

改正案	現 行
<p data-bbox="136 231 1111 268">6.9 情報および情報機器の持ち出しについて</p> <p data-bbox="136 268 1111 316">B. 考え方</p> <p data-bbox="136 347 1111 459">昨今、医療機関等において医療機関等の従業者や保守業者による情報および情報機器の持ち出しによる個人情報を含めた情報が漏えいする事案が発生している。</p> <p data-bbox="136 467 1111 619">情報の持ち出しについては、ノートパソコンのような情報端末やフロッピーディスク、USBメモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。</p> <p data-bbox="136 627 1111 738">従って、本項ではノートパソコンや可搬媒体、シンクライアントのような機器等による情報、また、情報機器そのものの持ち出しについて考え方と留意点を述べる。</p> <p data-bbox="136 746 1111 890">まず重要なことは、「6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」の「6.2.2 取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3 リスク分析」を実施することである。</p> <p data-bbox="136 898 1111 1050">その上で、医療機関等において把握されている情報もしくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。</p> <p data-bbox="136 1058 1111 1169">適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。</p> <p data-bbox="136 1177 1111 1361">一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱ったり、医療機関等の情報システムにアクセスしたことで、コンピュータウイルスや不適切な設定のされたアプリケーション（Winny等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、</p>	<p data-bbox="1111 231 2085 268">(新設)</p>

情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であつて、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。

ただし、この際留意しなくてはならないことは、可搬媒体や情報機器による情報の持ち出しは、医療機関等に設置されているような情報機器よりも、盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策を更に施す必要がある。

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、情報および情報機器の持ち出しに関する方針を運用管理規定で定めること。
2. 運用管理規定には、持ち出した情報およ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定に定めること。
4. 運用管理規定で定めた盗難、紛失時の対応に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などの利用を避けたり、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、このようなアプリケーション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。
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。

改正案	現 行
<p data-bbox="136 236 533 268">6.10 災害等の非常時の対応</p> <p data-bbox="136 272 1093 320">B. 考え方</p> <p data-bbox="136 352 1099 424">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を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。</p> <p data-bbox="136 429 1099 580">ここでは、「6.2.3 リスク分析」の「⑥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 障害などの非常時に、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。</p> <p data-bbox="136 585 1099 657">「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。</p> <p data-bbox="136 662 1099 774">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。</p> <p data-bbox="136 778 1099 970">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<u>不都合</u>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。</p> <p data-bbox="600 1018 651 1050">(略)</p>	<p data-bbox="1111 236 1496 268">6.9 災害等の非常時の対応</p> <p data-bbox="1111 272 2067 320">B. 考え方</p> <p data-bbox="1111 352 2074 424">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を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。</p> <p data-bbox="1111 429 2074 580">ここでは、「6.2.3 リスク分析」の「⑥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 障害などの非常時に、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。</p> <p data-bbox="1111 585 2074 657">「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。</p> <p data-bbox="1111 662 2074 774">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。</p> <p data-bbox="1111 778 2074 970">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<u>不合理</u>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。</p> <p data-bbox="1574 1018 1626 1050">(略)</p>

改正案	現 行
<p data-bbox="136 231 1115 271">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</p> <p data-bbox="136 271 1115 327">B. 考え方</p> <p data-bbox="136 327 1115 742">ここでは、組織の外部と情報交換を行う場合に、個人情報保護およ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。<u>ここでは、双方向だけではなく、一方向の伝送も含む。</u>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（Application Service Provider）型のサービスを利用する、<u>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場合等</u>が考えられる。</p> <p data-bbox="136 742 1115 1013">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、<u>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」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。</u></p> <p data-bbox="136 1013 1115 1204">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。</p>	<p data-bbox="1115 231 2101 271">6.10 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</p> <p data-bbox="1115 271 2101 327">B. 考え方</p> <p data-bbox="1115 327 2101 630">ここでは、組織の外部と情報交換を行う場合に、個人情報保護およ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。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（Application Service Provider）型のサービスを利用する場合等が考えられる。</p> <p data-bbox="1115 630 2101 1013">外部と医療情報を外部ネットワークを利用して交換する場合、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、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。</p> <p data-bbox="1115 1013 2101 1204">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。</p> <p data-bbox="1115 1204 2101 1364"><u>なお、医療機関等が法令による義務の有無に関わらず、個人情報を含む医療情報の保存を外部に委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要なため、8章に別途まとめて記述を行う。</u></p>

<p>B-1. 医療機関等における留意事項</p> <p>ここでは第4章の「<u>電子的な医療情報を扱う際の責任のあり方 4.2 責任分界点について</u>」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。</p> <p>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、適切に送信先の医療機関等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。</p> <p>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。</p> <p>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。</p> <p>(削除)</p>	<p>B-1. 責任分界点の明確化 (新設)</p> <p>医療情報を外部に提供することは個人情報保護法上、委託と第三者提供の2種類があり、<u>遵守すべき事項が異なる。</u></p> <p>委託の場合、管理責任は提供元医療機関等にあり、契約と監督で管理責任を果たす責務があり、説明責任・結果責任を負わなければならない。提供先</p>
---	---

機関は契約遵守と報告義務を負う。

第三者提供の場合、提供元は同法第23条で規定された例外を除き、「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」のⅢ-5-(3)-①のア～エに相当する場合は同ガイドラインで明記された方法で黙示の同意、それ以外の場合は明示の同意を得なければならない。また提供先は同法第15条、第16条にしたがって利用目的を特定し、同法および「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」にしたがって個人情報保護を達成する責務を負う。これらの要件を満たして提供された情報に対して提供元は責任を負わない。

オンラインで情報を提供する場合、情報の主体である患者と情報が乖離する。患者と乖離している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。また患者にとっての苦情の申し入れ先や開示等の要求先が明白でなければならない。

提供元医療機関等、オンラインサービス提供事業者、回線提供事業者、提供先機関または提供先になる可能性がある事業者等が関係事業者になりえる。以下の原則で責任分界点を考える必要がある。

まず、提供元医療機関等と提供先機関は通信経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となっていくかを明らかにする必要がある。ただし、前述のように結果責任、説明責任は委託の場合は提供元事業者、第三者提供の場合は提供元医療機関等または提供先機関にあり、オンラインサービス提供事業者や回線提供事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

回線事業者の提供する回線の発信元との責任分界点以前に適切に暗号化され、送信先との責任分界点以降に復号される場合は、回線事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の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は契約で明らかにすること。

オンラインサービス提供事業者の管理範囲の開始される責任分界点に情報が到達する以前に適切に暗号化され、管理範囲の終了する責任分界点以降に復号される場合は、オンラインサービス提供事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲やサービスの可用性等の品質に関しては契約で明らかにすること。

法令で定められている場合などの特別な事情により、オンラインサービス提供事業者および回線提供事業者のいずれかに暗号化されていない医療情報が送信される場合は、オンラインサービスもしくは回線において盗聴の脅威に対する対策を施す必要があるため、当該医療情報の通信経路上の管理責任を負っている医療機関等はオンラインサービス提供事業者もしくは回線提供事業者と医療情報の管理責任についての明確化をおこない、オンラインサービス提供事業者もしくは回線提供事業者に対して管理責任の一部もしくは全部を委託する場合はそれぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

提供元医療機関等と提供先機関が1対1通信である場合、または1対Nであってもあらかじめ提供先または提供先となる可能性がある機関を特定できる場合は委託または第三者提供の要件にしたがって両機関等が責務を果たさなければならない。

提供元医療機関等と提供先機関が1対N通信で、提供先機関が一つでも特定できない場合は原則として医療情報を提供できない。ただし法令で定められている場合等の例外を除く。

リモートログイン機能を用いたデータアクセスには、代表的用途としてシステムメンテナンスを目的とした遠隔保守のためのアクセスが考えられる。しかし、制限がゆるいと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。

他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。適切に管理されたリモートログイン機能のみに制限しなければならない。

(削除)

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。一方で、不適切なネットワーク機材の設定により、意図しない情報漏えいや誤送信等も想定され、こ

B-2. 医療機関等における留意事項

ここでは「B-1. 責任分界点の明確化」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、適切に送信先の医療機関等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-3. 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。一方、「B-3. 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。一方で、不適切なネットワーク機材の設定により、意図しない情報漏洩や誤送信等も想定され、この

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、先に例示した通りであり、情報そのものの暗号化のことを指している。

すなわちオブジェクト・セキュリティの考え方が必要となる。

どの程度の暗号化を施すか、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の高さ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 ID とパスワードを用いた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ることも重要な要素である。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リティの考え方」のネットワークの構成によっては、情報を暗号化せずに伝送する可能性も否定できず、その場合には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、送信先の医療機関等が確かに意図した相手であることを確認しなくては

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、意図しない情報漏洩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、先に例示した通りであり、情報そのものの暗号化のことを指している。

どの程度の暗号化を施すか、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の高さ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乖離する段階においては暗号化されていることが望ましい。

さらに、この盗聴防止については、例えば ID とパスワードを用いた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ることも重要な要素である。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-3.** 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、情報を暗号化せずに伝送する可能性も否定できず、その場合には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、送信先の医療機関等が確かに意図した相手であることを確認しなくては

ならない。逆に、情報の受け手となる送信先の医療機関等は、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、送られて来た情報が確かに送信元の医療機関等の情報であること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で医療機関等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、送信元の医療機関等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チャンネル・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、同じく医療機関等の情報を受信する機関の外部ネットワーク接続点や業務の必要性や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 4.2 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性の整理をする必要がある。「[B-1. 医療機関等における留意事項](#)」では情報そのもの

ならない。逆に、情報の受け手となる送信先の医療機関等は、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、送られて来た情報が確かに送信元の医療機関等の情報であること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で医療機関等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、送信元の医療機関等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「[6.9](#) 災害等の非常時の対応」を参照されたい。

B-3. 選択すべきネットワークのセキュリティの考え方

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、同じく医療機関等の情報を受信する機関の外部ネッ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性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

(略)

- ・ 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

(中略)

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

(略)

- ・ 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

(中略)

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。

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

(略)



図 B-2-① 専用線で接続されている場合

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-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

(略)

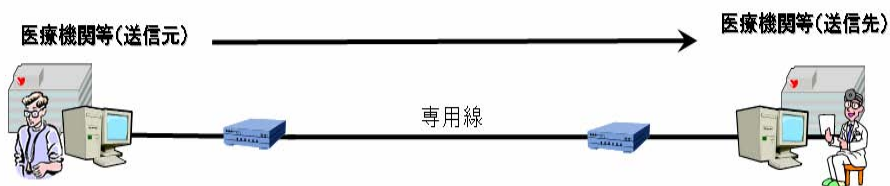


図 B-3-① 専用線で接続されている場合

②公衆網で接続されている場合

(略)



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

(略)

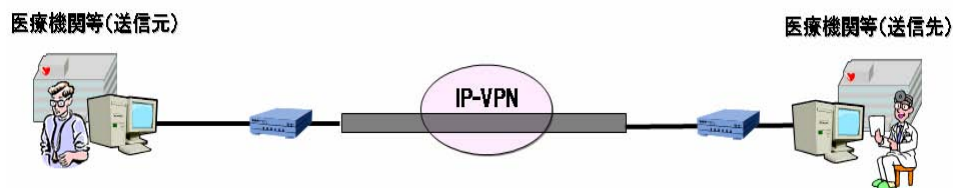


図 B-2-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

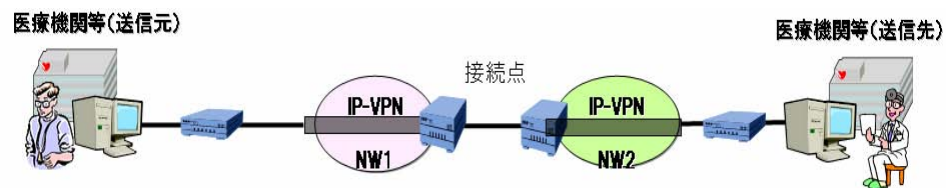


図 B-2-③-b 途中で複数の閉域ネットワークが相互接続して接続されている

②公衆網で接続されている場合

(略)



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

(略)

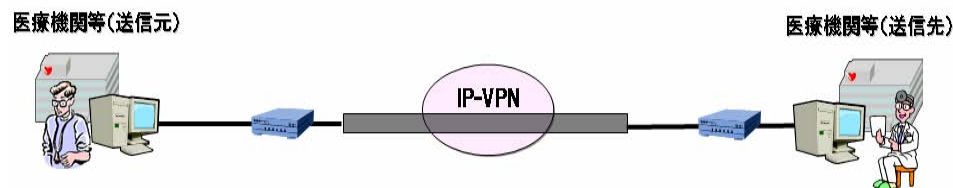


図 B-3-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

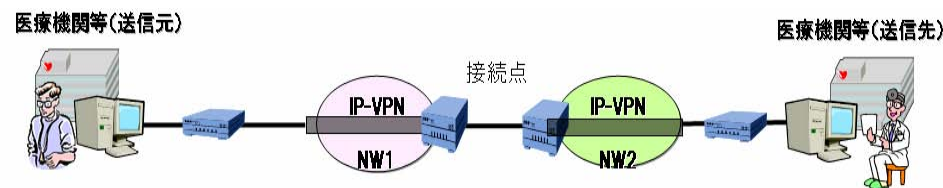


図 B-3-③-b 途中で複数の閉域ネットワークが相互接続して接続されている

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可能性がある。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

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可能性がある。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。

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。

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