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

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を利用する接続方式で、IP-VPN（Internet Protocol-Virtual Private Network）と総称される。主に、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。

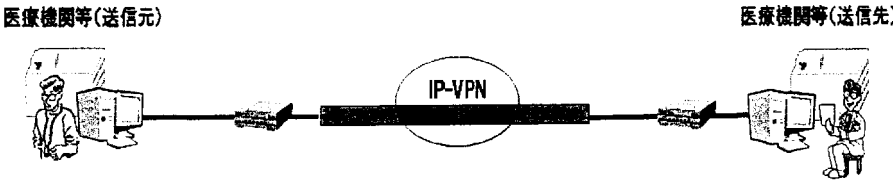

図 B-3-③-a　単一の通信事業者が提供する閉域ネットワークで接続されている場合

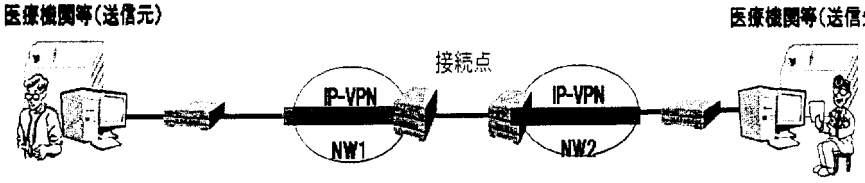

図 B-3-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

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うる。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する、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ことが望ましい。

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。この場合、「盗聴」、「侵入」、「改ざん」、「妨害」等のあらゆる脅威が存在していることを強く認識する必要がある。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。一方で、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

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。

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

（新設）

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-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、患者等に移る。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ハッカーによるパスワード盗聴、本文の

（新設）

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、たとえば、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定により、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。

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、ISO15408 で規定されるセキュリティターゲット若しくはそれに類するセキュリティ対策が規定されていること。

5. 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
- 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定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	