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。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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

⑴　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。

⑵　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。）。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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）

⑽　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。

⑾　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。

⑿　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。

⒀　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。

⒁　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

⑴　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⑼に示す方式にて確実に廃棄処分すること。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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。