「医療情報システムの安全管理に関するガイドライン」　改正案　【新旧対照表】

改正案	現　行
2　本指針の読み方	**2　本指針の読み方**
（略）	（略）
D．推奨されるガイドライン 実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解が得やすい対策を記載している。 また、最低限のシステムでは使用されていない技術で、その技術を使用する上で一定の留意が必要となる場合についての記載も含んでいる。	**D．推奨されるガイドライン** 実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解が得やすい対策を記載している。
なお、巻末の3つの付表は安全管理上の要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされてはじめて有効なものとなるが、技術的対策には複数の選択肢があることが多く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。	また、巻末の3つの付表は安全管理上の要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされてはじめて有効なものとなるが、技術的対策には複数の選択肢があることが多く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。
（略）	（略）

<table>
<tr><th>改正案</th><th>現　行</th></tr>
<tr><td>

6.2　医療機関における情報セキュリティマネージメント（ISMS）の実践

6.2.1　　ISMS 構築の手順

情報セキュリティマネジメントの構築は PDCA モデルによって行われる。JIPDEC ISMS 認証基準（Ver2.0）では PDCA の各ステップを次の様に規定している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。
Do－実施 (ISMS の導入及び運用)	その情報セキュリティ基本方針、管理策、プロセス及び手順を実施し運用する。
Check－点検 (ISMS の監視及び見直し)	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act－処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

P では ISMS 構築の骨格となる文書（基本方針、運用管理規程など）と文書化された ISMS 構築手順を確立する。
D では P で準備した文書や手順を使って実際に ISMS を構築する。
C では構築した ISMS が適切に運用されているか、監視と見直しを行う。
A では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるように、医療行為における安

</td><td>

6.2　情報の取扱いの把握とリスク分析

（新設）

</td></tr>
</table>

全管理のステップがどのようにおこなわれているかをJIPDECの「医療機関向けISMSユーザーズガイド」に記載された例を用いて確認してみる。

【医療の安全管理の流れ】

事故やミスの発見と報告
「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析
- 「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
（例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
- 作成したフロー図を分析し、どのプロセスに原因があったのかを調べる

↓

予防／是正策
- 再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底など）

上記を見ると、主にD→C→Aが中心になっている。これは医療分野においては診察、診断、治療、看護などの手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行するこ

とで安全が高まる仕組みが出来上がっているためと言える。 反面、情報セキュリティではIT技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため情報セキュリティ独自の管理方法が必要であり、ISMS はそのために考え出された。ISMSは医療の安全管理と同様PDCAサイクルで構築し、維持して行く。 逆に言えば、医療関係者にとってISMS構築はPのステップを適切に実践し、ISMS の骨格となる文書体系や手順などを確立すれば、あとは自然にISMSが構築されていく土壌があると言える。 Pのステップを実践するために必要なことは何かについて次に述べる。	
6.2.2　取扱い情報の把握	**6.2.1　取扱い情報の把握**
（略）	（略）
6.2.3　リスク分析	**6.2.2　リスク分析**
①～⑤（略）	①～⑤（略）
⑥　医療情報システム自身 (a) サイバー攻撃によるIT障害 ・ 不正侵入 ・ 改ざん ・ 不正コマンド実行 ・ 情報かく乱 ・ ウイルス攻撃 ・ サービス不能（DoS：DenialofService）攻撃 ・ 情報漏えい　等 (b) 非意図的要因によるＩＴ障害 ・ システムの仕様やプログラム上の欠陥（バグ）	（新設）

・ 換作ミス ・ 故障 ・ 情報漏えい　等 (c) 災害による IT 障害 ・ 地震、水害、落雷、火災等の災害による電力供給の途絶 ・ 地震、水害、落雷、火災等の災害による通信の途絶 ・ 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等 ・ 地震、水害、落雷、火災等の災害による重要インフラの機能不全 （略）	（略）

改正案	現　行
6.5　技術的安全対策	**6.5　技術的安全対策**
B. 考え方	**B. 考え方**
（略）	（略）
(1) ～ (4)（略）	**(1) ～ (4)**（略）
(5) ネットワーク上からの不正アクセス ネットワークからのセキュリティでは、ハッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。 ファイアウォールは 「パケットフィルタリング」、「アプリケーションゲートウェイ」および「ステートフルインスペクション」の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護することが望ましい。システム管理者はその方式が何をどのように守っているかを認識するべきである。 また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ等の対策を講じておく事も重要である。 無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃（サービス不能攻	**(5) ネットワーク上からの不正アクセス** ネットワークからのセキュリティでは、ハッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。 ファイアウォールは 「パケットフィルタリング」、「アプリケーションゲートウェイ」および「ステートフルインスペクション」の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護することが望ましい。システム管理者はその方式が何をどのように守っているかを認識するべきである。 また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。 無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、ネットワーク機器に対して攻撃を行なったり、不正にネッ

撃 DoS : Denial of Service　等）を行なったり、不正にネットワーク上のデータを傍受したり改ざん等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて PC を識別する場合が多いが、MAC アドレスは改ざん可能であるため、その事を念頭に置いた上で対策を行なう必要がある。不正アクセスの防止は、いかに保証を確実に確保するかが問題であり、特に、“なりすまし“の問題は絶えずついて廻る。	トワーク上のデータを傍受したり改ざん等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて PC を識別する場合が多いが、MAC アドレスは改ざん可能であるため、その事を念頭に置いた上で対策を行なう必要がある。不正アクセスの防止は、いかに保証を確実に確保するかが問題であり、特に、“なりすまし“の問題は絶えずついて廻る。
（略）	（略）
D．推奨されるガイドライン	**D．推奨されるガイドライン**
1.～4.（略）	1.～4.（略）
5. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクション）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。 　また、無線 LAN を用いる場合は最低限の使用とし、総務省発行の「安心して無線 LAN を利用するために」を参考にし、暗号化や容易に推測できない ID を用いる等、情報資産の評価にもとづき適切な配慮をおこなうこと。	5. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクション）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。
6.～7.（略）	6.～7（略）

改正案	現　行
6.8　情報システムの改造と保守	**6.8　情報システムの改造と保守**
B. 考え方	**B. 考え方**
医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。 ・ 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等 ・ 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等 ・ 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等 ・ 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等 これらの脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。 また、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。 なお、保守作業によっては保守会社からさらに外部委託業者に修理等を依頼することが考えられるため、保守会社との保守契約の締結にあたっては、	医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。 ・ 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等 ・ 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等 ・ 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等 ・ 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等 これらの脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。 また、保守作業によっては保守会社からさらに外部委託業者に修理等を依頼することが考えられるため、保守会社との保守契約の締結にあたっては、

再委託先への個人情報保護の徹底等について保守会社と同等の契約を求めることが重要である。 （略）	再委託先への個人情報保護の徹底等について保守会社と同等の契約を求めることが重要である。 （略）

改正案	現　行
6.9　災害等非常時の対応 **B. 考え方** 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。 医療機関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。「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。 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。 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不合理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。 (1) 非常時のおける事業継続計画(以下 BCP と略す) 異常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。異常事態を適切に分類することは難しく、可能な限り計画内容を事前演習などで検証することが望ましい。 医療施設として定められる BCP においては、医療情報システムについての計画を含め、全体としての整合性が必要である。 以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。	（新設）

① BCP として事前に周知しておく必要がある事項
事前に対応策を知ってもらい、信頼してもらっておくべきである。
- ポリシーと計画
  何が「情報セキュリティ」なのかを理解し、定義すべきである。
- 非常事態検知手段
  災害や故障の検知機能と発生情報の確認手段
- 非常時対応チームの連絡先リスト、連絡手段および対策ツール
- 非常時に公にすべき文書および情報

② BCP 発動フェーズ
災害や事故の発生（或いは発生の可能性）を検知してから、BCP 発動か通常の障害対策かの判断をおこない、BCP 発動と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡･協力依頼をおこない、システムの切替／縮退等の準備をおこなう。例えば、ネットワークから切り離しスタンドアロンで使用するとか、紙での運用にするとかが考えられる。

業務委託先との間の連絡体制や委託先と一体となったトラブル対処方法等が明示されるべきである。
具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」、および「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・手作業などの代替手段により業務を再開し、軌道に乗せるまでフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員など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」、「代替施設および設備の確保」、「再開／復旧活動の両立」、および「リスク対策のリスク対策」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」および「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「切替の判断」、「復旧手順の再確認」、「確認事項の整備」および「総括」である。

(2) 医療システムの非常時使用への対応(ブレイクグラス)

① 非常時用ユーザアカウントの用意
停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えること。例えば、非常時のユーザアカウントを用意するなどして、患者データへのアクセス制限が医療サービス低下を招かないように配慮すること。緊急用ユーザアカウントの配布の例としては、次のようなものが挙げられる。

- キャビネットのガラスの後ろに保管
  これはパスワードを入手するためには文字通りガラスを壊す必要があり、見た目で分かるだけでなく、不用な使用を防止する。

- 密封した封筒に保管
  封が開いていれば利用されたことがわかる。

・ 特定の人が保管
例えば看護師長、施設警備員が机に施錠して保管する。

・ ２名以上で鍵を管理

② 災害時は、通常時とは異なる人の動きが想定される。例えば、受付での患者登録を経ない診察が行われるため、診療科端末での仮患者登録機能が求められることが考えられる。

上記の様なブレイクグラス機能の用意は、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

C. 最低限のガイドライン

1. BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。非常時機能が定常時に不適切に利用されないように監査をすること。また、非常時用ユーザアカウントであれば正常復帰後は継続使用が出来ないように変更しておくこと。
4. サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、あらかじめ定められた所管官庁への連絡を行うこと。

改正案	現　行
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	**6.9　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**
B. 考え方	**B. 考え方**
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。 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」を、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。 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。 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。	ここでは、組織の外部と情報交換を行う場合に、個人情報保護に関して特に留意すべき項目について述べる。 外部と医療情報を交換するケースとしては、検査を外部機関に委託していて、オンラインでデータをやり取りする場合等が考えられる。 医療機関等が法令による義務の有無に係らず、外部と個人情報を含む医療情報を交換し、外部に保存を委託する場合は、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載を行う。 個人情報を電気通信回線により伝送する場合は以下による。

（削除）	① **秘匿性の確保のための適切な暗号化** 電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。したがって電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。 ② **通信の起点・終点識別のための認証** 通信手段によって、起点･終点の識別方法は異なる。例えば､インターネットを用いる場合は起点・終点の識別は IP パケットを見るだけでは確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の機関と受託先の機関を確実に相互に認証しなければならない。たとえば、認証付きの VPN、SSL/TLS や ISCL を適切に利用することにより実現できる。なお、当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。 ③ **リモートログイン制限機能** 個人情報を含む医療情報の保存業務を受託先の機関や委託元の機関のサーバへのリモートログイン機能に制限を設けないで容認すると、ログインのためのパスワードが平文で LAN 回線上を流れたり、ファイル転送プログラム中にパスワードがそのままの形でとりこまれたりすることにより、これが漏洩する可能性がある。 また、認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。また、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、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も考えられる。 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。
B-1. 責任分界点の明確化 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、遵守すべき事項が異なる。 委託の場合、管理責任は提供元医療機関にあり、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。提供先期間は契約遵守と報告義務を負う。 第三者提供の場合、提供元は法２３条で規定された例外を除き、厚生労働省個人情報保護ガイドラインの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。また提供先は法１５条、１６条にしたがって利用目的を特定し、法および厚労省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。 提供元事業者、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、提供元事業者と提供先機関は通信経路における責任分界点を定め、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を明らかにする必要がある。 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	（新設）

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。 　提供元事業者と提供先事業者が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事業者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事業者が責務を果たさなければならない。 　提供元事業者と提供先事業者が１対Ｎ通信で、提供先事業者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。	

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	（新設）

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	（新設）

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度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。 ・ 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 通信事業者が提供するネットワークサービスの内、通信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。ただし、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通信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定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。 ・ 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通信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。ただし、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。 **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	（新設）

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。

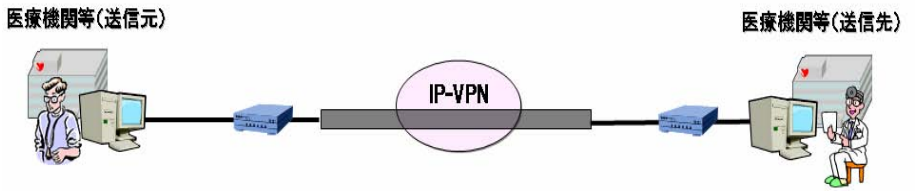

図 B-3-③-a　単一の通信事業者が提供する閉域ネットワークで接続されている場合

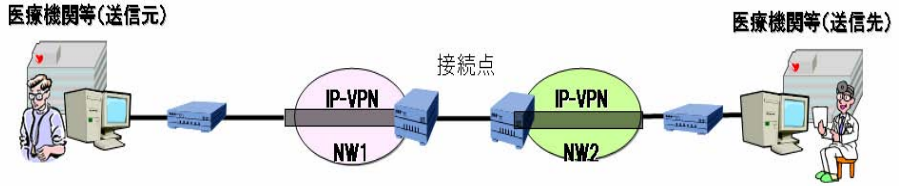

図 B-3-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

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、IS015408 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	

改正案	現　行
7　電子保存の要求事項について	**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	**7.1　真正性の確保について**
A. 制度上の要求事項	**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）	保存義務のある情報の真正性が確保されていること。 ○　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。 ○　作成の責任の所在を明確にすること。 （施行通知　第二　２（３）②）
（略）	（略）
7.2　見読性の確保について	**7.2　見読性の確保について**
A. 制度上の要求事項	**A. 制度上の要求事項**
保存義務のある情報の見読性が確保されていること。 必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 （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項第一号）	保存義務のある情報の見読性が確保されていること。 ○　情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。 ○　情報の内容を必要に応じて直ちに書面に表示できること。 （施行通知　第二　２（３）①）
（略）	（略）

7.3　保存性の確保について **A. 制度上の要求事項** 保存義務のある情報の保存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いて復元可能な状態で保存することができる措置を講じていること。 （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 項第三号） （略） **7.4　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** （略） **C. 最低限のガイドライン** （略） **（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。** 1～2（略） 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。 （略）	**7.3　保存性の確保について** **A. 制度上の要求事項** 保存義務のある情報の保存性が確保されていること。 ○　法令に定める保存期間内、復元可能な状態で保存すること。 （施行通知　第二　2（3）③） （略） **7.4　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** （略） **C. 最低限のガイドライン** （略） **（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。** 1～2（略） 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に留意しながら適切に対策を講じる必要がある。 （略）

改正案	現　行
8.1.1　電子保存の 3 基準の遵守	**8.1.1　電子保存の 3 基準の遵守**
（略）	（略）
C．最低限のガイドライン	**C．最低限のガイドライン**
（1）電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保	**（1）電気通信回線や外部保存を受託する機関の障害等に対する真正性の確保**
①～②（略）	①～②（略）
③　　リモートログイン制限機能を制限すること 保守目的等のどうしても必要な場合を除き、リモートログインが行なえないように適切に管理されたリモートログインのみに制限する機能を設けなければならない。	**③　　リモートログイン制限機能を制限すること** 保守目的等のどうしても必要な場合を除き、リモートログインが行なえないように適切に管理されたリモートログインのみに制限する機能を設けなければならない。
なお、これらの具体的要件については、「6.10　外部と診療情報等を含医療情報を交換する場合の安全管理　B-2．医療機関等における留意事項」を参照されたい。	
（2）～（3）（略）	**（2）～（3）**（略）
8.1.3　個人情報の保護	**8.1.3　個人情報の保護**
（略）	（略）
B．考え方	**B．考え方**
個人情報保護法が成立し、医療分野においても「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」が策定された。医療	個人情報保護法が成立し、医療分野においても「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」が策定された。医療

において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイドラインを参照し、十分な安全管理策を実施することが必要である。 診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、電気通信回線を通じて外部に保存する場合、委託元の医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶために、より一層の個人情報保護に配慮が必要である。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存の受託先機関との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。 電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては［6.10 章　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-3. 選択すべきネットワークのセキュリティの考え方］でも触れた通り、専用線等であっても十分な注意を払う必要がある。従って、電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。	において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイドラインを参照し、十分な安全管理策を実施することが必要である。 診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、電気通信回線を通じて外部に保存する場合、委託元の医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶために、より一層の個人情報保護に配慮が必要である。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存の受託先機関との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。 電気通信回線を通過する際の個人情報保護は、通信手段の種類によって、個別に考える必要がある。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。従って、電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。
C．最低限のガイドライン	**C．最低限のガイドライン**
（1）診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護	**（1）診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護**
①（略）	①（略）
②　通信の起点・終点識別のための認証をおこなうこと 外部保存を委託する医療機関等と受託する機関間の起点・終点の正当性を識別するために相互に認証を行うこと。 通信手段によって、起点･終点の識別方法は異なる。例えば､インターネットを用いる場合は起点･終点の識別は IP パケットを見るだけで	**②　通信の起点・終点識別のための認証をおこなうこと** 外部保存を委託する医療機関等と受託する機関間の起点・終点の正当性を識別するために相互に認証を行うこと。 通信手段によって、起点･終点の識別方法は異なる。例えば､インターネットを用いる場合は起点・終点の識別は IP パケットを見るだけで

は確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の医療機関等と受託先の機関を確実に相互に認証しなければならない。例えば、認証付きの VPN、SSL/TLS や ISCL を適切に利用することにより実現できる。 当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。 なお、情報の暗号化、ネットワーク回線における留意事項等の具体的要件については、「6.10　外部と診療情報等を含む医療情報を交換する場合の安全管理」の「B-2.医療機関等における留意事項」および「B-3.選択すべきネットワークのセキュリティの考え方」を参照されたい。	は確実にはできない。起点・終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で委託元の医療機関等と受託先の機関を確実に相互に認証しなければならない。例えば、認証付きの VPN、SSL/TLS や ISCL を適切に利用することにより実現できる。 なお、当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。
（2）～（3）（略）	**（2）～（3）**（略）
8.1.4　責任の明確化	**8.1.4　責任の明確化**
（略）	（略）
B．考え方	**B．考え方**
診療録等を電気通信回線等を通じて外部に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は、保存義務のある医療機関等にある。 ただし、管理責任や説明責任は、実際の管理や説明の一部について、受託先の機関やネットワーク管理者、機器やソフトウェアの製造業者と責任を分担することができ、この場合、一般にネットワークで結合されたシステムでは管理境界や責任限界が自明でない場合が多いことから、文書等により、その責任分担を明確にしなければならない。 結果責任は、患者に対しては委託元の医療機関等が負うが、受託先の機関やこれらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの	診療録等を電気通信回線等を通じて外部に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は、保存義務のある医療機関等にある。 ただし、管理責任や説明責任は、実際の管理や説明の一部について、受託先の機関やネットワーク管理者、機器やソフトウェアの製造業者と責任を分担することができ、この場合、一般にネットワークで結合されたシステムでは管理境界や責任限界が自明でない場合が多いことから、文書等により、その責任分担を明確にしなければならない。 結果責任は、患者に対しては委託元の医療機関等が負うが、受託先の機関やこれらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの

製造業者は、委託元の医療機関等に対して契約等で定められた責任を負うことは当然であり、法令に違反した場合はその責任も負うことになる。 　なお、これら責任分界点の考え方については、「6.10　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-1. 責任分界点の明確化」も併せて参照されたい。 （略）	製造業者は、委託元の医療機関等に対して契約等で定められた責任を負うことは当然であり、法令に違反した場合はその責任も負うことになる。 （略）

改正案	現　行
10.　運用管理について （略） **B. 考え方** 運用管理規程には、システムの導入に際して、「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基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。 医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の 6 章から 9 章の記載に従い、定めるべき管理項目を記載してある。(1) に電子保存する・しないに拘らず必要な一般管理事項を、(2) に電子保存の為の運用管理事項を、(3) に外部保存のための運用管理事項を、(4) にスキャナ等を利用した電子化、そして終わりに運用管理規程の作成にあたっての手順を記載している。 電子保存を行う医療機関等は (1) (2) (4) の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに (3) の管理事項を合わせて採用する必要がある。 **C. 最低限のガイドライン** 以下の項目を運用管理規程に含めること。本指針の 6 章から 9 章において「推奨」に記されている項目は省略しても差し支えない。 **(1) 一般管理事項** ①　(略)	**10.　運用管理について** （略） **B. 考え方** 運用管理規程には、システムの導入に際して、「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基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。 医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の 6 章から 9 章の記載に従い、定めるべき管理項目を記載してある。(1) に電子保存する・しないに拘らず必要な一般管理事項を、(2) に電子保存の為の運用管理事項を、(3) に外部保存のための運用管理事項を、そして終わりに運用管理規程の作成にあたっての手順を記載している。 電子保存を行う医療機関等は (1) (2) の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに (3) の管理事項を合わせて採用する必要がある。 **C. 最低限のガイドライン** 以下の項目を運用管理規程に含めること。本指針の 6 章から 9 章において「推奨」に記されている項目は省略しても差し支えない。 **(1) 一般管理事項** ①　(略)

② 管理体制 a) システム管理者、機器管理者、運用責任者の任命 b) 作業担当者の限定 c) マニュアル・契約書等の文書の管理 d) 監査体制と監査責任者の任命 e) 苦情の受け付け窓口の設置 f) 事故対策 g) 利用者への周知法	② 管理体制 a) システム管理者、運用責任者の任命 b) 作業担当者の限定 c) マニュアル・契約書等の文書の管理 d) 監査体制と監査責任者の任命 e) 苦情の受け付け窓口の設置 f) 事故対策 g) 利用者への周知法
③ 管理者及び利用者の責務 a) システム管理者や機器管理者、運用責任者の責務 b) 監査責任者の責務 c) 利用者の責務	③ 管理者及び利用者の責務 a) システム管理者や運用責任者の責務 b) 監査責任者の責務 c) 利用者の責務
④ 一般管理における運用管理事項 a) 来訪者の記録・識別、入退の制限等の入退管理 b) 情報保存装置、アクセス機器の設置区画の管理・監視 c) 委託契約における安全管理に関する条項 d) 個人情報の記録媒体の管理（保管・授受等） e) 個人情報を含む媒体の廃棄の規程 f) リスクに対する予防、発生時の対応 g) 情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理利用者識別と認証、アクセス権限管理、アクセスログ取得と監査、時刻同期、ウイルス等不正ソフト対策	④ 一般管理における運用管理事項 a) 来訪者の記録・識別、入退の制限等の入退管理 b) 情報システムへのアクセス制限、記録、点検等のアクセス管理 c) 委託契約における安全管理に関する条項 d) 個人情報の記録媒体の管理（保管・授受等） e) 個人情報を含む媒体の廃棄の規程 f) リスクに対する予防、発生時の対応 （新設）
⑤ 教育と訓練 a) マニュアルの整備 b) 定期または不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修	⑤ 教育と訓練 a) マニュアルの整備 b) 定期または不定期なシステムの取扱い及びプライバシー保護に関する研修

c) 従業者に対する人的安全管理措置 ・ 医療従事者以外との守秘契約 ・ 従事者退職後の個人情報保護規程	c) 従業者に対する人的安全管理措置 ・ 医療従事者以外との守秘契約 ・ 従事者退職後の個人情報保護規程
⑥ （略）	⑥ （略）
⑦ 監査 a) 監査の内容 b) 監査責任者の任務 c) アクセスログの監査	**⑦ 監査** a) 監査の内容 b) 監査責任者の任務
⑧ 災害等の非常時の対応 a) BCP の規定における医療情報システムの項 b) システムの縮退運用規定 c) 非常時の機能と運用規定 d) 報告先と内容一覧	（新設）
⑨ 外部と医療情報を交換する場合 a) 安全を技術的、運用的面から確認した文書の管理 b) リスク対策の検討文書の管理 c) 責任分界点を定めた契約文書の管理 d) リモート保守への基本方針	（新設）
⑩ 規定の見直し 運用管理規定の定期的見直し手順	（新設）
(2) 電子保存の為の運用管理事項 ①～④ （略）	**(2) 電子保存の為の運用管理事項** ①～④ （略）
（**(4)** へ）	**⑤ スキャナ読み取り書類の運用**

	a）スキャナ読み取り電子情報と元の文書等との同一性を担保する情報作成管理者の任命 スキャナ読み取り電子情報への作業責任者(実施者または管理者)の電子署名法に適合した電子署名 b）スキャナ読み取り電子情報への正確性な読みとり時刻の付加
(3)（略）	**(3)**（略）
(4)　スキャナ等により電子化して保存する場合	（新設）
①　スキャナ読み取りの対象文書の規程	((2)⑤から）
②　スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	((2)⑤a）から）
③　スキャナ読み取り電子情報への作業責任者(実施者または管理者)の電子署名及び認証業務に関する法律(電子署名法)に適合した電子署名	((2)⑤a）から）
④　スキャナ読み取り電子情報への正確性な読みとり時刻の付加	((2)⑤b）から）
⑤　過去に蓄積された文書を電子化する場合の、実施手順規程	（新設）
（略）	（略）