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。

⑴　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。

⑵　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。

⑶　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。

⑷　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

⑴　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。

⑵　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、⑴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。

⑶　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、⑴及び⑵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

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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。

⑽　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。