ＨＩＳＰＲＯ　医療クラウドサービス チェックシート(v2.00)

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス （文書名、ページ番号等）	判定結果	改善策	備考
1	ユーザとの契約	サービス提供者の責任	クラウドサービス事業者は、医療機関等の管理者が「医療情報システムの運用状況等が適切に行われていること等を患者等に説明する責任」を果たすため、以下の責任を負うこと。 (1)提供するクラウドサービスの仕様、運用、及び情報セキュリティ対策に関する事項の文書化。 (2)提供するクラウドサービスの仕様及び品質に関する説明及び必要な情報提供。 (3)提供するクラウドサービスに関する監査等の情報の提供。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
2	ユーザとの契約	サービス提供者の責任	クラウドサービス事業者は、医療機関等の管理者が「医療情報システムの運用管理を医療機関等が適切に行う責任」を果たすため、以下の責任を負うこと。 (1)医療機関等の管理者に対するクラウドサービス事業者側の最終的な管理責任者の明確化。 (2)個人情報保護責任者を含むクラウドサービスの提供体制の明確化。 (3)クラウドサービスの提供に関する運用状況等の定期的な報告。 (4)医療機関等の管理者からの問合せ等に対して、一元的に対応できる体制の構築。	契約書、サービス利用約款、体制図、組織図、苦情・質問の受付窓口、責任体制に関する書類等					
3	ユーザとの契約	サービス提供者の責任	クラウドサービス事業者は、医療機関等の管理者が「医療機関等において定期的な見直しを実施し、必要な改善を行う責任」を果たすため、クラウドサービス及び情報セキュリティの向上についての定期的なレビュー結果の報告等の責任を負うこと。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
4	ユーザとの契約	サービス提供者の責任	クラウドサービス事業者は、医療機関等の管理者が「情報セキュリティインシデント の原因・対策等に関する説明責任」を果たすため、以下の責任を負うこと。 (1)緊急時に医療機関等の管理者に対して提供する情報の内容、役割分担等の明確化。 (2)クラウドサービスの提供状況に関する記録の収集及び緊急時の報告体制の構築。 (3)媒体及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築。 (4)緊急時に備えた、アクセス制御等の手順等の明確化。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程、各種手順書、ユーザとの責任分界を示した書類、利用者向セキュリティ順守事項を説明する書類					
5	ユーザとの契約	サービス提供者の責任	クラウドサービス事業者は、医療機関等の管理者が果たすべき善後策を講ずる責任「情報セキュリティインシデントの原因を究明する責任」、「再発防止策を講ずる責任」を果たすため、以下の責任を負うこと。 (1)情報事故（個人情報漏洩等）等が発生した場合の原因追及に必要な情報提供の範囲、条件等の合意、及び情報提供の実施。 (2)善後策の提案。 (3)情報事故が発生した場合の損害填補責任に関する合意。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
6	ユーザとの契約	サービスの利用終了	クラウドサービス事業者は、クラウドサービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、クラウドサービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行うこと。また、医療機関等への対応の内容、条件等について、医療機関等に対し明確に提示できること。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
7	ユーザとの契約	サービスの利用終了	クラウドサービス事業者は、医療機関等のサービス利用開始後に、サービス仕様適合開示書等の内容を変更する場合にはクラウドサービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行うことを、医療機関等に対し明確に提示できること。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
8	ユーザとの契約	サービスの利用終了	クラウドサービス事業者は、医療機関等の都合如何に関わらず、クラウドサービス利用の終了やクラウドサービス変更に対する以下の内容を含む運用管理規程(ルール)等を策定し、医療機関等に対し明確に提示できること。 (1)クラウドサービス内の医療情報を、医療機関等に返却すること (2)返却するデータは可用性を確保するため、厚生労働省で定めている「医療情報システムの安全管理に関するガイドライン」（以下、厚生労働省ガイドライン）の「5．システム設計の見直し（標準化対応、新規技術導入のための評価等）」に従い、相互運用性を確保しながら行うこと (3)返却するデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式、厚生労働省標準規格への対応有無）、返却方法、条件(クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータの取扱いも含む)。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程					
9	ユーザとの契約	サービスの利用終了	クラウドサービス事業者は、クラウドサービス提供の停止又は医療機関等におけるクラウドサービス利用停止が生じた場合は、速やかに、記録の削除、媒体及び機器の廃棄等を行うこと。記録の削除、媒体及び機器の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出すること。 媒体及び機器を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認すること。 その際、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、医療機関等に対し明確に提示できること。	SLA、運用管理規程、電子媒体の扱いに関するルール、情報資産廃棄管理台帳、廃棄証明書（マニフェスト）、廃棄記録、廃棄報告書、サービス仕様適合開示書					
10	組織	実績・第三者評価	クラウドサービス事業者は、クラウドサービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行うこと。 (1)個人情報保護に関する方針。 (2)医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況。 (3)医療情報等の安全管理に係る実施体制の整備状況。 (4)実績等に基づく個人データ安全管理に関する信用度。 (5)財務諸表等に基づく経営の健全性。 (6)保存された医療情報を格納する情報機器等が、国内法の適用を受けることに対する情報。 (7)医療情報を保存する情報機器等が設置されている場所(地域、国)。 (8)受託事業者に対する国外法の適用可能性。 (9)不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況。	プライバシーポリシー、個人情報保護指針、安全管理に関する方針文書、体制図、組織図、苦情・質問の受付窓口、責任体制に関する書類等、サービス提供実績表、ISMS認証証明書、ISMS適用宣言書、プライバシーマーク登録証、第三者による監査結果、是正措置報告、財務諸表					
11	組織	実績・第三者評価	クラウドサービス事業者は、医療機関等の管理者に対して情報システムや運用情報等に対して、公正な説明責任を果たすため、以下の内容を実施すること。ただし、第三者認証を取得することをもってガイドラインの要求事項の全てを満たすことにはならない点に留意すること。 (1)クラウドサービス事業者は、プライバシーマーク認定(保健医療福祉分野)･ISMS 認証・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で示されているクラウドセキュリティ認証等の公正な第三者の認証等を取得していること。 (2)認証を取得する際、医療情報を管理するクラウドサービスの入口から出口まで包括的に取得対象とする認証取得を行い(ISMSにおける適用範囲)、安全管理の対策として医療情報を取り扱うために特別に配慮している安全管理策を盛り込み、適用宣言書で明確にすること。 (3)また、医療機関等が委託先クラウドサービス事業者を選定する際に、安全管理の対策が適切に適用されていることを確認できるように、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくこと。	ISMS適用宣言書、プライバシーマーク登録証、第三者による監査結果、是正措置報告					
12	組織	情報セキュリティ	クラウドサービス事業者の経営者は、自社における個人情報保護指針、プライバシーポリシー等を医療機関等に対し明確に提示できること。指針等には以下の内容を含めること。 (1)個人情報保護法及び個人情報保護委員会の個人情報の保護に関する法律についてのガイドラインならびに医療・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ダンス他、医療関連分野ガイダンスに定める安全管理措置等を実施すること。 (2)個人情報保護法の対象外の情報（死者に関する情報等）であっても、医療関連分野ガイダンスに示されているように医療情報の特殊性から個人情報保護法ならびに医療情報システムに関するガイドラインにおける運用に準じて取り扱うこと。	プライバシーポリシー、個人情報保護指針、安全管理に関する方針文書、サービス仕様適合開示書					
13	組織	情報セキュリティ	クラウドサービス事業者は、情報セキュリティに関する基本方針や運用管理規程(ルール)等、重要な文書の作成や管理に関する規程ならびに情報セキュリティポリシーを策定し、これに基づき文書の管理を行うこと。また、その文書の内容について、医療機関等に対し明確に提示できること。	安全管理に関する方針文書、情報セキュリティポリシー、情報セキュリティ基本方針、文書管理規程、サービス仕様適合開示書、運用管理規程					
14	組織	情報セキュリティ	クラウドサービス事業者における、運用管理規程(ルール)には、以下の内容を記載すること。 (1)情報セキュリティに対する組織的取組方針 (2)クラウドサービス事業者内の体制及び施設 (3)医療機関等及びクラウドサービス以外の外部事業者との契約書の管理 (4)情報処理に関わるハードウェア・ソフトウェアの管理方法 (5)リスクに対する予防、リスク発現時の対応 (6)医療情報を格納する媒体の管理（保管・授受等） (7)第三者による情報セキュリティ監査 (8)医療機関等の管理者からの問い合わせ窓口の設置、対応等	運用管理規程、情報セキュリティ実施手順、体制図、組織図、回線事業者や他のサービス提供事業者との契約、他のサービスとの責任分界を示した書類、機能仕様書一覧、監査規程					
15	組織	情報セキュリティ	クラウドサービス事業者は、クラウドサービスの提供に係る契約に、以下の事項を含めること。 (1)医療情報に関して、適切に他の情報と区別して管理を行うこと。 (2)死者に関する医療情報についても個人情報に準じて取り扱う旨を医療機関等に対し明確に提示すること。 (3)個人情報保護対応策、クラウドサービスに係る情報並びにクラウドサービス内の医療情報に関する守秘義務、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること、及び委託した情報の取り扱いに対する医療機関等による監督に関する内容を含めること。 (4)クラウドサービス内の医療情報の解析・分析は、クラウドサービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わないこと。 (5)クラウドサービス内の医療情報を匿名加工した情報も、医療情報に準じて取り扱うこと。 (6)クラウドサービス内の医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わないこと。 (7)厚生労働省ガイドラインに定める医療機関としての運用管理規程等の遵守内容、その他最新の関係法令等を遵守し、安全管理措置を実施すること。 (8)厚生労働省ガイドライン及び総務省、経済産業省で定めている「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」を遵守すること。各ガイドラインの遵守状況を医療機関等に提示する場合は、可能な限り具体的に行うこと。	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程、安全管理に関する方針文書、情報セキュリティポリシー、サービス仕様適合開示書					

整理番号	

評価申請元		評価者	
評価対象プロダクト名			

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス （文書名、ページ番号等）	判定結果	改善策	備考
16	組織	情報セキュリティ	クラウドサービス事業者における医療情報を含む個人情報を物理的に保存する機器や媒体は、原則サーバー機器のみとし、表示のための一時的な保存等を除き、端末上に保存しない旨、自社の運用管理規程(ルール)等に定めること。また、定期的に所在確認や棚卸し等を行うこと。	運用管理規程、資産目録、資産台帳、装置登録リスト、棚卸記録					
17	組織	情報セキュリティ	クラウドサービス事業者が、医療機関等の指示に基づき、クラウドサービス内の医療情報に対する第三者提供（閲覧等）を行う場合には、提供を行った内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行うための条件、範囲等について、医療機関等に対し明確に提示できること。	個人情報保護に関する記録、運用作業報告書、保守作業報告書、各種手順書、サービス仕様適合開示書					
18	組織	情報セキュリティ	クラウドサービス事業者が、クラウドサービス内の医療情報を保守・運用を行うために閲覧するのは必要最小限とし、仮に閲覧が必要な場合には、緊急時を除き、医療機関等のシステム管理者の事前・事後の承認により実施すること。緊急時に閲覧した場合には、閲覧した医療情報の範囲及び緊急で閲覧が必要な理由等を示して、医療機関等のシステム管理者の承認を得ること。閲覧に係る範囲、手順、閲覧後の速やかな報告方法等について、医療機関等に対し明確に提示できること。	個人情報保護に関する記録、運用作業報告書、保守作業報告書、各種手順書、サービス仕様適合開示書					
19	組織	情報セキュリティ	クラウドサービス事業者は、医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担、責任分界等について、医療機関等に対し明確に提示できること。	製品マニュアル、サービス構成図、サービス仕様適合開示書					
20	組織	情報セキュリティ	クラウドサービス事業者は、クラウドサービスで提供する医療情報システム、組織体制、運用等に関する監査の方針、内容等について、医療機関等に対し明確に提示できること。	運用管理規程、監査規程、サービス仕様適合開示書					
21	組織	情報セキュリティ	クラウドサービス事業者は、外部事業者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容について、医療機関等に対し明確に提示できること。	運用管理規程、監査規程、回線事業者や他のサービス提供事業者との契約、サービス仕様適合開示書					
22	組織	情報セキュリティ	クラウドサービス事業者は、クラウドサービスを運用するために組織として必要となる以下の事項について、医療機関等に対し明確に提示できること。 (1)クラウドサービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等 (2)医療情報の管理状況に関係する資料の提供 (3)クラウドサービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等 (4)媒体及び機器等の管理等に関する自社の運用管理規程(ルール) (5)個人情報を記録した媒体及び機器の管理等に関する運用管理規程(ルール) (6)医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割、責任分界等 (7)自社において実施する医療情報システム監査等 (8)医療機関等に開示する監査記録等の範囲・条件等	契約書、サービス利用約款、重要事項説明書、サービス仕様適合開示書、SLA、運用管理規程、ユーザとの責任分界を示した書類、監査規程					
23	組織	情報セキュリティ	クラウドサービス事業者は、クラウドサービスにおける医療情報システムへのアクセス権限、アカウント管理、認証管理及びアクセス等に対する記録の収集と保存、アクセス管理の運用状況に関する定期的なレビューの実施等、クラウドサービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定	アクセス管理規程					
24	組織	情報セキュリティ	クラウドサービス事業者は、クラウドサービスに供する媒体及び機器に関し、以下の内容について、方針、規則等を運用管理規程(ルール)に含めること。また従業員等（再委託先を含む）に対して教育を行うことについて、医療機関等に対し明確に提示できること。 (1)管理体制及び管理方法(持ち出し手順、申請承認プロセス、返却確認プロセス、返却時検証手段) (2)媒体及び機器の取扱い（媒体及び機器等に格納される情報の機密レベルを示すラベル付けを実施） (3)クラウドサービスに関する情報（医療情報、医療情報システムに関連する情報等）を格納する媒体及び機器等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） (4)原則、持ち出しがないよう管理領域での作業とするが、クラウドサービスに関する情報を持ち出した場合で、当該情報を格納する媒体及び機器等の盗難・紛失（持ち出し時の媒体及び機器等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応 (5)障害不良等が発見された場合の、装置内の情報の確実な消去もしくは物理的廃棄を行うなどの対応 (6)外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等）））	サービス仕様適合開示書、運用管理規程、情報交換に関するルール、電子媒体の扱いに関するルール、情報破棄に関するルール、情報資産持ち出し管理簿、情報セキュリティ教育・訓練報告書					
25	組織	体制	クラウドサービス事業者は、以下の責任者を設置し、任命・解任等のルールを策定すること。 (1)クラウドサービスの提供についての管理責任を有する責任者。 (2)医療情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）。 (3)クラウドサービスの提供に係る医療情報システムの運用に関する事務を統括する責任者。	体制図、組織図、服務規程、職員規定、サービス仕様適合開示書					
26	組織	体制	クラウドサービス事業者は、下記の体制（再委託に関する情報を含む）について構築し、責任者等を含め体制図等として、医療機関等に対し明確に提示できること。 (1)情報セキュリティポリシーの遵守を担保する組織体制 (2)クラウドサービスの提供に係る体制（保守体制、問合せ窓口、障害時保守体制、緊急時の対応体制等） (3)医療機関等の管理者からの一元化された医療機関等からの問合せ窓口ならびに受付時間帯等(自社で契約した外部事業者が提供するクラウドサービスを利用してサービスを提供する場合も含む)	体制図、組織図、苦情・質問の受付窓口、責任体制に関する書類等、サービス仕様適合開示書					
27	組織	体制	クラウドサービス提供に際して外部事業者等へ医療情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約に対する体制を医療機関等に対し明確に提示できること。	体制図、組織図、苦情・質問の受付窓口、責任体制に関する書類等、サービス仕様適合開示書					
28	組織	リスク管理	クラウドサービス事業者は、クラウドサービス自体、並びにクラウドサービス内の医療情報に対して分類に基づいたリスク分析を実施し、その結果に応じてリスク低減に必要な管理策、対応措置等を講じる旨を定め、実施するとともに、講じる内容について医療機関等に対し明確に提示できること。	リスクアセスメント手順書、リスク管理規程、リスク管理実施手順、リスク分析・評価結果、リスク評価結果報告書、サービス仕様適合開示書					
29	組織	資産管理	クラウドサービス事業者は、クラウドサービスの運用や資源管理に関して、セキュリティ対策を行う対象として管理し、医療機関等に対し明確に提示できるよう、以下の内容を含む資産台帳を整備し、盗難、紛失の発生を検証するため、定期的な検証により所在確認等を行う等、厳重に管理すること。 (1)全ての媒体及び機器等の管理方法 (2)クラウドサービス内の全ての医療情報 (3)媒体及び機器の利用に関する記録（媒体及び機器の廃棄後も一定期間にわたり記録を維持すること）	資産目録、資産台帳、装置登録リスト、棚卸記録、サービス仕様適合開示書					
30	組織	資産管理	クラウドサービス事業者における資産台帳等には次のような事項を記録すること。 (1)整理番号 (2)資産の名称（医療情報の名称(記載内容等)） (3)資産の医療情報としての種別 (4)データ形式及び見読化手段 (5)資産の所在地と複製の可否及び複製の所在地 (6)資産を保存する媒体及び機器の識別番号等 (7)資産を扱う医療機関等業務の概要 (8)クラウドサービス事業者における管理責任者 (9)設定されたアクセス権限とアクセス権限者 (10)資産の発生日時、保有する期限、廃棄予定日 (11)資産に対する処理の履歴（保存、配送、複製、廃棄等）	資産目録、資産台帳、装置登録リスト					
31	組織	資産管理	クラウドサービス事業者は、全てのクラウドサービス内の医療情報ならびに全ての媒体及び機器等が記録された資産台帳に対して、必要に応じて速やかに閲覧できる状態で管理しておくこと。	資産目録、資産台帳、装置登録リスト、情報セキュリティ実施手順					
32	組織	資産管理	クラウドサービス事業者における、資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限し、アクセス制限を侵害する行為について記録すること。	資産目録、資産台帳、装置登録リスト、情報セキュリティ実施手順、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、設定書・環境定義書					
33	組織	資産管理	クラウドサービス事業者は、クラウドサービスの提供に係る情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。	情報を分類するための指針、実施規程					
34	組織	資産管理	クラウドサービス事業者における情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。	情報を分類するための指針、実施規程					
35	組織	資産管理	クラウドサービス事業者は、重要度等の基準に対して分類を認識できるよう、情報に対して分類の目印となるラベル(識別情報)をつけること（電磁的記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得る)。	情報を分類するための指針、実施規程					
36	組織	資産管理	クラウドサービス事業者は、各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定めること。	情報を分類するための指針、実施規程					
37	組織	職員管理	クラウドサービス事業者における、雇用契約または服務規程等には従業員（委託契約員と派遣職員を含む）の守秘義務に関する内容や不正に情報を扱った場合の罰則（懲戒手続など）を含むこととし、契約時には秘密保持契約に署名を行うこと。違反した場合は適切なペナルティを課すなどの内容を服務規定に定めること。	服務規程、職員規定、雇用契約書、委託契約書、守秘義務契約書、秘密保持契約書、機密保持誓約書					
38	組織	職員管理	クラウドサービス事業者は、個人情報保護ポリシー及び個人情報の安全管理（退職時や契約終了以降の守秘義務も含む）に関する教育・訓練を、従業員（委託契約員と派遣職員を含む）に対して、就業開始時及び就業後の新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。	情報セキュリティ教育・訓練報告書					

整理番号	

評価申請元		評価者	
評価対象プロダクト名			

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
39	組織	職員管理	クラウドサービス事業者は、従業員（委託契約員と派遣職員を含む）が退職した場合、管理していた個人情報及び情報資産の全てについて返却するとともに、就業中に扱った情報や知り得た情報に関する守秘義務についても服務規程等に含め、署名すること。また、システム管理者は返却確認を行うこと。	服務規程、職員規定、雇用契約書、委託契約書、守秘義務契約書、秘密保持契約書、機密保持誓約書、情報資産貸出管理簿、廃棄証明書（マニフェスト）、廃棄記録、廃棄報告書					
40	組織	職員管理	クラウドサービス事業者の情報管理に関する管理方法については、従業員（委託契約員と派遣職員を含む）及びクラウドサービス提供に係る委託先に対して教育を行い、教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料を医療機関等へ明確に提示できるよう用意しておくこと。	服務規程、職員規定、雇用契約書、委託契約書、守秘義務契約書、秘密保持契約書、機密保持誓約書、情報セキュリティ教育・訓練報告書、サービス仕様適合開					
41	組織	職員管理	クラウドサービス事業者の従業員（委託契約員と派遣職員を含む）による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。	ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡					
42	組織	委託管理	クラウドサービス事業者において、サプライチェーンも含めた委託先には自社と同等の個人情報保護方針を遵守させる守秘義務があることを確認し、委託契約を行うこと。	委託契約書、守秘義務契約書、秘密保持契約書、機密保持誓約書					
43	組織	委託管理	クラウドサービス事業者は、サプライチェーンとしての提供も含め、外部事業者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認し、サービスの利用を決定、契約を行うこと。	委託契約書、回線事業者や他のサービス提供事業者との契約					
44	組織	委託管理	クラウドサービス事業者は、外部事業者により提供されるサービスも含め、クラウドサービスの提供状況、運用、維持について定期的に検証すること。提供状況については事前・事後報告を義務づけ、報告内容を確認すること。	委託契約書、回線事業者や他のサービス提供事業者との契約、提供状況に関する報告書					
45	組織	委託管理	クラウドサービス事業者は、外部事業者により提供されるクラウドサービスによりサービスを提供する場合は、クラウドサービス事業者もしくは外部事業者の正規職員が管理している状況で作業を行うことが望ましい。	委託契約書、回線事業者や他のサービス提供事業者との契約、提供状況に関する報告書					
46	組織	事業継続（BCP）	クラウドサービス事業者は、以下の事項について医療機関等に対し明確に提示できること。 (1)障害等が生じた場合の責任分界と稼動を保証するクラウドサービスの範囲 (2)医療情報を保存する場合の、医療機関側で講じうる方策に関する情報提供、必要な外部ファイル等の出力に関する機能の提供の有無、内容 (3)遠隔地に保存するバックアップデータの利用のための機能と代替施設の物理的安全対策等の必要な情報の提供、条件等 (4)緊急時に備えた医療機関等における診療録の見読性の確保を支援する機能をクラウドサービスに含めること及び必要な情報セキュリティ等の情報提供	事業継続計画書、コンテンジェンシープラン、非常時マニュアル、サービス仕様適合開示書					
47	組織	事業継続（BCP）	クラウドサービス事業者は、クラウドサービスに係るBCP及びコンテンジェンシープランの策定を行い、策定したBCP等については模擬試験を含めた適切な方法でレビューするとともに、定期的な見直しを行うこと。 なお、策定される事業継続計画では、次のような事項を含むことが考えられる。 (1)事前準備計画 (2)「非常時」判断手順 (3)関係者の召集、対応本部の設置、所管官庁への連絡体制等、非常時における体制 (4)機器及び作業員の縮退措置及び代替施設の手配措置 (5)バックアップ施設等、代替施設への切替え措置 (6)代替施設運用中のサービス内容 (7)代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮、規定時間外のログオンにおける妥当な承認プロセス等） (8)障害の拡大範囲に関する判断手順、基準 (9)正常復帰に関する回復手順、判断手順、基準	事業継続計画書、コンテンジェンシープラン、非常時マニュアル、事業継続計画書の更新履歴、レビュー表					
48	組織	事業継続（BCP）	クラウドサービス事業者は、クラウドサービスに係るBCP及びコンテンジェンシープランの策定を行うにあたり、事業継続上の要求事項の識別を以下の管理策により実施すること。 (1)医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別すること。 (2)業務プロセス間の相互関係を評価すること。 (3)事業を継続するための業務プロセスの優先順位を医療機関等に対し明確に提示できること。 (4)医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。 (5)医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。	事業継続計画書、コンテンジェンシープラン、事業継続計画書の更新履歴、レビュー表、サービス仕様適合開示書					
49	組織	監査	クラウドサービス事業者は、監査実施について記録し、当該記録の保存･管理方法を、医療機関等に対し明確に提示できること。	監査規程、サービス仕様適合開示書					
50	組織	監査	クラウドサービスにおける監査ログに記録する事項としては次のようなものが考えられる。 (1)作業者情報（作業者ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元IPアドレス） (2)ファイル及びデータへのアクセス、変更、削除記録（作業者ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） (3)データベース操作記録（作業者ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元IPアドレス、設定変更時にはその内容） (4)セキュリティパッチの適用作業（作業者ID、変更されたファイル） (5)特権操作（特権取得者ID、特権取得の可否、利用時刻及び時間、実行作業内容） (6)システム起動、停止イベント (7)ログ取得機能の開始、終了イベント (8)外部デバイスの取り外し (9)IDS･IPS等の情報セキュリティ装置のイベントログ (10)サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）	ログ、各種管理記録、入退室管理記録（認証記録）					
51	サービス仕様	サービスの構成	クラウドサービス事業者は、自身の提供するサービスが医療機関等に対して、何を提供することになるのかの内容(資源並びに機能、その他)について、医療機関等に対し明確に提示できること。	サービス仕様書、機能仕様書一覧、製品マニュアル、サービス構成図					
52	サービス仕様	サービスの構成	クラウドサービス事業者は、提供するクラウドサービスの環境のハードウェア機器、ソフトウェア、ネットワークの構成図及びシステム要件等を説明した資料を作成すること。	サービス仕様書、機能仕様書一覧、製品マニュアル、サービス構成図、SLA					
53	サービス仕様	サービスの構成	クラウドサービス事業者は、提供するクラウドサービスの環境の機器、ソフトウェア、ネットワークの更新仕様に関して資料及びその更新履歴を作成すること。	サービス仕様書、機能仕様書一覧、製品マニュアル、サービス構成図、SLA					
54	サービス仕様	サービスの構成	クラウドサービス事業者は、策定した資料等を医療機関等の求めに応じて提出することについて、開示内容、範囲、条件等を医療機関等に対し明確に提示できること。	サービス仕様書、機能仕様書一覧、製品マニュアル、サービス構成図、SLA、サービス仕様適合性開示書					
55	サービス仕様	サービスの構成	クラウドサービス事業者は、医療情報とそれ以外の情報を区分できる措置を講じること。	運用管理規定、システム仕様書					
56	サービス仕様	サービスの構成	クラウドサービス事業者は、仮想化技術を用いた資源をクラウドサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じること。	システム仕様書、SLA					
57	サービス仕様	サービスの構成	クラウドサービス事業者は、通信経路、通信手順について、通常運用時、非常時の場合のそれぞれについて、医療機関からサービスの提供を行うクラウドサービス事業者の間の起点、終点を明らかにし、クラウドサービスに関係する通信に対し、経路に関わる機器等も対象とし、適切な技術(専用線、IP-VPN、Ipsec、プロトコルを限定し高セキュリティ型で設定したTLS1.3)を使用していることを明らかにすると共に、クラウドサービス事業者として負う責任の範囲、役割を医療機関等に対し明確に提示できること。	サービス仕様書、機能仕様書一覧、製品マニュアル、サービス構成図、SLA、責任分界を示した書類、サービス仕様適合開					
58	サービス仕様	サービスの構成	クラウドサービス事業者は、医療機関等がクラウドサービス利用する際に、交換する情報の機密レベルが低下することが無いことを医療機関等に対し明確に提示できること。	システム仕様書、SLA、サービス仕様適合開示書					
59	サービス仕様	サービスの構成	クラウドサービス事業者は、医療機関等が患者等からの求めに対するが説明責任、管理責任等で応じるために、医療機関等が利用しているクラウドサービス、ならびに医療機関等が患者へ提供しているクラウドサービスに対して、クラウドサービス事業者として負う責任の範囲、役割を医療機関等に対し明確に提示できること。	サービス利用約款、サービス仕様書、責任分界を示した書類、サービス仕様適合開示書					
60	サービス仕様	サービスの構成	クラウドサービス事業者は、クラウドサービスで管理する医療情報に対し、患者等が閲覧可能とする場合、クラウドサービス事業者で対応すべき情報セキュリティ上の措置の条件、内容等を明らかにすると共に、医療機関等及び患者等が閲覧する環境で対応すべき情報セキュリティ対策の情報の提供条件、内容等についてマニュアル等で医療機関等に対し明確に提示できること。	サービス利用約款、サービス仕様書、責任分界を示した書類、サービス仕様適合開示書					
61	サービス仕様	サービスの構成	クラウドサービス事業者は、クラウドサービスに供するサーバーならびにソフトウェア等それぞれ情報セキュリティ要求事項を整理した事項を、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示					
62	サービス仕様	サービスの構成	クラウドサービス事業者は、医療情報を取り扱うクラウドサービスに供する医療情報システムに関する機器及びソフトウェアについて、導入ならびに更新を行う際、将来的な互換性確保を視野に入れて決定するとともに、クラウドサービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行い、医療機関等に対し明確に提示できること。 検討の結果、クラウドサービスの一部又は全部の提供が困難となる場合やクラウドサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行うこと。	システム仕様書、リスク分析・評価結果、リスク評価結果報告書、サービス仕様適合開示書					

整理番号	

評価申請元		評価者	
評価対象プロダクト名			

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
63	サービス仕様	外部サービス利用	クラウドサービス事業者は、自社のクラウドサービスを外部事業者が提供するクラウドサービスを用いて提供する場合に、導入ならびに更新、変更の際、クラウドサービスに供する機器及びソフトウェアについて、将来的な互換性確保を視野に入れるとともに、クラウドサービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行い、外部事業者を決定すること。その際、下記の事項を実施するとともに、医療機関等への対応の内容、条件等について、医療機関等に対し明確に提示できること。 (1)外部事業者がクラウドサービスを停止した際にも、自社のクラウドサービス提供に支障が生じないための対応策を検討すること。 (2)外部事業者のクラウドサービスの停止・変更に伴い、自社が提供するクラウドサービスの一部又は全部の停止、変更（軽微なバージョンアップも含む）等が生じる場合には、影響範囲について分析を行い、その結果、クラウドサービスの一部又は全部の提供が困難となる場合やクラウドサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行うこと。	システム仕様書、他のサービスとの責任分界を示した書類、リスク分析・評価結果、リスク評価結果報告書、事業継続計画書、サービス仕様適合開示書					
64	サービス仕様	外部サービス利用	外部事業者の運営するデータセンター内にサーバーラック等の設置場所を借りて利用する場合、及び、外部事業者の運営するサーバー環境（専有サーバー、仮想プライベートサーバー等）を利用する場合は、外部事業者においても以下の安全対策を行っていることを確認すること。 (1)医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行うこと。 (2)有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。 (3)有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること。 (4)クラウドサービスに供する媒体及び機器を保存する施設や設置場所への不明者の入退を発見するために、入退者に顔写真入りの職員証・名札等の着用を義務付けること。 (5)クラウドサービス事業者の職員は、クラウドサービス事業者の専有する領域にて、クラウドサービス事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。 (6)職員証・名札等を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する。 (7)クラウドサービス事業者職員の退職時には確実に職員証・名札等を回収・廃棄する等、職員証の厳密な発行及び失効管理を行うこと。 (8)職員の業務に応じてクラウドサービスに供する媒体及び機器の設置場所に滞在できる時間を指定すること。 (9)クラウドサービスに供する媒体及び機器の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限すること。 (10)医療情報システムの設置されるサーバーラックには施錠を行い、定められたクラウドサービス事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。 (11)クラウドサービス事業者が医療情報システムの設置されるサーバーラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録すること。 (12)医療情報システムであることが、同じデータセンター内に立ち入る他クラウドサービス事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしないこ	回線事業者や他のサービス提供事業者との契約、他のサービスとの責任分界を示した書類、委託契約書、守秘義務契約書、秘密保持契約書、機密保持誓約書、運用マニュアル					
65	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、医療情報について情報区分に従ってアクセス制御を行えること。また、それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、運用管理規程、設定書・環境定義書					
66	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、医療機関等による情報資産の区分の設定や、情報資産区分に対するアクセス制御の設定の対応について、医療機関等に対し明確に提示できること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、運用管理規程、設定書・環境定義書、サービス仕様適合開示書					
67	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、ユーザを特定し権限を確認するため、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能(ログオン機能等)を含め、与えられた権限外の情報や権限外の操作画面を表示しない、ならびにアプリケーションによる情報の登録、編集、削除等を行う等、情報管理を行うこと。	【運用管理規定】 運用管理規定に、与えられた権限外の情報や権限外の操作画面を表示しないような情報の管理方法を規定する。					
68	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて、医療機関等に対し明確に提示できること。なお、アクセス制御に係る情報の提供について、アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを、医療機関等に対し明確に提示できるこ	サービス仕様適合開示書					
69	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、運用管理規程(ルール)に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できること。資料の提供に係る条件等については、医療機関等に対し明確に提示できること。	サービス仕様適合開示書、運用管理規程					
70	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、クラウドサービス内の契約した医療機関ごとの医療情報を、患者等ごとに管理できる機能を含めること。	システム仕様書					
71	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、予定された保守・運用等を行う際にクラウドサービス内の医療情報を許可なく閲覧させないために、権限設定等の対策を講じると共に、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じること。	システム仕様書					
72	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者が、医療機関等の指示に基づき、クラウドサービス内の医療情報に対する第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないよう対策を講じること。 また、閲覧・取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応を行うこと。	システム仕様書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、設定書・環境定義書、運用管理規程、サービス仕様適合開示書					
73	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、医療情報システムの利用者を特定し識別できるように、アカウントの発行を行うこと（利用者には、医療機関等においてサービスを利用する者のほか、医療情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含め、複数の利用者によるIDの共同利用は行わないこと。ただし当該医療情報システムが他の医療情報システムを利用するためのID（non interactive ID）は除く。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、設定書・環境定義書、アクセス制御に関する証跡、運用管理規程					
74	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、医療情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行うこと。その際、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、設定書・環境定義書、運用管理規程、内部監査記録					
75	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、利用者のなりすまし等を防止するための認証を行うこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、運用管理規程					
76	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、利用者の認証において、多要素認証に対応しうる機能を備えること。なお、厚生労働省ガイドライン第6版（令和5年5月）においては、システム運用編の１４．認証・認可に関する安全管理例として、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、新規導入又は更新するに際しては二要素認証について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とされている。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、運用監視システム、サービス仕様適					
77	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、利用者の認証で採用する複数要素認証に対する認証方式について、医療機関等に対し明確に提示できること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡、運用管理規程、サービス仕様適合開示書、複数要素を利用した認証に関する証跡					
78	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、利用者の認証でパスワード方式を利用する場合は、利用者のパスワードポリシーについて、医療機関等に対し明確に提示できること。	サービス仕様書、情報セキュリティ対策基準、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理					
79	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、利用者の認証でパスワード方式を利用する場合は、利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行うこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
80	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスにおいて、本人の識別・認証に、ユーザIDとパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行うこと。具体的には以下のような対策を行うこと。 (1)利用者に対して乱数から生成した初期パスワードを発行した場合、最初の利用時にその初期パスワードを変更しないと医療情報システムにアクセスできないこと。 (2)初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求めること。 (3)パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上の推定困難な文字列等から構成されるもので定期的に変更される（最低でも２か月以内）、もしくは13文字以上のランダムな文字列が設定されるルールとすること。ただし、多要素認証における一要素としてユーザIDとパスワードを組み合わせて用いる場合は、パスワードの定期的な変更は必ずしも求めなくてよい。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
81	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、パスワード認証に係る以下のルールを実現する措置を講じること。 (1)パスワード変更時には変更前のパスワードの入力を要求すること。 (2)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の不応時間を設定すること。 (3)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仕組みとすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みとすること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
82	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、多要素認証に対応していない場合は、パスワードには十分な安全性を満たす有効期間を設定し、定期的な変更を強制すること。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、クラウドサービス提供側から患者等に対して定期的なパスワードの変更を要求しないこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、設定書・環境定義書、運用管理規程					
83	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、認証に際してID及びパスワードによらない場合でも、ID及びパスワードに関する対策と同等以上の安全性を確保すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
84	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、利用者のパスワードは、十分な強度を持ったハッシュ値での保存を行う等、暗号化して、パスワードを容易に復元できない形で情報を保管すること。また、一般の作業者による閲覧を制限すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、設定書・環境定義書、運用管理規程					
85	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行うこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、設定書・環境定義書、運用管理規程					
86	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行うこと。また、緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
87	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、運用監視システム					
88	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでは、パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、運用監視システム					
89	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでの利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体及び機器等がなくても一時的に認証するための代替的手段・手順を事前に定め、本来の利用者の認証方法による場合とのリスクの差を最小にすること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
90	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、複数要素認証が行えず、代替的手段・手順により医療情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
91	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、医療情報システムのサーバー機器等への同時ログオンユーザ数（OSアカウント等）に適切な上限を設けること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、設定書・環境定義書、運用管理規程					
92	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおける不正なアカウントの検出や防止について、以下の対策を実施すること。 (1)利用者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示すること (2)不正なアカウントの利用を防ぐため、利用者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限すること。 (3)認可されていない利用者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると利用者IDが存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、運用監視システム					
93	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスにおいて、医療情報システムの保守に従事する者及び管理者権限を有する者が当該業務を行う際は、当該要員ごとに発行されたアカウントを用いて、当該医療情報システムにアクセスを行うこと。アカウント情報が漏洩しないようにアカウントを再利用しない等の厳重に管理を行い、アクセスした個人が特定できる形でログなどにより記録し、保存すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規					
94	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、作業者IDは重複がなくユニークに設定し必要最低限の発行数にしたうえで、操作実施者が特定できること。グループIDを利用する場合は、作業者IDを用いること。また、過去に使用したIDについて再利用しないこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
95	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者におけるクラウドサービスでの医療情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の医療情報システム利用に係る認証は、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN ）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせ、2要素認証以上の認証強度のある方法によること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、複数要素を利用した認証に関する証					
96	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、パスワードを医療情報システムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。	運用管理規定、運用マニュアル、情報セキュリティ教育・訓練報告書					
97	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、作業者が変更あるいは退職した際には、ただちに当該作業者IDを利用停止とすること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
98	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、不要な作業者IDが残っていないことを定期的に確認すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
99	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、作業者IDのアクセス可能範囲が許可なく変更されていないことを定期的に確認すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規					
100	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、特権IDの発行は必要な最小限のものに留めることとし、使用時には実施内容を記録すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規					
101	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、特権使用者に昇格可能な作業者IDを制限すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
102	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限すること。また、システムの機能として可能であれば、特権IDで使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
103	サービス仕様	識別・認証・認可（アクセス制御）	クラウドサービス事業者は、クラウドサービスにおいて、管理端末以外からの特権ID による直接ログオンを禁止すること。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
104	サービス仕様	記録（ログ）	クラウドサービス事業者は、提供するクラウドサービスの環境（サーバー、プラットフォーム、データベース、端末等）に、以下の情報をログとして一定期間保存すること。 (1)利用者の利用状況の記録 (2)システム運用状況の記録 (3)例外処理、情報セキュリティ事象の記録	ログ、ログ設計書、システム設計書、アクセス制御に関する証跡					
105	サービス仕様	記録（ログ）	クラウドサービス事業者におけるクラウドサービスにおいて、ログには、医療機関等の管理者が説明責任を果たすための情報（ID、時刻、時間、対象（情報主体単位）等）を含めること。ログ機能を有しない場合には、同レベルの情報の取得、保存について、医療機関等に対し明確に提示できること。	ログ、ログ設計書、システム設計書、アクセス制御に関する証跡					
106	サービス仕様	記録（ログ）	クラウドサービス事業者が提供するクラウドサービスの環境上で取り扱う医療情報の診療録等に関するログ又はこれに代わる情報の保存期間は以下とすること。 (1)法定保存年限が設けられている場合は、当該法定年限以上の保存期間を設けること。 (2)法定保存年限が経過している及び法定保存年限が設けられていない医療情報の保存期間について、医療機関等に対し明確に提示できること。なお、保存期間を設けた場合は、原則として法定保存年限がある医療情報に準じて取り扱うこと。	システム仕様書、サービスに関わる設計書					
107	サービス仕様	記録（ログ）	クラウドサービス事業者は、クラウドサービスの利用者若しくは開発に従事する者又は管理者権限を有する者によるログの、定期的なレビューや検証を行い、不正な行為、提供する環境の異常等がないことを確認すること。また、確認した情報の医療機関等へ提供について、医療機関等に対し明確に提示できること。	ログ、ログ設計書、システム設計書、アクセス制御に関する証跡、サービス仕様適合開示書					
108	サービス仕様	記録（ログ）	クラウドサービス事業者は、ログ情報を不正なアクセスから適切に保護するため、保存方法について以下の管理策を適用すること。 (1)ログデータにアクセスする作業者及び操作を制限し、不正なアクセスを防止すること。 (2)容量超過によりログが取得できない事態を避けるため、ログサーバーの記憶容量を常時監視し、媒体及び機器への書き出し、容量の増強等の対策をとること。 (3)ログデータに対する不正な改ざん及び削除行為に対して、暗号化あるいは定期的に追記不能な媒体及び機器への記録を行う等、検出・防止策を施すこと。	アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、システム仕様書、運用監視システム					
109	サービス仕様	記録（ログ）	クラウドサービス事業者は、ログ上の時刻の信頼性を確保するために、クラウドサービスが提供する環境におけるハードウェア機器（サーバー、ネットワーク機器等）の時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次以上の頻度で行うこと。また、定期的に時刻が同期していることを検証すること。なお医療機関等内の時刻同期については、適切な時刻同期がなされるよう医療機関等と合意をとること。	システム仕様書					
110	サービス仕様	記録（ログ）	クラウドサービス事業者は、クラウドサービスが提供する環境の下記に関する監査に必要なログを取得すること。 (1)運用システムに関わるライブラリプログラムの更新時のログ (2)システム運用情報（システム及びサービス設定ファイル等）の複製及び利用時におけるログ (3)利用者又は開発者等の活動、機器で発生したイベント、システム障害、システム使用状況等を記録したログ	ログ、ログ設計書、システム設計書					
111	サービス仕様	記録（ログ）	クラウドサービス事業者は、ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、ログ参照環境を整備すること。医療機関等の管理者が説明責任を果たすための情報（ID、時刻、時間、対象（情報主体単位）等）を参照可能とし、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等を可能とすること。	システム仕様書、運用管理規程					
112	サービス仕様	情報漏洩対策	クラウドサービスにおける情報交換手順においては搬送の形態によらず次の事項を確実にすること。 (1)発送者、受領者を識別し記録すること。 (2)発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行うこと。 (3)交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと）。 (4)交換された情報に悪意のあるコードが含まれていないことを確実とすること。	情報交換に関するルール、運用管理規程、サービス仕様書					
113	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境の脆弱性に関する情報について、JPCERTコーディネーションセンター（JPCERT/CC）、国家サイバー統括室（NCO）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得・確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、マルウェアである、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）、ランサムウェア等がある。	運用管理規程、情報セキュリティ実施手順、脆弱性管理台帳、マニュアル、ウイルス対策、脆弱性管理、パッチ適用					

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
114	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境に関連する技術的脆弱性については、リスト、台帳等を利用して管理すること。	運用管理規程、情報セキュリティ実施手順、マニュアル、ウイルス対策、脆弱性管理、脆弱性管理台帳、パッチ適用、資産目録、資産台帳、装置登録リスト					
115	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境（サーバー、プラットフォーム、データベース、端末等）に対して、ウイルスやマルウェア等の混入が生じないための手順を策定し、これに則って構築すること。	情報セキュリティ実施手順、開発計画書、開発手順書、運用設計書、運用実施要領、運用手順書、運用管理規程					
116	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおけるウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新すること。	情報セキュリティ実施手順、ウイルス対策ソフトウェア設定書、運用管理規程					
117	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、ウイルスやマルウェア等の対策ソフトウェアにおいて次の設定を行うこと。 (1)リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信） (2)リスク評価の結果として必要であれば定期的にスキャンを実施 (3)媒体及び機器へのデータ書き出し・読み込み時におけるオンデマンドスキャン (4)定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 (5)管理者以外による設定変更やアンインストールの禁止	情報セキュリティ実施手順、ウイルス対策ソフトウェア設定書、運用管理規程					
118	サービス仕様	情報漏洩対策	クラウドサービス事業者は、ソフトウェアの情報セキュリティ等の潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（セキュリティパッチ適用、設定変更等）を決定すること。また、セキュリティパッチの適用前にセキュリティパッチが改ざんされていないこと及び有効性を検証すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
119	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境のハードウェア等に接続できる媒体及び機器の種別及びソフトウェアを限定するため、以下の対策を実施すること。 (1)管理者以外はソフトウェアやデバイスドライバのインストールやアンインストールを不可能とすること。 (2)不要なソフトウェアやドライバがインストールされていた場合は削除すること。 (3)不要なデバイスドライバが追加されていないことを定期的に検証すること。	情報セキュリティ実施手順、運用マニュアル、機能仕様書一覧、設定書・環境定義書、運用管理規程					
120	サービス仕様	情報漏洩対策	クラウドサービスにおいて提供するアプリケーションは、クラウドサービス事業者が開発したアプリケーションを用いること。また、外部事業者が開発したアプリケーションを用いる場合、事前に安全性を十分検証した上で用いること。提供アプリケーションについては、医療機関等から要求があった際に、アプリケーションの構成及び安全性を提示できるエビデンスを提示できること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
121	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境について、環境種別（ハードウェア、プラットフォーム、アプリケーション等）による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、セキュリティ診断					
122	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
123	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境へ外部からプログラムを媒体及び機器で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行うこと。また、クラウドサービスへの影響度を勘案して、最新のセキュリティパッチの適用を行うこと。	情報セキュリティ実施手順、ウイルス対策ソフトウェア設定書、運用管理規程					
124	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて一定期間、悪意のあるコードのチェックが行われていない、もしくは定義ファイル、スキャンエンジンが更新されていない機器について、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策を行うこと。	情報セキュリティ実施手順、ウイルス対策ソフトウェア設定書、運用管理規程					
125	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境に媒体及び機器等の持ち込み機器を接続する際には、以下の対応を行うこと。 (1)持ち込み機器が再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。 (2)不正な機器がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、セキュリティパッチが適用されていること等を接続前に検査を行う仕組みを整備し運用すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
126	サービス仕様	情報漏洩対策	クラウドサービス事業者は、提供するクラウドサービスの環境がウイルス等による攻撃を受けた場合に、医療機関等が厚生労働省等の所管省庁への連絡等、必要な対応を行うために、クラウドサービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求めること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、セキュリティ診断書、非常時マニュアル					
127	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができること。	システム仕様書、機能仕様書一覧					
128	サービス仕様	情報漏洩対策	クラウドサービス事業者は、不正・不審なトラフィックが、提供するクラウドサービスの環境上における内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視すること。	システム仕様書、機能仕様書一覧、不正アクセス防止措置、侵入検知装置、改ざん防止・検知、運用監視システム					
129	サービス仕様	情報漏洩対策	クラウドサービスにおける侵入検知の記録（ログ）には不正アクセス等の事後処理に必要な項目が含まれていること。	システム仕様書、機能仕様書一覧、不正アクセス防止措置、侵入検知装置、改ざん防止・検知、運用監視システム、ログ					
130	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、外部のネットワークを介し医療情報を格納する機器との接続を行う場合、セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、改ざん防止・検知、運用監視システム					
131	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、医療機関等との接続ネットワーク境界には、侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントを検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じること。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、改ざん防止・検知、運用監視システム					
132	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。	情報セキュリティ実施手順、運用マニュアル、設定書・環境定義書、運用管理規					
133	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおいて、侵入検知システム等自身が攻撃・不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施すること。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、情報セキュリティ実施手順、運用マニュアル、運用管理規程					
134	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおけるホスティングの利用時等、ネットワーク境界にクラウドサービス事業者による装置を設置できない場合は、クラウドサービス事業者の提供する個々の情報処理装置に対して、外部からの攻撃等の対策を行うこと。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、情報セキュリティ実					
135	サービス仕様	情報漏洩対策	クラウドサービスにおける侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定を行っていること。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、設定書・環境定義書、改ざん防止・検知、運用監視システ					
136	サービス仕様	情報漏洩対策	クラウドサービス事業者は、クラウドサービスにおけるセキュリティゲートウェイにおいて、不正なIPアドレスを持つトラフィックが通過できないように設定すること（接続機器類のIPアドレスをプライベートアドレスとして設定して、ファイアウォール、VPN装置等のセキュリティゲートウェイを通過しようとするトラフィックをIPアドレスベースで制御する等）。	システム仕様書、機能仕様書一覧、ネットワーク構成図、不正アクセス防止措置、侵入検知装置、情報セキュリティ実施手順、運用マニュアル、運用管理規程					
137	サービス仕様	データ管理	クラウドサービス事業者は、クラウドサービスに係るリスクの分析結果に基づき、提供するサービスの環境の情報についてバックアップを行うこと。バックアップの取得対象、取得頻度、保存方法、保存対象（媒体及び機器）、管理方法等を定め、その内容を医療機関等に対し明確に提示できること。なお、バックアップ先の媒体及び機器の管理方法に応じて、必要な定期的な検査等をおこない、記録内容の改ざん・破壊等がないことを確認し、その内容を医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示書、機能仕様書一覧、設定書・環境定義書、情報セキュリティ実施手順					
138	サービス仕様	データ管理	クラウドサービス事業者は、提供するクラウドサービスの環境を利用する際に、利用可能な資源に係る情報（保存可能容量（残量含む）、利用可能期間、リスク、バックアップ頻度、バックアップ施設、バックアップ方法等）について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示書、機能仕様書一覧、設定書・環境定義					
139	サービス仕様	データ管理	クラウドサービス事業者は、提供するクラウドサービスの環境の情報を保存する場所（内部、可搬媒体、機器等）、その場所ごとの保存可能容量、保存可能期間、リスク等を医療機関等に対し明確に提示できること。なお、媒体及び機器は、情報喪失のリスクを最小限にするため媒体及び機器の製造者により指定される保管環境にて保管すること。	システム仕様書、サービス仕様適合開示書					
140	サービス仕様	データ管理	クラウドサービス提供者は、外部事業者が提供するクラウドサービスを利用する場合においても、保存可能容量、保存可能期間、リスク等の情報を収集し、医療機関等に対し明確に提示できること。なお、仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス提供者が外部事業者との契約上利用可能な資源に関する情報を確認すること。	システム仕様書、回線事業者や他のサービス提供事業者との契約、サービス仕様適合開示書					
141	サービス仕様	データ管理	媒体及び機器に格納するバックアップについては、その媒体及び機器の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日及び有効利用期間より使用終了日を明らかにして管理すること。また、媒体及び機器の有効利用限度期間が近づいた場合は、他媒体及び機器に複写すること。バックアップに関する媒体及び機器に関する情報について、医療機関等に対し明確に提示できること。	運用マニュアル、電子媒体の扱いに関するルール、運用管理規程					
142	サービス仕様	データ管理	クラウドサービス事業者は、バックアップの手順を運用管理規程(ルール)等に含め、従業員及びクラウドサービス提供に係る委託先に対して教育を実施することについて、医療機関等に対し明確に提示できること。	運用管理規程、情報セキュリティ教育・訓練報告書					
143	サービス仕様	データ管理	クラウドサービス事業者は、提供するサービスの環境において、障害発生時においても通常の診療等に影響が生じないようサービスの継続に必要な代替機器、冗長化対策を講じること。	システム仕様書、サービス仕様適合開示					

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス （文書名、ページ番号等）	判定結果	改善策	備考
144	サービス仕様	データ管理	クラウドサービス事業者は、診療録等の情報をハードディスク等の媒体及び機器へ保存する場合、RAID-1又はRAID-6相当以上のディスク障害への対応策を講じること。	システム仕様書、機能仕様書一覧、設定書・環境定義書、サービス仕様適合開示					
145	サービス仕様	データ管理	クラウドサービス事業者は、障害等が生じた場合のクラウドサービスの継続性を保証する水準及び医療機関等の側の代替措置等について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示					
146	サービス仕様	データ管理	クラウドサービス事業者は、診療録等の情報が毀損した際に、速やかに回復するために講じる措置内容、手順及び回復が困難となる場合を想定した対応について、医療機関等に対し明確に提示できること。また、毀損した情報に関する責任の範囲、免責条件等について、医療機関等に対し明確に提示できること。	運用マニュアル、運用管理規程、サービス仕様適合開示書					
147	サービス仕様	データ管理	クラウドサービス事業者は、クラウドサービス内の医療情報を格納する媒体及び機器等の見読性が確保されていることを定期的に確認すること。	運用マニュアル、運用管理規程					
148	サービス仕様	データ管理	クラウドサービス事業者は、クラウドサービス内の医療情報を格納する媒体及び機器等の見読性確保が困難となる可能性がある場合（媒体及び機器の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行うこと。	運用マニュアル、運用管理規程、サービスに関わる設計書					
149	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供する媒体及び機器等の設置場所等の情報セキュリティ境界について、施錠管理を行うこと。	物理的安全管理策概要、情報セキュリティ実施手順書、運用管理規程					
150	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供するサーバー等を格納するラック等について、以下の安全管理策を実施すること。 (1)扉には十分な安全強度を持つ物理的施錠装置を設け、施錠管理を行うこと。 (2)震災時に転倒することが無いよう確実に設置すること。 (3)熱による障害を防ぐため十分な空調設備を設置し、サーバーラック内を十分に換気すること。	物理的安全管理策概要、情報セキュリティ実施手順書、運用管理規程					
151	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供する媒体及び機器等を格納するキャビネット等について、施錠管理を行うこと。	物理的安全管理策概要、情報セキュリティ実施手順書、運用管理規程					
152	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供する媒体及び機器の設置場所について、以下の事項を運用管理規程(ルール)等に規定し、実施すること。 (1)クラウドサービスに供する媒体及び機器の設置場所については、予め届け出を行い、許可された者のみが入退できるように制限すること。 (2)職員の業務に応じてクラウドサービスに供する媒体及び機器の設置場所に滞在できる時間を指定すること。 (3)クラウドサービスに供する媒体及び機器の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。また、作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、定期的に検証の上、不正な行為、システムの異常等を検出すること。 (4)クラウドサービスに供する媒体及び機器の設置場所等の情報セキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができること。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じること。 (5)クラウドサービスに供する媒体及び機器を保存する施設や設置場所への不明者の入退を発見するために、入退者に顔写真入りの職員証・名札等の着用を義務付けること。 (6)クラウドサービスに供する媒体及び機器の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限すること。 (7)クラウドサービスに供する媒体及び機器の設置場所には、クラウドサービス継続に不必要なものは置かないこと。 (8)火災発生時の消火設備が機器に損傷を与えないよう配慮すること。 (9)クラウドサービスに供する媒体及び機器の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないこと。	物理的安全管理策概要、情報セキュリティ実施手順書、運用管理規程					
153	サービス仕様	物理（設備・機器）	クラウドサービスに供する媒体及び機器を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置すること。 特に災害拠点病院の要件においても、病院機能を維持するために耐震構造が望まれていること、病院の基本的な機能を維持するために必要な設備について、自家発電機等から電源の確保が行われていること、設置場所が地域のハザードマップ等を参考にすること、広域災害・救急医療情報システムに参加する必要があることを踏まえると、建物に対する耐震性、電源の冗長性、自家発電設備の有無、立地、安定的に動作させるための空調について、クラウドサービスに使用するデータセンターの仕様を、サービス仕様適合性開示書等に含め、医療機関等に対し明確に提示できること。 なお、詳細はJDCCの「データセンターファシリティスタンダードの概要」が参考となる。	データセンター概要書、立地、構造、免震・耐震構造図、物理的安全管理策概要、情報セキュリティ実施手順書、運用管理規程					
154	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置するとともに、監視映像は記録して期間を定めて管理を行い、必要に応じて事後参照でき措置を講じること。	監視カメラ配置図、画像記録、情報セキュリティ実施手順書、運用管理規程					
155	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスに供する媒体及び機器等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存、状況を確認することで、不正な入退者がないことを確認すること。また、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じること。	監視カメラ配置図、画像記録、情報セキュリティ実施手順書、運用管理規程					
156	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、クラウドサービスの運用・保守端末等を設置している区域は監視カメラ等により適切に記録を取得・保存、状況を確認による監視を行うこと。	監視カメラ配置図、画像記録、情報セキュリティ実施手順書、運用管理規程					
157	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。	建物図面、フロアレイアウト図、建物仕様（壁、天井、床の厚み、扉等）、監視カメラ配置図、画像記録、情報セキュリティ実施手順書、運用管理規程					
158	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、医療情報システムを設置する区画、並びに医療情報を保管する区画の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行う。有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用すること。	建物図面、フロアレイアウト図、建物仕様（壁、天井、床の厚み、扉等）、監視カメラ配置図、画像記録、情報セキュリティ実施手順書、運用管理規程、入退室管理記録（認証記録）、複数要素を利用した認証に関する証跡					
159	サービス仕様	物理（設備・機器）	クラウドサービス事業者は、有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認すること。	入退室管理記録（認証記録）					
160	サービス仕様	物理（設備・機器）	クラウドサービス事業者における医療情報システムの設置されるサーバーラックの施錠装置については、ハードウェアトークン又はICカード等の認証デバイス、暗証番号（PIN ）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせ、2要素認証以上の認証強度のある方法によること。	複数要素を利用した認証に関する証跡					
161	サービス仕様	ネットワーク	クラウドサービス事業者は、回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、医療機関等に対し明確に提示できること。	ネットワーク機器の仕様書、設定に関する記述文書、責任分界を示した書類、サービス仕様適合開示書					
162	サービス仕様	ネットワーク	クラウドサービス事業者は、クラウドサービスにおけるネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために、以下の事項について、医療機関等に対し明確に提示できること。 (1)経路の安全性確保のため、IPSec+IKEへの対応や閉域ネットワークへの対応等及びその条件等。 (2)ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲。 (3)医療機関等がチャネル・セキュリティの確保を閉域ネットワークの採用に期待する場合、クラウドサービスの閉域性の範囲に関する情報。	システム仕様書、サービス仕様適合開示書					
163	サービス仕様	ネットワーク	クラウドサービス事業者は、クラウドサービスにおけるネットワークにおいて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために、以下の必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行うこと。 (1)アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐための必要な措置（サーバー証明書の導入等）。 (2)一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策。	システム仕様書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
164	サービス仕様	ネットワーク	クラウドサービス事業者は、医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。その際、以下の対策も講じること。 (1)医療機関等が外部接続するサーバー等とクラウドサービス事業者のサーバーとの間の相互認証。 (2)事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策。 (3)医療機関等が採用する通信方式認証手段(PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法)が妥当なものであることの確認について、医療機関等に対し明確に提示できること。	システム仕様書、ネットワーク機器の仕様書、設定に関する記述文書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程、サービス仕様適合開示書					
165	サービス仕様	ネットワーク	クラウドサービス事業者は、クラウドサービスにおける送信元と送信先の間で、暗号化等の情報そのものに対する情報セキュリティ対策を実施すること。 なお、電子的に情報を転送する際には以下の対策を実施すること。 (1)送信者、受信者は相互に電子的に認証を行って相手の正当性を検証する。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 (2)送受信する経路は適切な方法で傍受のリスクから保護すること。 (3)受信した情報について経路途中での損傷、改ざんが無いことを検証すること。	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					
166	サービス仕様	ネットワーク	クラウドサービス事業者の提供するクラウドサービスにおいてVPN接続を行う場合には以下の事項に従うこと。 (1)接続時にVPN装置間で相互に認証を行うこと。 (2)傍受、リプレイ等のリスクを最小限に抑えるために、適切な暗号技術を利用すること。 (3)インターネット上のトラフィックがVPNチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。 (4)複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPNチャンネルを医療機関等別に構築する等の対策を実施すること。	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム、運用管理規程					

整理番号	

評価申請元		評価者	
評価対象プロダクト名			

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
167	サービス仕様	ネットワーク	クラウドサービスにおけるルータ等のネットワーク機器は、ISO15408で規定されるセキュリティターゲット又はそれに類する文書が、各ガイドラインに適合しているものを選定すること。なお、ネットワーク機器及びサーバー、端末の利用していないネットワークポートへの物理的な接続を制限すること。	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、運用管理規程					
168	サービス仕様	ネットワーク	クラウドサービス事業者は、クラウドサービスで利用するネットワーク(VPN等)に関する経路設定における事業者の役割分担、責任分界等について、医療機関等に提示すると共に、医療機関等の施設内のルータ、端末等の経路設定により異なるサービスと提供するクラウドサービスとの中継等の送受信がされないよう、注意喚起として医療機関等に対し明確に提示できること。	ネットワーク構成図、ネットワーク機器の仕様書、設定に関する記述文書、責任分界を示した書類、サービス仕様適合開					
169	サービス仕様	ネットワーク	クラウドサービス提供に際して、ソフトウェア型のIPsec 又はTLS1.3 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施すること。（なお、TLS1.2を使用せざるを得ない場合は、その合理的な理由等について医療機関等に対し明確に提示できること。）	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、運用管理規程					
170	サービス仕様	ネットワーク	クラウドサービスに対して医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.3 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、医療機関等に対し明確に提示できること。（なお、TLS1.2を使用せざるを得ない場合は、その合理的な理由等について医療機関等に対し明確に提示できること。）	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、運用管理規程、サービス仕様適合開示書					
171	サービス仕様	ネットワーク	クラウドサービスの提供においてTLSを用いる際には、TLS1.3に対応した措置を講じるほか、医療機関等がメールの暗号化（S/MIME等）やファイルの暗号化その際、暗号化に関しては、以下の事項に対応でき、その実施事項について医療機関等に対し明確に提示できること。なお、TLS1.2を使用せざるを得ない場合は、その合理的な理由等について医療機関等に対し明確に提示できること。 (1)暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。 (2)暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。 (3)電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。 (4)暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。 (5)医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。 (6)暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用すること。 (7)暗号鍵の生成は耐タンパー性を有するICカード、USBトークンデバイスといった安全な環境で実施すること。 (8)暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うこと。 (9)電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できること。	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、運用管理規程					
172	サービス仕様	ネットワーク	クラウドサービスに対してオープンなネットワークを介してHTTPS を利用した接続で行う際は、TLS の設定はサーバー/クライアントともに、IPAより公開されている「TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行うこと。	システム仕様書、暗号化対策に関する仕様を提示した書類等、ネットワーク機器の仕様書、設定に関する記述文書、運用管理規程					
173	サービス仕様	ネットワーク	クラウドサービス事業者の提供するクラウドサービスにおいて、SSL-VPNは、原則として使用しないこと。 やむを得ずSSL-VPNを利用する場合は、TLS 暗号設定ガイドラインに基づき、「クライアント型」でのVPNとすることとし、その利用についての合理的な理由等について医療機関等に対し明確に提示できること。	システム仕様書、サービス構成図、ネットワーク構成図					
174	サービス仕様	ネットワーク	医療機関等の利用者が、医療機関等の外部からクラウドサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担、責任分界等について、医療機関等に対し明確に提示できること。	ネットワーク構成図、ネットワーク機器の仕様書、設定に関する記述文書、責任分界を示した書類、サービス仕様適合開					
175	サービス仕様	ネットワーク	クラウドサービスの提供において、医療情報システムからインターネット等のオープンネットワークを介した外部事業者のクラウドサービスを利用する場合、以下に挙げるクラウドサービスとの接続に限定すること。他に必要なクラウドサービスがある場合には、医療機関等の合意を得てから利用すること。 (1)外部からの医療情報システムの稼働監視・遠隔保守 (2)セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード (3)オペレーティングシステム及び利用アプリケーションのセキュリティパッチ等のダウンロード (4)電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス (5)ファイアウォール、IDS･IPS などのセキュリティ機器に対する不正アクセス監視 (6)時刻同期のための時刻配信サーバーへのアクセス (7)これらのクラウドサービスを利用するために必要なインターネットサービス（ドメインネームサーバーへのアクセス等） (8)その他の医療情報システムの稼動に必要なサービス（外部認証サーバー、外部医療情報データベース等）	システム仕様書、サービス構成図、ネットワーク構成図					
176	サービス仕様	個別サービス仕様（ブラウザ）	クラウドサービス事業者の提供するクラウドサービスにおいては、ウェブブラウザの接続するサーバーを業務上必要なサーバーに限定すること。	システム仕様書、設定書・環境定義書					
177	サービス仕様	個別サービス仕様（ブラウザ）	クラウドサービス事業者の提供するクラウドサービスにおいては、ウェブブラウザの設定で、認可していないサイトから、拡張機能等のプログラムコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバーのみを認可する）。また、許可したサイトからのダウンロードにおいても、悪意のあるコード対策ソフトウェアで対策漏れの無いように設定すること。	システム仕様書、設定書・環境定義書					
178	サービス仕様	個別サービス仕様（ブラウザ）	クラウドサービス事業者の提供するクラウドサービスにおいては、ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うこと。	システム仕様書、設定書・環境定義書					
179	サービス仕様	個別サービス仕様（e-文書法）	クラウドサービス事業者は、ｅ-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、医療機関等に対し明確に提示できること。 (1)医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様。 (2)正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
180	サービス仕様	個別サービス仕様（e-文書法）	クラウドサービス事業者は、ｅ-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、医療機関等に対し明確に提示できること。 (1)クラウドサービスとの連携におけるインタフェースの構築に関する役割分担、責任分界。 (2)正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
181	サービス仕様	個別サービス仕様（e-文書法）	クラウドサービス事業者は、ｅ-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、医療機関等に対し明確に提示できること。 (1)確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様 (2)入力された内容についての記録確定前における確認の可否等についての仕様 (3)記録の確定権限に関する仕様 (4)確定した記録の追記・削除の機能等に関する仕様 (5)確定した記録の原状回復の機能等に関する仕様 (6)記録の自動確定機能等に関する仕様 (7)代替的な確定権限の機能等に関する仕様	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
182	サービス仕様	個別サービス仕様（e-文書法）	真正性が求められる医療情報を取り扱うクラウドサービスでは、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含めること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
183	サービス仕様	個別サービス仕様（e-文書法）	真正性が求められる医療情報を取り扱うクラウドサービスでは、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含めること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
184	サービス仕様	個別サービス仕様（e-文書法）	クラウドサービス事業者は、真正性が求められる医療情報を取り扱うクラウドサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
185	サービス仕様	個別サービス仕様（e-文書法）	真正性が求められる医療情報を取り扱うクラウドサービスでは、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能、及び代行入力後の確定操作（承認）に関する機能を含めること。	システム仕様書、サービス仕様書、真正性の確保、見読性の確保、保存性の確保に関する書類、サービス仕様適合開示書					
186	サービス仕様	個別サービス仕様（電子署名）	クラウドサービス事業者は、法令で署名又は記名･押印が義務付けられた文書等において、記名･押印を電子署名に代える場合に、保健医療福祉分野PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
187	サービス仕様	個別サービス仕様（電子署名）	クラウドサービス事業者は、保健医療福祉分野PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名･押印を電子署名で行うクラウドサービスを提供する場合には、当該クラウドサービスにおける本人確認方法及び検証方法、ならびに医師等の国家資格の確認の電子的検証方法について、医療機関等に対し明確に提示できること。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律（平成12 年法律第102 号）」 第2 条1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該クラウドサービスにおける本人確認方法及び検証方法、ならびに医師等の国家資格の確認の電子的検証方法について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
188	サービス仕様	個別サービス仕様（電子署名）	クラウドサービス事業者は、公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名･押印を電子署名で行うクラウドサービスを提供する場合に、当該クラウドサービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
189	サービス仕様	個別サービス仕様（電子署名）	クラウドサービスにおいて電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。	システム仕様書、サービス仕様書					

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
190	サービス仕様	個別サービス仕様（電子署名）	クラウドサービスにおいて暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリボジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うこと。	システム仕様書、サービス仕様書、アクセス管理規程、ユーザ管理システム、ユーザ認証システム					
191	サービス仕様	個別サービス仕様（電子署名）	クラウドサービスにおいて電子署名法に基づき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できること。そのため、暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。	システム仕様書、サービス仕様書					
192	サービス仕様	個別サービス仕様（電子署名）	クラウドサービスにおいて電子署名を施す情報に対しては、タイムスタンプを付与すること。この場合には、以下の事項等について、医療機関等に対し明確に提示できること。 (1)タイムスタンプの内容・検証方法 (2)法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法、 (3)当該情報を長期保存する場合に講じる対策 (4)電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法	システム仕様書、サービス仕様書、サービス仕様適合開示書					
193	サービス仕様	個別サービス仕様（電子署名）	クラウドサービス事業者は、医療機関等で電子署名されたデータを検証するためのルート認証機関の公開鍵証明書を安全な経路で入手し、別の経路で入手したフィンガープリントと比較して真正性を検証すること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
194	サービス仕様	個別サービス仕様（留意する機器等）	クラウドサービス事業者は、クラウドサービスの利用に際して、医療機関等が無線LANを利用する場合に必要な情報セキュリティ対策について、クラウドサービス事業者との役割分担、責任分界等について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
195	サービス仕様	個別サービス仕様（留意する機器等）	クラウドサービス事業者は、IoT機器の利用を含むクラウドサービスを提供する場合、以下を対応すること。 (1)医療機関等との責任分界について、医療機関等に対し明確に提示できること。 (2)IoT機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視すること。 (3)利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
196	サービス仕様	個別サービス仕様（留意する機器等）	クラウドサービス事業者は、クラウドサービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止すること。仮にBYODを医療機関等から許可され個人所有の機器を利用する場合には、利用者が所有する機器からの情報漏えい等を防止する観点から、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分ける、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すなど、医療機関が管理する端末と同等の対策を施し、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
197	サービス仕様	個別サービス仕様（留意する機器等）	クラウドサービス事業者は、クラウドサービスの提供に係る目的（開発、保守、運用含む）機器について、サービスに関する情報を格納する場合は、公衆無線LANへの接続を行わないこと。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
198	サービス仕様	個別サービス仕様（オンライン診療）	クラウドサービス事業者は、オンライン診療システムを含む関連したシステムにおいて医療情報システムとの接続がある場合には、関連したシステムにおいても医療情報に配慮した対策を実施すること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
199	サービス仕様	個別サービス仕様（オンライン診療）	クラウドサービス事業者は、クラウドサービスでの患者側端末で利用するオンライン診療システムの機能において、オンライン診療の実施中に医療情報システムと接続する機能等を含まないこと、及びこれに関する情報提供について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
200	サービス仕様	個別サービス仕様（オンライン診療）	クラウドサービス事業者は、医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様書、サービス仕様適合開示書					
201	運用	運用	クラウドサービス事業者の職員は、クラウドサービス事業者の専有する領域にて、クラウドサービス事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
202	運用	運用	クラウドサービス事業者において、職員証・名札等を紛失あるいは不正利用された疑いがあった際には、ただちに管理者に連絡すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
203	運用	運用	クラウドサービス事業者は、クラウドサービス事業者職員の退職時には、確実に職員証・名札等を回収･廃棄する等、職員証の厳密な発行及び失効管理を行うこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
204	運用	運用	クラウドサービス事業者は、クラウドサービスにおけるデータセンターやリモートメンテナンスで運用に利用する端末に対し、運用中の画面が運用者以外の者の視野に入らないよう、覗き見対策のシートを貼る等の対策を行うこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
205	運用	運用	クラウドサービス事業者は、データセンターやリモートメンテで運用する場所において、個人情報が存在するPC等の重要な機器に盗難防止用チェーンを設置すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
206	運用	運用	クラウドサービス事業者は、クラウドサービスの運用･保守端末等に、クリアスクリーン等の情報漏洩防止策を講じることを運用管理規程(ルール)等に定めること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
207	運用	運用	クラウドサービス事業者は、医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、具体的な適用内容を医療機関等に対し明確に提示できること。 (1)離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。 (2)アクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、サービス仕様適合開示書					
208	運用	情報管理	クラウドサービス事業者は、次の情報交換方法について予め、医療機関等に対し明確に提示できること。 (1)情報を媒体及び機器に記録して交換する際の手順 (2)情報をネットワーク経由で文書ファイル形式にて交換する際の手順 (3)情報をネットワーク経由でアプリケーション入力にて交換する際の手順 (4)情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順	情報セキュリティ実施手順、運用マニュアル、運用管理規程、サービス仕様適合開示書					
209	運用	情報管理	クラウドサービス事業者は、媒体及び機器について保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮し、クラウドサービス事業者施設外への不要な持ち出しを行わないこと。持ち出す場合は、追記のできない光学メディア（CD-R、DVD-R等）を用い、情報交換作業終了後、媒体及び機器を物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等に対して報告し、破棄記録を提出するもしくは同等の手段をとる等の方式にて確実に廃棄処分すること。持ち出した際に外部のネットワークに接続する場合については、接続条件、安全管理措置等について運用管理規定（ルール）等として明確にし、医療機関等に対し明確に提示できること。	電子媒体の扱いに関するルール、情報セキュリティ実施手順、運用マニュアル、運用管理規程、情報資産持ち出し管理簿					
210	運用	情報管理	クラウドサービス事業者は、物理的に情報を搬送する際には以下の対策を実施すること。 (1)医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。 (2)配送時の作業については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。 (3)配送業者等による媒体及び機器の抜き取り等を防ぐため、交換する媒体及び機器の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。 (4)配送業者等による媒体及び機器からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。 (5)媒体及び機器を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。 (6)媒体及び機器により情報を交換する場合、移送中の安全管理上のリスクがある場合には媒体及び機器内のデータに暗号化を施すこと。	電子媒体の扱いに関するルール、情報セキュリティ実施手順、運用マニュアル、運用管理規程、情報資産持ち出し管理簿					
211	運用	情報管理	クラウドサービス事業者は、情報を格納する媒体及び機器について、以下の対応を行うこと。 (1)媒体及び機器へは起動パスワードの設定を行い、ログイン及びアクセスについては、複数の認証要素を組み合わせて行うこと。設定するパスワードについては、デフォルトからは変更し、利用者を識別・認証す際のパスワードと同様の基準で、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じること。 (2)媒体及び機器等を持ち出す場合の手順には、媒体及び機器自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含めること。 (3)当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。また、その手順を定めること。 (4)文字列を利用したパスワードは予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討すること。 (5)情報交換目的やバックアップ目的で大容量の媒体及び機器(MT、DAT、半導体記憶装置、ハードディスク等)を用いて複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。	電子媒体の扱いに関するルール、情報セキュリティ実施手順、運用マニュアル、運用管理規程、情報資産持ち出し管理簿					
212	運用	情報管理	クラウドサービス事業者における、医療情報を保存する医療情報システムのサービスを提供する場合は、一定以上の情報セキュリティが確保されていない無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LANを利用しないこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
213	運用	情報管理	クラウドサービス事業者は、管理する個人情報又はこれを格納する媒体及び機器等に関する運用管理規程(ルール)に以下の内容を定め、医療機関等に対し明確に提示できること。 (1)管理する個人情報又はこれを格納する媒体及び機器等に対する、クラウドサービス提供上の定期的な要否の確認実施。 (2)クラウドサービス提供上不要とされた個人情報及びこれを格納する媒体及び機器についての破棄手順。 (3)クラウドサービス提供上不要とされた個人情報及びこれを格納する媒体及び機器の破棄に際して、医療機関等が不測の損害を被らないための措置（事前に破棄の基準等を告知する等）。	情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程					
214	運用	情報管理	クラウドサービス事業者は、媒体及び機器の廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等に対して報告し、破棄記録を提出もしくは同等の手段をとり、医療機関等に対し明確に提示できること。	情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程、廃棄証明書（マニフェスト）、廃棄記録、廃棄報告書					
215	運用	情報管理	クラウドサービス事業者における、物理的な媒体及び機器の破壊措置についてはクラウドサービス事業者自身で行うことが望ましいが、外部事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておくこと。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておくこと。	体制図、組織図、情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程、廃棄証明書（マニフェスト）、廃棄記録、廃棄報告					
216	運用	情報管理	クラウドサービス事業者は、媒体及び機器の廃棄に際しサーバー等のBIOSパスワード、媒体及び機器のパスワード等のハードウェアに対するパスワードを消去すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					

整理番号	

評価申請元			評価者	
評価対象プロダクト名				

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス （文書名、ページ番号等）	判定結果	改善策	備考
217	運用	情報管理	クラウドサービス事業者において、媒体及び機器等を医療情報システム内の別の媒体及び機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
218	運用	保守・品質管理	クラウドサービス事業者は、提供するクラウドサービスの環境上のハードウェア機器等は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行うこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、保守作業報告書					
219	運用	保守・品質管理	クラウドサービス事業者は、ソフトウェア開発を行う際に、ソフトウェア障害の影響を避けるため、以下の対策を行うこと。 (1)運用施設とは直接に接続されていない開発用の施設を用いて行うこと。また、開発施設において不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合、悪意のあるコードに対して最新の情報収集を実施すると共に、対策ソフトウェア等の管理策を実施すること。 (2)アプリケーションの安全性診断は提供しているクラウドサービスに対して直接実施せず、別途、試験環境を用意して行うこと。	情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程					
220	運用	保守・品質管理	クラウドサービス事業者は、開発したソフトウェアを運用施設へ導入する際、以下の対策を行うこと。 (1)不正なソフトウェアの書き換えリスクを避けるため、ソフトウェアに対する改ざん防止、検知策（ソースコードレベルでの検証）を実施し、十分な試験を行うこと。 (2)システム運用情報（システム及びサービス設定ファイル等）の複製及び利用や運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、ログ					
221	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、医療機関等に対し明確に提示できること。	SLA、サービス仕様適合開示書					
222	運用	保守・品質管理	クラウドサービス事業者は、医療情報システムの保守業務を行う際に、事前に医療機関等の管理者に対して書面による通知を行い、保守業務実施後は医療機関への報告を行うこと。事前の了解を得ることが出来ない場合の対処について策定しておき、医療機関等に対し明確に提示できること。	情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程					
223	運用	保守・品質管理	クラウドサービス事業者は、事前の通知には保守業務の影響範囲を明記し、完遂できなかった場合の復旧時間を含めること。						
224	運用	保守・品質管理	クラウドサービス事業者は、医療情報システムの動作確認に際し、作業は守秘義務が課された従業員により動作確認を行う旨を含めた手順を定め、医療機関等に対し明確に提示できること。 (1)クラウドサービス事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。 (2)保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。 (3)クラウドサービス提供に際し、直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 (4)クラウドサービス事業者が再委託を行うか否かを明確にし、再委託を行う場合はクラウドサービス事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。 (5)プログラムの異常等で、保存データを救済する必要があるとき等、やむを得ない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。	情報セキュリティ実施手順、運用マニュアル、守秘義務契約書、秘密保持契約書、機密保持監約書、情報セキュリティ教育・訓練報告書、サービス仕様適合開示書、運用管理規程、保守作業報告書					
225	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスにおける情報処理装置及びソフトウェア等の適切な変更手順に対して、以下の事項を、医療機関等に対し明確に提示できること。なお、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。 (1)変更についての影響が及ぶ関係者への通知プロセス (2)装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等） (3)申請承認プロセス (4)変更試験プロセス (5)変更作業に支障が発生した場合の復旧手順 (6)変更終了確認プロセス (7)変更に伴う影響を監視するプロセス、等。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
226	運用	保守・品質管理	クラウドサービス事業者は、医療情報システムの保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程(ルール)及び安全管理措置等への対応を、当該外部事業者に対して求めること。また、その実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認すること。	運用管理規程、委託契約書、守秘義務契約書、秘密保持契約書、機密保持監約書					
227	運用	保守・品質管理	クラウドサービス事業者は、外部事業者が提供するクラウドサービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。	運用管理規程、委託契約書、回線事業者や他のサービス提供事業者との契約					
228	運用	保守・品質管理	クラウドサービス事業者は、保守作業を外部事業者に再委託する場合には、クラウドサービス提供者の基準と同様となっていることを確認して選定し、選定した外部事業者について、医療機関等に対し明確に提示できること。その際の管理策として、下記を実施すること。 (1)外部事業者により提供されるクラウドサービスの安全管理策及びサービスレベルが十分であることを確認すること。 (2)クラウドサービスの提供状況、運用、維持について定期的に検証すること。提供状況については事前・事後報告を義務づけ、報告内容を確認すること。 (3)クラウドサービス実施について、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を行い、点検確認すること。 (4)クラウドサービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。 (5)クラウドサービスを実施する人員は予め届け出を行い、実施時に不正な人員を受入れず、正規職員が管理している状況で作業を行うこと。 (6)保守会社ならびに作業員各人と守秘義務契約を締結し、これを遵守させること。 (7)クラウドサービス実施にともなう処理施設内への立ち入り手順に関しては、クラウドサービス事業者の入室、退室手順に準ずること。 (8)クラウドサービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。 (9)メンテナンスの際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すと共に、詳細なオペレーション記録を保守操作ログとして記録し、アクセスした医療情報に対して、指定時間内で患者毎に何回アクセスしたかが確認できること。（システム利用者を模して操作確認を行う場合も同様） (10)保守要員個人の専用アカウント情報は外部流出等による不正使用の防止の観点から、要員の離職や担当替え等に対して速やかにアカウントを削除できるよう、アカウント管理体制を整えておくこと。 (11)動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。 (12)やむを得ない状況で個人情報を含むデータを組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程(ルール)を定めると共に、作業に対して詳細な作業記録を残し、医療機関等の監査に応じること。 (13)リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。 (14)リモートメンテナンスにおいて、やむを得ずクラウドサービス事業者がファイルを医療機関等に送信等行う場合は、送信側で無害化処理が行っていることを確認すること。 (15)診療録等を保管している設備に障害が発生した場合等で、やむを得ず患者情報等にアクセスする必要がある場合においても、委託元の医療機関とうに許可を求めた上で、通常と同様の秘密保持を行うこと。	委託契約書、守秘義務契約書、秘密保持契約書、機密保持監約書、情報セキュリティ実施手順、運用マニュアル、サービス仕様適合開示書、運用管理規程					
229	運用	保守・品質管理	クラウドサービス事業者は、医療情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、医療機関等に対し明確に提示できること。	体制図、運用管理規程、サービス仕様適合開示書					
230	運用	保守・品質管理	クラウドサービス事業者は、保守業務により、医療機関等がクラウドサービスを利用できない状況に陥らないような対応策を講じ、その手順を、医療機関等に対し明確に提示できること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、サービス仕様適合開示書					
231	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスにおけるオペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
232	運用	保守・品質管理	クラウドサービス事業者は、保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行い、その結果、変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、変更手順を策定し、情報処理業務の停止時間等、影響を最小限に抑える方策と方策に対する計画をたて、保守作業については十分な余裕を持って事前に医療機関等に通知し実施すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程、サービス仕様適合開示書					
233	運用	保守・品質管理	クラウドサービス事業者は、不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施し、潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（セキュリティパッチ適用、設定変更等）を決定すること。セキュリティパッチの適用前にセキュリティパッチが改ざんされていないこと及び有効性を検証すること。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
234	運用	保守・品質管理	クラウドサービス事業者の提供するクラウドサービスにおいては、医療情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。操作ログにより、アクセスされた情報についての状況をレビューできる機能を有し、医療機関等に対し明確に提示できること。	情報セキュリティ実施手順、運用マニュアル、ログ、運用管理規程、サービス仕様適合開示書					
235	運用	保守・品質管理	クラウドサービス事業者は、データセンターにおいてサーバーラックを開錠する場合、事前連絡を原則とし、医療情報システム及び情報に影響を与えないこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
236	運用	保守・品質管理	クラウドサービス事業者は、医療機関等と合意の上で、保守に関わる目的で医療情報を格納した機器を持ち出す場合は手順書を策定し、医療機関等に対し明確に提示できること。	情報セキュリティ実施手順、運用マニュアル、情報資産持ち出し管理簿、運用管理規程、サービス仕様適合開示書					
237	運用	保守・品質管理	クラウドサービス事業者は、医療情報システム内の全ての情報（コピーを含む）の持ち出しの必要がある場合には、全ての場合において個人情報の消去及び元のデータを復元できないデータに置き換え、十分に安全性が補償されていることを当該医療機関に示し、了承を得た上で行うこと。なお、ここでいう「持ち出し」とは、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
238	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスにおいて運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類、その他不必要なファイルなどを運用システム上に置かないこと。	情報セキュリティ実施手順、運用マニュアル、運用管理規程					
239	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスにおいてアプリケーションの安全性診断を提供しているサービスに対して直接実施せず、別途、試験環境を用意して行うこと。	情報セキュリティ実施手順、運用マニュアル、サービス仕様、サービス構成、運用管理規程					
240	運用	保守・品質管理	クラウドサービス事業者は、診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示書					
241	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスにおける医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を医療情報システムに備えること。加えて、これが困難な場合の措置について、医療機関と予め検討し、医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示書					

整理番号	

評価申請元		評価者	
評価対象プロダクト名			

項番	分類		確認項目		チェックシートへの対応内容並びに、内容を確認したエビデンス等		評価員が記入する欄		参考
No.	大分類	中分類	対策項目	確認対象物例・エビデンス例	対応策	確認したエビデンス（文書名、ページ番号等）	判定結果	改善策	備考
242	運用	保守・品質管理	クラウドサービス事業者は、医療情報を保存･交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。変更などの実施時には、クラウドサービスの利用に与える影響を確認し、その結果、クラウドサービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、他の医療情報システムとのデータ連携等を考慮しつつ対応に必要な措置に関する具体的な情報提供に関して、医療機関等に対し明確に提示できること。仮に変更の結果サービス利用が終了となる場合は、利用終了に関する対策を講じ、医療機関等に対し明確に提示できること。	システム仕様書、SLA、重要事項説明書、サービス仕様適合開示書					
243	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービスに供する医療情報システムについて、定期的に劣化状況等に関する検査を行い、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、クラウドサービスへの影響範囲について分析を行い、必要な措置を講じること。終了等により、クラウドサービスの一部又は全部の提供が困難となる場合やクラウドサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行うと共に、医療機関等への対応の内容、条件等について、医療機関等に対し明確に提示できるこ	システム仕様書、SLA、重要事項説明書、サービス仕様適合開示書					
244	運用	保守・品質管理	クラウドサービス事業者は、クラウドサービス提供に必要な医療情報システムの保守を院内またはリモートメンテナンスで行う場合、その旨を医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示					
245	運用	保守・品質管理	クラウドサービス事業者は、リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、医療情報システムへの不正な侵入が生じないよう安全管理措置を講じること。保守作業は最小限の時間に努めるため計画をたて実施すること。また策定した手順、計画等について医療機関等に対し明確に提示できること。	システム仕様書、サービス仕様適合開示書					
246	運用	保守・品質管理	クラウドサービス事業者は、リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じること。	システム仕様書、ユーザ管理システム、ユーザ認証システム					
247	運用	保守・品質管理	クラウドサービス事業者は、リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認すること。	保守作業報告書、ログ、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡					
248	運用	非常時	クラウドサービス事業者は、非常時に用いる利用者のアカウント及び非常時用機能の有効化のための措置について、医療機関等に対し明確に提示できること。	非常時マニュアル、サービス仕様適合開示書					
249	運用	非常時	クラウドサービス事業者は、非常時に用いる利用者のアカウントの利用状況について、定期的にレビューを行うこと。	ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡					
250	運用	非常時	クラウドサービス事業者は、非常時に用いる利用者のアカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じること。	ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡					
251	運用	非常時	クラウドサービス事業者は、非常時に有効化した利用者のアカウント及び非常時用機能については、正常復帰後、速やかに無効化を図ること。	非常時マニュアル、ユーザ管理システム、ユーザ認証システム、アクセス制御に関する証跡					
252	運用	非常時	クラウドサービス事業者は、サイバー攻撃等により、クラウドサービスの提供に支障が生じた場合に、以下の措置を講じること。 (1)原因探査に必要なログ等の記録を保全すること。 (2)クラウドサービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告すること。 (3)医療機関等が所管官庁への連絡・報告のために提供する資料の範囲、条件等について、医療機関等に対し明確に提示できること。なお、その際に医療機関が円滑に資料提供できるよう、クラウドサービスの提供に用いるアプリケーション、プラットフォーム、サーバー・ストレージ等は国内法の執行がおよぶ場所に設置すること。	契約書、サービス仕様書、重要事項説明書、非常時マニュアル、サービス仕様適合開示書					
253	運用	非常時	クラウドサービス事業者は、非常時に行ったデータ処理の結果が、クラウドサービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じること。	非常時マニュアル					