### 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。

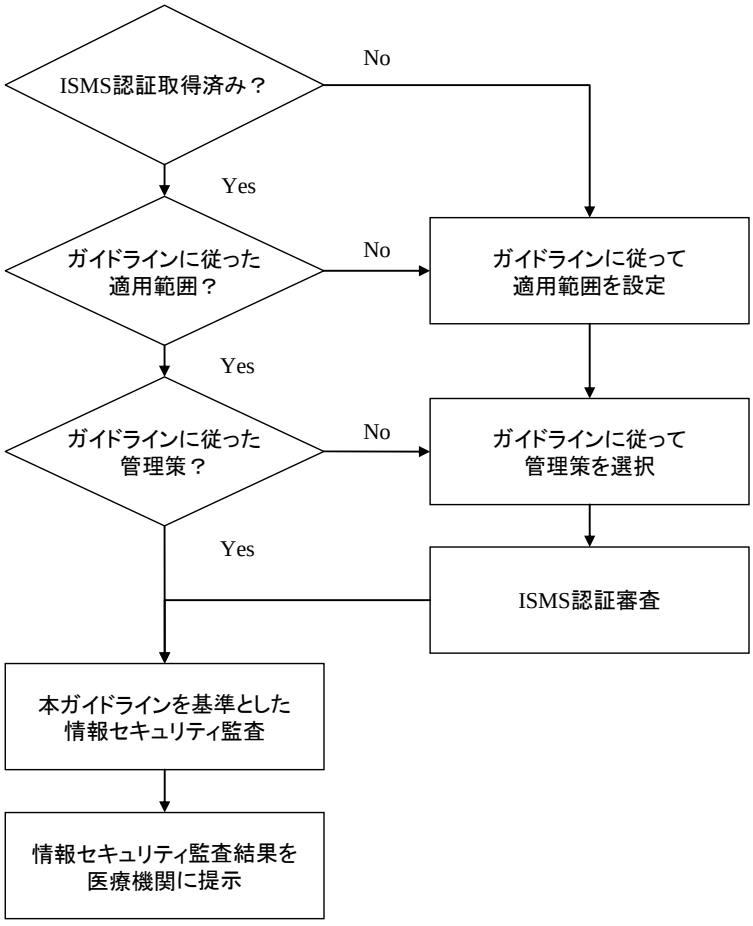


**図 12 医療情報の受託管理業務を実施するまでの認証及び監査の流れ**

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）<br>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<br>配送途中に盗まれる・すりかえられる<br>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<br>配送途中に盗まれる・すりかえられる<br>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<br>第三者が通信経路に介在して不正に情報を入手する<br>第三者が通信経路に介在して不正に情報を改ざんする<br>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<br>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<br>第三者が通信経路に介在して不正に情報を入手する<br>第三者が通信経路に介在して不正に情報を改ざんする<br>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<br>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<br>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<br>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。

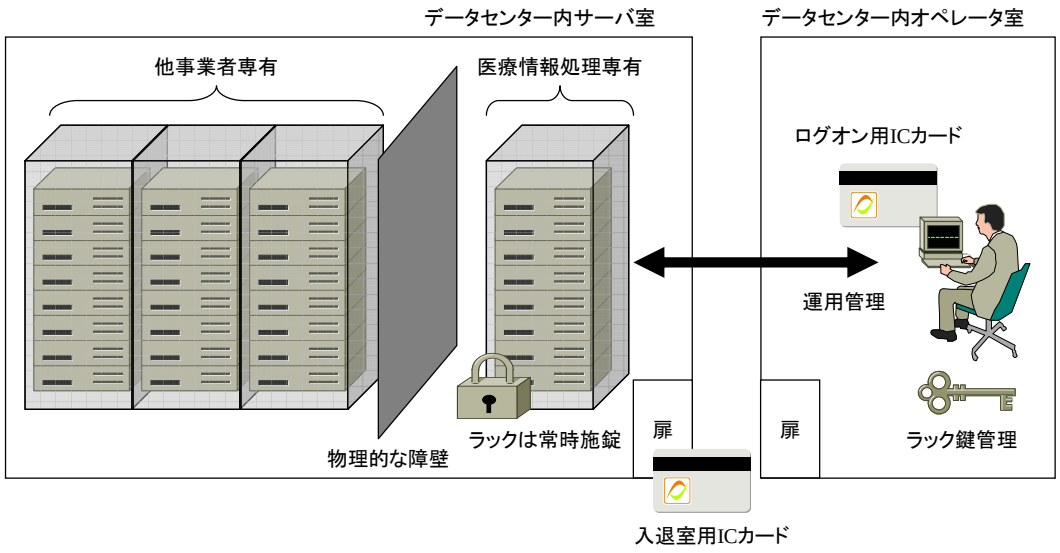


**図 13 データセンターで医療情報処理設備を運用管理する場合の安全管理の例**

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パ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)。

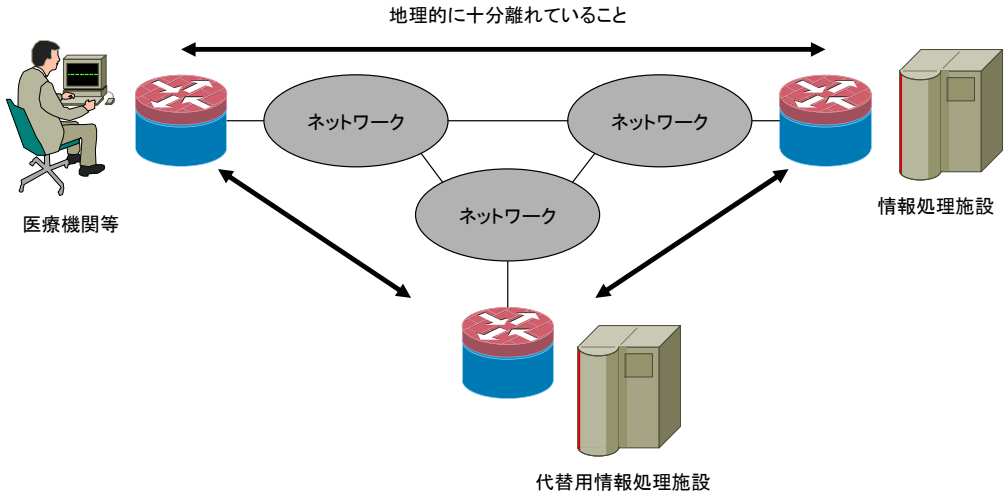


**図 14 災害の影響を避けるための情報処理システムの配置**

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

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 ..... 14
表 2 情報漏えいリスクに対する暗号化対象別の効果 ..... 27
表 3 医療情報の取扱に関する経緯 ..... 35
表 4 電子保存及び外部保存が許されている文書 ..... 39
表 5 ISMS 構築の 10 の STEP ..... 47
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 .. 54
表 7 医療情報をネットワーク経由で交換する際の脅威 ..... 55
表 8 医療情報をアプリケーションに入力する際の脅威 ..... 55

図 1 具体的な本ガイドラインの構成 ..... 12
図 2 本ガイドラインで対象とする情報システムの概念 ..... 15
図 3 データセンターの利用とサーバ及び端末の配置 ..... 17
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 ..... 23
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 ..... 26
図 6 インターネット上に構築された VPN ..... 28
図 7 患者と医療従事者と情報処理事業者の責任関係 ..... 30
図 8 閉域網/専用線利用時の責任分界点 ..... 34
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 ..... 38
図 10 医療情報の電子的扱いに関する区分 ..... 39
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） .... 42
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 ..... 48
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 ..... 57
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 ..... 81

以上