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

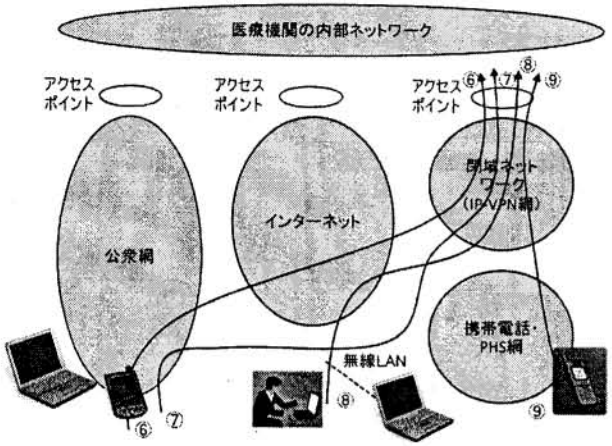

図 B-2-⑧　モバイル環境における接続形態（閉域ネットワーク経由）

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、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ネル・セキュリティが確保されないこともありうる。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、事前にサービス提供者との契約をよく確認して、チャネル・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等の管理面のリスク、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えいのリスク等である。

これについては「6.9　情報及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 従業者による外部からのアクセスに関する考え方

医療機関等の職員がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可することもあり得る。このような場合のネットワークに関わる安全管理の要件はすでに述べたが、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。加えて、外部からのアクセスに用いる機器の安全管理を運用管理規程で定めることは重要ではあるが、考慮すべきことが 3 点ある。

① PC 等と言ってもその安全管理対策を確認するためには一定の知識と技能が必要で、職員にその知識と技能を要求することは難しいこと。
② 運用管理規程で定めたことが確実に実施されていることを説明するためには適切な運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは通常は困難なこと。
③ 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等の管理下にある機器を必要に応じて使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性があること。

従って、通常は行うべきではないが、医師不足等に伴う医療従事者の過剰労働等に対応するために、やむを得ず行う場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術が普及しており、これらの導入を検討することが重要であるとともに、運用等の要件にも相当な厳しさが求められ

る。

B-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

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させ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医療情報の交換を想定しているが、患者に対する情報提供も十分想定される状況にある。ここではその際の考え方について触れる。

ここでの考え方の原則は、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の外部保存を受託する事業者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 で述べられているが、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 に関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、ウイルス混入等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 アドレス詐称等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に確認すること。

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・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、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等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. ルータ等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等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等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等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関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管理責任及び事後責任の明確化。
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　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及び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。

D. 推奨されるガイドライン

1. やむを得ず、従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。

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（平成12年法律第102号）　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」（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、e-文書法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り失効させた場合は検証ができないという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。例えば現在、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、2008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」によれば、2014年度以降、RSA 2048bitやSHA2等へ移行される予定となっている。

従って、電子署名を付与する際はこのような点を考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名の検証が継続できる必要がある。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。近年、デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、JIS規格としても制定された（JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル）。

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。

(1) 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）。
(2) 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。
(3) 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。

医療情報の保存期間は5年以上の長期に渡るものも有り、システム更新や検証システムの互換性等の観点からも、標準技術を用いることが望ましい。従って、例えば、前述の標準技術を用い、必要な期間、電子署名の検証を継続して行うことが出来るようにすることが重要である。

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、同等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. タイプスタンプは、「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こと。
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。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。

7 電子保存の要求事項について

法的に保存義務のある文書等を電子的に保存するためには、日常の診療や監査等において、電子化した文書を支障なく取り扱えることが当然担保されなければならないことに加え、その内容の正確さについても訴訟等における証拠能力を有する程度のレベルが要求される。誤った診療情報は、患者の生死に関わることであるので、電子化した診療情報の正確さの確保には最大限の努力が必要である。また、診療に係る文書等の保存期間については各種の法令に規定されており、所定の期間において安全に保存されていなくてはならない。

これら法的に保存義務のある文書等の電子保存の要件として、真正性、見読性及び保存性の確保の３つの基準が示されている。それらの要件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かったり、煩わしさばかりが募ったりすることが想定され、両者のバランスが取れた総合的な対策が重要である。各医療機関等は、自らの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。

7.1 真正性の確保について

A. 制度上の要求事項

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。

（e-文書法省令　第４条第４項第２号）

② 真正性の確保

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。

（ア） 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。

（イ） 作成の責任の所在を明確にすること。

（施行通知　第２　２（３）②）

「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