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

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

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。 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。 **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	（新設）

削除: 通信事業者

削除: 通信

削除: 事業者

削除: ただし、

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。

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。

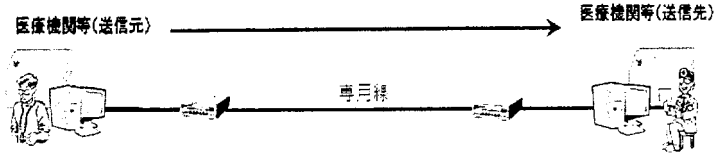


図 B-3-① 専用線で接続されている場合

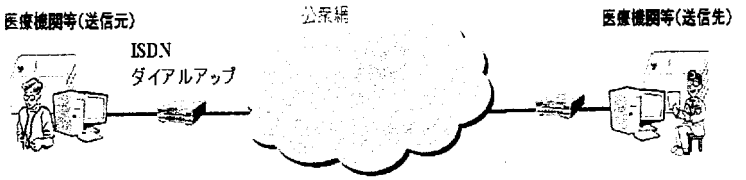
②公衆網で接続されている場合

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先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際に適用範囲を適切に見定める必要がある。



図B-3-②　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。

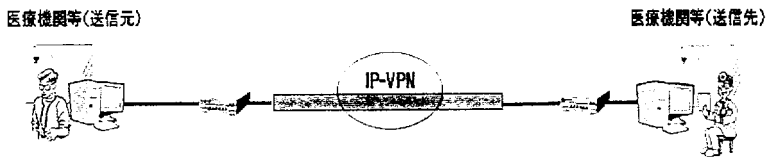


図 B-3-③-a　単一の通信事業者が提供する閉域ネットワークで接続されている場合

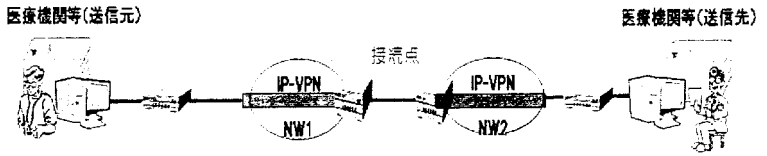


図 B-3-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

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

削除: を利用する接続方式で、

削除: 総称される。

削除: に

削除: ることが多い

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。しかし、接続サービスだけでは一般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。また異なる通信事業者の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など、一般に責任分解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。

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-2. 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。

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。ただし、B-3 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

（新設）

削除: うる

削除: する

削除: ことが望ましい

削除: あらゆる

削除: していることを強く認識する必要がある

削除: しかし、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、医療機関等の自己責任において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「医療情報システムに関する安全基準のガイドラインの実装事例に関する報告書（案）（HEASNET 協議会；平成19年　月）」が参考になる。

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。

削除: この接続方式を安易に導入すると、医療情報が様々な脅威にさらされる危険性をはらむ。
そのため、オープンなネットワークを用いようとする場合は「B-1. 責任分界点の明確化」、「B-2. 医療機関等における留意点」、ネットワーク経路上の責任分界点の考え方、接続されるコンピュータの技術的

----------改ページ----------

安全管理等の全ての観点を満たしつつ、情報そのものの暗号化はもとより、通信網においても最新のセキュリティ技術を組み合わせる等の対策を取らなければならない。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。

図 B-3-④　オープンネットワークで接続されている場合

（患者等に診療情報等を提供する場合）

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する可能性も出てきた。本ガイドラインは、医療機関等間における情報のやり取りを想定しているが、今後、このような事例も十分想定される。そのため、ここでその際の考え方について触れる。ただし、ここで触れる考え方は、医療機関等が自ら実施して患者等に情報を提供する場合であり、第８章で定める診療録及び診療諸記録を外部に保存している場合は、第三者に委託しており、委託先が情報提供を行うことになるため想定しない。

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洩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オープンネッ

削除:

削除: 移る

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 B-1 や B-2 で述べられているが、オープン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 に係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。

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などの容易に解読されない方法を用いるのが望ましい。

（新設）

削除: ハッカー

削除: たとえば

削除: 規定

3. 施設内において、正規利用者への成りすまし、許可機器への成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、IS015408 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. 医療機関間の情報通信には、当該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係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

削除: 若

削除: ていること。

削除: インターネットなどの専用線方式以外の接続の場合には、中継サーバが介在することがあり、中継サーバによる蓄積、転送が入る可能性がある。この中継点での盗聴、改ざんを防止するため、

・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結果責任の明確化。
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章　情報システムの改造と保守」

削除: 規定

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および4を満たしていることを確認すること。	

削除:

改正案	現　行
7　電子保存の要求事項について	7　電子保存の要求事項について
7.1　真正性の確保について	7.1　真正性の確保について
A. 制度上の要求事項	A. 制度上の要求事項
保存義務のある情報の真正性が確保されていること。 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）	保存義務のある情報の真正性が確保されていること。 ○　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。 ○　作成の責任の所在を明確にすること。 （施行通知　第二　２（３）②）
（略）	（略）
7.2　見読性の確保について	7.2　見読性の確保について
A. 制度上の要求事項	A. 制度上の要求事項
保存義務のある情報の見読性が確保されていること。 必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 （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項第一号）	保存義務のある情報の見読性が確保されていること。 ○　情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。 ○　情報の内容を必要に応じて直ちに書面に表示できること。 （施行通知　第二　２（３）①）
（略）	（略）

7.3　保存性の確保について

A. 制度上の要求事項

保存義務のある情報の保存性が確保されていること。
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いて復元可能な状態で保存することができる措置を講じていること。
（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項第三号）

（略）

7.4　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

（略）

C. 最低限のガイドライン

（１）（略）

（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。
１～２（略）

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）（略）

7.3　保存性の確保について

A. 制度上の要求事項

保存義務のある情報の保存性が確保されていること。
○　法令に定める保存期間内、復元可能な状態で保存すること。
（施行通知　第二　２（３）③）

（略）

7.4　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

（略）

C. 最低限のガイドライン

（１）（略）

（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。
１～２（略）

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に留意しながら適切に対策を講じる必要がある。

（３）（略）

改正案	現　行
8.1.1　電子保存の 3 基準の遵守 （略） C．最低限のガイドライン (1)　電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保 ①～②（略） ③　　リモートログイン制限機能を制限すること 保守目的等のどうしても必要な場合を除き、リモートログインが行なえないように適切に管理されたリモートログインのみに制限する機能を設けなければならない。 なお、これらの具体的要件については、「6.10　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-2．医療機関等における留意事項」を参照されたい。 (2) ～ (3)（略） 8.1.3　個人情報の保護 （略） B．考え方 個人情報保護法が成立し、医療分野においても「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」が策定された。医療	8.1.1　電子保存の 3 基準の遵守 （略） C．最低限のガイドライン (1)　電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保 ①～②（略） ③　　リモートログイン制限機能を制限すること 保守目的等のどうしても必要な場合を除き、リモートログインが行なえないように適切に管理されたリモートログインのみに制限する機能を設けなければならない。 (2) ～ (3)（略） 8.1.3　個人情報の保護 （略） B．考え方 個人情報保護法が成立し、医療分野においても「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」が策定された。医療

において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイドラインを参照し、十分な安全管理策を実施することが必要である。 診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、電気通信回線を通じて外部に保存する場合、委託元の医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶために、より一層の個人情報保護に配慮が必要である。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存の受託先機関との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。 電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては「6.10章　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-3. 選択すべきネットワークのセキュリティの考え方」でも触れた通り、専用線等であっても十分な注意を払う必要がある。従って、電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。	において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイドラインを参照し、十分な安全管理策を実施することが必要である。 診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、電気通信回線を通じて外部に保存する場合、委託元の医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶために、より一層の個人情報保護に配慮が必要である。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存の受託先機関との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。 電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。従って、電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。
C．最低限のガイドライン **（1）診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護** ①（略） **②　通信の起点・終点識別のための認証をおこなうこと** 外部保存を委託する医療機関等と受託する機関間の起点・終点の正当性を識別するために相互に認証を行うこと。 通信手段によって、起点・終点の識別方法は異なる。例えば、インターネットを用いる場合は起点・終点の識別はIPパケットを見るだけで	**C．最低限のガイドライン** **（1）診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護** ①（略） **②　通信の起点・終点識別のための認証をおこなうこと** 外部保存を委託する医療機関等と受託する機関間の起点・終点の正当性を識別するために相互に認証を行うこと。 通信手段によって、起点・終点の識別方法は異なる。例えば、インターネットを用いる場合は起点・終点の識別はIPパケットを見るだけで

削除: [

削除:]

は確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の医療機関等と受託先の機関を確実に相互に認証しなければならない。例えば、認証付きの VPN、SSL/TLS や ISCL を適切に利用することにより実現できる。

当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。

なお、情報の暗号化、ネットワーク回線における留意事項等の具体的要件については、「6.10　外部と診療情報等を含む医療情報を交換する場合の安全管理」の「B-2. 医療機関等における留意事項」および「B-3. 選択すべきネットワークのセキュリティの考え方」を参照されたい。

（2）～（3）（略）

8.1.4　責任の明確化

（略）

B．考え方

診療録等を電気通信回線等を通じて外部に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は、保存義務のある医療機関等にある。

ただし、管理責任や説明責任は、実際の管理や説明の一部について、受託先の機関やネットワーク管理者、機器やソフトウェアの製造業者と責任を分担することができ、この場合、一般にネットワークで結合されたシステムでは管理境界や責任限界が自明でない場合が多いことから、文書等により、その責任分担を明確にしなければならない。

結果責任は、患者に対しては委託元の医療機関等が負うが、受託先の機関やこれらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの

は確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の医療機関等と受託先の機関を確実に相互に認証しなければならない。例えば、認証付きの VPN、SSL/TLS や ISCL を適切に利用することにより実現できる。

なお、当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。

（2）～（3）（略）

8.1.4　責任の明確化

（略）

B．考え方

診療録等を電気通信回線等を通じて外部に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は、保存義務のある医療機関等にある。

ただし、管理責任や説明責任は、実際の管理や説明の一部について、受託先の機関やネットワーク管理者、機器やソフトウェアの製造業者と責任を分担することができ、この場合、一般にネットワークで結合されたシステムでは管理境界や責任限界が自明でない場合が多いことから、文書等により、その責任分担を明確にしなければならない。

結果責任は、患者に対しては委託元の医療機関等が負うが、受託先の機関やこれらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの

製造業者は、委託元の医療機関等に対して契約等で定められた責任を負うことは当然であり、法令に違反した場合はその責任も負うことになる。 　なお、これら責任分界点の考え方については、「6.10　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-1. 責任分界点の明確化」も併せて参照されたい。	製造業者は、委託元の医療機関等に対して契約等で定められた責任を負うことは当然であり、法令に違反した場合はその責任も負うことになる。
（略）	（略）

改正案	現　行
10.　運用管理について （略） **B. 考え方** 運用管理規程には、システムの導入に際して、「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基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。 医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の６章から９章の記載に従い、定めるべき管理項目を記載してある。(1) に電子保存する・しないに拘らず必要な一般管理事項を、(2) に電子保存の為の運用管理事項を、(3) に外部保存のための運用管理事項を、(4) にスキャナ等を利用した電子化、そして終わりに運用管理規程の作成にあたっての手順を記載している。 電子保存を行う医療機関等は (1) (2) (4) の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに (3) の管理事項を合わせて採用する必要がある。 **C. 最低限のガイドライン** 以下の項目を運用管理規程に含めること。本指針の６章から９章において「推奨」に記されている項目は省略しても差し支えない。 **(1) 一般管理事項** ①　(略)	**10.　運用管理について** （略） **B. 考え方** 運用管理規程には、システムの導入に際して、「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基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。 医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の６章から９章の記載に従い、定めるべき管理項目を記載してある。(1) に電子保存する・しないに拘らず必要な一般管理事項を、(2) に電子保存の為の運用管理事項を、(3) に外部保存のための運用管理事項を、そして終わりに運用管理規程の作成にあたっての手順を記載している。 電子保存を行う医療機関等は (1) (2) の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに (3) の管理事項を合わせて採用する必要がある。 **C. 最低限のガイドライン** 以下の項目を運用管理規程に含めること。本指針の６章から９章において「推奨」に記されている項目は省略しても差し支えない。 **(1) 一般管理事項** ①　(略)

② 管理体制 a) システム管理者、機器管理者、運用責任者の任命 b) 作業担当者の限定 c) マニュアル・契約書等の文書の管理 d) 監査体制と監査責任者の任命 e) 苦情の受け付け窓口の設置 f) 事故対策 g) 利用者への周知法	② 管理体制 a) システム管理者、運用責任者の任命 b) 作業担当者の限定 c) マニュアル・契約書等の文書の管理 d) 監査体制と監査責任者の任命 e) 苦情の受け付け窓口の設置 f) 事故対策 g) 利用者への周知法
③ 管理者及び利用者の責務 a) システム管理者や機器管理者、運用責任者の責務 b) 監査責任者の責務 c) 利用者の責務	③ 管理者及び利用者の責務 a) システム管理者や運用責任者の責務 b) 監査責任者の責務 c) 利用者の責務
④ 一般管理における運用管理事項 a) 来訪者の記録・識別、入退の制限等の入退管理 b) 情報保存装置、アクセス機器の設置区画の管理・監視 c) 委託契約における安全管理に関する条項 d) 個人情報の記録媒体の管理（保管・授受等） e) 個人情報を含む媒体の廃棄の規程 f) リスクに対する予防、発生時の対応 g) 情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理利用者識別と認証、アクセス権限管理、アクセスログ取得と監査、時刻同期、ウイルス等不正ソフト対策	④ 一般管理における運用管理事項 a) 来訪者の記録・識別、入退の制限等の入退管理 b) 情報システムへのアクセス制限、記録、点検等のアクセス管理 c) 委託契約における安全管理に関する条項 d) 個人情報の記録媒体の管理（保管・授受等） e) 個人情報を含む媒体の廃棄の規程 f) リスクに対する予防、発生時の対応 （新設）
⑤ 教育と訓練 a) マニュアルの整備 b) 定期または不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修	⑤ 教育と訓練 a) マニュアルの整備 b) 定期または不定期なシステムの取扱い及びプライバシー保護に関する研修

c) 従業者に対する人的安全管理措置 ・ 医療従事者以外との守秘契約 ・ 従事者退職後の個人情報保護規程	c) 従業者に対する人的安全管理措置 ・ 医療従事者以外との守秘契約 ・ 従事者退職後の個人情報保護規程
⑥ （略）	⑥ （略）
⑦ 監査 a) 監査の内容 b) 監査責任者の任務 c) アクセスログの監査	⑦ 監査 a) 監査の内容 b) 監査責任者の任務
⑧ 災害等の非常時の対応 a) BCP の規程における医療情報システムの項 b) システムの縮退運用規程 c) 非常時の機能と運用規程 d) 報告先と内容一覧	（新設）
⑨ 外部と医療情報を交換する場合 a) 安全を技術的、運用的面から確認した文書の管理 b) リスク対策の検討文書の管理 c) 責任分界点を定めた契約文書の管理 d) リモートメンテナンスの基本方針	（新設）
⑩ 規程の見直し 運用管理規程の定期的見直し手順	（新設）
(2) 電子保存の為の運用管理事項 ①～④ （略）	(2) 電子保存の為の運用管理事項 ①～④ （略）
((4) へ)	⑤ スキャナ読み取り書類の運用

削除: 規定

削除: 規定

削除: 規定

削除: 保守

削除: へ

削除: 規定

削除: 規定

	a) スキャナ読み取り電子情報と元の文書等との同一性を担保する情報作成管理者の任命 スキャナ読み取り電子情報への作業責任者(実施者または管理者)の電子署名法に適合した電子署名 b) スキャナ読み取り電子情報への正確性な読みとり時刻の付加
(3) (略)	(3) (略)
(4) スキャナ等により電子化して保存する場合	(新設)
① スキャナ読み取りの対象文書の規程	((2)⑤から)
② スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	((2)⑤a) から)
③ スキャナ読み取り電子情報への作業責任者(実施者または管理者)の電子署名及び認証業務に関する法律(電子署名法)に適合した電子署名	((2)⑤a) から)
④ スキャナ読み取り電子情報への正確な読みとり時刻の付加	((2)⑤b) から)
⑤ 過去に蓄積された文書を電子化する場合の、実施手順規程	(新設)
(略)	(略)

削除: 性