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係わる情報を取扱い、法令上の守秘義務のある者
(b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元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診療を維持するための業務に携わる者
(d) 患者、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洩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」の委託先の機関等に該当するが、これに関しては、その主旨と実施の詳細を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. 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. 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病院事務、運用等で、外部受託業者を採用する場合は、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 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・作業結果の確認をおこなうこと。
   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等の手順を明確化したものを作成しておくべきである。

外部の委託機関等に保存を委託している診療録等について、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、受託先の機関等も、委託元の医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を明確に示す必要がある。

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. 破棄を外部事業者に委託した場合は、「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、さらに委託元の医療機関等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

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、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。

なお、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等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、およ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等の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。

削除: 保守

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ことは避けるべきであるが、やむ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。

6.9 災害等の非常時の対応

B. 考え方

医療機関等は医療情報システムに不具合が発生した場合でも患者安全を配慮した医療サービスの提供が最優先されなければならない。

ここでは、「6.2.3 リスク分析」の「⑥医療情報システム自身」に掲げる自然災害やサイバー攻撃によるＩＴ障害などの非常時に、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留意事項について述べる。

「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、使用環境が非定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合理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。

削除: 医療機関は医療情報システムに不具合が発生した場合でも患者安全を配慮した医療サービスの提供が最優先されなければならない。

(1) 非常時における事業継続計画(BCP : Business Continuity Plan)

異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。異常事態を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などで検証することが望ましい。

医療施設として定められるBCPにおいては、医療情報システムについての計画を含め、全体としての整合性が必要である。

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。

削除: の

削除: 以下

削除: と略す

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「情報セキュリティ」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、連絡手段および対策ツール
- 非常時に公にすべき文書および情報

② BCP 発動フェーズ

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 発動か通常の障

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しスタンドアロンで使用するとか、紙での運用にするとかが考えられる。
業務委託先との間の連絡体制や委託先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」、および「影響度の確認」である。

削除: おこない

削除: おこない

削除: おこなう

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・手作業など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、要員など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」、「代替施設および設備の確保」、「再開／復旧活動の両立」、および「リスク対策のリスク対策」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」および「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「切替の判断」、「復旧手順の再確認」、「確認事項の整備」および「総括」である。

(2) 医療システムの非常時使用への対応

削除: (ブレイクグラス)

① 非常時用ユーザアカウントの用意

削除:

・ 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、定常状態に戻った後は変更し新しい非常時ユーザアカウントへの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、受付での患者登録を経ない診察が行われるため、診療科端末での仮患者登録機能が求められることが考えられ、これを想定した医療情報システムが必要である。

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。
4. 非常時機能が定常時に不適切に利用されないように使用されたことが多くの人に判る管理および監査をすること。
5. 非常時用ユーザアカウントであれば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。
6. サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、あらかじめ定められた所管官庁への連絡を行うこと。

削除: ること。

削除: 非常時のユーザアカウントを用意するなどして、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すること。緊急用ユーザアカウントの配布の例としては、次のようなものが挙げられる。

<#>キャビネットのガラスの後ろに保管
これはパスワードを入手するためには文字通りガラスを壊す必要があり、見た目で分かるだけでなく、不用な使用を防止する。

<#>密封した封筒に保管
封が開いていれば利用されたことがわかる。

<#>特定の人が保管
例えば看護師長、施設警備員が机に施錠して保管する。

２名以上で鍵を管理

削除: る

削除: ブレイクグラス

書式変更: フォント：(特殊) Century

書式変更：箇条書きと段落番号

削除: また、

書式変更: フォント：(特殊) Century

書式変更：箇条書きと段落番号

6.10 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、個人情報保護およ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。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（Application Service Provider）型のサービスを利用する場合等が考えられる。

外部と医療情報を外部ネットワークを利用して交換する場合、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、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。

削除: を

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、医療機関等が法令による義務の有無に関わらず、個人情報を含む医療情報の保存を外部に委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要なため、８章に別途まとめて記述を行う。

B-1. 責任分界点の明確化

医療情報を外部に提供することは個人情報保護法上、委託と第三者提供の２種類があり、遵守すべき事項が異なる。

委託の場合、管理責任は提供元医療機関にあり、契約と監督で管理責任を果たす責務があり、説明責任・結果責任を負わなければならない。提供先機関は契約遵守と報告義務を負う。

削除: 期間

第三者提供の場合、提供元は同法第２３条で規定された例外を除き、厚生労働省個人情報保護ガイドラインのⅢ－５－（３）－①のア～エに相当する場合は同ガイドラインで明記された方法で黙示の同意、それ以外の場合は明示の同意を得なければならない。また提供先は同法第１５条、第１６条にしたがって利用目的を特定し、同法および厚労省ガイドラインにしたがって個人情報保護を達成する責務を負う。これらの要件を満たして提供された情報に対して提供元は責任を負わない。

オンラインで情報を提供する場合、情報主体である患者と情報が乖離する。患者と乖離

している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。また患者にとっての苦情の申し入れ先や開示等の要求先が明白でなければならない。

提供元事業者、オンラインサービス提供事業者、回線提供事業者、提供先機関または提供先になる可能性がある事業者等が関係事業者になりえる。以下の原則で責任分界点を考える必要がある。

まず、提供元事業者と提供先機関は通信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する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供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する必要がある。ただし、前述のように結果責任、説明責任は委託の場合は提供元事業者、第三者提供の場合は提供元事業者または提供先事業者にあり、オンラインサービス提供事業者や回線提供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。

削除: を明らかにする必要がある。

回線事業者の提供する回線の発信元との責任分界点以前に適切に暗号化され、送信先との責任分界点以降に復号される場合は、回線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る。ただし、改ざん、侵入、妨害の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は契約で明らかにすること。

オンラインサービス提供事業者の管理範囲の開始される責任分界点に情報が到達する以前に適切に暗号化され、管理範囲の終了する責任分界点以降に復号される場合は、オンラインサービス提供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る。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲やサービスの可用性等の品質に関しては契約で明らかにすること。

法令で定められている場合などの特別な事情により、オンラインサービス提供事業者および回線提供事業者のいずれかに暗号化されていない医療情報が送信される場合は、オンラインサービスもしくは回線において盗聴の脅威に対する対策を施す必要があるため、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はオンラインサービス提供事業者もしくは回線提供事業者と医療情報の管理責任についての明確化をおこない、オンラインサービス提供事業者もしくは回線提供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。

提供元事業者と提供先事業者が１対１通信である場合、または１対Ｎであってもあらかじめ提供先または提供先となる可能性がある事業者を特定できる場合は委託または第三者提供の要件にしたがって両事業者が責務を果たさなければならない。

提供元事業者と提供先事業者が１対Ｎ通信で、提供先事業者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。

リモートログイン機能を用いたデータアクセスには、代表的用途として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が考えられる。しかし、制限がゆる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。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。

B-2. 医療機関等における留意事項

ここでは「B-1. 責任分界点の明確化」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、適切に送信先の医療機関等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-3. 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。一方、「B-3. 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。一方で、不適切なネットワーク機材の設定により、意図しない情報漏洩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、意図しない情報漏洩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、先に例示した通りであり、情報そのものの暗号化のことを指している。

どの程度の暗号化を施すか、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性の高さ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乖離する段階においては暗号化されていることが望ましい。

さらに、この盗聴防止については、例えばIDとパスワードを用いた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ることも重要な要素である。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-3. 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、情報を暗号化せずに伝送する可能性も否定できず、その場合には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、送信先の医療機関等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医療機関等は、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か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で医療機関等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、送信元の医療機関等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「6.9　災害等の非常時の対応」を参照されたい。

削除: .

B-3. 選択すべきネットワークのセキュリティの考え方

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、同じく医療機関等の情報を受信する機関の外部ネットワーク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、「B-1. 責任分界点の明確化」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洩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度の整理をする必要がある。「B-2. 医療機関等における留意事項」では情報そのものに対する暗号化について触れているが、同様の観点から、情報の機密度に応じてネットワーク種別も選択しなくてはならない。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、機密度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がある。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最終的な結果責任を負うにせよ、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、善良なる管理者として注意義務を払い、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。

削除: 通信事業者
削除: 通信事業者
削除: 通信
削除: ただし
削除: 通信
削除: 定

・ 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、導入され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発信端末、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担保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。

削除:

削除: 通信事業者

削除: 通信

削除: 事業者

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。

削除: ただし、

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。

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-2. 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ウイルス定義ファイルや 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。