4.3 例示による考え方の整理

本項では「4.2 責任分界点について」について、いくつか例を挙げて解説する。ただし、本項は4.2の考え方を例として考えた場合であるため、医療情報システムの安全管理や接続時のネットワークの考え方、保存義務のある書類の保存、外部保存が受託可能な機関の選定基準等は、それぞれ6章、7章、8章を参照すること。

A. 地域医療連携で患者情報を交換する場合

I 医療機関等における考え方

① 情報処理関連事業者の提供するネットワークを通じて医療情報の提供元医療機関等と提供先医療機関等で患者情報を交換する場合の責任分界点

提供元医療機関等と提供先機関はネットワーク経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意しておく。

その上で、自らの責任範囲において、情報処理関連事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにしておく。

ただし、通常運用における責任、事後責任は、委託の場合は、原則として提供元医療機関等にあり、第三者提供において適切に情報が提供された場合は、原則として提供先医療機関等にあり、情報処理関連事業者に瑕疵のない場合は、情報処理関連事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

② 提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界点

ここでいう独自とは、情報処理関連事業者のネットワークではあるが、接続しようとする医療機関等同士がルータ等の接続機器を自ら設定して1対1や1対Nで相互に接続する場合や電話回線等の公衆網を使う場合について述べる。

この場合、あらかじめ提供先または提供先となる可能性がある機関を特定できる場合は、委託または第三者提供の要件に従って両機関が責務を果たさなければならない。

情報処理関連事業者に対しては、管理責任の分担は発生せず、通信の品質確保は発生するとしても、情報処理関連事業者が提示する約款に示される一般的な責任しか存在しない。

更に、提供元医療機関等と提供先機関が1対N通信で、提供先機関が一つでも特定できない場合は原則として医療情報を提供できない。ただし、法令で定められている場合等の例外を除く。

II 情報処理関連事業者に対する考え方

① 医療情報が発信元／送信先で適切に暗号化される場合の責任分界点

患者情報を送信しようとする医療機関等の情報システムにおいて、送信前に患者情報が暗号化され、情報を受け取った医療機関等の情報システムにおいて患者情報が復号される場合、情報処理関連事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係であり、4.2で述べた責任は限定的になる。

この場合、情報処理関連事業者に存在するのは管理責任であり、ネットワーク上の情報の改ざんや侵入、妨害の脅威に対する管理責任の範囲やネットワークの可用性等の品質に関して契約で明らかにしておく。

なお、暗号化等のネットワークに係る考え方や最低限のガイドラインについては、「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

② 医療情報が情報処理関連事業者の管理範囲の開始点で適切に暗号化される場合の責任分界点

情報処理関連事業者の中には、例えば暗号化された安全なネットワーク回線の提供を主たるサービスとしている事業者も存在する。

そのようなネットワーク回線を使う場合、事業者が提供するネットワーク回線上における外部からの情報の盗聴や改ざん、侵入等やサービスの可用性等の品質については事業者に管理責任が発生する。従って、それらの責任については契約で明らかにしておく。

ただし、事業者が提供するネットワーク回線に到達するまでの管理責任やネットワーク回線を流れる情報に対する管理責任は医療機関等に存在するため、「I 医療機関等における考え方　①医療情報の提供元医療機関等と提供先医療機関等の責任分界点」に則った考え方の整理が必要である。

なお、ネットワーク回線上とネットワーク回線を流れる情報に対する考え方や最低限のガイドラインについては、「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

III 外部保存機関が介在する場合の考え方

この場合、保存する情報は外部保存機関に委託することになるため、通常運用における責任、事後責任は医療機関等にある。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等における管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要がある。

また、外部保存機関とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておく。

なお、医療機関等が外部保存機関を通じて患者情報を交換する場合の医療機関等および外部保存機関に対する考え方は、「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」で定める保存機関毎に「2. 情報の取り扱い」および

「3. 情報の提供」として別途、詳細に規定しているため 8.1.2 を参照されたい。

B. 業務の必要に応じて医療機関等の施設外から情報システムにアクセスする場合

I　自機関の情報システムにアクセスし業務を行う、いわゆるテレワーク

昨今、医療機関等においても医療機関等の施設外から自機関の情報システムにアクセスし業務を行う、いわゆるテレワークも一般的になってきた。

この場合、責任分界の観点では自施設に閉じているが、情報処理関連事業者が間に入って通信回線の両端で一医療機関等の従業者が係わることになる。

更に、この場合には通信回線がインターネットだけでなく携帯電話網、公衆回線など多彩なものが利用されることになり、個人情報保護について広範な対応が求められることになる。

特に、医療機関等の管理責任者でない医療機関等の従業者についても管理責任が問われる事態も発生することに注意を払う必要がある。

この例の場合、責任分界点としては基本的に自施設に閉じているため、責任のあり方の原則としては、「4.1　医療機関等の管理者の情報保護責任について」となることに留意しなくてはならない。

II　第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス

この例のような、リモートログインを用いた保守業者の遠隔保守のためのアクセスが考えられる。この場合、適切な情報管理や情報アクセス制御がなされていないと一時保存しているディスク上の個人情報を含む医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、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、保守に要する時間等の保守コストが増大する。

従って、保守の利便性と情報保護との兼ね合いを見極めつつ実施する必要がある。

ただし、この場合でも、当然、医療機関等に対して「通常運用における責任」、「事後責任」が存在するため、管理状況の報告を定期的に受け、管理に関する最終的な責任の所在を明確にする等の監督を行い、管理責任を果たす必要がある。

なお、リモートログインも含めた、保守の考え方については「6.8　情報システムの改造と保守」を参照されたい。

なお、「I　自機関の情報システムにアクセスし業務を行う、いわゆるテレワーク」、「II　第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス」のどちらにおいても、施設外から情報システムにアクセスする場合のネットワークの考え方については、「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」の、特に「B-2. 選択すべきネットワークのセキュリティの考え方　III. モバイル端末等を使って医療機関の外部から接続する場合」を参照されたい。

C. 診療を目的とした第三者委託の場合

ここでいう第三者委託とは遠隔画像診断、臨床検査、治験等、診療を目的とした第三者委託であり、一時的にせよ情報を第三者が保管する。

委託元である医療機関の管理者は委託先に対して、委託先の選定や委託先への（セキュリティ等の）改善指示を含めた管理責任があるとともに、情報の保存期間の規定等の管理監督を行う必要がある。

ただし、委託先は保存した情報の漏洩防止、改ざん防止等の対策を講じることは当然であるが、感染症情報や遺伝子情報など機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。

D. 法令で定められている場合

法令で定められている場合などの特別な事情により、情報処理関連事業者に暗号化されていない医療情報が送信される場合は、情報処理関連事業者もしくはネットワークにおいて盗聴の脅威に対する対策を施す必要がある。

そのため、当該医療情報の通信経路上の管理責任を負っている医療機関等は、情報処理関連事業者と医療情報の管理責任についての明確化を行わなくてはならない。

また、情報処理関連事業者に対して管理責任の一部もしくは全部を委託する場合は、それぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

【参考】技術的対策と運用による対策

情報システムの安全を担保するためには、「技術的な対応」と「組織的な対応（運用による対策）」の総合的な組み合わせによって達成する必要がある。

技術的な対応は医療機関等の総合的な判断の下、主にシステム提供側（ベンダー）に求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。

総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により一定レベルの安全性を確保することである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化により異なってくるので、その動向に注意を払う必要がある。

運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として「基準適合チェックリスト」等を作成して整理しておく必要がある。このようなチェックリストは第三者へ説明する際の参考資料に利用できる。

5　情報の相互利用性と標準化について

本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において情報処理システムを導入する目的は当初は事務処理の合理化だけであったが、現在は平成13年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報の共有の推進や、医療安全、医療の質の向上に寄与できるものであることが求められている。

これらの目的を実現するためには情報の適切な標準化が必要であることは論を待たない。本ガイドラインは医療に関係する情報システムの安全な管理・運用を目的としているが、情報の安全性の重要な要素として、必要時に利用可能であることを確保する可用性を上げることができる。

可用性は情報を保持しなければならない任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い新旧のシステム間での情報の互換性を保ち旧システムで保存された医療情報を確実に読み出せるという、「新旧システムで医療情報の相互利用性」を確保することは、電子保存の見読性及び保存性原則確保の点からみても医療情報システムの必須の要件である。

医療に有用な意味のある情報を長期間にわたり読み出し可能な形で保存するためには、将来にわたりメンテナンスを継続することが期待される標準的な用語集やコードセットを出来る限り利用して保存を行うことが望ましい。

5.1　標準的な用語集やコードセットの利用

すでに公開されている用語集やコードセットのうち、日本での各分野における実質的な標準的用語コード集と考えられるものについては情報の保存の際にこれらを利用することが強く推奨される。使用しない場合でもこれらの用語集やコードセットに容易に変換できることが必要である。以下に標準的な用語集やコードセットの例をあげるが、医療情報標準化推進協議会（ Health Information and Communication Standards Board：HELICS協議会）がわが国での用語集やコードセットの標準案の登録を進めており、随時参照されたい。

病名：ICD10対応電子カルテ用標準病名マスタ
医薬品名：標準医薬品マスタ
臨床検査：JAHIS臨床検査データ交換規約

5.2 国際的な標準規格への準拠

DICOM (Digital Imaging and Communications in Medicine)、HL7 (Health Level Seven) 等の規格及びこれらの規格の標準的な運用方法を定めた IHE (Integrating the Healthcare Enterprise) は、国際的な標準や規格として提唱され、一部はわが国でも利用が進んでいる。

これらの国際的な標準や規格の中で、我が国の医療に適合するものについては、情報の相互利用性の観点から直接これらの規格や標準を採用するか、少なくともこれらの規格や標準に適合した情報形式に容易に変換可能な状態にしておくことが強く推奨される。

また、注意しなければならない点として外字の問題がある。外字とは JIS 文字コードのような容易に移行可能な文字セット以外の文字を独自に定義してもちいた表記文字であるが、そのような外字を使用したシステムではあらかじめ使用した外字のリストを管理し、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要がある。標準化の観点から見れば外字を使用する必要がない文字セットが検討されることを期待したい。

6　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等や個人情報保護関連各法（個人情報保護法、行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号)、独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号)）に規定された安全管理・確保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。守秘義務は医療専門職や行政機関の職員等の個人に、安全管理・確保は個人情報取扱事業者や行政機関の長等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。この章での制度上の要求事項は個人情報保護法の条文を例示する。

A. 制度上の要求事項

（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。

6.1　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、取扱いや保存の方法と期間、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。

6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践

6.2.1 ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 では PDCA の各ステップを次の様に規定している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実施 (ISMS の導入及び運用)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及び見直し)	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P では ISMS 構築の骨格となる文書（基本方針、運用管理規程など）と文書化された ISMS 構築手順を確立する。
D では P で準備した文書や手順を使って実際に ISMS を構築する。
C では構築した ISMS が適切に運用されているか、監視と見直しを行う。
A では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのようにおこなわれているかについて JIPDEC（財団法人 日本情報処理開発協会）の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されている。

【医療の安全管理の流れ】

事故やミスの発見と報告

「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析

- 「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
  （例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
- 作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。

↓

予防／是正策

- 再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底など）

上記を見ると、主にD→C→Aが中心になっている。これは医療分野においては診察、診断、治療、看護などの手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みが出来上がっているためと言える。

反面、情報セキュリティではIT技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため情報セキュリティ独自の管理方法が必要であり、ISMSはそのために考え出された。ISMSは医療の安全管理と同様PDCAサイクルで構築し、維持して行く。

逆に言えば、医療関係者にとってISMS構築はPのステップを適切に実践し、ISMSの骨格となる文書体系や手順などを確立すれば、あとは自然にISMSが構築されていく土壌があると言える。

Pのステップを実践するために必要なことは何かについて次に述べる。

6.2.2 取扱い情報の把握

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視点からの影響の大きさと、継続した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。この他に医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類する。

一般に医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。

6.2.3 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。医療機関等では一般に他の職員等への信頼を元に業務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、6.3～6.10の対策を行うことになる。

特に安全管理や個人情報保護関連各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ことであり、これが限界である。従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。

医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 医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、毀損、滅失、漏えい
- (b) 権限のある者による不当な目的でのアクセス、改ざん、毀損、滅失、漏えい
- (c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい

② 入力の際に用いたメモ・原稿・検査データ等
- (a) メモ・原稿・検査データ等の覗き見
- (b) メモ・原稿・検査データ等持ち出し
- (c) メモ・原稿・検査データ等のコピー
- (d) メモ・原稿・検査データの不適切な廃棄

③ 個人情報等のデータを格納したノートパソコン等の情報端末

(a)情報端末の持ち出し

(b)ネットワーク接続によるコンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい

(c)ファイル交換ソフト（Winny 等）の不適切な取扱いによる情報漏えい

(d)情報端末の盗難、紛失

(e)情報端末の不適切な破棄

④ データを格納した可搬型媒体等

(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) 可搬型媒体の盗難、紛失

⑤ 参照表示した端末画面等

(a) 端末画面の覗き見

⑥ データを印刷した紙やフィルム等

(a) 紙やフィルム等の覗き見

(b) 紙やフィルム等の持ち出し

(c) 紙やフィルム等のコピー

(d) 紙やフィルム等の不適切な廃棄

⑦ 医療情報システム自身

(a) サイバー攻撃による IT 障害

- 不正侵入
- 改ざん
- 不正コマンド実行
- 情報かく乱
- ウイルス攻撃
- サービス不能（DoS：Denial of Service）攻撃
- 情報漏えい　等

(b) 非意図的要因による IT 障害

- システムの仕様やプログラム上の欠陥（バグ）
- 操作ミス

- 故障
- 情報漏えい　等

(c) 災害によるIT障害

- 地震、水害、落雷、火災等の災害による電力供給の途絶
- 地震、水害、落雷、火災等の災害による通信の途絶
- 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- 地震、水害、落雷、火災等の災害による重要インフラ事業者等におけるITの機能不全

これらの脅威に対し、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。

6.3 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、その実施状況を日常の自己点検等によって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 医療情報の取扱い台帳の整備
④ 医療情報の安全管理対策の評価、見直し及び改善
⑤ 情報や情報端末の外部持ち出しに関する規則等の整備
⑥ 情報端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その情報端末等の管理規定
⑦ 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（基本方針と管理目的の表明）
- 医療機関等の内部の体制、外部保存に関わる外部の人及び施設
- 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

なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報および情報機器の持ち出しについて」に記載しているので参照されたい。

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。ただし小規模医療機関等において役割が自明の場合は、明確な規程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、入退を制限する等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次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
   (b) リスクに対する予防、発生時の対応の方法

6.4 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入力、参照、格納される情報端末やコンピュータ、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。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
② 盗難、窃視等の防止
③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護および措置

なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報および情報機器の持ち出しについて」に記載しているので参照されたい。

C. 最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じること。
   ただし、本体策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
3. 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。
4. 個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること。
5. 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。

6.5 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「6.2.3 リスク分析」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) 利用者の識別及び認証
(2) 情報の区分管理と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
(5) ネットワーク上からの不正アクセス

なお、情報および情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9 情報および情報機器の持ち出しについて」に記載しているので参照されたい。

(1) 利用者の識別及び認証

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。

小規模な医療機関等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及び関係者に対し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とパスワードが書かれた紙等が貼られていて、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ＩＤ・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等から、パスワードが盗まれる。
- コンピュータウイルスにより、ID や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、クリアスクリーン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、署名等を目的として、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。

従って、利用者の識別や認証、署名等が、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効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、安全管理のレベルを安易に下げることがないように、本人確認を十分におこなった上で代替手段の使用を許し、さ

らに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、上記緊急時の操作の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、声紋等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。医療情報システムで一般的に利用可能と思われる現存する各種のバイオメトリクス機器の測定精度は、1対N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。

従って、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等個人を識別できるものと組合せて利用するべきである。

また、生体情報を基に認証するために以下のような、生体情報特有の問題がある。

- 事故や疾病等により認証に用いる部位の損失等
- 成長等による認証に用いる部位の変化
- 一卵性の双子の場合、特徴値が近似することがある
- 赤外線写真等による"なりすまし"(ICカード等の偽造に相当)

上記の事を考慮のうえ、生体情報の特徴を吟味し適切な手法を用いる必要がある。

"なりすまし"や欠損等の対処として、異なる手法や異なる部位の生体情報を用いたり、IC カード等のセキュリティ・デバイスと組み合わせを行う方法や、従来のパスワードを付加する方法も有効である。

(2) 情報の区分管理とアクセス権限の管理

情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）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、追加等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等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