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ガイドライン

（平成２４年１０月１５日経済産業省告示第２２８号）

平成２４年１０月
経済産業省

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。

本ガイドラインは、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。

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、本ガイドラインに関する参考資料「医療情報を受託管理する情報処理事業者向けガイドライン第２版（経済産業省、平成24年10月）」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】

診療録、処方せん、手術記録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約その他の診療の過程で患者の身体状況、病状、治療等について作成、記録又は保存された書類、画像等の記録をいう。本ガイドラインに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、患者の既往歴、家族歴、嗜好等のこと。高度なプライバシー情報であり、医療機関等にとっては守秘義務が課せられていることからも、機密性への高い配慮が求められる。なお、要介護者は言葉の定義としては患者には含まれないと考えられるが、その情報は同様に高度なプライバシーに関する情報であることから、要介護者の情報についても患者情報と同等と考え、要介護者情報を扱うシステムは下記の医療情報システムに含まれるものとする。

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

【医療情報システム】

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

【医療機関等】

主に病院、診療所、薬局、助産所等を指す。

1.2. 本ガイドラインで用いる制度及び技術用語の説明

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

以下に示す。

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

【適用宣言書】
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）、ＩＰ－ＶＰＮ（閉域ＩＰ網／閉域網ＶＰＮ）、インターネットＶＰＮ】
不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のことをＶＰＮ（仮想私設網）と呼ぶ。
ＶＰＮのうち、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を提供する接続サービスを、特に、ＩＰ－ＶＰＮ（閉域ＩＰ網／閉域網ＶＰＮ）と呼ぶ。
また、オープンなネットワークであるインターネット上に構築されたＶＰＮを、特に、インターネットＶＰＮと呼ぶ。
なお、本ガイドラインでは、回線の種別を表す用語として、専用線、ＩＰ－ＶＰＮ、インターネットＶＰＮの三種類を用いることにする。

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

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

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装置を操作するものを作業者と呼ぶ。

【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。

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

2．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、医療情報の安全確保を目的として、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。

2.2.情報資産管理

2.2.1.資産台帳

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

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

2.2.2.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） 預託される情報に対して分類にもとづいたリスク分析を実施すること。
（4） リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。
（5） 分類がわかるように情報にラベルをつけること（電磁的な記録にラベルをつける方式に

は様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること)。

（6） 各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。

2.3.組織的安全管理策（体制、運用管理規程）

（1） 医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

（2） 個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。

（3） 個人情報保護に関しては、医療機関等の監督の下に行うこと。

（4） 情報処理の安全管理に関わる手順書、運用管理規程を整備すること。

（5） 運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等)、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。

2.4.医療情報の伝達経路におけるリスク評価

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

2.5.物理的安全対策

2.5.1.医療情報処理施設の建物に関する要求事項

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

（1） 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。

（2） 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては、十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。

（3） 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。

（4） 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。

2.5.2. 医療情報処理施設への入退館、入退室等に関する要求事項

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

- 医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。
- 有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。
- 有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること（履歴の保全については「2.6.12.ログの取得及び監査」を参照)。
- 情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。
- 情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。
- 職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、情報処理事業者の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。
- 情報処理事業者の職員の業務に応じて執務室内に滞在できる時間を指定すること。
- 医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。

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

- データセンターを運営する外部事業者が、（1）と同等な安全管理策を実施する等、情報処理事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認すること。
- 医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。
- 情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。
- データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことを確認すること。
- 医療情報システムであることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこと。

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

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

2.5.3.情報処理装置のセキュリティ

（1） 不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。

（2） 医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。

（3） 医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。

（4） 医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。

（5） 火災発生時の消火設備が機器に損傷を与えないよう配慮すること。

（6） 医療情報システムを配置する室内での喫煙、飲食を禁止すること。

（7） 医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。

（8） それぞれの装置は製造元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。

（9） 保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については、補修ではなく物理的な破壊を行ってから廃棄を選択すること。

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

・震災時に転倒することが無いよう確実に設置すること。

・熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されていること。

・扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。

(11) 起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「2.6.14.作業者アクセス及び作業者ＩＤの管理」に従うこと。

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

(13) 不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録され

たネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。

2.5.4. 情報処理装置の廃棄及び再利用に関する要求事項

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

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

（3） ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。

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

2.5.5. 情報処理装置の外部への持ち出しに関する要求事項

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

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

（2） 持ち出した機器を再度設置するための適切な検証手順を策定すること。

2.6. 技術的安全対策

2.6.1. 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、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。

（3） 医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。

（4） 情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画を立てて実施すること。

（5） 情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。

（6） 不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。

（7） 医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。
（8） 潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。
（9） 修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。
(10) 保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。

2.6.2.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アプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。
（2） ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設（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「2.6.3.悪意のあるコードに対する管理策」に従うこと。
（4） 不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること。
（5） 運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。
（6） 医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関に示し、了解を得た上で利用すること。

2.6.3.悪意のあるコードに対する管理策

（1） 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。
（2） 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。
- リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）
- リスク評価の結果として必要であれば定期的にスキャンを実施
- 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン
- 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
- 管理者以外による設定変更やアンインストールの禁止

（3） 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への

通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとるといった対策が行われていること。

2.6.4. ウェブブラウザを使用する際の要求事項

医療情報システム内で必要とする、ネットワーク監視ソフトウェア、サーバ制御ソフトウェア等でユーザインタフェースとしてウェブブラウザを使用する場合は、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） 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「2.6.3.悪意のあるコードに対する管理策」に即して検査されること。

2.6.5. 第三者が提供するサービスの管理

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

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

（2） サービスの実施、運用、維持について定期的に検証すること。

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

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

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

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

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

（8） 医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第４．１版（厚生労働省、平成22年２月）」６．８章Ｃ項の管理策を実施すること。

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

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

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

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

（5） 医療機関等との接続ネットワーク境界には侵入検知システム（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。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。

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

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

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

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

- 外部からの医療情報システムの稼働監視・遠隔保守
- セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード
- オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード
- 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス
- ファイアウォール、ＩＤＳ・ＩＰＳなどのセキュリティ機器に対する不正アクセス監視
- 時刻同期のための時刻配信サーバへのアクセス
- これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等)
- その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等)

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

(11) ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。

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

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

(14)　ＶＰＮ接続を行う場合には以下の事項に従うこと。

・接続時にＶＰＮ装置間で相互に認証を行うこと。

・傍受、リプレイ等のリスクを最小限に抑えるために、「2.6.11.暗号による管理策」に従い、適切な暗号技術を利用すること。

・インターネット上のトラフィックがＶＰＮチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。

・複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためＶＰＮチャンネルを医療機関等別に構築する等の対策を実施すること。

2.6.7.電子媒体の取扱

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

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

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

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

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

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

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

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

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

2.6.8.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。

・情報を電子媒体に記録して交換する際の手順

・情報をネットワーク経由で文書ファイル形式にて交換する際の手順

・情報をネットワーク経由でアプリケーション入力にて交換する際の手順

・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

（2） 情報交換手順では搬送の形態によらず次の事項を確実にすること。

・発送者、受領者を識別し記録すること。

・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止策を行うこと。

・交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと。）。

・交換された情報に悪意のあるコードが含まれていないことを確実とすること。

（3） 物理的に情報を搬送する際には以下の対策を実施すること。

・医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。

・配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。

・配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。

・配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。

・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。

・電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

（4） 電子的に情報を転送する際には以下の対策を実施すること。

・送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。

・送受信する経路は適切な方法で傍受のリスクから保護されていること。

・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。

・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。

2.6.9. 医療情報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） 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。

2.6.10. アプリケーションに対するセキュリティ要求事項

（1） 提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。

（2） アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

（3） アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。

（4） アプリケーションにて医療事業者側の作業者を認証する情報（ＩＤ／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

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

2.6.11. 暗号による管理策

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

（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） 暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。

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

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

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

2.6.12. 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、システム使用状況等を記録した監査ログを作成し管理すること。

（2） 監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。

（3） ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。

（4） 標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。

（5） ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。

・ログデータにアクセスする作業者及び操作を制限すること。

・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。

・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。

2.6.13. アクセス制御方針

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

2.6.14. 作業者アクセス及び作業者ＩＤの管理

（1） 作業者は情報処理装置上においてユニークな作業者ＩＤにより識別されること。
（2） 作業者ＩＤを発行する際に、既存のＩＤとの重複を排除する仕組みを導入すること。
（3） 複数作業者で共用するためのグループＩＤの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者ＩＤでログオンしてからグループＩＤに変更する仕組みを利用すること。
（4） 作業者ＩＤの発行は医療情報システムの管理に必要な最小限の人数に留めること。
（5） 作業者が変更あるいは退職した際には、ただちに当該作業者ＩＤを利用停止とすること。
（6） 監視ログの監査時に作業者を確実に特定するため、作業者ＩＤは過去に使われたものを再利用しないこと。
（7） 不要な作業者ＩＤが残っていないことを定期的に確認すること。
（8） 特権ＩＤの発行は必要な最小限のものに留めること。
（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) 管理端末以外からの特権ＩＤによる直接ログオンを禁止すること。
(12) 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。
(13) 医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。
(14) 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。
(15) 医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。
(16) パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。
(17) パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対す

る対策を実施すること。

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

(19) 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。

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

(21) 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。

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

2.6.15. 作業者の責任及び周知

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

（1） 各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。

（2） システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。

（3） 離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。

2.7. 人的安全対策

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

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

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

育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

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

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

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

2.8. 情報の破棄

（1） ＣＤ－Ｒ等の廃棄については「2.6.7. 電子媒体の取扱」を参照すること。

（2） ハードディスク等の廃棄については「2.5.4. 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。

（3） 情報処理事業者は「医療情報システムの安全管理に関するガイドライン」に従って情報の破棄を行った記録を提出すること 。

2.9. 医療情報システムの改造と保守

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

2.10. 医療情報処理に関する事業継続計画

2.10.1. 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作業員を含む)、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） 医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。

（5） 医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。

（6） ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を検討すること 。

（7） 医療機関等に提供する情報処理サービスの継続に必要であれば、受託する医療情報のバックアップ施設等、情報処理サービスを継続するための代替情報処理施設を設置し、それらの施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。

2.10.2.事業継続計画の立案及びレビュー

（1） 医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画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。