「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 I T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。