5．情報システムの基本的な安全管理

情報システムの安全管理は刑法等で定められた医療専門職に対する守秘義務と個人情報保護法（個人情報保護に関する法律、行政機関個人情報保護法、独立行政法人等個人情報保護法の 3 法を一括して個人情報保護法と呼ぶ）の安全管理に関する条文によって法的な責務として求められている。守秘義務は専門職に個人としての責務として課せられているが、個人情報保護法は事業者に課せられた責務である。安全管理をおろそかにすることは上記法律に違反することになるが、医療においてもっとも重要なことは患者等のサービス受給者との信頼関係であり、単に違反事象がおこっていないことを示すだけでなく、安全管理が十分であることを説明できること、つまり説明責任を果たすことが求められる。この章で法規の要求事項は「個人情報保護に関する法律」の要求事項を指す。

A．法規の要求事項

（安全管理措置）法第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。
（従業者の監督）法第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
（委託先の監督）法第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

5．1　方針の制定と公表

「医療・介護関係事業者における個人情報の適切な取り扱いのためのガイドライン」でも個人情報保護に関する方針を定め公表することが求められているが、情報システムの安全管理も個人情報保護対策の一部として考えることができるため、上記の方針の中に情報システムの安全管理についても言及する必要がある。少なくとも情報システムで扱う情報の範囲、保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

5．2　情報の取り扱いの把握とリスク分析

5．2．1　取り扱い情報の把握

情報システムで扱う情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理されなければならない。

安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等のサービス受給者の視点からの影響の大きさと、継続した診療業務を行う視点からの影響の大きさを考慮する必要がある。この他に医療機関の事業者としての経営上の視点や、人事管理上の視点など、必要な視点を加えて重要度を分類する。

一般に診療に係る情報が個人識別可能な状態で安全性に問題が生じた場合、患者等にきわめて深刻な影響を与える可能性があり、もっとも重要度の高い情報として分類される。

5．2．2　リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関では一般に他の従業員への信頼を元に診療を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、以下の5．3～5．8の対策を行うことになる。

特に安全管理や個人情報保護法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障するのが限界である。したがって人の行為も含めた脅威を想定し、運用規程を含めた対策を講じることが重要である。

診療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。

① 診療情報システムに格納されている電子データ
- (a) 権限のない者による不正アクセス、改ざん
- (b) 権限のある者による不当な目的でのアクセス、改ざん
- (c) コンピュータウィルス等の不正なソフトウェアによるアクセス、改ざん

② 入力の際に用いたメモ・原稿・検査データなど
- (a) メモ・原稿・検査データなどの覗き見
- (b) メモ・原稿・検査データなど持ち出し
- (c) メモ・原稿・検査データなどのコピー

(d) メモ・原稿・検査データの不適切な廃棄

③ データを格納した可搬型媒体など

(a) 可搬型媒体の持ち出し

(b) 可搬型媒体のコピー

(c) 可搬型媒体の不適切な廃棄

(d) 非可搬型媒体（ハードディスクを搭載したPC等）の不適切な廃棄

④ 参照表示した端末画面など

(a) 端末画面の覗き見

⑤ データを印刷した紙やフィルムなど

(a) 紙やフィルムなどの覗き見

(b) 紙やフィルムなどの持ち出し

(c) 紙やフィルムなどのコピー

(d) 紙やフィルムなどの不適切な廃棄

上記の脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要になる。

5．3　組織的安全管理対策（体制、運用管理規程）

B．考え方

安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

① 安全管理対策を講じるための組織体制の整備

② 安全管理対策を定める規程等の整備と規程等に従った運用

③ 医療情報取り扱い台帳の整備

④ 医療情報の安全管理対策の評価、見直し及び改善

⑤ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程はきわめて重要であり、必ず定めなければならない。運用管理規程には必ず以下の項目を含めること。

- 理念

- 院内の体制、外部保存に関わる院外の人および施設
- 契約書・マニュアル等の文書の管理
- 機器を用いる場合は機器の管理
- 患者等への説明と同意を得る方法
- 監査
- 苦情の受け付け窓口

C．最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模施設などにおいて役割が自明の場合は、明確な規定を定めなくとも良い。
2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限するなどの入退管理を定めること。
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取り扱いを委託する場合、委託契約において安全管理に関する条項を含めること。
5. 運用管理規程等において下記の内容を定めること。
   (a) 個人情報の記録媒体の管理（保管・授受等）の方法について定めた規程
   (b) リスクに対する予防、発生時の対応の方法

5．4　物理的安全対策

B．考え方

物理的安全対策とは、情報システムにおいて個人情報が格納される、コンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には以下の事項を考慮する必要がある。

① 入退館（室）の管理
② 盗難、窃視等の防止
③ 機器・装置・情報媒体等の物理的な保護

C．最低限のガイドライン

1. 個人情報が保管されている機器の設置場所および記録媒体の保存場所には施錠すること。
2. 個人情報の物理的保存を行っている区画への入退管理を実施すること。

○　入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。

○　入退者の記録を定期的にチェックし、妥当性を確認すること。

3. 個人情報が存在するPCなど重要な機器に盗難防止用チェーンを設置すること。
4. 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

D. 推奨されるガイドライン

1. 防犯カメラ、自動侵入監視装置等を設置すること。

5．5　技術的安全対策

B．考え方

技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。ここでは5．2．1で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。

(1) 利用者の識別および認証
(2) アクセス権限の管理
(3) アクセスの記録（アクセスログ）
(4) 不正ソフトウェア対策

（1）利用者の識別および認証

情報システムへのアクセスを正当な利用者のみに限定するために、情報システムは利用者の識別と認証を行う機能を持たなければならない。小規模な施設などで情報システムの利用者が限定される場合には、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、一般的に言ってこの機能は必須である。

認証を実施するためには、情報システムへのアクセスを行う全ての職員および関係者に対しID・パスワードやICカード、電子証明書、生体認証等、本人の識別、認証に用いられる手段を用意し、統一的に管理する必要がある。また更新が発生する都度速やかに更新作業が行われなければならない。

このような本人の識別、認証に用いられる情報は本人しか知り得ない、または持ち得ない状態を保つ必要がある。例えば、以下のような行為により、本人の識別、認証に用いられる情報が第三者に漏れないように防止策を取らなければならない。

- ID/パスワードが書かれた紙などが貼られていて、第三者が簡単に知ることができて

しまう。

- パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- 代行作業等のためにパスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- 認証用の個人識別情報を格納するトークン（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
- 退職した職員の ID が有効になったままで、ログインができてしまう。
- 医療情報部等で、印刷放置されている帳票などから、パスワードが盗まれる。
- コンピュータウィルスにより、システムの ID とパスワードが盗まれ、悪用される。

認証強度の考え方

ID、パスワードの組合せは、これまで広く用いられてきた方法である。しかし、ID、パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務づける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。認証に用いられる手段としては、IC カード等のセキュリティ・デバイス＋パスワードのように利用者しか持ち得ない２つの独立した要素を用いて行う方式（２要素認証）やバイオメトリクス等、より認証強度が高い方式を採用することが望ましい。

また、入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、スクリーンロック等の防止策を講じるべきである。

IC カード等のセキュリティ・デバイスを配布する場合の留意点

利用者の識別や認証、署名などを目的として、IC カード等のセキュリティ・デバイスに個人識別情報や暗号化鍵、電子証明書等を格納して配布する場合は、これらのデバイスが誤って本人以外の第三者の手に渡ることのないような対策を講じる必要がある。また、万一そのデバイスが第三者によって不正に入手された場合においても、簡単には利用されないようになっていることが重要である。

したがって、利用者の識別や認証、署名などが、これらデバイス単独で可能となるような運用はリスクが大きく、必ず利用者本人しか知りえない情報との組合せによってのみ有

功になるようなメカニズム、運用方法を採用すること。

IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替え手段による一時的なアクセスルールを用意するべきである。その際、ログ等を残し後日再発行された本人の正規の識別情報により、緊急アクセスログ等の確認操作をすることが望ましい。

バイオメトリクスを利用する場合の留意点

識別・認証に指紋や虹彩、声紋などのバイオメトリクス（生体計測情報）を用いる場合は、その測定精度にも注意を払う必要がある。現存する各種のバイオメトリクス機器の測定精度は、N 対 1 照合（入力された１つのサンプルが、登録されている複数のサンプルのどれに一致するか）には十分とは言えず、１対１照合（入力されたサンプルが、特定の１つのサンプルと一致するか）での利用が妥当であると考えられる。

したがって、バイオメトリクスを用いる場合は、単独での識別・認証を行わず、必ずユーザ ID 等（いわゆる PIN に対応するもの）と組合せて利用するべきである。

（2）アクセス権限の管理

情報システムの利用に際しては、組織における利用者や利用者グループ（業務単位など）ごとに、情報ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクが低減される。情報システムに、参照、更新、実行、追加などのようにきめ細かな権限の設定を行う機能があれば、さらにリスクは低減される。

アクセス権限の見直しは、人事異動等による利用者の担当業務の変更やなどに合わせて適宜行う必要があり、組織の規程で定められていなければならない。

（3）アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。したがって、アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対策を講じなければならない。

また、アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いものを使用し、組織内の全てのシステムで同期をとらねばならない。

（4）不正ソフトウェア対策

ウィルス、ワームなどと呼ばれる様々な形態を持つ不正なコードは、電子メール、ネットワーク、可搬媒体などを通して情報システム内に入る可能性がある。これら不正コードの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用などの重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正コードの侵入に気づくことになる。

対策としては不正コードのスキャン用ソフトウェアの導入が最も効果的であると考えられ、このソフトウェアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正コードの検出と除去が期待できる。しかし、これらのコンピュータウィルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。

ただし、たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正コードが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制なども効果が大きい。

C．最低限のガイドライン

1. ID、パスワード等により、診療録データへのアクセスにおける識別と認証を行うこと。
2. 動作確認等で個人データを使用するときは、漏洩等に十分留意すること。
3. 医療施設内の医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。
4. アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと。
5. ウィルスなどの不正なソフトウェアの混入を防ぐ適切な措置をとること。

D．推奨されるガイドライン

1. 診療録データへのアクセスにおける識別と認証を行うこと。
2. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
3. 医療施設内の医療従事者、関係職員ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。
4. アクセスの記録および定期的なログの確認を行うこと。
5. ウィルスなどの不正なソフトウェアの混入を防ぐ適切な措置をとること。また、そ

の対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）をとること。

6. 離席の場合のクローズ処理を施すこと（クリアスクリーン）。

5．6　人的安全対策

診療情報システムに関連する者として、次の5種類を想定する。

(a) 医師、看護師など診療業務で診療情報を取り扱い、法令上の守秘義務のある者
(b) 医事課職員、その事務委託者など診療を維持するための業務に携わり、雇用契約の元に診療情報を取り扱い、守秘義務を負う者
(c) システムの保守業者など雇用契約を結ばずに診療を維持するための業務に携わる者
(d) 患者、見舞い客など、診療情報にアクセスする権限を有しない第三者
(e) 診療碌等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a) (b)については、医療機関の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の2つに分けて説明する。

(d)の第三者については、人的安全管理措置は困難であり、他の方策による対策が必要である。

(e)については平成14年3月の通知「診療録等の保存を行う場所について」で認められた、いわゆる「外部保存」の委託先事業者に該当する。これに関しては、その主旨と実施の詳細を7章に記述する。

（1）従業者に対する人的安全管理措置

C．最低限のガイドライン

医療施設管理者は、個人情報に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

1. 医療従事者以外の事務職員の採用にあたっては、雇用及び契約時に守秘・非開示契約を締結することなどにより安全管理を行うこと。
2. 定期的に従業者に対し教育訓練を行うこと。
3. 従業者の退職後の個人情報保護規程を定めること。

D．推奨されるガイドライン

1. サーバ室などの管理上重要な場所では、モニタリング等により従業者に対する行動

の管理を行うこと。

（2）事務取扱委託業者の監督及び守秘義務契約

C．最低限のガイドライン

1. プログラムの異常等で、保存データを救済する必要があるときなど、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、施設内における適切な個人情報保護が行われるように、以下のような措置を行うこと。

   ① 包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
   ② 保守作業など電子保存システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。
   ③ 清掃など、直接電子保存システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
   ④ 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策および契約がなされていることを条件とすること。

2. プログラムの異常等で、保存データを救済する必要があるときなど、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

5．7　情報の破棄

B．考え方

診療に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報がお互いに関連して存在する場合は一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もある。

実際の廃棄に備えて、事前に廃棄プログラムなどの手順を明確化したものを作成しておくべきである。

外部の委託事業者に保存を委託している診療碌等について、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（または 監督する責任）を果たさなくてはならない。また、受託先の施設も、委託元の施設の求めに応じて、保存されている診療録等を厳正に取り扱い、処理を行った旨を委

託元施設に明確に示す必要がある。

C．最低限のガイドライン

1. ５．２．１で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。
3. 破棄を外部事業者に委託した場合は、５．６(2)に準じ、さらに委託者が確実に情報の破棄が行なわれたことを確認すること。
4. 運用管理規程において下記の内容を定めること。
   (a) 不要になった個人情報を含む媒体の廃棄を定める規程の作成の方法

５．８　情報システムの改造と保守

B．考え方

電子カルテシステムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂などがあるが、特に障害対応においては、原因特定や解析などのために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接診療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。

- 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センターなどで解析中のデータの第三者による覗き見や持ち出しなど
- 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変など
- 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止など
- 保存性の点では、意図的な媒体の破壊および初期化や、オペレーションミスによる媒体の初期化やデータの上書きなど

これらの脅威からデータを守るためには、医療機関の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。

また、保守作業によっては保守会社からさらに外部委託業者に修理などを依頼することが考えられるため、保守会社との保守契約の締結にあたっては、再委託先への個人情報保護の徹底などについて保守会社と同等の契約を求めることが重要である。

C．最低限のガイドライン

1. 動作確認で個人データを使用するときは、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去するなどの処理を行うことを求めること。
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
4. 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。
5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関側の責任者が逐次承認すること。
6. 保守会社と守秘義務契約を締結し、これを遵守させること。
7. 保守会社が個人情報を含むデータを組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取り扱いについて運用管理規程を定めることを求め、医療機関側責任者が逐次承認すること。
8. リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関側責任者が確認すること。
9. 再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。

D．推奨されるガイドライン

1. 詳細なオペレーション記録を保守操作ログとして記録すること。
2. 保守作業時には病院関係者立会いのもとで行うこと。
3. 作業員各人と保守会社との守秘義務契約を求めること。
4. 保守会社が個人情報を含むデータを組織外に持ち出す場合、詳細な作業記録を残すことを求めること。また必要に応じて医療機関の監査に応じることを求めること。
5. 保守作業にかかわるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べで表示し、かつ指定時間内でどの患者に何回のアクセスが行われたか

が確認できる仕組みが備わっていること。

5．9　外部と診療情報を交換する場合の安全管理

B．考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護に関して特に留意すべき項目について述べる。外部と診療情報を交換するケースとしては、検査を外部に委託していて、オンラインでデータをやり取りする場合等が考えられる。また法的な保存義務が存在しない診療記録等を外部に保存委託する場合もありえる。

法的に保存義務のある診療録等を外部に保存する場合もこの項に該当するが、さらに詳細な要件や留意事項があるため、７章に別途まとめて記述を行う。

(1) 個人情報の電気通信回線による伝送
(2) 診療情報の保管を外部委託する際に受託側施設内での個人情報の取り扱い
(3) 診療情報の保管を外部委託することの患者への説明

（1）個人情報の電気通信回線による伝送

① 秘匿性の確保のための適切な暗号化

電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。したがって電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。

② 通信の起点・終点識別のための認証

通信手段によって、起点･終点の識別方法は異なる。例えば､インターネットを用いる場合は起点・終点の識別はIPパケットを見るだけでは確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の施設と受託先の施設を確実に相互に認証しなければならない。たとえば、認証付きのVPN、SSL/TLSやISCLを適切に利用することにより実現できる。なお、当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。

③ リモートログイン制限機能

診療情報の受託先の施設や委託元の施設のサーバへのリモートログイン機能に制限を設けないで容認すると、ログインのためのパスワードが平文でLAN回線上を流れたり、ファ

イル転送プログラム中にパスワードがそのままの形でとりこまれたりすることにより、これが漏洩する可能性がある。また、認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。また、一時保存しているディスク上の診療情報の不正な読み取りや改ざんが行われる可能性もある。他方、システムメンテナンスを目的とした遠隔保守のためのアクセスも考えられる。

リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間など保守コストが増大する。適切に管理されたリモートログイン機能のみに制限しなければならない。

（2）診療に係る情報の保存を外部委託する際に受託側施設内での個人情報の取り扱い

① 保存を受託する施設における診療情報へのアクセス禁止

診療情報を受託した施設においては、診療録等の個人情報の秘密保持は厳格であるべきで、施設の管理者であっても、受託した診療録等の個人情報に正当な理由なくアクセスすることができない仕組みを備えるべきである。

② 障害対策時のアクセス通知

プログラムの異常等で保存データを救済する必要があるときなど、やむを得ない事情で、受託した診療録等の個人情報にアクセスしなければならない場合は、自施設における診療録等の個人情報と同様の秘密保持を行うと同時に、アクセスする許可を予め外部保存の委託元の施設に求めなければならない。

③ アクセスログの完全性とアクセス禁止

診療情報の受託先施設における保存データの安全性を確保するために、アクセスログを確認し、アクセスログの完全性を確立させることが重要である。一方でログ情報には、特定の診療録等の有無が含まれることがあり、ログを閲覧することは個人情報の侵害になりうる。したがって、外部保存を受託する施設でのログ管理は、その完全性のみを保証することとし、システム設計上、または運用面でシステムの異常などのやむを得ない場合を除いて、内容にはアクセスしないことが求められる。また、ログ情報にアクセスした場合には、その都度委託施設への報告を行うことが求められる。

④ 診療情報を受託する施設の監督責任

診療情報受託の際の管理責任や説明責任については、ネットワーク管理者、機器やソフトウェアの製造業者にも応分の責任があり、契約においてその責任分担を明確にしておかなければならないが、診療録等の個人情報の保護に関する最終的な責任は、当該診療録等を保存する法的義務のある委託元の施設が負わなければならない。したがって委託元の施設は、外部保存を委託する際に、受託先の施設内における個人情報保護に関する対策が実

施されることを契約等に含めるとともに、その実施状況を監督する必要がある。