「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の見方

項目名		解説
対策項目	大項目 小項目 No. 内容	対策項目例に関連する従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインの要求事項を、「人的・組織的」・「物理的」・「技術的」の３つの対策の観点毎に整理・統合した内容。 主な実施主体として、対象事業者を想定する。
	区分	◎：従前の情報処理事業者ガイドライン及びクラウド事業者ガイドラインにおける遵守事項に該当 ○：従前の情報処理事業者ガイドラインにおける推奨事項に該当
対策項目により対策可能なリスクシナリオ例		対策項目により対策可能となる、代表的なリスクシナリオを例示
関連する医療情報安全管理ガイドラインの要求事項	項番 区分 内容	関連する医療情報安全管理ガイドラインの要求事項。 主な実施主体として、医療機関等を想定する。

記載全般に係る注意事項

別紙2における「利用者」という表記については、従前のクラウド事業者ガイドラインと同様に、医療機関等においてサービスを利用する者のほか、医療情報システム等の運用も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た位置づけとしている。対象事業者は関連する情報流やリスクによって利用者が異なることに留意すること。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1. 人的・組織的対策								
1.1. 規程・手順の策定	①アクセス管理規定の策定	①-1	医療情報システム等へのアクセス制限、記録、点検等を定めたアクセス管理規定を作成し、医療機関等の求めに応じて提出できる状態にしておく。	◎	権限のない第三者や内部不正による不正な閲覧や操作が行われる。	6.3 組織的安全管理対策（体制、運用管理規程）	C.最低限のガイドライン	3.情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
		①-2	アクセス管理規定には以下の内容を含める。 ・アクセス権限、アカウント管理における登録申請、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 ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・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	◎				
	②持ち出した機器の外部のネットワークに接続する場合の対策の策定	②-1	持ち出した機器を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竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	◎	持ち出した機器を情報セキュリティ対策の不十分なネットワークに接続することで、不正プログラムへ感染する。	6.5 技術的安全対策	C.最低限のガイドライン	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。
	③情報の廃棄対応	③-1	CD-R 等の廃棄手順について定める。	◎	情報の廃棄が不十分なまま、再利用が行われることで、情報漏洩が生じる。	6.7 情報の破棄	C.最低限のガイドライン	1.「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
		③-2	ハードディスク等の廃棄手順について定める。	◎				
		③-3	破棄手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。	◎				
		③-4	ハードディスク等を医療情報システム等内の別の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。	◎		6.7 情報の破棄	C.最低限のガイドライン	2.情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。
		③-5	サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去する。	◎				
		③-6	ハードディスクを機器に接続する際には、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。	◎				
		③-7	ハードディスクの廃棄については、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、医療機関等の求めに応じ、速やかに提出できるよう整備する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		③-8	物理的な破壊措置については受託事業者自身で行うことが望ましいが、外部の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。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。 なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。	○				
		③-9	電子媒体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。	◎				
		③-10	運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、医療情報システム等提供上の要否の確認を定期的に行うこと。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等）。	◎		6.7 情報の破棄	C.最低限のガイドライン	4.運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成
		③-11	情報の破棄手順について、医療機関等と合意する。	◎				
	④情報や機器の組織外への持出に対する対策	④-1	受託する個人情報を運用や保守に用いる端末に原則保存しない旨、自社の運用管理規程等に定める。	◎	持ち出した機器に格納された情報が漏洩する又は、持ち帰った機器から不正なプログラムが感染拡大する。	6.8 情報システムの改造と保守	C.最低限のガイドライン	7.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で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を定めることを求め、医療機関等の責任者が逐一承認すること。
		④-2	医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又は受託事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。	◎				
		④-3	④-2で定める手順及び情報の提供条件について、医療機関等と合意する。	◎				
		④-4	持ち出した機器を再度設置するための適切な検証手順を策定する。	◎				
		④-5	保守点検で障害不良等が発見された際の対応作業等を行う際には受託事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出す。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-6	持ち出し手順に含まれる事項には次のようなものが考えられる。 ・ 装置の持ち出し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、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ・ 申請承認プロセス ・ 返却確認プロセス、等。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	4.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
		④-7	返却時の検証手順に含まれる事項には次のようなものが考えられる。 ・ 装置の動作確認 ・ 盗聴装置等、情報の安全性を脅かす装置の有無 ・ 悪意のあるプログラムの検出作業 ・ 収められている情報の検証作業（不正な改竄等）、等。	◎				
	⑤持ち出した機器や媒体の管理手順の策定	⑤-1	サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。	◎	持ち出しを行う機器や媒体について不適切な管理が行われることで、機器や媒体内の情報が漏洩する。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	1.組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
		⑤-2	⑤-1における「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。	◎				
		⑤-3	⑤-1で定める内容について、医療機関等と合意する。	◎				
		⑤-4	電子媒体について受託事業者施設外への不要な持ち出しを行わない。CD、DVD、MO 等の電子媒体については、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、電子媒体を確実に廃棄処分する。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	2.運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
		⑤-5	情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行う。これらの電子媒体に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。	◎				
		⑤-6	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行う。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		⑤-7	記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（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。） ・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機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、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	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	3.情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
		⑤-8	⑤-7の内容に関する教育を従業員等に対して行う。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	4.運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。
		⑤-9	⑤-7の内容を含む運用管理規程については、再委託先に対しても遵守等を求める。	◎				
	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-1	情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、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。	◎	機器・ソフトウェアの変更の影響により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		⑥-2	機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。	◎				
		⑥-3	機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。	◎				
		⑥-4	医療情報システム等に係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。	◎				
		⑥-5	変更手順に含まれる事項には次のようなものが考えられる。 ・ 変更についての影響が及ぶ関係者への通知プロセス ・ 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）申請承認プロセス変更試験プロセス ・ 変更作業に支障が発生した場合の復旧手順変更終了確認プロセス ・ 変更に伴う影響を監視するプロセス、等。	○		7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	2.　機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.2. 個人情報を含まないテストデータの利用	①個人情報を含むデータの利用に対する対策	①-1	医療情報を開発及び試験用データとして直接利用しない。利用する場合には、個人を識別できる情報等の削除及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用する。	◎	動作確認のために利用したテストデータに含まれた個人情報の漏洩が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-1	医療情報を操作する可能性のある受託事業者の職員全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める。派遣従業員については守秘義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求める。	◎	医療情報システム等提供に係る職員（派遣従業員含む）のうち悪意をもった者による情報漏洩が行われる。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	1.法令上の守秘義務のある者以外を事務職員等として採用するに当たって、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
		①-2	医療情報を操作する可能性のある受託事業者の職員（派遣従業員含む）については、守秘義務に関する内容を就業規則等に含める。	◎				
		①-3	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておく。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める。	◎		6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	3.従業者の退職後の個人情報保護規程を定めること。
		①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。	◎				
		①-5	上記に違反した受託事業者（派遣従業員含む）の職員に対して、適切な懲戒手続きを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行う。	◎		6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約	C.最低限のガイドライン	1.医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する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・作業結果の確認を行うこと。 ③ 清掃等の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 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託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。
		①-6	医療情報を操作する受託事業者の職員（派遣従業員含む）に対する教育･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の提供について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②医療機関等や再委託先との守秘義務を含めた契約の締結	②-1	医療情報システム等に係る情報及び受託した情報に関する守秘義務について、医療情報システム等提供に係る契約に含める。契約には、守秘義務に違反した受託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。	◎	医療情報システム等提供に係る事業者（再委託先も含む）による故意又は過失による情報漏洩が行われる。	6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約	C.最低限のガイドライン	2.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。
						6.8 情報システムの改造と保守	C.最低限のガイドライン	6.保守会社と守秘義務契約を締結し、これを遵守させること。
						6.8 情報システムの改造と保守	D.推奨されるガイドライン	3.作業員各人と保守会社との守秘義務契約を求めること。
						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	3(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。
		②-2	医療情報システム等の動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	1.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。
		②-3	医療情報システム等の動作確認に際し、受託した個人情報をやむを得ず使用する場合について、医療機関等と合意する。	◎				
1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-1	医療情報を操作する可能性のある受託事業者の職員の全てに個人情報保護及び情報セキュリティに関する教育を行い、一定水準の理解を得た職員だけを業務に従事させる。	◎	医療情報システム等提供に係る職員（派遣従業員含む）が定められた手順を理解しないことで、過失による事故が発生する。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	2.定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。
		①-2	派遣従業員に関しては、派遣元に対し、個人情報保護及び情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行う。	◎				
		①-3	この教育は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。	◎				
		①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）の退職時又は契約終了時以降の守秘義務について、教育･訓練に含める。	◎		6.6 人的安全対策　（1）従業者に対する人的安全管理措置	C.最低限のガイドライン	3.従業者の退職後の個人情報保護規程を定めること。
1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-1	受託事業者の職員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、改竄又は破壊等の行為が行われていないことを検証する。	◎	医療情報システム等提供に係る職員（派遣従業員含む）が業務上不必要な医療情報の閲覧や操作を行う。	6.6 人的安全対策　（1）従業者に対する人的安全管理措置	D.推奨されるガイドライン	1.サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。
		①-2	医療情報システム等の保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、医療機関等と合意する。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	5.保守会社がメンテナンスを実施する際には、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求めること。それらの書類は医療機関等の責任者が逐一承認すること。
		①-3	保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、医療機関等と合意する。	◎				
		①-4	医療情報システム等の保守業務を医療機関等の施設内で行う際の対応について、医療機関等と合意する。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	2.保守作業時には医療機関等の関係者立会いの下で行うこと。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②機器や媒体の定期的な所在確認	②-1	電子媒体は台帳を作成して管理する。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証する。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持する。	◎	機器や媒体の紛失・盗難発生時に、紛失・盗難を早期を発見できず、被害が拡大する。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	5.医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。
		②-2	情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。	◎				
		②-3	個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。	◎				
	③システム構成やソフトウェアの動作状況に関する内部監査の実施	③-1	システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。	◎	システム構成やソフトウェアの不備により、意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	4.　システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。
1.6. 物理的に情報を搬送する場合の対策	①組織外に持出する情報に対する暗号化等の対策	①-1	物理的に情報を搬送する際には以下の対策を実施する。 ・ 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。 ・ 配送時の作業者については、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。 ・ 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体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。 ・ 配送業者等による電子媒体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。 ・ 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さない。 ・ 電子媒体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電子媒体内のデータに暗号化を施す。	◎	搬送中の電子媒体内の情報が抜き取られることで、情報漏洩が生じる。	6.8 情報システムの改造と保守	C.最低限のガイドライン	7.保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で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を定めることを求め、医療機関等の責任者が逐一承認すること。
1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-1	受託した医療情報を保守･運用を行うために閲覧するのは必要最小限とする。	◎	患者等からの同意を得ないまま、医療情報の解析や第三者提供が行われる。	6.6 人的安全対策　（2）事務取扱委託業者の監督及び守秘義務契約 ----- 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 ----- C.最低限のガイドライン D.最低限のガイドライン	1.医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する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・作業結果の確認を行うこと。 ③ 清掃等の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 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託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。 ----- (C.最低限のガイドライン) 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 (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
		①-2	①-1の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。	◎				
		①-3	受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。	◎				
		①-4	①-1～①-3における閲覧に係る範囲、手順等について、医療機関等と合意する。また①-2、①-3により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。	◎				
		①-5	受託した医療情報の解析･分析は、医療情報システム等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。	◎				
		①-6	受託した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。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-7	受託した医療情報は、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。	◎				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。 (D.推奨されるガイドライン) (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。 (エ) 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、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。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。
		①-8	①-7の内容を、医療情報システム等提供に係る契約に含める。	◎				
		①-9	医療機関等の指示に基づき、受託した医療情報の第三者提供（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･取得できないように対応策を講じる。	◎				
		①-10	①-9により、第三者提供（閲覧）を行う場合には、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。	◎				
		①-11	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。	◎				
		①-12	①-7～①-11により第三者提供及びその報告を行うための条件、範囲等について、医療機関等と合意する。	◎				
1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-1	情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁･物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。	◎	情報の破棄が正しく行われず、電子媒体が再利用された場合に残留した情報の漏洩が生じる。	6.7 情報の破棄	C.最低限のガイドライン	3.外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 （2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
		①-2	物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については受託事業者自身で行うことが望ましい。外部の専門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十分な理解を得る。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。	○				
		①-3	①-1で講じる措置及び資料を提供するのに必要な条件等について、医療機関等と合意する。	◎				
		①-4	医療情報システム等提供の停止又は医療機関等における医療情報システム等利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体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。	◎				
		①-5	①-4に関して、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、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-1	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、合意を得る。また、当該再委託に係る契約において体制を明確にする。	◎	再委託先において対象事業者と同等の対策が講じられないことで、再委託先が原因となる事故が発生する。	6.8 情報システムの改造と保守	C.最低限のガイドライン	9.再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。
		①-2	再委託先には、自社と同等の個人情報保護指針等を遵守させる。	◎				
		①-3	再委託に係る契約に、委託業務に係る守秘義務を含める。	◎				
		①-4	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。	◎				
		①-5	医療情報システム等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、医療機関等と合意する。	◎				
		①-6	医療情報システム等の保守に関して、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。	◎				
		①-7	①-6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。	◎				
		①-8	再委託先により提供される医療情報システム等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。	◎				
		①-9	再委託先による医療情報システム等の実施、運用、維持について定期的に検証する。	◎				
		①-10	再委託先による医療情報システム等の実施、運用、維持について定期的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。	◎				
		①-11	再委託先による医療情報システム等を実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。	◎				
		①-12	医療情報システム等の実施中に再委託先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。	◎				
		①-13	再委託先による医療情報システム等の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、受託事業者の職員の入室、退室手順に準ずる。	◎				
		①-14	再委託先による医療情報システム等の変更時には、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。	◎				
		①-15	医療情報システム等の保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 5 版」6.8 章 C 項の管理策を実施する。	◎				
		①-16	外部事業者が医療情報システム等を実施する際は、受託事業者又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。	○				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-1	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。	◎	災害発生時における事業継続のための対策が過少又は費用対効果の観点で過剰となる。	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	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。
		①-2	業務プロセス間の相互関係を評価する。	◎				
		①-3	事業を継続するための業務プロセスの優先順位を明確にする。	◎				
		①-4	医療情報システム等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。	◎				
		①-5	医療情報システム等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。	◎				
	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-1	医療情報システム等の提供における業務プロセス及び医療情報システム等の優先順位にもとづいて、医療情報処理に関する事業継続計画を策定する。	◎	災害発生時に、医療情報システム等を最大許容停止時間内に復旧できない。	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	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。
		②-2	策定した事業継続計画について模擬試験を含めた適切な方法でレビューする。	◎				
		②-3	事業継続計画について定期的に見直しを行う。	◎				
		②-4	策定される事業継続計画には次のような事項を含むことが望ましい。 ・ 事前準備計画 ・ 「非常時」判断手順 ・ 関係者の召集、対応本部の設置 ・ 機器及び作業員の縮退措置及び代替施設の手配措置 ・バックアップ施設等、代替施設への切替え措置 ・ 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等） ・障害の拡大範囲に関する判断手順、基準 ・正常復帰の判断手順、基準 ・正常復帰後の医療情報システム等の点検手順（不正侵入、情報改竄、情報破損等の検出等） ・ 所管官庁への連絡体制、等	○				
		②-5	策定した事業継続計画に基づくサービス内容について、医療機関等と合意する。	◎				
	③医療情報システム等復旧後における整合性確保	③-1	非常時に行ったデータ処理の結果が、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。	◎	非常時の代替手段で処理した情報が医療情報システム等復旧後に正しく処理できない。	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	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。
	④非常時用の利用者アカウントや機能の管理手順の策定	④-1	非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、医療機関等と合意する。	◎	非常時用のアクセス制限が緩和された利用者アカウントや機能が通常時に悪用される。	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	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
		④-2	非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-3	非常時に用いる利用者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。	◎				・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。
		④-4	非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。	◎				
1.11. サイバー攻撃等による障害発生時の対応	①サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-1	サイバー攻撃等により、サービスの提供に支障が生じた場合において、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を行う。	◎	サイバー攻撃発生時に医療機関等に求められる関係者及び所管官庁への速やかな報告が実施できないことで、必要な措置が講じられない。	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	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）
		①-2	サイバー攻撃等により、サービスの提供に支障が生じた場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、医療機関と合意する。	◎				
		①-3	医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、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・ストレージ等は国内法の執行が及ぶ場所に設置する。	◎				
	②サイバー攻撃等による原因調査のためのログ等の記録の保全	②-1	サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。	◎	サイバー攻撃発生後にログ等を用いた被害範囲や原因調査が困難となる。			
1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-1	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竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	◎	他の事業者及び医療機関等との間で責任範囲の認識の相違が生じることで、本来必要な対策が通信回線のいずれの箇所でも講じられない。	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	C.最低限のガイドライン	1.ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。 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してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。
		①-2	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竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	◎				
		①-3	ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関する受託事業者の役割分担について、医療機関等と合意する。	◎		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	C.最低限のガイドライン	6.医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通又は著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・患者等に対する説明責任の明確化 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置
		①-4	回線の管理、品質等に対する受託事業者の責任の範囲、役割等について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	通常運用時及び非常時の医療機関等と受託事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、受託事業者の負う責任の範囲、役割等について、医療機関等と合意する。	◎				・交換した医療情報等に対する管理責任及び事後責任の明確化（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）
		①-6	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	◎		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	C.最低限のガイドライン	8.回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。 また、上記 1 及び 4 を満たしていることを確認すること。
		①-7	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	◎				
		①-8	サービスにより管理する医療情報を患者等の閲覧に供する場合に、受託事業者において対応すべきセキュリティ上の措置の条件、内容等について、医療機関等と合意する。	◎		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	C.最低限のガイドライン	9.患者に情報を閲覧させる場合、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、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た対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外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すること。
		①-9	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	◎				
		①-10	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	◎				
1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-1	医療情報システム等における機器及びソフトウェアの構成図を作成する。	◎	医療情報システム等の構成や仕様の問題に起因する意図しない情報の虚偽入力、書き換えや消去、混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	1.　システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。
		①-2	医療情報システム等のネットワーク構成図を作成する。	◎				
		①-3	①-1、①-2で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。	◎				
		①-4	医療情報システム等を構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。	◎				
		①-5	①-1～①-4で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と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②機器・ソフトウェアの導入や変更における事前検証の実施	②-1	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う。	◎	機器・ソフトウェアのバージョン不整合やバグの混入等に起因する意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		②-2	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、影響を最小限に抑える方策を講じる。	◎				
		②-3	情報処理に供するアプリケーションについては、受託事業者自身で開発したアプリケーションを用いる。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いる。	◎				
		②-4	ソフトウェアに不正プログラムが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。	○				
		②-5	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入する。	◎				
	③本番環境と開発環境の分離	③-1	ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。	◎	本番環境と開発環境が分離されておらず、本番環境に不正プログラムが混入されたり、不適切なデータ・プログラムが置かれてしまう。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		③-2	開発施設では不正プログラムが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には不正プログラムへの対策を行う。	◎				
		③-3	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしない。	◎				
		③-4	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かない。	◎				
		③-5	情報処理に不必要なファイル等を運用システム上におかない。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-1	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。	◎	機器やソフトウェアの不具合発生時に、機器の交換やソフトウェアのパッチ適応等の是正が行われない。	7.2 見読性の確保について	C.最低限のガイドライン	（2）見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。
		①-2	受託する医療情報を格納する機器･媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、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。	◎				
		①-3	それぞれの装置は製造元又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。	◎				
		①-4	情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	（2）ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。
		①-5	医療情報システム等について、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、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。	◎				
		①-6	医療情報システム等について、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合や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。	◎				
		①-7	①-6においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、医療機関等と合意する。	◎				
	②保守作業に伴う医療情報システム等停止時間の最小化	②-1	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施する。	◎	保守作業に伴う情報システム・サービ停止が長引くことにより、医療サービス提供に支障が生じる。	該当なし	ー	ー
		②-2	保守業務における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。	◎				
		②-3	保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。	◎				
		②-4	②-3に定めた手順を医療機関等に示し、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、医療機関等と合意する。	◎				
		②-5	②-3で示された手順について、医療機関等が対応すべき事項がある場合、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③医療情報システム等の停止や仕様変更時の対応	③-1	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、医療情報システム等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。	◎	突然の医療情報システム等の停止や仕様変更により、医療機関等において十分な準備が行えず大きな影響を及ぼす。	該当なし	―	―
		③-2	③-1の場合、受託した医療情報を、医療機関等に返却する。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）、返却方法、条件については、医療機関等と合意する。また医療機関等のサービス利用開始後に、医療機関等と合意した内容を変更する場合には、③-1に準じた対応策を講じる。	◎				
		③-3	③-2におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、受託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）によるデータが含まれる場合があるので、その旨も合わせて、医療機関等と合意する。	◎				
		③-4	③-1においてサービスの変更を含む医療情報システム等の一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、③-2の対応は除く）、条件等について、医療機関等と合意する。	◎				
		③-5	医療機関等の都合により医療機関等の医療情報システム等利用が終了する場合も、③-2、③-3に示す対応策を講じる。	◎				
		③-6	③-1～③-5についての手順等を、運用管理規程等に含める。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.物理的対策								
2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-1	機器や媒体の設置場所等の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ようにする。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。	◎	許可された者以外が機器や媒体に直接アクセスする。	6.3 組織的安全管理対策（体制、運用管理規程）	C.最低限のガイドライン	2.個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
		①-2	機器や媒体の設置場所については、許可された者のみが入退できるように制限する。	◎		6.4 物理的安全対策	C.最低限のガイドライン	2.個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることができない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。
		①-3	医療情報システム等を設置、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。	◎		6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		①-4	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。	◎				
		①-5	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。	◎				
		①-6	受託事業者の職員の業務に応じて執務室内に滞在できる時間を指定する。	◎				
		①-7	機械式の認証装置で利用する認証要素としては、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）等を組み合わせることが望ましい。	○				
		①-8	機器や媒体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。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理を行う。	◎	サーバラックやキャビネット内の機器や媒体の紛失・盗難が生じる。	6.4 物理的安全対策	C.最低限のガイドライン	1.個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
		①-2	機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。	◎				
		①-3	サーバ等を格納するラック等について、施錠管理を行う。	◎				
		①-4	媒体等を格納するキャビネット等について、施錠管理を行う。	◎				
		①-5	電子媒体を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する。	◎				
		①-6	データセンターを運営する外部事業者が、自社専有の建物と同等な安全管理策を実施する等、受託事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認する。	◎				
		①-7	医療情報システム等の設置されるサーバラックには施錠を行い、定められた受託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。	◎				
		①-8	受託事業者が医療情報システム等の設置されるサーバ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。	◎				
		①-9	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム等、医療情報に影響を与えないことを確認する。	◎				
		①-10	医療情報システム等であることが、同じデータセンター内に立ち入る他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。	◎				
		①-11	医療情報システム等の設置されるサーバ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）等を組み合わせることが望ましい。	○				
		①-12	受託事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認する。	◎				
		①-13	機器や媒体の保存場所（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ようにする。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-14	①-1~①-13につき、運用管理規程等に規定する。	◎				
2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処理する施設内への侵入監視	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 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。 ・ 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入する。	◎	部外者の侵入への抑止や侵入による被害範囲の特定が困難となる。	6.4 物理的安全対策	D.推奨されるガイドライン	1.防犯カメラ、自動侵入監視装置等を設置すること。
		①-2	防犯カメラ等の監視映像は記録し、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。	◎				
		①-3	機器、媒体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、その記録を保存し、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。	◎				
		①-4	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監視を行う。	◎				
	②受託事業者の職員に対する職員証等の着用の義務付け	②-1	受託事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した受託事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、受託事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。	◎	対象事業者の職員と部外者の見分けが付かず、侵入が容易となる。	6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		②-2	受託事業者の職員は、受託事業者の専有する領域にて、受託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。	◎				
		②-3	職員証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、受託事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行う。	◎				
2.4. バックアップ施設における対策	①バックアップ施設に対する物理的安全対策の実施	①-1	医療機関等に提供する医療情報システム等の継続に必要であれば、受託する医療情報のバックアップ施設等、医療情報システム等を継続するための代替情報処理施設を設置し、それらの施設に対しても物理的安全対策を施す。	◎	物理的安全対策が手薄となったバックアップ施設へ侵入される。	6.4 物理的安全対策	C.最低限のガイドライン	1.個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2.5. 個人所有物の持ち込み制限	①医療情報を処理する施設内への個人所有物の持ち込み制限	①-1	医療情報処理施設内への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。	◎	医療情報の窃取・破壊・改竄を目的とした機器や媒体、機具等の持ち込みが生じる。	6.4 物理的安全対策	C.最低限のガイドライン	3.個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
		①-2	機器や媒体の設置場所には、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。	◎				
2.6. 機器の盗難への対策	①重要な機器への盗難防止用チェーン等の取付	①-1	個人情報が存在するPC 等の重要な機器には、盗難防止用チェーン等を取り付ける。	◎	個人情報が存在するPC等の重要な機器が盗難される。	6.4 物理的安全対策	C.最低限のガイドライン	4.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等を設置すること。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
2.7. 覗き見への対策	①覗き見防止対策	①-1	医療情報等が表示される端末画面等がアクセス権限の無いものが視野に入らないような対応（室内の機器レイアウト等）を行う。	◎	アクセス権限の無い者に医療情報等が表示される端末画面を覗き見される。	6.4 物理的安全対策	C.最低限のガイドライン	5.覗き見防止の対策を実施すること。
		①-2	個人情報の表示中の覗き見を予防するために、端末に覗き見対策のシートを貼る等の対策を行う。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	1.外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-1	機器や媒体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、及び、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。	◎	地震、水害、落雷、火災等、及び、それに伴う停電等により、医療情報システム等が停止もしくは不具合が生じる。	該当なし	ー	ー
		①-2	①-1の施設を設置する建築物について、医療機関等と合意する。	◎				
		①-3	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。	◎				
		①-4	医療情報システム等を配置する室内での喫煙、飲食を禁止する。	◎				
		①-5	医療情報システム等を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮する。	◎				
		①-6	医療情報システム等を設置するサーバラックについては以下の安全管理策を実施する。 ・ 震災時に転倒することが無いよう確実に設置する。 ・ 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されている。 ・ 扉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する。	◎				
3.技術的対策								
3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-1	医療情報システム等にて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う。	◎	正当な利用者以外により、医療情報システム等上の情報が閲覧・操作される。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		①-2	医療情報システム等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（複数の利用者によるIDの共同利用は行わない。ただし当該医療情報システム等が他の医療情報システム等を利用するためのID（non interactive ID）は除く）。	◎				
		①-3	利用者のなりすまし等を防止するための認証を行う。	◎				
		①-4	医療情報システム等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。	◎				
	②一時的な認証手段の用意	②-1	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･手順を事前に定める。	◎	利用者の認証に用いる物理的な媒体・身体情報等が欠損した場合、情報システムが利用できない。	6.5 技術的安全対策	C.最低限のガイドライン	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。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-2	代替的手段･手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。	◎				
		②-3	代替的手段･手順により、医療情報システム等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。	◎				
		②-4	その他、一時的な利用者の認証方法について医療機関等と合意する。	◎				
	③長時間離席時の対策	③-1	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。	◎	端末から離席している間、正当な利用者以外により、当該端末上での不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		③-2	サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。	◎				
		③-3	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、医療機関等と合意する。	◎				
		③-4	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、あるいは強制ログオフを行う。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	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）。
		③-5	離席の場合のクローズ処理の具体的な適用について、医療機関等と合意する。	◎				
	④安全なパスワード要件の定義	④-1	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、すべてのパスワードが品質基準を満たしていることを確実とする。	◎	パスワードが窃取もしくは推測されることで、認証の突破及び不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		④-2	パスワードポリシーについて、医療機関等と合意する。	◎				
		④-3	パスワードには有効期限の設定を行い、定期的な変更を強制する。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、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ようにする。	◎				
		④-4	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。	◎				
		④-5	パスワード発行時には、乱数から生成した仮の医療情報システム等へのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施する。	◎				
		④-6	パスワードを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利用者に徹底する。	◎				
		④-7	利用者がパスワードを登録及び変更する際には、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、利用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行う。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		④-8	本人の識別・認証に用いる情報は、本人しか知り得ない状態に保つよう対策を行う。	◎				
		④-9	利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと医療情報システム等にアクセスできないようにする。	◎				
		④-10	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。	◎				
		④-11	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文字以上等、十分に安全な長さの文字列等から構成されるルールとする。	◎				
		④-12	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。	◎				
		④-13	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し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とする。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	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。
		④-14	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。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とする。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を導入する。	◎				
	⑤多要素認証方式の採用	⑤-1	ログオン時に利用する認証要素としては、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）又はパスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせた多要素認証とすることが望ましい。	○	単一の要素による認証情報が窃取もしくは推測されることで、正当な利用者以外による認証の突破及び不正な閲覧・操作が行われる。	6.5 技術的安全対策	D.推奨されるガイドライン	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。
		⑤-2	医療情報システム等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情報システム利用に係る認証は、多要素認証とする。	◎				
		⑤-3	利用者の認証で採用する認証方式について、医療機関等と合意する。	◎				
		⑤-4	利用者の認証において、ID･パスワードによる認証方式を採用している場合には、ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。	◎				
3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-1	医療情報システム等の操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、閲覧、編集、削除等を防止する。	◎	一般利用者の権限が高いため、任意のソフトウェアのインストール、持込機器接続、持込Wi-Fiの接続等をされ、不正アクセスを誘発する。	6.5 技術的安全対策 ----- 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 ----- C.最低限のガイドライン D.推奨されるガイドライン	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

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-2	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合意する。	◎				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。 ----- (C.最低限のガイドライン) 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 (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。 (D.推奨されるガイドライン) (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。 (エ) 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、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。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。
		①-3	医療情報システム等の構成要素（情報処理装置、ソフトウェア）それぞれのアクセス管理に係るセキュリティ要求事項を整理する。	◎				
		①-4	それぞれの情報にアクセスする権限を持つ利用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。	◎				
		①-5	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定する。	◎				
		①-6	定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。	○				
		①-7	予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。	◎				
		①-8	システム管理者、運用担当者、保守担当者等が、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。	◎				
	②医療情報に対するアクセス制御	②-1	医療情報とそれ以外の情報を区分できる措置を講じる。	◎	情報の区分に依らない一律のアクセス管理が行われることで、医療情報等のより重要な情報に対しても、重要性の低い情報と同じレベルで不正な閲覧・操作が行われる。	6.5 技術的安全対策	D.推奨されるガイドライン	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。
		②-2	医療情報については、情報区分に従ってアクセス制御を行えるようにする。	◎				
		②-3	仮想化技術を用いた資源を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。	◎				
		②-4	医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、医療機関等と合意する。	◎				
3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-1	利用者は医療情報システム等上においてユニークな利用者ごとのID により識別する。	◎	情報システムで保存される履歴から、不正な閲覧・操作を行った利用者が特定できない。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		①-2	利用者のID を発行する際に、既存の ID との重複を排除する仕組みを導入する。	◎				
		①-3	複数利用者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、利用者ごとのID でログオンしてからグループ ID に変更する仕組みを利用する。	◎				
		①-4	利用者のID の発行は医療情報システム等の管理に必要な最小限の人数に留める。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	監視ログの監査時に利用者を確実に特定するため、利用者の ID は過去に使われたものを再利用しない。	◎				
		①-6	アクセスを許可された利用者 のID によるアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。	○				
		①-7	不正なアカウントの利用又は試みが行われたことを利用者自身で検出するため、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が望ましい。	○				
		①-8	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が望ましい。	○				
		①-9	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」と表示すると当該 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が望ましい。	○				
		①-10	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が望ましい。	○				
		①-11	医療情報システム等に許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知する。	◎				
		①-12	利用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。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	4.保守要員の離職や担当替え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付け、また、それに応じるアカウント管理体制を整えておくこと。
		①-13	不要な利用者の ID が残っていないことを定期的に確認する。	◎				
	②特権IDの最小限の利用及び作業実施内容の記録	②-1	特権 ID の発行は必要な最小限のものに留める。	◎	特権IDが不正利用又は乗っ取られることにより、広範囲での不正な閲覧・操作が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		②-2	特権使用者に昇格可能な利用者の ID を制限する。	◎				
		②-3	特権の使用時には作業実施内容を記録する。	◎				
		②-4	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。	◎				
		②-5	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が望ましい。	○				
		②-6	医療情報システム等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竄、削除など不正な行為を防止することが望ましい。	○				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③パスワードの管理・運用	③-1	各利用者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護する。	◎	パスワードやパスワードファイルが漏洩した場合に、不正利用される。	6.5 技術的安全対策	C.最低限のガイドライン	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。
						6.8 情報システムの改造と保守	C.最低限のガイドライン	3.その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適切に管理することを求めること。
		③-2	医療情報システム等及びソフトウェアを使用する前に、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の棚卸を行い、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。	◎		6.5 技術的安全対策	C.最低限のガイドライン	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。
		③-3	パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管する。	◎				
		③-4	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用する。また、一般の作業者による閲覧を制限する。	◎				
		③-5	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。	◎				
		③-6	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。	◎				
3.4. ログの取得と検証	①ログの取得と検証	①-1	利用者の活動、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ログを作成し、一定期間保存する。	◎	ログが取得・保存されておらず、ログの監視・分析による不正な行為などの検出や、情報事故発生後のログの解析による検証ができない。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		①-2	ログを定期的に検証して不正な行為、システムの異常等を検出する。	◎				
		①-3	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。 ・ 利用者情報（利用者の 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） ・ ファイル及びデータへのアクセス、変更、削除記録（利用者の 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） ・ データベース操作記録（利用者の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）修正パッチの適用作業（利用者の ID、変更されたファイル） ・ 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） ・ システム起動、停止イベント ・ ログ取得機能の開始、終了イベント外部デバイスの取り外し ・ IDS・IPS 等のセキュリティ装置のイベントログ ・ 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）	○				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-4	ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理する。	◎				
		①-5	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。	◎				
		①-6	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）の複製及び利用については監査証跡とするためにログを取得する。	◎				
		①-7	医療情報システム等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よるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。	◎				
		①-8	①-7に関する情報の医療機関等への提供について、医療機関等と合意する。	◎				
		①-9	ログの取得機能を有しない場合には、医療機関等と合意する。	◎				
		①-10	医療情報システム等の保守に従事する者及び管理者権限を有する者が、その業務の目的で当該医療情報システム等にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。	◎		6.8 情報システムの改造と保守	C.最低限のガイドライン	2.メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、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こと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
		①-11	①-10で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。	◎				
		①-12	医療情報システム等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。	◎		6.8 情報システムの改造と保守	D.推奨されるガイドライン	1.詳細なオペレーション記録を保守操作ログとして記録すること。
		①-13	取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。	◎				
		①-14	ログを検証するため、利用者がアクセスした医療情報等を迅速に確認できるよう、利用者の ID と、情報の識別子（資産台帳記載の番号等）、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が行うことができるようなシステムを整備することが望ましい。	○		6.8 情報システムの改造と保守	D.推奨されるガイドライン	5.保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。
	②ログの改竄や削除を防止するためのアクセス制限や外部保存	②-1	ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用する。 ・ ログデータにアクセスする利用者及び操作を制限する。 ・ 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとる。 ・ ログデータに対する不正な改竄及び削除行為に対する検出・防止策を施す。	◎	内部不正やサイバー攻撃による不正アクセスなどでログが改竄、消去される。	6.5 技術的安全対策	C.最低限のガイドライン	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。
	③時刻の標準時刻への同期	③-1	ログを利用して正確に事故原因等を検証するため、医療情報システム等のすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておく。	◎	機器が時刻同期しておらず、診療記録等に不整合が生じたり、製品やサービス間のログ突合が困難となることで不正な閲覧・操作が行われた範囲の特定ができな	6.5 技術的安全対策	C.最低限のガイドライン	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。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		③-2	医療情報システム等のすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。	○	い。			
		③-3	ログの時刻の信頼性を確保するために、医療情報システム等の時刻と、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又はそれよりも多い頻度で行う。	◎				
	④リモートメンテナンスにおける不正な侵入防止とログの取得・検証	④-1	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、医療情報システム等への不正な侵入が生じないよう安全管理措置を講じる。	◎	リモートメンテナンスに用いるIDやパスワード等の認証情報の不適切な管理により医療情報システム等への不正な侵入が生じ、ログから被害が特定できない。	6.8 情報システムの改造と保守	C.最低限のガイドライン	8.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。
		④-2	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。	◎				
		④-3	サービス提供に必要な医療情報システム等の保守をリモートメンテナンスで行う場合、医療機関等と合意する。	◎				
	⑤取り扱う医療情報の法定保存年限に基づくログの保存期間の設定	⑤-1	取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するログ又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。	◎	法定保存期間中の医療情報への不正な閲覧・操作があった場合の影響範囲が特定できない。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		⑤-2	法定保存年限が経過した医療情報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、医療機関等と合意する。なお、本項におけるログの管理方法について保存期間を設けた場合には、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。	◎				
3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-1	最新の脅威についての情報収集に努め、導入している不正プログラム対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認する。対応すべき脅威の例としては、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）等がある。	◎	不正プログラムの実行により、端末・サーバ内の情報の漏洩・改竄・破壊のほか、資源の不正使用が行われる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		①-2	不正プログラム対策ソフトウェアにおいて次の設定を行う。 ・ 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）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 ・ 電子媒体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 ・ 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 ・ 管理者以外による設定変更やアンインストールの禁止	◎				
		①-3	一定期間、不正プログラム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又は隔離措置をとる。	◎				
		①-4	医療情報システム等の構築に際しては、不正プログラム等の混入が生じないようにするための手順を策定し、これに則って構築する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	不正プログラム対策ソフトウェアのパターン定義ファイルを常に最新のものに更新する。	◎				
		①-6	医療情報システム等の構築に際して、外部からプログラムを媒体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、必ず事前に最新の不正プログラム対策ソフトウェア等の導入を行う。また情報システム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。	◎				
		①-7	医療情報システム等利用環境がウイルス等による攻撃を受けた場合に、医療情報システム等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。	◎				
3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-1	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにする。	◎	端末やサーバで利用していない機能やアプリケーションが悪用されることにより、不正プログラムが実行される。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		①-2	ウェブブラウザの接続するサーバを業務上必要なサーバに限定する。	◎				
		①-3	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 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とする（管理ソフトウェアが実行されるサーバのみを認可する）。	◎				
		①-4	認可したサイトからダウンロードされるコードについても不正プログラム対策ソフトウェアにより検査する。	◎				
		①-5	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が望ましい。	○				
		①-6	医療情報システム等のサーバ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。	◎				
		①-7	医療情報システム等に用いる装置には、必要のないアプリケーション等をインストールしない。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	9.持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。
		①-8	医療情報システム等に関する情報を格納する機器を持ち出す場合には、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。	◎				
		①-9	医療情報システム等に関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。	◎				
3.7. 機器・ソフトウェアの脆弱性への対応	①安全性が確認できるネットワーク機器の利用	①-1	ルータ等のネットワーク機器は、安全性が確認できる機器を利用する。	◎	VPNルータ等のネットワーク機器の脆弱性から医療情報システム等へ不正アクセスが発生し、医療情報システム等の停止や情報の窃取・漏洩が生じる。	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	C.最低限のガイドライン	4.ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット若しくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。
		①-2	ルータ等のネットワーク機器は、ISO/IEC 15408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、本ガイドラインに適合しているものを選定する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②パッチ適用等の実施	②-1	医療情報システム等に関連する技術的脆弱性については台帳等を利用して管理する。	◎	脆弱性への対応漏れや脆弱性是正のための設定変更等により医療情報システム等に不具合が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		②-2	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（パッチ適用、設定変更等）を決定する。	◎				
		②-3	修正パッチの適用前にパッチが改竄されていないこと及び有効性を検証する。	◎				
		②-4	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、医療情報システム等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。	◎				
	③医療情報システム等への脆弱性診断の実施	③-1	提供するアプリケーションについては、アプリケーションの種別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。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。	◎	医療情報システム等に設定不備や古いバージョン利用等の脆弱性が混入し、攻撃に悪用される。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		③-2	アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。	○				
		③-3	開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。 パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的な脆弱性検査を行う。	○				
	④最新の脆弱性に関する情報の収集	④-1	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとる。	◎	新しく発見された脆弱性を狙って急増する攻撃への対処が遅れ、被害を受ける。	6.5 技術的安全対策	C.最低限のガイドライン	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。
		④-2	医療情報システム等の脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、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し、確認する。	◎				
	⑤IoT機器に関する情報収集及び脆弱性への対応	⑤-1	IoT機器の利用を含むサービスを提供する場合、医療機関等との役割分担について、医療機関等と合意する。	◎	IoT機器について製造販売業者が想定していない利用方法により、脆弱性が生じる。	6.5 技術的安全対策	C.最低限のガイドライン	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、対策を講じること。
		⑤-2	IoT機器の利用を含むサービスを提供する場合、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。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
3.8. ネットワーク上のアクセス制御	①ネットワークのアクセス制御	①-1	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。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行う。	◎	業務上通信する必要のないIPアドレスやTCP/UDPポートにより、ネットワークを経由した攻撃を受ける。	6.5 技術的安全対策	D.推奨されるガイドライン	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。
		①-2	セキュリティゲートウェイでは、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（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）。	◎				
		①-3	医療情報システム等において、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定する。他に必要な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。 ・ 外部からの医療情報システム等の稼動監視・遠隔保守 ・ 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 ・ 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ファイル等のダウンロード ・ 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 ・ 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 ・ 時刻同期のための時刻配信サーバへのアクセス ・ これらの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へのアクセス等） ・ その他の医療情報システム等の稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）	◎				
	②なりすましの防止	②-1	次の情報交換方法について予め合意しておく。 ・ 情報を電子媒体に記録して交換する際の手順 ・ 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 ・ 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 ・ 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	◎	不正なアクセス元もしくはアクセス先における通信の盗聴・なりすましが行われる。	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	C.最低限のガイドライン	2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。
		②-2	情報交換手順では搬送の形態によらず次の事項を確実にする。 ・ 発送者、受領者を識別し記録する。 ・ 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。 ・ 交換する情報の機密レベルに関して合意する（受領側で機密レベルが低くならないようにする）。 ・ 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。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-3	電子的に情報を転送する際には以下の対策を実施する。 ・ 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。 ・ 送受信する経路は適切な方法で傍受のリスクから保護されている。 ・ 受信した情報について経路途中での損傷、改竄が無いことを検証する対策を講じる。 ・ 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施する。	◎				
		②-4	医療機関等から受託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。	◎				
		②-5	②-4において、医療機関等が外部接続するサーバ等と受託事業者のサーバとの間の相互認証を行う。	◎				
		②-6	②-4について、受託事業者が保守業務を再委託している場合には、受託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を講じる。	◎				
		②-7	厚生労働省ガイドライン第5版6.11 C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、医療機関等と合意する。	◎				
	③ネットワークポートへの不正な装置の接続制限	③-1	ネットワーク機器及びサーバ、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。	◎	未許可の端末が施設内のネットワークに物理的に接続され、通信の盗聴・なりすましが行われる。	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	C.最低限のガイドライン	3.施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
		③-2	不正な装置を識別するため、医療情報システム等内で利用する情報処理装置を登録したリストを作成・維持する。	◎				
		③-3	不正な情報処理装置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、脆弱性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運用する。	◎				
	④無線LAN利用時の対策	④-1	医療情報を取り扱う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セキュリティ対策について、医療情報システム等事業者の役割分担等について、医療機関等と合意する。	◎	無線LAN利用時に適切な暗号化やアクセス元の端末の制限が行われず、通信の盗聴・なりすましが行われる。	6.5 技術的安全対策	C.最低限のガイドライン	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。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
						6.5 技術的安全対策	D.推奨されるガイドライン	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。
		④-2	業務上、医療情報システム等に関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。	◎		6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	8.持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「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」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。
3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-1	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の検出、あるいは不正なトラフィックの遮断を行う。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。	◎	不正プログラムや不正アクセス等の被害がネットワーク内で拡大する。	6.5 技術的安全対策	D.推奨されるガイドライン	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。
		①-2	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。	◎				
		①-3	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とする。	◎				
		①-4	侵入検知の記録には不正アクセス等の事後処理に必要な項目が含める。	◎				
		①-5	医療情報システム等から、不正・不審なトラフィックが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が望ましい。	○				
		①-6	侵入検知システム自身が攻撃・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が望ましい。	○				
		①-7	IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システム等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。	◎		6.5 技術的安全対策	D.推奨されるガイドライン	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。
3.10. 外部へ持ち出す機器や情報の管理	①持ち出しを行う機器の認証	①-1	機器等については、起動パスワードの設定を行う。	◎	紛失・盗難した機器が起動され、機器を不正に利用される。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	6.情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
		①-2	起動パスワードは、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。	◎				
		①-3	医療情報システム等に関する情報を格納する情報機器への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。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	2.情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	②搬送する情報に対する対策	②-1	情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体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。	◎	紛失・盗難した機器や媒体内に保存された情報の漏洩や改竄が生じる。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	7.盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
3.11. 仮想デスクトップやMDM・MAMによる情報漏洩への対策	①個人所有の機器の管理	①-1	利用者が個人所有する機器による医療情報システム等利用に関する対応策について、医療機関等と合意する。 なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏洩等を防止する観点から、例えば、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、業務利用領域を医療機関等が管理できるようにするほか、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）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。	◎	セキュリティレベルの低い個人所有のモバイル端末（ノートパソコン、スマートフォン、タブレット）に格納した情報の窃取・漏洩が生じる。	6.9 情報及び情報機器の持ち出しについて	C.最低限のガイドライン	10.個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。
		①-2	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原則禁止とする。	◎		6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	4.スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・ BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・ 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。
	②端末側に情報を残さない技術の導入	②-1	医療機関等の利用者が、医療機関等の外部から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受託事業者の役割分担等につき、医療機関等と合意する。	◎	外部から医療情報システム等を利用した際、端末内に保存された情報の窃取・漏洩が生じる。	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	D.推奨されるガイドライン	1.やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。
3.12. 未登録の電子媒体の接続制限	①サーバ等への未登録の電子媒体の接続制限	①-1	医療情報システム等においてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除する。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。	○	利用を許可していない電子媒体へ機器内の情報が不正に複製される。	6.9 情報及び情報機器の持ち出しについて	D.推奨されるガイドライン	3.情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。
		①-2	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が望ましい。	○				
3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-1	ネットワークにおいて、情報の盗聴、改竄、誤った経路での通信、破壊等から保護するために必要な措置（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。	◎	ネットワーク経路上の通信において、安全性の低い暗号化・電子署名について解読もしくは偽装される。	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	C.最低限のガイドライン	1.ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。 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してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。
		①-2	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）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。	◎				
		①-3	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について、医療機関等と合意する。	◎				
		①-4	情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。	○				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	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。選択基準としては電子政府推奨暗号リスト 等を用いる。	◎		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	C.最低限のガイドライン	5.送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
		①-6	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セキュリティ対策を実施する。	◎				
		①-7	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。	◎				
		①-8	①-7のほか、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への対応を求める場合には、その対応に必要な措置及び条件等について、医療機関等と合意する。	◎				
		①-9	VPN 接続を行う場合には以下の事項に従う。 ・ 接続時に VPN 装置間で相互に認証を行う。 ・ 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。 ・ 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。 ・ 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。	◎		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	10.オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 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）等による攻撃からの防護について、適切な対策を実施すること。
		①-10	オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/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。	◎				
		①-11	SSL-VPNは、原則として使用しない。	◎				
		①-12	サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 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。	◎				
		①-13	医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 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、医療機関等と合意する。	◎				
②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理		②-1	暗号鍵が漏洩した場合に備えた対応策を策定しておく。	◎	暗号アルゴリズムの危殆化や暗号鍵の漏洩時に、暗号化・電子署名について解読もしくは偽装される。	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	C.最低限のガイドライン	5.送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
		②-2	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。	◎				
		②-3	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。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		②-4	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。	◎				
		②-5	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が望ましい。	○				
		②-6	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が望ましい。	○				
		②-7	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が望ましい。	○				
		②-8	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ようにすることが望ましい。	○				
3.14. リモートメンテナンスのアクセス管理	①リモートメンテナンスの不必要なログインを防止するためのアクセス管理	①-1	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。	◎	リモートメンテナンスにより不正な閲覧・操作が行われた場合に気が付くことができない。	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	C.最低限のガイドライン	7.リモートメンテナンスを実施する場合は、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を行って不必要なログインを防止すること。 また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。
3.15. 電子署名を利用する場合の管理	①信頼できる第三者機関が発行した電子証明書の利用	①-1	医療情報システム等において電子署名を利用する場合、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等の信頼できる第三者機関が発行した電子証明書を利用する。	◎	信頼できる第三者機関と同等の厳格さで本人確認や署名の検証が行われない。	6.12 法令で定められた記名・押印を電子署名で行うことについて	C.最低限のガイドライン	（1）厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと 1.　保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野 PKI 認証局の発行する電子署名を活用することが推奨される。 ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。 2.　電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても A の要件を満たすことは可能であるが、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必要がある。 3.　「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成 14 年法律第 153 号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者が全て公的個人認証サービスを用いた電子署名を検証できることが必要である。
	②電子署名を施す場合のタイムスタンプの付与	②-1	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。この場合には、タイムスタンプの内容・検証方法について、医療機関等と合意する。	◎	電子署名を行う機器等の時刻情報が改竄されることで、電子署名付与時点の時刻及び当該時刻以降の改竄の有無が証明できない。	6.12 法令で定められた記名・押印を電子署名で行うことについて	C.最低限のガイドライン	（2）電子署名を含む文書全体にタイムスタンプを付与すること 1.　タイムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。 2.　法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。 3.　タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。
		②-2	タイムスタンプを付与した情報を取り扱う場合に、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、対応方法等について、医療機関等と合意する。	◎				
		②-3	タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
	③タイムスタンプを付与する時点で有効な電子証明書の使用	③-1	タイムスタンプを付与した情報を取り扱う場合に、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等について、医療機関等と合意する。	◎	タイムスタンプ付与時点で電子署名を検証することができない。	6.12 法令で定められた記名・押印を電子署名で行うことについて	C.最低限のガイドライン	（3）上記タイムスタンプを付与する時点で有効な電子証明書を用いること 1.　当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。
3.16. 改竄防止・検知策の実装	①ソフトウェアの改竄防止・検知策の実装	①-1	不正な改竄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（改竄検知）を実施する。	◎	ソフトウェアの改竄により、意図しない情報の虚偽入力、書き換え、消去及び混同が生じる。	7.1 真正性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （5）機器・ソフトウェアの品質管理	3.　機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。
		①-2	不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改竄防止、検知策を実施する。	◎				
3.17. 患者ごとの情報の管理	①患者ごとに情報を管理する機能の実装	①-1	医療情報システム等には、受託する医療情報を患者等ごとに管理できる機能を含める。	◎	各種媒体に分散管理された患者の情報の相互関係がすぐに明らかにできない。	7.2 見読性の確保について	C.最低限のガイドライン	（1）情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの情報の全ての所在が日常的に管理されていること。
3.18. 利用目的に応じた応答時間の確保	①医療情報システム等の利用目的に応じた応答時間の確保	①-1	医療機関等が医療情報システム等を利用する際の、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、医療機関等と合意する。	◎	情報の表示や検索等の応答時間が長いことで医療情報システム等の利用目的に支障が生じる。	7.2 見読性の確保について	C.最低限のガイドライン	（3）見読目的に応じた応答時間 目的に応じて速やかに検索表示若しくは書面に表示できること。
3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-1	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施する。	◎	医療情報システム等の単一障害点の障害により、情報システム・サービスが停止する。	7.2 見読性の確保について	C.最低限のガイドライン	（4）システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。
		①-2	医療情報システム等、ネットワーク等に関し、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冗長化対策を講じる。	◎				
		①-3	①-2を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、医療機関等と合意する。	◎				
		①-4	障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、医療機関等と合意する。	◎				
	②ディスク障害対策	②-1	診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。	◎	ディスクの劣化や故障により、情報の読み取り不能又は不完全な読み取りが生じる。	7.3 保存性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】 （2）記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくは RAID-6 相当以上のディスク障害に対する対策を行うこと。
3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-1	医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、医療機関等と合意する。	◎	医療情報システム等障害時に医療情報システム等内に保存された医療情報が一切閲覧できない。	7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（1）バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-2	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を講じる。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（2）見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。
		①-3	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために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、内容について、医療機関等と合意する。	◎				
		①-4	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために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、利用に必要な情報の提供、条件等について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】	（3）遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。
		①-5	緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等)をサービスに含め、これに必要なセキュリティ等の情報提供について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【ネットワークを通じて外部に保存する場合】	（1）緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。
		①-6	障害等が生じた場合の役割分担を明確にした上で、稼動を保証するサービスの範囲について、医療機関等と合意する。	◎		7.2 見読性の確保について	D.推奨されるガイドライン 【ネットワークを通じて外部に保存する場合】	（2）緊急に必要になるとまではいえない診療録等の見読性の確保 緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。
3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-1	電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管する。	◎	情報が毀損や滅失した場合にバックアップされたデータを用いて元の状態に復元できない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	1.　記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。
		①-2	各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	2.　システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。
		①-3	医療機関等が医療情報システム等を利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、医療機関等と合意する。	◎				
		①-4	医療情報システム等が情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。	◎				
		①-5	①-4において、他の事業者が提供する医療情報システム等を利用する場合においても、同様の情報を収集して、対応する。仮想化技術による医療情報システム等を利用する場合には、受託事業者が他の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。	◎				
		①-6	①-4により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。	◎				
		①-7	医療情報システム等に係る委託先に対しても、①-4の運用管理規程に定める管理方法への対応等を求める。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-8	情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （2）不適切な保管・取扱いによる情報の滅失、破壊の防止	5.　各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。
		①-9	①-8に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。	◎				
		①-10	①-9で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、医療機関等と合意する。	◎				
		①-11	リスク分析結果に基づき医療情報システム等のバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。	◎		7.3 保存性の確保について	D.推奨されるガイドライン 【医療機関等に保存する場合】 （1）不適切な保管・取扱いによる情報の滅失、破壊の防止	3.　診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。
		①-12	取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改竄・破壊等がないことを確認する。	◎				
	②バックアップに用いる記録媒体の管理	②-1	記録媒体に格納するバックアップについては、その媒体の特性（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、使用終了日を明らかにして管理する。	◎	バックアップにおける記憶媒体の劣化や容量超過により、バックアップが正常に行われない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （3）記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止	1.　記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。
		②-2	バックアップの記録媒体の使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。	◎				
		②-3	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、別の媒体等に複写する。	◎				
		②-4	②-1～②-3の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。	◎				
		②-5	バックアップに係る情報の提供について、医療機関等と合意する。	◎				
3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-1	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。	◎	医療情報システム等を更改等により移行する際、移行元で記録された情報が移行後に正しく読みだせない。	7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （4）媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	1.　システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。
		①-2	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、医療機関等と合意する。	◎				
		①-3	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等に備える。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【医療機関等に保存する場合】 （4）媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	2.　マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。
		①-4	①-3に示す機能等を備えることが困難な場合の医療情報システム等更新・移行の手順について、医療機関等と合意する。	◎				

別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインの対応表

対策項目					対策項目で対応できるリスクシナリオ例	関連する医療情報安全管理ガイドライン要求事項		
大項目	小項目	No.	内容	区分		項番	区分	内容
		①-5	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。	◎		7.3 保存性の確保について	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	（1）データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。
		①-6	データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。	◎				
		①-7	①-6の結果、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、対応に必要な措置に関する具体的な情報提供を行う。	◎				
		①-8	①-7は、他の医療情報システム等とのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、医療機関等と合意する。	◎				
		①-9	データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、見読性確保の対策を講じる。	◎				
		①-10	医療情報システム等に関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、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う。	◎		7.3 保存性の確保について	D.推奨されるガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】 （1）ネットワークや外部保存を受託する機関の設備の互換性を確保すること	1. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。
		①-11	他の事業者が提供する医療情報システム等を用いて、サービスを提供する場合には、他の事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他の事業者のサービスの停止・変更に伴い、自社が提供する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は含まない）等が生じる場合には、機器の劣化対策を講じる。	◎				
		①-12	医療情報システム等に係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他の事業者のサービスの変更を行う場合には、①-10、①-11を考慮して行う。	◎				