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

第 2 版

平成 24 年 10 月

経済産業省

目次

【 改訂履歴 】

改訂時期	改訂内容
平成 24 年 10 月 第 2 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」及び平成 22 年 2 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 4.1 版」、平成 21 年 7 月「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」及び平成 22 年 12 月「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第 1.1 版」に対応するための修正として、全般的な要求事項の見直しを行った。 第 7 章の要求事項において、技術の進歩により第一版に示した安全管理策の他に選択肢が増えた事項については「推奨される安全管理策」を新設し、移動した。 「7.2 原則として行うべきでない行為」については項目自体を削除した。 「7.7.13 バックアップ」については事業継続計画の要求事項とみなし、項目としては削除した。

1　はじめに

医療機関等で扱う文書類のうち、診療録、助産録、調剤録等（以下、「診療録等」という。）については、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[1]」によって、初めて診療録等の電子媒体による保存について基準が示された[2]。更に、平成 14 年 3 月通知「診療録等の保存を行う場所について[3]」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[4]（調剤録は電子保存可能だが、外部保存は許されていない）。この通知においては、それまで認められていなかった診療録等の外部保存を行う場合の基準が明記されていた。また、それぞれの通知に対して「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[5]」及び「診療録等の外部保存に関するガイドライン[6]（以下、「外部保存ガイドライン」という。）」が示されていた。一方、平成 15 年に「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」）が成立し、これを受けて医療・介護分野において平成 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 月の個人情報保護法の全面実施に際しての指針が示された。

さらに、平成 17 年 3 月、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に関して、厚生労働省に設置された「医療情報ネットワーク基盤検討会」にて「医療情報システムの安全管理に関するガイドライン」が策定された。このガイドラインは、「診療録等の電子媒体による保存について」及び「診療録等の保存を行う場所について」の各通知に基づき作成された各ガイドラインを統合し、新た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である。また、個人情報保護法及び「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）、「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）に対する医療情

---

1 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

2 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）にて廃止

3 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

4 「「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）にて一部改正

5 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

6 平成 14 年 5 月 31 日付け医政発第 0531005 号通知に添付

報システムの具体的指針という側面も持ち合わせる。

その後、平成 19 年 3 月には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等を追加して、「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」が策定された。

平成 20 年 3 月には、医療資格を持たないものが医療・健康情報を取扱う際のルール策定を検討した上で、責任のあり方についてまとめ、更に昨今の業務体系の多様化にも対応するため、モバイルアクセスで利用できるネットワークの接続形態毎の脅威を検討し、情報および情報機器の持ち出し等について追記した、「医療情報システムの安全管理に関するガイドライン 第 3 版」、平成 21 年 3 月には、より適切な医療分野の情報基盤構築を目指した「医療情報システムの安全管理に関するガイドライン 第 4 版」、平成 22 年 2 月には「医療情報システムの安全管理に関するガイドライン 第 4.1 版」が策定された（以下、第 4.1 版を「医療情報安全管理ガイドライン」という。）。

このような一連の施策等により診療録等の情報を電子的に作成し保存することが許容されてきた。また、それらを外部に保存する場合も外部保存ガイドラインで具体的指針が示されている。医療情報安全管理ガイドライン第 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が行われ、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」が取りまとめられた。これを受けて、外部保存通知の改正が行われ、医療情報安全管理ガイドラインにおいても関連する各章の一部を中心に改定が実施され、医療情報安全管理ガイドラインの第 4.1 版が策定された。

医療機関等から医療情報を受託する事業者となる立場の情報処理事業者については、現在、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の規定が適用されている。同ガイドラインは、多様な業種の事業者が広汎な種類の個人情報を取り扱うことを想定しているため、機微性の高い医療情報の取扱に携わる医療情報受託者に対しては、必ずしも十分な安全管理措置が規定されていない。

このため、「パーソナル情報研究会[7]」にて、医療情報の外部保存の安全性に万全を期すべ

[7] 「パーソナライゼーション時代の本格到来をにらみ、個人情報その他個人に関する情報に

く、医療情報受託者が義務的に講ずべき措置を具体的に明記した本ガイドラインを別途策定することとした。その後、平成 20 年 7 月には、本ガイドラインの第 1 版に従い、「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）を制定した。

本ガイドライン第 2 版では、医療情報安全管理ガイドラインの第 4 版及び第 4.1 版に合わせて内容を改めるとともに、経済産業省告示の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に関する参考資料としての位置付けを明確にしたものである。すでに、安全基準、即ち情報セキュリティマネジメントシステムに関する標準規格として JIS Q 27001:2006、個人情報保護マネジメントシステムに関する標準規格として JIS Q 15001:2006 が策定され多くの組織において活用されているが、既存の情報セキュリティ対策に関する各種の規格は広範な事業を対象として一般化されたものであり、本ガイドラインで扱う「医療情報取扱情報処理」事業の特殊性を鑑みて一段と具体化及び対策の深化を図る必要がある。このため、本ガイドラインでは「医療情報の外部委託」という事業特有の課題に配慮し、この分野において情報セキュリティマネジメントシステムを実装する上でのガイドラインを示すことを目的とする。

また、本ガイドライン第 1 版の公開後に、医療情報の処理を ASP・SaaS で提供する事業者及び団体向けに「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（総務省平成 21 年 7 月）」が策定されたことで、医療情報の外部保存を受託する事業者向けの本ガイドラインと合わせて、受託事業者サイドの情報処理事業に関するガイドラインの構成は図 1 のように整理されることとなった。なお、「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」は平成 22 年 12 月に第 1.1 版が公開されている（以下、第 1.1 版を「ASP・SaaS 事業者向けガイドライン」という。）。

本ガイドラインを含め、医療情報安全管理ガイドライン、ASP・SaaS 事業者向けガイドラインの関係を図 1 に示す。

ついて、将来想定される様々な利活用の方法を体系化すると共に、国民にとって安全・安心かつ適切な個人に関する情報の利活用を保証するための個人情報保護、セキュリティ、認証などのあり方について検討を行う」ことを目的として経済産業省商務情報政策局に設置された研究会。

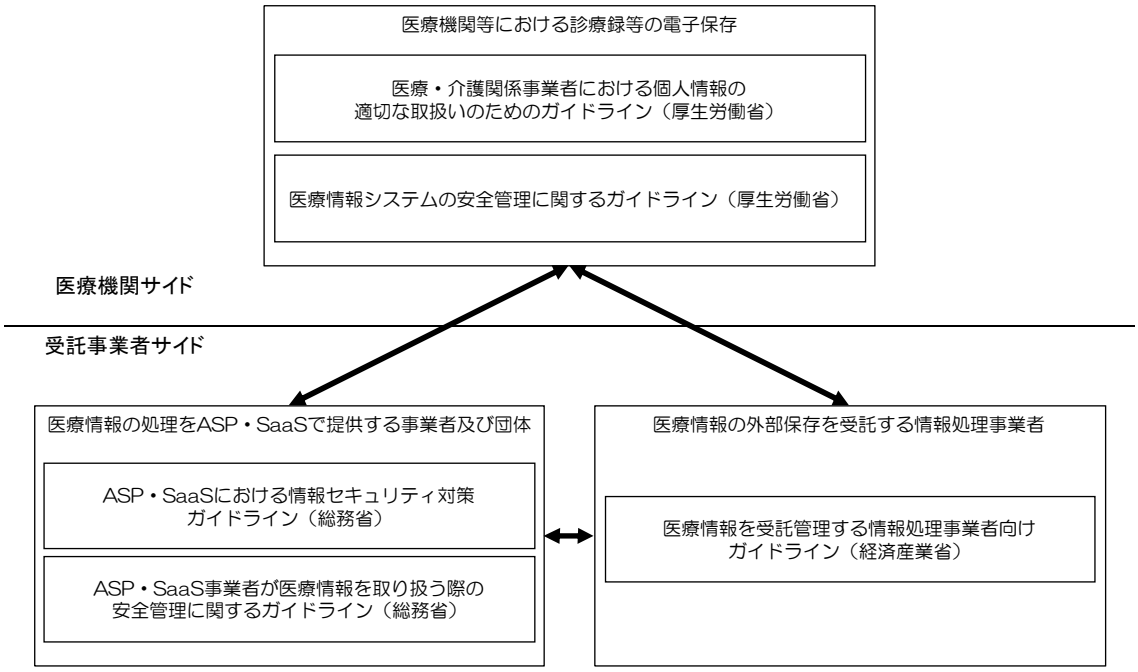

図 1 医療情報の取り扱いに係るガイドラインの関係

なお、本ガイドラインは、医療情報安全管理ガイドラインで示される安全管理策と同等の安全管理策として「実施すべき安全管理策」を示し、医療機関等及び情報処理事業者の判断で実施することが望ましい、同等以上の安全管理策を「推奨される安全管理策」として示している。どの安全管理策を実装するのかの判断において、単にセキュリティレベルの高さに配慮するだけではなく、個々の安全管理策が要求されている理由及び背景について、医療情報安全管理ガイドラインに記されている事柄を十分に理解しておくことが必要である。

1.1　本ガイドラインで用いる医療情報用語の説明

本ガイドラインで扱う医療情報に関する特有の用語について、法令及びガイドライン類にて定義されている用語の内、本ガイドラインの理解に必要なものについて以下に示す。

【 診療録 】

医師及び歯科医師が患者を診療した経過を記録したもの。カルテとも呼ばれ、診療終了後所定年限（5 年等）の保存が義務づけられている。医師法施行規則第 23 条及び歯科医師施行規則第 22 条により「診療を受けた者の住所、氏名、性別及び年齢、病名及び主要症状、治療方法（処方及び処置）、診療の年月日」が記載事項とされている。

【 診療記録 】

診療録、処方せん、手術記録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約その他の診療の過程で患者の身体状況、病状、治療等について作成、記録又は保存された書類、画像等の記録をいう。本ガイドラインにもとづき安全管理策を実施する際には、情報の種類に応じたリスク評価を行い、必要な安全レベルを考慮した安全管理策を選択することが求められる。

【 患者情報 】

上記の記録類に記載されている情報のうち、患者の既往歴、家族歴、嗜好等のこと。高度なプライバシー情報であり、医療機関等にとっては守秘義務が課せられていることからも、機密性への高い配慮が求められる。なお、要介護者は言葉の定義としては患者には含まれないと考えられるが、その情報は同様に高度なプライバシーに関する情報であることから、要介護者の情報についても患者情報と同等と考え、要介護者情報を扱うシステムは下記の医療情報システムに含まれるものとする。

なお、これらのプライバシーに関する情報は、疾患に伴って医療機関等にかかった患者の情報に限らず、例えば介護保険申請時に主治医が主治医意見書を作成する際に行った問診情報も含まれると解される。従って、患者情報は疾患に係わり収集された既往歴等だけに限らないことに留意しなくてはならない。

【 医療情報システム 】

医療において発生する患者情報を含む医療情報を、情報処理事業者が受託管理するためのシステムを指す。

【 医療機関等 】

主に病院、診療所、薬局、助産所等を指す。

1.2　本ガイドラインで用いる制度及び技術用語の説明

本ガイドラインで扱う制度及び技術用語について、本ガイドラインの理解に必要なものについて以下に示す。

【 ISMS （Information Security Management System） 】

ISMS 適合性評価制度[8]では「ISMS とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することである。[9]」と定義している。ISO[10]のマネジメントモデルに準拠しており、P（Plan）、D（Do）、C（Check）、A（Act）サイクルを継続することで組織的な改善を図ることを特徴とする。

【 JIS Q 27001:2006 】

ISMS の国際標準規格として ISO/IEC 27001:2005 が定められており、これに対応する日本工業規格として JIS Q 27001:2006（情報セキュリティマネジメントシステム要求事項）が定められている（以下、「JIS Q 27001」）。

【 ISMS 適合性評価制度 】

ISMS 適合性評価制度は、ある組織が構築した ISMS が JIS Q 27001 に適合しているかどうかを「認証機関」が審査して、認定された場合には「認定機関」に登録を行う仕組みである（以下、ISMS 評価制度）。ISMS 認定を受けて登録されることを「ISMS 認証を取得する」とも呼ぶ。

【 JIS Q 15001:2006 】

通商産業省（現在の経済産業省）が作成した「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を基礎として、1999 年に制定された。その後、「個人情報の保護に関する法律」が 2003 年に制定され、規格の取り巻く環境は大きく変化したことから、2006 年に改正を行い、個人情報の保護に関する法律に基づく個人情報保護ルール及びマネジメントシステムを併せもった規格となった（以下、「JIS Q 15001」）。

【 プライバシーマーク制度 】

「日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用

8 一般財団法人日本情報経済社会推進協会により運営されている。
9 http://www.isms.jipdec.jp/isms/index.html より引用。
10 International Organization for Standardization、国際標準化機構

を認める制度[11]のこと。

【 情報資産 】

組織にとって価値のある情報のことである。記載される媒体は紙、電子媒体等の形態を問わない。情報資産を漏れなく識別し、その資産価値及びリスクを評価し、保護レベルを決定することが ISMS 構築において不可欠である。

【 機密性、完全性、可用性 】

機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）は CIA とも呼ばれ、情報セキュリティ上の要求事項の中でも最たるものと位置づけられる。ISMS 適合性評価制度における機密性とは「認可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性」、完全性とは「資産の正確さ及び完全さを保護する特性」、可用性とは「認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性」と定義されている。

【 安全管理策（Controls） 】

リスクに対応するために実施される手順等のことを指す。

【 適用宣言書（statement of applicability）】

組織の確立する ISMS に関して適用される管理目的及び安全管理策を記述した文書のこと。一般には JIS Q 27001 付属書 A に沿って記述する。

【 専用線 】

特定の事業者間を接続する専用の回線であり、他事業者の通信の影響を受けず、通信回線上の機密性が高い性質を持つ。

【 VPN（仮想私設網、Virtual Private Network）、IP-VPN（閉域 IP 網／閉域網 VPN）、インターネット VPN 】

不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のことを VPN（仮想私設網、Virtual Private Network）と呼ぶ。

VPN のうち、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提供する接続サービスを、特に、IP-VPN（閉域 IP 網／閉域網 VPN）と呼ぶ。

また、オープンなネットワークであるインターネット上に構築された VPN を、特に、イ

[11] http://privacymark.jp/privacy_mark/about/outline_and_purpose.html より引用。

ンターネット VPN と呼ぶ。

なお、本ガイドラインでは、回線の種別を表す用語として、専用線、IP-VPN、インターネット VPN の三種類を用いることにする。

【 電子媒体 】

電子情報を保存、記録する媒体の総称であり、ハードディスクドライブ、USB メモリのような、情報を記録、記憶する媒体と装置が一体となった記憶装置、光学ディスク（CD-R、DVD-R 等）や磁気ディスク（フロッピーディスク等）、光磁気ディスク（MO)、磁気テープ等の、情報を記録、記憶する記憶媒体等を含む。

【 ASP（Application Service Provider）・SaaS（Software as a Service）】

ASP（Application Service Provider）及び SaaS（Software as a Service）は、ともにネットワークを通じてアプリケーション・サービスを提供するものであり、基本的なビジネスモデルに大きな差はないものと考えられる。

したがって、本ガイドラインでは、ASP・SaaS インダストリ・コンソーシアム・ジャパンの発行した 2005 年版『ASP 白書』による ASP の定義『ネットワークを通じて、アプリケーション・ソフトウェア及びそれに付随するサービスを利用させること、あるいはそうしたサービスを提供するビジネスモデルを指す』を採用するとともに、ASP と SaaS を特に区別せず、「ASP・SaaS」と連ねて呼称することとする。また ASP・SaaS を行う事業者及び団体等を「ASP・SaaS 事業者」と呼ぶこととする[12]。

[12] 本用語の説明については、ASP・SaaS 向けガイドラインの「1.4.1 ASP・SaaS の定義」を引用した。

1.3　本ガイドラインで用いる独自用語の説明

この他に、本ガイドラインで用いる用語の内、特定の意味を持たせている用語について以下に示す。

【 作業者 】

情報処理事業者において情報処理装置を操作するものを作業者と呼ぶ。

【 情報処理事業者 】

本ガイドラインにおいては医療情報処理を受託する情報処理事業者を意味する。

【 医療情報処理施設 】

情報処理装置及び配置される物理的施設（データセンター、サーバラック等）を含んだ情報処理施設全体を意味する。

2　本ガイドライン策定の基本方針

本ガイドラインは外部保存等のために医療情報を受託管理する業務を提供する情報処理事業者にとって、預かっている情報の安全性[13]を確保するために実装すべき管理策（以下、「安全管理策」）を具体化して提示することが主要な目的である。

安全管理策の選考については、 (1)提供される情報処理業務を想定し、業務で扱う情報、業務で利用する情報処理装置、業務を実施する作業者及び組織構成等を情報資産として数え上げる、(2)それぞれの潜在的リスクを、機密性、完全性、可用性といった情報セキュリティの要素、さらに医療情報取扱に求められる真正性、見読性、保存性の要求事項から考察する、(3)リスクの大きさにもとづいたリスク対応を選択する、(4)JIS Q 27001 のカテゴリに倣って具体的な安全管理策として記述及び整理する、といった手順を採用した。これは ISMS[14]ユーザーズガイド[15]に示される ISMS 構築ステップに倣ったものである。

情報処理事業者が本ガイドラインに従っていることを、法令及び医療情報安全管理ガイドライン等にて高い安全管理レベルを求められている医療機関等に対して客観的に示すため、過不足なく適用範囲を定めた適用宣言書に基づく情報セキュリティに関する認証及び認定を活用することが有効である。

このような客観的評価による認証及び認定には、プライバシーマーク制度、ISMS 適合性評価制度等がある。情報処理事業者は本ガイドラインに示される安全管理策を適用した上で、適切な制度を選び、認証または認定等を受けることが求められる。また、審査を行う審査機関においても、本ガイドラインについて十分に理解し、医療情報システムの特質を反映した審査活動を行うよう、情報処理事業者から要望することが望ましい [16]。

---

[13] 6 章で説明する真正性、見読性、保存性を含む。
[14] Information Security Management System、情報セキュリティマネジメントシステム
[15] 一般財団法人日本情報経済社会推進協会
[16] 医療情報を取り扱う保健医療福祉分野等の事業者のプライバシーマーク認定については、一般財団法人医療情報システム開発センターが審査を実施している。

2.1　安全管理策の整理と本ガイドラインの基本構成

安全管理策としては、医療情報安全管理ガイドラインの最新の版である「医療情報システムの安全管理に関するガイドライン 第 4.1 版」に JIS Q 27001、JIS Q 15001 を加え、JIS Q 27001 で示される管理策のカテゴリの形で整理して本ガイドラインを構成する。厚生労働省、総務省のガイドラインとの関係を図 2 に示す。

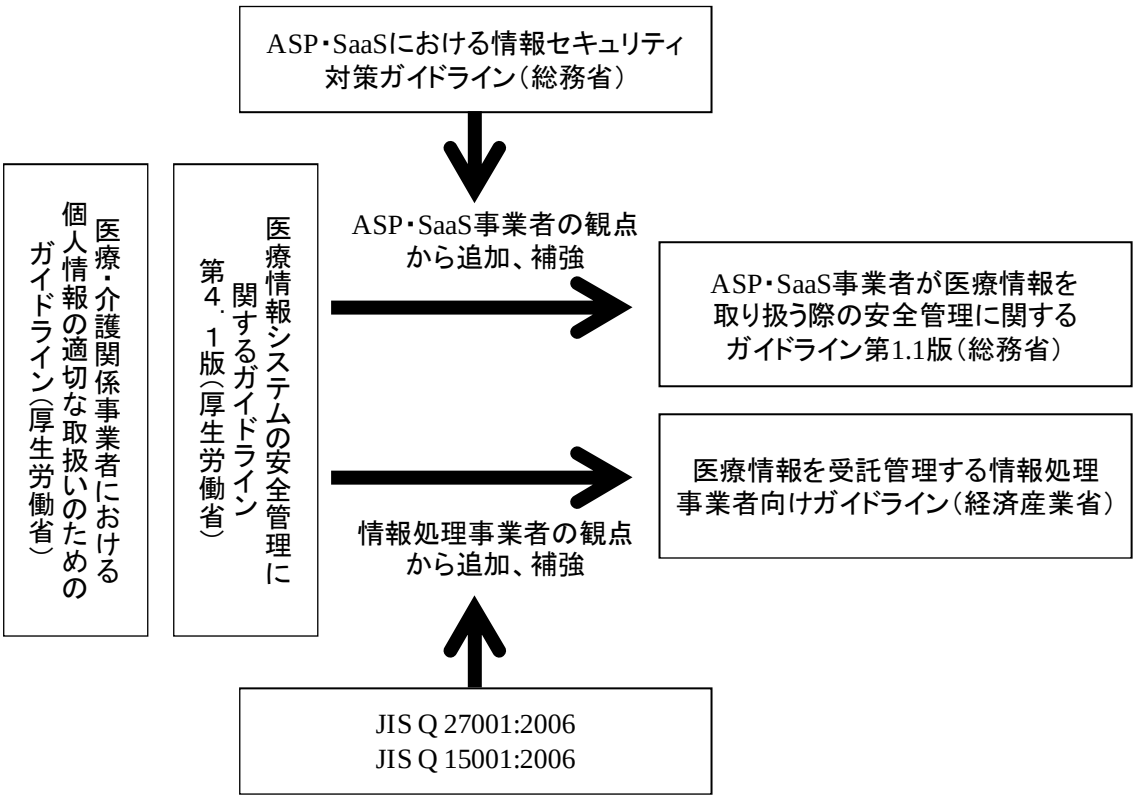

図 2 本ガイドラインの構成と各ガイドラインの関係

医療情報安全管理ガイドラインでは、制度上の要求事項を満たすための管理策として「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」を示している。本ガイドラインでは、情報処理事業者の安全管理策として、C の必須事項は当然のこととして D の推奨事項の中でも実施することが必要であると考えられる管理策については、合わせて必須事項として示している。これら、本ガイドラインで示される必須の安全管理策に加え、個人情報保護マネジメントシステムの要求事項である JIS Q 15001 及び情報セキュリティマネジメントシステムの要求事項である JIS Q 27001 等の標準規格に準拠するよう、包括的に安全管理策を具体化することが求められる。

平成 20 年 3 月策定の医療情報安全管理ガイドライン第 3 版では、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」としていた。その後、本ガイド

ラインが策定されたため、医療情報安全管理ガイドラインから上記の記述が削除されたが、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要件とする。

保健医療福祉分野においては「保健医療福祉分野のプライバシーマーク認定指針（第 3.1 版）[17]」が策定されている。医療情報を受託管理する情報処理事業者がプライバシーマーク認定を取得する際には、この認定指針を参照し、準拠に努めることが望まれる。

[17]一般財団法人 医療情報システム開発センター

2.2 医療情報安全管理ガイドラインとの対応関係

本ガイドラインと対となる医療情報安全管理ガイドラインに記載される安全管理措置との対応関係を表 1 に示す。

表 1 医療情報安全管理ガイドラインと本ガイドラインの対応関係

医療情報安全管理ガイドライン	本ガイドラインの対応する部分
6 章 情報システムの基本的な安全管理	7 章 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
7 章 電子保存の要求事項について	6 章 電子保存の要求事項について
8 章 診療録及び診療諸記録を外部に保存する際の基準	8 章 診療録及び診療諸記録を外部に保存する際の基準

なお、医療情報安全管理ガイドラインでは、「7 電子保存の要求事項について」の中で真正性、見読性、保存性を確保するための安全管理策をまとめているが、本ガイドラインでは、「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」の中で、真正性、見読性、保存性を確保するための安全管理策を JIS Q 27001 の分類でまとめている。

3　本ガイドラインの対象システム及び対象情報

本ガイドラインは外部の情報処理事業者が医療機関等から「医療情報の外部保存に関する業務」を受託して医療情報を取扱う際の安全管理基準を示すものであり、対象とする情報の種類としては、法令で外部保存が認められる医療情報（表 4 外部保存を認める文書等を参照）を主な対象とし、他にも医療情報安全管理ガイドラインの「3.3 取扱に注意を要する文書等」に記載された文書、医療機関等から前記の医療情報と同様の取り扱いで保存するよう依頼された文書等を対象とする。情報システムとしては、医療情報を電磁的記録として媒体経由及びネットワーク経由で受入れ、保管し、医療機関等の要請で検索する等、一定の処理を行うシステムを対象と考える。この全体概要は図 3 に示される。つまり、医療機関等においては医療情報安全管理ガイドラインに従ってシステム構築及び個人情報の保護に係る安全管理措置を適用し、情報処理事業者においては本ガイドラインに従ってシステム構築及び個人情報の保護に係る安全管理措置を適用するという関係にある。

本ガイドラインの対象とする情報処理に関する医療情報交換経路は、（1）電子媒体に情報を格納した上で物理的に運搬する経路、（2）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経路、（3）情報処理事業者が提供するアプリケーションに情報を入力することで情報処理事業者側に電磁的記録が作成される経路の三通りを単独または組み合わせて利用することを想定する。

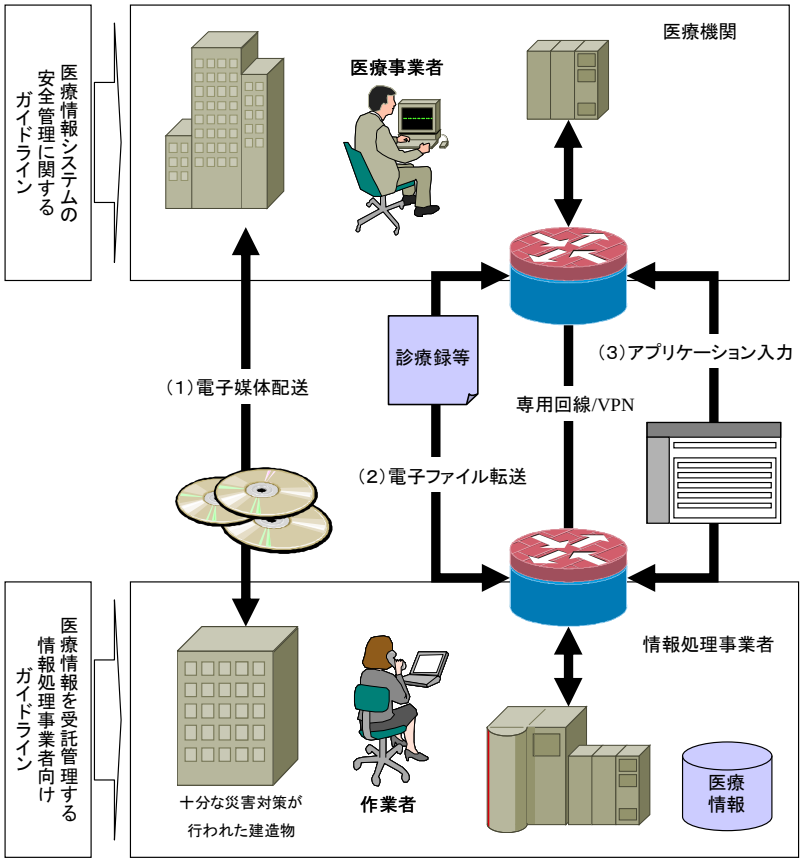

図 3 本ガイドラインで対象とする情報システムの概念

情報サービスの概念としては外部ストレージサービス及び情報検索サービスと呼ばれているシステムに類し、どの程度の検索機能や情報処理機能を提供するのかは医療機関等の要請に従うものである。ただし、医療情報安全管理ガイドラインに「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、不当な営利、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。(P.95)」、また「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。(P.96)」(医療情報安全管理ガイドライン「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り扱いに関する基準」参照) とあるように、原則として、機密管理の観点から受託管理する医療情報の全体を情報処理事業者が閲覧・処理することを行うことは想定されていない。

他方、サービスの内容によって情報処理事業者が閲覧しなければならない情報の範囲は変わるため、医療機関等が求めるサービスの実現のために必要であるならば、上記の医療情報安全管理ガイドラインにおける記述を踏まえつつ、医療情報の秘匿性の高さに十分配

慮して、適切なアクセス管理を実施した上で情報処理事業者が医療情報を閲覧することも考えられる。

なお、医療情報システムを設置する場所については、情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のハウジング領域のうち独立した領域等）が望ましいが、現実的には外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合及び外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ[18]等）を利用する場合も多いと考えられる。そのような場合には、情報処理事業者が専有する建造物あるいは領域と同等の安全性を確保するため、本ガイドラインの物理的安全対策に準拠したデータセンター、サービス事業者を選択することが求められる。いずれの場合も、扱う情報として、法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。また、法令により作成や保存が定められていない文書であっても、個人情報保護に十分に留意して適切な管理を行うことが必要である。

情報処理ソフトウェアをサーバ上で動作させる場合、サーバに管理者権限でアクセスするための管理端末の配置が問題になる。サーバはデータセンター内の入退室管理された領域に置いたとしても、管理端末を配置する領域の安全性が劣ることは避けなければならない。管理端末を同じサーバラック内に設置することは現実的ではないため、データセンター内に端末室があればデータセンター内のLANを経由してサーバと端末室の端末を接続する、端末室が無い場合にはデータセンターの外部にある情報処理事業者自身の施設内に安全を確保した端末室を設けて、IP-VPN あるいは IPsec[19]と IKE[20]を併用したインターネットVPN を経由してサーバと端末を接続するといった方法が考えられる（図 4）。

[18] Virtual Private Server、レンタルサーバのサービス品目の一つで、共用サーバながら仮想的に専用サーバと同等の機能を提供するサービス。
[19] Security Architecture for Internet Protocol、IP レイヤにて認証、完全性、機密性を提供するプロトコル。
[20] Internet Key Exchange、IPsec において通信に用いる鍵に関するパラメータ交換及び、定期的な鍵更新を行う仕組み。

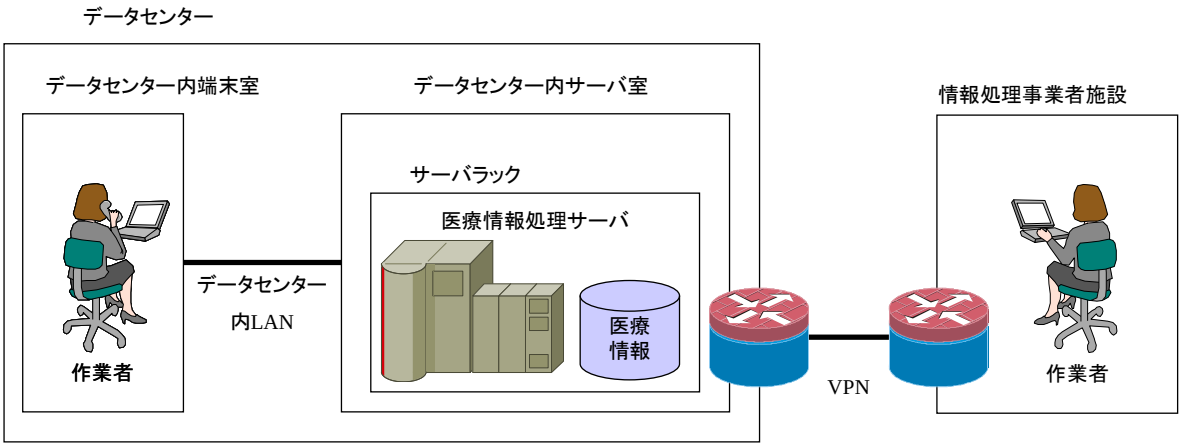

図 4 データセンターの利用とサーバ及び端末配置の例

いずれの場合も、ネットワークの安全管理を厳密に行うとともに、端末へのアクセス、ログオンアカウント管理を厳密に行うこと。

以下で述べるように医療機関等と情報処理事業者間をネットワークで接続して情報交換を行う場合には、図 3 にあるように専用線あるいは VPN といった第三者による傍受のリスクが低いネットワークを利用すること。さらに医用画像（レントゲンデータ等）等、転送する情報量が相当に大きくなることもあることから、必要なネットワーク容量の見積もりを適切に行い、十分なネットワーク容量を確保すること。

3.1　電子媒体の選択についての考慮事項

電磁的記録としての医療情報は電子媒体に保管することとなる。「診療録等の電子媒体による保存に関する解説書[21]」によると電子媒体とは「保存による情報の劣化を防ぐためデジタル記録ができる媒体及び機器」のこととされている。具体的な媒体及び機器としては、MO[22]等の光磁気ディスク、CD、DVD 等の光学ディスク、USB[23]メモリ、コンパクトフラッシュカード、SD メモリーカード[24]等の半導体メモリ、ハードディスク等の磁気ディスク装置等が考えられる。

長期保存を目的として、これらの電子媒体を利用する場合には、製造元の保存仕様に準拠した保管を行い、見読性、保存性を損なわないように配慮すること。また電子媒体の劣化特性を考慮して、劣化が起こる前に新たな電子媒体に複写すること。

長期保存が主目的であり頻繁に情報を閲覧する必要がない場合には、光学ディスク、光磁気ディスクに記録し、適切な保管環境で管理することが望ましいが、頻繁に情報を閲覧する場合には情報処理装置に接続された磁気ディスク等に記録して管理することになる。この場合には、情報処理装置上のアクセス権限管理を厳密に行い、不正なアクセスから情報を保護することが必要である。また、適切に暗号技術を利用することで情報を保護する方策も検討すること。

なお、媒体としての小型半導体メモリは、例えば micro SD のような極めて小型で記憶容量が大きな媒体が存在し、衣服などのわずかな隙間にも隠すことができるため、不正な情報の持ち出しを企図するものにとっても有益なものといえる。医療情報を格納する電子媒体として、小型半導体メモリの有益性は認められるものの、漏洩等の大きなリスクも考えられることから、原則として医療情報システムでは外部デバイスとして小型半導体メモリの使用を行うことができないよう配慮することが望ましい。必要により使用する場合、使用前には不要なデータが書き込まれていないことを確認し、使用後には電子媒体上の全てのデータを削除すること。また、利用時間及び電子媒体の移動範囲を最小にするなどの管理を行うこと。

---

21 平成 11 年 10 月 厚生省健康政策局研究開発振興課医療技術情報推進室監修 （財）医療情報システム開発センター 編集

22 Magneto Optical Disc

23 Universal Serial Bus

24 Secure Digital Memory Card

3.2　ネットワーク利用上の考慮事項

医療情報安全管理ガイドライン「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」には「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。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」および「改ざん」、通信経路への「侵入」および「妨害」などの脅威から守らなければならない。(P.55)」とある。

このため、保管のためのデータ移動等、ネットワーク経由での情報管理機能を提供する場合には、医療機関等と情報処理事業者側設備をつなぐネットワーク部分に適切な安全管理措置を施す必要がある。この際、安全面への配慮からは専用線と同等の回線を用いるべきである。しかし、一般に専用線は利用コストが高価であることから、公衆回線上に仮想の閉域網を構築する技術等を採用することも検討対象と考えることができる。

インターネット等、不特定事業者と共有するオープンなネットワーク上の VPN は、専用線及び IP-VPN といったクローズなネットワークでは存在しない、サービス不能攻撃（Denial of Service)、ブルートフォース攻撃[25]等を受けるリスクがあり、安全性が、専用線や IP-VPN と比べて低いと考えられる。しかし、運用を適切に行うことで十分な安全性を確保することは可能であり、これまでに例として上げた種類の回線と比べて回線コストが格段に安いというメリットもあることから、適切に運用すること及び医療機関等の合意を得ることを前提として、IPsec に IKE を組み合わせ、自動鍵更新を行う設定にて、オープンなネットワーク上の VPN を採用することも可能とする。

ただし、インターネットからの第三者による不正なアクセスを防止するため、医療機関等の機器と情報処理事業者側の機器において、ネットワーク境界のファイアウォールまたは VPN 装置等により、適切なアクセス制御を行うこと（「3.5.2 ネットワーク利用上の考慮事項」を参照)。

医療機関等とのネットワーク選択に際しては、医療情報安全管理ガイドライン「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 B-2. 選択すべきネットワークのセキュリティの考え方」を参照し、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されている場合、それぞれの考慮事項をよく理解すること。

また、いずれの種別の回線であっても、通信ログ及び通信状況を監視し、異常が発生した場合には迅速に対処すること。

---

[25] brute force attack（力任せの攻撃)。ログオンに成功するまで ID とパスワードの様々な組み合わせを試しつづける攻撃等を意味する。

3.3　外部保存を電子媒体経由で行う場合の手順

医療情報を CD、DVD、MO 等の電子媒体を利用して情報処理事業者の施設に保存する場合の一連の手順を例として以下のように考える。

- 医療機関等の医療従事者の作業手順

  (1) 医療情報を外部保存することに関する内部申請及び承認プロセスの実施

  (2) 情報処理事業者受け取り後の真正性検証のため、外部保存対象の電子ファイルについて電子署名を付与等の対策を実施する（必要に応じて暗号化を行う）。

  (3) 外部保存対象の電子ファイルを電子媒体に書き込み、施錠可能な容器等に納める等、配送経路上での開封を検知できるように封印を行う。

  (4) 信頼できる配送業者に配送を指示する（信頼確保の手順は後述）。

  (5) 情報処理事業者に対し、配送する電子媒体の数量・種類、配送業者の作業者情報、予想到着時刻等を通知する。

- 情報処理事業者の作業手順

  (1) 到着した配送業者の身分確認後に受領する。

  (2) 受け取った電子媒体の数量、封印が正常であること等を確認する。

  (3) 医療情報システムとネットワーク接続されていない機器上で電子媒体に悪意のあるコードが混入していないことを検証する。さらに、電子署名検証等の真正性検査を実施する（悪意のあるコードについては「7.6.3 悪意のあるコードに対する管理策」を参照）。

  (4-1) 電子媒体そのものを保管する場合には受領した電子媒体を保管庫等に格納する。

  (4-2) 電子媒体上の電子ファイルを情報処理装置上で保管する場合には情報処理装置に電子媒体中の電子ファイルを複写し、電子媒体内の情報あるいは電子媒体自身を適切な手段で廃棄処分する（廃棄手順については「7.6.7 電子媒体の取扱」を参照）。

  (5) 受領した電子ファイル又は電子媒体の情報を管理台帳に記載する。

  (6) 医療機関等に受付情報を通知する。

このような電子媒体の交換手順について医療事業者と合意し、手順書として双方で管理すること。

配送事業者の信頼性については、機密保持契約の締結が可能である、機密情報の配送に特化した配送サービスを提供している、配送状況を利用者が把握する機能を提供している等の条件により事業者を選択することで確保すること。

3.4　外部保存をネットワーク経由で行う場合の手順

医療情報をネットワーク経由で情報処理事業者の施設に保存する場合の一連の手順を例として以下のように考える。

- 医療機関等の医療従事者の作業手順

(1) 医療情報を外部保存することに関する内部申請及び承認プロセスを実施する。

(2) 情報処理事業者受け取り後の真正性検証のため、外部保存対象の電子ファイルについて電子署名付与等の対策を実施する。

(3) 医療機関等と情報処理事業者を接続するネットワーク上の機器に電子ファイルを複写する（なお、医療機関等の内部ネットワークと電子ファイル転送用のネットワークが接続されている場合は不要な通信が行われないよう適切な安全管理対策、アクセス制御を適用すること）。

(4) ネットワークを経由して情報処理事業者の受入れ機器に電子ファイルを複写する。

(5) 情報処理事業者に送出完了を通知する。

- 情報処理事業者の作業手順

(1) 医療事業者からの電子ファイル転送を常時監視するようシステムを整備する。

(2) 電子ファイルが転送されてきたことを検知した際は悪意のあるコードが混入していないことを検証する。さらに、電子署名検証等の真正性検査を実施する（異常を検出した場合には即座に医療事業者に通知すること）。

(3) 医療機関等から電子ファイルを転送するフォルダは一時フォルダとし、上記検証後に電子ファイルを保管用フォルダに移動する（一時フォルダ内の電子ファイルは削除する）。

(4) 複写した電子ファイルの受付情報をまとめて管理台帳に記載する。

(5) 医療機関等に受付情報を通知する。

管理台帳に記載すべき、転送された電子ファイルの情報については「7.2.1 資産台帳」を参照すること。管理台帳を活用して、定期的に医療機関等と情報処理事業者間における医療情報電子ファイルの真正性を検証することが望ましい。

このようなネットワーク経由の交換手順について医療機関等と合意し、手順書として双

方で管理すること。なお、ファイル転送についてインターネット標準技術である FTP[26]プロトコルを用いる場合においては専用回線あるいはVPN等を利用して少なくともネットワークレイヤでの安全対策を施し、パスワード及びデータ漏洩のリスクを低減すること。単一の安全対策ではなく、ネットワークレイヤでの安全対策に加えて、アプリケーションレイヤにおいても SFTP[27]、SCP[28]等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用するといった、多重防御を実装することが望ましい。

なお、FTP のアカウント情報を不正に取得する悪意のあるコードが広範囲に被害を及ぼした事例があることから、FTP を採用する場合には FTP アクセスログを定期的に検証し、不必要な FTP アクセスが行われていないことを確認するなどの対策を行うこと。

上記手順を図 5 に示す。

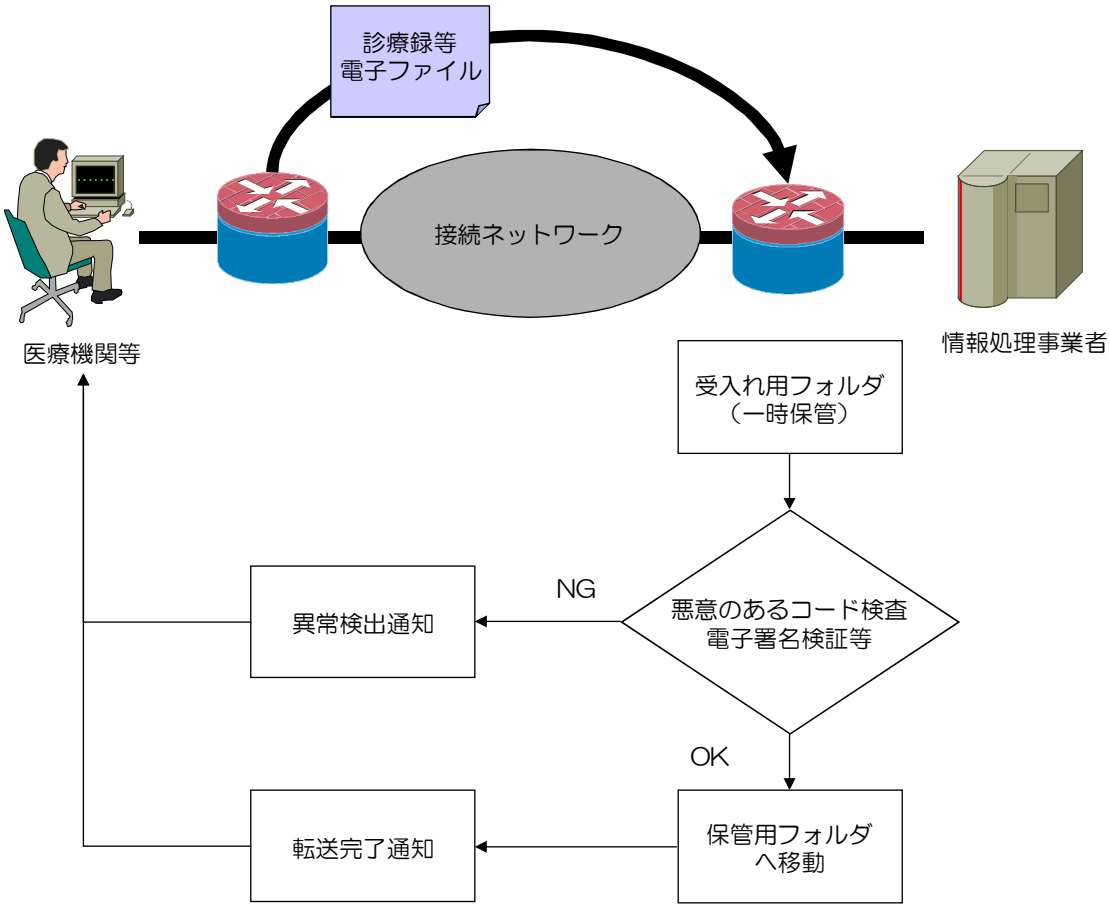

図 5 電子媒体による外部保存をネットワーク経由で行う場合

悪意のあるコード検査及び電子署名検証等の過程で問題が発見された場合はただちに医

[26] File Transfer Protocol
[27] Secure File Transfer Protocol
[28] Secure Copy

療機関等に通知すること。なお、問題が発見された電子ファイルは原因特定を行う必要があることから、削除せずに情報処理装置から隔離したかたちで保管すること。

ここまでに示した電子媒体の外部保存に関して、その経路に拠らず実施すべき作業について以下に示す。

- 医療機関等の医療従事者の作業手順

(1) 情報処理事業者からの定時報告を確認、検証する。

(2) 不審な点があれば、ただちに確認を行う。

- 情報処理事業者の作業手順

(1) 受入れた電子ファイル、払出した電子ファイル、預かっている電子ファイルの数量、発生したイベント等について定期的に確認できる仕組みを構築し医療機関等が確認できるようにする。

(2) 検証手続き中に異常が検出された場合は、直ちに医療機関等に連絡し、適切な事故対応手順を実施する。

医療機関等への通知については、自動的に通知メッセージを作成・送付する仕組みを設けることがコスト面でも安全面でもメリットがある。このような通知メッセージを実装する場合、メッセージ中に機微な情報が含まれる場合には、医療機関等と受託情報処理事業者を結ぶ安全なネットワーク上で転送することが原則であるが、保護されていないインターネット経由で転送する場合には、暗号技術を用いて、メッセージの機密性、完全性を確保すること。(なお、ここでは情報の受入れ手順について記述したが、廃棄手順については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」および「7.6.7 電子媒体の取扱」、「7.8 情報の破棄」等に示される管理策を適用すること)。

3.5　外部保存をネットワーク経由のアプリケーション入力により行う場合の手順

外部の情報処理事業者が所有する情報処理システムで実施される情報処理サービスを、ネットワーク経由で提供する形態を ASP（Application Service Provider）又は SaaS（Software as a Service）と呼ぶ（以下、「ASP・SaaS」）。ASP・SaaS とは利用者別に開発したアプリケーションあるいはカスタマイズしたパッケージソフトウェアの運用と稼働環境である情報処理システムの運用を合わせて提供するサービス、いわゆるアプリケーションホスティングと呼ばれる形態から、共同アウトソーシングのように施設を共同で利用する形態、さらに全ての利用者が情報処理システムを共有し、さらに同一のアプリケーションを利用することで価格面のメリットを追及した形態まで様々なものがある。

本ガイドラインの対象とする情報処理システムは「医療機関等の要請で検索等、一定の処理を行うシステム」であることを述べた。このシステムの提供形態としても ASP・SaaS が想定される。しかし、ASP・SaaS では計算機環境を共有する場合があり、利用者間の悪影響が発生する可能性が存在すると考えられるため、システム構築、システム運用時の考慮事項について、「3.5.2 ネットワーク利用上の考慮事項」及び「ASP・SaaS 事業者向けガイドライン」の要求事項に従い、適切な対策を行うことが要求される。

ASP・SaaS 形式のサービス等を利用して医療情報をアプリケーション入力する場合の一連の手順を以下のように考える。

- 医療機関等の医療従事者の作業手順

  (1) アプリケーションにログオン

  (2) アプリケーションに医療情報を入力

  (3) 医療情報の送信又は保存

  (4) アプリケーションからログオフ

- 情報処理事業者の作業手順

  (1) 入力された医療情報の暗号化（必要に応じて）

  (2) データベースへの登録

このようなアプリケーション入力による医療情報の交換手順について医療事業者と合意し、手順書として双方で管理すること。また、電子署名の付与が求められる情報については、電子ファイルとして作成してファイルを転送する形をとることが望ましく、その場合には、情報処理事業者にて受け取ったファイルの電子署名を検証することになる。

なお、ASP・SaaS ではウェブブラウザをクライアントとした、いわゆるウェブアプリケ

ーションを提供することが多いと考えられる。ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、サービス提供時はもちろん、リスク評価を行い、必要に応じて定期的にアプリケーションの脆弱性検査[29]を実施して、安全性を確認すること。

3.5.1 データベース利用上の考慮事項

アプリケーション入力による外部保存では、一般的に入力データはデータベースに格納されることになると考えられる（図 6）。

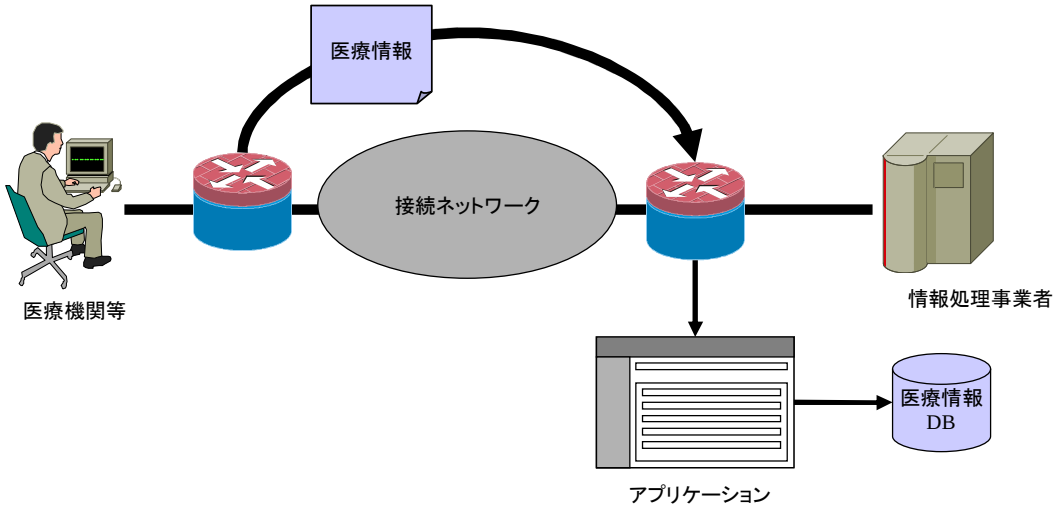

図 6 アプリケーション入力による外部保存をネットワーク経由で行う場合

ここで検討しなければならないことの一つは情報漏洩対策として暗号化を行うことである。データベース及びデータベースシステムにおける暗号化とは、データベースファイルをハードディスクのパーティションとして構成してパーティション全体を暗号化すること、電子ファイルとしてデータベースファイルを暗号化すること、データベース中のデータ（テーブル、行、カラム等）を個々に暗号化すること等、いくつかの手法が知られている。ここで配慮しなければならないリスクとしては、データベースを格納した機器の盗難等による情報漏洩、電子ファイルとしてのデータベースファイルの盗難等による情報漏洩、データベースにアクセスすることによる個々のデータの盗難等による情報漏洩等である。

ここであげた三つの情報漏洩リスクに対する三つの暗号化手法の効果を表 2 にまとめる。

[29] 検査すべき脆弱性としては「『安全なウェブサイトの作り方 改訂第 5 版』独立行政法人情報処理推進機構」を参照のこと。

表 2 情報漏洩リスクに対する暗号化対象別の効果

	機器の盗難等による情報漏洩	電子ファイルとしてのデータベースファイルの盗難	データベースアクセスによる情報漏洩
パーティションの暗号化	○	×	×
データベースファイルの暗号化	○	○	×
データベース中のデータの暗号化	○	○	○

パーティション全体を暗号化した場合、機器の盗難に対しては一定の効果があるが、機器の稼動中はオペレーティングシステムに対しては復号された状態になり、ログオンユーザ、特に特権ユーザに対しての保護策にはならない。このため、不正にログオンする行為、あるいはログオンユーザの不正行為には効果が薄い。電子ファイルとしてデータベースを暗号化した場合、オペレーティングシステムからも暗号化されたままの状態であるため、ユーザアカウントからデータベースを保護することができる。しかし、データベースプロセスに対しては復号された状態であるため、データベースアクセスを悪用した情報漏洩行為に対しては効果がない場合がある。このため、データベースのユーザアカウントに対しては保護にならない。データベース中のデータを個別に暗号化した場合には、そのデータに対するアクセス権限をデータベースシステム上で与えられていなければデータを復号された状態で知ることはできないため、機器及びデータベースファイルの盗難等、データベースアクセスを悪用した情報漏洩行為の全てに対して保護を提供することが可能である。ただし、データ毎に細かい粒度のアクセス設定を間違いなく行う必要があり、管理運用のコスト及び設定ミスによるリスクも高くなるという側面があることに注意が必要である。

なお、データベースを利用したシステムでは、内部関係者による不正行為、情報漏洩を視野に入れて対策を講じる必要がある。一般的にウェブアプリケーションの利用環境ではデータベースに直接アクセスする管理者、開発者といったアカウントはその職責上多くの権限が付与されているケースがあり、リスクが大きい。そのため「なりすまし」によってこれらのアカウントの不正使用を防ぐため、パスワードの管理を厳密に行うだけでなく、必要に応じて多要素認証などの技術を利用し十分な認証強度を確保しなければならない。また、「なりすまし」が行われた際の被害を小さくするため、管理者機能を分割した上でおのおのに別の特権 ID を割り当て、それぞれの特権 ID の権限を必要最小限とする最小特権の原則を実装することが望ましい。

このように、アプリケーション入力による外部保存をネットワーク経由で行ってデータ

をデータベースにより保管する場合には、システムの構成に配慮したリスク評価を行い、暗号技術等を利用した適切なリスク低減策を適用すること。

3.5.2 ネットワーク利用上の考慮事項

アプリケーション入力をおこなう場合には、第三者による傍受のリスクを避けるため、アプリケーションを提供する情報処理事業者と医療機関等を接続するネットワークとして専用線あるいは VPN を利用することが要求される。VPN はインターネット等の不特定多数が接続されるネットワーク上に構築されたものであっても、医療機関等の理解と合意があれば利用することができるとするが、インターネット VPN には傍受以外にも第三者による不正な中継（man in the middle）、サービス不能攻撃等のリスクが存在し、回線品質も、専用線や IP-VPN と比較して低いため、交換する情報に求められる機密性のレベルを判断し、コスト及び運用に対して、閉域網上に構築された VPN との比較を行い、適切なネットワークを選択すること。

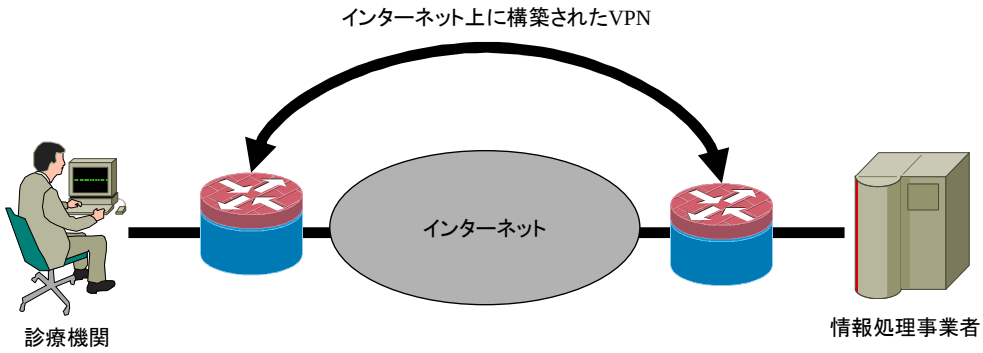

図 7 インターネット上に構築された VPN

インターネット上の VPN を利用する場合には、第三者からの不正なアクセスを防止するため、「7.6.6 ネットワークセキュリティ管理」に示される制約に従うこと。

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程に基づいて守秘義務が課されている。図 8 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。

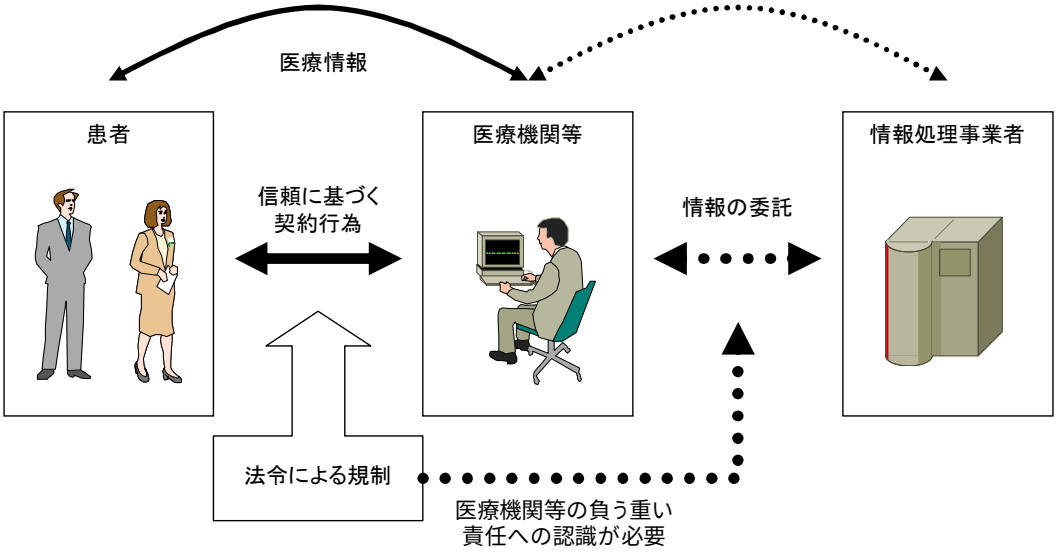

図 8 患者と医療従事者と情報処理事業者の責任関係

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。従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。（P.124）」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、医療機関等と情報処理事業者との責任分界点の考えについて示す。

なお、本章とともに、医療情報安全管理ガイドラインの「4 電子的な医療情報を扱う際の責任のあり方」について十分に理解しておくこと。

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、医療機関等における管理者の善管注意義務[30]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（典型的には情報漏洩）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[31]。

「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方法が、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。」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、結果及び是正措置報告についても

30 社会通念上、善良なる管理者として果たすべき注意義務。
31 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。

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次のように定められている。

医療情報を取り扱うシステムの運用管理を行う責任であり、当該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ため、医療機関等においては、以下のことが必要である。

・少なくとも管理状況の報告を定期的に受けること

・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こと。

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応にあたる必要がある。

・個人情報保護の責任者を定めること

・電子化された個人情報の保護について一定の知識を有する責任者を決めること

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、及び電子化された個人情報の保護に一定の知識を有する責任者を定め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次のように定められている。

情報保護に関する技術は日進月歩であるため、情報保護体制が陳腐化する恐れがあり、それを適宜見直して改善するためには以下の責任を果たさなくてはならない。

・当該情報システムの運用管理の状況を定期的に監査すること

・問題点を洗い出し、改善すべき点があれば改善すること

そのために医療機関等の管理者は、医療情報保護の仕組み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。

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等に報告し、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次のように定められている。

特に医療機関等は一定の公共性を有するため、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明・公表も求められる。そのため、以下のことが必要である。 ・医療機関等の管理者はその事態発生を公表すること ・原因とそれに対していかなる対処法をとるかについて説明すること

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、確定された原因にもと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、医療機関等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 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、このようなリスクが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と考えられる。

医療機関等と情報処理事業者の間を、閉域網 VPN また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と考えられる（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）。

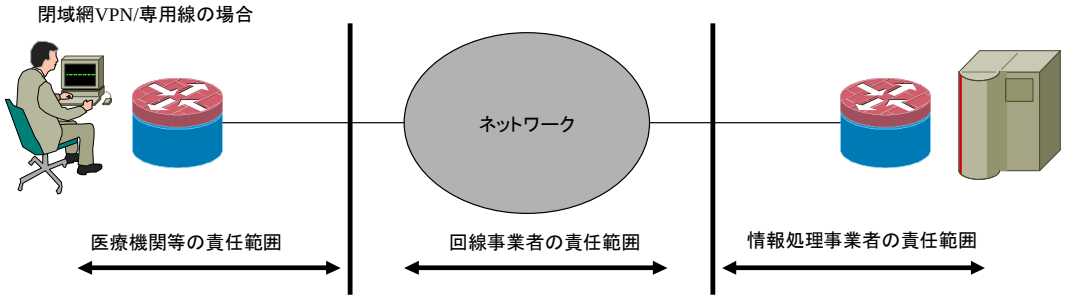

図 9 閉域網/専用線利用時の責任分界点

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必要がある。

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[32]」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、ワードプロセッサー等所謂 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。

更に、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）。

その後、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[33]」（以下、「外部保存改正通知」）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り、平成 22 年 2 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[34]」にて、「医療情報システムの安全管理に関するガイドライン」、「ASP・SaaS における情報セキュリティ対策ガイドライン」、「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」及び「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」の遵守を徹底することが示された。

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。

---

32 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

33 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

34 平成 22 年 2 月 1 日付け医政発 0201 第 2 号・保発 0201 第 1 号厚生労働省医政局長・保険局長連名通知

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 63 年）	診療録等の記載方法について	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[35]」および「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[36]」により「診療録等の電子媒体による保存について[37]」は廃止となった。
2010 年 2 月（平成 22 年 2 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	「医療情報安全管理ガイドライン」、「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」及び本ガイドラインを遵守する旨が記載された。

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（最新版は平成 22 年に策定された 4.1 版である）。

35 平成 16 年法律第 149 号
36 平成 17 年厚生労働省令第 44 号
37 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）
- 「「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 22 年 2 月 1 日付け医政発第 0201 第 2 号・保発第 0201 第 1 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 10 にまとめた。

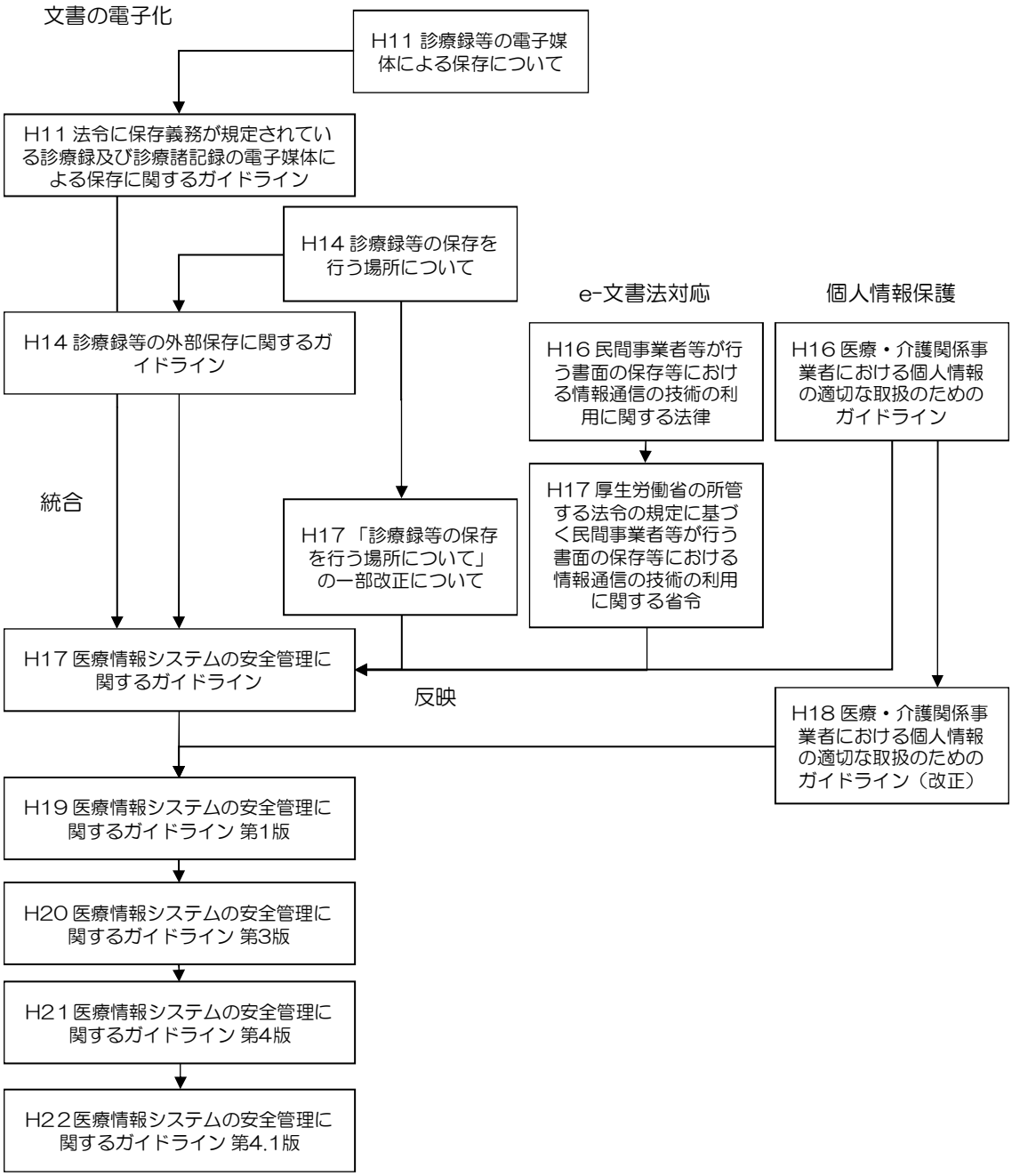

図 10 医療情報の電子記録に関する通知・省令及びガイドライン類の策定経緯

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。

外部保存の対象となる文書等は、「「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 22 年 2 月 1 日付け医政発 0201 第 2 号・保発 0201 第 1 号厚生労働省医政局長・保険局長連名通知）で定められる下記の文書等である。

表 4 外部保存を認める文書等

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	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
7	外国医師等が行う臨床修練に係る医師法第十七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
8	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
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 項に規定されている帳簿
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 条に規定されている診療録等
11	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
12	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
13	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

この他にも、個人情報の保護について留意しなければならない文書等として以下の文書がある。

表 5 個人情報の保護について留意しなければならない文書等

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）

これらの文書の外部保存に関しては、医療情報安全管理ガイドライン「3.3 取扱いに注意を要する文書等」に記される留意事項に従うこと。

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[38]」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「正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であること」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。医療情報を作成する医療従事者及び医療機関等が真正性を確保することができるよう、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、例えば電子署名を付与するなど、真正性を担保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、付与された電子署名を検証するなど、真正性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や光学ディスク等の電子媒体に情報を書き込んで保存する。情報を保存した電子媒体について、認可されていない着脱、持出が行われていないことを保証するため、定期的に検査を行うこと。また、電子媒体上の情報に対して、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等の作業により改ざんの検出を行い、正しく元の情報を提供する。

---

[38] 平成 22 年 2 月 1 日付け医政発第 0201 第 2 号･保発第 0201 第 1 号厚生労働省医政局長･保険局長連名通知

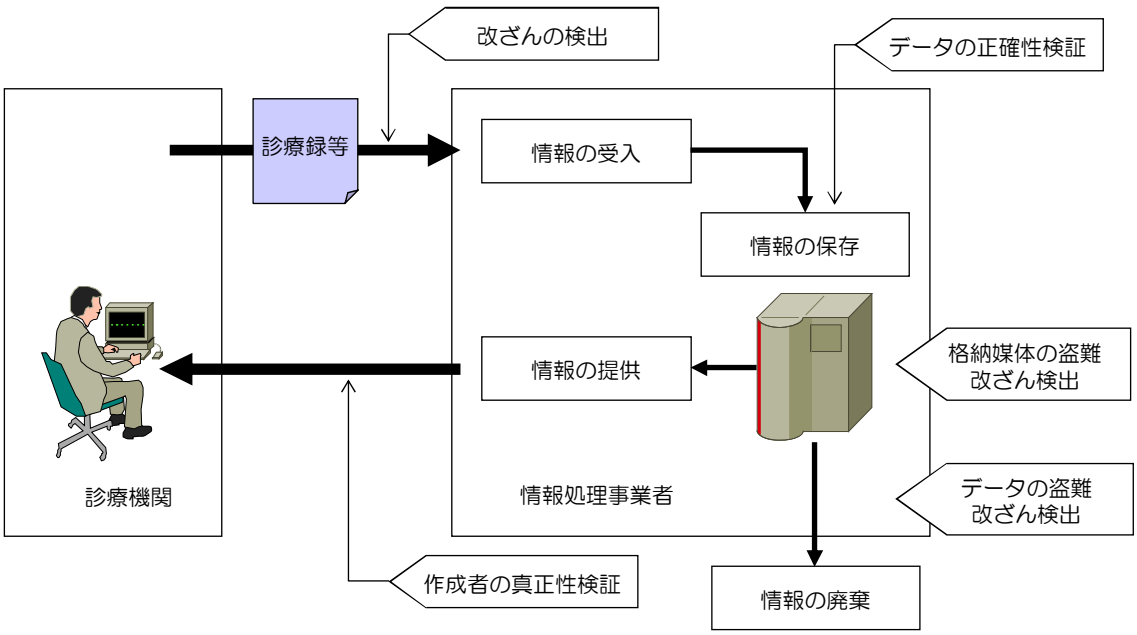

図 11 情報の生成（登録）から廃棄まで（各チェックポイントで改ざんを検査）

なお、情報の廃棄に関しては医療機関等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等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 3 に示すものであり、見読する現場は医療機関等側となる。それぞれの情報に求められる見読可能となるまでの時間的要求について、医療機関等と合意しておくことが求められる。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[39]。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。また、情報処理事業者側の経営上の判断または経済的理由等から、サービス提供を終了せざるを得ない状況も想定される。このような状況においても、医療機関等の業務継続に悪影響を与えないよう、預託データの速やかな返却、他情報処理事業者へのサービス移管を可能とする配慮を行う必要がある。アプリケーション入力の場合は医療情報安全管理ガイドラインの「5 情報の相互運用性と標準化について」に示されている、基本データセット、標準的な用語集、コードセット、データ交換のための国際的な標準規格について、十分に理解し、実装するアプリケーションにおいて提供サービスの可用性、データの互換性の確保に務めること。

[39] 「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「7.6.3 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「7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項」、「7.5.3 情報処理装置のセキュリティ」等に準拠すること。
- 「記憶媒体、設備の劣化による読み取り不能または不完全な読み取り」に対しては「7.6.7 電子媒体の取扱」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」および「(5)　障害等によるデータ保存時の不整合」に対しては「7.10 医療情報処理に関する事業継続計画」等に準拠すること。

情報処理装置に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。

なお、例えば病院又は診療所に勤務する医師による診療に関する診療録においては、医師法 24 条の 2 にあるように、5 年間の保存義務が規定されている。文書の種類によっては診療録よりも長期の保存が義務づけられたものもあるため、情報処理事業者においても、各種文書の保存義務より長期の保存が可能であるよう、事業継続に配慮することが望まれる。

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、業務記録を作成や保存を行わ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に特有の要求であり、これらの国内法の円滑な執行のためにも、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。

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施すべき安全管理策又は実施することが望ましい推奨される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。

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、受託した医療情報を扱う部門、部署を全て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、以下の推奨事項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

(1)　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。
(2)　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。
(3)　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）。

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。

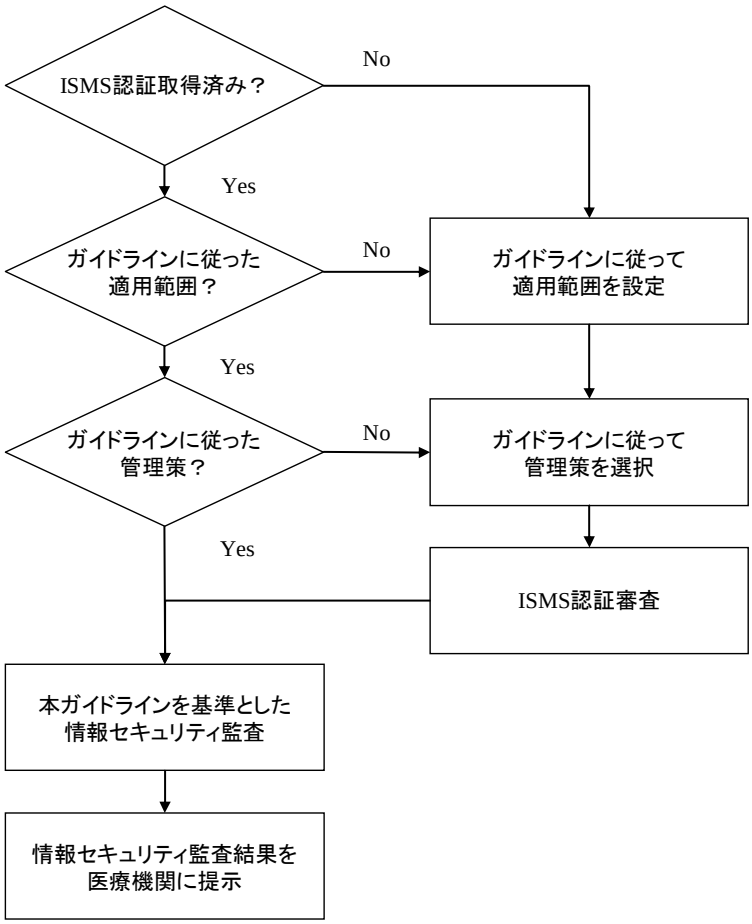

図 12 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

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等に提示することが望まれる。

7.2　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。預託された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。但し、「3 本ガイドラインの対象システム及び対象情報」で示した医療情報交換経路(1)(2)では、情報の分類を行うことができないため、合理的な範囲で本章の記述に従うこと。

7.2.1　資産台帳

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

(1)　医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。
(2)　預託された情報の全てを資産台帳に記録すること。
(3)　必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。
(4)　資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。
(5)　資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。

推奨される安全管理策

(1)　資産台帳等を紙文書として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について検出・記録できるような仕組みを実装することが望ましい。
(2)　資産台帳等に記録する情報には次のようなものが考えられる。
- 整理番号
- 資産の名称（医療情報の名称）
- 資産の医療情報としての種別
- データ形式及び見読化手段
- 資産の所在地と複製の可否及び複製の所在地
- 資産を保存する情報処理装置、電子媒体の識別番号等
- 資産を扱う医療機関等業務の概要
- 情報処理事業者における管理責任者
- 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、複製、廃棄等）

7.2.2 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

(1) 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。
(2) 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。
(3) 預託される情報に対して分類にもとづいたリスク分析を実施すること。
(4) リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。
(5) 分類がわかるように情報にラベルをつけること（電磁的記録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）。
(6) 各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定めること。

推奨される安全管理策

(1) 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が望ましい。

7.3　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作業者の責任を規定し、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。

情報処理装置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。また、医療情報は個人情報であることから、個人情報の保護に関する方針を文書化し、医療機関等に示すことができる状態にしておくことが求められる。

実施すべき安全管理策

(1)　医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
(2)　個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。
(3)　個人情報保護に関しては、医療機関等の監督の下に行うこと。
(4)　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。
(5)　運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。

7.4　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高い機密性が求められていることに配慮しなければならない。機密性を確保するためには、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、及び医療機関等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	第三者が情報処理事業者の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	第三者が情報処理事業者の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）は医療情報システム専用のものと考え、そこでは情報漏洩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	第三者が通信を傍受して不正に情報を入手する

するネットワーク	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を不正に操作して情報を入手する 第三者がアプリケーションを不正に操作して情報を改ざんする 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。アプリケーション開発及び試験の段階で、これらの脆弱性を検出するための試験を十分に実施し、検出された脆弱性に対する対策を施すこと。

7.5　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。

7.5.1　医療情報処理施設の建物に関する要求事項

医療情報システムの設置場所として以下の三種の状況を想定する。

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合

② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合

③ 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合

それぞれの場合において、以下の実施すべき安全管理策を講じなければならない。

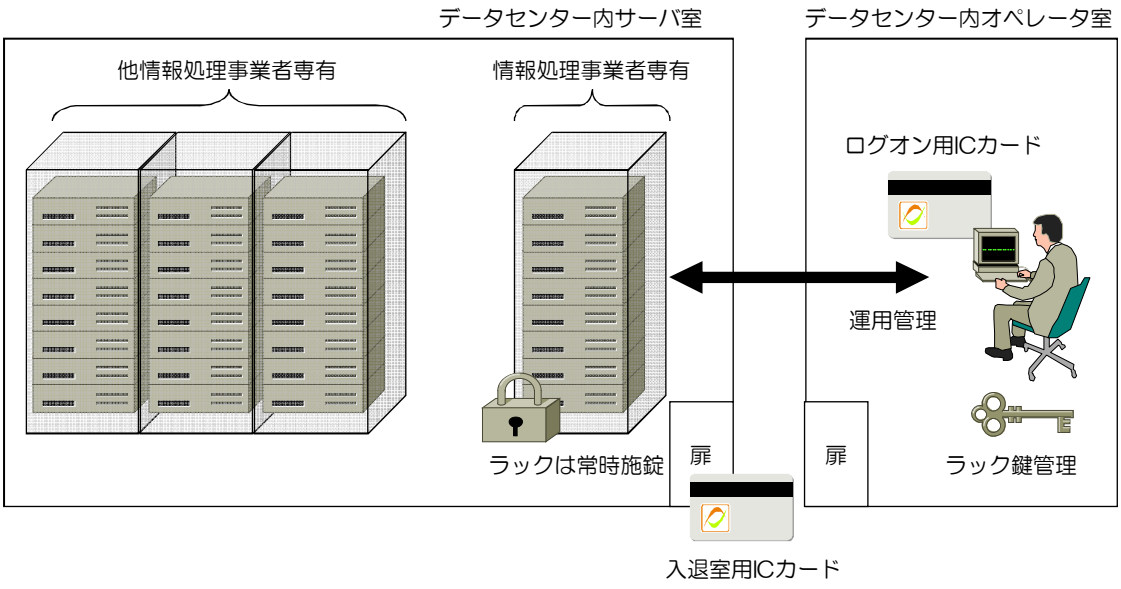

図 13 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合の安全管理の例

なお、外部事業者が運用管理するデータセンターに医療情報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等をセキュリティ領域と考え、不足する物理的安全管

理策に相当するその他の対策を施すことが求められる。

実施すべき安全管理策

(1) 情報処理事業者の専有する領域に医療情報システムを設置する場合には、以下に示す物理的安全管理策を施すこと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。

- 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。
- 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、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、監視カメラ等の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。

7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項

医療情報システムに対する、情報処理事業者の管理外にある者による物理的な不正操作を防止するため、医療情報システム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。7.5.1 に示した三種の状況のそれぞれの場合における安全管理策について示す。

① 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合

実施すべき安全管理策

(1) 医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。

(2) 有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。

(3) 有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、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「7.6.12 ログの取得及び監査」を参照）。

(4) 情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録

した情報処理事業者の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、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。

(5) 情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。

(6) 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、情報処理事業者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。

(7) 情報処理事業者の職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。

(8) 医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。

推奨される安全管理策

(1) 機械式の認証装置で利用する認証要素としては､ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN[40]）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

② 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合

実施すべき安全管理策

(1) データセンターを運営する外部事業者が、①と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認すること。

(2) 医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。

(3) 情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。

(4) データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。

(5) 医療情報システムであることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこと。

[40] Personal Identification Number

推奨される安全管理策

(1)　医療情報システムの設置されるサーバラックの施錠装置については、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

③ 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合

実施すべき安全管理策

(1)　サーバ環境を運営する外部事業者が、①及び②と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認すること。

7.5.3　情報処理装置のセキュリティ

医療情報システム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の管理策を適用すること。

実施すべき安全管理策

(1)　不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。
(2)　医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。
(3)　医療情報等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。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。
(4)　医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。
(5)　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。
(6)　医療情報システムを配置する室内での喫煙、飲食を禁止すること。
(7)　医療情報システム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。
(8)　それぞれの装置は製造元また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。
(9)　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実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択すること。

(10) 医療情報システムを設置するサーバラックについては以下の安全管理策を実施すること。

- 震災時に転倒することが無いよう確実に設置すること。
- 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。
- 扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

(11) 起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「7.6.14 作業者アクセス及び作業者 ID の管理」に従うこと。

(12) 情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。

(13) 不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。

推奨される安全管理策

(1) 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が望ましい。

7.5.4 情報処理装置の廃棄及び再利用に関する要求事項

情報処理装置には様々な情報が格納されている。廃棄及び再利用する際は医療情報及び医療情報システムに関する情報を完全に削除することが望ましい。情報処理装置を廃棄又は再利用する場合には以下の管理策を適用すること。

実施すべき安全管理策

(1) ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。

(2) サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。

(3) ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証

用の機器で不正なプログラム等が記録されていないことを検証すること。

(4) ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。

推奨される安全管理策

(1) 物理的な破壊措置については情報処理事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておくこと。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。

7.5.5 情報処理装置の外部への持ち出しに関する要求事項

利用中の情報処理装置を外部に持ち出す行為は原則として禁止するが、製造元でのみ可能な補修が必要な場合など、止むを得ない事情により外部への持ち出しを行う場合には、以下の管理策を適用すること。

実施すべき安全管理策

(1) 情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。

(2) 持ち出した機器を再度設置するための適切な検証手順を策定すること。

推奨される安全管理策

(1) 持ち出し手順に含まれる事項には次のようなものが考えられる。

- 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等）
- 申請承認プロセス

- 返却確認プロセス、等。

(2) 返却時の検証手順に含まれる事項には次のようなものが考えられる。

- 装置の動作確認
- 盗聴装置等、情報の安全性を脅かす装置の有無
- 悪意のあるプログラムの検出作業
- 収められている情報の検証作業（不正な改ざん等)、等。

7.6　技術的安全対策

医療情報システムの管理、運用における責任体制、扱い手順を確立すること。全ての手順を文書化し、定期的に改善することで、時々刻々と変化するリスクに対処すること。

7.6.1　情報処理装置及びソフトウェアの保守

情報処理装置の更新、補修などのために文書化された保守手順を確立し、適切に運用しなければならない。以下の管理策を適用すること。

実施すべき安全管理策

(1)　保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。
(2)　変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。
(3)　医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。
(4)　情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。
(5)　情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。
(6)　不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。
(7)　医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。
(8)　潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。
(9)　修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。
(10)　保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「7.6.5 第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。

推奨される安全管理策

(1)　変更手順に含まれる事項には次のようなものが考えられる。
- 変更についての影響が及ぶ関係者への通知プロセス
- 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概

要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等）

- 申請承認プロセス
- 変更試験プロセス
- 変更作業に支障が発生した場合の復旧手順
- 変更終了確認プロセス
- 変更に伴う影響を監視するプロセス、等。

7.6.2 開発施設、試験施設と運用施設の分離

データの漏洩、破壊等のリスクを避けるため、医療情報システムの開発施設及び試験施設と運用施設は分離されていなくてはならない。開発主体が情報処理事業者あるいは外部事業者、どちらの場合においても以下の措置を行うこと。

実施すべき安全管理策

(1) 情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。

(2) ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて行うこと。

(3) 開発施設では悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には「7.6.3 悪意のあるコードに対する管理策」に従うこと。

(4) 不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること

(5) 運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。

(6) 医療情報を開発及び試験用データとして直接､利用しないこと｡利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用すること。

推奨される安全管理策

(1) ソフトウェアに悪意のあるコードが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。

7.6.3 悪意のあるコードに対する管理策

医療情報システムに悪意のあるコードが混入しないよう、施設内のサーバ及び端末にて

以下の対策を施す必要がある。アプライアンスサーバ[41]のように、サーバ上で悪意のあるコード対策ソフトウェアを稼動させることができない場合には、サーバと他機器を接続するネットワーク経路上で同様の悪意のあるコード対策を行うこと。

実施すべき安全管理策

(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム)、バックドア（トロイの木馬)、スパイウェア（キーロガー)、ボットプログラム（ダウンローダー）等がある。

(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。
- リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）
- リスク評価の結果として必要であれば定期的にスキャンを実施
- 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン
- 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
- 管理者以外による設定変更やアンインストールの禁止

(3) 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。

7.6.4 ウェブブラウザを使用する際の要求事項

本ガイドラインでの想定において、医療情報システムからインターネット上のウェブコンテンツの閲覧は認めていないため、不正なウェブコンテンツがもたらすリスクは大きなものではないと思われる。しかし、医療情報システム内で必要とする、ネットワーク監視ソフトウェア、サーバ制御ソフトウェア等でユーザインタフェースとしてウェブブラウザを利用し、ダウンロードして動作するコンテンツ、ActiveX、Java アプレット、Flash 等が使われている場合も考えられるため、ウェブブラウザを使用する場合は以下の要求事項を満足する体制を確立すること。

実施すべき安全管理策

(1) ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること

(2) ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定にな

[41] 電子メールサーバ、ウェブサーバ等、特定の用途向けに設計されたサーバのこと。管理が容易であるよう配慮されている。

っていること（管理ソフトウェアが実行されるサーバのみを認可する）。

(3) 認可したサイトからダウンロードされるコードについても「7.6.3 悪意のあるコードに対する管理策」に即して検査されること。

推奨される安全管理策

(1) ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。

7.6.5 第三者が提供するサービスの管理

医療情報システムが設置される領域において、有人監視、機械監視、保守点検作業、清掃作業等については外部の事業者に作業依頼をすることが考えられる。このような第三者が提供するサービスの利用に関して以下の管理策を実施すること。

実施すべき安全管理策

(1) 第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。

(2) サービスの実施、運用、維持について定期的に検証すること。

(3) サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

(4) サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れないこと。

(5) サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。

(6) サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者の職員の入室、退室手順に準ずること。

(7) サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。

(8) 医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 4.1 版」6.8 章 C 項の管理策を実施すること。

推奨される安全管理策

(1) 外部事業者がサービスを実施する際は、情報処理事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。

7.6.6 ネットワークセキュリティ管理

本ガイドラインでは、インターネット等のオープンネットワークとの接続は、以下の「実

施すべき安全管理策」に示すように限定的とするが、リスクとしては、なお大きなものがあるため、インターネット接続に用いられる安全管理措置と同等の措置として、以下の管理策を適用すること。

実施すべき安全管理策

(1) セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。

(2) セキュリティゲートウェイでは､不正な IP アドレスを持つトラフィックが通過できないように設定すること(接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等)。

(3) ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。

(4) ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。

(5) 医療機関等との接続ネットワーク境界には侵入検知システム（IDS)、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。

(6) 侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。

(7) 侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。

(8) 侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。

(9) 医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。

- 外部からの医療情報システムの稼働監視・遠隔保守
- セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード
- オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード
- 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認

証局へのアクセス

- ファイアウォール、IDS・IPS などのセキュリティ機器に対する不正アクセス監視
- 時刻同期のための時刻配信サーバへのアクセス
- これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等）
- その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）

(10) 医療情報システムのサーバ機器等への同時ログオンユーザ数（OS アカウント等）に適切な上限を設けること。

(11) ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。

(12) ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。

(13) 医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないこと。

(14) VPN 接続を行う場合には以下の事項に従うこと。

- 接続時に VPN 装置間で相互に認証を行うこと。
- 傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11 暗号による管理策」に従い、適切な暗号技術を利用すること。
- インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。
- 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるため VPN チャンネルを医療機関等別に構築する等の対策を実施すること。

推奨される安全管理策

(1) 医療情報システムから、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。

(2) 侵入検知システム自身が攻撃・不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施することが望ましい。

7.6.7 電子媒体の取扱

持ち運びが容易な電子媒体からの情報漏えいの被害を抑制するため、電子媒体の扱いに

関する次の管理策を実施して情報流通範囲の限定を確実にすること。また、見読性を確保するため、媒体の保存状況、保存手法について考慮すること。

実施すべき安全管理策

(1) 電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を（9）に示す方式にて確実に廃棄処分すること。

(2) 情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。

(3) 電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。

(4) 電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

(5) 電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管すること。

(6) 製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。

(7) 情報を保管するためにハードディスク装置を用いる場合には、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策を取ること。

(8) 全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行うこと。

(9) 電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。

推奨される安全管理策

(1) 物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については情報処理事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得ること。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。

(2) 医療情報システムにおいてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除することが望ましい。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。

(3)　不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。

7.6.8　情報交換に関するセキュリティ

医療機関等と情報処理事業者間の情報交換に関しては、互いの十分な合意の下に必要な対策を実施する必要がある。

実施すべき安全管理策

(1)　次の情報交換方法について予め合意しておくこと。
- 情報を電子媒体に記録して交換する際の手順
- 情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- 情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

(2)　情報交換手順では搬送の形態によらず次の事項を確実にすること。
- 発送者、受領者を識別し記録すること。
- 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行うこと。
- 交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと）。
- 交換された情報に悪意のあるコードが含まれていないことを確実とすること。

(3)　物理的に情報を搬送する際には以下の対策を実施すること。
- 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。
- 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。
- 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。
- 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。
- 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
- 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

(4)　電子的に情報を転送する際には以下の対策を実施すること。
- 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。

- 送受信する経路は適切な方法で傍受のリスクから保護されていること。
- 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。
- 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。

7.6.9 医療情報システムに対するセキュリティ要求事項

以下に示す、医療情報システムのオペレーティングシステム及び運用に用いるソフトウェア等におけるセキュリティ要求事項を適用すること。

実施すべき安全管理策

(1) 運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類を運用システム上に置かないこと。
(2) 情報処理に不必要なファイル等を運用システム上におかないこと。
(3) 業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。
(4) 運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。
(5) システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

7.6.10 アプリケーションに対するセキュリティ要求事項

アプリケーションにて情報を入力・出力する場合には、アプリケーションに起因する問題の発生を避けるため、以下の管理策を適用すること。

実施すべき安全管理策

(1) 提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。
(2) アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。
(3) アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。
(4) アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証

の際のパスワード)は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

(5) アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。

推奨される安全管理策

(1) アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。

7.6.11 暗号による管理策

アプリケーション及び情報処理装置で暗号を利用する場合には以下の管理策を適用すること。

実施すべき安全管理策

(1) 暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト[42]等を用いること。

(2) 暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。

(3) 電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。

(4) 暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。

(5) 医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリント[43]と比較して、真正性を検証すること。

推奨される安全管理策

(1) 暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。

(2) 暗号鍵の生成は耐タンパー性[44]を有する IC カード、USB トークンデバイスといった安全な環境で実施することが望ましい。

---

[42] http://www.cryptrec.jp/list.html

[43] 公開鍵証明書のハッシュ値のこと。証明書とフィンガープリントを別々の経路で入手し、比較することで証明書の正しさを確認する。

[44] 外部からハードウェア・ソフトウェアの内部構造を解析しようとする攻撃に対する耐性。

(3)　暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。
(4)　電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望ましい。

7.6.12　ログの取得及び監査

医療情報システムの運用に関わるすべてのイベントに対する監査及び事故発生時の原因追及等のためにログを取得する必要がある。以下の管理策を適用すること。

実施すべき安全管理策

(1)　作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。
(2)　監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。
(3)　ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。
(4)　標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。
(5)　ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。
- ログデータにアクセスする作業者及び操作を制限すること。
- 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。
- ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。

推奨される安全管理策

(1)　医療情報システムのすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。
(2)　監査ログに記録する事項としては次のようなものが考えられる。
- 作業者情報（作業者 ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス）
- ファイル及びデータへのアクセス、変更、削除記録（作業者 ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類）
- データベース操作記録（作業者 ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）
- 修正パッチの適用作業（作業者 ID、変更されたファイル）
- 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内

容）

- システム起動、停止イベント
- ログ取得機能の開始、終了イベント
- 外部デバイスの取り外し
- IDS・IPS 等のセキュリティ装置のイベントログ
- サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）

(1) 監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者 ID と、情報の識別子（資産台帳記載の番号等)、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。

ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理することが望ましい。

7.6.13 アクセス制御方針

業務上の要求事項及びセキュリティ上の要求事項にもとづいてアクセス制御方針を確立し、文書化する必要がある。以下の管理策を適用すること。

実施すべき安全管理策

(1) 情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること
(2) 情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること
(3) アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。
(4) それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。
(5) 業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。

推奨される安全管理策

(1) 作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。
(2) 定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。

7.6.14　　作業者アクセス及び作業者 ID の管理

作業者による情報処理装置へのアクセス管理について以下の事項を規定すること。

作業者 ID について実施すべき安全管理策

(1)　作業者は情報処理装置上においてユニークな作業者 ID により識別されること。
(2)　作業者 ID を発行する際に、既存の ID との重複を排除する仕組みを導入すること。
(3)　複数作業者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者 ID でログオンしてからグループ ID に変更する仕組みを利用すること。
(4)　作業者 ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。
(5)　作業者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とすること。
(6)　監視ログの監査時に作業者を確実に特定するため、作業者 ID は過去に使われたものを再利用しないこと。
(7)　不要な作業者 ID が残っていないことを定期的に確認すること。

作業者 ID について推奨される安全管理策

(1)　アクセスを許可された作業者 ID のアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。

特権 ID について実施すべき安全管理策

(1)　特権 ID の発行は必要な最小限のものに留めること。
(2)　特権使用者に昇格可能な作業者 ID を制限すること。
(3)　特権の使用時には作業実施内容を記録すること。
(4)　管理端末以外からの特権 ID による直接ログオンを禁止すること。

特権 ID について推奨される安全管理策

(1)　特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。
(2)　システムの機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。

パスワード管理について実施すべき安全管理策

(1)　情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについて

は削除あるいはパスワード変更を行うこと。

(2) 医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。

(3) 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

(4) 医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。

(5) パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。

(6) パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。

(7) パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。

(8) パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。

(9) パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。

<u>パスワード管理について推奨される安全管理策</u>

(1) 作業者が医療情報システムへのログオン用パスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。

(2) パスワードの品質基準としては、パスワードを十分に長くすること (8 文字以上等)、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。

<u>作業者のログオンについて実施すべき安全管理策</u>

(1) 端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。

(2) パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導

入すること。

作業者のログオンについて推奨される安全管理策

(1) 不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。
(2) 不正なアカウントの利用を防ぐため、作業者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。
(3) 認可されていない作業者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると作業者 ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。
(4) 緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。
(5) ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。

7.6.15 作業者の責任及び周知

各作業者に対しては、自己の責任範囲を認識し、責任を果たすことを周知することが必要である。以下の管理策について作業者に対し周知し、理解したことを確認すること。

実施すべき安全管理策

(1) 各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。
(2) システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。
(3) 離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。

7.7　人的安全対策

医療情報処理を受託する情報処理事業者において医療情報処理に関する管理を的確に行うため、医療情報に触れる機会を持つ情報処理事業者職員は、原則として情報処理事業者の正規職員に限ることを原則とするが、雇用形態が多様化している実態を踏まえ、派遣従業員等の非正規職員についても、秘密保持契約や情報セキュリティ教育等の履行に万全を期し、正規職員のみによる管理と同等レベルの管理が行われることを前提として、認めることとする。

医療情報処理に関わる情報処理事業者職員の選定について、以下の管理策を適用すること。

実施すべき安全管理策

(1)　医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。

(2)　医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

(3)　情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。

(4)　医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

(5)　医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。

推奨される安全管理策

(1)　医療情報を操作する情報処理事業者職員については、規定の安全管理策に違反する

行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これは服務規程等に含めることもできる。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行うこと。

7.8　情報の破棄

医療情報安全管理ガイドラインでは情報の破棄に関して次の表記がされている。「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。」。情報処理事業者は、医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出しなければならない。

「3.1 電子媒体の選択について」で示したように、情報の格納場所つまり電子媒体については、光学ディスク、光磁気ディスク、磁気ディスク等が考えられる。一般に磁気ディスクはハードディスクとして装置に内蔵して使うことが多いが、USB 接続を介して取り外すことができる磁気ディスク装置も広まってきたため、ここでは可搬型か固定型の区別をせずに、電磁的記録の形態として電子的な文書ファイルの破棄手段について示すこととする。

一般のオペレーティングシステムが提供する電磁的記録としての電子ファイルに対する削除機能とは、ファイルの一覧を管理している表[45]において削除というマークをつけることに過ぎず、媒体上の電子文書ファイルはそのままの状態で存続する。医療情報安全管理ガイドラインで求めている情報の破棄に対する適正な措置とはいえず、電磁的記録としての消去、つまり、異なるデータでの上書き、電子媒体であれば物理的破壊を行うことが必要である。以下の管理策を適用すること。

実施すべき安全管理策

(1)　CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。
(2)　ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。
(3)　情報処理事業者は医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出すること。

[45] File Allocation Table 等と呼ばれる。

7.9　医療情報システムの改造と保守

医療情報システムについては製造元が指定する期間ごとに指定の方式で保守を行う。この際には、外部の保守作業者が医療情報システムに触れることになるため、医療情報を第三者からのアクセスから保護する方策が必要になる。この点に関する管理策は「7.5.3 情報処理装置のセキュリティ」および「7.6.5 第三者が提供するサービスの管理」の中でも示しているので参照すること。これらに加えて、以下に示す管理策を適用すること。

実施すべき安全管理策

(1)　オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。

推奨される安全管理策

(1)　開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的なぜい弱性検査を行う。

7.10　医療情報処理に関する事業継続計画

医療情報システムの重大な故障、災害の影響等によるサービスの中断を防止あるいは影響を最小限にとどめるための計画を策定しておかなければならない。また、医療情報処理においては見読性の確保が求められており、医療機関等の要請に応じて速やかに医療情報を閲覧可能な状態に置かなければならない。

本ガイドラインで対象としている医療情報システムではネットワーク経由で情報のやり取りを想定しているため、医療機関等の所在地と情報処理事業者及び医療情報システムの所在地が相当に離れている場合が考えられる。その場合、局地的な災害、地震、火事、水害、停電等により、医療機関等には影響せず、情報処理事業者及び医療情報システムのみが影響を受ける事態も考えられる。このような事態においても、最小限のサービス停止時間でサービスを再利用可能とするためには、医療機関等の所在地に発生する災害の影響を受けない遠隔地であり、互いに影響を受けない二箇所以上を選んで医療情報システムを配置する必要がある（図 14）。

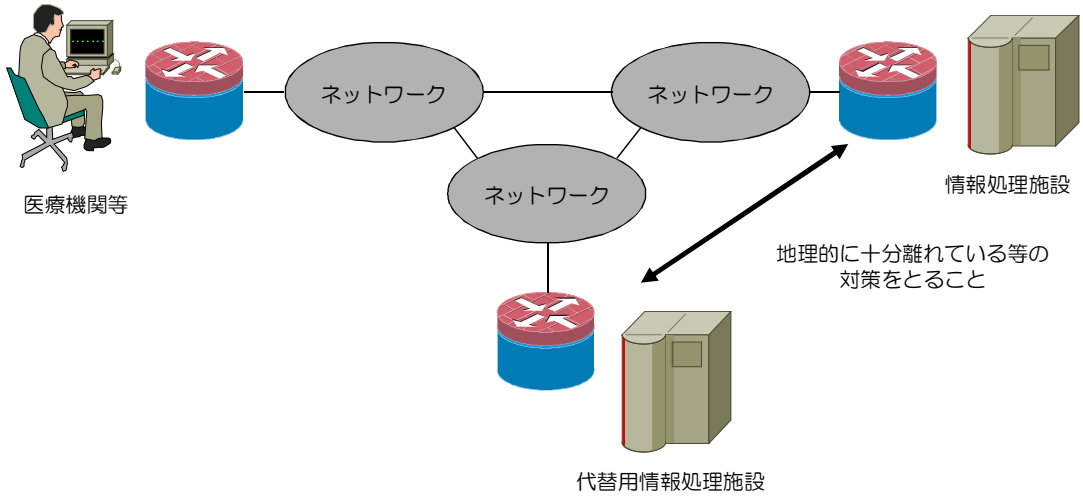

図 14 災害の影響を避けるための情報処理システムの配置

ただし、医療情報システムだけでは事業継続には不足しており、医療情報システムの稼動に必要な作業員を配置しておく、あるいは作業員が迅速に移動する必要がある。

ここでは、医療事業者等に対して事業すなわち情報処理サービスを継続して提供することを主要な目的と考え、事業継続計画の立案と改善についての管理策を示す。

7.10.1　要求事項の識別

医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について洗い出し、それぞれに対する事業継続上の要求事項を識別する必要があ

る。以下の管理策を適用すること。

実施すべき安全管理策

(1) 医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む)、情報処理装置等について識別すること。
(2) 業務プロセス間の相互関係を評価すること。
(3) 事業を継続するための業務プロセスの優先順位を明確にすること。
(4) 医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。
(5) 医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。
(6) ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット[46]）で外部ファイルに出力可能とすることなどの方策を検討すること。
(7) 医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。

7.10.2 事業継続計画の立案及びレビュー

災害または深刻なセキュリティ事故等が発生した際においても事業を継続するために必要な体制を準備しておく必要がある。ここでは事業活動の中断に至る危機状況において情報処理サービスを継続するための計画策定に関する管理策を示す。

実施すべき安全管理策

(1) 医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画を策定すること。
(2) 策定した事業継続計画について模擬試験を含めた適切な方法でレビューすること。
(3) 事業継続計画について定期的に見直しを行うこと。

[46] Portable Document Format、Joint Photographic Experts Group、Portable Network Graphics

推奨される安全管理策

(1)　策定される事業継続計画には次のような事項を含むことが望ましい。

- 事前準備計画
- 「非常時」判断手順
- 関係者の召集、対応本部の設置
- 機器及び作業員の縮退措置及び代替施設の手配措置
- バックアップ施設等、代替施設への切替え措置
- 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等）
- 障害の拡大範囲に関する判断手順、基準
- 正常復帰の判断手順、基準
- 正常復帰後の医療情報システムの点検手順（不正侵入、情報改ざん、情報破損等の検出等）
- 所管官庁への連絡体制、等

8　診療録及び診療諸記録を外部に保存する際の基準

本ガイドラインは情報処理事業者が医療情報を受託して管理するための安全管理策について示すものだが、医療機関等の立場で考えると、情報処理事業者をどのような基準で選ぶべきか、また情報の取扱についてどのような基準を示すべきなのかを考える必要がある。医療情報安全管理ガイドラインでは、この問題について「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」の項で扱っている。

8.1　外部保存を受託する機関の選定基準および情報の取扱に関する基準

ここでは、本ガイドラインで示すような外部の情報処理事業者がデータセンター等を保存場所として情報を保管する場合の、医療機関等が情報処理事業者に要請する規定として以下の事項が示されている。

> この場合、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。
>
> そのため、それらの事業者等が、本章の他の項の要求事項、本ガイドラインの他の章で言及されている、責任のあり方、安全管理対策、真正性、見読性、保存性および C 項で定める情報管理体制の確保のための全ての要件を満たす必要がある。(医療情報安全管理ガイドライン 8.1.2 1. ③)

つまり、「情報を保管する機関」すなわち本ガイドラインの対象である医療情報管理を受託する情報処理事業者は、医療情報安全管理ガイドラインの「8. 診療録及び診療諸記録を外部に保存する際の基準」の要求事項その他、全ての要件を満たす必要があるということになる。

加えて、情報の取扱については以下のような事柄を要請することとされている。

> 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、不当な営利、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。
>
> 民間等で医療情報の外部保存を受託する事業者に対しては、これらの行為を規制するための指針が外部保存通知にある通り経済産業省や総務省で定められている。従って、医療機関等は契約も含め、その遵守状況を十分確認する必要がある。
>
> 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したり、あるいは情報処理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。

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。（医療情報安全管理ガイドライン 8.1.2 2. ③）

これは、医療情報については外部保存を目的として預かるのであって、情報処理事業者による医療情報の閲覧は禁止されており、暗号化やアクセス制御により技術的にも閲覧を行うことができないような管理策を適用せよということと考えられる。

更に情報の提供に関しては次のように規定されている。

いかなる形態であっても、保存された情報を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。これは匿名化された情報であっても同様である。

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以外にも提供する場合は、あくまで医療機関等同士の同意で実施されなくてはならず、当然、個人情報の保護に関する法律に則り、患者の同意も得た上で実施する必要がある。（医療情報安全管理ガイドライン 8.1.2 3. ③）

受託した医療情報は保存主体である医療機関等あるいは保存主体及び患者本人の同意を得た上で他の医療機関等に提供することだけが許されるということで、後者については、患者が別の医療機関等に移動あるいは分析等を依頼する場合を想定したものと考えられる。

このように、外部の情報処理事業者が医療情報を受託管理する際の医療機関等からの要請事項は厳しいものとなっている。本ガイドラインは、このような要請事項を満足できるように構成しているが、医療情報安全管理ガイドラインの「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」の「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」に従っていることを示すことができるよう、適用している安全管理策を適用宣言書の形で整理しておくことが望ましい。

8.2　外部保存契約終了時の処理について

医療情報については個人情報と同等の扱いが必要であり、医療機関等との契約により定められた保存期間が経過した場合、あるいは医療機関等と情報処理事業者との委託契約が終了する時点で迅速に廃棄処理をしなくてはならない。このためには、医療機関等と情報処理事業者間で廃棄処理手順について定め、合意しておく必要がある。ネットワークを介して医療機関等の外部に保存された情報については、確実に情報が廃棄されたことを医療機関等に保証する必要がある。このためには、受領した情報と管理している情報の一覧の整合性を医療機関等が確認できるように、預かっている情報について台帳を維持管理することが求められる。また、台帳の操作については特定の作業員だけが行うこととし、複数人による確認等を行うことで、台帳上の情報の整合性について保証を行うこと。

情報処理業務の一部を再委託している場合には、再委託先においても同等の廃棄手順により確実に情報を廃棄すること。

9　参考文献

● 情報セキュリティマネジメントシステム要求事項（JIS Q 27001:2006）
2006 年 5 月　日本工業標準調査会審議（日本規格協会発行）

● 情報セキュリティマネジメントシステムの実践のための規範（JIS Q 27002:2006）
2006 年 5 月　日本工業標準調査会審議（日本規格協会発行）

● ISMS ユーザーズガイド －JIS Q 27001:2006（ISO/IEC 27001:2005）対応－
2006 年 12 月財団法人　日本情報処理開発協会

● 医療機関等向け ISMS ユーザーズガイド – ISMS 認証基準（Ver.2.0）対応
2004 年 11 月 8 日　財団法人　日本情報処理開発協会

● 個人情報保護マネジメントシステム-要求事項　（JIS Q 15001:2006）
2006 年 5 月　日本工業標準調査会審議（日本規格協会発行）

● IT セキュリティマネジメントのためのガイドライン（TR X 0036-1～5::2001）
2001 年 3 月　財団法人　日本規格協会

● 情報システムの設備ガイド　（JEITA ITR-1001B）
2006 年 5 月改正　社団法人　電子情報技術産業協会

● 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
2010 年 9 月改正　厚生労働省

● 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
2009 年 10 月改正　経済産業省

● 保健医療福祉分野のプライバシーマーク認定指針（第 3.1 版）
2011 年 7 月　一般財団法人　医療情報システム開発センター

● 事業継続計画策定ガイドライン
（企業における情報セキュリティガバナンスのあり方に関する研究会　報告書　参考資料）
2005 年 6 月　経済産業省

● SaaS 向け SLA ガイドライン
2008 年 1 月　経済産業省

● 安全なウェブサイトの作り方 改訂第 5 版
2011 年 4 月　独立行政法人情報処理推進機構

10 図表一覧

以上