資料３－１
（参考資料２）

医療情報システムの安全管理に関するガイドライン

第 5.2 版

別冊

（抜粋）

抽出に当たっては主に以下の観点から行った

・事例や具体的な情報の参照に過ぎないもの
・背景を説明するにとどまるもの
・C 項、D 項等について、例示も含めて詳細に解説していると考えられるもの
・A 項、C 項等との関係性が薄いと考えられるもの
・前回の別冊案に対して、本編から移動したものは緑色のマーカーを塗っている。

医療情報システムの安全管理に関するガイドライン
第 5.2 版 別冊
目次

1. 内容

先への連絡」及び「影響度の確認」である。

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・手作業等の代替手段により業務を再開し、軌道に乗せるまでのフェーズで、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」、「代替施設及び設備の確保」、「再開／復旧活動の両立」及び「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。

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」及び「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「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」及び「総括」である。

⑥ 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。

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に関する解説

外部と診療情報等を交換（双方向だけではなく、一方向の伝送も含む）するケースとしては、地域医療連携で医療機関等や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よう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医療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。

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、いく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。

(1)　医療機関等における留意事項に関する解説

4.2 章で述べた責任のうち、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、情報が電気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されるまでの一連の流れにおいて適用される。

ただし、誤解のないように整理すると、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）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一つである。このように情報の内容に対するセキュリティをオブジェクト・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をチャネル・セキュリティと呼ぶことがある。

このような視点から、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するため、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、何者かが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ったりする等、必ずしも医療機関等の責任といえない明らかな犯罪行為も想定される。一方、ネットワーク機材の不適切な設定による意図しない情報漏えいや誤送信等、医療機関等が責任を負うべき事例も考えられる。

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。その一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。

どのような暗号化を施すか、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性や医療機関等で構築している医療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について、保守作業を受託する事業者等に確認し、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リティの考え方」のネットワークの構成によっては、ネットワーク自体に情報の秘匿化機能が不十分な場合もあり、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の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、送信元が正当な送信元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。

なお、上記の危険性がサイバー攻撃による場合の対応は 6. 10 章を参照されたい。

④　暗号化を行うための適切な鍵管理

経路の暗号化や、電子署名・電子認証によるなりすましの防止や情報の改ざん防止を図る場合には、暗号／復号、デジタル署名に用いる鍵の管理を適切に行うことが重要である。特に共通鍵や、秘密鍵の管理を適切に行うことは、暗号化、デジタル署名の安全性を保証するために必要な対応である。

鍵管理に求められる具体的な対応は、暗号鍵の利用目的に応じて異なる。すなわち、SSL/TLS、電子署名、その他外部との情報交換の際の暗号化、通信機器の認証などに応じて異なるため、それぞれにおいて必要な共通鍵、秘密鍵を保護する機能を具備することが求められる。例えば電子署名や電子証明書を利用した本人認証などでは、電子証明書の認証を行う認証局が定める「証明書ポリシー」(Certificate Policy)に従って、管理することが求められる。

また、共通鍵や暗号鍵を格納する機器や媒体についても、一定の安全性が求められる。暗号モジュールに関するセキュリティ要件の仕様を規定するものとしては、米国連邦標準規格であるFIPS 140-2 (Federal Information Processing Standardization 140-2)※が定められている。機器等の安全性を担保するためには、この基準の最低限のレベルで求められる要件を具備することが望ましい。

※ FIPS140-2では、製品に求めるセキュリティ要件として、Level１からLevel4の４段階のレベルのものを定めている。このうち最も低いLevel１では、「製品レベルのコンポーネントの基本要件を満たす物理的セキュリティメカニズムが存在すればよい」とされる。(”SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES” P4 (NIST、2002.3.12)

B-2. (2)選択すべきネットワークのセキュリティの考え方に関する解説

選択すべきネットワークのセキュリティの考え方については、

・クローズドなネットワークで接続する場合
・オープンなネットワークで接続する場合
・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

の３つの場合について、それぞれ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留意し、確認する責務がある。

医療機関等になるか又は双方の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「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チャネル・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までや、業務の必要性から従業員に外部からのアクセスを許可した場合、患者等からのアクセスを許可した場合等における外部から医療機関等の医療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 は対象としていない。ただし、4.2 章でも触れたとおり、医療機関等には、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留意し、確認する責務がある。

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、医療機関等は交換しようとする情報の機密性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が必須であるが、例えば、予約システムが扱う再診予約情報のように機密性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リスク分析を行った上で、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の所在が、電気通信事業者又は情報処理事業者となるか、医療機関等になるか又は双方の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。

- **電気通信事業者とクラウドサービス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**

  電気通信事業者とクラウドサービス事業者が提供するネットワークサービスのうち、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るネットワークとして電気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、医療機関等は、通信経路上におけるセキュリティに関する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。

- **電気通信事業者とクラウドサービス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電気通信事業者とクラウドサービス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、導入し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を持たない者が安易にネットワークを構築して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、情報の送信元・送信先に導入されるネットワーク接続機器に加え、医療機関等内に設置されている情報端末、当該端末に導入されている機能及び端末の利用者等を確実に確認する手段を確立する必要がある。また、情報をやり取りする機関同士での情報の取扱いに関する契約の締結、(脅威が発生した際に備えて) 電気通信事業者にネットワーク経路上のセキュリティを委託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も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ネットワークを通じて医療情報を交換しようとする場合には、利用する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。

ネットワークサービスの形態は様々存在するため、以降ではいく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、スマートフォン、タブレット等の可搬型コンピュータ、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、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。

① クローズドなネットワークで接続する場合における接続方式に関する解説

以下、それぞれの接続方式について特徴を述べる。

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（図 B-2-①)。電気通信事業者によってネットワークの品質と通信速度（以下「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、その導入に当たってやり取りされる情報の重要性と情報の量等との兼ね合いを見極める必要がある。

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等、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」という。）に接続する方法ではなく、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（図 B-2-②）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や誤送信のリスクがあること、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、大量の情報又は画像等の容量の大きな情報の送信には不向きであることから、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

※ なお ISDN は 2024 年 1 月にサービスの終了がアナウンスされていることから、現在同サービスを利用している場合には、代替策を講じることが求められる。ISDN の代替策としては、現在のネットワーク機器に INS から IP-VPN に変換するアダプタを装着する方法等や、閉域モバイル網を利用するサービス等による例がある。

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、電気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いう。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（図 B-2-③-a、図 B-2-③-b）。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。

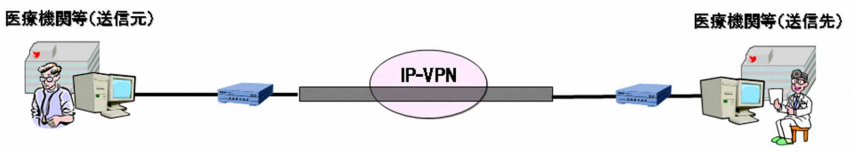

図 B-2-③-a　単一の電気通信事業者が提供する閉域ネットワークで接続されている場合

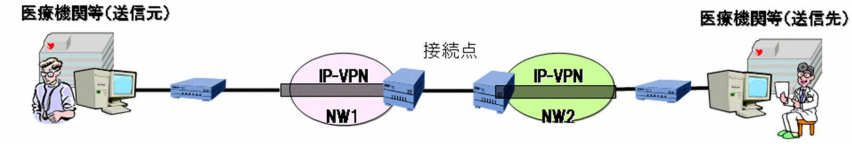

図 B-2-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

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に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、異なる電気通信事業者のクローズドな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いえない。電気通信事業法（昭和 59 年法律第 86 号）があり、万一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。その他、医療機関等から閉域 IP 通信網に接続する点等、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て、改ざんを検知可能な仕組みを導入する等の措置を取る必要がある。

Ⅱ．②オープンなネットワークで接続する場合に関する解説

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いくことが考えられる。

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 Systems 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	ビットデータを電気的、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」とい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。また、偽サーバへの対策が不十分なものが多いため、医療情報システムでは原則として使用するべきではない。一方、IPsec を用いる場合は、2 階層目の「データリンク層」又は 3 階層目の「ネットワーク層」といわれる部分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。ただし、この場合でも、経路を暗号化するための暗号鍵の取り交わしに 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。

IPsec を用いた VPN 接続等によるセキュリティの担保を行わず、インターネット等のオープンなネットワークを介し、他の医療機関や患者等が医療情報システムへ接続する場合（少なくとも TLS による暗号化を用いた HTTPS の利用が求められる。昨今 TLS においてプロトコルやソフトウェアの脆弱性を突いた攻撃の報告が相次いでおり、TLS を適切に利用しなければ接続に HTTPS を用いても安全性を確保することができない。TLS を利用する上での適切な設定方法は、CRYPTREC が作成し独立行政法人情報処理推進機構によって発行された「TLS 暗号設定ガイドライン」にて指針が示されている。「TLS 暗号設定ガイドライン」にて示される設定をすることで、TLS への既知の攻撃から、一定の安全性を確保することができる。なお現時点で最新の「TLS 暗号設定ガイドライン 3.0.1 版」では 3 段階の設定基準が定めら

れているところ、医療情報システムで利用する場合は、そのうち最も安全性水準の高い「高セキュリティ型」の設定を反映することで TLS への攻撃リスクを低減する必要がある。なお、「高セキュリティ型」の設定の一つとして、利用可能なプロトコルバージョンを TLS1.3 に設定するが、システムやサービス等の対応上、これによることが難しい場合には、TLS1.2 以上に限定して設定する必要がある。そのため、サーバ・クライアントともに TLS1.2 以上をサポートしていることが必須となることに注意されたい（TLS1.2、TLS1.3 のいずれかの利用に限定している場合には、それぞれのプロトコルをサポートしていることが求められる）。加えて、オープンなネットワークの場合、不特定の端末から接続されるリスクがあるため、対策の一つとして TLS クライアント認証を行う必要がある。

さらに、オープンネットワークで接続する場合には、IPsec や TLS によるセッションが安全でも、他セッションが同居できるため、ネットワークに接続している機器やシステムが標的型メール等の攻撃にさらされるリスクがある。仮に、このような攻撃によってネットワークに接続する端末等がコンピュータウイルスに感染し、遠隔操作が可能になると、IPsec や TLS1.2 以上によるセッションへの正規のアクセスが発生し得る。

IPsec や TLS による接続は、適切な経路設定を行うことで、セッション間の回り込みを回避することが可能である。一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公開している「レセプト・オンライン請求用チェックシート項目集」（※）が参考になる。

※ 「レセプト・オンライン請求用チェックシート項目集」

http://www.hispro.or.jp/open/pdf/200909OnRece%20koumoku.pdf

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。なお、日頃からセキュリティインシデントの報道や事業者からの情報提供等を通じて、TLS 等の脆弱性リスクについて注意、認識しておくことが求められる。また、多くの場合、ネットワーク導入時に事業者等に委託をすることになるが、その際、リスクの説明を求め、理解しておくことも必要である。

なお、オープンネットワークを通じて外部から情報を取り込む際に、取り込む情報の安全性を確認する必要がある。そのため、例えば取り込むデータ等についての無害化を図るなど、標的型攻撃等によるリスクを減少する対応を図ることが求められる。

また、外部との接続については、医療機関等がクラウドサービスを利用し、受託事業者等のサーバからデータを取得する場合も、同様のリスクを想定する必要がある。特にクラウドサービスの場合には、利用するサービスによって、取り扱う情報の機密性等が異なるため、事業者によってセキュリティの水準が異なることがある。したがって、医療情報を取り扱う場合には、利用する各クラウドサービスにおけるリスク等を鑑みた対応をとることが求め

られる。必要に応じて、ネットワークの分離（例えばメールシステムと医療情報システムの分離）や、これを踏まえた情報交換のルールに基づく管理を行うことが望ましい。

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．③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に関する解説

外部から医療機関等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。

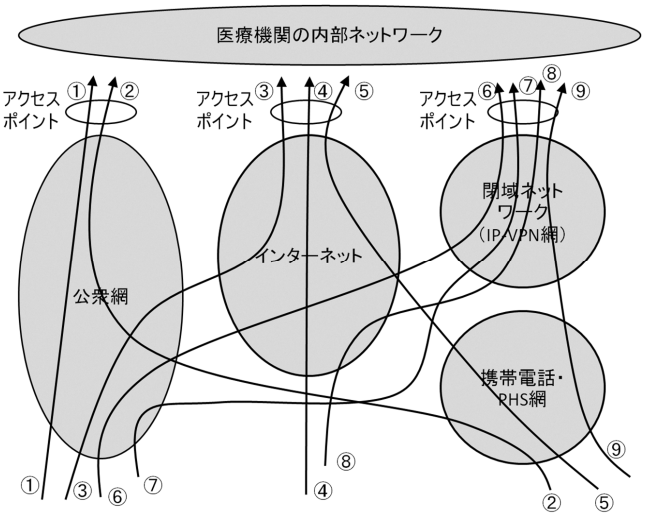

図 B-2-⑤　モバイル環境における接続形態

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）

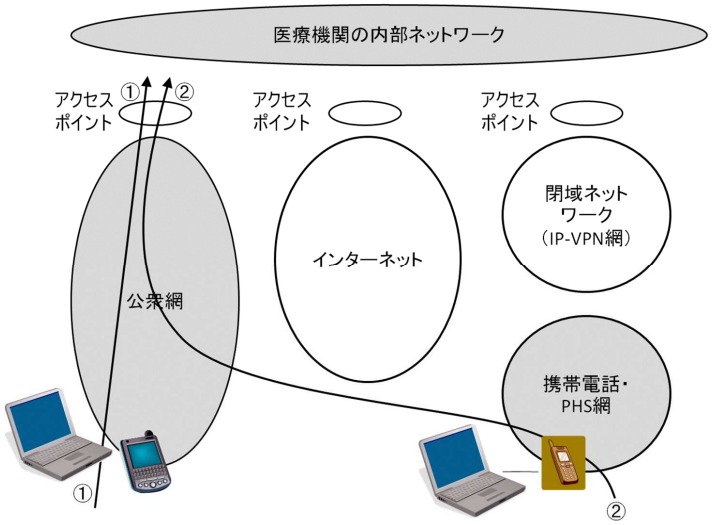

図 B-2-⑥　モバイル環境における接続形態（公衆網経由）

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、医療機関等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 網に接続するケースである。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「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、セキュリティ上の要件は、そこでの記述を適用する必要がある。全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。

2）インターネットを経由して接続する場合（図 B-2-⑦）

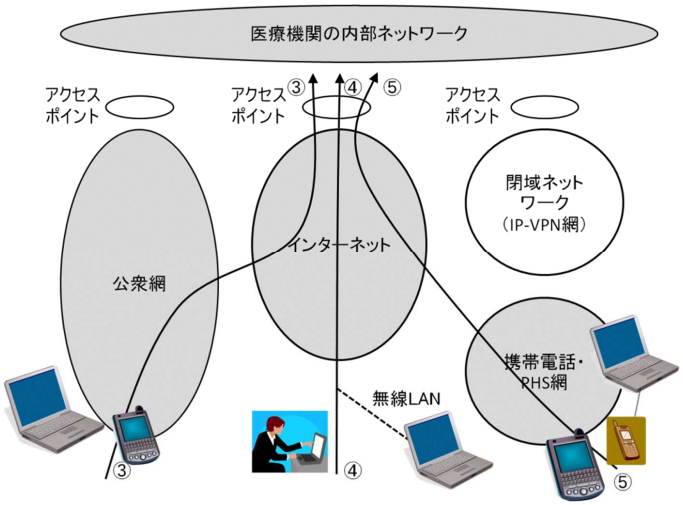

図 B-2-⑦　モバイル環境における接続形態（インターネット経由）

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等のアクセスポイントに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、電気通信事業者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はある。

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。したがって、セキュリティ上の要件は、そこでの記述を適用する必要がある。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。

3）閉域ネットワークを経由して接続する場合（図 B-2-⑧）に関する解説

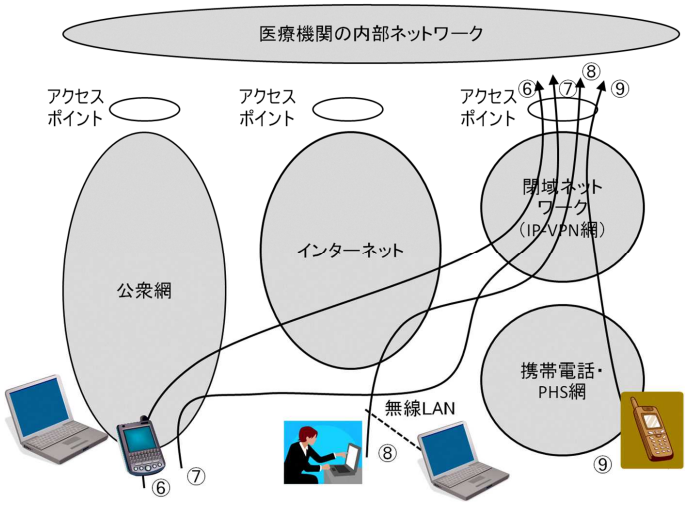

図 B-2-⑧　モバイル環境における接続形態（閉域ネットワーク経由）

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等のアクセスポイントに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、オープンなネットワークを通じて閉域ネットワークへ接続するケースでは、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、電気通信事業者によって提供されるサービスである。

B-4. 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に関する解説

ここでの考え方の原則は、医療機関等が患者等との同意の上で、自ら実施して患者等に診療情報等を提供する場合であり、診療録及び診療諸記録の外部保存を受託する事業者が独自に診療情報等の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、診療情報等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、一旦診療情報等を提供すれば、その情報保護の責任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、診療情報等を提供する医療機関等が患者等の納得のい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る。また、説明が不足している中で万一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。

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診療情報等を提供することは、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な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 4 章や B-1 で述べているが、オープンなネットワーク接続であるため、利活用と安全確保の両面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 TLS 暗号化、PKI 個人認証等の技術を用いる必要がある。

また、患者の委託先に診療情報等を送付する(クラウドサービスへのアップロード含む)際、外部の事業者に対して送付するよう、患者から依頼を受ける場合も想定される。この場合、患者の委託先への送付であることから、第三者提供には当たらないものの、診療情報等の流出などに対する留意が求められる。送信先／アップロード先についての安全性等を確認し、疑義が生じた場合に患者からの依頼を断るなどのほか、送信等を行うに当たっては、患者との関係で責任分界についても取り決めておくことが求められる。

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

法令で定められた記名・押印を電子署名を行うことの経緯に関する解説

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、法令で署名又は記名・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。

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として e-文書法省令において指定された文書においては、「A. 制度上の要求事項」に示した電子署名によって、記名・押印に代わり電子署名を施すことで、作成・保存が可能となった。

電子署名で用いられる暗号に関するの解説

電子署名法における特定認証業務の基準として、電子署名法施行規則第 2 条で RSA 2048bit の暗号方式が定められており、電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針(平成十三年四月二十七日総務省・法務省・経済産業省告示第二号)で SHA-256 以上のハッシュ関数が定められている。~~電子署名に一般的に用いられている暗号方式の RSA 1024bit やハッシュ関数の SHA1 は、政府機関の情報システムからの移行スジュールが決まっており、平成 20 年 4 月の情報セキュリティ政策会議が決定した「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA1 及び RSA1024 に関わる移行指針」(平成 24 年 10 月改定)を基に、2014 年度以降、RSA 2048bit や SHA2 等への移行が進められている。~~

長期署名方式に関するの解説

長期署名方式では、下記により、署名検証の継続を可能としている。

- 署名に付与するタイムスタンプにより署名時刻を担保する(署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること)。
- 署名当時の検証情報(関連する証明書や失効情報等)を保管する。
- 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。