

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。

- ・ 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。

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、およ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。

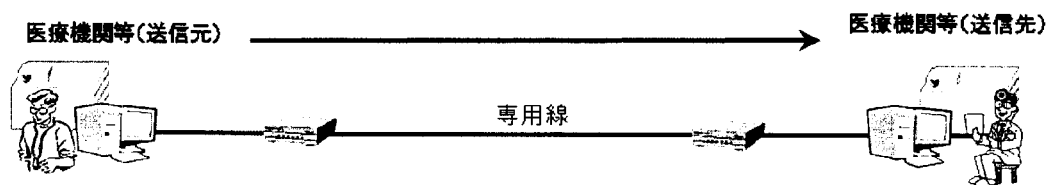


図 B-2-① 専用線で接続されている場合

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。

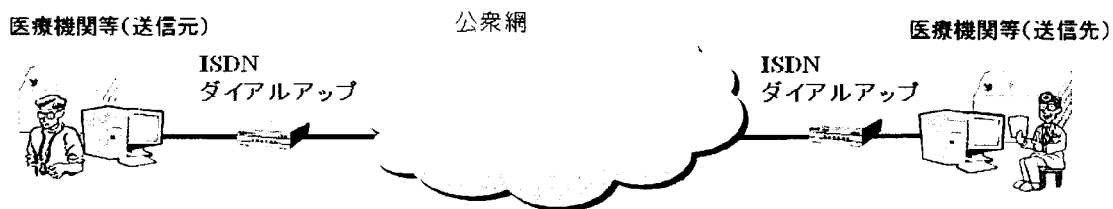


図 B-2-② 公衆網で接続されている場合

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。

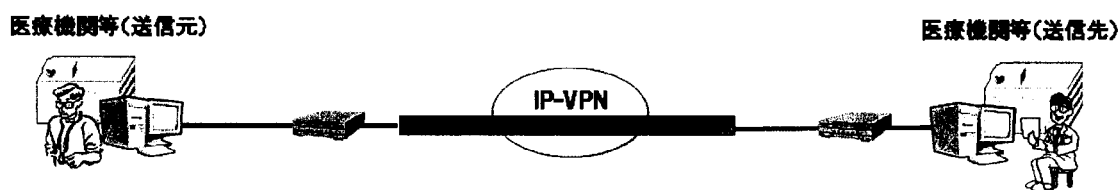


図 B-2-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

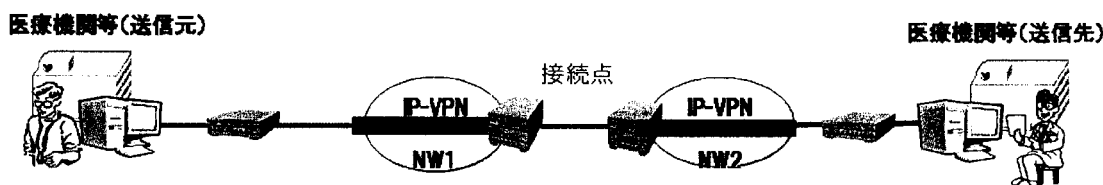


図 B-2-③-b 途中で複数の閉域ネットワークが相互接続して接続されている場合

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など、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。

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 Interconneciton)

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ール。

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ですが、経路を暗号化するための暗号鍵の取り交しにIKE (Internet Key Exchange) といわれる標準の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。

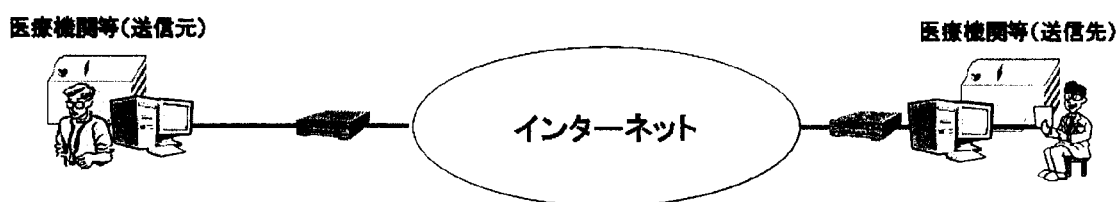


図 B-2-④ オープンネットワークで接続されている場合

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、「6.9 情報および情報機器の持ち出しについて」で述べた医療機関の職員による業務上のアクセス (テレワーク)、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など、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、およ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。

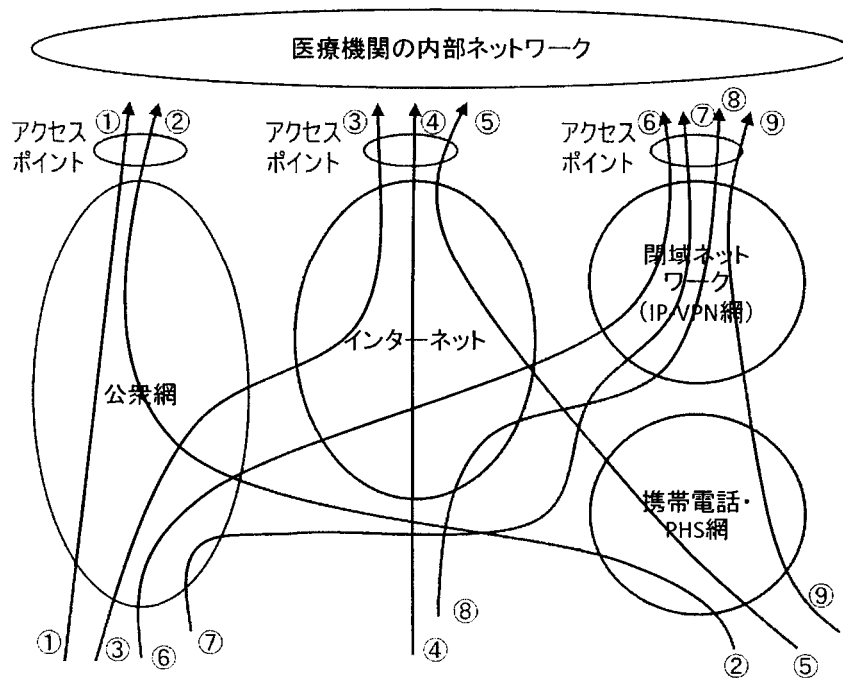


図 B-2-⑤ モバイル環境における接続形態

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）を經由して直接ダイアルアップする場合

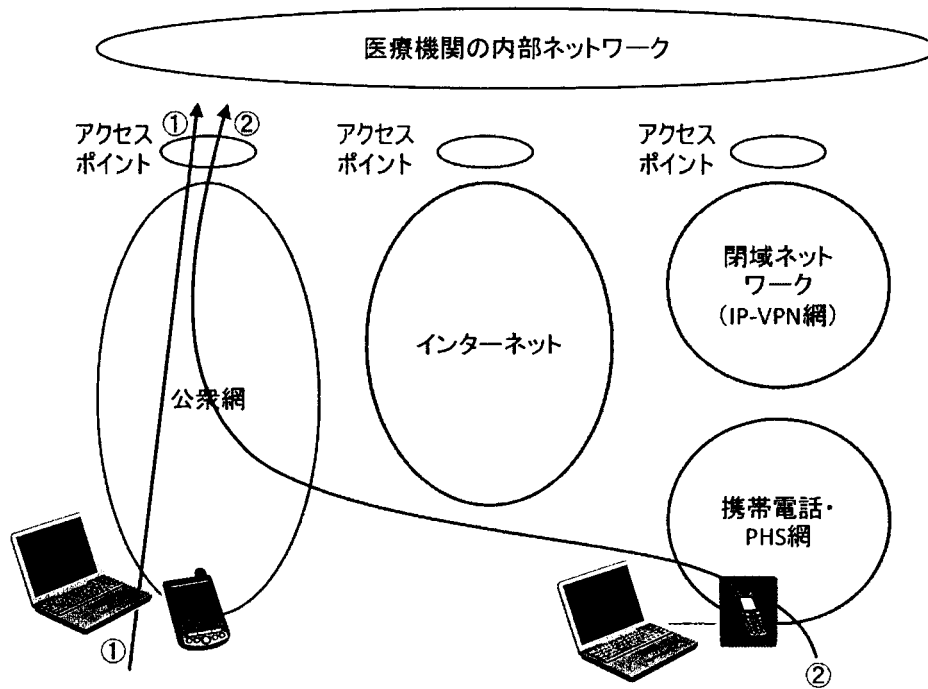


図 B-2-⑥ モバイル環境における接続形態（公衆網経由）

①は自宅やホテルなど、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など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 網を經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經由するため、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

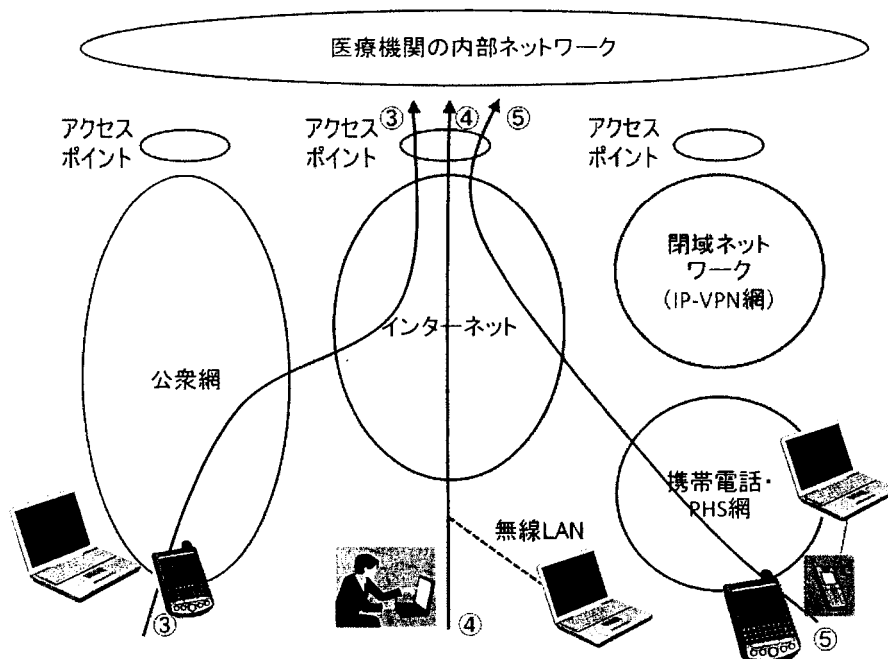


図 B-2-⑦ モバイル環境における接続形態（インターネット経由）

③は自宅やホテルなど、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、自宅やホテルなど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「6.9 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

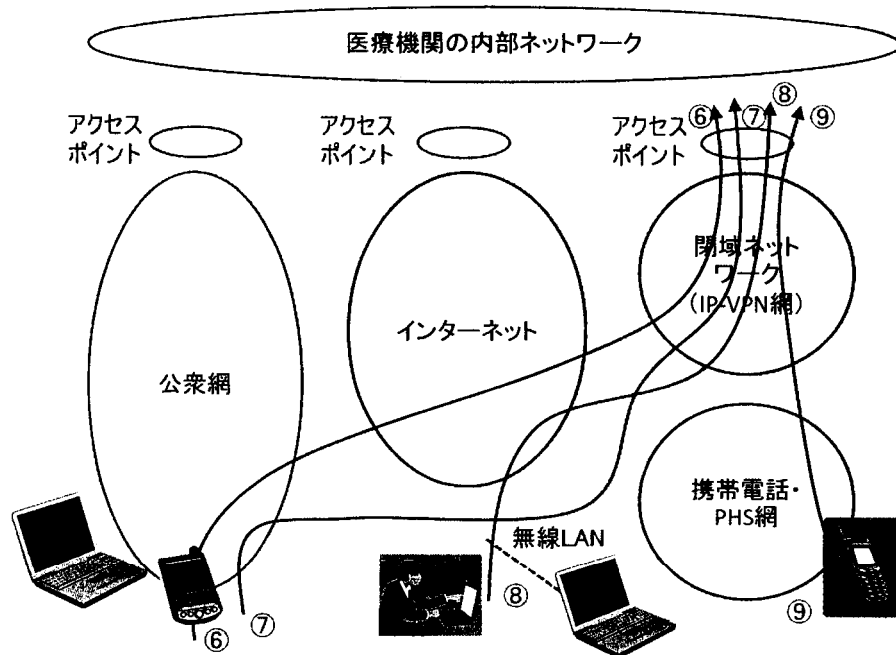


図 B-2-⑧ モバイル環境における接続形態 (閉域ネットワーク経由)

⑥と⑦はいずれも自宅やホテルなど、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、自宅やホテルなど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 など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などの管理面のリスク、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洩のリスクなどである。

これについては「6.9 情報およ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.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す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情報のやり取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。そのため、ここでその際の考え方について触れる。

ただし、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に保存し、その委託先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、既に第4章やB-1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。
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。
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」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。
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。

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」（平成12年法律第102号。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。

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。

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

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」（平成12年法律第102号。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。

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。

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、少なくとも同様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14年法律第153号)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。

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

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)

「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))

B. 考え方

真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。

なお、混同とは、患者を取り違えた記録がなされたり、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。

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、技術面の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、両者のバランスが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、ネットワークを通じて外部に保存を行う場合、第三者が診療録等の外部保存の受託先の機関になりすまして、不正な診療録等を外部保存の委託元の医療機関等へ転送することは、診療録等の改ざんとなる。また、ネットワークの転送途中で診療録等が改ざんされないように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. 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

保存義務のある情報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、その内容が改ざん、消去されたり、過失による誤入力、書き換え・消