子媒体による保存について」により診療録等の電子媒体による保存について基準が示され電磁的記録を電子媒体の形で保存することが認められた。この段階では、必要に応じて利用する情報として、電磁的記録を作成した医療機関等内に保存を行うものという認識がもたれていた。

さらに、ネットワーク環境が一般的なものとなったことを受けて、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。この段階において、一定の基準を満たすことを条件に、診療録等の医療情報を電磁的記録として医療機関等外部の施設に保存することが可能となった。ただし、この段階では施設とは病院又は診療所に準ずるものという規定であった（安全管理レベルを医療機関等と同等以上にするということ）。

さらに、平成 17 年 3 月通知「「診療録等の保存を行う場所について」の一部改正について[32]」（以下「外部保存改正通知」という。）にて、危機管理上の目的であれば外部のデータセンターをハウジング（サーバラック等を設置する場所を借りることでサーバ機器類は医療機関等自身で所有管理するものを設置する）利用して医療情報を保管することが許されるようになった。このような医療情報の取扱に関する経緯を表 3 にまとめる。

表 3 医療情報の取扱に関する経緯

時期	法令名称	内容
1988 年（昭和	診療録等の記載方法	診療録等についてOA機器を使って電磁的に作成することが認められた。ここでは紙に出力するために

31 昭和 63 年 5 月 6 日付け厚生省健康政策局総務・指導・医事・歯科衛生・看護・薬務局企画・保険局医療課長、歯科医療管理官連名通知

32平成 17 年 3 月 31 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知

63年)	について	OA機器を用いるという観点である。
1999年(平成11年)	診療録等の電子媒体による保存について	電磁的記録を電子媒体で保存することが認められた。電子媒体は作成した医療機関等内で保管する。
2002年(平成14年)	診療録等の保存を行う場所について	一定の基準を満たすことを条件に、診療録等の医療情報を電磁的記録として医療機関等外部の施設に保存することが可能 (ただし病院又は診療所に準ずる施設に限る)。
2005年3月(平成17年3月)	「診療録等の保存を行う場所について」の一部改正について	「医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」であれば外部のデータセンター等に医療情報を保管することが許される。
2005年3月(平成17年3月)	民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について	「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[33]」及び「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[34]」により「診療録等の電子媒体による保存について[35]」は廃止となった。

これらの通知・省令及びガイドライン類は平成17年に策定された医療情報安全管理ガイドラインに反映・統合されている。

33 平成16年法律第149号
34 平成17年厚生労働省令第44号
35 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

5.1 法令・通知

以下に、医療情報の取扱に関する法令・ガイドライン類を示す。医療情報の外部保存業務を請け負うことになる情報処理機関は、これらの法令・ガイドラインについて詳細を把握し、示される基準を満たすよう、対策を行うことが求められる。

- 「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)
- 「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」(平成16年12月24日通達、平成18年4月21日改正)
- 「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)
- 「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」(平成17年3月31日付け医政発第0331009号・薬食発第0331020号・保発第0331005号厚生労働省医政局長・医薬食品局長・保険局長連名通知)
- 「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)
- 「「診療録等の保存を行う場所について」の一部改正について」(平成17年3月31日付け医政発第0331010号・保発第0331006号厚生労働省医政局長・保険局長連名通知)

これらの法令・ガイドライン類を反映・統合した医療情報安全管理ガイドライン策定の経緯を図9にまとめた。

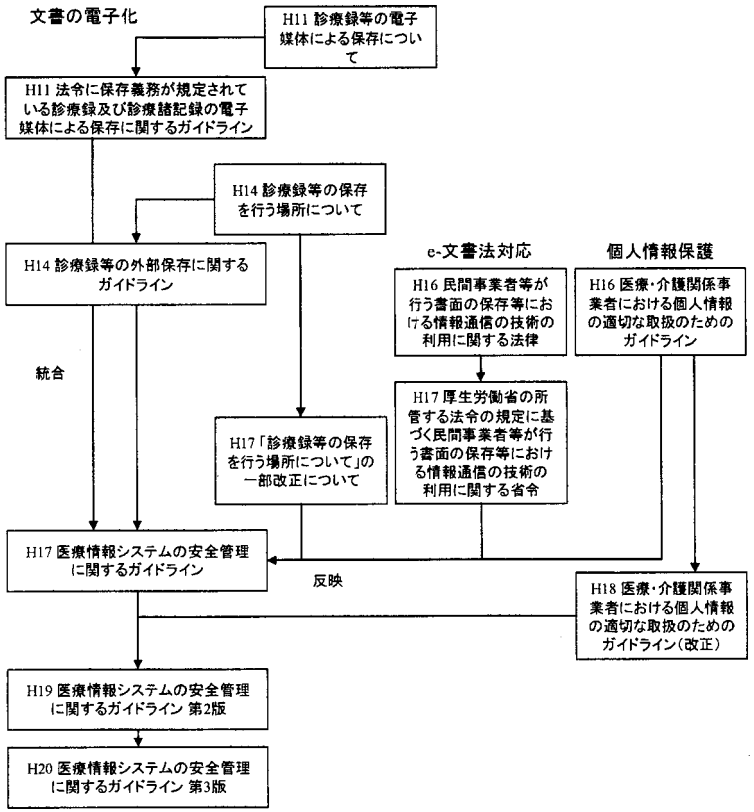

図 9 医療情報の電子記録に関する通知・省令及びガイドライン類の策定経緯

図で示されるように、文書の電子化、e-文書法対応、個人情報保護法対応といった大きな流れを反映しているものである。

なお、医療情報の電子的な扱いについては図 10 に示されるような区分が定められている。本ガイドラインで扱う医療情報とは「外部保存が許されている情報」が主なものとなる。

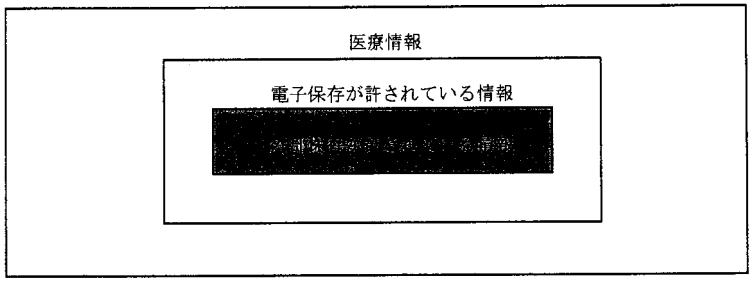

図 10 医療情報の電子的扱いに関する区分

電子保存が許されている文書及び外部保存が許されている文書は以下のものである。

表 4 電子保存及び外部保存が許されている文書

1	医師法(昭和 23 年法律第 201 号)第 24 条の規定による診療録	○	○
2	歯科医師法(昭和 23 年法律第 202 号)第 23 条の規定による診療録	○	○
3	保健師助産師看護師法(昭和 23 年法律第 203 号)第 42 条の規定による助産録	○	○
4	医療法（昭和 23 年法律第 205 号）第 52 条の規定による財産目録及び貸借対照表並びに損益計算書	○	○
5	歯科技工士法(昭和 30 年法律第 168 号)第 19 条の規定による指示書	○	○
6	薬剤師法(昭和 35 年法律第 146 号)第 28 条の規定による調剤録	○	
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十七条及び歯科医師法第十七条の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条の規定による診療録	○	○
8	救急救命士法(平成 3 年法律第 36 号)第 46 条の規定による救急救命処置録	○	○
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 項の規定による帳簿	○	○
10	保険医療機関等及び保険医療養担当規則(昭和 32 年厚生省令第 15 号)第 9 条の規定による診療録等	○	○

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 条の規定による調剤録	○	
12	臨床検査技師、衛生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 の規定による書類	○	○
13	医療法（昭和 23 年法律第 205 号）第 21 条第 1 項の規定による記録（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 条の規定による記録（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。）、及び第 22 条の 2 の規定による記録（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 号に処方せんに限る。） なお、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については外部保存も可とされている。	○	○
15	薬剤師法(昭和 35 年法律第 146 号)第 27 条の規定による処方せん	○	
16	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 条の規定による処方せん	○	
17	医療法(昭和 23 年法律第 205 号)第 21 条第 1 項の規定による記録(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。)、第 22 条の規定による記録（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。）、及び第 22 条の 2 の規定による記録（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。）	○	
18	歯科衛生士法施行規則(平成元年厚生省令第 46 号)第 18 条の規定による歯科衛生士の業務記録	○	○
19	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	○	○

6　電子保存の要求事項について.

医療情報を電磁的記録として電子保存する際の要求事項として、真正性、見読性、保存性の三点が規定されている。ここでは、情報処理事業者として確保すべき要求事項を、真正性、見読性、保存性のそれぞれについて述べる。

6.1　真正性の確保に関する要求事項

「診療録等の電子媒体による保存について[39]」にて示される、医療情報を取り扱う上で医療従事者に求められている要件の一つに真正性がある。医療情報安全管理ガイドラインによれば、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と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていること」とされる。情報セキュリティの概念としては完全性（integrity）が近いものであるが、それ以上の概念である。このうち、「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と所在が明確」であることは、情報を作成する医療従事者及び医療機関等が確保すべきことである。そのため、情報記録者が誰であるのかについて電磁的記録として認識できるよう、文書フォーマット等について医療機関等と十分な合意を形成しておくべきである。

「虚偽入力、書き換え、消去、及び混同が防止されていること」に関しては、まず、情報の受入れ時に正しい情報であることを確認すること。このためには医療機関等側で情報を生成した際に電子署名を付与しておくことが求められる。情報を受入れた情報処理事業者は電子署名を検証することで情報が通信路上で変更されていないことを確認できる。

受入れ後はハードディスク等の固定記憶媒体に情報を書き込んで保存する。記憶媒体は定期的に検査を行い認可されていない着脱が行われていないことを保証する。また、記憶媒体上の情報に対しては、認可されていない書き込み、削除が行われないように、アカウント管理、アクセス権限管理を行い、定期的に電子署名を検証する等の作業により改ざんの検出を行う。情報の預け主である医療機関等の要請により情報を提供する際にも電子署名を検証して改ざんの検出を行い、正しく元の情報を提供する。

[39] 平成 17 年 3 月 31 1 7 年 3 月 3 1 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知

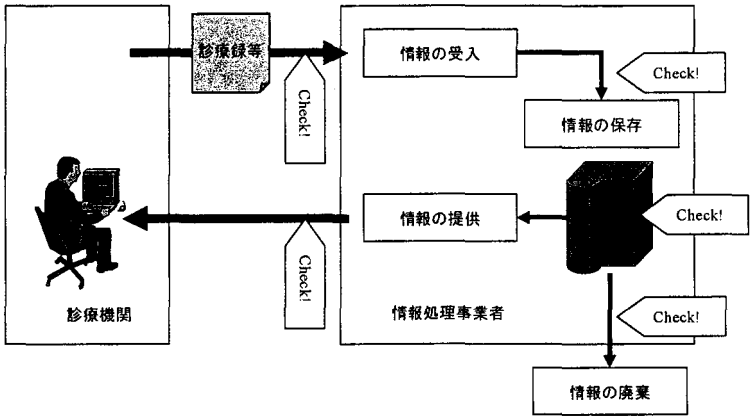

図 11 情報の生成（登録）から廃棄まで（各チェックポイントで改ざんを検査）

なお、情報の廃棄に関しては医療機関からの依頼により行うことであり、処理が厳正に執り行われたことを医療機関に対し証明する必要がある。

6.2 見読性の確保に関する要求事項

二つ目の要件に見読性がある。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」とされる。情報セキュリティの概念としては可用性（availability）が近いものであるが、それ以上の概念である。本ガイドラインで想定するシステム構成は図 2 に示すものであり、見読する現場は医療機関等側となる。情報処理設備との間にはネットワークが介在することから、ネットワークの可用性について十分に検討する必要がある。特に、データ容量が大きい高精細デジタル画像である医用画像（レントゲンデータ等）を扱う場合は、ネットワークの回線容量について配慮しておくこと。

診療は 24 時間 365 日行われるものであるため、情報処理事業者においても同様にサービス提供を行う必要がある。ここで特に考えるべきこととして、医療機関等は広域災害等の非常事態においてサービスの継続が市民生活に大きく影響する重要インフラの一つであるということである[40]。通常の情報処理事業者ではサービス提供継続が困難となる状況こそ、医療機関等においては情報処理の継続が不可欠となるということである。このため、医療機関等に情報処理機能を提供する事業者は、自らも重要インフラの一部に相当するという意識を持ち、適切な事業継続計画を策定すること。

また、システムの更新、アプリケーションの変更等に伴い、電子保存された医療情報の読み出しに関する互換性を失わないように配慮することが求められる。そのためには、標準が存在するデータ形式を採用する、データについては標準的な用語集を活用する、文字コードを国際標準に統一する等の対策を考慮すること。

[40] 「重要インフラの情報セキュリティ対策に係る行動計画」平成 17 年 5 月情報セキュリティ政策会議決定

6.3　保存性の確保に関する要求事項

保存性とは「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」とされる。具体的には情報の損傷に対する備えを意味すると考えられる。医療情報安全管理ガイドラインで列挙されている保存性を脅かす原因ごとに要求事項を上げる。

- 「ウイルスや不適切なソフトウェア等による情報の破壊及び混同等」に対しては「7.7.3 悪意のあるコードに対する管理策」等に準拠すること。
- 「不適切な保管・取扱による情報の滅失、破壊」に対しては 7.6.2 情報処理システムへの入退館、入退室に関する要求事項」、「7.6.3 情報処理装置のセキュリティ」等に準拠すること。
- 「記録媒体、設備の劣化による読み取り不能又は不完全な読み取り」に対しては「7.7.7 媒体の取扱」等に準拠すること。
- 「媒体・機器・ソフトウェアの整合性不備による復元不能」及び「(5)　　障害等によるデータ保存時の不整合」に対しては「7.11 医療情報処理に関する事業継続計画」等に準拠すること。

なお、ハードディスク等の記憶装置については利用に耐えうる耐用期間が製造ベンダにより定められているので、その耐用期間を越えないよう及び事業に支障を来たさないよう余裕を持った交換計画を策定しておくこと。

7　医療情報を受託管理する情報処理事業者における安全管理上の要求事項

一般的な情報と比較して機密性が極めて高く要求される医療情報の取扱は、医師法、歯科医師法、薬剤師法、医療法等、法令において医療行為及び従事者の職務として規定されている。医師の職務に関して規定する医師法第 24 条では、「医師は、診療をしたときは、遅滞なく診療に関する事項を診療録に記載しなければならない。前項の診療録であって、病院又は診療所に勤務する医師のした診療に関するものは、その病院又は診療所の管理者において、その他の診療に関するものは、その医師において、五年間これを保存しなければならない。」とされている。これに対して「第二十四条の規定に違反した者」に対する罰則も「五十万円以下の罰金に処する（同法第 33 条の 2)」と規定されている。通常の業務であれば、業務記録を作成しなかったからといって刑罰に処されることは考えにくい。このような厳しい規定は、生命に関わる情報を扱う医療分野の特異性といえる。

医療情報の取扱については、法令の規定外となるような医療情報の取扱が行われないように、情報処理事業者は配慮を行う義務がある。また、情報を取り扱う上での、真正性、見読性、保存性を確保することが求められており、これらを合わせて、情報処理事業者への要求事項と考えることができる。本章では、これらの要求事項を満たすために情報処理事業者が実装すべき又は実装することが望ましい安全管理策について示す。

7.1　医療情報に係る情報処理事業を受託する上で推奨される認証及び認定

医療情報安全管理ガイドラインでは、外部情報保存受託機関に対して「プライバシーマーク制度や不足なく適用範囲を定めた適用宣言書に基づく ISMS 認定制度等による公正な第三者の認定を受けていること」としている。医療情報の秘匿性の高さを考えれば、この方針は必要と考えられる。本ガイドラインにおいても同様にプライバシーマーク認定・ISMS 認証等の公正な第三者の認定を取得することを必要な要件とする。

本ガイドラインでは ISMS 認証の取得時に役立つように、安全管理策を「7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項」において、JIS Q 27001 に沿った形で具体的に示すという構成をとる。

7.1.1　ISMS 認証取得時の考慮事項

情報処理事業者が医療情報処理の安全確保を目的として ISMS 認証を取得する場合には、医療情報処理システムの開発、運用に関わる部門、部署、及び受託した医療情報を扱う部門、部署を含むよう適用範囲を設定した上で ISMS 認証を取得することが求められる。すでに ISMS 認証を取得しているが適用範囲が上記部門、部署全体をカバーしていない場合は、適用範囲を再設定して取得しなおすことが求められる。加えて、医療情報処理システムに対しては、本ガイドラインで示される安全管理策を基準とした第三者機関による情報セキュリティ監査等を定期的に（少なくとも一年に一回以上の頻度で）実施して、十分な情報セキュリティレベルを確保していることを検証することが望まれる。

医療情報の高い機微性、完全性の要求を鑑みて、通常の ISMS 認証取得プロセス、維持プロセスに加え、以下の要件を満たすよう本ガイドラインを活用すること。

推奨される安全管理策

- 認証取得あるいは更新の際に ISMS の安全管理策として、本ガイドライン「7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項」にて提示する安全管理策を盛り込むことが望ましい（この安全管理策は医療情報安全管理ガイドラインで規定される医療機関等側と同等以上の安全管理措置として提示されている）。
- 受託管理する医療情報の入り口から出口まで包括的に ISMS の適用範囲とすることが望ましい。
- 安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくことが望ましい（適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること）。

本ガイドラインの要求事項を満たすために実施すべき作業を ISMS ユーザーズガイド JIS Q 27001:2006(ISO/IEC 27001:2005)対応[41]に記される ISMS 構築の 10 の STEP に対応する形で表 5 に示す。

表 5 ISMS 構築の 10 の STEP

ISMS 構築の STEP	対応する作業
1 ISMS の適用範囲及び境界を設定する	受託管理する医療情報の入り口から出口までを包括するように適用範囲を設定し、適用範囲外との境界を明確にする
2 ISMS の基本方針を策定する	医療情報の特性に合わせた管理を行っていることを基本方針で示す
3 リスクアセスメントの取組方法を策定する	ISMS で行うリスクアセスメント同等に行う
4 リスクを識別する	取り扱う医療情報の性質、配慮事項を精査し、リスクを正しく識別する
5 リスクを分析し評価する	リスク対策として残留リスクを受け入れる際の基準を文書化し、顧客となる医療機関等に明示しておくこと
6 リスク対応を行う	識別評価した各リスクに対し、適切に、低減、回避、移転、受容を選択する
7 管理目的と管理策を選択する	本ガイドライン 7 章にて提示する安全管理策を盛り込む
8 残留リスクを承認する	残留リスクの最新の値を常に把握し、値が閾値を越えた場合には、直ちに対策をとる、あるいは顧客となる

41 （財）日本情報処理開発協会（http://www.isms.jipdec.jp/）

	医療機関等から受入れしがたいという意見を受けた場合には適切に対処を行う
9 ISMS の実施を許可する	情報処理事業者のマネジメント層が、構築したシステム、体制について、本ガイドラインへの準拠を確認し、医療情報処理業務に対する ISMS の実施を承認する
10 適用宣言書を策定する	医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくこと

7.1.2 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

医療情報を受託管理する業務を行う情報処理事業者が ISMS 認証を取得する際には、図 12 に従って、その適用範囲及び管理策が本ガイドラインで示す基準に従っているかどうか確認し、必要であれば再（拡大）審査を受けることが望ましい。

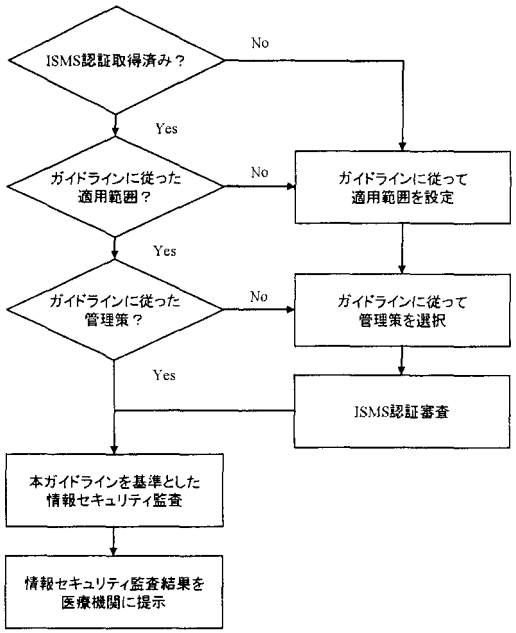

図 12 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

また、本ガイドラインに従って ISMS 認証を取得した後に第三者による情報セキュリティ監査等を受け、監査結果を医療機関に提示することが望まれる。

7.2 原則として行うべきではない行為

安全性の観点から、医療情報を扱う情報処理業務、情報処理システムにおいて原則として行うべきではないと考えられる行為を以下にあげる。理由があって行わざるを得ない場合には、そのリスクについて医療機関等に説明し、合意を得ること。

- 情報処理事業者施設において無線 LAN を利用すること

  原則として医療情報処理システムは無線 LAN を使う必要性が無いように近接して配置すること。

- 情報処理事業者がリモートアクセスにより情報処理システムを運用管理すること

  情報処理システムの稼働を監視するために専用回線にてアクセスする場合、あるいはファイアウォール、侵入検知システム（IDS[42]）及び侵入防止システム（IPS[43]）等のセキュリティ機器に対する不正アクセス監視の場合は除く。その場合、外形的な監視に留めリモートからシステムにログオンしての作業は行わないことが望ましい。

- 情報処理システムにおいて電子メール、ワードプロセッサ、プレゼンテーションツール等、汎用アプリケーションを利用すること。

  不要なリスクを避けるため、医療機関等との医療情報以外の情報交換に電子メールを使う際には別系統のネットワーク及び情報処理システムを用いること。

[42] Intrusion Detection System
[43] Intrusion Prevention System

7.3 情報資産管理

本ガイドラインで示す情報処理業務においては医療機関等から預かる情報個々の分類を正確に行う必要がある。情報の種別等を記載した台帳等を作成し、その管理を厳密に行うこと。なお、当該台帳には患者情報等、個人を特定できる情報を含まないよう、記載情報の構成に留意すること。

7.3.1 資産台帳

受託管理する医療情報が完全な状態にあることを確実にするため、情報処理事業者自身の医療情報処理システム（システム構成、ネットワーク構成等）に加え、医療機関等から預かった情報についても資産台帳等を作成し管理する必要がある。

医療情報が完全な状態にあることを保証するために資産台帳等を適切に維持管理することを目的として、以下の管理策を適用すること。なお、資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること。

実施すべき安全管理策

- 重要な情報について資産台帳等を作成管理すること。
- 資産台帳等には少なくとも次の情報を記録すること。
  - 資産の種別
  - データ形式
  - 資産の所在地と複製の可否及び複製の所在地
  - 資産価値[44]
  - 資産を扱う業務の概要
  - 情報処理事業者における資産の所有者及び管理責任者
  - 設定されたアクセス権限とアクセス権限者
  - 資産の発生日時、保有する期限、廃棄予定日
  - 資産に対する処理の履歴（保存、配送、閲覧、廃棄等）

[44] 資産価値の算定手法としては ISO/IEC TR 13335（The Guidelines for the management of IT Security）Part3：Techniques for the management of IT Security 等を参照すること

- 資産台帳等の情報が正確であるよう管理手続きを規定すること。
- 資産台帳等へのアクセスを制限し、アクセス制限を侵害する行為について記録すること。
- 資産台帳等の他に、情報処理に関わる機器及びソフトウェアについては構成図、一覧表（仕様、バージョン番号含む）を整備し、医療機関等の要請に応じて即座に提出できるように準備すること。

7.3.2 情報の分類

情報の保護の程度を識別するため、情報のそれぞれについて適切な分類を行い、外形的に分類が判断できるようにしておくことが必要である。以下の管理策を適用すること。

実施すべき安全管理策

- 情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。
- 情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。
- 分類がわかるように情報にラベルをつけること（電磁的な情報にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。
- 各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。
- 情報の処理について履歴を取得し、資産台帳等に記録すること。

7.4 組織的安全管理策（体制、運用管理規程）

情報処理事業者は医療情報処理に関与する要員の責任を規定し、各処理について手順書を整備するといった安全管理策を策定する必要がある。

情報処理機器等の管理責任を明確にすることで管理作業が正しく遂行されることが確実になる。以下の管理策を適用すること。

実施すべき安全管理策

- 情報処理に関わるハードウェア、ソフトウェアのそれぞれについて責任者を割り当て、文書化して管理すること。
- 情報処理に関わるハードウェア、ソフトウェアを導入する際には、目的、用途等について文書化し、適切な承認を受ける手続きを整備すること。この手続きには「7.7.1 情報処理装置及びソフトウェアの保守」に定める変更管理プロセスが含まれる。
- 情報処理の安全管理に関わる手順書、運用管理規程を整備すること。
- 運用管理規程には、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理機器の管理、第三者による情報セキュリティ監査等について記載しておくこと。

7.5　医療情報の伝達経路におけるリスク評価

医療情報の取扱に際しては機密性が極めて高いことに配慮しなければならない。第一に医療情報の移動する範囲を限定することが必要である。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うことが要求される。

「3 本ガイドラインの対象システム及び対象情報」で示したように、想定される医療情報の交換経路は三種類である。

医療情報を電磁的記録の形で電子媒体（CD、DVD、MO 等）に格納して物理的に運搬して交換する場合における経路と、そこで想定される脅威を示す。

表 6 医療情報を電磁的記録の形で電子媒体に格納して物理的に運搬する際の脅威

情報が移動する経路	想定される脅威
医療機関等からの配送経路	配送先を誤って指定して第三者に配送される（誤配送） 第三者が配送業者になりすまして不正に情報を入手する 配送途中に盗まれる・すりかえられる 配送中に損傷を受け利用できない状態になる
事業者側配送受入れ領域	第三者が職員になりすまして不正に情報を入手する
建物内の移動	第三者が職員になりすまして不正に情報を入手する 配送途中に盗まれる・すりかえられる 配送中に損傷を受け利用できない状態になる

次に、電磁的記録として作成された電子ファイルをネットワーク経由で転送する場合における経路と、そこで想定される脅威を示す。ここでは、医療機関等と事業者を結ぶネットワーク機器（ルータ、LAN スイッチ等）は医療情報処理システム専用のものと考え、そこでは情報漏えい等の脅威は無いものと考える（機器障害のみを脅威とした）。

表 7 医療情報をネットワーク経由で交換する際の脅威

情報が移動する経路	想定される脅威
医療機関等と事業者を接続するネットワーク	第三者が通信を傍受して不正に情報を入手する 第三者が通信経路に介在して不正に情報を入手する 第三者が通信経路に介在して不正に情報を改ざんする 第三者が通信を妨害して利用できない状態になる
ネットワーク機器	機器の障害により通信不能状態になる 機器の障害により情報に損傷が起こる

次に、ネットワーク経由で医療情報をアプリケーションに入力する場合における経路と、そこで想定される脅威を示す。

表 8 医療情報をアプリケーションに入力する際の脅威

情報が移動する経路	想定される脅威
医療機関等と事業者を接続するネットワーク	第三者が通信を傍受して不正に情報を入手する 第三者が通信経路に介在して不正に情報を入手する 第三者が通信経路に介在して不正に情報を改ざんする 第三者が通信を妨害して利用できない状態になる
ネットワーク機器	機器の障害により通信不能状態になる 機器の障害により情報に損傷が起こる
アプリケーション	第三者がアプリケーションに介在して不正に情報を入手する 第三者がアプリケーションに介在して不正に情報を改ざんする 第三者がアプリケーション自体を改ざんする

アプリケーション利用の場合には、アプリケーション固有の脅威を考慮する必要がある。ユーザインタフェースにウェブブラウザ、つまり HTML[45]を用いる場合には、サーバとクライアントとのやり取りは HTTP[46]で行われることになる。このような形態で提供されるアプリケーションをウェブアプリケーションと呼ぶ。ウェブアプリケーションには、クロスサイトスクリプティング、SQL インジェクション等、良く知られた脆弱性が存在する。アプリケーション開発及び試験の段階で、これらの脆弱性が存在しないことを十分に検証すること。

[45] HyperText Markup Language
[46] HyperText Transfer Protocol

7.6 物理的安全対策

リスク評価で示した脅威を含め、情報セキュリティの三原則、機密性、完全性、可用性を確保するための要求事項について、物理的な安全管理策を以降に示す。

7.6.1 医療情報処理システムを配置する建物に関する要求事項

医療情報処理に関わる施設及び人員を配置する領域、つまり、建物、部屋については以下の管理策を講じなければならない。なお、外部事業者が運用管理するデータセンターに情報処理システムを設置する場合には、以降で述べる物理的安全管理策の全てに準拠することは難しい状況が考えられる。その場合には、専有するサーバラックスペースをセキュリティ領域と考え、不足する物理的安全管理策に相当する対策を施すことが求められる。

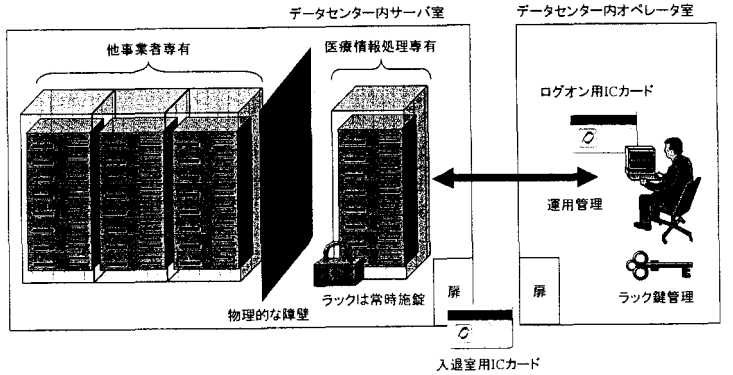

図 13 データセンターで医療情報処理設備を運用管理する場合の安全管理の例

専有サーバラックは十分な強度を持ったものを選定し常時施錠すること。他事業者のサーバラックとの間に物理的な障壁を設けることが望ましい。

実施すべき安全管理策

- 情報処理システムを配置する場所としては、情報処理事業者の専有する建物、あるいは情報処理事業者が全体を専有するフロア、あるいは十分に安全性が確保された外部事業者のデータセンター内に設置された医療情報処理設備専用のサーバラックとすること。
- 外部事業者のデータセンターを利用する場合には、情報処理システムに利用する全ての機器をサーバラックに納め、同じデータセンターを利用する他事業者から

の不正なアクセスに対する保護対策を施した上で利用すること。

- 医療情報を保管及び処理する施設を配置する部屋は他の業務を行う施設とは独立した部屋とすること。外部事業者のデータセンターにてサーバラックを利用する場合には、情報処理事業者専有のサーバラックとし、十分な強度を持ったサーバラックを選定し常時施錠すること。
- 複数医療機関から医療情報処理を受託しており、医療機関の職員が医療情報処理施設に物理的にアクセスする機会がある場合には、医療機関毎に情報処理機器を分け、それらの機器の間に物理的な障壁を設け、物理的なアクセス中は情報処理事業者が立ちあう等、別の医療機関から受託した医療情報にアクセスする機会を作り出さないように配慮すること。
- 部屋を区切る壁面、天井、床部分においては、傍受、盗撮等の不正な行為を防止するため、十分な厚みを持たせる、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。
- 建物、部屋に対する不正な物理的な侵入を抑止するため、侵入検知装置を導入すること。
- 自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。

7.6.2 情報処理システムへの入退館、入退室に関する要求事項

情報処理設備に対する第三者の不正なアクセスを防止するため、情報処理設備を配置する建物及び部屋について、適切なアクセス管理を行うこと。

実施すべき安全管理策

- 医療情報を保管及び処理する施設を配置する部屋の出入りを制限するため、有人の受付を設置して、入退館及び入退室者の確実な認証を行うこと。又はハードウェアトークン又はICカード（以下「認証デバイス」という。）に生体認証又は暗証番号（PIN[47]）を組み合わせた二要素以上の認証をサポートする機械式の認証装置により入退館、入退室者を管理すること。
- 認証を受けた要員に続いて認証を受けずに入退室する行為、及び、認証を受けて入退室した要員から認証装置越しに認証デバイスを受け取り、同じデバイスで再

[47] Personal Identification Number

度入退室を行うこと等の不正行為を防ぐ装置[48]を設置すること。

- 有人受付、機械式入退管理、いずれも履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること（履歴の保全については「7.7.12 ログの取得及び監査」を参照）。
- 職務中においては、要員の顔写真を券面に記録した職員証を外部から目視で確認できる状態で携帯することを義務付けること。
- 職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行うこと。
- 要員の業務に応じて執務室内に滞在できる時間を指定すること（例：平日かつ営業時間内、平日かつ24時間等）。
- 医療情報施設内への個人的所有物の持ち込みを認めないこと。

7.6.3 情報処理装置のセキュリティ

医療情報処理に用いる装置について、認められていないアクセス、事業に影響を与える損傷等のリスクから保護するために以下にあげる安全管理策を適用すること。

実施すべき安全管理策

- 情報が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。
- 火災発生時の消火設備が機器に損傷を与えないよう配慮すること。
- 情報処理装置を配置する室内での喫煙、飲食を禁止すること。
- 情報処理装置を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。
- 情報伝送に用いるケーブル類については直接の傍受リスクについて配慮すること。
- それぞれの装置は製造元又は供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。
- 保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確

[48] アンチパスバック（Anti Passback）装置