資料Ⅱ①

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

目次

1．はじめに

このガイドラインは、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第７条第１項に基づき平成１６年４月２日に閣議決定された「個人情報の保護に関する基本方針」（以下、「基本方針」という。）を踏まえ、また、法第６条及び第８条に基づき法に定める事項に関して必要な事項を定め、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等（以下、「医療情報受託者」という。）が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定めるものである。

医療情報については、基本方針及び国会における附帯決議において、個人情報の性質や利用方法等から、特に適正な取扱いの厳格な実施を確保する必要がある分野の一つであると指摘されており、安全管理措置に関して積極的な取組が求められている。

他方、医療情報受託者には、「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」（以下、「経済産業分野ガイドライン」という。）の規定が適用されているが、経済産業分野ガイドラインは、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いに携わる医療情報受託者に対しては、同ガイドラインで規定される安全管理措置よりも十分な安全管理措置が求められる。

これらを踏まえ、医療情報受託者が講ずべき措置について、経済産業省商務情報政策局に設置された「パーソナル情報研究会」において検討がなされ、平成２０年３月、「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」（以下、「研究会ガイドライン」という。）が示された。本ガイドラインは、研究会ガイドラインに従い、法の趣旨を踏まえ医療情報受託者における個人情報の適正な取扱いが確保されるよう、医療情報受託者が講ずべき措置に関連する項目を挙げている。

本ガイドラインのうち、「２．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」に記載されている項目については、それに従わなかった場合、経済産業大臣により法の規定違反と判断され得る。一方、「望ましい」と記載されている項目については、それに従わなかった場合でも法の規定違反と判断されることはない。しかし、「望ましい」と記載されている項目についても、法の理念（法第３条）や医療情報の高い機微性を考慮し、できるだけ取り組むことが望まれるものである。

なお、本ガイドラインに記載されている各項目に取り組むに当たっては、研究会ガイドラインの内容を十分に理解することが必要である。

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うち、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。なお、本ガイドラインにおいて「医療情報」とは、医療に関する患者情報（個人識別情報）を含む情報という意味で用いている。

【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条及び歯科医師法施行規則第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】
診療諸記録ともいわれ、診療の過程で知りえた患者に関わる情報及び作成された記録から診療録を除いた部分のことで、検査結果、手術所見、医用画像（レントゲン写真等）、看護記録等を指す。本ガイドラインに基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、患者の既往症、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、例えば介護認定時に医師が医師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。したがって、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】
患者を対象とする医療に関して、患者情報を含む医療情報及びその医療情報を扱うシステムを指す。

【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（情報セキュリティマネジメントシステム）】
ＩＳＭＳ適合性評価制度では、「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。」と定義している。ＩＳＯ（国際標準化機構）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」という。）。

【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」という。）。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 】
日本工業標準調査会により審議された個人情報保護マネジメント要求事項の日本工業規格である（以下、「JIS Q 15001」という。）。

【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】
リスクに対して実施される対策のことを指す。

【適用宣言書】
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）】
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。インターネット上に構築されたものをインターネットＶＰＮと呼ぶ。

【閉域網／閉域網ＶＰＮ（IP － VPN）】
回線提供事業者が専有する回線上に構築された、特定加入事業者間のみを接続するネットワークの提供形態を指す。国内においては閉域ＩＰ網を提供するIP-VPNとして利用されることが多い。

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、インターネットＶＰＮ、閉域網ＶＰＮ（IP-VPN）の三種類を用いることにする。

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うち、特定の意味を持たせている用語について以下に示す。

【情報処理事業者】
医療情報処理を受託する情報処理事業者を意味する。

【作業者】
情報処理事業者において情報処理機器を操作する者を意味する。

【医療情報処理施設】
情報処理機器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。

【医療情報処理システム】
サーバ、端末、接続デバイス等、情報処理に関与する機器全体を意味する。

2．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

2.1. 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

医療情報に係る情報処理事業を受託する機関においては、合理的・客観的な基準による公正な第三者認証を取得すること。

2.1.1. ＩＳＭＳ認証取得時の考慮事項

（１）認証取得又は更新の際にＩＳＭＳの安全管理策として、本ガイドライン「２．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。）。
（２）受託管理する医療情報の入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）安全管理策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安全管理策を明確に記載すること。）。

2.1.2. 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

情報処理事業者がＩＳＭＳ認証を取得する際には、その適用範囲が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、部署を含んでいること、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。
また、本ガイドラインに従ってＩＳＭＳ認証を取得した後に、本ガイドライン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受け（少なくとも１年に１回以上の頻度で）、監査結果を医療機関に提示することが望まれる。

2.2. 原則として行うべきではない行為

（１）情報処理事業者施設において無線ＬＡＮを利用すること。
（２）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、侵入検知システム及び侵入防止システム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。）。
（３）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。）。

2.3. 情報資産管理

2.3.1. 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。

（１）重要な情報について資産台帳等を作成管理すること。
（２）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
・資産の価値
・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）
（３）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。
（４）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。
（５）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。

2.3.2. 情報の分類

（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）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）。
（４）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。
（５）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。

2.4. 組織的安全管理策（体制、運用管理規程）

（１）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。
（２）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「2.7.1.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。
（３）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。
（４）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。

2.5. 医療情報の伝達経路におけるリスク評価

医療情報の取扱い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。

2.6. 物理的安全対策

2.6.1. 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

（１）医療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。
（２）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。
（３）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。
（４）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、医療機関ごと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合う等、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。
（５）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。
（６）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。
（７）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。

2.6.2. 医療情報処理システムへの入退館、入退室に関する要求事項

（１）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。またはハードウェアトークン若しくはＩＣカード（以下、「認証デバイス」という。）に生体認証若しくは暗証番号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。
（２）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、同じデバイスで再度入退室を行うこと等の不正行為を防ぐ装置を設置すること。
（３）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「2.7.12.ログの取得及び監査」を参照）。
（４）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。
（５）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。
（６）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）。
（７）医療情報処理施設内への個人的所有物の持ち込みを認めないこと。

2.6.3. 情報処理装置のセキュリティ

（1）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。
（2）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。
（3）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。
（4）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。
（5）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。
（6）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。
（7）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廃棄を選択すること。
（8）機器を設置するサーバラックについては、震災時に転倒することが無いよう確実に設置し、熱による障害を防ぐため十分な換気装置を設け、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。

2.6.4. 情報処理装置の廃棄及び再利用に関する要求事項

（1）ハードディスク等の固定記憶装置について医療情報処理システム内の別の機器で再利用する場合には、再利用前に確実な方法でデータを消去すること。
（2）パスワードの生成規則に関する情報を漏らさないよう、計算機のＢＩＯＳパスワード、ハードディスクパスワード等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、運用しているシステムとは独立した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、データの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）等を適用すること。
（5）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、十分な理解を得ておくこと。

2.6.5. 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。

（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。手順には、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が含まれる。
（2）持ち出した機器を再度設置する際には、情報処理装置に悪影響を及ぼさないよう、適切な検証手続きを行うこと。検証手続きには、悪意のあるプログラムの検出作業、納められている情報の検証作業（不正な改ざんの有無等）等が含まれる。

2.7. 技術的安全対策

2.7.1. 情報処理装置及びソフトウェアの保守

（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、影響を最小限に抑える方策を検討すること。
（3）情報処理に関わる機器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が医療機関等の業務に過大な影響を与えないよう適切な計画を立てて実施すること。
（4）適切な変更手順を策定すること。手順には以下の事項を含むこと。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。
（5）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、定期的に監査を実施すること。
（7）医療情報処理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すること。

2.7.2. 開発施設、試験施設と運用施設の分離

（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もの又は十分に安全性を検証した上で外部開発事業者に開発依頼したものを用いること。
（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（以下、「開発施設」という。）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「2.7.3.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に示し、了解を得た上で利用すること。

2.7.3. 悪意のあるコードに対する管理策

本ガイドラインの想定するシステムではサーバ等の機器類は、インターネットとは直接接続することが無いため、インターネット上で提供される悪意のあるコード対策ソフトウェアのアップデートファイル又はリポジトリに直接アクセスすることができない。このため、アップデートファイルについては電子媒体等を利用して運用システムに設置する等の対策を実施すること。

（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。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）、（週に１回以上の）定期的な自動スキャン、外部記憶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。
（３）管理者以外が悪意のあるコード対策ソフトウェアの設定変更やアンインストールができないような設定がされていること。
（４）悪意のあるコード対策ソフトウェアにおいて、定義ファイル、スキャンエンジンの自動アップデート、又は定期的な更新が十分な頻度で行われていること。
（５）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、ユーザ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又は隔離措置をとるといった対策が行われていること。

2.7.4. ウェブブラウザを使用する際の要求事項

医療情報処理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。

（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）ウェブブラウザからメールクライアント等のアプリケーションが起動されないこと。
（４）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「2.7.3.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。

2.7.5. 外部事業者が提供するサービスの管理

医療情報処理システム内において、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。

（１）提供されるサービスについてセキュリティ管理策及びサービスレベルを確認すること。
（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）サービス実施中は顔写真を券面に入れた身分証明を携帯し、情報処理事業者の正規職員が監督している状況で作業を行うこと。
（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、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。

2.7.6. ネットワークセキュリティ管理

（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）において、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。
（２）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）ネットワーク機器及びサーバ、端末の空いているネットワークポートへの接続を制限すること。
（４）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（以下、「ＩＤＳ」という。）及び侵入防止システム（以下、「ＩＰＳ」という。）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。
（５）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。
（６）侵入検知システムが、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必要な項目が含まれていること。
（９）医療機関等と情報処理事業者を接続するインターネット上のＶＰＮ回線を通じたアクセス、及び医療情報処理システムの稼働監視、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、電子署名検証における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の場合を除いて、インターネット等のオープンネットワークを介した情報処理設備へのアクセスを行わないこと。
（１０）専用回線等のクローズネットワークを介して情報処理設備に接続する場合においても適切な認証を用いること。
（１１）情報処理システムへの同時ログオンユーザ数に適切な上限を設けること。
（１２）認識されていないログオンユーザを識別できるように、ログオンするユーザアカウントについては計画を立て、計画に即していることを常に確認すること。
（１３）ネットワーク経由で直接、特権ユーザとしてログオンする行為を禁止すること。
（１４）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。

（１５）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。
（１６）ＶＰＮ接続を行う場合にはＶＰＮ装置間で相互に認証を行うこと。
（１７）ＶＰＮ接続を行う場合における認証は、傍受、リプレイ等のリスクを最小限に抑えるために適切な暗号技術を利用すること。
（１８）不正なトラフィックがネットワーク境界を越えて流れていないことを監視すること。

2.7.7. 媒体の取扱

（１）可搬型の記憶媒体について医療情報処理システム外の不要な持ち出しを行わないこと。
（２）ＣＤ、ＤＶＤ、ＭＯ等の可搬型記憶媒体については、追記のできない光学メディア、ＣＤ－Ｒ、ＤＶＤ－Ｒを用いる等して、情報処理システムの内外を問わず再利用できないようにする。なお、バックアップ目的でＭＴ（磁気テープ）、ＤＡＴ等の大容量媒体を用いる場合には、その管理を厳重に行うことで再利用を認める。
（３）情報交換の目的で記憶媒体を使う場合には媒体上の情報をハードディスク等の固定記憶装置に複製した後に記憶媒体を廃棄処分とする。
（４）情報交換、情報保管以外の目的で記憶媒体を用いないこと。
（５）医療情報処理施設内においては情報処理機器に接続できる外部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。加えて、認められていない種類の外部媒体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。
（６）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。
（７）媒体の利用に関する記録を行い、媒体の廃棄後も一定期間にわたり保存すること。
（８）媒体損失のリスクを最小限にするため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。
（９）製造者の定める保管期間を超過することがないよう、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。
（１０）媒体の一覧表を管理し、媒体の盗難、紛失を迅速に検知できる体制を構築すること。
（１１）全ての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。
（１２）媒体により情報を交換する場合には媒体内のデータにパスワードによるアクセス制限又は暗号化を施すこと。
（１３）配送業者が媒体の配送中のリスクに対して適用している対策を確認した上で配送業者を選択すること。
（１４）配送業者から媒体を受け取る時は、情報処理設備とは別の搬入・搬出専用の区域で正規職員が直接受け取ること。受け取る際には、配送業者の身分確認を行うこと。
（１５）配送に際しては内容物を外部から知ることができないコンテナを用い施錠した

上で配送すること。
（１６）ＣＤ、ＤＶＤ等の光学メディア、ＭＴ（磁気テープ）等の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）を適用すること。
（１７）媒体の破壊については情報処理事業者自身で行うこと。破壊した媒体の処理は外部の専門事業者に依頼することが可能である。
（１８）ハードディスク等の固定記憶装置の扱いについては「2.6.4.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。

2.7.8. 情報交換に関するセキュリティ

（１）医療機関等と情報処理事業者間の情報交換に関して、次の事項を予め合意しておくこと。
・情報を記憶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
（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、アプリケーションログオン時の確実な認証を行うこと。
・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。）。
（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。
・配送業者等による記憶媒体の抜き取り等を防ぐため、交換する記憶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。
・配送業者等による記憶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。
・記憶媒体を発送、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。
（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。

2.7.9. 医療情報処理システムに対するセキュリティ要求事項

（１）運用システムの混乱を避けるため、開発用コード又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）作業者個人のファイル、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。

2.7.10. アプリケーションに対するセキュリティ要求事項

（１）アプリケーションに対するデータ入力に関して、操作上の誤りによりデータの不整合が発生しないよう、データ範囲及びデータタイプの制限、入力文字種及び長さの制限等を設定、自動的な検査等により誤りを検出する機構を導入すること。
（２）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。
（３）アプリケーションの入力及び出力データに悪意を持った不正なデータ（不正な画面エスケープシーケンス、ＨＴＭＬにおけるメタキャラクタ、シェルコマンド等）が含まれていた場合の悪影響を避けるため、自動的な検査及び妥当性確認機構を導入すること。
（４）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。
（５）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。
（６）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こと。

2.7.11. 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。

（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等を用いること。

（2）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。
（3）暗号鍵の生成は耐タンパー性を有する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。
（4）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。
（5）暗号鍵が漏えいした場合に備えた対応策を策定しておくこと。
（6）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。
（7）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。
（8）医療機関等から受け付けるデータを検証するための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と比較して、正確性を検証すること。

2.7.12. ログの取得及び監査

（1）作業者の活動、機器で発生したイベント、システム障害等を記録した監査ログを作成し管理すること。
（2）ログを利用して正確に事故原因等を検証するため機器の時刻を同期し、定期的に検証を行うこと。
（3）時刻の同期のため、運用施設内に時刻サーバを導入し、時刻サーバの提供する時刻にすべてのサーバ、コンピュータ、その他機器類を同期しておくこと。
（4）以下に示すシステム使用状況等について監査ログに記録し、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。
- 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）

（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、記憶媒体への書き出し、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。

2.7.13. バックアップ

（1）バックアップ施設は自然災害の影響を同時に受けないよう、医療情報処理システムから十分離れた地点に構築すること。
（2）バックアップ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。
（3）見読性の要求から、医療情報について医療情報処理システムとバックアップ施設の間で同期をとること。同期をとるためのネットワーク回線については本ガイドラインで規定するネットワーク安全管理策に従うこと。
（4）バックアップ施設及びバックアップ装置は情報処理事業者自らが管理することを原則とするが、遠隔地に設置するため緊急時の対応が遅れる等の事態を避けるため緊急時対応を再委託する場合には、再委託先事業者の安全管理基準を医療機関に通知し承認を受けること。
（5）災害時などにおいても見読性を損なわないよう、バックアップ施設においても同等の情報処理機能を備えることが望ましいが、情報処理事業者に保存される医療情報の性質、サービス提供コスト等との兼ね合い等を考慮し、医療機関等に事前にバックアップ施設における情報処理サービス機能等について説明し、了解を得ること。

2.7.14. アクセス制御方針

（1）情報処理に用いる情報処理機器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。
（6）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。
（7）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。

2.7.15. 作業者アクセス及び作業者ＩＤの管理

（１）作業者は情報処理機器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の発行は情報処理及び情報処理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）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。
（８）不要な作業者ＩＤやアカウントが残っていないことを定期的に確認すること。
（９）特権使用者に昇格可能な作業者ＩＤを制限すること。
（１０）特権の使用時には作業実施内容を記録すること。
（１１）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。
（１２）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。
（１３）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。
（１４）システムログオン用のパスワードはハッシュ値等、パスワードを復元できない形で情報を保管すること。
（１５）システムログオン用のパスワードを保管するファイルは一般作業者による閲覧を制限すること。
（１６）作業者がシステムログオン用の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、例えば乱数によりパスワードを生成するプログラム等を導入すること。品質の基準としては、パスワードを十分に長くすること、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。
（１７）システムログオン用の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。
（１８）システムログオン用の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。

（１９）変更時には変更前のパスワードの入力を要求し、一定回数以上間違えた場合には、そのアカウントを一時的に使用できない（ロックアウト）ようにすること。
（２０）パスワード発行時には、乱数から生成した仮のシステムログオン用の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こと。
（２１）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。
（２２）リモートログオンを行う際には傍受によるパスワードの漏えいリスクを避けるため、暗号により通信データを保護する方式を採用すること。
（２３）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。
（２４）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。
（２５）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。
（２６）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。
（２７）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。
（２８）連続したログオンの失敗回数を制限するアカウントロック機能を有効とすること。更に、ログオンの連続した失敗が許容限度回数に達した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。
（２９）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。

2.7.16. 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。

（１）各作業者は自身のパスワードを秘密にし、紙、電子ファイル、携帯電話又はPDA等に記録及び保管しないこと。パスワードを記録する必要がある場合は、予め定められた方法で記録し、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。

2.8. 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要員は、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。

（1）医療情報を操作する可能性のある要員の全てについて、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あるいは守秘義務契約への署名を求めること。派遣従業員については機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要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）要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要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。

2.9. 情報の破棄

（1）破棄する電子文書ファイルが電子媒体上で一つだけ記録されている場合、電子媒体が光学メディアであれば媒体自身を破壊処分すること。
（2）光学メディアに複数の電子ファイルを記録する場合には、電子媒体ごと破棄できるように、予定された廃棄時期が同じ電子ファイルをまとめて記録しておくこと。
（3）ハードディスク等の固定記憶装置の扱いについては「2.6.4.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。

2.10. 情報システムの改造と保守

（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、情報処理ソフトウェアに対する影響を評価及び試験して確認すること。
（2）開発された情報処理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。ただし、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こと。

2.11. 医療情報処理に関する事業継続計画

2.11.1. 要求事項の識別

（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要員を含む）、情報処理設備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）医療情報処理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）医療情報処理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、大きすぎるものがあれば、影響度を低減する方策及びその可能性について検討すること。

2.11.2. 事業継続計画の立案及びレビュー

（1）医療情報処理サービスの提供における業務プロセス及び医療情報処理システムの優先順位にもとづいて、機器及び要員の代替を含めた復旧措置を立案し、医療情報処理に関する事業継続計画として策定すること。
（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。

3．ガイドラインの見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて見直しを行うよう努めるものとする。

資料Ⅱ②

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 3 月

パーソナル情報研究会

【 目 次 】

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」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]。さらに、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]。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」という。）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、厚生労働省医政局に設置された「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）に対する医療情報システムの具体的指針という側面も持ち合わせる。

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

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。

さらに、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、情報及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」（以下「医療情報安全管理ガイドライン」という。）が策定された。

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。しかし、外部保存ガイドラインでは医療に関連する情報は高度な機密性が求められるという理由により、医療機関等自らが外部保存を実施することを前提として策定されている。他方、医療機関が保有する診療録等を専門の民間情報処理事業者が管理することで、医療機関にとっては個人情報漏えい等のリスクを低減することが可能になると指摘されている。このため、厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」において、医療情報の外部保存が認められる際のルール化を進めるべく、現在、医療ガイドラインの改正作業が進められている。

医療機関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、本「パーソナル情報研究会[7]」は、医療情報の外部保存の安全性に万全を期す

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」ことを目的に設置されている。

べく、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。

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。

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医療機関等で実施される安全管理策と同等以上のセキュリティレベルを情報処理事業者に求めるものであるが、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うち、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 】

診療諸記録ともいわれ、診療の過程で知りえた患者に関わる情報及び作成された記録から診療録を除いた部分のことで、検査結果、手術所見、医用画像（レントゲン写真等）、看護記録等を指す。本ガイドラインに基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、患者の既往症、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、例えば介護認定時に医師が医師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。したがって、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 】

患者を対象とする医療に関して、患者情報を含む医療情報及びその医療情報を扱うシステムを指す。

【 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」という。）。

【 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」という。）。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 】

日本工業標準調査会により審議された個人情報保護マネジメント要求事項の日本工業規格である（以下「JIS Q 15001」という。）。

【 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を認める制度[11]」

[8] 財団法人 情報処理開発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
[11] http://privacymark.jp/privacy_mark/about/outline_and_purpose.html より引用

【 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） 】

リスクに対して実施される対策のことを指す。

【 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） 】

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。インターネット上に構築されたものをインターネット VPN と呼ぶ。

【 閉域網／閉域網 VPN（IP－VPN） 】

回線提供事業者が専有する回線上に構築された、特定加入事業者間のみを接続するネットワークの提供形態を指す。国内においては閉域 IP 網を提供する IP-VPN として利用されることが多い。

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、閉域網 VPN（IP-VPN）、インターネット VPN の三種類を用いることにする。

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うち、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機器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 】

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

【 医療情報処理システム 】

サーバ、端末、接続デバイス等、情報処理に関与する機器全体を意味する。

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[12]を確保するために実装すべき管理策（以下「安全管理策」という。）を具体化して提示することが主要な目的である。安全管理策を選考するために、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機器、業務を実施する職員及び組織構成等を情報資産として数え上げ、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、更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し、リスクの大きさにもとづいたリスク対応を選択、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、という手順を行った。これは ISMS[13]ユーザーズガイド[14]に示される ISMS 構築ステップに倣ったものである。

本ガイドライン策定において重視した点は、医療情報及び医療情報処理に関わる機器を情報資産と考え、情報セキュリティ対策の原則として、情報資産へのアクセス可能領域、情報資産の流通経路、情報資産の可用性について認識し、リスクを極小化するため、移動経路を最小化すること、いずれの場所、時間においても制御可能とすること、迅速な異常の検出を可能とすることといった情報処理事業者の安全管理策に加えて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に対して情報処理事業者の安全対策レベルを客観的に示すため、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である。

このような認証及び認定には、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、認証又は認定等を受けることが求められる。

---

12 6 章で説明する真正性、見読性、保存性を含む
13 Information Security Management System、情報セキュリティマネジメントシステム
14 （財）日本情報処理開発協会

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3版」に JIS Q 27001 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（図 1）。

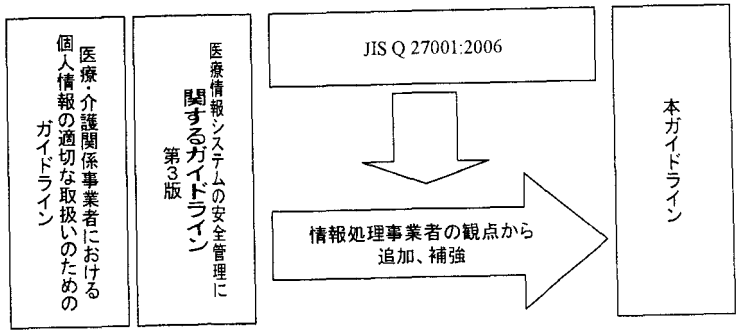

図 1 具体的な本ガイドラインの構成

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も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。

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要件とする。

このため、適用範囲を医療情報処理システム全般として、上記の包括的安全管理策を記した適用宣言書を元にして、ISMS 評価制度に基づく第三者認証を取得することが推奨される。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。

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 情報システムの基本的な安全管理	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
7 電子保存の要求事項について	6 電子保存の要求事項について
8 診療録及び診療諸記録を外部に保存する際の基準	8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情報処理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、扱う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 電子保存及び外部保存が許されている文書を参照）を対象とし、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 2 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組み合わせることを想定する。

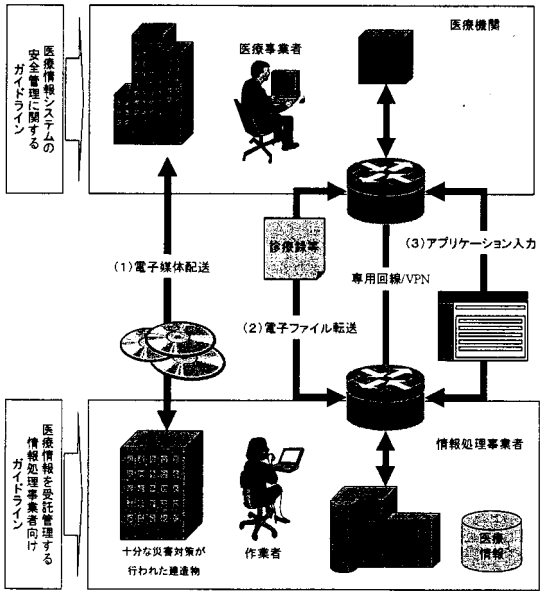

図 2 本ガイドラインで対象とする情報システムの概念

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、情報を閲覧、分析等を目的として取り扱うことはあってはならず、許されない。」、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。」（医療情報安全管理ガイドライン 8.1.2 章参照）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、情報処理システムを設置する場所については、情報処理事業者が専有する建造物あるいはフロア（自社所有のデータセンター等）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設置場所を借りて利用する場合が多いと考えられる。その場合には、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を選択すること。設置するサーバラックについては、情報処理事業者の専有とし、医療情報処理装置以外の機器を設置しない、扉の鍵管理を厳格に行う等の物理的対策を施すこと。

情報処理ソフトウェアをサーバ上で動作させる場合、サーバにアクセスするための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、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。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、閉域網 VPN（IP-VPN）あるいは IPsec[15]と IKE[16]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 3）。

[15] 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
[16] 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

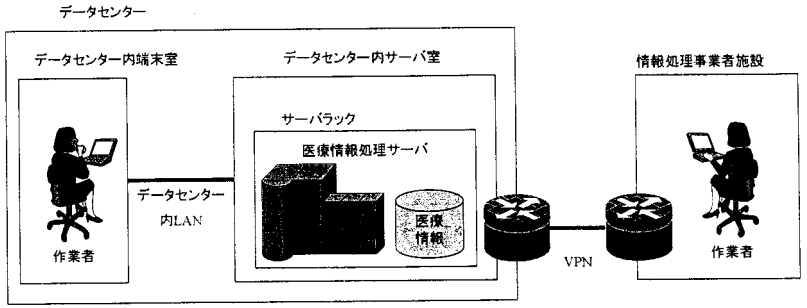

図 3 データセンターの利用とサーバ及び端末の配置

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 2 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。更に医用画像（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上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[17]」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[18]等の光磁気ディスク、CD、DVD 等の光学ディスク、USB[19]メモリ、コンパクトフラッシュカード、SD メモリーカード[20]等の半導体メモリ、ハードディスク等の磁気ディスク等が考えられる。

医療情報は長期保存が求められる性質上、紫外線による劣化が進むといわれる色素を用いた書き込み型の光学ディスクよりも、経年変化に強いとされる光磁気ディスクが望ましいといえるが、光学ディスクであっても保管環境を整備することで寿命を延ばすことができる。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。

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、媒体としての半導体メモリについては 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する。衣服などのわずかな隙間にも隠すことができるため、不正に情報の持ち出しを行おうとするものにとっては便利なものである。医療情報を格納する電子媒体としての有益性は認められるものの、大きなリスクも認められることから、原則として医療情報処理機器では外部デバイスとして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、利用時間及び媒体の移動範囲を最小にするなどの管理を行うこと。

[17] 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
[18] Magneto Optical Disc
[19] Universal Serial Bus
[20] 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「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」には「外部と医療情報を外部ネットワークを利用して交換する場合、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、送受信データに対する「傍受」及び「改ざん」、ネットワークに対する「侵入」及び「妨害」などの脅威から守らなければならない。」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の一種である、広域イーサネット、VPN 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ネットワーク上の VPN は、専用線及び閉域網 VPN（IP-VPN）では存在しない、サービス不能攻撃、ブルートフォース攻撃[21]等を受けるリスクがあり、安全性が比較的低いと考えられる。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、インターネット上の 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、VPN チャンネル[23]上のプライベートネットワークインタフェースではプライベートアドレス[24]のみを利用して接続することとし、ネットワーク境界のファイアウォール又は 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）。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。

[21] brute force attack（力任せの攻撃）、ここではログインに成功するまで 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を意味する。
[23] VPN として確立される仮想回線を指す
[24] インターネット上で通信可能な IP アドレスをグローバルアドレスと呼び、インターネットと直接の通信を行わない IP アドレスをプライベートアドレスと呼ぶ。

3.3　電子媒体による外部保存を可搬型媒体経由で行う場合の手順

医療情報を CD、DVD、MO 等の可搬型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) 外部保存対象の電子ファイルについて電子署名を付与（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可搬型媒体に書き込み、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、配送する可搬型媒体の数量、配送業者の作業者情報、予想到着時刻等を通知

- 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

(2) 受け取った可搬型媒体の数量、封印が正常であること等を確認

(3) 医療情報処理システムとネットワーク接続されていない機器上で媒体に悪意のあるコードが混入していないことを検証及び添付された電子署名を検証（悪意のあるコードについては「7.7.3 悪意のあるコードに対する管理策」を参照）

(4-1) 可搬型媒体そのものを保管する場合には可搬型媒体を保管庫に格納

(4-2) 可搬型媒体上の電子ファイルを情報処理機器上で保管する場合には医療情報処理機器に媒体中の電子ファイルを複写し、可搬型媒体は適切な手段で廃棄処分（廃棄手順については「7.7.7 媒体の取扱」を参照）

(5) 受領した電子ファイル又は可搬型媒体の情報を管理台帳に記載

(6) 医療機関等に受付情報を通知

このような可搬型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。なお、受領した可搬型媒体そのものを保管する場合には、情報を破棄する際に媒体ごと破棄できるように電子ファイルを整理して記録するよう医療機関等と協調して配慮すること。

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　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の実施

(2) 外部保存対象の電子ファイルについて電子署名を付与（必要に応じて暗号化を行う）

(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（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

(5) 情報処理事業者に送出完了を通知

- 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

(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及び電子ファイルに添付された電子署名を検証（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（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

(5) 医療機関等に受付情報を通知

このようなネットワーク経由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。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[25]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技術等を利用してネットワーク上で

[25] File Transfer Protocol

のパスワード及びデータ漏えいのリスクを低減すること。若しくはSFTP[26]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こと。

上記手順を図 4 に示す。

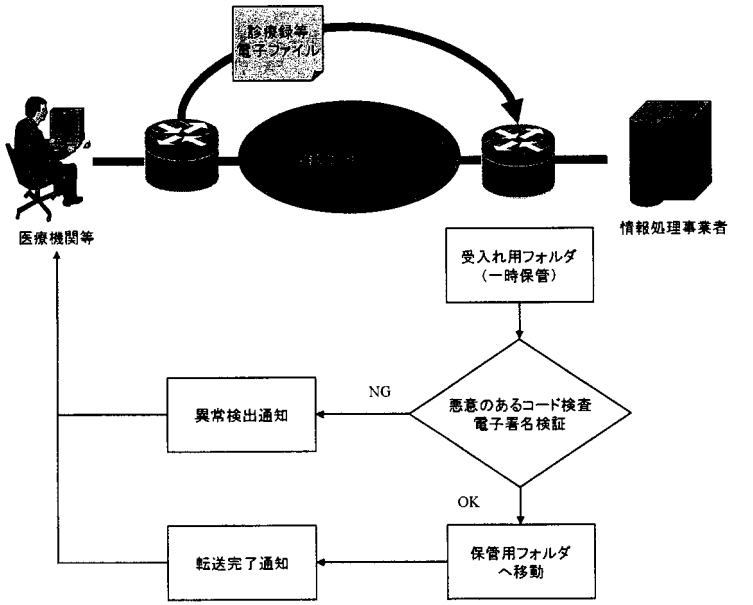

図 4 電子媒体による外部保存をネットワーク経由で行う場合

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

[26] Secure File Transfer Protocol

(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) 一日ごとに、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医療機関等に通知する。

(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。

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「7.6.4 情報処理装置の廃棄及び再利用に関する要求事項」及び「7.7.7 媒体の取扱」、「7.9 情報の破棄」等に示される管理策を適用すること。

3.5 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「SaaS・ASP」という。）。SaaS・ASP 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、更に全ての利用者が情報処理システムを共有し、更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（この形態を特に SaaS という）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 SaaS・ASP が想定される。しかし、SaaS・ASP 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」に従い、適切な対策を行うことが要求される

SaaS・ASP 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、SaaS・ASP 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[27]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 5）。

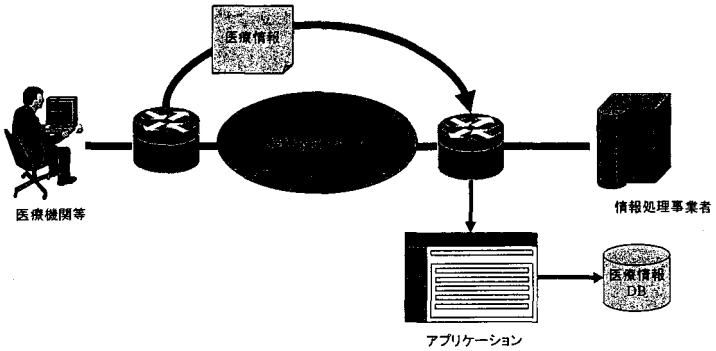

図 5 アプリケーション入力による外部保存をネットワーク経由で行う場合

ここで検討しなければならないことの一つは情報漏えい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えい、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えい、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えい等である。

ここであげた三つの情報漏えい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。

[27] 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 3 版」IPA を参照のこと

表 2 情報漏えい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えい	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えい
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えい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えい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すること。

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。

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を接続するネットワークは専用回線あるいは 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、回線品質も比較的低いため、閉域網上に構築された VPN を利用することが望ましい。

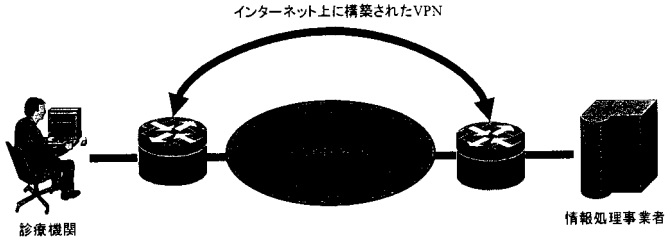

図 6 インターネット上に構築された VPN

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、以下に示す制約に従うこと。

- 医療機関側機器と情報処理事業者側機器を接続する VPN チャンネル上のプライベートネットワークインタフェースに割り当てるアドレスをプライベートアドレス[28]に限定すること（VPN チャンネル上のインターネットインターフェースアドレスはグローバルアドレスで良い）。
- 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経路を設定しないこと。

また、複数の医療機関等から情報処理業務を委託している場合には、医療機関等の間で

[28] RFC1918 “Address Allocation for Private Internets” で規定される。RFC は国際団体 IETF が発行するインターネット標準文書。

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別に構築すること。

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。

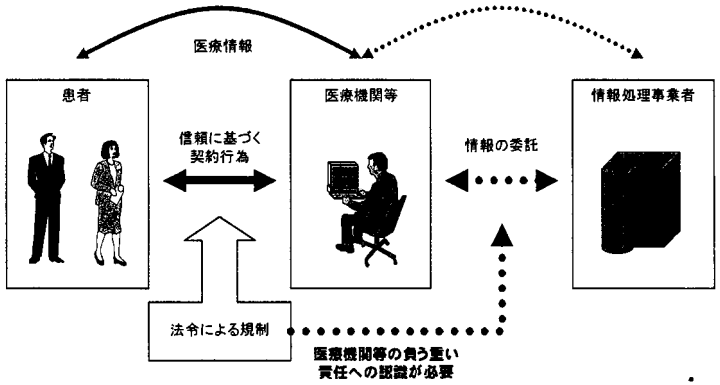

図 7 患者と医療従事者と情報処理事業者の責任関係

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）。

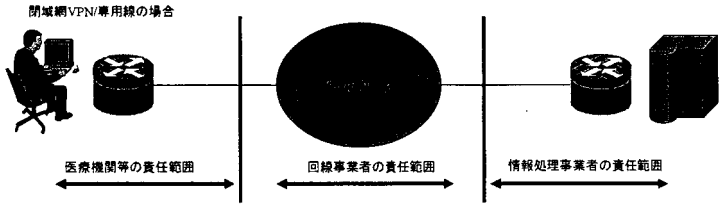

図 8 閉域網/専用線利用時の責任分界点

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。

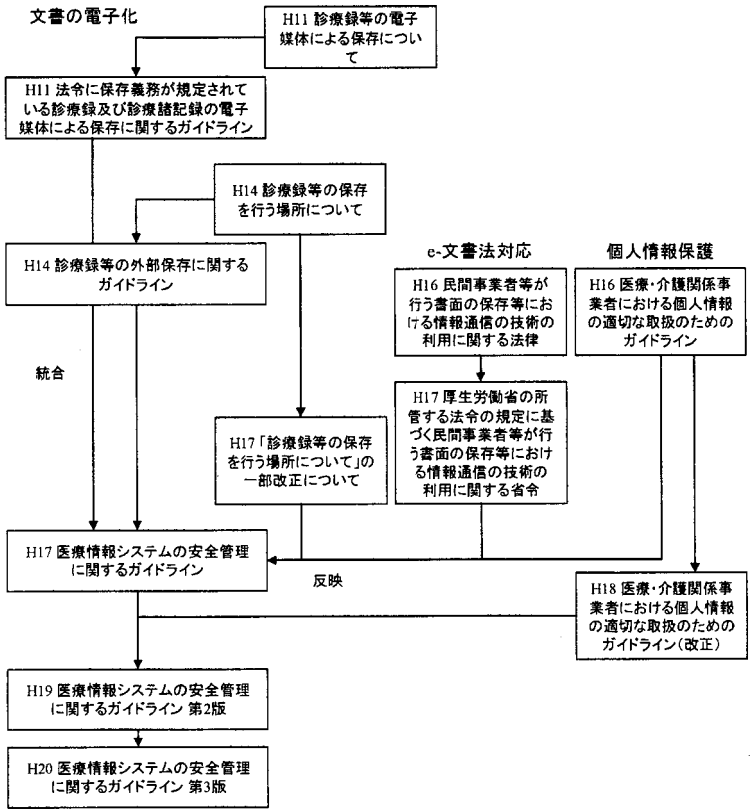

図 9 医療情報の電子記録に関する通知・省令及びガイドライン類の策定経緯

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。

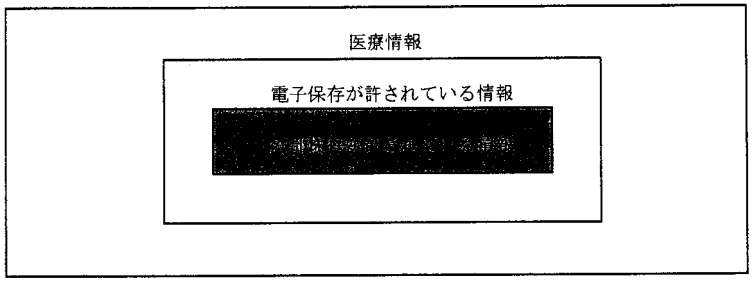

図 10 医療情報の電子的扱いに関する区分

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

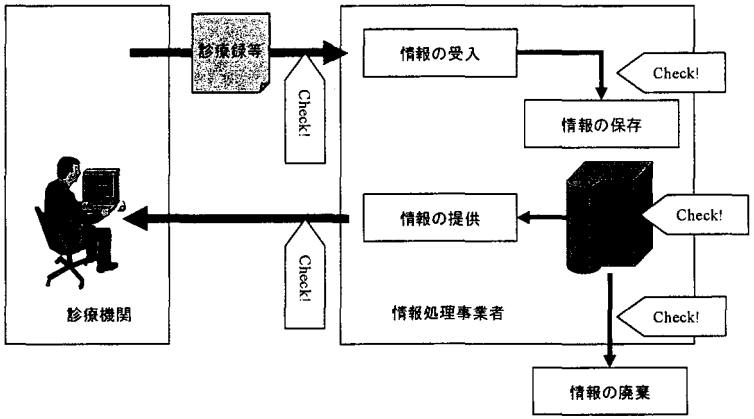

図 11 情報の生成（登録）から廃棄まで（各チェックポイントで改ざんを検査）

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。

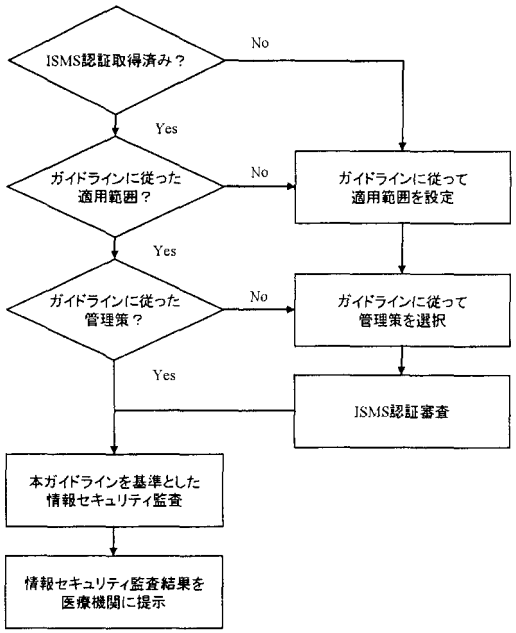

図 12 医療情報の受託管理業務を実施するまでの認証及び監査の流れ

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。

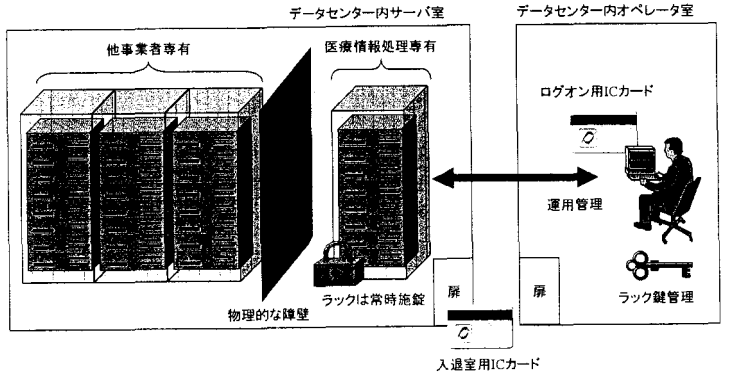

図 13 データセンターで医療情報処理設備を運用管理する場合の安全管理の例

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

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廃棄を選択すること。

- 機器を設置するサーバラックについては、震災時に転倒することが無いよう確実に設置し、熱による障害を防ぐため十分な換気装置を設け、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。

7.6.4 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処理に関わ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

- ハードディスク等の固定記憶装置について情報処理システム内の別の機器で再利用する場合には、再利用前に確実な方法でデータを消去すること。
- パスワードの生成規則に関する情報を漏らさないよう、計算機の BIOS パスワード、ハードディスクパスワード等を設定している場合には、それらを消去すること。
- 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、運用しているシステムとは独立した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。
- 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、データの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）等を適用すること。
- 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、医療機関等に示し十分な理解を得ておくこと。

なお、装置の最も確実な廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法がある。しかし、ディスク上の管理情報も消去されてしまうため、再利用するためには製造ベンダによる再処理が必要となる。本ガイドラインではハードディスクの施設外部での補修作業を認めない方針であるため、この方式では再利用が出来ない。このため、ランダムデータ及び固定パターンの複数回の書き込みなど、ソフトウェア実行によるデータ消

去方式は完全とはいえないものの、NSA[49]推奨方式、米国防総省準拠方式、NATO[50]方式、グートマン方式等から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し、合意を得た上で実施することが望ましい。

7.6.5 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

- 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。手順には、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が含まれる。
- 持ち出した機器を、再度設置する際には、情報処理装置に悪影響を及ぼさないよう、適切な検証手続きを行うこと。検証手続きには、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）等が含まれる。

---

[49] 米国防総省安全保障局

[50] 北大西洋条約機構

7.7 技術的安全対策

情報処理システムの管理、運用における責任体制、扱う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。

7.7.1 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

- 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。
- 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、影響を最小限に抑える方策を検討すること。
- 情報処理に関わる機器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。
- 適切な変更手順を策定すること。手順には以下の事項を含むこと。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。
- 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。
- 不正な改ざんを受けていないことを検証するため、定期的に監査を実施すること。
- 情報処理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。
- 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。
- 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。
- 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すること。

7.7.2 開発施設、試験施設と運用施設の分離

データの漏えい、破壊等のリスクを避けるため、情報処理システムの開発及び試験用の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

- 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もの又は十分に安全性を検証した上で外部開発事業者に開発依頼したものを用いること。
- 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。
- 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「7.7.3 悪意のあるコードに対する管理策」に従うこと。
- 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
- 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。
- 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に示し、了解を得た上で利用すること。

加えて、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。

7.7.3 悪意のあるコードに対する管理策

情報処理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[51]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

[51] 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。

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。

なお、本ガイドラインの想定するシステムではサーバ等の機器類はインターネットとは直接接続することが無いため、インターネット上で提供される悪意のあるコード対策ソフトウェアのアップデートファイル又はリポジトリに直接アクセスすることができない。このため、アップデートファイルについては電子媒体等を利用して運用システムに設置する等の対策が求められる。

実施すべき安全管理策

- 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。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。
- 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）、（週に 1 回以上の）定期的な自動スキャン、外部記憶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。
- 管理者以外が悪意のあるコード対策ソフトウェアの設定変更やアンインストールができないような設定がされていること。
- 悪意のあるコード対策ソフトウェアにおいて、定義ファイル、スキャンエンジンの自動アップデート、又は定期的な更新が十分な頻度で行われていること。
- 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、ユーザ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又は隔離措置をとるといった対策が行われていること。

7.7.4 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、医療情報処理システムはインターネット等の外部ネットワークとは直接接続されないため、不正なウェブコンテンツを医療情報処理システム内の機器にて閲覧するリスクは低いと思われる。しかし、医療情報処理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

- 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
- 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）。
- ウェブブラウザからメールクライアント等のアプリケーションが起動されないこと。
- 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「7.7.3 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。

7.7.5 外部事業者が提供するサービスの管理

情報処理システム内において、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

- 提供されるサービスについてセキュリティ管理策及びサービスレベルを確認すること。
- 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。
- 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。
- 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。
- サービス実施中は顔写真を券面に入れた身分証明を携帯し、情報処理事業者の正規職員が監督している状況で作業を行うこと。
- 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、職員の入室、退室手順に準ずること。
- 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。

7.7.6 ネットワークセキュリティ管理

本ガイドラインでは情報処理システムのインターネット等、不特定多数が接続するネットワークとの直接接続を認めていない。よって、ネットワーク経由での情報処理システム

への不正なアクセスは限定された経路のみと考えられる。しかしながら、リスクとしては、なお大きなものがあるため、不特定多数が接続するネットワークとの接続時と同等の安全管理措置として、以下の管理策を適用すること。

実施すべき安全管理策

- 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）において、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。
- 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）。
- ネットワーク機器及びサーバ、端末の空いているネットワークポートへの接続を制限すること。
- 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）及び侵入防止システム（IPS）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。
- 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。
- 侵入検知システムが、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。
- 侵入検知システムが、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。
- 侵入検知の記録には必要な項目が含まれていること。
- 医療機関等と情報処理事業者を接続するインターネット上の VPN 回線を通じたアクセス、及び情報処理システムの稼働監視、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、電子署名検証における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の場合を除いて、インターネット等のオープンネットワークを介した情報処理設備へのアクセスを行わないこと。
- 専用回線等のクローズネットワークを介して情報処理設備に接続する場合においても適切な認証を用いること。
- 情報処理システムへの同時ログオンユーザ数に適切な上限を設けること。
- 認識されていないログオンユーザを識別できるように、ログオンするユーザアカウントについては計画を立て、計画に即していることを常に確認すること。
- ネットワーク経由で直接、特権ユーザとしてログオンする行為を禁止すること。
- 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。
- 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。
- VPN 接続を行う場合には VPN 装置間で相互に認証を行うこと。
- VPN 接続を行う場合における認証は、傍受、リプレイ等のリスクを最小限に抑えるために適切な暗号技術を利用すること。
- 不正なトラフィックがネットワーク境界を越えて流れていないことを監視すること。

7.7.7 媒体の取扱

情報流出経路の大半は記憶媒体の持ち出しによるものとされる。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。

実施すべき安全管理策

- 可搬型の記憶媒体について情報処理システム外の不要な持ち出しを行わないこと。
- CD、DVD、MO 等の可搬型記憶媒体については、追記のできない光学メディア、CD-R、DVD-R を用いる等して、情報処理システムの内外を問わず再利用できないようにする。なお、バックアップ目的で MT、DAT 等の大容量媒体を用いる場合には、その管理を厳重に行うことで再利用を認める。
- 情報交換の目的で記憶媒体を使う場合には媒体上の情報をハードディスク等の固定記憶装置に複製した後に記憶媒体を廃棄処分とする。
- 情報交換、情報保管以外の目的で記憶媒体を用いないこと。
- 医療情報処理施設内においては情報処理機器に接続できる外部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。加えて、認められていない

種類の外部媒体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。

- 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。
- 媒体の利用に関する記録を行い、媒体の廃棄後も一定期間にわたり保存すること。
- 媒体損失のリスクを最小限にするため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。
- 製造者の定める保管期間を超過することがないよう、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。
- 媒体の一覧表を管理し、媒体の盗難、紛失を迅速に検知できる体制を構築すること。
- 全ての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。
- 媒体により情報を交換する場合には媒体内のデータにパスワードによるアクセス制限又は暗号化を施すこと。
- 配送業者が媒体の配送中のリスクに対して適用している対策を確認した上で配送業者を選択すること。
- 配送業者から媒体を受け取る時は、情報処理設備とは別の搬入・搬出専用の区域で正規職員が直接受け取ること。受け取る際には、配送業者の身分確認を行うこと。
- 配送に際しては内容物を外部から知ることができないコンテナを用い施錠した上で配送すること。
- CD、DVD 等の光学メディア、MT（磁気テープ）等の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）を適用すること。
- 媒体の破壊については情報処理事業者自身で行うこと。破壊した媒体の処理は外部の専門事業者に依頼することが可能である。
- ハードディスク等の固定記憶装置の扱いについては「7.6.4 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。

7.7.8 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

- 次の情報交換方法について予め合意しておくこと。
  - 情報を記憶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、アプリケーションログオン時の確実な認証を行うこと。
  - 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）。
- 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。
  - 配送業者等による記憶媒体の抜き取り等を防ぐため、交換する記憶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。
  - 配送業者等による記憶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。
  - 記憶媒体を発送、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。

7.7.9 情報処理システムに対するセキュリティ要求事項

以下に示す、情報処理装置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

- 運用システムの混乱を避けるため、開発用コード又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。
- 作業者個人のファイル、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。
- 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
- 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。
- 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。

7.7.10 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

- アプリケーションに対するデータ入力に関して、操作上の誤りによりデータの不整合が発生しないよう、データ範囲及びデータタイプの制限、入力文字種及び長さの制限等を設定、自動的な検査等により誤りを検出する機構を導入すること。
- 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。
- アプリケーションの入力及び出力データに悪意を持った不正なデータ（不正な画面エスケープシーケンス、HTMLにおけるメタキャラクタ、シェルコマンド等）

が含まれていた場合の悪影響を避けるため、自動的な検査及び妥当性確認機構を導入すること。

- 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。
- 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。
- 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こと。

7.7.11 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

- 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[52]等を用いること。
- 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。
- 暗号鍵の生成は耐タンパー性[53]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。
- 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。
- 暗号鍵が漏えいした場合に備えた対応策を策定しておくこと。
- 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。
- 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。
- 医療機関等から受け付けるデータを検証するための認証機関の公開鍵証明書は安

[52] http://www.cryptrec.jp/list.html
[53] 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

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[54]と比較して、正確性を検証すること。

7.7.12 ログの取得及び監査

すべての行為、作業は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

- 作業者の活動、機器で発生したイベント、システム障害等を記録した監査ログを作成し管理すること。
- ログを利用して正確に事故原因等を検証するため機器の時刻を同期し、定期的に検証を行うこと。
- 時刻の同期のため、運用施設内に時刻サーバを導入し、時刻サーバの提供する時刻にすべてのサーバ、コンピュータ、その他機器類を同期しておくこと。
- 以下に示すシステム使用状況等について監査ログに記録し、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。
  - 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

[54] 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。

  - 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）
- 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、記憶媒体への書き出し、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。

なお、本ガイドラインの想定するシステム構成では情報処理システムからインターネット上の時刻サーバには直接アクセスすることはできないので、時刻サーバについては GPS 等を利用したハードウェア装置を情報処理システム内に設置して利用する等の方法を用いることが望ましい。

また、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。

7.7.13 バックアップ

本ガイドラインの対象とする情報処理は医療情報に関わるものであることから外部保存に関しては見読性の確保が要求されている。つまり、バックアップ施設は単に情報をバックアップするだけでなく、同等の情報処理機能を備えることで見読性の確保に努めるべきといえる。しかし、コストが増大することが想定されるため、原則的には、医療機関が求める水準の情報処理機能を提供することとする。

実施すべき安全管理策

- バックアップ施設は自然災害の影響を同時に受けないよう、情報処理システムから十分離れた地点に構築すること。
- バックアップ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。
- 見読性の要求から、医療情報について情報処理システムとバックアップ施設の間で同期をとること。同期をとるためのネットワーク回線については本ガイドラインで規定するネットワーク安全管理策に従うこと。

- バックアップ施設及びバックアップ装置は情報処理事業者自らが管理することを原則とするが、遠隔地に設置するため緊急時の対応が遅れる等の事態を避けるため緊急時対応を再委託する場合には、再委託先事業者の安全管理基準を医療機関に通知し承認を受けること。

災害時などにおいても見読性を損なわないよう、バックアップ施設においても同等の情報処理機能を備えることが望ましいが、情報処理事業者に保存される医療情報の性質、サービス提供コスト等との兼ね合い等を考慮し、医療機関等に事前にバックアップ施設における情報処理サービス機能等について説明し、了解を得ること。

7.7.14 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。以下の管理策について適用すること。

実施すべき安全管理策

- 情報処理に用いる情報処理機器それぞれのセキュリティ要求事項を整理すること
- 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
- 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。
- 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。
- 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。
- 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。
- 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。

7.7.15 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機器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

- 作業者は情報処理機器上においてユニークな作業者 ID により識別されること。

- 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。
- 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。
- 作業者 ID の発行は情報処理及び情報処理システムの管理に必要な最小限の人数に留めること。
- 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。
- 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。
- 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。
- 不要な作業者 ID やアカウントが残っていないことを定期的に確認すること。

特権 ID について実施すべき安全管理策

- 特権使用者に昇格可能な作業者 ID を制限すること。
- 特権の使用時には作業実施内容を記録すること。
- 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。
- 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。

パスワード管理について実施すべき安全管理策

- 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。
- システムログオン用のパスワードはハッシュ値等、パスワードを復元できない形で情報を保管すること。
- システムログオン用のパスワードを保管するファイルは一般作業者による閲覧を制限すること。
- 作業者がシステムログオン用の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、例えば乱数によりパスワードを生成するプログラム等を導入すること。品質の基準としては、パスワードを十分に長くすること、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。

- システムログオン用の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。
- システムログオン用の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。
- 変更時には変更前のパスワードの入力を要求し、一定回数以上間違えた場合には、そのアカウントを一時的に使用できない（ロックアウト）ようにすること。
- パスワード発行時には、乱数から生成した仮のシステムログオン用の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こと。
- 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。
- リモートログオンを行う際には傍受によるパスワードの漏えいリスクを避けるため、暗号により通信データを保護する方式を採用すること。
- 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。

作業者のログオンについて実施すべき安全管理策

- 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。
- 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。
- 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。
- 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。
- 連続したログオンの失敗回数を制限するアカウントロック機能を有効とすること。更に、ログオンの連続した失敗が許容限度回数に達した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。
- 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。

7.7.16 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

- 各作業者は自身のパスワードを秘密にし、紙、電子ファイル、携帯電話又は PDA[55] 等に記録及び保管しないこと。パスワードを記録する必要がある場合は、予め定められた方法で記録し、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。
- 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。
- 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。

[55] Personal Digital Assistant、携帯情報端末

7.8　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要員は、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要員の選定について、以下の管理策を適用すること。

実施すべき安全管理策

- 医療情報を操作する可能性のある要員の全てについて、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あるいは守秘義務契約への署名を求めること。派遣従業員については機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。
- 医療情報を操作する可能性のある要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。
- 要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。
- 医療情報を操作する要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。

医療情報を操作する要員については、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員に周知し、理解したことの確認を行うこと。

7.9　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（又は監督する責任）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固定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[56]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

- 破棄する電子文書ファイルが電子媒体上で一つだけ記録されている場合、電子媒体が光学メディアであれば媒体自身を破壊処分すること。
- 光学メディアに複数の電子ファイルを記録する場合には、電子媒体ごと破棄できるように、予定された廃棄時期が同じ電子ファイルをまとめて記録しておくこと。
- ハードディスク等の固定記憶装置の扱いについては「7.6.4 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。

[56] File Allocation Table 等と呼ばれる

7.10　情報システムの改造と保守

情報処理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情報施設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「7.6.3 情報処理装置のセキュリティ」及び「7.7.5 外部事業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

- 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、情報処理ソフトウェアに対する影響を評価及び試験して確認すること。
- 開発された情報処理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。ただし、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こと。

7.11　医療情報処理に関する事業継続計画

情報処理システムの重大な故障、災害の影響等による情報処理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情報処理システムではネットワーク経由で情報のやり取りを行うため、医療機関等の所在地と情報処理事業者及び情報処理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情報処理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情報処理システムを配置する必要がある（図 14）。

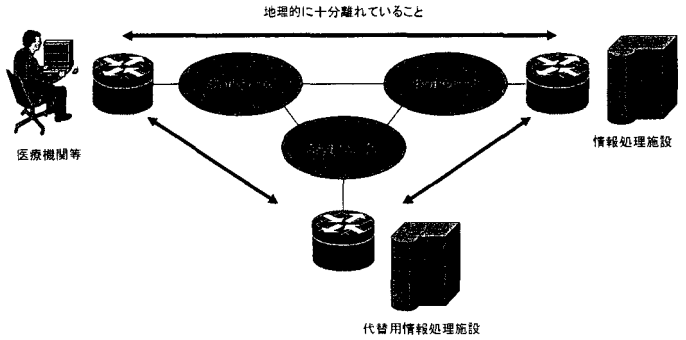

図 14 災害の影響を避けるための情報処理システムの配置

ただし、情報処理システムだけでは事業継続には不足しており、稼動に必要な要員を配置しておくか、要員が迅速に移動する必要がある（「7.7.13 バックアップ」に示されるように、緊急時の対応を再委託する際には医療機関の承認を得ること）。

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と主要な目的と考え、事業継続計画の立案と改善についての管理策を示す。

7.11.1　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要員を含む）、情報処理設備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

- 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要員を含む）、情報処理設備等について識別すること
- 業務プロセス間の相互関係を評価すること
- 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。
- 情報処理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。
- 情報処理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。
- 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、大きすぎるものがあれば、影響度を低減する方策及びその可能性について検討すること。

7.11.2 事業継続計画の立案及びレビュー

災害又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のための管理策を示す。

実施すべき安全管理策

- 医療情報処理サービスの提供における業務プロセス及び情報処理システムの優先順位にもとづいて、機器及び要員の代替を含めた復旧措置を立案し、医療情報処理に関する事業継続計画として策定すること。
- 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。
- 事業継続計画について定期的に見直しを行うこと。

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及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の確保によるセキュリティ対策の向上や災害時の危機管理の推進、安全に情報が保存された場所を通じて医療機関等相互の有機的な情報連携や適切な患者への情報提供が途切れない医療情報の提供体制を構築すること等を目的としている必要がある。
>
> また、情報を保管する機関が、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、情報を閲覧、分析等を目的として取り扱うことはあってはならず、許されない。
>
> 現段階では民間等の外部保存を受託する事業者に対する明確な規制としては個人情報の保護に関する法律しか存在せず、身体情報の保護に関する特段の措置が講じられていないため、委託する医療機関等において、医療情報が機微であることを踏まえた契約や技術的担保等の特段の保存情報の取り扱いを十分検討した上で実施する必要がある。

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。

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。

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、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要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
2006年4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
2007年3月改正 経済産業省

● 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

10 図表一覧

以上