

### 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程
- 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。

なお、情報及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 情報及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) 理念（基本方針と管理目的の表明）
  - (b) 医療機関等の体制
  - (c) 契約書・マニュアル等の文書の管理

- (d) リスクに対する予防、発生時の対応の方法
- (e) 機器を用いる場合は機器の管理
- (f) 個人情報の記録媒体の管理（保管・授受等）の方法
- (g) 患者等への説明と同意を得る方法
- (h) 監査
- (i) 苦情・質問の受付窓口

## 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及び措置

なお、情報及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 情報及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、運用管理規程に基づき許可された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、本対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。例えば、以下のことを実施すること。
  - ・ 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。
  - ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
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. 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、技術的な対策は強力な安全対策の手段となりうる。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、情報及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 情報及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、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以下のようなリスクに対処しなければならない。

- ・ 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。

- ・ ひとつの ID を複数の利用者が使用している。
- ・ 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セキュリティ・デバイス（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。

認証に用いる手段としては、ID・パスワードの組合せのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難である。そこで、IC カード等のセキュリティ・デバイス+パスワードやバイオメトリクス+IC カ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）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、これらのセキュリティ・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、万一そのセキュリティ・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し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、これらセキュリティ・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。

- ・事故や疾病等による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。

欠損への対処としては異なる手法や異なる部位の生体情報を用いること。なりすましへの対処としては二要素認証(ICカードやパスワードとバイオメトリクスの組み合わせ等)を用いること。

## (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、重要性和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を低減できる。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、さらにリスクを低減できる。

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。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／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、管理対象の全てのシステムで同期を取らなければならない。

### (4) 不正ソフトウェア対策

ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正ソフトウェア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、資源の不正使用等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、不正ソフトウェアの侵入に気づくことになる。

対策としては不正ソフトウェア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、不正ソフトウェアの検出と除去が期待できる。また、このことは医療機関等の外部で利用する情報端末や PC 等についても同様であるが、その考え方と対策については、「6.9 情報及び情報端末の持ち出しについて」を参照されたい。

ただし、これらのコンピュータウイ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、全ての不正ソフトウェア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・ホールが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

実行の抑制等も効果が大きい。

#### (5) ネットワーク上からの不正アクセス

ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。

ファイアウォールは「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望ましい。システム管理者はその方式が何をどのように守っているかを認識すべきである。このことは、医療機関等の外部から医療機関等の情報システムに接続される PC 等の情報端末に対しても同様であるが、その考え方と対策については、「6.9 情報及び情報端末の持ち出しについて」を参照されたい。

不正な攻撃を検知するシステム (IDS : Intrusion Detection System) もあり、医療情報システムと外部ネットワークとの関係に応じて、IDS の採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール (脆弱性等) に対する診断 (セキュリティ診断) を定期的 to 実施し、パッチ等の対策を講じておくことも重要である。

無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃 (サービス不能攻撃 DoS : Denial of Service 等) を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて PC を識別する 경우가多いが、MAC アドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の窃視を防止するために、暗号化等による”情報漏えい”への対策も必要となる。

#### (6) その他

無線 LAN は、看護師等が情報端末を利用し患者のベッドサイドで作業する場合等に利便性が高い反面、通信の遮断等も起こる危惧があるので、情報の可用性が阻害されないように留意する必要がある。また、無線電波により重大な影響を被るおそれのある機器等の周辺での利用には注意が必要である。

最近では、電力線搬送通信 (PLC : Power Line Communication) が利用可能になった。しかし、医療機関等において PLC を利用する場合、医療機器に対する安全性が確認されておらず、厚生労働省医薬食品局から「広帯域電力線搬送通信機器による医療機器への影



響に関する医療関係者等からの照会に対する対応について」(平成18年11月9日付け薬食安発第1109002号)の通知が出されているため可用性の確保と他の医療機器への影響の双方に留意する必要がある。

### C. 最低限のガイドライン

1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。
2. 本人の識別・認証にユーザIDとパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。
3. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。
4. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。
5. 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。また、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よう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。
6. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。

情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録(操作者及び操作内容)を必ず行うこと。

7. アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を講じること。
8. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。
9. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等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)を行うこと。

#### 10. パスワードを利用者識別に使用する場合

システム管理者は以下の事項に留意すること。

- (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。(利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること)
- (2) 利用者がパスワードを忘れてたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。
- (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)

また、利用者は以下の事項に留意すること。

- (1) パスワードは定期的に変更し(最長でも 2 ヶ月以内)、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。
- (2) 類推しやすいパスワードを使用しないこと。

#### 11. 無線 LAN を利用する場合

システム管理者は以下の事項に留意すること。

- (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。
- (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。
- (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。
- (4) 電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。
- (5) 無線 LAN の適用に関しては、総務省発行の「安心して無線 LAN を利用するために」を参考にすること。

### D. 推奨されるガイドライン

1. 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。
2. 離席の場合のクローズ処理等を施すこと(クリアスクリーン:ログオフあるいはパスワード付きスクリーンセーバー等)。
3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール(ステートフルインスペクションやそれと同等の機能を含む)を設置し、ACL(アクセス制御リスト)等を適切に設定すること。

4. パスワードを利用者識別に使用する場合以下の基準を遵守すること。
  - (1) パスワード入力不成功に終わった場合の再入力に対して一定不応時間を設定すること。
  - (2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。
5. 認証に用いられる手段としては、ID+バイオメトリックスあるいはICカード等のセキュリティ・デバイス+パスワードまたはバイオメトリックス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)等、より認証強度が高い方式を採用すること。
6. 無線LANのアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば802.1xや電子証明書を組み合わせたセキュリティ強化をすること。

## 6.6 人的安全対策

### B. 考え方

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。

医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、看護師等の業務で診療に関わる情報を取扱い、法令上の守秘義務のある者
- (b) 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取扱い、守秘義務を負う者
- (c) システムの保守業者等の雇用契約を結ばずに医療機関等の業務に携わる者
- (d) 見舞い客等の医療情報にアクセスする権限を有しない第三者
- (e) 診療録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、医療機関等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、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏えい等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、いわゆる「外部保存」を受託する機関等に該当するが、これに関しては詳細を8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

医療機関等の管理者は、個人情報の安全管理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る、以下の措置をとること。

1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
2. 定期的に従業者に対し個人情報の安全管理に関する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. サーバ室等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. 医療機関等の事務、運用等を外部の事業者へ委託する場合は、医療機関等の内部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 受託する事業者に対する包括的な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 保守作業等の医療情報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・作業結果の確認を行うこと。
  - ③ 清掃等の直接医療情報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事業者と同等の個人情報保護に関する対策及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等、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。

## 6.7 情報の破棄

### B. 考え方

医療に係る電子情報は破棄に関しても安全性を確保する必要がある。破棄は確実に行う必要がある。しかし、例えばデータベースのように情報が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り、注意しなくてはならない。

実際の破棄に備えて、事前に破棄の手順を明確化しておくべきである。

### C. 最低限のガイドライン

1. 「6.1 方針の制定と公表」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. 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行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破棄を定める規程の作成

## 6.8 情報システムの改造と保守

### B. 考え方

医療情報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、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等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医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、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
- ・ 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等
- ・ 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等
- ・ 保存性の点では、意図的な媒体の破壊及び初期化や、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等

これらの脅威からデータを守るためには、医療機関等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作業時の医療機関等の関係者による監督、等の運用面を中心とする対策が必要である。

保守作業によっては保守会社からさらに外部の事業者へ修理等を委託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、再委託する事業者への個人情報保護の徹底等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. 動作確認で個人情報を含む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ともに、終了後は確実にデータを消去する等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、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む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等の責任者が逐一承認すること。
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すことは避けるべきであるが、やむを得ない状況で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、医療機関等の責任者が逐一承認すること。
8. リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。
9. 再委託が行われる場合は、再委託する事業者にも保守会社の責任で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. 保守作業時には医療機関等の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ことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、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等の監査に応じることを求めること。
5. 保守作業に関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て表示し、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。



## 6.9 情報及び情報機器の持ち出しについて

### B. 考え方

昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。

一方で、在宅医療、訪問診療等の増加、モバイル端末の発展により医療情報を持ち出すニーズや機会が増加していることも事実である。

情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末や CD-R、USB メモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。

まず重要なことは、「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」の「6.2.2 取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3 リスク分析」を実施することである。

その上で、医療機関等において把握されている情報もしくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。

一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。

ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。

なお、スマートフォンを利用する際の安全対策については、「スマートフォン・クラウドセキュリティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～（総務省；平成24年6月）」が参考になる。

### C. 最低限のガイドライン

1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
3. 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。
6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「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」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあり、使用する場合は 6.11 章で述べている基準を満たした通信手段を使うこと。
9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
10. 個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を取るとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。

#### D. 推奨されるガイドライン

1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせる用いること。
3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。
  - ・ 個人の所有する、あるいは個人の管理下にある端末は原則として使用せず、機器の設定の変更は管理者のみが可能とすること。
  - ・ 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化するなどの対策を行うこと。

## 6.10 災害等の非常時の対応

### B. 考え方

災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画(BCP: Business Continuity Plan)と呼ぶ。

我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため適切な BCP の作成と訓練は可能であり、必須の事項と考えられる。

医療機関全体の BCP は本ガイドラインの範疇を超えるため、ここでは「6.2.3 リスク分析」の「⑦医療情報システム」に掲げる自然災害やサイバー攻撃による IT 障害等の非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における医療情報システムの BCP や留意事項について述べる。ただし、医療機関全体の BCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならないとしないことには言うまでもない。

「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非正常状態になる場合がある。

前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。

後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合である。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。

#### (1) 非常時における事業継続計画

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り計画内容を事前演習等で検証することが望ましい。以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。

##### ① BCP として事前に周知しておく必要がある事項

事前に対応策を知ってもらい、信頼してもらっておくべきである。

- ・ ポリシと計画  
何が「非常事態」なのかを理解し、定義すべきである。
- ・ 非常事態検知手段  
災害や故障の検知機能と発生情報の確認手段

- ・ 非常時対応チームの連絡先リスト、連絡手段及び対策ツール
- ・ 非常時に公にすべき文書及び情報

## ② BCP 実行フェーズ

災害や事故の発生（或いは発生の可能性）を検知してから、BCP 実行か通常の障害対策かの判断を行い、BCP 発動と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡・協力依頼を行い、システムの切替／縮退等の準備を行う。例えば、ネットワークから切り離れたスタンドアロンでの使用や、紙での運用等が考えられる。

業務を受託する事業者との間の連絡体制や受託する事業者と一体となったトラブル対処方法等が明示されるべきである。

具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」及び「影響度の確認」である。

## ③ 業務再開フェーズ

BCP を発動してから、バックアップサイト・手作業等の代替手段により業務を再開し、軌道に乗せるまでフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員等の人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。

最も緊急度の高い業務（基幹業務）から再開する。

具体的項目は「人的資源の確保」、「代替施設及び設備の確保」、「再開／復旧活動の両立」及び「リスク対策によって新たに生じるリスクへの対策」である。

## ④ 業務回復フェーズ

最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイントとなる。

具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」及び「制限の確認」である。

## ⑤ 全面復旧フェーズ

代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。

具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」及び「総括」である。

## ⑥ BCPの見直し

正常な状態に復帰した後に、BCPに関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCPの見直しを行い、次の非常時に備えることが重要である。

## (2) 医療システムの非常時使用への対応

### ① 非常時用ユーザアカウントの用意

- ・ 停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えなくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データへのアクセス制限が医療サービス低下を招かないように配慮している。ブレークグラスでは非常時用ユーザアカウントは通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更をすることを基本としている。

- ② 災害時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮する等、必要に応じて非常時の運用に対応した機能を実装すること。

上記の様な非常時使用への対応機能の用意は、関係者に周知され非常時に適切に用いる必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

## C. 最低限のガイドライン

1. 医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 非常時の情報システムの運用
  - ・ 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。
  - ・ 非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監

査をすること。

- ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。

4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。

## 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

### B. 考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。ここでは、双方向だけではなく、一方向の伝送も含む。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS型のサービスを利用する、医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する、患者等による外部からのアクセスを許可する、等が考えられる。

医療情報をネットワークを利用して外部と交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

なお、可搬媒体や紙を用いて情報を搬送する場合は、付則1及び2を参照願いたい。

#### B-1. 医療機関等における留意事項

ここでは4章の「電子的な医療情報を扱う際の責任のあり方 4.2 委託と提供における責任分界点について」で述べた責任の内、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は送信元の医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の機関に受け渡しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、ここでいう管理責任とは電子的に記載されている情報の内容に対して負うべきものでありその記載内容や記載者の正当性の保持（真正性の確保）のことを指す。つまり、後述する「B-2. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮



に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。このような情報の内容に対するセキュリティのことをオブジェクト・セキュリティと呼ぶことがある。一方、「B・2. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。このような回線上の情報に対するセキュリティのことをチャネル・セキュリティと呼ぶことがある。

このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

### ①「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。例えば、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取る等、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。一方、ネットワーク機材の不適切な設定により、意図しない情報漏えいや誤送信等も想定され、このような場合には医療機関等における責任が発生する事例も考えられる。

このように様々な事例が考えられる中で、医療機関等においては、万が一、伝送途中で情報が盗み取られたり、意図しない情報漏えいや誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報の暗号化が考えられる。ここでいう暗号化とは、先に例示した情報そのものの暗号化（オブジェクト・セキュリティ）のことを指している。

どの様な暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密度や医療機関等で構築している情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ではあるが、少なくとも情報を伝送し、医療機関等の設備から情報が送出される段階においては暗号化されていることが望ましい。

この盗聴防止については、例えばリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託事業者等に確認し、監督する責任を負う。

### ②「改ざん」の危険性への対応

ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えなければならない。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。また、後述する「B・2. 選択すべきネットワークセキュリティ

の考え方」のネットワークの構成によっては、ネットワーク自体に情報の秘匿化機能が不十分な場合もあり、改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

### ③「なりすまし」の危険性への対応

ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の機関が確かに意図した相手であるかを確認しなくてはならない。逆に、情報の受け手となる送信先の機関は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であることを確認しなくてはならない。これは、ネットワークが非対面による情報伝達手段であることに起因するものである。

そのため、例えば通信の起点と終点の機関を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。また、改ざん防止と併せて、送信元が正当な送信元であることを確認するために、医療情報等に対して電子署名を組み合わせることも考えられる。

また、上記の危険性がサイバー攻撃による場合の対応は「6.10 災害等の非常時の対応」を参照されたい。

## B-2. 選択すべきネットワークのセキュリティの考え方

「B-1. 医療機関等における留意事項」では主に情報内容が脅威に対応するオブジェクト・セキュリティについて解説したが、ここでは通信経路上での脅威への対応であるチャネル・セキュリティについて解説する。

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、情報を受信する機関の外部ネットワーク接続点までや、業務の必要性から並びに患者からのアクセスを許可する等、外部から医療機関等の情報システムにアクセスする接続点までのことを指し、医療機関等の内部で構成される LAN は対象とならない。ただし、4章「電子的な医療情報を扱う際の責任のあり方 4.2 責任分界点について」でも触れた通り、接続先の医療機関等のネットワーク構成や経路設計によって意図しない情報漏えいが起こる可能性については留意をし、確認をする責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等としては交換しようとする情報の機密性の整理をする必要がある。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、予約システムが扱う再診予約情報の様な機密性の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この

整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要はある。その際の考え方としては、大きく次の2つに類型化される。

- ・ 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPN サービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等においては、善管注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確認しなくてはならない。

- ・ 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入したネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。

そのため、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り扱いに関する契約の締結、脅威が発生した際に備えて、通信事業者がネットワーク経路上のセキュリティを委託する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等を考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定

して留意点を述べる。

また、想定するケースの中でも、携帯電話・PHS や可搬型コンピュータ等のいわゆるモバイル端末等を使って医療機関等の外部から接続する場合は、利用するモバイル端末とネットワークの接続サービス及びその組み合わせによって複数の接続形態が存在するため、これらについては特に「Ⅲ モバイル端末等を使って医療機関等の外部から接続する場合」を設けて考え方を整理している。

## I. クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、いわゆるインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低い。ただし、「B-1. 医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、ウイルス対策ソフトのパターン定義ファイルや OS のセキュリティ・パッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特長を述べる。

### ①専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（「帯域」という）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性和情報の量等の兼ね合いを見極める必要もある。



図 B-2-① 専用線で接続されている場合

## ②公衆網で接続されている場合

公衆網とは ISDN（Integrated Services Digital Network）やダイヤルアップ接続等、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続はインターネットサービスプロバイダ（以下、ISP）に接続する接続方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイヤルしてネットワーク接続を確立するため、ネットワーク接続を確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様に拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため大量の情報もしくは画像等の容量の大きな情報の送信には不向きであるため、適用範囲を適切に見定める必要がある。



図 B-2-② 公衆網で接続されている場合

## ③閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を言う。このような接続サービスを本ガイドラインでは IP-VPN（Internet Protocol-Virtual Private Network）と呼び、クローズドなネットワークとして取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

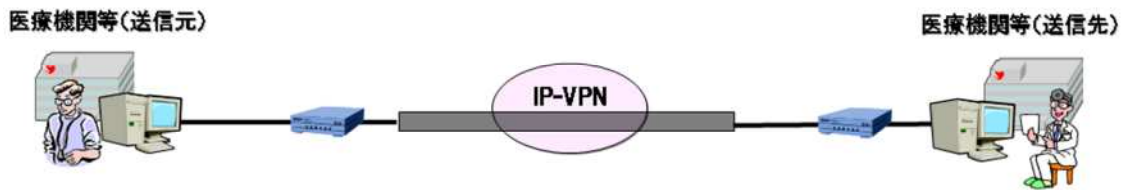


図 B-2-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

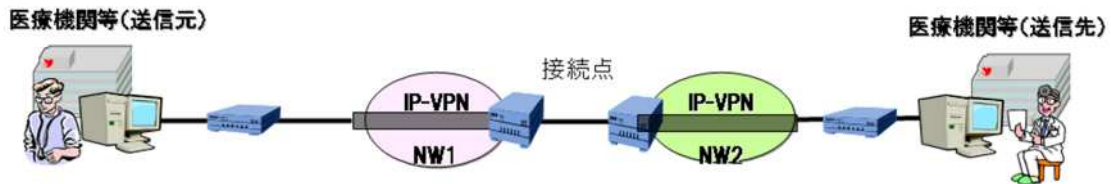


図 B-2-③-b 途中で複数の閉域ネットワークが相互接続して接続されている場合

以上の3つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。また異なる通信事業者のクローズドなネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする必要がある。この際、偶発的に情報の中身が漏示する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。そのほか、医療機関等から閉域 IP 通信網に接続する点等、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

これらの接続サービスでは、一般的に送られる情報そのものに対する暗号化は施されていない。そのため、クローズドなネットワークを選択した場合であっても、「B-1. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入する等の措置を取る必要がある。

## II. オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。すなわち、オブジェクト・セキュリティの考え方に沿った対策を施す必要がある。



ただし、B-2 の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の判断で導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI (Open Systems Interconnection) 階層モデル※」で定義される 7 階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平成 19 年 2 月」が参考になる。

#### ※OSI 階層モデル (Open System Interconnection)

開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコル。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択のための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電氣的、物理的に変換。機器の形状・特性を規定している層

例えば、SSL-VPN を用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPSec を用いる場合は、2 階層目もしくは 3 階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE (Internet Key Exchange) といわれる標準的手順を組み合わせる等して、確実にその安全性を確保する必要がある。

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要がある。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。



図 B-2-④ オープンネットワークで接続されている場合

### Ⅲ. モバイル端末等を使って医療機関等の外部から接続する場合

ここでは、携帯電話・PHS や可搬型コンピュータ等の、いわゆるモバイル端末を用いて、医療機関の外部から医療機関内部のネットワークに接続する場合のセキュリティ要件を整理しておく。

外部からの接続については、「6.8 情報システムの改造と保守」で述べた保守用途でのアクセス、医療機関の職員による業務上のアクセス、さらには本章「B-3 患者等に診療情報等を提供する場合のネットワークに関する考え方」で述べる患者等からのアクセス等、さまざまなケースが想定される。

従って、実際の接続において利用されるモバイル端末とネットワークの接続サービス及びそれらの組み合わせが、本章で説明する接続形態のどれに該当するかを明確に識別することが重要になる。

外部から医療機関の内部ネットワークに接続する場合、現状で利用可能な接続形態の俯瞰図を図 B-2-⑤に示す。



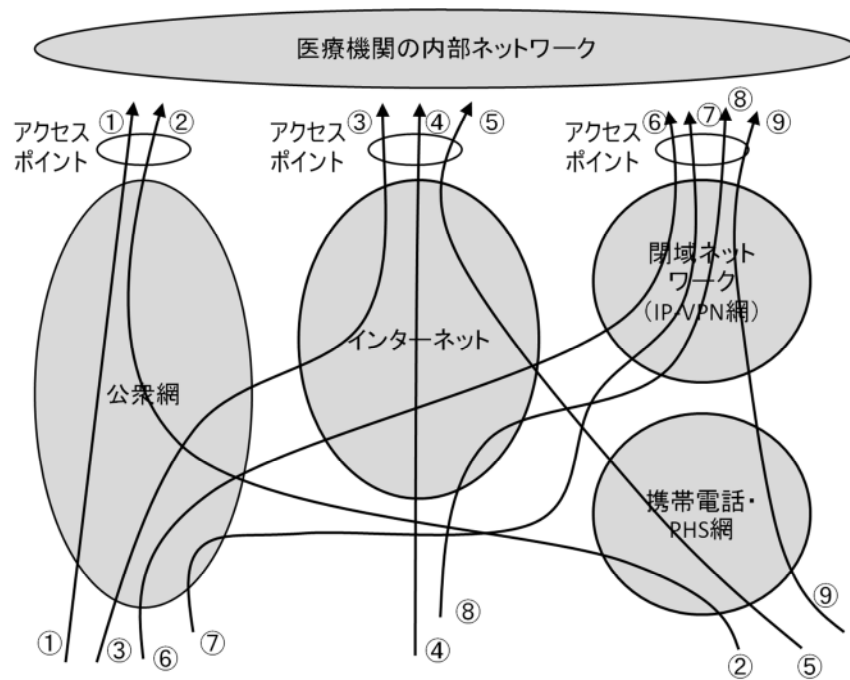


図 B-2-⑤ モバイル環境における接続形態

図 B-2-⑤に示したように、接続形態は下記の3つの系統に類型化できる。(括弧内の丸数字はそれぞれ図 B-2-⑤と対応する)

- 1) 公衆網（電話網）を經由して直接ダイアルアップする場合（①、②）
- 2) インターネットを經由して接続する場合（③、④、⑤）
- 3) 閉域ネットワーク（IP-VPN 網）を經由して接続する場合（⑥、⑦、⑧、⑨）

ここでは、本章の「I. クローズドなネットワークで接続する場合」と「II. オープンなネットワークで接続する場合」で説明したどのケースに該当するかを示し、それぞれのケースにおけるセキュリティ上の留意点をまとめる。

1) 公衆網（電話網）を経由して直接ダイアルアップする場合

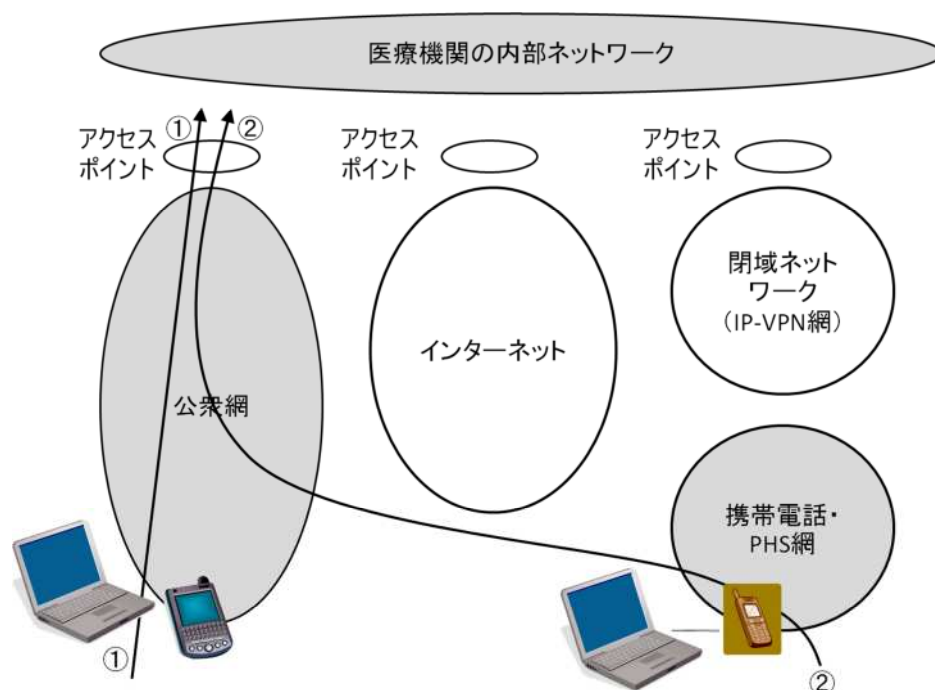


図 B-2-⑥ モバイル環境における接続形態（公衆網経由）

①は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続し、医療機関内に設けられたアクセスポイントに直接ダイアルアップするケースである。

②は①における電話回線の代わりに、携帯電話・PHS やその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS 網に接続ケースである。①と②は携帯電話・PHS 網を経由するかどうかの違いがある。

いずれも「I. クローズドなネットワークで接続する場合」における「②公衆網で接続されている場合」に相当するため、セキュリティ的な要件は、そこでの記述を適用すること。すべてクローズドなネットワークを経由するため、比較的安全性は高い。

## 2) インターネットを経由して接続する場合

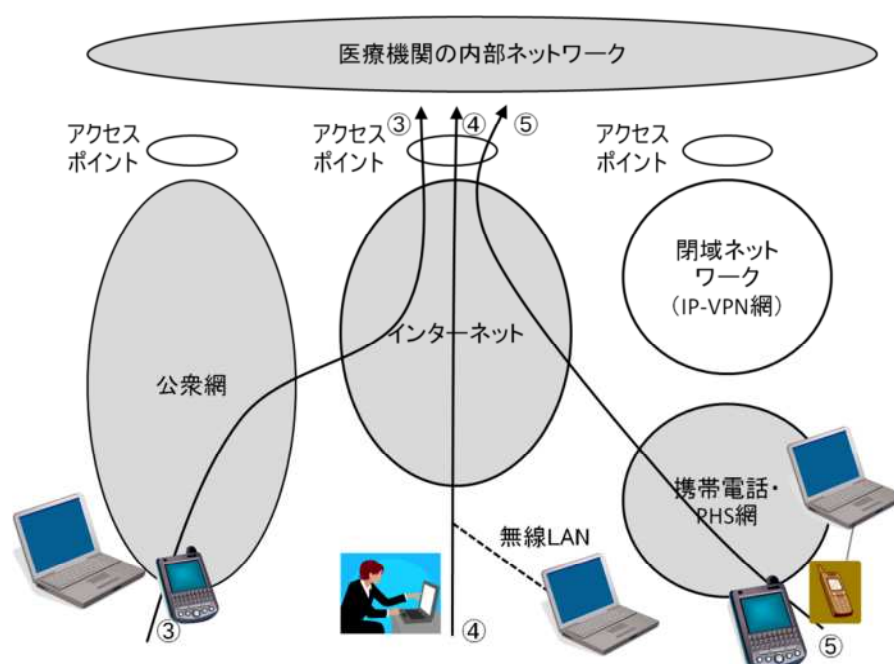


図 B-2-⑦ モバイル環境における接続形態（インターネット経由）

③は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続してインターネットのサービスプロバイダのアクセスポイントにダイヤルアップし、インターネット経由で医療機関のアクセスポイント接続するケースである。

④は③における電話回線の代わりに、自宅やホテル等インターネットへの接続インターフェースのあるところで LAN を使って接続するケースである。LAN として有線の LAN の代わりに無線 LAN を利用するケースもある。いわゆる公衆無線 LAN を利用した接続もこの形態に含まれる。

⑤は携帯電話・PHS 網を経由して、携帯電話・PHS 等のサービス提供会社の提供するサービスを利用してインターネットへ接続するケースである。

③から⑤のいずれのケースも「Ⅱ. オープンなネットワークで接続されている場合」に相当する。従って、セキュリティ的な要件は、そこでの記述を適用すること。オープンなネットワークを経由するので、「B-1 医療機関等における留意事項」で述べたオブジェクト・セキュリティとチャネル・セキュリティを担保するための対策が必要である。

具体的には、モバイル端末として携帯電話・PHS 機や、より高機能な端末装置（いわゆるスマートフォン等）を利用する場合には、その端末で SSL/TLS が利用できるのか、接続経路に IPSec と IKE が適用されているのか、等のサービス内容を確認する必要がある。

なお、これらのケースは、いずれも操作者が自分のモバイル端末を用いて接続することを想定しているが、いわゆるネットカフェ等の備え付けの端末を利用して医療機関内の情報にアクセスするケースも考えられる。このようなアクセス方法はリスクが大きい。

医療機関が組織の方針として、このようなアクセス形態を認めるかどうかについては、慎重な検討が必要である。

### 3) 閉域ネットワークを経由して接続する場合

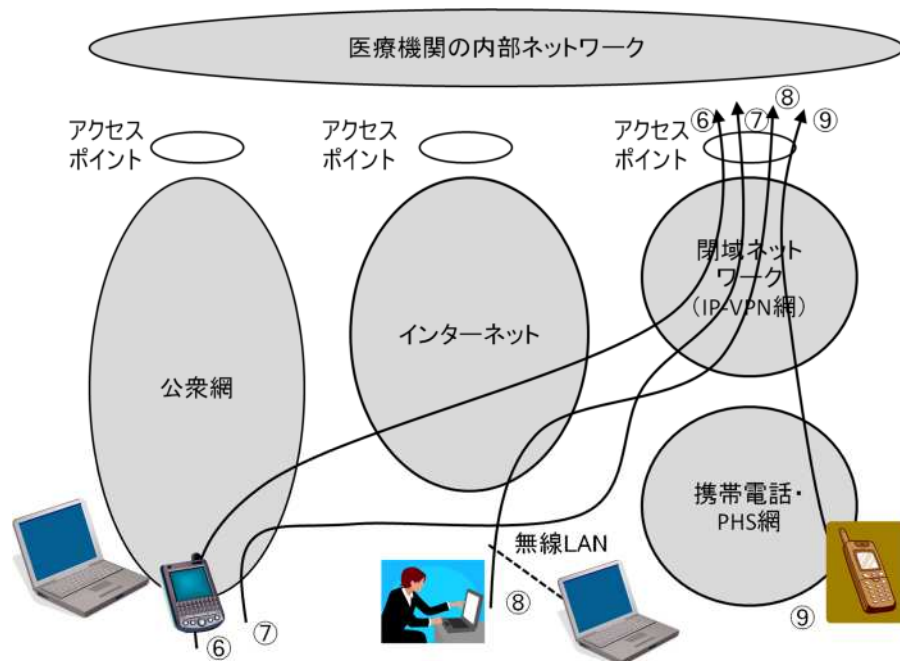


図 B-2-⑧ モバイル環境における接続形態（閉域ネットワーク経由）

⑥と⑦はいずれも自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続して閉域ネットワークのサービスプロバイダのアクセスポイントにダイヤルアップし、閉域ネットワーク経由で医療機関のアクセスポイント接続するケースである。

⑥は⑦とよく似ているが、⑥がダイヤルアップする際に一度オープンなネットワーク（インターネット）を提供するプロバイダを経由するのに対して、⑦では閉域ネットワークを提供するプロバイダに直接ダイヤルアップするという違いがある。

⑧は⑥における電話回線の代わりに、自宅やホテル等インターネットへの接続インターフェースのあるところで LAN を使って接続するケースである。このケースのバリエーションとして、LAN として有線の LAN の代わりに無線 LAN を利用するケースもあり、いわゆる公衆無線 LAN 等もこのケースに含まれる。

⑨は携帯電話・PHS 網を経由して、閉域ネットワークへ接続するケースである。この場合の携帯電話・PHS 網から閉域ネットワークへの接続は、携帯電話・PHS サービス提供会社によって提供されるサービスである。

いずれも「I. クローズドなネットワークで接続する場合」における「③閉域 IP 通信網で接続されている場合」に相当するため、セキュリティ的な要件は、そこでの記述を適用すること。クローズドなネットワークを経由するため、比較的安全性は高い。

ただし、⑥と⑧のケースでは、閉域ネットワークに到達するまでにオープンなネットワーク（インターネット）を経由するため、サービス提供者によってはこの間でのチャンネル・セキュリティが確保されないこともありうる。チャンネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前にサービス提供者との契約をよく確認して、チャンネル・セキュリティが確実に確保されるようにしておく必要がある。

なお、ここで述べたようなモバイル接続形態に関連するセキュリティ要件に加え、医療機関の外部で情報にアクセスするという行為自体に特有のリスクが存在する。

例えば、機密情報が格納されたモバイル端末の盗難や紛失等の管理面のリスク、さらには公共の場所で情報を閲覧することによる他者からの窃視等による機密漏えいのリスク等である。

これについては「6.9 情報及び情報機器の持ち出しについて」に詳細を記述したので、参照すること。

### B-3 従業者による外部からのアクセスに関する考え方

医療機関等の職員がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可することもあり得る。このような場合のネットワークに関わる安全管理の要件はすでに述べたが、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。加えて、外部からのアクセスに用いる機器の安全管理を運用管理規程で定めることは重要ではあるが、考慮すべきことが 3 点ある。

- ① PC 等と言ってもその安全管理対策を確認するためには一定の知識と技能が必要で、職員にその知識と技能を要求することは難しいこと。
- ② 運用管理規程で定めたことが確実に実施されていることを説明するためには適切な運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは通常は困難なこと。
- ③ 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等の管理下にある機器を必要に応じて使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性があること。

従って、通常は行うべきではないが、医師不足等に伴う医療従事者の過剰労働等に対応するために、やむを得ず行う場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術が普及しており、これらの導入を検討することが重要であるとともに、運用等の要件にも相当な厳しさが求められる。

#### **B-4.患者等に診療情報等を提供する場合のネットワークに関する考え方**

診療情報等の開示が進む中、ネットワークを介して患者（または家族等）に診療情報等を提供する、もしくは医療機関内の診療情報等を閲覧させる可能性も出てきた。本ガイドラインは、医療機関等の間における医療情報の交換を想定しているが、患者に対する情報提供も十分想定される状況にある。ここではその際の考え方について触れる。

ここでの考え方の原則は、医療機関等が患者との同意の上で、自ら実施して患者等に情報を提供する場合であり、診療録及び診療諸記録の外部保存を受託する事業者が独自に情報提供を行うことはあってはならない。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、情報を閲覧する患者等のセキュリティ知識と環境に大きな差があるということである。また、一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。しかし、セキュリティ知識に大きな差がある以上、情報を提供する医療機関等が患者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏えい等の事故が起きた場合は、その責任を逃れることはできないことを認識しなくてはならない。

また、今まで述べてきたような専用線等のネットワーク接続形態で患者等に情報を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、提供に用いるネットワークとしては、一般的にはオープンなネットワークを介することになる。この場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

医療機関等における基本的な留意事項は、既に4章やB-1で述べられているが、オープンなネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。特に、患者等に情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。そのため、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いる必要がある。

このように、患者等に情報を提供する場合には、ネットワークのセキュリティ対策のみならず、医療機関等内部の情報システムのセキュリティ対策、情報の主体者となる患者等へ危険性や提供目的の納得できる説明、また非ITに関わる各種の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にした上で実施しなくてはならない。

### **C. 最低限のガイドライン**

1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとること。  
施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止す

る対策をとること。

セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することがあげられる。

チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者を確認すること。

2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。
3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
4. 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し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。
5. 送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
6. 医療機関等との間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。

そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

- ・ 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定
- ・ 送信元の医療機関等がネットワークに接続できない場合の対処
- ・ 送信先の医療機関等がネットワークに接続できなかった場合の対処
- ・ ネットワークの経路途中が不通または著しい遅延の場合の対処
- ・ 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対

処

- ・ 伝送情報の暗号化に不具合があった場合の対処
- ・ 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
- ・ 障害が起こった場合に障害部位を切り分ける責任
- ・ 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

- ・ 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
- ・ 患者等に対する説明責任の明確化。
- ・ 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
- ・ 交換した医療情報等に対する管理責任及び事後責任の明確化。

個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

7. リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。  
また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。
8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記1及び4を満たしていることを確認すること。
9. 患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。  
また、情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、ITに係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。

#### D. 推奨されるガイドライン



1. やむを得ず、従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。