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。
9. 持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなソフトウェアをインストールしないこと。
10. 個人保有の情報機器（パソコン等）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て用いること。
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。

削除: および

削除: および

削除: など

削除: 取り扱ったり、医療機関等のシステムへアクセスするような

6.10 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に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「②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(BCP : Business Continuity Plan)

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。

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。

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

削除: な

削除: など

削除: など

削除: および

削除: および

害対策の判断を行い、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を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ていること。
具体的項目は、「基本方針の確定」、「発生事象の確認」、「安全確保・安否確認」と、「影響度の確認」である。

② 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・手作業へ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・設備の確保」、「再開／復旧活動の両立」と、「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。

③ 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」と、「制限の確認」である。

④ 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」と、「総括」である。

⑤ 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。

削除: および
削除: なら
削除: および
削除: および
削除: および
削除: および

(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上の用意
- 停電、火災、漏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。医療情報システムでは使用可能であること、使用者側の事情で通常時とは著しく違い、正規のアクセス権者による操作が望ましく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、主に用意し、患者データへのアクセス制限や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用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、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。

削除: なし

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、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、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。

削除: および
削除: など
削除: 別途定める

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

ここでは第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

削除: および

削除: （Application Service Provider）

削除: 場合

削除: および

削除: ネットワークに対する

削除: および

削除: など

削除: 医療

削除: 等

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ンネル・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

削除: チャンネル

削除: て、不適切な

削除: 通りであり、

削除: のことを指している。すなわち

削除: 考え方が必要となる

削除: 程度の

削除: 機密性の高さ

削除: ID とパスワードを用いた

削除: ②

削除: 伝えることも重要な要素である

リティの考え方」のネットワークの構成によっては、[illegible]に[illegible]場合、[illegible]改ざんに対する対処は確実に実施しておく必要がある。[illegible]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

ネットワークを通して情報を伝達する場合、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、送られてき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、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[illegible]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[illegible]・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[illegible]や、業務の必要性[illegible]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、第4章「電子的な医療情報を扱う際の責任のあり方 1.2 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度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、[illegible]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、医療機関等となるか、また、どこまで負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[illegible]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[illegible]ネットワーク経路上のセキュリティを[illegible]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して交換しようとする場

削除: 情報を暗号化せず
削除: 信頼する可能性も高まります。そ
削除: ため
削除: 医療
削除: 等
削除: 医療
削除: 等
削除: 医療
削除: 等
削除: の医療機関等
削除: ネットワーク
削除: 同じ医療機関等の
削除: や
削除: 「B-1. 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。
削除: された
削除: 発信
削除: や
削除: 担保

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．

削除: ，および

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．

削除: ウイルス

削除: セキュリティパッチ

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と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）やダイアルアップ接続など、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、接続先に直接ダイア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で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を送信する場合には適用範囲を適切に見定める必要がある．

削除: など

削除: 接続先

削除: を

削除: する際に

図 B-2-② 公衆網で接続されている場合

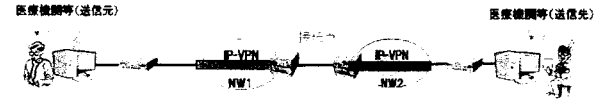
③閉域 IP 通信網で接続されている場合

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、遠隔地を含めた企業内LANのように利用され、責任主体間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も可能である。

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　中間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[illegible]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場合がある。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か、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も、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などの措置を取る必要がある。

削除: など

削除: など

Ⅱ．オープンなネットワークで接続されている場合

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など、その利用範囲を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要である。また、医療情報システムの安全化の対策を取らなければならないことはもちろん、オブジェクト・セキュリティの考え方に基づいた対策を施す必要がある。

さらに、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切断に関係する層
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	ビットデータを電気的、物理的に変換、機械の形状・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。

削除：「6.9　情報および情報機器の持ち出しについて」で述べた

削除：（テレワーク）

削除：など

削除：、および

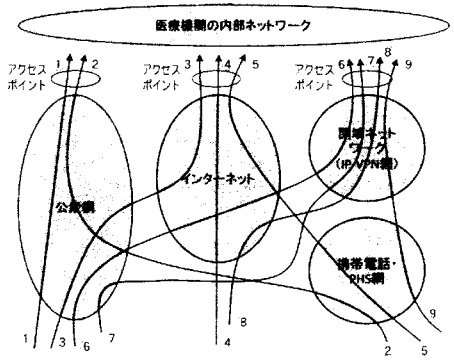


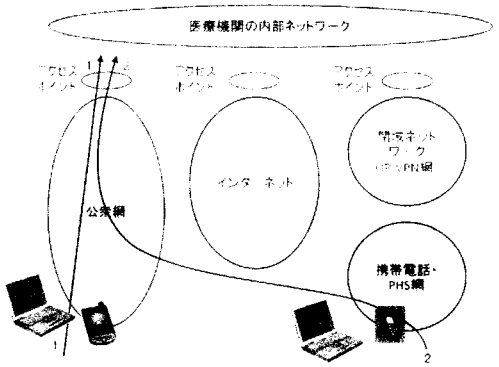
図 B-2-⑤　モバイル環境における接続形態

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）を経由して直接ダイアルアップする場合（①、②）
2）インターネットを経由して接続する場合（③、④、⑤）
3）閉域ネットワーク（IP-VPN網）を経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。

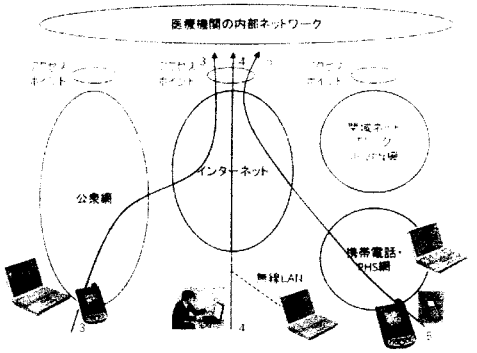
②は①における電話回線の代わりに、携帯電話・PHSやその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS網に接続ケースである。①と②は携帯電話・PHS網を経由するかどうかの違いがある。

いずれも「1．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。すべてクローズなネットワークを経由するため、比較的安全性は高い。

削除: など

削除: など

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アルアップし、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。

削除: など

削除: な

削除: 「8章　情報および情報機器の持ち出しについて」の記述からもわかるように

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

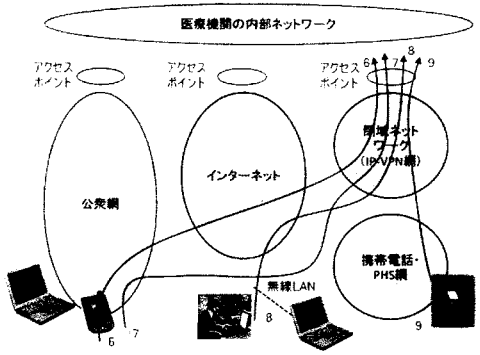


図 B-2-⑧　モバイル環境における接続形態（閉域ネットワーク経由）

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アルアップし、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がダイア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ア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「1．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。クローズなネットワークを経由するため、比較的安全性は高い。

削除: など

削除: など

削除: など

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ネル・セキュリティが確保されないこともありうる。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、事前にサービス提供者との契約をよく確認して、チャネル・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覗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　情報と、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。

削除: など

削除: などである

削除: および

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、PCを含めて自宅等から、病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する安全管理の要件は、すでに述べてきたが、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など、非管理端末であること、一定の安全管理が可能な技術的対策を講じられたものでないこと、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、考慮すべきことがいくつかある。

1．PC等、自己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など、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て、不具合があること。

従って、通常は行うべきではないが、医療従事者の過剰な労働や医師の過疎等に対応するためには、それを許す場合、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の普及しており、これらの導入を検討することが重要であると共に、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

診療情報等の開示の進む中、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ケースや医療機関内の診療情報等を閲覧でき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、診療情報のやりとりを想定しているが、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、その際の考え方について触れる。

基本的な考え方の原則は、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を外部保存を受託する事業者から直接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だけで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、一般的にはインターネット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、既に第4章やB-1で述べられているが、インターネットに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 に関す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、ウイルス混入など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 アドレス詐称など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。
   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に確認すること。
2. データ送信元と送信先での、機器の出入口・使用機器・使用機器上の機能単位・利用者などの必要な単位で、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 4.5 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. ルータなど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など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など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など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必要な動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。

削除: および

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 章　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。

削除: および

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

6.12 法令で定められた記名・押印を電子署名で行うことについて

A. 制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

（「電子署名及び認証業務に関する法律」　第2条1項）

B. 考え方

平成11年4月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」においては、法令で署名または記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていた。

削除: 平成１２年法律第１０２号

しかし、平成12年5月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書等として、「民間事業者が行う書面の保存等における情報通信の技術の利用に関する法律に基づく厚生労働省令」において指定された文書等においては、「A. 制度上の要求事項」に示した電子署名によって、記名・押印にかわり電子署名を施すことで、作成・保存が可能となった。

ただし、医療に係る文書等では一定期間、署名を信頼性を持って検証できることが必要である。電子署名は紙媒体への署名や記名・押印と異なり、「A. 制度上の要求事項」の一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が[illegible]

[illegible]

削除: 過ぎた場合は検証ができないという特徴がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある

[illegible]

C. 最低限のガイドライン

法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。

(1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

1. 保健医療福祉分野 PKI 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用するのが望ましい。
   ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。
2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件を満たすことは可能であるが、[illegible]の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。
3. 「電子署名に係る地方公共団体の認証業務に関する法律」（平成[illegible]法律[illegible]）に基づき、平成16年1月29日から開始されている公的個人認証サービスを

削除: [illegible]同様

削除: １４年

削除: 第１５３号

用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。

(2) 電子署名を含む文書全体にタイムスタンプを付与すること。

1. タイムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成16年11月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能である事.
2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること.
3. タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。

(3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いること。

1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値と共に署名の全体に対してタイムスタンプを付与する等の対策が必要である。

7 電子保存の要求事項について

[illegible]

7.1 真正性の確保について

A. 制度上の要求事項

電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。

（厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令、第４条第４項第二号、平成17年3月25日）

B. 真正性の確保

電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。

（1） 故意または過失による虚偽入力、書換え、消去及び混同を防止すること。

（2） 作成の責任の所在を明確にすること

（施行通知 第２ 第３ ２(2)）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知 第２ １ (1)）

削除: 保存義務のある情報の真正性が確保されていること。

削除: （厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令 第４条第４項第二号）。

削除: 第２

削除: １

B. 考え方

真正性とは、正当な[redacted]されたことに対し、虚偽入力、書き換え、消去、及び混同が防止されて[redacted]ことである。なお、混同とは、患者を取り違えた記録がされたり、記録された情報間での関連性を誤ったりすることをいう。

[redacted]、ネットワークを通じて外部に保存を行う場合、[redacted]の外部保存[redacted]の転送途中で、診療録等が[redacted]されないように[redacted]注意する必要がある。

従って、ネットワークを通じて医療機関の外部に保存する場合は、医療機関等に保存する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。

B-1. 虚偽入力、書き換え、消去及び混同を防止すること

保存義務のある[redacted]の電子保存に際して、電子保存を実施するシステム管理者は、正当な手続きを経ずに、[redacted]電子的な[redacted]が誤入力、書き換え・消去及び混同されたりすることを防止する対策を講じる必要がある。また、作成責任者（情報を作成、書き換え、消去しようとする者）は、情報の保存を行う前に情報が正しく入力されており、過失による書き換え・消去及び混同がないことを確認する義務がある。

故意または過失による虚偽入力、書き換え、消去及び混同に関しては、入力者[redacted]の操作者の故意[redacted]過失、起因するものと、使用する機器、ソフトウェアに起因するものの２つに分けることができる。

前者は、例えば、入力者が故意に診療録等の情報を改ざんする場合、あるいは、入力ミス等の過失により誤った情報が入力されてしまう場合等が考えられる。

後者は、例えば、入力者は正しく情報を操作しているが、使用している機器やソフトウェアの誤動作やバグ等により、入力者の入力した情報が正しくシステムに保存されない場合等が考えられる。

これらの虚偽入力、書き換え、消去及び混同の防止は、技術的な対策だけで防止することが困難なため、運用的な対策も含めて防止策を検討する必要がある。

(1) 故意または過失による虚偽入力、書き換え、消去及び混同の防止

故意による虚偽入力、書き換え、消去及び混同はそもそも違法行為であるが、それを防止するためには、以下が守られなければならない。

1. 情報の作成責任者が明確で、いつでも確認できること。
2. 作成責任者の識別・認証を確実に行うこと。すなわち、なりすまし等が行えないような運用操作環境を整備すること。

削除: 上の記録と確認

削除: 情報に関し責任者の果たすべき作成責任者の所在が明確であり、かつ、故意又は過失

削除: また

削除: いる

削除: 制度上の要求事項に対する対応は運用面と技術面の両方で行う必要がある。運用面、技術面どちらかに偏重すると高コストの割に要求事項が充分満たされない事が想定され、両者のバランスを取れた総合的な対策が重要と考えられる。各医療機関等は、自らの機関の規模や各部門システム、既存システムの特性を良く見極めた上で、最も効果的に要求を満たす運用面と技術面の対応を検討されたい。

一方、

削除: 第三者が診療録等

削除: を受託する事業者になりすまして、不正な診療録等を医療機関等

削除: 転送することは、診療録等の改ざんとなる。また、ネットワーク

削除: 改ざん

削除: 故意または過失による

削除: 情報

削除: その内容

削除: 改ざん、消去されたり、過失による

削除: その

削除: に

削除: 何らかの理由により

3. [redacted]を[redacted]すること
4. [redacted]作業[redacted]こと
5. 作成責任者が行った操作に関して、いつ、誰が、どこで、どの情報に対して、どのような操作を行ったのかが記録され、必要に応じて、操作記録に対して適正な利用であることが監査されること
6. 確定され保存された情報は、運用管理規程で定めた保存期間内は履歴を残さないで改変、消去ができないようにすること
7. システムの改造や保守等で診療録等にアクセスされる可能性がある場合には、真正性確保に留意し、「6.8 情報システムの改造と保守」に記載された手続きに従う必要がある。

過失による虚偽入力、書き換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じる。誤入力等を問題ないレベルにまで低減する技術的方法は存在しない[redacted]と、[redacted]

[redacted]

(2) 使用する機器、ソフトウェアに起因する虚偽入力、書き換え、消去及び混同の防止

使用する機器、ソフトウェアに起因する虚偽入力、書き換え、消去及び混同とは、作成責任者が正当に入力したにもかかわらず、利用しているシステム自体に起因する問題により、結果が作成責任者の意図したものと異なる状況となるリスクを指す。このような状況が発生する原因として下記のケース等が考えられる。

1. システムを構成する機器、ソフトウェア自体に問題がある場合（故障、熱暴走、[redacted]、バージョン下整合等）
2. 機器、ソフトウェアに問題はないが、正しく設定されていないために所定の機能動作をしない状態になっている場合
3. 正当な機器、ソフトウェアが悪意ある第三者により別のものに置き換えられている場合

[redacted]

これらの脅威は[redacted]を[redacted]とともに、システムの維持と管理を適切に行うことで防止できると考えられ、医療機関等自らがシステムの品質管理を率先して行う姿勢が重要である。具体的な方策については、C及びDの記述を参照すること。

削除: 作成責任者が行う作業について手順書

削除: 作成

削除: 手順書

削除: 果たす作業の実施する

削除: 、

削除: 点検・規則等で定められた保存期間に基づいて

削除: 従って、

削除: 言える

削除: そのため、入力ミス等はどう発生するとの認識のもと、運用上の対策と技術的対策の両面から誤入力等を防止する対策を講じることが求められる。例えば、情報の確定を行う前に十分に内容の確認を行うことを運用管理規程に定める、あるいは、ヒヤリ・ハット事例をもとに誤入力の発生しやすい個所を色分け表示する等のシステム的対策を施すことが望ましい。

削除: ソフトウェア

削除: （

削除: ）

削除: 保存された情報

削除: 保護する

削除: 維持