参考資料３-７

医療情報システムの契約における当事者間の役割分担等に関する確認表

別添１

ー　推奨される対応例　ー

Part１　主に医療機関が実施する項目

（契約を締結する上で医療機関が主体となって、必要に応じてシステム関連業者の協力を得ながら実施することが望ましい項目の例）

項番	項目	内容	推奨される対応例	ガイドライン等関連部分
A	**事業者選定・事業者管理**			
1	事業者からの開示資料の確認	事業者から開示を受けたサービス仕様適合開示書[*1]等（MDS/SDS[*2]、MDS2[*3]等）を確認しているか。	事業者から開示を受けたサービス仕様適合開示書[*1]等（MDS/SDS[*2]、MDS2[*3]等）を確認する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編5.1 別添小規模医療機関向けガイダンス3.5
2	事業者管理	①事業者との契約・協働体制を把握・管理できているか。	(a)　どの事業者と、どのシステム・サービスについて、どのような契約を締結しているかいつでも確認できるようにしておく。 (b)　医療情報システム・サービス事業者の体制、連絡先などを整理し、非常時の対応内容や非常時の連絡体制や連絡手順もいつでも確認できるようにしておく。 (c)　契約終了時のデータの取り扱い等も確認しておく。	・医療情報システムの安全管理に関するガイドライン第6.0版 別添小規模医療機関向けガイダンス3.5.2
		②医療情報を第三者提供する場合の管理体制が整備されているか。	法令遵守の上で第三者提供の手続き等の記録等を適切に管理する体制を整備し、医療機関と提供先それぞれが負う責任の範囲を契約においてあらかじめ明確にし、認識の齟齬等が生じないよう、書面等で可視化し、適切に管理する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編1.4
B	**医療機関の内部体制**			
1	「医療情報システムの安全管理に関するガイドライン」の確認	「医療情報システムの安全管理に関するガイドライン」を確認したか。	「医療情報システムの安全管理に関するガイドライン」の内容を把握し、特に弱みがある部分を把握し、必要な対策を検討する。	・医療情報システムの安全管理に関するガイドライン第6.0版
2	「医療機関におけるサイバーセキュリティ対策チェックリスト」に基づく契約時での現状把握及び対応	「医療機関におけるサイバーセキュリティ対策チェックリスト」を用いて、契約時に医療情報システムの現状把握及び対応を実施しているか。	厚生労働省から公表している立入検査マニュアルや関係団体が作成しているマニュアル等を参考に、必要な対策について確認する。 医療機関におけるサイバーセキュリティ対策チェックリストをもとに、医療情報システムの脆弱性[*8]等現状を把握し、適切な対策について契約時に対応する。	・医療機関におけるサイバーセキュリティ対策チェックリスト
3	安全管理のための人的管理	① 医療情報を取り扱う職員に関して人的安全管理対策を実施しているか。	医療情報を取り扱う職員に対し、退職後を含めた守秘義務や教育・訓練等を受ける義務を課す雇用契約等を締結することで、人的管理を行う。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編3.2.2、企画管理編7
		② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施し、教育・訓練の実施状況について定期的に経営層に報告しているか。	(a)　職員が安全管理に関して遵守すべき内容を十分理解できるよう、教育や非常時に向けての訓練を定期的に行う。 (b)　サイバー攻撃被害により地域医療の安全性を脅かされる近年の事案等を参考に、職員への教育を実施する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編3.2.2、企画管理編7
4	通常時における管理責任	医療情報システムの管理や運用を適切に行っているか。	管理責任を適切に果たすために必要な組織体制を整備し、定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編1.2.1
5	通常時における説明責任	① 医療情報システムの機能や運用につき、医療機関として状況を適切に把握し、必要に応じて患者等に説明ができるようになっているか。	システムの機能仕様やシステムの運用手順等について、事業者の協力を得ながら文書化し、管理しておく。また、それらの情報を患者等への説明を適切に行うための窓口の設置を行う。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編1.2.1 別添小規模医療機関向けガイダンス3.53.1.2
		② システム構築等を実施する際に、医療機関として状況を適切に把握し、必要に応じて事業者に説明ができるようになっているか。	システム構築等を実施する際に必要な情報について適切に事業者に対して提供すること等を行う。医療機関が既存事業者に情報提供を依頼する場合であっても、役割分担について取り決めること。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編6.2
6	物理的リスクの対応	① 機器や記憶媒体を持ち出す際の紛失・盗難リスクの対応を行っているか。	機器や記憶媒体を業務上の理由で施設等の外へ持ち出す際、誤って紛失、あるいは第三者に盗難されないよう、持ち出しルールの策定や、機器等へのセキュリティ対策等の対応を行う。	・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5.1.1
		② 施設への物理的侵入リスクの対応を行っているか。	正当な権限を持たない者（組織の内外を問わない）が、執務エリアやデータセンター等、医療情報システム等に関連する機器や記憶媒体が設置されている施設に侵入しないよう、入退室管理等の対応を行う。	・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5.1.1
C	**規程類の整備**			
1	医療情報システムの運用ルール及び規程類の策定	医療情報システムの運用ルールを定め、明文化された規程類を整備しているか。必要に応じて規程類の見直しを行っているか。	必要に応じて事業者と協力しながら、自医療機関と同規模、同様の医療サービス提供形態、同じ医療情報システム・サービスを利用しているなどの条件に適合する他の医療機関の運用ルールや規程類を参考にして整備（不要なソフトウェアのインストールの禁止等）する。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編4 別添小規模医療機関向けガイダンス3.3.2 ・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5.1
2	通常時における定期的な見直し、改善責任	医療情報システムの運用につき、適宜事業者からの情報提供を受け、定期的に見直し、必要な改善を行えるようになっているか。	医療機関で利用している医療情報システムを提供する事業者の協力を得ながら、医療機関として安全管理の改善に必要な情報を収集し、安全管理を適切に維持するための計画を策定し、必要に応じて、文書化して管理しているシステム運用手順等を改善する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編1.2.1 別添小規模医療機関向けガイダンス3.1.2
3	インシデント発生に備えた対応	BCP[*4]（事業継続計画）について、定期的な見直しや従業員への訓練・周知等を行っているか。	BCP[*4]について、従業員に対する訓練・周知等を通じて、必要に応じて事業者の協力を得ながら、改善の要否を定期的に確認する。	・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編3.4.1、企画管理編11.1 別添小規模医療機関向けガイダンス3.3.4

項番	項目	内容	推奨される対応例	ガイドライン等関連部分
参考	「医療機関におけるサイバーセキュリティ対策チェックリスト」該当項目			
1	適切な事業者の選定	① 事業者の情報セキュリティにおける対応状況を、事業者から提供された資料をもって確認しているか。 ② 情報セキュリティについて十分な対応をしていることが確認できる事業者を選定しているか。	事業者からサービス仕様適合開示書[*1]等（MDS/SDS[*2]、MDS2[*3]等)の開示を受けた上で、それらを参考にして、事業者の安全管理に係る基本方針や管理的・技術的・物理的安全管理対策措置の状況、実績等に基づく安全管理に関する信用度、財務諸表等に基づく経営の健全性等、必要な事項を確認し、適切な事業者の選定を行う。以下の要件等を参考に、利用者との契約に基づく事業実施体制内において、事業者が情報セキュリティに対応しているかについて確認し、適切な事業者を選定する。 ・事業者がプライバシーマーク[*9]等認証を取得していること ・事業者における、セキュリティに関する資格［情報処理安全確保支援士[*10]・情報セキュリティマネジメント試験[*11]等］や一定の実務経験を有する者の人数 ・事業者が、医療機関が容易に理解できるように、「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」に即した情報提供を行っていること	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編5.1 別添小規模医療機関向けガイダンス3.5
2	安全管理のための体制と責任・権限	医療情報システムの安全管理を行うために必要な運用管理の管理責任者として医療情報システム安全管理責任者及び企画管理者を任命し、適切な体制を整備できているか。	(a)　情報セキュリティ方針の策定、推進、実効性確保のために、経営層の適切な人物が医療情報システム安全管理責任者に就く。 (b)　その上で企画管理者を任命し、企画管理者の業務範囲と権限を明確化し、企画管理者において、 ・　安全管理に関する技術的な対応を行う担当者の任命 ・　非常時の対応を想定した安全管理に必要な体制の構築 ・　医療情報の漏えい等が生じた際の必要な体制の構築 ・　医療情報の安全な取扱いに必要な教育や訓練を講じるための体制の整備 ・　内部検査及び監査等の体制の構築 ・　患者等からの相談や苦情への対応体制の構築 これらに関して整備した内容の可視化等を行う。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編3、経営管理編3.1.2、3.2
3	医療情報システムの管理・運用	① 情報機器等（サーバ、端末PC、ネットワーク機器等）の台帳管理を行っているか。	(a)　情報機器等（※）の所在と、それらの使用可否の状態を適切に管理するため、機器台帳を作成して、情報機器等の所在や利用者、ソフトウェアやサービスのバージョン等の管理を行い、情報機器等が利用に適した状況にあることを確認できるようにする。事業継続の観点から紙及びクラウド等を用いた管理等、台帳管理を行う媒体の種類及び媒体数等も検討すること。 （※）サーバ、端末PC、ネットワーク機器のほか、ネットワークに接続される可能性がある医療機器等も含む。 (b)　必要に応じて事業者と協力しながら、リモートメンテナンス[*12]（保守）を利用している機器の有無の把握も行う。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編1.2.1、企画管理編9.1
		② 利用者の職種・担当業務別の情報区分ごとのアクセス利用権限を設定しているか。	必要に応じて事業者と協力しながら、医療従事者の資格や医療機関内の権限規程に応じて利用権限を設定する。また、利用者に付与したID等について台帳等により一覧化して管理する。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編13
		③ 退職者や使用していないアカウント等、不要なアカウントを削除しているか。	不要なIDによる不正アクセス[*13]等のリスクを防ぐため、退職者や使用していないID等が残存していないかを確認し、速やかに削除する。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編13
4	インシデント発生に備えた対応	① インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図があるか。	サイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成し、施設内の連絡先に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等を明示しておく。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編3.4.2、3.4.3、企画管理編12.3
		② サイバー攻撃を想定した事業継続計画（BCP[*4]）を策定しているか。	万が一サイバー攻撃を受けても重要業務が中断しない、または中断しても短い期間で再開できるよう、サイバー攻撃を想定したBCP[*4]等を整備しておく。例えば機器等が機能しなくなった場合の業務遂行・復旧方法や、復旧した後に、機能しなくなった間に講じた措置をどのように反映させるのか等をあらかじめ整理する。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 経営管理編3.4.1、企画管理編11.1 別添小規模医療機関向けガイダンス3.53.3.4

医療情報システムの契約における当事者間の役割分担等に関する確認表
ー　推奨される対応例　ー

別添１

Part２　医療機関と事業者が共同で実施する項目
（技術的な対策等医療機関だけでは実施することが困難な事項で、役割分担等を明確にしておくことが望ましい項目の例）

項番	項目	内容	想定されるリスク	推奨される対応例	ガイドライン等関連部分
A	共通				
1	「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」の確認	事業者は「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」を確認する。	事業者が提供する医療情報システムについて、「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」の遵守ができておらず、不十分な安全管理によって情報漏えいや事故につながるおそれがある。	事業者は医療情報システム等の提供方法等が「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」に遵守しているか等、本ガイドラインを確認する。	・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
2	複数事業者間の役割分担	医療機関が複数事業者と契約する場合における、事業者間の役割分担及び抜け漏れがないことを確認する。	システム関連業務について、医療機関が複数事業者と契約する場合、どの事業者も責任を負わない間隙が生じると、当該部分についてのセキュリティ対策が不十分となるほか、事故発生時の責任の所在が不明確になるおそれがある。	(a)　医療機関はシステムを構成する機器、ソフトウェア、クラウドサービス[*6]等の一覧表や全体図をもとに、いずれの事業者が責任をもって導入、保守、運用等を担当するのか不明な部分がないよう確認する（特に、複数事業者への発注を行う中で、システム全体を取りまとめる役割を担う事業者（プライム事業者）がいる場合には、当該事業者が再委託先から調達する構成要素を含めてリスクマネジメント及び制度上の要求事項に対応するなど、当該事業者がどこまで責任を負うのか明確にしておく。また、プライム事業者においても再委託先との適切な連携体制を確保する必要がある。）。 (b)　また、必要があれば事業者間の連携や役割分担に関する事項（例えば事故発生時の情報連携・対応における相互協力等）も契約に含める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編2.2.2、システム運用編3.4.2 ・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2.2.3
3	「医療情報システムの安全管理に関するガイドライン」の遵守	下記「B.システム導入」「C.システム運用・保守契約」で例として示すもの以外にも、事業者が提供する医療情報システムやサービスが「医療情報システムの安全管理に関するガイドライン」の遵守事項を満たす上で必要な仕様や運用となっていることを確認する。	「医療情報システムの安全管理に関するガイドライン」の遵守ができておらず、またそのことを医療機関が把握していなかった場合、不十分な安全管理によって情報漏えいや事故につながるおそれがある。	(a)　契約において、事業者が「医療情報システムの安全管理に関するガイドライン」の遵守事項を満たしたセキュリティ対策を提案・実施することを取り決める。事業者による情報の開示内容に即して、必要に応じて想定されるリスクについても協議し、その場合の対応についても取り決める。 (b)　契約後も必要に応じて当該遵守状況を示す資料の提出を求めることができること等を取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編2.1.2(1)
4	継続的なリスクマネジメントプロセスの実施	「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」5.1に示されたリスク特定、リスク分析、リスク評価、リスク対応の選択肢の選定、リスク対応策の設計・評価、リスクコミュニケーションのプロセスを継続的に実施する。	リスクマネジメントに始まる一連のプロセスの継続的な実行とそれによるシステム上のリスク対策の見直しを行わなければ、新たなリスクに対応できなくなるおそれがある。	「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5.1.1～5.1.6に示されているリスクアセスメント[*14]に始まる一連のプロセス（リスク特定、リスク分析、リスク評価、リスク対応の選択肢の選定、リスク対応策の設計・評価、リスクコミュニケーション）を契約後も継続的に実施し、対応の見直しを行うこと、それを行うに当たっての具体的な時期・頻度・役割分担等を取り決める。 医療情報システムを構成するシステムごとに、それらが使用できなくなった場合の影響等についてもリスク評価を行い、事業継続の観点から代替措置等を検討すること。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編6.1.2 ・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 5.1.7、5.2
5	開示されたサービス仕様等の事後的な変更	契約締結前に事業者から提示された医療情報システム関連情報について、変更があった場合に情報提供する。	事前に提示された情報に変更があったにもかかわらず、それを医療機関が把握していなければ、想定外の事故が生じるおそれがある。	「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」4.1「医療機関へ情報提供すべき項目」に記載された情報（「医療機関が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要のある項目、及び「医療機関との共通理解を形成するために情報提供すべき項目」）について、契約締結後に変更があった場合に改めて情報を提供することを取り決める。	・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4.1
6	サービス・レベル合意書（SLA）[*5]の締結	事業者が提供するサービスの保証範囲を合意するため、サービス・レベル合意書（SLA）[*5]を締結する。	具体的なサービス・レベルが定まらないまま委託をした場合、障害等が発生した際の責任分担があいまいになるおそれがある。	「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」別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」」を参考に、事業者は、医療機関との共通理解を醸成した上で、医療機関が必要とするサービス・レベルを満たすSLA案を作成し、その内容について事業者から十分な説明を行った上で、検討して取り決める。	・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3.2.1、別紙１「ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）参考例」における「サービス・レベル合意書（SLA）参考例」
7	事業者の責任と秘密保持義務	医療情報システムに関わる事業者に対して、医療機関の職員と同様の責任や秘密保持義務を課す。	医療情報を開示するに当たり、事業者による秘密保持義務がないと、漏えいが生じるおそれが高まる。 また、事業者による情報漏洩等が発生した場合に、医療機関が事業者に対して対応や協力を求めたり、責任追及したりすることができないおそれがある。	委託先事業者と当該事業者で業務にあたる者との雇用契約等において、守秘義務契約を含んでいることを確認する。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編7.2

項番	項目	内容	想定されるリスク	推奨される対応例	ガイドライン等関連部分
8	個人情報の管理	個人情報の適切な取り扱いについて取り決める。	医療情報には要配慮情報を含む個人情報[*15]が含まれるため、漏えい等の事故が発生した場合の影響は重大なものとなる。	事業者が医療機関が保有する個人情報を取り扱う場合には、個人情報保護法及び厚生労働分野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基づき、十分な安全管理措置を確保した取り扱いをすることや、事故発生時の対応等について契約で取り決める。	・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3.1.3
9	医療情報の外部保存	診療録及び診療諸記録等の機密情報や個人情報について事業者が提供するサービスを用いた外部保存を行う場合に満たすべき要件（特にクラウドサービス[*6]を利用する場合）を遵守する。	① 医療情報等を外部保存する場合、関連する通知や「医療情報システムの安全管理に関するガイドライン第6.0版」企画管理編7に記載の要件を遵守しない形での外部委託の場合、安全管理が不十分となり事故が生じるおそれが高まる。 また、外部保存にあたってセキュリティ対策や事故発生時の義務・責任に不足がある場合、事故発生時に必要な対応がとられないおそれがある。	(a) 診療録及び診療諸記録等の機密情報や個人情報について事業者による外部保存を行う場合には、関連する法令及び右記通知の要求事項を満たすことのほか、「医療情報システムの安全管理に関するガイドライン第6.0版」企画管理編7の【遵守事項】のうち、契約において取り決めるべきと記載された項目（委託先事業者の担当人員に守秘義務を課すほか、安全管理に関する教育訓練を行うこと、守秘義務等の違反に対するペナルティ、保存された情報についての独断での分析・解析等の禁止や提供の禁止、匿名化した情報を含めた情報の適切な取り扱い、アクセス権限の適切な設定）を取り決める必要がある。 (b) また、事業者が医療情報等の安全管理のための基本方針・取扱規程等や必要な実施体制の整備状況、サイバー攻撃による被害防止のためのバックアップの取得・管理の状況、実績等に基づく個人データ安全管理に関する信用度、財務諸表等に基づく経営の健全性、関連する認定・認証等（プライバシーマーク＊9、ISMS＊16、ISMAP＊17 等）の取得状況、医療情報等を保存する機器の設置場所（地域・国）、事業者に対する国外法の適用可能性を確認するほか、事業者が施している具体的なセキュリティ対策、漏えい・消失等の事故発生時に事業者が負担する契約上の対応義務や責任の内容に不足がないか確認する。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編7 ・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6.5 ・外部保存通知 ・e文書法省令施行通知
			② 事業者による外部保存の期間が終了したり、外部保存の委託自体が終了しているにもかかわらず、外部に医療情報等の機密情報や個人情報が残存していると流出のリスクが残る。	情報の保存期間が満了した場合や外部保存を終了する場合の医療情報（バックアップを含む。）の破棄や返却について、破棄時に適切に破棄されたことを確認できる証跡の提供等も含め、契約において具体的に取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編7、7.4、7.5、8.3、 システム運用編7.3
10	再委託先の選定・管理	医療情報システムに関する業務を事業者が再委託する場合に、再委託先の選定・管理について医療機関が関与する。	医療機関が認識しないまま、医療情報システムの一部や医療情報等が再委託先で取り扱われ、不十分な安全管理によって情報漏えいや事故につながるおそれがある。	医療情報システムに関する業務を事業者が再委託する場合には、 (a) 事前に医療機関の承諾が必要であること、 (b) 再委託先の行為について事業者が責任を負うこと、 (c) 事業者が再委託先から実施状況の報告等必要な情報を得て医療機関に提供すること等を取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編2.1.2(2)、経営管理編5.2.2、 システム運用編3.3.1 ・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2.2
11	医療情報システムのセキュリティに関する情報提供義務	事業者が医療機関に対して、医療機関が患者に対する安全管理義務を履行するために必要なセキュリティに関する情報を適時適切に提供する義務（説明義務）の具体的内容・範囲について定める。	説明義務について具体的な定めがない場合、事業者から医療機関に対する情報提供が不十分となり、その結果必要なセキュリティ対策をとれないおそれがある。 また、事故発生時等に、事業者が事前にどこまで説明する義務を負っていたのかを巡ってトラブルとなるおそれがある。	医療機関は医療の専門家であって、セキュリティについての専門性は乏しい場合が多いのに対し、専門的な医療情報システム等を提供する事業者は、セキュリティに関する専門的な知識・経験・人材を擁しているべきであり、こうした専門性の格差に鑑みて、事業者は、医療機関に対し、委託契約又は信義則に基づく付随義務として、医療機関が患者に対する安全管理義務を履行するために必要な情報を、適時適切に提供する義務（説明義務）を負うとされる。 契約においては、説明義務の範囲を明確にし、医療機関にとって適時適切な情報提供がなされるよう、こうした事業者の説明義務の対象や内容をなるべく具体的な形で取り決める。	・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3.1.2
12	セキュリティ対策の見直し提案	情報セキュリティを巡る情勢に鑑み、事業者から自発的に対策の見直しを提案する。	医療機関では情報セキュリティに関する最新の情勢を把握できない場合、事業者からの自発的提案がなければ対策が遅れるおそれがある。	情報セキュリティの最新情勢に鑑みて、安全管理上必要であれば、事業者において自発的に対策の見直しを行い、医療機関に提案することを取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編2.1.2(3)
B	**システム導入契約**				
1	利用者認証	医療情報システムへのアクセスを正当な利用者のみに限定するため、利用者の識別・認証機能を設定する。	医療情報システムに利用者認証機能が適切に設定されていないと、不正アクセス[*13]が生じる可能性がある。	類推されにくいパスワードの設定や、二要素認証の採用などの利用者認証の強度について、リスク評価に基づいて適切に取り決める。 なお、「医療情報システムの安全管理に関するガイドライン」において、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ている。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編14.1
2	通信相手の認証	医療情報システムにおいて通信しようとする相手方が、通信目的に適った正当な相手かどうか認証する。	相手がなりすましである場合に、情報漏えいが生じるおそれがある。	(a) 医療情報システムにおいてネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと、 (b) また診療録等のオンライン外部保存を受託する事業者と委託する医療機関が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること等を、システム又はサービスの要件として取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編13⑫ ・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
3	通信経路に対する安全対策の確保	通信経路に対する安全対策を確保する。	不正アクセス[*13]による情報漏えいが生じるおそれがある。	外部から接続先が限定されているオープンではないセキュアなネットワークへの接続を認める場合、セキュアなネットワークに到達するまでのオープンなネットワーク（インターネット）において、チャネル・セキュリティ[*18]が確実に確保されるよう事業者において必要な対策を講じることを取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編 13

項番	項目	内容	想定されるリスク	推奨される対応例	ガイドライン等関連部分
4	暗号化	通信及び保存情報の暗号化を実施する。	通信及び保存情報が暗号化されていないと、通信の盗聴、保存情報の紛失・不正アクセス[*13]が生じた場合に情報が読み取られ、漏えいするリスクが高まる。	用いるシステム、サービスの内容に応じて、通信及び保存情報の暗号化の有無および程度（全部か、一定範囲か等）について取り決める。 特に、医療情報システムに対する外部からの接続を認める場合、安全対策が確保された内部ネットワーク に到達するまでのオープンなネットワーク（インターネット）において、通信経路に関する安全対策が確実に確保されるよう、事業者において暗号化等必要な対策を講じることを取り決める。 なお、暗号化にあたっては、復号のための手段を確保するなど、医療情報の可用性に留意すること。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編13.1.2 ・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
5	ネットワーク構成	診療等に必要なネットワークを適切に構築する。	リスク分析等に基づき、ネットワークを適切に構築する必要がある。例えばリモートメンテナンス[*12]等のために外部接続点を多数設置する等、必要以上の外部アクセスを許容する設計としたような場合、管理等が困難となり脆弱性[*8]の原因となるおそれがある。	(a)　十分なセキュリティを確保しつつ、適切な保守・運用（システム障害対応等を含む）を行うことも見据えて、ネットワークを適切に構築する（論理的/物理的な構成分離、ネットワーク間のアクセス制御等）。 (b)　外部ネットワーク利用等に関連する具体的な役割分担等、責任の所在の範囲について取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編8.1、システム運用編12.2
6	品質確保の状況	医療情報システムの品質管理方法等について両者で確認するための情報提供を行う。	品質管理の状況について医療機関が把握できず、品質が適切に確保されないと、必要な改修や将来的なシステムの刷新の計画等を立てることが困難になるおそれがある。	医療情報システムを構成するオープンソースソフトウェア[*19]を含むソフトウェア等を事業者に委託して開発する場合に、ソースコード[*20]の開示や、使用している製品やテストでの検証状況の報告等を行うことで、品質確保の状況について医療機関にオープンソースソフトウェア等の汎用ソフトウェアをどの程度使用するかについて、情報交換を行いつつ取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編9.2
C	**システム保守・運用契約**				
1	ネットワークのトラフィック[*7]監視	ネットワークのトラフィック[*7]の監視及び異常発生時の対応を確認する。	ネットワーク障害や大量のデータ転送により、ネットワークが正常に利用できなくなるおそれがある。	事故発生時の対応方法及び、事業者が事故の発生又は発生のおそれを認識した場合、直ちに医療機関に連絡するよう取り決める。	・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
2	機器運用監視	サーバ、ネットワーク機器の稼働監視を行う。	システムの状況を把握できないことにより、障害への対応が遅れてシステムへのアクセスが長時間停止するおそれがある。	稼働状況を常時把握可能とし、異常が検知された場合には、事業者及び医療機関に通知をすることを取り決めておく。	・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
3	運用委託先によるシステムの管理状況の報告	医療情報システムの運用を委託する場合において、医療機関が管理状況を把握し、安全管理がなされていることを確認できるような体制を構築する。	事業者による管理状況が不十分になったり、当初の想定から乖離したりするおそれがある。	事業者による定期的な報告のほか、医療機関が求めた場合には直ちに報告することを取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編10、経営管理編5.2.1、 システム運用編3.3.1
4	事故発生時の報告	事故発生時の対応方法及び医療機関への報告について取り決める。	事故発生時に事業者及び医療機関が速やかに対応できなければ、被害が拡大するおそれがある。	事業者が事故の発生又は発生のおそれを認識した場合は、直ちに医療機関に連絡するよう取り決める。	・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4.1
5	事故発生時の原因究明・対策	事故発生時の原因究明、善後策の策定・実施、再発防止策の策定・実施に係る役割分担を行う。	事故発生時に状況や関連情報を分析し、原因を究明して善後策を策定・実施すること。 また、再発防止策の策定・実施についての役割分担を定めておかなければ、事故発生時に迅速かつ適切な対応ができず、被害が拡大するおそれがある。	(a)　事故発生時には相互に連携を行い情報共有を行うほか、 (b)　事業者において原因究明を実施し、診療への影響を踏まえた善後策及び再発防止策を提案すること、 (c)　医療機関は当該方策を検討・承認して事業者とともに実施すること を取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編2.1.3 ・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3.2.2
参考	**「医療機関におけるサイバーセキュリティ対策チェックリスト」該当項目**				
1	脆弱性[*8]情報の確認・報告	医療情報システムで用いる機器及びソフトウェアに関する脆弱性[*8]情報の確認義務、脆弱性が発見された場合に医療機関へ適切なタイミングで報告する。	新たに発見・公表される脆弱性[*8]情報が医療機関に適時に伝えられない場合、脆弱性を利用したサイバー攻撃のリスクが高まる。	医療情報システムに関連する新たなセキュリティ上の脆弱性[*8]について、(独) 情報処理推進機構（IPA） 等が公表する情報その他の情報を継続的に収集すること（又は合理的な範囲で収集に努めること）、および脆弱性発見時の医療機関への報告や対策の実施を行うこと等を取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編9.2 ・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4.1
2	担当業務等に基づくアクセス制御	医療情報システムを利用する医療従事者等の資格や担当業務、医療機関内の権限規程などに応じた利用権限の設定が可能なシステムを導入する。	アクセス権限の管理が不十分だと、知る必要のない情報の提供や、必要のない権限の付与がなされ、情報漏えい等のリスクが高まる。	医療機関によって医療従事者等の資格や担当業務毎にアクセス権限を設定できるような仕様とすることを取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編14.2
3	医療情報システムに対する外部アクセス	外部アクセスによる医療情報の参照や利用についての条件や制限、安全管理対策等を実施する。	医療情報システムに対する外部アクセスの条件や制限、安全管理対策等が不十分なままだと、安全性を欠く外部アクセス（あるいは不適切な経路の追加）により情報漏えい等が発生するリスクが高まる。	外部アクセスによる医療情報の参照や利用について、これを認めるかどうか、どのような場合に認めるか、認める際の条件や制限、技術的な対応による安全管理対策等について、医療機関と事業者が共同で具体的な規則や手順を設定すること、それを遵守することを取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編8.2.4 ・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
4	ウイルスチェック	ウイルス等の悪意あるプログラムを検出する機能を導入し、適切にアップデートする。	コンピュータに誤動作を起こさせる悪意のあるプログラムにより、システムが利用できなくなる、データが消去される、情報が外部に漏えいしてしまう、などのおそれがある。	システム導入時には適切なウイルスチェック機能を導入するものとし、継続的なウイルス定義ファイル（パターンファイル）[*21]等のアップデートの実施についての役割分担を取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・情報システム・モデル取引・契約書追補版 セキュリティチェックシート

項番	項目	内容	想定されるリスク	推奨される対応例	ガイドライン等関連部分
5	バックアップ環境・冗長性の確保	医療情報システムの異常発生時に備え、診療機能の維持等に必要なバックアップ環境を確保する。	医療情報システムの異常発生時に切り替えることができるバックアップ環境を適切に構築していないと、非常時に診療機能が低下または停止する恐れがある。 また、冗長性を適切に確保していない場合、システム障害時に診療機能が低下するだけでなく、セキュリティパッチ[*22]等の適用の際に診療機能の確保が困難になるおそれがある。	異常発生時に切り替えて利用するためのバックアップ環境を適切に構築する（ホットスタンバイ／コールドスタンバイ[*23]、ネットワーク等の二重化[*24]、バックアップデータの確保）など、システム障害時やセキュリティパッチ[*22]の適用等を想定し、冗長性を適切に確保する方法について取り決める。バックアップデータについては、激甚災害、媒体劣化、ランサムウェア[*25]等への対策も考慮し、ネットワークからの分離状況等についても取り決める。	・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編11.2、システム運用編11.1
6	ソフトウェア及びハードウェアの保守	ＯＳやアプリケーション、ハードウェアの保守を実施する。	不具合・故障の発生や、セキュリティホールによって情報が漏えいするおそれがある。	システムを構成する機器、ソフトウェア、クラウドサービス[*6]等については、保守契約に基づき事業者による保守（セキュリティパッチ[*22]の適用等）がなされるよう取り決める。オープンソースソフトウェア[*19]等の汎用ソフトウェアを使用する際も、脆弱性[*8]情報等のチェックやその対応についても取り決める。	・情報システム・モデル取引・契約書追補版 セキュリティチェックシート
7	データバックアップの 取得・管理	事故発生時に利用可能なデータバックアップの取得の有無・対象・頻度・復旧できる世代・バックアップ方法・保存場所等を確認する。	サイバー攻撃による被害が発生した際に、復旧のために用いられるデータのバックアップが存在しなかったり、古いものであった場合は、迅速なシステムの復旧ができないおそれがある。	事故発生時に備えてバックアップの取得を事業者に委託し、取得頻度、世代数、医療情報システムとの連携、バックアップを取得するタイミング、事故発生時の対応、復旧作業における役割分担等を取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 システム運用編12.2 ・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4.1
8	医療情報システムのログ[*26]の扱い	医療情報システムにおける利用者の操作やシステムの動作に関するログ[*26]の保存、管理及びその内容の分析、異常検知を実施する。	システムのログ[*26]を適切に管理し、異常検知に活用できなければ、サイバー攻撃等の発見が遅れるおそれがある。	医療情報システムにおける利用者の操作やシステムの動作に関するログ[*26]の保存、管理についての役割分担を定めた上、その内容の分析、異常検知について、事業者が継続的に実施することを取り決める。	・医療機関におけるサイバーセキュリティ対策チェックリスト ・医療情報システムの安全管理に関するガイドライン第6.0版 企画管理編5、システム運用編17.1