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。