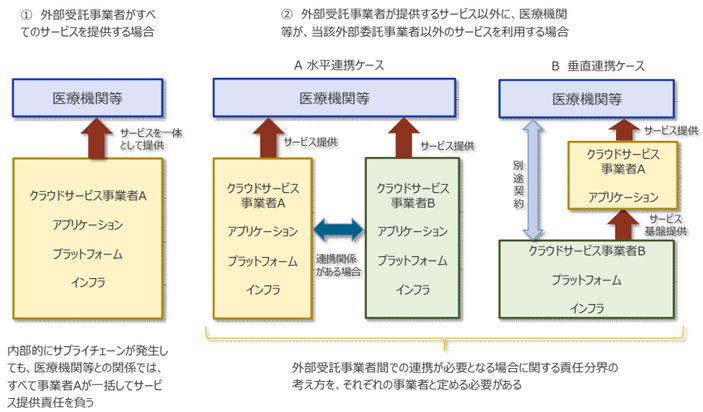
医療情報システムの安全管理に関するガイドライン改定素案　新旧対照表

（取消線は削除部分、赤字は追記部分）　**（※）以下の表は、主な修正のみ記載（表現の修正に伴う変更については含まない）**

5.0 版における記載(ページ数は第 5 版のもの)	5.1 版における記載（ただし表現の修正に伴う変更については含まない）	変更理由
4.3　例示による責任分界点の考え方の整理 (4)　　オンライン外部保存を委託する場合(P30) 委託先が医療機関等、行政機関、又は民間事業者であるかによって要件は異なるので、本ガイドラインの「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」を十分理解して委託先の選定と適切な契約を結ぶ必要がある。患者等に対する責任の主体は委託を行う医療機関等であり、医療機関等が説明責任を果たすための資料や説明の提供を委託契約で定め、医療機関等としても理解する努力は必要である。さらにネットワーク事業者と外部保存を受託する事業者は異なることが多いが、障害が起こった際の対処の責任範囲についても、明確に定めた上で、医療機関等が理解しておく必要がある。 さらに委託先に対する監督も必須であり、定期的に安全管理に関する状況の報告を受ける必要がある。	**4.3　例示による責任分界点の考え方の整理** (4)　　オンライン外部保存を委託する場合(P32) ~~委託先が医療機関等、行政機関、又は民間事業者であるかによって要件は異なるので、~~本ガイドラインの「8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」を十分理解して委託先の選定と適切な契約を結ぶ必要がある。患者等に対する責任の主体は委託を行う医療機関等であり、医療機関等が説明責任を果たすための資料や説明の提供を委託契約で定め、医療機関等としても理解する努力は必要である。さらにネットワーク事業者と外部保存を受託する事業者は異なることが多いが、障害が起こった際の対処の責任範囲についても、明確に定めた上で、医療機関等が理解しておく必要がある。 さらに委託先に対する監督も必須であり、定期的に安全管理に関する状況の報告を受ける必要がある。 医療情報システムにおいても、アプリケーションの稼働に必要な情報システムのすべてを医療機関等の内部で保有する、いわゆるオンプレミスばかりではなく、クラウドサービスを利用するケースも増えている。クラウドサービスは、受託事業者等によって提供されるサービスで、利用者が情報システム及びこれに必要な機器を保有することなく、ネットワーク経由で事業者が提供する情報システムにアクセスし、必要な処理や、データ保管等の管理を行うものである。医療情報においても、外部保存を行うほか、必要な情報処理を行うのに用いることができる。 クラウドサービスを利用する場合には、情報システムの整備や運用は、受託事業者経由で行うことになるほか、サービスの性格上、共同利用型となる。そのため、医療情報システムの管理監督や責任分界においても、このような特性を踏まえた管理方法による取決めを行う必要がある。 外部保存を受託事業者が1社ではなく複数の事業者を通じて行われることもある。この場合には障害や情報漏洩等の事故が生じた場合に、責任分界を明瞭にしておかないと、原因の特定や対策などが遅滞する危険性がある。 下図の②の場合は、医療機関等が複数の事業者と外部保存に関する契約を行う例であるが、障害等の非常時が発生した場合に、最初に原因調査の範囲を決める責任を負う主体や、原因調査に必要な調査協力義務などについての役割、範囲等をそれぞれの事業者と取り決めておくことが求められる。また、複数事業者の提供サービス内容や契約内容を合わせて、本ガイドラインの要求に漏れが無く適合	・8.1.2 において行政機関が設置するデータセンターと民間事業者が設置するデータセンターの選定基準の統合に伴う措置 ・クラウドサービスに関する追記 ・サプライチェーン型サービスを利用する場合の責任分界の考え方を追記

	している ことの確認が必要である。  	
6.2.3 リスク分析(P42) 分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼に基づいて業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、例え起こり得る可能性は低くても、万一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析により得られた脅威に対して、6.3 章～6.12 章の対策を行うことになる。 また、情報の安全管理や、個人情報保護法で原則禁止されている目的外利用の防止は、システム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障することであり、これが限界である。従って、人の行為も含めた脅威を想定し、運用管理規程を含めた対策を講じることが重要である。 医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データの保護に関してだけでなく、入出力の際に露見等の脅威にさらされるおそれのある個人情報を保護するための方策についても考える必要がある。以下に様々な状況で想定される脅威を列挙する。	6.2.3 リスク分析(P46) 分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼に基づいて業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、例え起こり得る可能性は低くても、万一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析により得られた脅威に対して、6.3 章～6.12 章の対策を行うことになる。 また、情報の安全管理や、個人情報保護法で原則禁止されている目的外利用の防止は、システム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障することであり、これが限界である。従って、人の行為も含めた脅威を想定し、運用管理規程を含めた対策を講じることが重要である。加えて、この観点から、組織が管理しない機器やソフトウェア、サービスの利用を禁止することが求められる。 医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データの保護に関してだけでなく、入出力の際に露見等の脅威にさらされるおそれのある個人情報を保護するための方策についても考える必要がある。以下に様々な状況で想定される脅威を列挙する。	・許可されない機器やソフトウェア、サービス（許可のない BYOD や、シャドウ IT 等）の利用禁止を追記
6.2.3 リスク分析(P42) ①　～　⑥　抄 ⑦　医療情報システム (a)　抄 (b)　非意図的要因による IT 障害	6.2.3 リスク分析(P47) ①　～　⑥　抄 ⑦　医療情報システム (a)　～ (c)　抄 (b)　非意図的要因による IT 障害等	・リスクアセスメントの脅威の対象に、外部サービス利用に伴うシステムポリシーの意図しない変更や、許可されていない情報システムの利用について追記

・システムの仕様やプログラム上の欠陥（バグ） ・操作ミス ・故障 （c） 抄	・システムの仕様やプログラム上の欠陥（バグ） ・操作ミス ・故障 ・外部サービスの利用に伴うシステムポリシー等の意図しない変更 （c） 抄 （d）許可されていない情報システムの利用 ・許可されていない機器、ソフトウェア、サービスの業務利用 ・管理されている機器、ソフトウェア、サービスの目的外利用	
6.4 物理的安全対策（P47） B. 考え方 物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義し、以下の事項を考慮して、適切に管理する必要がある。 ・ 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ・ 盗難、覗き見等の防止 ・ 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置	**6.4 物理的安全対策（P52）** B. 考え方 物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義し、以下の事項を考慮して、適切に管理する必要がある。 ・ 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ・ 盗難、覗き見等の防止 ・ 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置 また、情報システムを格納するデータセンター等の場所については、6.2.3 章のリスク分析を踏まえて、適切に選定することが重要である。	・データセンターの適切な選定を物理的セキュリティに入れるため追記
6.5 技術的安全対策 **(1) 利用者の識別及び認証** ＜認証強度の考え方＞（P49） ID・パスワードの組み合わせは、これまで広く用いられてきた方法である。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務付ける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。 このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。 認証に用いる手段としては、ID・パスワードの組み合わせのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つ	**6.5 技術的安全対策** **(1) 利用者の識別及び認証** ＜認証強度の考え方＞（P55） ID・パスワードの組み合わせは、これまで広く用いられてきた方法である。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務付ける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。 このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。 認証に用いる手段としては、ID・パスワードの組み合わせのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つこ	・2 要素認証導入の期限を明示 ・今後導入等の検討を予定するシステムにおいて、2 要素認証を採用することの明示 ・2 要素認証と 2 段階認証の違いを明確化するため追記

ことは一般には困難である。そこで、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）を採用することが望ましい。 現状において、医療情報システムにアクセスする端末ごとに 2 要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる。※ ※ 認証技術の端末等への実装状況等を鑑み、本ガイドライン第 5 版の公表から約 10 年後を目途に「C. 最低限のガイドライン」とすることを想定する。 また、例えば、放射線管理区域のモダリティを扱う又は薬局において薬歴の参照・入力を行う場合等において、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。 シングル・サインオン方式を用いて、一度の認証により複数のアプリケーションを操作する場合であっても、最初のログイン時に 2 要素認証を行っていれば、セキュリティは担保されていると考えられる。 ただし、ログイン状態のまま長時間放置したり、特定の端末でログインしただけで、院内の複数の端末にログイン可能となるような運用は認められない。 入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。 なお、パスワードの定期的な変更を強制することにより、「C. 最低限のガイドライン」における「類推しやすいパスワードを使用しない」という要件を満たさないことになるリスクが指摘されている。しかしながら、患者情報を取り扱う医療情報システムの性格に鑑み、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが必要である。ただし、2 要素認証を採用している場合、必ずしもパスワードの定期的な変更は求められない。	とは一般には困難である。そこで、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カード、ID・パスワード＋バイオメトリクスのように 2 つの独立した要素を用いて行う方式（二要素認証）を採用することが望ましい。 現状において、医療情報システムにアクセスする端末ごとに 2 要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる。※ ※ 二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、導入または更新する場合、原則として二要素認証を採用することが求められる。 また、例えば、放射線管理区域のモダリティを扱う又は薬局において薬歴の参照・入力を行う場合等において、情報システムを利用する端末に二要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、二要素認証~~と同等~~に相当すると考えてよい。と考えてよい。 なお、認証に際して、二段階で認証を行う二段階認証と呼ばれる方法があるが、この場合には利用される認証要素が同一となることもあるため、実質的にリスク低下につながらないこともある。そのため二段階認証を選択するだけでは二要素認証の要求を満たさないと考えるべきである。 シングル・サインオン方式を用いて、一度の認証により複数のアプリケーションを操作する場合であっても、最初のログイン時に 2 要素認証を行っていれば、セキュリティは担保されていると考えられる。 ただし、ログイン状態のまま長時間放置したり、特定の端末でログインしただけで、院内の複数の端末にログイン可能となるような運用は認められない。 入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。 なお、パスワードの定期的な変更を強制することにより、「C. 最低限のガイドライン」における「類推しやすいパスワードを使用しない」という要件を満たさないことになるリスクが指摘されている。しかしながら、患者情報を取り扱う医療情報システムの性格に鑑み、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが必要である。ただし、2 要素認証を採用している場合、必ずしもパスワードの定期的な変更は求められない。	
(2) 情報の区分管理とアクセス権限の管理(P51) 情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ	**(2) 情報の区分管理とアクセス権限の管理(P58)** 情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ	・クラウドサービス等を使う際に、システムポリシーの自動変更が生じた場合の検知等の必要性について追記

（業務単位等）ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。 知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定を行う機能があれば、さらにリスクを低減できる。 アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行う必要があり、組織の規程で定めなければならない。	（業務単位等）ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。 知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定を行う機能があれば、さらにリスクを低減できる。 アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行う必要があり、組織の規程で定めなければならない。 また、クラウドサービスを利用する場合、利用するサービスによっては、医療機関等の規程に基づいて定めたシステム上の設定（ポリシー）が、デフォルトの設定となる等、自動的に意図しない内容に変更されてしまう危険性がある。これにより、アクセス権限等が変更され、医療情報が意図しない相手先に送付されるなどのリスクが想定される。このような状況を防ぐため、設定の変更に関して検知できる措置を講じることが求められる。特に自動的に検知し、運用に反映できることが必要となる。	
(3)　アクセスの記録（アクセスログ）(P52) 個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。 アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であることから、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。 また、アクセスログの証拠性確保のために、記録する時刻は重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取らなければならない。 なお、医療機関等において取り扱っている医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理する必要がある。	**(3)　アクセスの記録（アクセスログ）(P58)** 個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。 アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であることから、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。 また、アクセスログの証拠性確保のために、記録する時刻は重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取らなければならない。 加えて、ログを分析し、緊急時にアラートを発する仕組みを講じることも求められる。 情報システムの管理を事業者に委託している場合には、ログの管理方法や提供等に関して、明確にする必要がある。 なお、医療機関等において取り扱っている医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理する必要がある。	・外部事業者がログ管理をしている場合の保存に関する責任を明示するため追記
(5)　ネットワーク上からの不正アクセス(P53) ネットワークからのセキュリティでは、クラ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の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」、「ステートフルインスペクション」等の各種方式がある。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導入すれば安心というもので	**(5)　ネットワーク上からの不正アクセス(P59)** ネットワークからのセキュリティでは、クラ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の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」、「ステートフルインスペクション」等の各種方式がある。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導入すれば安心というもので	・内部に侵入した不正なパケット等を監視するための内部脅威監視についての考え方を追記 ・複数拠点にある無線 LAN に関して、なりすまし防止を特に加える旨を追記（D 項にある考え方の移動）

はない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処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。このことは、医療機関等の外部から医療機関等の情報システムに接続される PC 等の情報端末に対しても同様であるが、その考え方と対策については、「6.9　情報及び情報端末の持ち出しについて」を参照されたい。 不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、医療情報システムと外部ネットワークとの関係に応じて、IDS の採用も検討すべきである。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ことも重要である。 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（サービス不能攻撃 DoS：Denial of Service 等）を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて 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、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の盗聴を防止するために、暗号化等による“情報漏えい”への対策も必要となる。	はない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処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。このことは、医療機関等の外部から医療機関等の情報システムに接続される PC 等の情報端末に対しても同様であるが、その考え方と対策については、「6.9　情報及び情報端末の持ち出しについて」を参照されたい。 不正な攻撃を検知するシステム（IDS：Intrusion Detection System）、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）もあり、医療情報システムと外部ネットワークとの関係に応じて、IDS、IPS の採用も検討すべきである。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ことも重要である。 さらに、近時のサイバー攻撃の高度化・多様化に鑑みると、上記対策等に加えて、コンピュータウイルス等が侵入した場合を想定した内部脅威監視などのモニタリングを講じることも、有効な対策として挙げられる。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。 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（サービス不能攻撃 DoS：Denial of Service 等）を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて 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、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。無線 LAN のアクセスポイントを複数設置して運用する場合等、マネジメントの複雑さが増し、侵入の危険が高まるような設置をする場合には、一層留意が必要である。 また、ネットワーク上を流れる情報の盗聴を防止するために、暗号化等による“情報漏えい”への対策も必要となる。	
(6)　医療等分野における IoT 機器の利用（P53） 「近年、様々なモノがネットワークに繋がることで新たなサービス等を実現する～患者等に説明する必要がある。」略 IoT 機器には、機器やサービスの導入後に脆弱性が発見されることがあるので、サービスへの提供に支障が生じないよう適切な時期・方法により対策を講じる必要がある。 また、IoT の活用状況によって、大量の IoT 機器が同時に接続している環境が想定	**(6)　医療等分野における IoT 機器の利用（P60）** 「近年、様々なモノがネットワークに繋がることで新たなサービス等を実現する～患者等に説明する必要がある。」略 IoT 機器には、機器やサービスの導入後に脆弱性が発見されることがあるので、サービスへの提供に支障が生じないよう適切な時期・方法により対策を講じる必要がある。脆弱性に関しては、IoT 機器が用いる通信規格（例:Bluetooth、NFC 等）の脆弱性についても、併せて対応することが望ましい。	・Bluetooth 等近距離無線通信に関するセキュリティ上の考え方を明示するために追記

されるが、この場合、機器の接続状況や異常の発生を正確に把握することが難しい。IoT 機器を含むシステムが単独でそれぞれの状態を把握できることが望ましいが、機器・システムの中には、大量のログを管理したり、ログの暗号化を行う等の対策を講じることが難しい場合がある。この場合、上位のシステムに監視装置を設置する等、システムやサービス全体での対策が検討される。 このほか、IoT のリスクとして、使用を終えた又は停止した機器をネットワークに接続した状態のままにしておくと、利用者さえ気付かない間に当該機器が不正に接続される場合がある。IoT 機器のネットワーク接続状況を監視する等の対策も考えられるが、使用を終えた又は停止した機器は電源を切り、接続を遮断する等、運用面での対策も可能である。 IoT の更なる普及によって、活用方法の多様化や安全性に対する脅威やその対策に係る技術的変化が進み、医療等分野のセキュリティに大きな影響を及ぼす可能性がある。医療機関等においても、今後の動向に注意を払う必要がある。	また、IoT の活用状況によって、大量の IoT 機器が同時に接続している環境が想定されるが、この場合、機器の接続状況や異常の発生を正確に把握することが難しい。IoT 機器を含むシステムが単独でそれぞれの状態を把握できることが望ましいが、機器・システムの中には、大量のログを管理したり、ログの暗号化を行う等の対策を講じることが難しい場合がある。この場合、上位のシステムに監視装置を設置する等、システムやサービス全体での対策が検討される。 このほか、IoT のリスクとして、使用を終えた又は停止した機器をネットワークに接続した状態のままにしておくと、利用者さえ気付かない間に当該機器が不正に接続される場合がある。さらに、機器の利用状況に関する情報を収集し、不正に利用者を特定される等のリスクも想定される。 IoT 機器が通信で用いる PAN（Personal Area Network）※と呼ばれる Bluetooth や Zigbee などの 802.15.XX の標準による規格、NFC（Near Field Communication）、赤外線通信などを用いた規格においては、必ずしも十分通信の暗号化対策が取られているわけではないため、技術的な対応に限界があるとされる。IoT 機器のネットワーク接続状況を監視する等の対策も考えられるが、使用を終えた又は停止した機器は電源を切り、接続を遮断する~~等~~、不要な接続は行わない等、運用面での対策も可能である。 ※人体表面や周辺においてデータをやり取りする通信距離の極めて短いワイヤレスネットワークである BAN（Body Area Network）を含めた広義の意味で、PAN という表現が用いられることもある。 IoT の更なる普及によって、活用方法の多様化や安全性に対する脅威やその対策に係る技術的変化が進み、医療等分野のセキュリティに大きな影響を及ぼす可能性がある。医療機関等においても、今後の動向に注意を払う必要がある。	
6.5　技術的安全対策 **C. 最低限のガイドライン(P55)** 1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。 2. 本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 3. 本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。 4. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防止策を講じること。 5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。 6. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、その	**6.5　技術的安全対策** **C. 最低限のガイドライン(P62)** 1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。 2. 本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 3. 本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。 4. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防止策を講じること。 5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。 6. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、その	・今後新規導入する、あるいは更新を図る医療情報システムについては、二要素認証を採用するものを導入する旨を追記

レベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。 7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。 8. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。 9. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。 10. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。 11. パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはなら	レベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。 7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。 8. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。 9. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。 10. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。 11. パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはなら	

ない)。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し(最長でも2ヶ月以内　※D.5に規定する2要素認証を採用している場合を除く。)、極端に短い文字列を使用しないこと。英数字、記号を混在させた8文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。 12. 無線LANを利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY接続拒否等の対策を行うこと。 (2) 不正アクセスの対策を施すこと。少なくともSSIDやMACアドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えばWPA2/AES等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線LANを利用するために」や「企業等が安心して無線LANを導入・運用するために」を参考にすること。 13.　IoT機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。 (4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対	ない)。 (4)　令和９年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新する際には、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し(最長でも2ヶ月以内　※D.5に規定する二要素認証を採用している場合を除く。)、極端に短い文字列を使用しないこと。英数字、記号を混在させた8文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。 12. 無線LANを利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY接続拒否等の対策を行うこと。 (2) 不正アクセスの対策を施すこと。少なくともSSIDやMACアドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えばWPA2~~/AES~~ -AES、WPA2-TKIP等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線LANを利用するために」や「企業等が安心して無線LANを導入・運用するために」を参考にすること。 13.　IoT機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を	

策を講じること。	検討し、適用すること。 (4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。	
6.5　技術的安全対策 **D. 推奨されるガイドライン(P57)** 1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。 2. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等)。 3. 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やそれと同等の機能を含む。）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。 4. パスワードを利用者識別に使用する場合、以下の基準を遵守すること。 (1) パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 (2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。 5. 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又は IC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。 6. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。 7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。	**6.5　技術的安全対策** **D. 推奨されるガイドライン(P65)** 1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。 2. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等)。 3. 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やそれと同等の機能を含む。）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。 4. パスワードを利用者識別に使用する場合、以下の基準を遵守すること。 (1)　パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。 (2)　パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。 5. 認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又は IC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証に相当する~~と同等~~と考えてよい。 6. 許可された者以外の無線 LAN の利用を防止するため、~~無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、~~例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。 7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。	・無線 LAN で電子証明書と組み合わせて用いるべきケースを拡大
6.10.　災害、サイバー攻撃等の非常時の対応(P70)	**6.10.　災害、サイバー攻撃等の非常時の対応(P79)** (4) 非常時に備えたセキュリティ体制の整備（新設） 非常時やサイバー攻撃などに対して、的確に対応できるためにセキュリティ体制を医療機関等においても構築することが求められる。非常時等において必要な	・非常時のセキュリティ体制を整備する必要性の明示 ・一定規模の医療機関等における CISO や CSIRT 設置の推奨

	原因関係の調査、必要なセキュリティ対応等に関する指揮、所管官庁等への報告などの体制については、平常時から明確にする必要がある。 　また、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなどが強く求められる。	
6.10　災害、サイバー攻撃等の非常時の対応 **C. 最低限のガイドライン(P71)** 1. 医療サービスを提供し続けるための 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. 非常時の情報システムの運用 ・「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ることがないようにして、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。 ・非常時用ユーザアカウントが使用された場合、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。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。 4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先　厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先　情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	**6.10　災害、サイバー攻撃等の非常時の対応** **C. 最低限のガイドライン(P79)** 1. 医療サービスを提供し続けるための 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. 非常時における対応に関する教育及び訓練を従業者に対して行うこと。なお、医療情報システムの障害時の対応についても同様に行うこと。 3. 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。 4. 非常時の情報システムの運用 ・「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ることがないようにして、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。 ・非常時用ユーザアカウントが使用された場合、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。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。 ~~5. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。~~ コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発 1029 第１号　医政地発 1029 第３号　医政研発 1029 第１号　平成 30 年 10 月 29 日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。	・非常時のための訓練、教育について明示 ・サイバー攻撃を受けた場合の報告等について、直近の通知に基づいて実施すべき旨を明示

	厚生労働省 連絡先　URL　https://~~厚生労働省 医政局研究開発振興課医療技術情報推進室 (03-3595-2430)~~ ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先　情報処理推進機構 情報セキュリティ安心相談窓口 (03-5978-7509)	
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 **B-1. 医療機関等における留意事項**	**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** **B-1. 医療機関等における留意事項** **④　暗号化を行うための適切な鍵管理(P84)　(新設)** 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、Level 1 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 Level 1 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))	・鍵管理の考え方について追記
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 **B-2. 選択すべきネットワークのセキュリティの考え方**	**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** **B-2. 選択すべきネットワークのセキュリティの考え方**	・ISDN サービス終了に関する注記を追記

Ⅰ．クローズドなネットワークで接続する場合(P77) **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、大量の情報若しく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。	**Ⅰ．クローズドなネットワークで接続する場合(P87)** **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、大量の情報若しく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。 ※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-VPN変換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などによる例がある。	
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 **B-2．選択すべきネットワークのセキュリティの考え方** **Ⅱ．オープンなネットワークで接続されている場合（P79）** 「いわゆるインターネットによる接続形態である。(P79)～ネットワークの分離やこれを踏まえた情報交換のルールを踏まえた管理を行うことが望ましい。(P80)」　略 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、SSL/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	**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** **B-2．選択すべきネットワークのセキュリティの考え方** **Ⅱ．オープンなネットワークで接続されている場合（P90）** 「いわゆるインターネットによる接続形態である。(P91)～ネットワークの分離やこれを踏まえた情報交換のルールを踏まえた管理を行うことが望ましい。」　略 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、SSL/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	・オープンネットワークからデータを取り込む際の対応についての考え方を追記 ・クラウドサービスの種類等に応じたネットワーク分離の必要性等について追記

	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。	
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 **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(P86)** 「診療情報等の開示が進む中（P86)、～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。(P87)」略 　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 TLS 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。	**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** **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(P100)** 「診療情報等の開示が進む中、～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。」略 　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 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。 　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。	・患者の依頼により医療情報を患者が利用する事業者に送付等する際の医療機関等の責務や責任分界の取決めの必要性について追記
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 **C. 最低限のガイドライン(P89)**	**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** **C. 最低限のガイドライン(P102)(新設)** 11.　電子署名に用いる秘密鍵の管理は、認証局が定める「証明書ポリシー」(CP)等で定める鍵管理の要件を満たして行うこと。	・電子署名に用いる暗号鍵管理について追記
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	**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**	・共通鍵、秘密鍵等を管理する媒体等

D. 推奨されるガイドライン(P90)	D. 推奨されるガイドライン(P103)（新設） 2. 共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-2 レベル 1 相当以上の対応を図ること。	に係る安全管理要件を追記
8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 B. 考え方 1. 外部保存を受託する機関の選定基準(P114) ② 行政機関等が開設したデータセンター等に保存する場合 国の機関、独立行政法人、国立大学法人、地方公共団体等が開設したデータセンター等に保存する場合が該当する。 この場合、本章の他の項の要求事項、本ガイドラインの他の章で言及されている責任のあり方、安全管理対策、真正性、見読性、保存性及び C で定める情報管理体制の確保のための全ての要件を満たす必要がある。 ③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 ①及び②以外の機関が医療機関等の委託を受けて情報を保存するデータセンター等が該当する。 この場合、法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要がある。 そのため、それらの事業者等が、本章の他の項の要求事項、本ガイドラインの他の章で言及されている、責任のあり方、安全管理対策、真正性、見読性、保存性及び C で定める情報管理体制の確保のための全ての要件を満たす必要がある。 また、それらのサービス形態によって、経済産業省の定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の要求事項も満たす必要がある。	8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準 B. 考え方 1. 外部保存を受託する事業者の選定基準(従来の②および③を統合）（P126）（下線は新規に加えた内容） ② 医療機関等以外の外部の機関に対して契約に基づいて確保した安全な場所に保存する場合 ①以外の機関が医療機関等の委託を受けて情報を保存するデータセンター等が該当する。 法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要がある。 また、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の要求事項も満たす必要がある。 なお、選定にあたっては、外部委託事業者のセキュリティ対策状況を確認することが必要である。例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」や『製造業者による医療情報セキュリティ開示書』ガイド（Ver.3.0a）によって、外部保存を受託する事業者におけるセキュリティ対応状況の概要を確認することができるため、サービスの性質等、必要に応じてその提供を求めることなどの有効である。 外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、所管する行政機関の調査等に供するため、提出等を行う必要が生じうることから、これを円滑に実現できる保存場所であることが求められる。そのため外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められる。	・行政機関が設置するデータセンターと、民間事業者が設置するデータセンターの選定基準の考え方を統合。 ・2 省ガイドライン名を明示 ・事業者のセキュリティ状況を確認するために MDS/SDS を利用することについて追記。 ・外部保存されている医療情報に関する国内法の適用、国外法の不適用に関する考え方を追記
8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 B. 考え方 2. 情報の取扱い(P115) ② 行政機関等が開設したデータセンター等に保存する場合 行政機関等に保存する場合、開設主体者が公務員等の守秘義務が課せられた者であることから、情報の取扱いについては一定の規制が存在する。しかし、保存された情報はあくまで医療機関等から委託を受けて保存しているのであり、外部保存を受託する事業者が独自に分析、解析等を行うことは医療機関等及び患者の	8.1.2 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準 B. 考え方 2. 情報の取扱い(P129)（従来の②および③を統合） ② 医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合 本項で定める外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、不当な営利、利益追求を目的として情報を閲覧、分析等を行うことはあってはならず、許されない。したがって、外部保存を受託する事業者を選	・行政機関が設置するデータセンターと、民間事業者が設置するデータセンターの選定基準の考え方を統合

同意がない限り許されない。 　従って、外部保存を受託する事業者を選定する場合、医療機関等はそれらが実施されないことの確認、若しくは実施させないことを明記した契約書等を取り交わす必要がある。 　また、技術的な方法としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。 　また、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理したり、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつことも考えられる。 ③　医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 　冒頭でも触れたとおり、本項で定める外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、不当な営利、利益追求を目的として情報を閲覧、分析等を行うことはあってはならず、許されない。 　民間等で医療情報の外部保存を受託する事業者に対しては、これらの行為を規制するための指針が外部保存通知にあるとおり経済産業省や総務省で定められている。従って、医療機関等は契約も含め、その遵守状況を十分確認する必要がある。 　外部保存の技術的な方法としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。 　さらに、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、あるいは情報処理関連事業者の管理者といえどもアクセスできない制御機構をもつことも考えられる。 　具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられる。 　この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならない。 　医療機関等が自ら暗号化を行って暗号鍵を保管している場合、火災や事故等で暗号鍵が利用不可能になった場合、全ての保存委託を行っている医療情報が利用不可能になる可能性がある。 　これを避けるためには暗号鍵を外部保存を受託する事業者に預託する、複数の信頼できる他の医療機関等に預託する等が考えられる。分散保管においても同様の可用性の保証が必要である。 　ただし、外部保存を受託する事業者に暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要である。	定する場合、医療機関等はそれらが実施されないことの確認、若しくは実施させないことを明記した契約書等を取り交わす必要がある。 　外部保存の技術的な方法としては、例えばトラブル発生時のデータ修復作業等、緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。 　さらに、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、あるいは情報処理関連事業者の管理者といえどもアクセスできない制御機構をもつことも考えられる。 　具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられる。 　この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならない。 　医療機関等が自ら暗号化を行って暗号鍵を保管している場合、火災や事故等で暗号鍵が利用不可能になった場合、全ての保存委託を行っている医療情報が利用不可能になる可能性がある。 　これを避けるためには暗号鍵を、外部保存を受託する事業者に預託する、複数の信頼できる他の医療機関等に預託する等が考えられる。分散保管においても同様の可用性の保証が必要である。 　ただし、外部保存を受託する事業者に暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要である。 　外部保存を受託する事業者による暗号鍵の不正利用を防止するため、暗号鍵の使用について運用管理規程を策定し、使用を非常時に限定しなければならない。また、実行時に暗号鍵を使用した証跡が残る暗号手法等を利用し、情報システムにおける証跡管理等を適切に実施することで、暗号鍵が不正利用されていないかを確認する必要がある。	

外部保存を受託する事業者による暗号鍵の不正利用を防止するため、暗号鍵の使用について運用管理規程を策定し、使用を非常時に限定しなければならない。また、実行時に暗号鍵を使用した証跡が残る暗号手法等を利用し、情報システムにおける証跡管理等を適切に実施することで、暗号鍵が不正利用されていないかを確認する必要がある。		
8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 **B. 考え方** **3.　情報の提供(P117)** ②　行政機関等が開設したデータセンター等に保存する場合 いかなる形態であっても、保存された情報を外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。 外部保存を受託する事業者を通じて、保存された情報を保存主体の医療機関等以外に提供する場合は、あくまで医療機関等同士の同意の上で実施されなくてはならず、当然、患者の同意も得た上で実施する必要がある。このような場合において、外部保存を受託する事業者がアクセス権の設定を受託しているときは、医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等して、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにしなくてはならない。 従って、このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定する必要がある。 ③　医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 いかなる形態であっても、保存された情報を外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。これは匿名化された情報であっても同様である。 外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関等以外にも提供する場合は、あくまで医療機関等同士の同意で実施されなくてはならず、当然、個人情報保護法に則り、患者の同意も得た上で実施する必要がある。 このような場合において、外部保存を受託する事業者がアクセス権の設定を受託しているときは、医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等して、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにしなくてはならない。	**8.1.2　外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準** **B. 考え方** **3.　情報の提供(P131)（従来の②および③を統合）(下線は新規に加えた内容)** ②　医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合 いかなる形態であっても、保存された情報の外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。匿名化された情報であっても同様である。なお医療機関等が管理する端末等を用いて、医療機関等または患者が患者情報に関するサービスを利用する場合に、受託する事業者においてCookie を取得することがある。Cookie は直ちに個人を特定するものではないため、患者情報には当たらないとされうるものの、第三者提供することにより、患者等が特定されるリスクがあるため、受託する事業者において第三者に提供することは許されない。 外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関等以外にも提供する場合は、あくまで医療機関等同士の同意で実施されなくてはならず、当然、個人情報保護法に則り、患者の同意も得た上で実施する必要がある。 このような場合において、外部保存を受託する事業者がアクセス権の設定を受託しているときは、医療機関等若しくは医療機関等との間で同意を得た患者の求めに応じて適切な権限を設定する等して、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにしなくてはならない。 したがって、このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定しなくてはならない。	・行政機関が設置するデータセンターと、民間事業者が設置するデータセンターの選定基準の考え方を統合 ・事業者が取得したCookie 情報等、患者情報には含まれない患者に関する情報の第三者提供の禁止について追記

従って、このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定しなくてはならない。		
8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 **C. 最低限のガイドライン(P118)** ②　行政機関等が開設したデータセンター等に保存する場合 （ア） 法律や条例により、保存業務に従事する個人若しくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。 （イ） 適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及びCertified Information Systems Auditor （ISACA認定）等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。 （ウ） 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。 （エ） 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。 ③　医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 （ア） 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取扱いに対して監督を行えること。 （イ） 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「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」を遵守していること。 （ウ） 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。	**8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準** **C. 最低限のガイドライン(P133)（下線は新規に加えた内容）** ②　医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合 (ア)保存した情報の取扱いに関して監督できるようにするため、外部保存を受託する事業者及びその管理者、電子保存作業従事者等に対する守秘に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。 (イ)医療機関等と外部保存を受託する事業者を結ぶネットワーク回線に関しては6.11章を遵守させること。 (ウ)総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。 (エ)外部保存を受託する事業者の選定に当たっては、事業者のセキュリティ対策状況を示す資料を確認すること。例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」の提供を求めて、確認することなどが挙げられる。 (オ)外部保存を受託する事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。なお保守に関しては、6.8章を遵守すること。 (カ)保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記するとともに、外部保存を受託する事業者に遵守させること。 (キ)保存した情報を、外部保存を受託する事業者が独自に提供しないように、契約書等で情報提供について定めること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。 (ク)保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。 (ケ)外部保存を受託する事業者を選定する際は、(ア)から(ク)のほか、少なくとも次に掲げる事項について確認すること。 a　医療情報等の安全管理に係る基本方針・取扱規程等の整備状況 b　医療情報等の安全管理に係る実施体制の整備状況 c　実績等に基づく個人データ安全管理に関する信用度	・行政機関が設置するデータセンターと、民間事業者が設置するデータセンターの選定基準の考え方を統合 ・受託事業者におけるセキュリティ情報の確認について追記 ・Cookie等の第三者提供の禁止について追記 ・医療情報を格納する機器についての国内法適用の追記 ・受託事業者における能力判断をするのに必要な認証、あるいはこれに代替する監査について追記 ・受託事業者におけるデータセンターの所在地の確認について追記 ・受託事業者における国外法適用可能性の確認について追記

（エ） 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。 （オ） 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。 （カ） 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。 （キ） 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点について確認すること。 (a) 医療情報等の安全管理に係る基本方針・取扱規程等の整備 (b) 医療情報等の安全管理に係る実施体制の整備 (c) 実績等に基づく個人データ安全管理に関する信用度 (d) 財務諸表等に基づく経営の健全性	d 財務諸表等に基づく経営の健全性 e 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力を有すること ・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7 号） ・AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力を有していることを確認すること。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 f 医療情報を保存する機器が設置されている場所(地域、国) g 受託事業者に対する国外法の適用可能性	
8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 **D. 推奨されるガイドライン(P119)** （ア） 「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、保存を受託した機関全体としてのより一層の自助努力を患者・国民に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークや ISMS 認定等の第三者による認定を取得すること。 （イ） 「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、（ア）で述べた第三者による認定を受けること。 （ウ） 「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	**8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準** **D. 推奨されるガイドライン(P135)** （ア）~~「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、~~保存を受託した~~機関~~事業者全体としてのより一層の自助努力を患者・国民に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークや ISMS 認定等の第三者による認定を取得すること。なお ISMS については、管理しているリスクに応じて、適合性を示す資料の提供を求めること。 ~~（イ）「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、（ア）で述べた第三者による認定を受けること。~~ （イ）~~「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」~~医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	・受託事業者に求められる認証等の一本化、ISMS については適合性情報提出について追記

10　運用管理について B. 考え方(P134) 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 4 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いる。(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) に電子保存のための運用管理事項を、(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、(5) に運用管理規程の作成に当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。	10　運用管理について B. 考え方(P149) 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 4 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いる。(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) に電子保存のための運用管理事項を、(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、(5) に運用管理規程の作成に当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。 運用管理規程等の作成に際しては、以下の文書を参照することが有用である。 ・監査証跡の取り組み方については、「個人情報保護に役立つ監査証跡ガイド」～あなたの病院の個人情報を守るために～（医療情報システム開発センター）を参考にされたい。 ・技術的対応の検討のための情報収集には、6.2 章 B で紹介している「製造業者による医療情報セキュリティ開示書　チェックリスト」を参考にされたい。	・参考のための具体的な文書については、C 項に記載するよりも、B 項の「考え方」に記載する方が適切であるため、移動。
10　運用管理について C. 最低限のガイドライン(P134) (1)　一般管理事項 ①～②　抄 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 ・　監査証跡の取り組み方については、「個人情報保護に役立つ監査証跡ガイド」～あなたの病院の個人情報を守るために～（医療情報システム開発センター）を参考にされたい。 ④一般管理における運用管理事項 a)～f)　抄 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規程システムの導入に際して、技術的に対応するか、運用によって対応するかを判定し、その内容を文書化し管理する旨の規程。 ・　技術的対応の検討のための情報収集には、6.2 章 B で紹介している「製造業者による医療情報セキュリティ開示書　チェックリスト」を参考にされたい。	10　運用管理について C. 最低限のガイドライン(P149) (1)　一般管理事項 ①～②　抄 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 ~~・　監査証跡の取り組み方については、「個人情報保護に役立つ監査証跡ガイド」～あなたの病院の個人情報を守るために～（医療情報システム開発センター）を参考にされたい。~~ ④一般管理における運用管理事項 a)～f)　抄 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規程システムの導入に際して、技術的に対応するか、運用によって対応するかを判定し、その内容を文書化し管理する旨の規程。 ~~・　技術的対応の検討のための情報収集には、6.2 章 B で紹介している「製造業者による医療情報セキュリティ開示書　チェックリスト」を参考にされたい。~~	・参考のための具体的な文書については、C 項に記載するよりも、B 項の「考え方」に記載する方が適切であるため、移動 ・2 省ガイドライン名を明示

h)～k)　抄 **⑤～⑪　抄** **(2)　抄** **(3)　ネットワークによる外部保存に当たっての「医療機関等としての管理事項」** ①　管理体制と責任 a)　委託する事業者選定規約、選定時に「適合」と判断した根拠記載の規程 ・　受託事業者が医療機関等以外の場合には、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」に記された要件を参照されたい。 ・　民間事業者等との契約に基づいて確保した安全な場所に該当する機関を選定する場合には、データセンター等の情報処理関連事業者が経済産業省が定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に準拠していることを確認する規程 **以下　抄**	h)～k)　抄 **⑤～⑪　抄** **(2)　抄** **(3)　ネットワークによる外部保存に当たっての「医療機関等としての管理事項」** ①　管理体制と責任 a)　委託する事業者選定規約、選定時に「適合」と判断した根拠記載の規程 ・　受託事業者が医療機関等以外の場合には、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」に記された要件を参照されたい。 ~~・　民間事業者等との契約に基づいて確保した安全な場所に該当する機関を選定する場合には、データセンター等の情報処理関連事業者が経済産業省が定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に準拠していることを確認する規程~~ ・　医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合には、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に準拠していることを確認する規程 **以下　抄**	