HISPRO　外部保存、ASP・SaaS　チェックシート項目集（試行版）

項番 大分類	中分類	小分類	要件	分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
1	1	1	1	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。	総務省ASP-GL	Ⅱ．1．1．1	・情報セキュリティへの取り組みに関する基本方針が定められ、文書化されているか ・その基本方針文書は経営陣から承認され、署名されているか
1	1	1	2	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報セキュリティに関する基本的な方針を定めた文書は、定期的又はサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。この見直しの結果、変更の必要性が生じた場合には、経営陣の承認の下で改定等を実施すること。	総務省ASP-GL	Ⅱ．1．1．2	・情報セキュリティ基本方針文書が見直されているか
1	1	1	3	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	経営陣は、情報セキュリティに関する取組についての責任と関与を明示し、人員・資産・予算の面での積極的な支援・支持を行うこと。	総務省ASP-GL	Ⅱ．2．1．1	・情報セキュリティマニュアル等に左記の要求事項が盛り込まれているか
1	1	1	4	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。	総務省ASP-GL	Ⅱ．2．1．2	・情報セキュリティマニュアル等に左記の要求事項が盛り込まれているか ・当該の記述が見直されているか
1	1	1	5	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。	総務省ASP-GL	Ⅱ．2．1．3	・情報セキュリティマニュアル等に左記の要求事項が盛り込まれているか
1	1	1	6	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。	総務省ASP-GL	Ⅱ．2．2．1	・情報セキュリティマニュアル等に左記の要求事項が盛り込まれているか ・情報資産がリストアップされているか ・リストアップされた情報資産のリスクが識別され、評価されているか ・識別され、評価され対策が必要となったたリスクへの管理策が実施されているか
1	1	1	7	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。	総務省ASP-GL	Ⅱ．2．2．2	・情報資産へのアクセスが可能となる外部組織がすべて識別されているか ・それらすべての外部組織と先の要求事項を含む契約が締結されているか
1	1	1	8	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	連携事業者が提供するサービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携事業者によって確実に実施されることを担保すること。	総務省ASP-GL	Ⅱ．3．1．1	・連携事業者との間でSLAに関する契約が締結されているか ・そのSLAの内容が相手事業者に実施されていることを担保する仕組みがあるか
1	1	1	9	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	連携事業者が提供するサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。	総務省ASP-GL	Ⅱ．3．1．2	・連携事業者のサービスの運用に関する報告と記録を常に確認する運用になっているか ・定期的に監査を実施しているか
1	1	1	10	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。	総務省ASP-GL	Ⅱ．4．1．1	・情報資産台帳が作成されているか ・そこに左記の要求事項が含まれているか
1	1	1	11	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。	総務省ASP-GL	Ⅱ．4．2．1	・左記の要求事項に則り、情報資産が分類されているか
1	1	1	12	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。	総務省ASP-GL	Ⅱ．4．3．1	・リスクアセスメントの結果が定期的に見直されているか
1	1	1	13	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	サービスの提供に用いる情報システムが、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に点検・監査すること。	総務省ASP-GL	Ⅱ．4．3．2	・定期的に内部監査を実施しているか ・内部監査での指摘事項が、速やかに是正されているか
1	1	1	14	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。	総務省ASP-GL	Ⅱ．5．1．1	・雇用に際して、左記の要求事項を満たす契約が締結されているか
1	1	1	15	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。	総務省ASP-GL	Ⅱ．5．2．1	・情報セキュリティに関する意識向上を目的とした従業員の訓練と教育を実施しているか
1	1	1	16	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	従業員が、情報セキュリティポリシーもしくはサービス提供上の契約に違反した場合の対応手続を備えること。	総務省ASP-GL	Ⅱ．5．2．2	・左記の要求事項に則り、罰則等の対応手続きが用意されているか
1	1	1	17	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。	総務省ASP-GL	Ⅱ．5．3．1	・雇用の終了または変更に際して、左記の要求事項を満たす手続きが定められているか
1	1	1	18	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん・破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続きを定め、実施を要求すること。 報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。	総務省ASP-GL	Ⅱ．6．1．1	・左記の要求事項に対応した手続きが定められているか ・その手続きが実際に発動した形跡が見られるか
1	1	1	19	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。	総務省ASP-GL	Ⅱ．7．1．1	・保持する情報に関する法令等が識別されているか ・その法令等を遵守するための対策が実施されているか
1	1	1	20	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。	総務省ASP-GL	Ⅱ．7．1．2	・左記の要求事項に関連する記録が取得され、管理、保護されているか
1	1	1	21	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。	総務省ASP-GL	Ⅱ．7．1．3	・情報セキュリティマニュアル等に左記の要求事項が盛り込まれているか
1	1	1	22	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	サービスの提供に支障が生じた場合には、その原因が連携事業者に起因するものであったとしても、利用者と直接契約を結ぶ事業者が、その責任において一元的にユーザサポートを実施すること。	総務省ASP-GL	Ⅱ．8．1．1	・左記の要求事項に関する内容が利用者と締結したSLAに盛り込まれているか
1	1	1	23	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	運用管理規程等において次の内容を定めること。 (a) 理念（基本方針と管理目的の表明） (b) 医療機関等の体制 (c) 契約書・マニュアル等の文書の管理 (d) リスクに対する予防、発生時の対応の方法 (e) 機器を用いる場合は機器の管理 (f) 個人情報の記録媒体の管理（保管・授受等）の方法 (g) 患者等への説明と同意を得る方法 (h) 監査 (i) 苦情・質問の受付窓口	総務省医療ASP-GL	3.2.1	・左記の内容が含まれるように運用管理規程等を定めているか
1	1	1	24	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	・医療機関等の管理者に対する最終的な管理責任者の明確化 ・個人情報保護管理を含むサービス提供体制の明確化 ・サービス提供に関する運用等の定期的な報告 ・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	総務省医療ASP-GL	2.3.1	・左記体制を明確にしているか
1	1	1	25	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	過不足なく適用範囲を定めた適用宣言書に基づく情報セキュリティに関する認証及び認定を活用することが有効	経産省医療外部保存-GL	2	・過不足なく適用範囲を定めた適用宣言書に基づく情報セキュリティに関する認証及び認定を活用しているか
1	1	1	26	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	認証及び認定には、プライバシーマーク制度、ISMS 適合性評価制度等がある。情報処理事業者は本ガイドラインに示される安全管理策を適用した上で、適切な制度を選び、認証または認定等を受けること	経産省医療外部保存-GL	2	・プライバシーマーク制度、ISMS 適合性評価制度等、適切な制度を選び、認証または認定等を受けているか
1	1	1	27	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、サービス提供時はもちろん、リスク評価を行い、必要に応じて定期的にアプリケーションの脆弱性検査を実施して、安全性を確認すること。	経産省医療外部保存-GL	3.5	・ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、サービス提供時はもちろん、リスク評価を行い、必要に応じて定期的にアプリケーションの脆弱性検査を実施して、安全性を確認しているか。
1	1	1	28	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	アプリケーション入力による外部保存をネットワーク経由で行ってデータをデータベースにより保管する場合には、システムの構成に配慮したリスク評価を行い、暗号技術等を利用した適切なリスク低減策を適用すること。	経産省医療外部保存-GL	3.5.1	・アプリケーション入力による外部保存をネットワーク経由で行ってデータをデータベースにより保管する場合には、システムの構成に配慮したリスク評価を行い、暗号技術等を利用した適切なリスク低減策を適用しているか。
1	1	1	29	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	インターネットVPNを使用する場合は、交換する情報に求められる機密性のレベルを判断し、コスト及び運用に対して、閉域網上に構築されたVPN との比較を行い、適切なネットワークを選択すること。	経産省医療外部保存-GL	3.5.2	・インターネットVPNを使用する場合は、交換する情報に求められる機密性のレベルを判断し、コスト及び運用に対して、閉域網上に構築されたVPN との比較を行い、適切なネットワークを選択しているか。
1	1	1	30	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと	経産省医療外部保存-GL	4.2	・ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におかれ、且、提出要求があった場合、提出手順が定められているか
1	1	1	31	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告についても、提出可能な状態におくこと	経産省医療外部保存-GL	4.2	・定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告についても、提出可能な状態におかれ、且、提出要求のあった場合提出手順が定められているか
1	1	1	32	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	電子化された個人情報の保護に一定の知識を有する責任者を定めること	経産省医療外部保存-GL	4.2	・電子化された個人情報の保護に一定の知識を有する責任者が定められているか

項番 大分類	中分類	小分類	要件	分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
1	1	1	33	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	システムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行うこと	経産省医療外部保存-GL	4.2	・システムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を行う為のPDCAサイクル体制ができているか、また定期的に行っているか/その為の運用規程が出来ているか
1	1	1	34	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	事態の発生を認識次第、ただちに医療機関等に通知し、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために、協力して情報収集を図ること	経産省医療外部保存-GL	4.3	・事態の発生を認識次第、ただちに医療機関等に通知し、医療機関等の管理者が個々の患者、行政機関や社会へ説明・公表するために、協力して情報収集を図ることが規定されているか、その内容が実施可能なもになっているか
1	1	1	35	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	前もって発生しうる事故と考えられる原因を洗い出して対応手順を策定しておくこと	経産省医療外部保存-GL	4.3	・前もって発生しうる事故と考えられる原因を洗い出して対応手順を策定しているか、実施体制が出来ているか
1	1	1	36	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	確定された原因にもとづき再発防止策を講じること	経産省医療外部保存-GL	4.3	・確定された原因にもとづき再発防止策を講じることが出来るか
1	1	1	37	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	プライバシーマーク認定・ISMS認証等の公正な第三者の認定を取得すること	経産省医療外部保存-GL	7.1	・公正な第三者認証を取得しているか ・その認証は有効か
1	1	1	38	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	ISMS認証を取得する場合には、受託した医療情報を扱う部門、部署を全て含むよう適用範囲を設定した上でISMS認証を取得すること	経産省医療外部保存-GL	7.1.1	＜ISMSの場合のみ＞ ・ISMSの場合の対象範囲に受託した医療情報を扱う部門、部署をすべて含んでいるか
1	1	1	39	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療情報の高い機微性、完全性の要求を鑑みて、通常のISMS認証取得プロセス、維持プロセスに加え、以下の事項を満たすよう本ガイドラインを活用すること ・認証取得あるいは更新の際にISMSの安全管理策として、本ガイドライン「7医療情報を受託管理する情報処理事業者における安全管理上の要求事項」にて提示する安全管理策を盛り込む ・受託管理する医療情報の入り口から出口まで包括的にISMSの適用範囲とする ・安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう準備を行う(適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること)	経産省医療外部保存-GL	7.1.1	＜ISMSの場合のみ＞ ・左記の推奨事項を考慮しているか
1	1	1	40	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	「7.1.2　図 12」に従って、その適用範囲及び管理策が本ガイドラインで示す基準に従っているかどうか確認し、必要であれば再（拡大）審査を受けること	経産省医療外部保存-GL	7.1.2	＜ISMSの場合のみ＞ ・本ガイドラインに従って適用範囲が設定されているか ・本ガイドラインに従って管理策が選択されているか ・本ガイドラインを基準とした情報セキュリティ監査を受けているか ・情報セキュリティ監査結果を医療機関に提示しているか
1	1	1	41	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること	経産省医療外部保存-GL	7.2.1	・資産台帳自身を保護するための管理策が実施されているか
1	1	1	42	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること	経産省医療外部保存-GL	7.2.1	・資産台帳の整備に関するルールが文書化されているか
1	1	1	43	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	預託された情報の全てを資産台帳に記録すること	経産省医療外部保存-GL	7.2.1	・明文化されたルールに従って記録されているか ・全ての預託情報が記録されているか
1	1	1	44	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと	経産省医療外部保存-GL	7.2.1	・資産台帳の閲覧と検索が速やかにできるか
1	1	1	45	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	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すること	経産省医療外部保存-GL	7.2.1	・資産台帳の閲と編集が必要な作業者に限定されているか
1	1	1	46	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること	経産省医療外部保存-GL	7.2.1	・資産台帳（電子文書）へのアクセス侵害が記録されているか
1	1	1	47	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	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	経産省医療外部保存-GL	7.2.2	・情報を分類するための指針があるか ・情報の管理責任者が指針に従って適切な分類を実施できるようになっているか
1	1	1	48	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	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	経産省医療外部保存-GL	7.2.2	・情報の分類が指針通り行われていることを定期的に確認することを定めたルールが明文化されているか ・そのルール通りに定期的な確認が実施されているか
1	1	1	49	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	預託される情報に対して分類にもとづいたリスク分析を実施すること	経産省医療外部保存-GL	7.2.2	・情報が分類に基づいてリスク分析されているか
1	1	1	50	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること	経産省医療外部保存-GL	7.2.2	・リスク分析結果に基づいて管理策が実施されているか
1	1	1	51	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	分類がわかるように情報にラベルをつけること（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、承認を得ること）	経産省医療外部保存-GL	7.2.2	・情報が分類に基づいてラベル付けされているか（単独で見て識別できるか）
1	1	1	52	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	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	経産省医療外部保存-GL	7.2.2	・各ラベルに応じた処理方式が定められ、文書化されているか
1	1	1	53	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと	経産省医療外部保存-GL	7.3	・医療情報の安全管理に関する方針が定められているか ・医療機関の求めに応じて提出できる状態になっているか
1	1	1	54	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと	経産省医療外部保存-GL	7.3	・個人情報保護に関する方針が定められているか ・医療機関の求めに応じて提出できる状態になっているか
1	1	1	55	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	個人情報保護に関しては、医療機関等の監督の下に行うこと	経産省医療外部保存-GL	7.3	・医療機関の監督のもとに個人情報保護を実施しているか
1	1	1	56	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報処理の安全管理に関わる手順書、運用管理規程を整備すること	経産省医療外部保存-GL	7.3	・情報処理の安全管理に関わる手順書、運用管理規程が整備されているか
1	1	1	57	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、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、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと	経産省医療外部保存-GL	7.3	・運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、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、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載されているか
1	1	1	58	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うこと	経産省医療外部保存-GL	7.4	・情報の移動に関してのリスクが分析されているか
1	1	1	59	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること	経産省医療外部保存-GL	7.6.13	・情報処理装置それぞれのセキュリティ要求事項を整理し明文化しているか
1	1	1	60	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること	経産省医療外部保存-GL	7.6.13	・情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理して明文化しているか
1	1	1	61	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	各作業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こと。	経産省医療外部保存-GL	7.6.15	・各作業者は自身のパスワードを秘密にしているか ・パスワードを記録する必要がある場合、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しているか
1	1	1	62	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	システム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こと。	経産省医療外部保存-GL	7.6.15	・システム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の対応が定めてあるか ・システム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しているか
1	1	1	63	1. 設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療情報を操作する可能性のある職員の全てについて、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こと。派遣従業員については秘密保持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こと。	経産省医療外部保存-GL	7.7	・医療情報を操作する可能性のある職員の全てについて、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ているか ・派遣従業員については秘密保持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ているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
1	1	1	64	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療情報を操作する可能性のある職員の全てに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ものだけを選定すること。派遣従業員に関しては、派遣元に対し、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こと。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こと。	経産省医療外部保存-GL	7.7	・医療情報を操作する可能性のある職員の全てに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ものだけを選定しているか ・派遣従業員に関しては、派遣元に対し、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ているか ・受入れ後に正規職員同等の教育を行っているか ・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っているか
1	1	1	65	1．設備・運用　1）一般的条件 ①組織・運用への対策項目	必須	医療情報を操作する職員が退職する際には、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こと。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こと。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こと。	経産省医療外部保存-GL	7.7	・医療情報を操作する職員が退職する際には、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いるか ・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ているか ・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ているか
1	1	2	1	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。	総務省ASP-GL	Ⅲ．1．1．1	・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、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を、適切な間隔（5分、10分）で行っているか。
1	1	2	2	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	稼働停止を検知した場合は、利用者に速報を通知すること。	総務省ASP-GL	Ⅲ．1．1．1	・稼働停止を検知した場合は、利用者に適切な時間（20分、60分）内に速報を通知することとなっているか。
1	1	2	3	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。	総務省ASP-GL	Ⅲ．1．1．2	・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、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を、適切な間隔（10分、30分）で行っているか。
1	1	2	4	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	障害を検知した場合は、利用者に速報を通知すること。	総務省ASP-GL	Ⅲ．1．1．2	・障害を検知した場合は、利用者に適切な時間（20分、60分）内に速報を通知することとなっているか。
1	1	2	5	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	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、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。	総務省ASP-GL	Ⅲ．1．1．3	【推奨】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、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を、適切な間隔（10分、30分）で行っているか。
1	1	2	6	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	また、利用者との取決めに基づいて、監視結果を利用者に通知すること。	総務省ASP-GL	Ⅲ．1．1．3	【推奨】また、利用者との取決めに基づいて、監視結果を利用者に適切な時間（20分、60分）内に通知することとなっているか。
1	1	2	7	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	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・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。	総務省ASP-GL	Ⅲ．1．1．4	【推奨】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・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告することとなっているか。
1	1	2	8	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。	総務省ASP-GL	Ⅲ．1．1．5	・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（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施しているか。
1	1	2	9	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	総務省ASP-GL	Ⅲ．1．1．6	・サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、適切な期間（24時間、24時間）内にパッチによる更新を行っているか。
1	1	2	10	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	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（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に報告すること。	総務省ASP-GL	Ⅲ．1．1．7	【推奨】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（情報セキュリティ対策機器、通信機器等）の監視結果（障害監視、死活監視、パフォーマンス監視）について、定期報告書を作成して利用者等に適切な間隔（1か月、3か月）で報告することとなっているか。
1	1	2	11	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。	総務省ASP-GL	Ⅲ．1．1．8	・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（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に適切な期間（1時間、1時間）内に対して行うこととなっているか。
1	1	2	12	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。	総務省ASP-GL	Ⅲ．1．1．9	・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めているか。
1	1	2	13	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	また、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、ネットワークの運用・管理に関する手順書を作成すること。	総務省ASP-GL	Ⅲ．1．1．9	・また、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、ネットワークの運用・管理に関する手順書を作成しているか。
1	1	2	14	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サービスを利用者に提供する時間帯を定め、この時間帯におけるサービスの稼働率を規定すること。	総務省ASP-GL	Ⅲ．2．1．1	・サービスを利用者に提供する時間帯を定め、この時間帯におけるサービスの稼働率を適切な値（99．5%、99%）に規定しているか。
1	1	2	15	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。	総務省ASP-GL	Ⅲ．2．1．1	・また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定しているか。
1	1	2	16	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。	総務省ASP-GL	Ⅲ．2．1．2	・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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、適切な期間（サービス提供期間＋1年間、サービス提供期間＋6か月）保存しているか。
1	1	2	17	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	利用者の利用状況、例外処理及び情報セキュリティ事象の基本記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。	総務省ASP-GL	Ⅲ．2．1．3	・利用者の利用状況、例外処理及び情報セキュリティ事象の基本記録（ログ等）を取得し、ログ種類に応じた適切な期間（利用状況：3か月、1か月、基本記録：5年、1年）保管しているか。また、記録（ログ等）の保存期間を明示しているか。
1	1	2	18	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	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・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。	総務省ASP-GL	Ⅲ．2．1．4	【推奨】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・ストレージについて種類に応じた適切な間隔（自動診断：1か月、1か月、詳細診断：6か月、1年、アプリケーション：1年、1年）でぜい弱性診断を行い、その結果に基づいて対策を行っているか。
1	1	2	19	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。	総務省ASP-GL	Ⅲ．2．2．1	・サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する適切な間隔（パターンファイルの更新：24時間、24時間）で対策を講じているか。
1	1	2	20	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	データベースに格納されたデータの暗号化を行うこと。	総務省ASP-GL	Ⅲ．2．2．2	【推奨】データベースに格納されたデータの暗号化を行っているか。
1	1	2	21	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。	総務省ASP-GL	Ⅲ．2．3．1	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の適切な間隔（1日、1週間）でバックアップを実施しているか。さらに適切な数の世代バックアップ（5世代、2世代）を実施しているか。
1	1	2	22	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。	総務省ASP-GL	Ⅲ．2．3．2	【推奨】バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて適切な間隔（バックアップ実施都度、実施都度）で確認しているか。
1	1	2	23	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。	総務省ASP-GL	Ⅲ．3．1．1	・ネットワーク構成図を作成しているか（ネットワークをアウトソーシングする場合を除く）。
1	1	2	24	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。	総務省ASP-GL	Ⅲ．3．1．1	・また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別しているか。提供する場合は利用者の接続回線も含めてアクセス制御の責任を負っているか。
1	1	2	25	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。	総務省ASP-GL	Ⅲ．3．1．1	・また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定しているか。
1	1	2	26	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。	総務省ASP-GL	Ⅲ．3．1．2	・情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限しているか。
1	1	2	27	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。 また、運用管理規定を作成すること。	総務省ASP-GL	Ⅲ．3．1．3	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を、それぞれの権限者別に適切な方式（利用者：生体認証 又は ICカード、ICカード 又はID・パスワード、管理者：デジタル証明書による認証、生体認証 又は ICカード、生体認証 又は ICカード）で行っているか。 また、運用管理規定を作成しているか。

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
1	1	2	28	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。	総務省ASP-GL	Ⅲ．3．1．3	・ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めているか。
1	1	2	29	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。	総務省ASP-GL	Ⅲ．3．1．4	・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じているか。
1	1	2	30	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS /IPS の導入等）を講じること。	総務省ASP-GL	Ⅲ．3．1．5	【推奨】不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS /IPSの導入等）を講じているか。そのパターンファイルの更新を適切な間隔（1日、3週間）で行っているか。
1	1	2	31	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。	総務省ASP-GL	Ⅲ．3．2．1	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えているか。
1	1	2	32	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	総務省ASP-GL	Ⅲ．3．2．2	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、適切な方式（IP暗号通信（VPN(IPsec)等） 又はHTTP暗号通信（SSL(TLS)等））での通信の暗号化を行っているか。
1	1	2	33	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。	総務省ASP-GL	Ⅲ．3．2．3	・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施しているか。
1	1	2	34	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。	総務省ASP-GL	Ⅲ．3．2．4	・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定しているか。
1	1	2	35	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。	総務省ASP-GL	Ⅲ．3．2．5	【推奨】外部ネットワークの障害を監視しているか。障害を検知した場合は管理責任者に適切な時間（60分、無し）内に通報しているか。
1	1	2	36	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、地震・水害に対する対策が行われていること。	総務省ASP-GL	Ⅲ．4．1．1	【推奨】サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）について、地震・水害に対する対策を行っているか。
1	1	2	37	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じること。	総務省ASP-GL	Ⅲ．4．2．1	・サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所には、停電や電力障害が生じた場合に電源を確保するための適切な対策（UPSによる電源供給：10分、10分、複数給電：実施、実施、非常用発電：実施、無し）を講じているか。
1	1	2	38	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供すること。	総務省ASP-GL	Ⅲ．4．2．2	【推奨】サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置する場所では、設置されている機器等による発熱を抑えるのに十分な容量の空調を提供しているか。
1	1	2	39	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	サーバルームに設置されているサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する対策を講じること。	総務省ASP-GL	Ⅲ．4．3．1	【推奨】サーバルームに設置されているサービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、放水等の消火設備の使用に伴う汚損に対する適切な対策（ガス系消火設備等）の使用）を講じているか。
1	1	2	40	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えること。	総務省ASP-GL	Ⅲ．4．3．2	・サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムを設置するサーバルームには、火災検知・通報システム及び消火設備を備えているか。
1	1	2	41	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	情報処理施設に雷が直撃した場合を想定した対策を講じること。	総務省ASP-GL	Ⅲ．4．3．3	・情報処理施設に雷が直撃した場合を想定した対策を講じているか。
1	1	2	42	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。	総務省ASP-GL	Ⅲ．4．3．4	【推奨】情報処理施設付近に誘導雷が発生した場合を想定した対策を講じること。
1	1	2	43	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じること。	総務省ASP-GL	Ⅲ．4．3．5	【推奨】サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムについて、作業に伴う静電気対策を講じているか。
1	1	2	44	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。	総務省ASP-GL	Ⅲ．4．4．1	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間（2年以上、2年以上）保存しているか。
1	1	2	45	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。	総務省ASP-GL	Ⅲ．4．4．2	【推奨】重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間（365日24時間）と監視範囲を定めて監視を行っているか。また、監視カメラの映像を予め定められた適切な期間（6か月、1か月）保存しているか。
1	1	2	46	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成すること。	総務省ASP-GL	Ⅲ．4．4．3	・重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成しているか。
1	1	2	47	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置すること。	総務省ASP-GL	Ⅲ．4．4．4	【推奨】重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置しているか。
1	1	2	48	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	重要な物理的セキュリティ境界に警備員を常駐させること。	総務省ASP-GL	Ⅲ．4．4．5	【推奨】重要な物理的セキュリティ境界に警備員を常駐（365日24時間）させているか。
1	1	2	49	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	サーバルームやラックの鍵管理を行うこと。	総務省ASP-GL	Ⅲ．4．4．6	・サーバルームやラックの鍵管理を行っているか。
1	1	2	50	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	電子データの原本性確保を行うこと。	総務省ASP-GL	Ⅲ．5．1．1	【推奨】電子データの適切なレベルで原本性確保（時刻認証、署名 及び印刷データ電子化・管理、署名 及び印刷データ電子化・管理）を行っているか。
1	1	2	51	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	個人情報は関連する法令に基づいて適切に取り扱うこと。	総務省ASP-GL	Ⅲ．5．1．2	・個人情報は関連する法令に基づいて適切に取り扱っているか。
1	1	2	52	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。	総務省ASP-GL	Ⅲ．5．2．1	・運用管理端末に、許可されていないプログラム等のインストールを行わせないこととしているか。
1	1	2	53	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。	総務省ASP-GL	Ⅲ．5．2．1	・従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行っているか。パターンファイルの更新を適切な間隔（ベンダリリースから24時間以内）で行っているか。
1	1	2	54	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。	総務省ASP-GL	Ⅲ．5．2．1	・技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を適切な間隔で収集し、適切なタイミング（ベンダリリースから24時間以内）でパッチによる更新を行っているか。
1	1	2	55	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	総務省ASP-GL	Ⅲ．5．3．1	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行っているか。
1	1	2	56	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	機器及び媒体を正式な手順に基づいて廃棄すること。	総務省ASP-GL	Ⅲ．5．3．2	・機器及び媒体を正式な手順に基づいて廃棄しているか。
1	1	2	57	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	バックアップ媒体も含め、個人情報を含むサーバ以外の機器媒体等の保管場所を施錠管理すること。	総務省医療ASP-GL	3.2.2	・機器・媒体等の保管場所を定めているか ・機器・媒体等に対する規程が定めてあるか ・機器・媒体等の保管場所は施錠管理されているか
1	1	2	58	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	委託業務に基づき受託する個人情報の内容を参照する必要が生じる場合には、データアクセスが可能な端末が設置されている部屋に対する入退出の施錠管理及び入退出管理を行うこと。	総務省医療ASP-GL	3.2.2	・受託した個人情報を参照可能である区域を定めてあるか ・個人情報を参照可能である区域に対して入退室に関するルールが定めてあるか ・受託した個人情報を参照可能である区域への入退室の施錠管理及び入退出管理がされているか
1	1	2	59	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	受託する個人情報を保守に用いる端末に保存しない旨、自社の運用管理規程等に定めること。	総務省医療ASP-GL	3.2.2	・運用管理規程等を定めているか ・運用管理規程等に受託する情報の扱いに対する項目があるか ・運用管理規程等に保守に用いる端末に対する項目があり、個人情報を保存しないことを定めているか
1	1	2	60	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること。	総務省医療ASP-GL	3.2.3	・運用管理規程等を定めているか ・運用管理規程等に受託情報を扱う運用端末にクリアスクリーン等の防止策を施すことを定めてあるか
1	1	2	61	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	受託した情報の処理に必要な、システムに関する動作確認に際し、原則個人情報を含むデータを使用せず、テスト用のデータを使用すること。	総務省医療ASP-GL	3.2.3	・動作確認を行う際のデータは、テスト用のデータを使用することになっているか
1	1	2	62	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	総務省医療ASP-GL	3.2.3	・動作確認に際し、やむを得ず受託した個人情報を使用する場合の規定が定められているか ・規定について医療機関等と合意を得ているか
1	1	2	63	1．設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	提供するサービスにおいて、医療機関等の利用者の職種、担当業務等に応じたアクセス制御が可能な機能を含めること。	総務省医療ASP-GL	3.2.3	・提供するサービスにアクセス制御機能が備えてあるか ・アクセス制御機能が医療機関等の利用者の職種、担当業務等に応じることが可能か

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
1	1	2	64	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	医療情報について、医療機関等が行う情報資産分類の区分に従い、アクセス制御を行うこと。	総務省医療ASP-GL	3.2.3	・情報資産について、重要度等に応じて分類が行われているか ・情報の分類に関して医療機関等と合意を得ているか ・アクセス権の設定を情報の分類に従い実施しているか ・アクセス制御機能のグループの権限や適用範囲について、医療機関等と合意を得ているか ・グループに所属するユーザについて、医療機関等と合意を得ているか
1	1	2	65	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	推奨	受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること。	総務省医療ASP-GL	3.2.3	・運用管理規程等を定めているか ・運用管理規程等に受託情報を扱う運用端末にクリアスクリーン等の防止策を施すことを定めてあるか
1	1	2	66	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	インターネットからの第三者による不正なアクセスを防止するため、医療機関等の機器と情報処理事業者側の機器において、ネットワーク境界のファイアウォールまたはVPN 装置等により、適切なアクセス制御を行うこと.	経産省医療外部保存-GL	3.2	・インターネットからの第三者による不正なアクセスを防止するため、医療機関等の機器と情報処理事業者側の機器において、ネットワーク境界のファイアウォールまたはVPN 装置等により、適切なアクセス制御を行っているか.
1	1	2	67	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	いずれの種別の回線であっても、通信ログ及び通信状況を監視し、異常が発生した場合には迅速に対処すること。	経産省医療外部保存-GL	3.2	・いずれの種別の回線であっても、通信ログ及び通信状況を監視し、異常が発生した場合には迅速に対処しているか。あるいは体制になっているか
1	1	2	68	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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こと。	経産省医療外部保存-GL	7.6.10	・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っているか。
1	1	2	69	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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こと。	経産省医療外部保存-GL	7.6.10	・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、迅速に対応策をとっているか。
1	1	2	70	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	アプリケーションにて情報の登録、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こと	経産省医療外部保存-GL	7.6.10	・アプリケーションにて情報の登録、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っているか
1	1	2	71	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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、管理すること。	経産省医療外部保存-GL	7.6.12	・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ているか ・監査ログを適切に管理しているか
1	1	2	72	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	監査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こと。	経産省医療外部保存-GL	7.6.12	・監査ログを定期的に検証しているか ・検証の結果で、不正な行為、システムの異常等を検出できているか
1	1	2	73	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	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こと。	経産省医療外部保存-GL	7.6.12	・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いるか
1	1	2	74	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。	経産省医療外部保存-GL	7.6.12	・標準時刻に同期するための時刻提供元は信頼できる機関を利用しているか
1	1	2	75	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	・ ログデータにアクセスする作業者及び操作を制限すること。	経産省医療外部保存-GL	7.6.12	・ ログデータにアクセスする作業者及び操作を制限しているか
1	1	2	76	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。 ・電子媒体は台帳を作成して管理すること。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こと。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こと。(3.6.7.3)	経産省医療外部保存-GL	7.8	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・電子媒体の台帳を作成し、利用に関する記録が行われているか ・台帳と電子媒体を定期的に検証しているか ・電子媒体廃棄後も一定期間にわたり、記録を維持しているか
1	1	2	77	1. 設備・運用　1）一般的条件 ②物理的・技術的対策項目	必須	代替施設、バックアップ施設に対しても本ガイドラインで提示する物理的安全対策を施すこと。	経産省医療外部保存-GL	7.10.1	・代替施設、バックアップ施設に対しても経済産業省ガイドラインで提示する物理的安全対策を実施しているか
1	2	1	1	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・提供サービスの仕様及び運用、セキュリティ対策に関する文書化 ・提供するサービスの仕様及び提供する品質に関する説明及び必要な情報提供 ・サービス提供に関する監査等情報提供	総務省医療ASP-GL	2.3.1	・提供サービスの仕様及び運用、セキュリティ対策に関する文書化 ・提供するサービスの仕様及び提供する品質に関する説明及び必要な情報提供 ・サービス提供に関する監査等情報提供 に関する情報提供を行っているか
1	2	1	2	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	・サービス提供改善及びセキュリティ向上の必要性についての定期的なレビュー結果の報告	総務省医療ASP-GL	2.3.1	・サービス提供改善及びセキュリティ向上の必要性についての定期的なレビュー結果の報告を行っているか、またその体制となっているか
1	2	1	3	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	・緊急時における医療機関の管理者に対して提供する情報内容、役割分担等の明確化	総務省医療ASP-GL	2.3.2	・緊急時における医療機関の管理者に対して提供する情報内容、役割分担等が明確になっているか
1	2	1	4	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	・サービス提供状況に関する記録を収集、緊急時の報告体制の構築	総務省医療ASP-GL	2.3.2	・サービス提供状況に関する記録の収集、緊急時の報告体制が構築されているか
1	2	1	5	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	・媒体管理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	総務省医療ASP-GL	2.3.2	・緊急時の媒体管理及び機器の管理等に関する手順が明確化され、緊急時の報告体制が構築されているか
1	2	1	6	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・情報事故等が発生した場合の原因追及に必要な情報の提供の範囲、条件等の合意、及びその実施 ・善後策として講じる対応策等の提案 ・情報事故が発生した場合の損害填補責任に関する合意	総務省医療ASP-GL	2.3.2	・情報事故等が発生した場合の原因追及に必要な情報の提供の範囲、条件等の合意、及びその実施 ・善後策として講じる対応策等の提案 ・情報事故が発生した場合の損害填補責任に関する合意 上記に関して合意され実施されているか、あるいは実施体制となっているか
1	2	1	7	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・通常運用時、緊急時の医療機関等と事業者との起点から終点までの通信手順を明確にし、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こと。	総務省医療ASP-GL	3.2.9	・通信手順について、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・通信手順の責任範囲に事業者が含まれる場合、医療機関等と事業者との起点から終点までの通信手順を明確にしているか ・通信手順の責任範囲に事業者が含まれる場合、通常時の手順と、緊急時の手順についてそれぞれ作成し、明確にしているか
1	2	1	8	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・医療機関等の管理者において発生する患者等に対する説明責任、管理責任等、各種責任に関し、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こと。	総務省医療ASP-GL	3.2.9	・発生する患者等に対する各種責任について、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・患者等に対する各種責任に事業者が含まれる場合、責任範囲を満たす対応について明確にしているか
1	2	1	9	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・サービスを提供する際に用いる回線の管理責任、品質等に対する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こと。	総務省医療ASP-GL	3.2.9	・サービスを提供する際に用いる回線の責任範囲を明確にして、医療機関等と合意を得ているか ・回線の責任範囲に事業者が含まれる場合、管理責任、品質等について明確に示しているか
1	2	1	10	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・患者が情報を閲覧する情報システムの安全性に関する説明責任等において、事業者は責任の範囲、役割等について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・患者が情報を閲覧する情報システムの責任範囲を明確にして、医療機関等と合意を得ているか ・情報システムの責任範囲に事業者が含まれる場合、安全性に関する説明責任等を明確に示しているか
1	2	1	11	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	推奨	・障害等が生じた場合の責任分界を明確にし、稼動を保証するサービスの品質について医療機関等と合意すること。	総務省医療ASP-GL	3.3.3	・障害等が生じた際のサービス品質が明確になっているか ・障害等が生じた際のサービス品質について、医療機関等と合意を得ているか
1	2	1	12	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	悪意のあるコード検査及び電子署名検証の過程で問題が発見された場合はただちに医療機関等に通知すること	経産省医療外部保存-GL	3.4	・悪意のあるコード検査及び電子署名検証の過程で問題が発見された場合はただちに医療機関等に通知しているか、または通知する体制となっているか
1	2	1	13	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	問題が発見された電子ファイルは原因特定を行う必要があることから、削除せずに情報処理装置から隔離したかたちで保管すること。	経産省医療外部保存-GL	3.4	・問題が発見された電子ファイルは原因特定を行う為に、削除せずに情報処理装置から隔離したかたちで保管しているか。
1	2	1	14	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	受入れた電子ファイル、払出した電子ファイル、預かっている電子ファイルの数量、発生したイベント等について定期的に確認できる仕組みを構築し医療機関等が確認できるようにする。	経産省医療外部保存-GL	3.4	・受入れた電子ファイル、払出した電子ファイル、預かっている電子ファイルの数量、発生したイベント等について定期的に確認できる仕組みを構築し医療機関等が確認できるようにしているか。
1	2	1	15	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	検証手続き中に異常が検出された場合は、直ちに医療機関等に連絡し、適切な事故対応手順を実施する。	経産省医療外部保存-GL	3.4	・検証手続き中に異常が検出された場合は、直ちに医療機関等に連絡し、適切な事故対応手順を実施しているか、またする体制となっているか。
1	2	1	16	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	「通常運用における責任」および「事後責任」について規定化され、実施されていること	経産省医療外部保存-GL	4.1	・「通常運用における責任」および「事後責任」について規定化され、実施されているか
1	2	1	17	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	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。	経産省医療外部保存-GL	7.7	・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、改ざん又は破壊等の行為が行われていないことを検証しているか
1	2	1	18	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在	必須	受領した情報と管理している情報の一覧の整合性を医療機関等が確認できるように、預かっている情報について台帳を維持管理することが求められる。	経産省医療外部保存-GL	8.2	・預かっている情報について台帳を作成し、適切な形で維持管理しているか
1	2	1	19	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ①通常運用／事後の責任の在り方	必須	・特定の職員だけが台帳の操作できるようになっていること ・情報の整合性について、複数人によるチェックが行われていること	経産省医療外部保存-GL	8.2	・台帳へのアクセス権限を特定の職員に絞っているか ・情報の整合性を確認する場合に、複数人によるチェックを行うようにルール化されており、証跡を残しているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
1	2	2	1	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	・緊急時に備えたアクセス制御等の手順等の明確化	総務省医療ASP-GL	2.3.2	・緊急時に備えたアクセス制御等の手順等が明確化されているか
1	2	2	2	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	・自社において定めた非常時におけるBCP に関する運用手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.8	・非常時におけるBCP に関する運用手順等が定めてあるか ・非常時におけるBCP に関する運用手順等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
1	2	2	3	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	・自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.8	・非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）が定めてあるか ・非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
1	2	2	4	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	医療機関等に情報処理機能を提供する事業者は、広域災害等の非常事態には自らも重要インフラの一部に相当するという意識を持ち、適切な事業継続計画を策定しておくこと。	経産省医療外部保存-GL	6.2	・医療機関等に情報処理機能を提供する事業者は、広域災害等の非常事態には自らも重要インフラの一部に相当するという意識を持ち、適切な事業継続計画を策定されているか
1	2	2	5	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	サービス提供を終了せざるを得ない状況においても、医療機関等の業務継続に悪影響を与えないよう、預託データの速やかな返却、他情報処理事業者へのサービス移管を可能とする配慮を行うこと	経産省医療外部保存-GL	6.2	・サービス提供を終了せざるを得ない状況においても、医療機関等の業務継続に悪影響を与えないよう、預託データの速やかな返却、他情報処理事業者へのサービス移管を可能とする配慮が行われているか
1	2	2	6	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	情報処理装置の耐用期間を越えないよう及び事業に支障を来たさないよう余裕を持った交換計画を策定しておくこと。	経産省医療外部保存-GL	6.3	・情報処理装置の耐用期間を越えないよう及び事業に支障を来たさないよう余裕を持った交換計画が策定され、実施されているか
1	2	2	7	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	預託された文書の種類による保存義務期間を契約で明記しておくこと	経産省医療外部保存-GL	6.3	・預託された文書の種類による保存義務期間を契約で明記するための契約条項とそれを裏付ける手段を有しているか
1	2	2	8	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	各種文書の契約に明記された保存義務期間より長期の保存が可能であるよう、事業継続に配慮すること	経産省医療外部保存-GL	6.3	・各種文書の契約に明記された保存義務期間より長期の保存が可能であるよう、事業継続に配慮されているか
1	2	2	9	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。 ・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、情報の読み出しが不可能であることを確認すること。	経産省医療外部保存-GL	7.8	・電子媒体の破棄に物理的破壊を用いているか ・破壊後に情報の読み取りができないことを確認しているか
1	2	2	10	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	医療情報システムのサービス提供における業務プロセス及び医療情報システム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こと。	経産省医療外部保存-GL	7.10.2	・医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいた医療情報処理に関する事業継続計画を策定しているか
1	2	2	11	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	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こと。	経産省医療外部保存-GL	7.10.2	・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しているか
1	2	2	12	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	必須	事業継続計画について定期的に見直しを行うこと。	経産省医療外部保存-GL	7.10.2	・事業継続計画の定期的な見直しを行っているか
1	2	2	13	1. 設備・運用　2）医療情報の保存／取扱いに関する条件 ③事業継続	推奨	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 ・機器及び職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の点検手順（不正侵入、情報改ざん、情報破損等の検出等） ・所管官庁への連絡体制、等	経産省医療外部保存-GL	7.10.2	・事業継続計画の事項はもれなく策定しているか
2	1	1	1	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	情報システム運用責任者を明確に定めて、合意すること。	総務省医療ASP-GL	3.2.1	・情報システム運用責任者を定めているか ・情報システム運用責任者を記載した書面をもって、利用者の合意を得ているか
2	1	1	2	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	受託した個人情報を参照可能な事務室等における入退室管理のルールが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.1	・受託した個人情報を参照可能である区域を定めてあるか ・個人情報を参照可能である区域に対して入退室に関するルールが定めてあるか ・入退室管理のルールについて、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	1	3	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	運用しているアクセス管理に関する規程類が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.1	・アクセス管理に関する規程が整備されているか ・アクセス管理に関する規程について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	1	4	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	自社の規程類の情報を医療機関に対して開示する範囲･条件等について、医療機関等と合意すること。	総務省医療ASP-	3.2.1	・事業者の規程を開示する範囲・条件を定めているか ・開示範囲等について医療機関等の合意を得ているか
2	1	1	5	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること。	総務省医療ASP-GL	3.2.1	・個人情報保護指針等を作成しているか ・個人情報保護指針等に委託業務を行う際の対応について記載されていること ・個人情報保護指針等を順守して、委託業務を行うことを契約・約款に記載していること
2	1	1	6	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	自社で定める個人情報保護指針等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.1	・個人情報保護指針等を作成しているか ・個人情報保護指針等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	1	7	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	個人情報保護法の対象に満たない件数(5,000 件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP-GL	3.2.1	・件数に関わらず、個人情報保護法における運用に準じることになっているか ・運用方式について医療機関に提出できるようにしているか
2	1	1	8	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	・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、内容等について合意すること。	総務省医療ASP-GL	3.2.6	・体制図を作成しているか ・体制図について、変更があった際に速やかに更新されているか ・体制図について、更新があった場合に速やかに医療機関等の合意を得ているか
2	1	1	9	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	・サービス提供に必要な保守業務を行うに際して、医療機関等の管理者に対して書面等により作業の事前及び事後に通知を行うこと、及び事前の了解を必要とする作業等について医療機関等と合意すること。	総務省医療ASP-GL	3.2.6	・保守作業を実施する際の手順について定めてあるか ・保守作業を実施する際の手順として、医療機関等に対し通知を行っているか ・保守作業の通知について事前でなければならない事項について、医療機関等と合意を得ているか
2	1	1	10	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	・サービス提供に必要なシステムの保守をリモートメンテナンスで行う場合の医療機関等の管理者に対する報告、承認等について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.6	・保守作業をリモートメンテナンスで実施する際の手順について定めてあるか ・リモートメンテナンスを行う際の作業手順、報告方法、承認等について、医療機関等と合意を得ているか
2	1	1	11	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	推奨	・サービス提供に必要な保守業務を医療機関施設内で行う際に、医療機関等の立会いの下で実施する旨を、医療機関等と合意すること。	総務省医療ASP-GL	3.2.6	・保守作業を実施する際の手順について定めてあるか ・保守作業を実施する際の手順として、医療機関施設内で行う際に、医療機関等の立会いの下で実施することとしてあるか ・保守作業を実施する際の手順について、医療機関等と合意を得ているか
2	1	1	12	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	運用状況及び管理状況について医療機関等に定期的に報告し、意見又は指摘を受けること、	経産省医療外部保存-GL	4.2	・運用状況及び管理状況について医療機関等に定期的に報告し、意見又は指摘を受けているか/運用規程が出来ているか
2	1	1	13	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	「システムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行うこと」を医療機関等に報告し、意見又は指摘を受けること	経産省医療外部保存-GL	4.2	・「現行の運用管理全般の再評価・再検討」結果を医療機関等に報告し、意見又は指摘を受けること/運用規程が出来ているか
2	1	1	14	2. 機能と運用　1）安全管理上の要求事項　①組織的安全性	必須	事故に対する緊急対応が完了した後で原因を確定するために、事故発生時の状況を保存あるいは記録する手順、対応過程で行われた作業を記録する手順等も策定しておくこと	経産省医療外部保存-GL	4.3	・事故に対する緊急対応が完了した後で原因を確定するために、事故発生時の状況を保存あるいは記録する手順、対応過程で行われた作業を記録する手順等が策定されているか

項番 大分類	中分類	小分類	要件	分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
2	1	2	1	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	必須	職員は情報処理事業者の専有する領域にて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。	経産省医療外部保存-GL	7.5.2	・運用の中で、職員は情報処理事業者の専有する領域にて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になっているか。
2	1	2	2	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	必須	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、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こと。	経産省医療外部保存-GL	7.5.2	・運用の中で、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、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ことになっているか。
2	1	2	3	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.2	・運用の中で、職員の業務に応じて執務室内に滞在できる時間を指定しているか。
2	1	2	4	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	必須	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認めないこと。	経産省医療外部保存-GL	7.5.2	・運用の中で、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認めないことになっているか。
2	1	2	5	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	必須	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。	経産省医療外部保存-GL	7.6.14	・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 を利用停止としているか
2	1	2	6	2. 機能と運用 1）安全管理上の要求事項 ②人的安全性	推奨	医療情報を操作する職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これは服務規程等に含めることもできる。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こと。	経産省医療外部保存-GL	7.7	・医療情報を操作する職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めているか ・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っているか
2	1	3	1	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.5	・情報の破棄手順について定めてあるか ・情報の破棄手順について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	3	2	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	・情報の破棄を実施した場合に、電磁記録媒体の消磁、物理的破壊等、情報の削除方法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こと。	総務省医療ASP-GL	3.2.5	・情報の廃棄手順として、実施内容を作成しているか ・実施内容に情報の削除方法について記録してあるか ・実施内容を記録した破棄記録等を医療機関に提出しているか
2	1	3	3	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.5	・情報の破棄手順について定めてあるか ・情報の破棄手順について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	3	4	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	情報の廃棄に関しては医療機関等からの依頼により行うこと	経産省医療外部保存-GL	6.1	・情報の廃棄に関しては医療機関等からの依頼により行うことに契約上および運用規約上なっているか
2	1	3	5	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	その際、処理が厳正に執り行われたことを医療機関等に対し証明すること	経産省医療外部保存-GL	6.1	・その際、処理が厳正に執り行われたことを医療機関等に対し証明するための手段を有しているか
2	1	3	6	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。 ・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こと。(3.6.7.9)	経産省医療外部保存-GL	7.8	・電子媒体の破棄に物理的破壊を用いているか ・破壊後に情報の読み取りができないことを確認しているか
2	1	3	7	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。 ・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、それらを消去すること。	経産省医療外部保存-GL	7.8	・廃棄前にハードディスクのパスワードを消去しているか
2	1	3	8	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	医療機関等と情報処理事業者間で廃棄処理手順について定め、合意しておく必要がある。	経産省医療外部保存-GL	8.2	・情報の廃棄処理手順について、文書で合意しているか
2	1	3	9	2. 機能と運用 1）安全管理上の要求事項 ③情報破棄	必須	・委託先に対して、情報の破棄を確実とする手段をとっていること	経産省医療外部保存-GL	8.2	・委託先に対しても、情報の破棄を確実としているか
2	1	4	1	2. 機能と運用 1）安全管理上の要求事項 ④情報の外部への持ち出し	必須	・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.6	・情報の持ち出しに関する運用管理規程等が定めてあるか ・情報の持ち出しに関する運用管理規程等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	4	2	2. 機能と運用 1）安全管理上の要求事項 ④情報の外部への持ち出し	必須	・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.7	・情報の持ち出しに関する運用管理規程等が定めてあるか ・情報の持ち出しに関する運用管理規程等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	4	3	2. 機能と運用 1）安全管理上の要求事項 ④情報の外部への持ち出し	必須	・自社において定めた機器･媒体の盗難、紛失が生じた際の対応についての手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.7	・機器・媒体等に対する規程が定めてあるか ・機器・媒体等の規定に盗難・紛失があった場合の対応について記載されているか ・盗難・紛失があった場合の対応について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	4	4	2. 機能と運用 1）安全管理上の要求事項 ④情報の外部への持ち出し	必須	・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.7	・情報の持ち出しに関する運用管理規程等が定めてあるか ・規定の中で、可搬媒体により外部に持ち出し、受託情報の処理を行わない旨が記載されているか ・情報の持ち出しに関する運用管理規程等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	4	5	2. 機能と運用 1）安全管理上の要求事項 ④情報の外部への持ち出し	必須	・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP-GL	3.2.7	・情報の持ち出しに関する運用管理規程等が定めてあるか ・規定の中で、可搬媒体により外部に持ち出し、受託情報の処理を行わない旨が記載されているか ・情報の持ち出しに関する運用管理規程等について、医療機関等の求めに応じ提出できるようにしているか
2	1	5	1	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理事業者の専有する領域に医療情報システムを設置する場合に、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、鍵管理が行われていること。 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こと。	経産省医療外部保存-GL	7.5.1	・運用の中で医療情報が保存されるサーバラックの施錠管理、鍵管理を行っているか。
2	1	5	2	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理事業者の専有する領域に医療情報システムを設置する場合に、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。 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こと。	経産省医療外部保存-GL	7.5.1	・部屋を区切る壁面、天井、床部分に十分な厚みがあるか。 ・運用の中で、監視カメラでの常時監視および画像記録の保存、不正に取り付けられた装置の定期的な検出を行っているか。
2	1	5	3	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理事業者の専有する領域に医療情報システムを設置する場合に、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こと。 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こと。	経産省医療外部保存-GL	7.5.1	・監視カメラ等の侵入検知装置を導入しているか。
2	1	5	4	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理事業者の専有する領域に医療情報システムを設置する場合に、自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。 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こと。	経産省医療外部保存-GL	7.5.1	・建物の防災対策を適切に実施しているか。
2	1	5	5	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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、有人の受付又は機械式の認証装置を設置して、入退館及び入退室者の確実な認証を行うこと。	経産省医療外部保存-GL	7.5.2	・医療情報を保管する部屋に有人の受付又は機械式の認証装置を設置しているか。 ・運用の中で、入退館及び入退室者の確実な認証を行っているか。
2	1	5	6	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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、生体認証複数要素を利用した認証装置を利用すること。	経産省医療外部保存-GL	7.5.2	・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している場合には、生体認証複数要素を利用した認証装置を利用しているか。
2	1	5	7	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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（履歴の保全については「7.6.12ログの取得及び監査」を参照）。	経産省医療外部保存-GL	7.5.2	・運用の中で、定期的に履歴を検証して、不審な活動がないことを確認しているか。
2	1	5	8	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理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、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こと。	経産省医療外部保存-GL	7.5.2	・運用の中で、情報処理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ているか。
2	1	5	9	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合、および、外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合、医療情報システムの設置されるサーバラックには施錠を行い、定められた職員以外が鍵を扱わないよう、確実な鍵管理を行うこと。	経産省医療外部保存-GL	7.5.2	・運用の中で、医療情報システムの設置されるサーバラックには施錠を行い、定められた職員以外が鍵を扱わないよう、確実な鍵管理を行っているか。

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	5	10	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合、および、外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合、情報処理事業者が医療情報システム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こと。	経産省医療外部保存-GL	7.5.2	・運用の中で、情報処理事業者が医療情報システム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しているか。
2	1	5	11	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合、および、外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合、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、医療情報に影響を与えないことを確認すること。	経産省医療外部保存-GL	7.5.2	・運用の中で、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、医療情報に影響を与えないことを確認することになっているか。
2	1	5	12	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合、および、外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合、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と。	経産省医療外部保存-GL	7.5.2	・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とになっているか。
2	1	5	13	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。	経産省医療外部保存-GL	7.5.3	・運用の中で、不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持しているか。
2	1	5	14	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。	経産省医療外部保存-GL	7.5.3	運用の中で、医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないことになっているか。
2	1	5	15	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	医療情報等が表示される端末画面等を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。	経産省医療外部保存-GL	7.5.3	・医療情報等が表示される端末画面等を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っているか。 ・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っているか。
2	1	5	16	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.3	・運用の中で、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、端末上に保存することを禁止しているか。
2	1	5	17	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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。	経産省医療外部保存-GL	7.5.3	・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されているか。
2	1	5	18	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	医療情報システムを配置する室内での喫煙、飲食を禁止すること。	経産省医療外部保存-GL	7.5.3	・運用の中で、医療情報システムを配置する室内での喫煙、飲食を禁止しているか。
2	1	5	19	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	医療情報システム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こと。	経産省医療外部保存-GL	7.5.3	・医療情報システム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しているか。
2	1	5	20	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	それぞれの装置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。	経産省医療外部保存-GL	7.5.3	・運用の中で、それぞれの装置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っているか。
2	1	5	21	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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情報処理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こと。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こと。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こと。	経産省医療外部保存-GL	7.5.3	・運用の中で、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情報処理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しているか。 ・運用の中で、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ことになっているか。 ・運用の中で、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ことになっているか。
2	1	5	22	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	・震災時に転倒することが無いよう確実に設置すること。	経産省医療外部保存-GL	7.5.3	・震災時に転倒することが無いよう確実に設置されているか。
2	1	5	23	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	・熱による障害を防ぐため十分な換気装置を設けること。	経産省医療外部保存-GL	7.5.3	・熱による障害を防ぐため十分な換気装置を設けられているか。
2	1	5	24	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	・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こと。	経産省医療外部保存-GL	7.5.3	・扉には十分な安全強度を持つ物理的施錠装置を設けているか。 ・運用の中で、鍵管理について十分に配慮しているか。
2	1	5	25	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「7.6.14作業者アクセス及び作業者ID の管理」に従うこと。	経産省医療外部保存-GL	7.5.3	・運用の中で、起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定しているか。 ・設定されるパスワードの品質、管理については「7.6.14作業者アクセス及び作業者ID の管理」に従っているか。
2	1	5	26	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.3	・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しているか。
2	1	5	27	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.3	・運用の中で、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しているか。
2	1	5	28	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	推奨	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。	経産省医療外部保存-GL	7.5.3	・情報伝送に用いるケーブル類の取り扱い方法について十分に配慮してあるか
2	1	5	29	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に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。	経産省医療外部保存-GL	7.5.4	・運用の中で、ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に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になっているか。
2	1	5	30	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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、それらを消去すること。	経産省医療外部保存-GL	7.5.4	・運用の中で、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、それらを消去することになっているか。
2	1	5	31	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.4	・運用の中で、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ことになっているか。
2	1	5	32	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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、情報の読み出しが不可能であることを確認すること。	経産省医療外部保存-GL	7.5.4	・運用の中で、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、情報の読み出しが不可能であることを確認することになっているか。
2	1	5	33	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	推奨	物理的な破壊措置については情報処理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。	経産省医療外部保存-GL	7.5.4	・外部の事業者に破棄を依頼する場合には、手順書があるか。
2	1	5	34	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。	経産省医療外部保存-GL	7.5.5	・運用の中で、情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定しているか。
2	1	5	35	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	必須	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こと。	経産省医療外部保存-GL	7.5.5	・運用の中で、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しているか。
2	1	5	36	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	推奨	情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。 ・ 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。	経産省医療外部保存-GL	7.5.5	・運用の中で、機器持ち出しの手順を策定しているか。
2	1	5	37	2. 機能と運用 1）安全管理上の要求事項 ⑤物理的安全性	推奨	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（不正な改ざん等）、等。	経産省医療外部保存-GL	7.5.5	・運用の中で、機器返却の手順を策定しているか。

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	1	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。	総務省医療ASP-GL	3.2.6	・ASP・SaaSサービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する適切な間隔（パターンファイルの更新：24時間、24時間）で対策を講じているか。
2	1	6	2	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・医療機関等がASP・SaaS を利用するネットワークにつき、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置についての事業者の役割の範囲について医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・ASP・SaaS を利用するネットワークについて、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・ASP・SaaS を利用するネットワークの責任範囲に事業者が含まれる場合、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置等、必要なセキュリティ対策を施しているか
2	1	6	3	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・ASP・SaaS を利用するネットワークで用いられる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、医療機関等から事業者までの確認を行うこと（但し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本項の対応を適用せず、別途なりすましを防止する策を講じること）。	総務省医療ASP-GL	3.2.9	・ASP・SaaS を利用するネットワークにおいて、相手確認を行っているか ・相手確認を行う際に、医療機関等から事業者までのネットワークで、機器や機能等、確認可能な単位で相手確認を行っているか ・（事業者が保守業務を再委託している場合、相手確認だけでなく、なりすましを防止する策がとられているか）
2	1	6	4	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・厚生労働省ガイドライン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を確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・通信方式認証手段について、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・医療機関等が採用する通信方式認証手段の責任範囲に事業者が含まれる場合、厚生労働省のガイドラインに基づいているかの確認を行っているか
2	1	6	5	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・ASP・SaaS を利用するネットワークで用いられるルータ等のネットワーク機器が厚生労働省ガイドラインで求める安全性が確認されているものであること、ASP・SaaS を利用する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、これを経由して医療機関等の施設間を結ぶ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等に関して、事業者の役割、範囲を医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・ネットワーク機器について、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・ネットワーク機器の責任範囲に事業者が含まれる場合、厚生労働省ガイドラインで求める安全性が確認されているもので構成しているか ・ネットワーク機器の責任範囲に事業者が含まれる場合、ASP・SaaS を利用する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で、他の施設に対するVPNの通信ができないように経路設定されているか
2	1	6	6	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・ASP・SaaS において送受信されるデータに対して、電子政府推奨の暗号を用いた暗号化等によるセキュリティ対策を講じること。	総務省医療ASP-GL	3.2.9	・送受信データに対して、電子政府推奨の暗号を用いた暗号化等によるセキュリティ対策を講じているか
2	1	6	7	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	・暗号化によるセキュリティ対策が、医療機関等が求める水準を満たすものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・暗号化によるセキュリティ対策について、規定を定めているか ・暗号化によるセキュリティ対策について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
2	1	6	8	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	・医療機関等の利用者が、医療機関の外部からASP・SaaS を利用する場合に、事業者は、医療機関の利用者が用いる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等の技術導入に関する事業者の役割、範囲等を医療機関等と合意すること。	総務省医療ASP-GL	3.2.9	・ASP・SaaSに関する技術導入の責任範囲を明確にして、医療機関等と合意を得ているか ・情報システムの責任範囲に事業者が含まれる場合、医療機関の利用者が用いるPC の作業環境の安全管理を実施しているか
2	1	6	9	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	サーバに管理者権限でアクセスするための管理端末に関して、データセンター内に端末室があればデータセンター内のLANを経由してサーバと端末室の端末を接続する、端末室が無い場合にはデータセンターの外部にある情報処理事業者自身の施設内に安全を確保した端末室を設けて、IP-VPN あるいはIPsecとIKEを併用したインターネットVPN を経由してサーバと端末を接続するといった方法が考えられる。。 上記いずれの場合も、ネットワークの安全管理を厳密に行うとともに、端末へのアクセス、ログオンアカウント管理を厳密に行うこと。	経産省医療外部保存-GL	3	・サーバに管理者権限でアクセスするための管理端末に関して、ネットワークの安全管理を厳密に行うとともに、端末へのアクセス、ログオンアカウント管理を厳密に行っているか。
2	1	6	10	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	医療機関等と情報処理事業者間をネットワークで接続して情報交換を行う場合には、専用線あるいはVPN といった第三者による傍受のリスクが低いネットワークを利用すること	経産省医療外部保存-GL	3	・医療機関等と情報処理事業者間をネットワークで接続して情報交換を行う場合には、専用線あるいはVPN といった第三者による傍受のリスクが低いネットワークを利用しているか
2	1	6	11	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	医用画像（レントゲンデータ等）等、転送する情報量が相当に大きくなることもあることから、必要なネットワーク容量の見積もりを適切に行い、十分なネットワーク容量を確保すること。	経産省医療外部保存-GL	3	・医用画像（レントゲンデータ等）等、転送する情報量が相当に大きくなることを配慮して、必要なネットワーク容量の見積もりを適切に行い、十分なネットワーク容量を確保しているか。
2	1	6	12	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	長期保存を目的として、これらの電子媒体を利用する場合には、製造元の保存仕様に準拠した保管を行い、見読性、保存性を損なわないように配慮すること。また電子媒体の劣化特性を考慮して、劣化が起こる前に新たな電子媒体に複写すること。	経産省医療外部保存-GL	3.1	・長期保存を目的として、これらの電子媒体を利用する場合には、製造元の保存仕様に準拠した保管を行い、見読性、保存性を損なわないように配慮すること。また電子媒体の劣化特性を考慮して、劣化が起こる前に新たな電子媒体に複写しているか。
2	1	6	13	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	漏洩等の大きなリスクも考えられることから、原則として医療情報システムでは外部デバイスとして小型半導体メモリの使用を行うことができないよう配慮することが望ましい。	経産省医療外部保存-GL	3.1	・原則として医療情報システムでは外部デバイスとして小型半導体メモリの使用を行うことができないよう配慮しているか。
2	1	6	14	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	必要により小型半導体メモリを使用する場合、使用前には不要なデータが書き込まれていないことを確認し、使用後には電子媒体上の全てのデータを削除すること。また、利用時間及び電子媒体の移動範囲を最小にするなどの管理を行うこと。	経産省医療外部保存-GL	3.1	・必要により小型半導体メモリを使用する場合は、使用前には不要なデータが書き込まれていないことを確認し、使用後には電子媒体上の全てのデータを削除し、また、利用時間及び電子媒体の移動範囲を最小にするなどの管理を行っているか。
2	1	6	15	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	電子ファイルが転送されてきたことを検知した際は悪意のあるコードが混入していないことを検証する。さらに、電子署名検証等の真正性検査を実施する（異常を検出した場合には即座に医療事業者に通知すること）。	経産省医療外部保存-GL	3.4	・電子ファイルが転送されてきたことを検知した際は悪意のあるコードが混入していないことを検証し、電子署名検証等の真正性検査を実施しているか（また、異常を検出した場合には即座に医療事業者に通知しているか、あるいは通知する体制となっているか）。
2	1	6	16	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	医療機関等から電子ファイルを転送するフォルダは一時フォルダとし、悪意コード混入検証並びに真正性検査後に電子ファイルを保管用フォルダに移動する（一時フォルダ内の電子ファイルは削除する）。	経産省医療外部保存-GL	3.4	・医療機関等から電子ファイルを転送するフォルダは一時フォルダとし、悪意コード混入検証並びに真正性検査後に電子ファイルを保管用フォルダに移動しているか（さらに、移動後に一時フォルダ内の電子ファイルを削除しているか）。
2	1	6	17	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	医療事業者からの電子ファイル転送を常時監視するようシステムを整備すること	経産省医療外部保存-GL	3.4	・医療事業者からの電子ファイル転送を常時監視するようシステムを整備しているか
2	1	6	18	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	複写した電子ファイルの受付情報をまとめて管理台帳に記載する。	経産省医療外部保存-GL	3.4	・複写した電子ファイルの受付情報をまとめて管理台帳に記載しているか。
2	1	6	19	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	医療機関等に受付情報を通知する。	経産省医療外部保存-GL	3.4	・医療機関等に受付情報を通知しているか。
2	1	6	20	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	ファイル転送についてインターネット標準技術であるFTPプロトコルを用いる場合においては専用回線あるいはVPN等を利用して少なくともネットワークレイヤでの安全対策を施し、パスワード及びデータ漏洩のリスクを低減すること	経産省医療外部保存-GL	3.4	・ファイル転送についてインターネット標準技術であるFTPプロトコルを用いる場合においては専用回線あるいはVPN等を利用して少なくともネットワークレイヤでの安全対策を施し、パスワード及びデータ漏洩のリスクを低減しているか
2	1	6	21	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	ネットワークレイヤでの安全対策に加えて、アプリケーションレイヤにおいてもSFTP、SCP等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用するといった、多重防御を実装することが望ましい。	経産省医療外部保存-GL	3.4	・ネットワークレイヤでの安全対策に加えて、アプリケーションレイヤにおいてもSFTP、SCP等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用するといった、多重防御を実装しているか。
2	1	6	22	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	FTP を採用する場合にはFTP アクセスログを定期的に検証し、不必要なFTP アクセスが行われていないことを確認するなどの対策を行うこと。	経産省医療外部保存-GL	3.4	・FTP を採用する場合にはFTP アクセスログを定期的に検証し、不必要なFTP アクセスが行われていないことを確認するなどの対策を行っているか。
2	1	6	23	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	医療機関等への通知メッセージを実装する場合、メッセージ中に機微な情報が含まれる場合には、医療機関等と受託情報処理事業者を結ぶ安全なネットワーク上で転送することが原則である.	経産省医療外部保存-GL	3.4	・医療機関等への通知メッセージを実装する場合、メッセージ中に機微な情報が含まれる場合には、医療機関等と受託情報処理事業者を結ぶ安全なネットワーク上で転送しているか
2	1	6	24	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	保護されていないインターネット経由で医療機関等への通知を転送する場合には、暗号技術を用いて、メッセージの機密性、完全性を確保すること。	経産省医療外部保存-GL	3.4	・保護されていないインターネット経由で医療機関等への通知を転送する場合には、暗号技術を用いて、メッセージの機密性、完全性を確保しているか
2	1	6	25	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	管理者機能を分割した上でおのおのに別の特権ID を割り当て、それぞれの特権ID の権限を必要最小限とする最小特権の原則を実装することが望ましい。	経産省医療外部保存-GL	3.5.1	・管理者機能を分割した上でおのおのに別の特権ID を割り当て、それぞれの特権ID の権限を必要最小限とする最小特権の原則を実装しているか
2	1	6	26	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	「虚偽入力、書き換え、消去、及び混同が防止されていること」に関して、情報の受入れ時に正しい情報であることを確認すること。 ・医療機関等側で情報を生成した際に、例えば電子署名を付与するなど、真正性を担保しておくこと	経産省医療外部保存-GL	6.1	・「虚偽入力、書き換え、消去、及び混同が防止されていること」に関して、情報の受入れ時に正しい情報であることを確認する機能があるか。
2	1	6	27	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	情報が通信路上で真正性にかかわる事項が変更されていないことを確認できること。 ・情報を受入れた情報処理事業者は、付与された電子署名を検証するなど、真正性を検証することで情報が通信路上で変更されていないことを確認できること	経産省医療外部保存-GL	6.1	・情報が通信路上で真正性にかかわる事項が変更されていないことを確認できる機能があるか
2	1	6	28	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	電子媒体について、認可されていない着脱、持出が行われていないことを保証するため、定期的に検査を行うこと。	経産省医療外部保存-GL	6.1	・電子媒体について、認可されていない着脱、持出が行われていないことを保証するため、定期的に検査を行っているか。
2	1	6	29	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	電子媒体上の情報に対して、認可されていない書き込み、削除が行われないように、改ざんの検出を行うこと ・例えばアカウント管理、アクセス権限管理を行い、定期的に電子署名を検証する等の作業	経産省医療外部保存-GL	6.1	・電子媒体上の情報に対して、認可されていない書き込み、削除が行われないように、改ざんの検出を行っているか／行う為の機能があるか／規定が出来ているか／実施されているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	30	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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が行われていること	経産省医療外部保存-GL	7.6.1	・運用の中で保守の手順が明確に定められており、その保守手順の影響評価が行われており、内容が妥当か。
2	1	6	31	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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検討すること。	経産省医療外部保存-GL	7.6.1	・運用の中での変更におけるリスク評価が行われており、内容が妥当か。
2	1	6	32	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.1	・利用者との契約の中でデータ形式、プロトコル変更の際に以前のものの利用もサポートすることが明記されているか。
2	1	6	33	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.1	・運用の中で保守の手順が明確に定められているか。 ・保守手順の中で、停止時間が最小限に留めるようになっているか。
2	1	6	34	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。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。	経産省医療外部保存-GL	7.6.1	・運用の中で保守の手順が明確に定められているか。 ・保守手順の中で、保守作業について事前に医療機関等に通知し承認を得ることになっているか。 ・上記の内容が保守契約書に明記されているか。
2	1	6	35	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.1	・運用の中で定期的な整合性検査を行うことが定められているか。 ・整合性検査結果報告書が存在し、内容が妥当か。
2	1	6	36	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	医療情報システム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こと。	経産省医療外部保存-GL	7.6.1	・運用の中で技術的な脆弱性を管理することが定められているか。 ・脆弱性管理台帳が存在し、内容が妥当か。
2	1	6	37	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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）を決定すること。	経産省医療外部保存-GL	7.6.1	・運用の中で技術的な脆弱性を管理することが定められているか。 ・脆弱性管理台帳が存在し、内容が妥当か。 ・脆弱性が特定された場合のリスク評価が行われ、記録が残っているか。 ・結果に従い行われた処置について脆弱性管理台帳に記載されているか
2	1	6	38	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	修正パッチの適用前に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。	経産省医療外部保存-GL	7.6.1	・運用の中でパッチの改ざん及び有効性の検証を行うことが定められているか。 ・パッチの改ざん及び有効性検証の報告書が存在し、内容が妥当か。
2	1	6	39	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	保守作業を外部事業者に再委託する場合には、経産省GL「7.6.1 情報処理装置及びソフトウェアの保守」の要件を満たしていることを確認して選定し、経産省GL「7.6.5 第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。	経産省医療外部保存-GL	7.6.1	・保守作業を再委託する場合は、再委託契約の中で、経産省GL「7.6.1 情報処理装置及びソフトウェアの保守」の要件を満たしていることを確認し再委託契約を結んでいるか。 ・再委託した外部事業者について、医療機関等に報告、合意を得た再委託報告書が存在かするか。
2	1	6	40	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.1	・変更するにあたっての手順書が作成されているか。
2	1	6	41	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	最新の脅威についての情報収集に努め、導入している悪意のあるコード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こと。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	経産省医療外部保存-GL	7.6.3	・運用手順書の中で、最新の脅威についての情報収集に努め、導入している悪意のあるコード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ことが定められているか。 ・あるいは、導入している悪意のあるコード対策ソフトウェアのリスク評価の結果報告書が存在し、内容が妥当か。
2	1	6	42	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ・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	経産省医療外部保存-GL	7.6.3	・悪意のあるコード対策プログラムにおいて左記の要件の設定が行われていることが設定記録書に記録されているか。 ・あるいは、導入している悪意のあるコード対策ソフトウェアのリスク評価の報告書が存在し、内容が妥当か。
2	1	6	43	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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が行われていること	経産省医療外部保存-GL	7.6.3	・運用手順書の中で、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等の場合、利用者に警告を表示する、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が定められてるか。 ・あるいは、導入している悪意のあるコード対策ソフトウェアのリスク評価の報告書が存在し、内容が妥当か。
2	1	6	44	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと	経産省医療外部保存-GL	7.6.4	・運用手順書の中で、ウェブブラウザの接続するサーバを限定するように定められているか。
2	1	6	45	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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のみを認可する）。	経産省医療外部保存-GL	7.6.4	・運用手順書の中で、ウェブブラウザの設定で認可していないサイトからプログラムコードをダウンロードおよび実行することを行わないように定められているか。 ・ウェブブラウザ設定記録書に上記の設定が記録されているか。
2	1	6	46	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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「7.6.3 悪意のあるコードに対する管理策」に即して検査されること。	経産省医療外部保存-GL	7.6.4	・運用手順書の中で、ウェブブラウザで認可したサイトからプログラムコードをダウンロードした場合、そのコードの検査が定められているか。 ・検査結果報告書に上記の検査結果が記録されており、内容に問題がないか。
2	1	6	47	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.4	・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よう定められているか
2	1	6	48	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。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こと。	経産省医療外部保存-GL	7.6.6	（ハウジング構成の場合） ・ネットワークインタフェースに対するアクセス制御に関するセキュリティポリシーが作成され、文書化されているか。 ・各ネットワークインタフェースが、セキュリティポリシーに従ってアクセス制御されているか。 （ホスティング構成の場合） ・情報処理装置(サーバ)に対するアクセス制御に関するセキュリティポリシーが作成され、文書化されているか。 ・各サーバが、セキュリティポリシーに従ってアクセス制御されているか。
2	1	6	49	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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）。	経産省医療外部保存-GL	7.6.6	・通過トラフィックのIPアドレスを検証する仕組みがあるか。 ・その仕組みを使って不正なトラフィックがフィルタリングされるように設定されているか。
2	1	6	50	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.6	・どのようなネットワーク機器（メーカー、機種名、バージョン等）を使っているか。
2	1	6	51	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.6	・ネットワーク環境で使用するポートが識別されているか。 ・使用しないポートが閉じられているか。
2	1	6	52	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。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、同様の制御を行うこと。	経産省医療外部保存-GL	7.6.6	・外部とのネットワーク境界に何らかの不正トラフィックに対抗する仕組みが導入されているか。
2	1	6	53	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.6	・セキュリティパッチ等の適用に関する運用が組織のルールとして制定されているか。 ・そのルール通り運用が行われ、実際に適用されているか。
2	1	6	54	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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にしていること。	経産省医療外部保存-GL	7.6.6	・情報システムに対する攻撃を検知した場合に管理者に通知する仕組みが構築されているか。
2	1	6	55	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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まれていること。	経産省医療外部保存-GL	7.6.6	・侵入検知の記録をとることが組織の運用ルールとして制定されているか。 ・そのルールには不正アクセス等の事後処理に関する項目が定められているか。 ・そのルールに従った記録が取られているか。

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	56	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	医療情報システムにおいて、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こと。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こと。 ・ 外部からの医療情報システムの稼働監視・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）	経産省医療外部保存-GL	7.6.6	・どのような接続サービスを提供しているか。 ・提供しているサービスが、要件にあるものに含まれているか。 ・含まれないものがある場合に、医療機関等の合意を得ているか。
2	1	6	57	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	医療情報システム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こと。	経産省医療外部保存-GL	7.6.6	・医療情報システム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）に適切な上限が設けてあるか。
2	1	6	58	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。	経産省医療外部保存-GL	7.6.6	・ネットワーク接続のログ（認証ログ及び接続ログ）が記録されるか。
2	1	6	59	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。	経産省医療外部保存-GL	7.6.6	・ネットワークの接続ログを定期的に検証することが運用ルールとして定められているか。 ・その実施記録が取られているか。
2	1	6	60	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LANを利用しないこと。	経産省医療外部保存-GL	7.6.6	・医療情報を保存するシステムで無線ネットワークを利用していないか。
2	1	6	61	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	VPN接続を行う場合には以下の事項に従うこと。 ・ 接続時にVPN装置間で相互に認証を行うこと。 ・ 傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11暗号による管理策」に従い、適切な暗号技術を利用すること。 ・ 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。 ・ 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。	経産省医療外部保存-GL	7.6.6	（VPN接続を行っている場合） ・要件に示される内容が運用ルールとして定められているか。 ・そのルールに従った運用が行われているか。
2	1	6	62	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	医療情報システムから、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。	経産省医療外部保存-GL	7.6.6	・ネットワーク境界において不正トラフィック監視機能があるか。
2	1	6	63	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.6	・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できるか。
2	1	6	64	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないことが望ましい。	経産省医療外部保存-GL	7.6.6	・無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用することが無いか。
2	1	6	65	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。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(9)に示す方式にて確実に廃棄処分すること。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	66	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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と。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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	67	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	電子媒体は台帳を作成して管理すること。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こと。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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	68	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	69	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	70	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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、他媒体に複写すること。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	71	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	情報を保管するためにハードディスク装置を用いる場合には、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策を取ること。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	72	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	73	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	74	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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情報処理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。	経産省医療外部保存-GL	7.6.7	・電子媒体破棄のルールが明文化されているか。 ・外部専門業者に委託するルールが有るか。
2	1	6	75	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	医療情報システム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ことが望ましい。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。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールにデバイスドライバに関する規定があるか。
2	1	6	76	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.7	・電子媒体の取り扱いに関するルールにデバイスドライバに関する規定があるか。
2	1	6	77	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	次の情報交換方法について予め合意しておくこと。 ・ 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	経産省医療外部保存-GL	7.6.8	・情報交換に関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	78	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。 ・ 発送者、受領者を識別し記録すること。 ・ 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。 ・ 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）。 ・ 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。	経産省医療外部保存-GL	7.6.8	・情報交換に関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	79	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。 ・ 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。 ・ 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こと。 ・ 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こと。 ・ 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こと。 ・ 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。 ・ 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こと。	経産省医療外部保存-GL	7.6.8	・情報交換に関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	80	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。 ・ 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こと。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こと。 ・ 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対策を講じること。 ・ 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こと。	経産省医療外部保存-GL	7.6.8	・情報交換に関するルールが制定され、明文化されているか。 ・そのルールに要件にある内容が盛り込まれているか。 ・そのルールに従った運用が行われているか。
2	1	6	81	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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、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で外部ファイルに出力ができること。見読性が確保される形式としては、PDF41、JPEG42及びPNG42等のフォーマットが想定される。	経産省医療外部保存-GL	7.6.9	・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、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で外部ファイルに出力ができるか。（見読性が確保される形式としては、PDF41、JPEG42及びPNG43等のフォーマットが想定される。）
2	1	6	82	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。	経産省医療外部保存-GL	7.6.10	・アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存しているか。
2	1	6	83	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.10	・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っているか。
2	1	6	84	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	アプリケーションによる情報操作については、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、編集、削除等を防止すること。	経産省医療外部保存-GL	7.6.10	・アプリケーションによる情報操作については、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、編集、削除等を防止しているか。
2	1	6	85	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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が望ましい。	経産省医療外部保存-GL	7.6.11	・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、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か。
2	1	6	86	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.11	・暗号アルゴリズムは電子政府推奨暗号リスト等を用い、十分な安全性を有するものを使用しているか。
2	1	6	87	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.11	・暗号鍵が漏洩した場合に備えた対応策を策定しているか。
2	1	6	88	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.11	・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を利用しているか。
2	1	6	89	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.11	・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しているか。
2	1	6	90	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.11	・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、真正性を検証しているか。
2	1	6	91	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.11	・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しているか。
2	1	6	92	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.11	・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しているか。
2	1	6	93	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.11	・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っているか。
2	1	6	94	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	・ 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こと。	経産省医療外部保存-GL	7.6.12	・ログサーバの記憶容量を常時監視しているか ・記憶容量の状況に応じ電子媒体への書き出し、容量の増強等の対策をとっているか
2	1	6	95	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	・ ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。	経産省医療外部保存-GL	7.6.12	・ ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施しているか
2	1	6	96	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	医療情報システム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。	経産省医療外部保存-GL	7.6.12	・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いるかを定期的に検証しているか
2	1	6	97	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。 ・ 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） ・ 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） ・ 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） ・ 修正パッチの適用作業（作業者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）	経産省医療外部保存-GL	7.6.12	・左記のような項目で監査ログを作成しているか
2	1	6	98	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	監査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、作業者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。	経産省医療外部保存-GL	7.6.12	・監査ログの検証のため、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しているか
2	1	6	99	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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ことが望ましい。	経産省医療外部保存-GL	7.6.12	・専用のログサーバにログデータを集約して分析管理しているか
2	1	6	100	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.13	・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っているか
2	1	6	101	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.13	・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しているか
2	1	6	102	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	作業者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権限管理を行うことが望ましい。	経産省医療外部保存-GL	7.6.13	・作業者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権限管理を行っているか
2	1	6	103	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.13	・定められたアクセス制御方針が、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しているか
2	1	6	104	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	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規定すること。	経産省医療外部保存-GL	7.6.13	・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規定しているか
2	1	6	105	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	作業者は情報処理装置上においてユニークな作業者ID により識別されること。	経産省医療外部保存-GL	7.6.14	・作業者に対してユニークなIDを発行して、1対1で対応をとっているか
2	1	6	106	2. 機能と運用　1）安全管理上の要求事項　⑥技術的安全性	必須	作業者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こと。	経産省医療外部保存-GL	7.6.14	・既存IDとの重複を排除する仕組みが導入されているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	107	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	複数作業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、作業者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こと。	経産省医療外部保存-GL	7.6.14	・複数作業者で共用するためのグループID の利用を行っていないか ・やむなくグループIDを利用する場合、作業者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し、グループIDを使用している人が特定できるようにしているか
2	1	6	108	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	作業者ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。	経産省医療外部保存-GL	7.6.14	・作業者IDの発行を最小限に留めているか
2	1	6	109	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	監視ログの監査時に作業者を確実に特定するため、作業者ID は過去に使われたものを再利用しないこと。	経産省医療外部保存-GL	7.6.14	・作業者ID は過去に使われたものを再利用していないか
2	1	6	110	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.14	・不要な作業者ID が残っていないことを定期的に確認しているか
2	1	6	111	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	アクセスを許可された作業者IDの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。	経産省医療外部保存-GL	7.6.14	・アクセスを許可された作業者IDの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）を定期的に確認しているか
2	1	6	112	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	作業者がシステムログオン用の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、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が望ましい。	経産省医療外部保存-GL	7.6.14	・作業者がシステムログオン用の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、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をしているか
2	1	6	113	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	パスワードの品質基準としては、パスワードを十分に長くすること（8 文字以上等）、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。	経産省医療外部保存-GL	7.6.14	・パスワードの品質基準を定めているか ・パスワードの長さを十分に長くしているか ・パスワードにアルファベット及び数字並びに記号を一つ以上含むように設定されているか
2	1	6	114	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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、作業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こと。	経産省医療外部保存-GL	7.6.14	・作業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っているか
2	1	6	115	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	特権ID の発行は必要な最小限のものに留めること。	経産省医療外部保存-GL	7.6.14	・特権ID の発行は必要な最小限のものに留めているか
2	1	6	116	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	特権使用者に昇格可能な作業者ID を制限すること。	経産省医療外部保存-GL	7.6.14	・特権使用者に昇格可能な作業者ID を制限しているか
2	1	6	117	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	特権の使用時には作業実施内容を記録すること。	経産省医療外部保存-GL	7.6.14	・特権の使用時には作業実施内容を記録しているか
2	1	6	118	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	管理端末以外からの特権ID による直接ログインを禁止すること。	経産省医療外部保存-GL	7.6.14	・管理端末以外からの特権ID による直接ログインを禁止いるか
2	1	6	119	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.14	・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しているか
2	1	6	120	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	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が望ましい。	経産省医療外部保存-GL	7.6.14	・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ているか ・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しているか
2	1	6	121	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	情報処理装置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、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。	経産省医療外部保存-GL	7.6.14	・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っているか
2	1	6	122	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	システムログオン用の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こと。	経産省医療外部保存-GL	7.6.14	・パスワードを容易に復元できない形で情報を保管しているか
2	1	6	123	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	システムログオン用のパスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。	経産省医療外部保存-GL	7.6.14	・パスワードには有効期限の設定を行い、定期的な変更を作業者に強制しているか
2	1	6	124	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	システムログオン用のパスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。	経産省医療外部保存-GL	7.6.14	・パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにしているか
2	1	6	125	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.6.14	・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しているか
2	1	6	126	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	パスワード発行時には、乱数から生成した仮のシステムログオン用の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こと。	経産省医療外部保存-GL	7.6.14	・パスワード盗難リスクに対する対策を実施しているか
2	1	6	127	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	パスワードの満たすべき品質の基準を策定し、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こと。	経産省医療外部保存-GL	7.6.14	・パスワードの満たすべき品質の基準を策定しているか ・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しているか
2	1	6	128	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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作業者に徹底すること。	経産省医療外部保存-GL	7.6.14	・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させていないか
2	1	6	129	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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こと。また、一般の作業者による閲覧を制限すること。	経産省医療外部保存-GL	7.6.14	・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の保護策を採用しているか ・一般の作業者による閲覧を制限しているか
2	1	6	130	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。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を導入すること。	経産省医療外部保存-GL	7.6.14	・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しているか ・続け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し、失敗した場合は警告メッセージを管理者に送出する仕組みであるか
2	1	6	131	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業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。	経産省医療外部保存-GL	7.6.14	・作業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ているか ・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しているか
2	1	6	132	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	不正なアカウントの利用を防ぐため、作業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。	経産省医療外部保存-GL	7.6.14	・作業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、時間帯に制限しているか
2	1	6	133	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	認可されていない作業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」と表示すると作業者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が望ましい。	経産省医療外部保存-GL	7.6.14	・認証が失敗した場合、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ているか
2	1	6	134	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	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。	経産省医療外部保存-GL	7.6.14	・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しているか
2	1	6	135	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	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）、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。	経産省医療外部保存-GL	7.6.14	・ログオン時に利用する認証要素を、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）等を組み合わせているか
2	1	6	136	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.6.15	・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いるか ・上記の事項を明文化したルールとして策定しているか
2	1	6	137	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.9	・アップグレードなど、医療情報システムに修正を加える場合、事前に影響を評価しているか
2	1	6	138	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	推奨	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、外形的なぜい弱性検査を行う。	経産省医療外部保存-GL	7.9	・ソフトウェアの脆弱性検出をソースコードレベルで実施しているか ・最低でも外形的な脆弱性検査を行っているか
2	1	6	139	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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職員を含む）、情報処理装置等について識別すること。	経産省医療外部保存-GL	7.10.1	・業務プロセスや情報資産について識別しているか
2	1	6	140	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	業務プロセス間の相互関係を評価すること。	経産省医療外部保存-GL	7.10.1	・業務プロセス間の相互関係を評価しているか
2	1	6	141	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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こと。	経産省医療外部保存-GL	7.10.1	・事業継続時の業務プロセスの優先順位を策定しているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	1	6	142	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.10.1	・ハードウェア及びソフトウェアによる障害が業務プロセスに与える影響について識別しているか
2	1	6	143	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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。	経産省医療外部保存-GL	7.10.1	・障害による、他のハードウェア及びソフトウェアへの相互作用について評価し、影響度が大きいシステムに対して識別しているか
2	1	6	144	2. 機能と運用 1）安全管理上の要求事項 ⑥技術的安全性	必須	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、大きすぎるものがあれば、影響度を低減する方策及びその可能性について検討すること。	経産省医療外部保存-GL	7.10.1	・影響度が大きいハードウェア及びソフトウェアについて、影響度を低減する方策及びその可能性について検討した結果が文章に反映されているか
2	1	7	1	2. 機能と運用 1）安全管理上の要求事項 ⑦電子署名	必須	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。	総務省医療ASP-GL	3.2.10	・電子署名の方式について医療機関等と合意を得ているか ・情報に対して、法令によって記名・押印を電子署名で行うものとされたものを抽出できているか
2	1	7	2	2. 機能と運用 1）安全管理上の要求事項 ⑦電子署名	必須	・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子証明書、もしくは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によるものであることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP-GL	3.2.10	・合意した電子署名の方式が、保健医療福祉分野PKI認証局の発行する電子証明書、もしくは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によるものであることを確認しているか ・合意した電子署名の方式について、明文化して資料を提出できるようにしてあるか
2	1	7	3	2. 機能と運用 1）安全管理上の要求事項 ⑦電子署名	必須	情報の預け主である医療機関等の要請により情報を提供する際にも電子署名等を検証して改ざんの検出を行い、正しく元の情報を提供すること。	経産省医療外部保存-GL	6.1	・情報の預け主である医療機関等の要請により情報を提供する際にも電子署名等を検証して改ざんの検出を行い、正しく元の情報を提供できる機能となっているか
2	2	1	1	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・提供する電子カルテシステム等に関するサービスにおいて、医療機関等の職務権限等に応じたアクセス制御が可能であることを含め、仕様内容について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・提供するサービスにアクセス制御機能が備えてあるか ・アクセス制御機能が医療機関等の利用者の職種、担当業務等に応じることが可能か ・アクセス制御機能のグループの権限や適用範囲について、医療機関等と合意を得ているか ・グループに所属するユーザについて、医療機関等と合意を得ているか
2	2	1	2	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・システムの連携に関するインターフェイス構築の責任範囲を明確にして、医療機関等と合意を得ているか ・システム連携に関するインターフェイスの仕様について明確にしているか
2	2	1	3	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・入力された内容が記録の確定前に作成責任者によって確認できる仕様とすることを、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・入力された内容について、作成責任者によって確認した上で記録を確定する仕様となっているか ・記録の確定に関する仕様について、医療機関等と合意を得ているか
2	2	1	4	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・システムの連携に関するインターフェイス構築の責任範囲を明確にして、医療機関等と合意を得ているか ・連携に関するインターフェイスの仕様について明確にしているか
2	2	1	5	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せられる機能を含めること。	総務省医療ASP-GL	3.3.2	・記録の確定をしたデータに対して更新履歴を保存しているか ・記録の確定をしたデータの更新前と更新後の照合が行えるように機能を備えているか
2	2	1	6	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・更新管理の仕様について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・記録の確定したデータの更新管理の仕様について、医療機関等と合意を得ているか
2	2	1	7	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・代行操作を実施するID や運用方法について、予め医療機関等の管理者と内容を合意すること。	総務省医療ASP-GL	3.3.2	・記録の確定を行う際に代行操作された場合の仕様を明確にしているか ・記録の確定に関する仕様について、医療機関等と合意を得ているか
2	2	1	8	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・代行操作された際の、データの確定に関する仕様について、医療機関等の管理者と内容を合意すること。	総務省医療ASP-GL	3.3.2	・記録の確定を行う際に代行操作された場合の仕様を明確にしているか ・記録の確定に関する仕様について、医療機関等と合意を得ているか
2	2	1	9	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・機器、ソフトウェア構成について、医療機関等と合意をとること。	総務省医療ASP-GL	3.3.2	・機器、ソフトウェア構成が明確になっているか ・機器、ソフトウェア構成について、医療機関等と合意を得ているか
2	2	1	10	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・機器、ソフトウェア構成について文書化を行い、医療機関等の管理者に対して報告できる内容とすること。	総務省医療ASP-GL	3.3.2	・機器、ソフトウェア構成について文書化されているか ・文書化された機器、ソフトウェア構成について、医療機関等に報告しているか
2	2	1	11	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・提供するサービスにおけるシステムの導入プロセスについて、文書化を行うこと。	総務省医療ASP-	3.3.2	・システムの導入プロセスについて文書化されているか
2	2	1	12	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・システムの構成管理内容を示す資料の開示内容・範囲・条件について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・システムの構成管理内容を示す資料の開示内容・範囲・条件について、医療機関等と合意を得ているか
2	2	1	13	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・運用・操作に関する利用者教育における事業者の役割、範囲等について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・運用・操作に関する利用者教育の責任範囲を明確にして、医療機関等と合意を得ているか ・運用・操作に関する利用者教育に事業者が含まれる場合、教育内容について明確に示しているか
2	2	1	14	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・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について、事業者の役割、範囲等について医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・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責任範囲を明確にして、医療機関等と合意を得ているか ・内部監査の責任範囲に事業者が含まれる場合、監査に提示する内容について明確に示しているか
2	2	1	15	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	・ASP・SaaS提供に必要なシステムの保守をリモートメンテナンスで行う場合の、医療機関等への報告対象とするシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容等について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.2	・システムの保守をリモートメンテナンスで行う場合、メンテナンスを行うシステムの範囲を明確にして、医療機関等と合意を得ているか ・リモートメンテナンスを行う際の実施条件を取り決め、医療機関等と合意を得ているか ・リモートメンテナンス実施後の報告で内容について医療機関等と合意を得ているか
2	2	1	16	2. 機能と運用 2）電子保存の要求事項 ①真正性の確保	必須	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。	経産省医療外部保存-GL	7.6.10	・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しているか。
2	2	2	1	2. 機能と運用 2）電子保存の要求事項 ②見読性の確保	必須	・見読性を保証するサービス仕様について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.3	・見読性を保証するサービス仕様が明確になっているか ・見読性を保証するサービス仕様について、医療機関等と合意を得ているか
2	2	2	2	2. 機能と運用 2）電子保存の要求事項 ②見読性の確保	推奨	・緊急時の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ASP・SaaS において含めることについて、医療機関等の管理者と協議し、合意すること。	総務省医療ASP-GL	3.3.3	・緊急時の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が明確になっているか ・見読性の確保支援機能について、医療機関等と合意を得ているか
2	2	2	3	2. 機能と運用 2）電子保存の要求事項 ②見読性の確保	必須	情報処理設備との間に介在するネットワークの可用性について十分に検討すること	経産省医療外部保存-GL	6.2	・情報処理設備との間に介在するネットワークの可用性について十分に検討され具体的に提案しているか
2	2	2	4	2. 機能と運用 2）電子保存の要求事項 ②見読性の確保	必須	特に、データ容量が大きい高精細デジタル画像である医用画像（レントゲンデータ等）を扱う場合は、ネットワークの回線容量について配慮しておくこと。	経産省医療外部保存-GL	6.2	・特に、データ容量が大きい高精細デジタル画像である医用画像（レントゲンデータ等）を扱う場合は、ネットワークの回線容量について配慮し、実際の速度を提示しているか。
2	2	2	5	2. 機能と運用 2）電子保存の要求事項 ②見読性の確保	必須	アプリケーション入力の場合は医療情報安全管理ガイドラインの「5 情報の相互運用性と標準化」に示されている、基本データセット、標準的な用語集、コードセット、データ交換のための国際的な標準規格について、十分に理解し、実装するアプリケーションにおいて提供サービスの可用性、データの互換性の確保に務めること。	経産省医療外部保存-GL	6.2	・アプリケーション入力の場合は医療情報安全管理ガイドラインの「5 情報の相互運用性と標準化」に示されている、基本データセット、標準的な用語集、コードセット、データ交換のための国際的な標準規格について、十分に理解し、実装するアプリケーションにおいて「提供サービスの可用性」、「データの互換性」が確保されているか。
2	2	3	1	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	必須	・バックアップのき損箇所の確認に関する仕様、方法等ついて、医療機関等と合意すること。	総務省医療ASP-GL	3.3.4	・バックアップのき損箇所の確認に関する仕様、方法等が明確になっているか ・バックアップのき損箇所の確認に関する仕様、方法等について、医療機関等と合意を得ているか
2	2	3	2	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	推奨	・バックアップされたデータに対して、内容が改ざんされていないことを確認できる仕様について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.4	・バックアップデータの内容が改ざんされていないことを確認するための機能の仕様が明確になっているか ・バックアップデータの内容が改ざんされていないことを確認するため機能の仕様について、医療機関等と合意を得ているか
2	2	3	3	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	推奨	・医療情報のデータを格納するサーバのディスクの障害対策について、医療機関等と合意する。	総務省医療ASP-GL	3.3.4	・サーバのディスクの障害対策が明確になっているか ・サーバのディスクの障害対策について、医療機関等と合意を得ているか
2	2	3	4	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	必須	・入出力するデータ項目の形式ついて、標準形式を採用する。標準形式によることができない場合には、妥当なデータ項目の形式について医療機関等と合意すること。	総務省医療ASP-GL	3.3.4	・入出力するデータ項目の形式が標準形式であるか ・入出力するデータ項目の形式が標準形式でない場合、代替となるデータ形式が妥当なものであるかについて、医療機関等と合意を得ているか
2	2	3	5	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	必須	・マスターテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備える。本機能を備えることが困難な場合には、妥当な提案を行い、医療機関等と合意すること。	総務省医療ASP-GL	3.3.4	・マスタデータベースの変更の際に、データ移行に利用する機能について、情報の内容に変更が起こらないことを検証しているか ・データ移行に利用する機能及び検証が困難である場合は、医療機関等と合意を得ているか
2	2	3	6	2. 機能と運用 2）電子保存の要求事項 ③保存性の確保	必須	・ASP・SaaS によりデータ保存する際に用いるデータ形式及び転送プロトコルを変更する場合、変更前の方式との互換性の確保等について、医療機関等と合意する。	総務省医療ASP-GL	3.3.4	・データ保存のデータ形式および転送プロトコルを変更する場合に、互換性を検証しているか ・互換性の検証結果を基に、医療機関等と合意を得ているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
2	2	3	7	2. 機能と運用　2）電子保存の要求事項　③保存性の確保	必須	・ASP・SaaS に用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	総務省医療ASP−GL	3.3.4	・ASP・SaaS に用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画を定めているか ・ASP・SaaS に用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意を得ているか
2	2	3	8	2. 機能と運用　2）電子保存の要求事項　③保存性の確保	必須	システムの更新、アプリケーションの変更等に伴い、電子保存された医療情報の読み出しに関する互換性を失わないように配慮すること	経産省医療外部保存−GL	6.2	・システムの更新、アプリケーションの変更等に伴い、電子保存された医療情報の読み出しに関する互換性を失わないように配慮されているか
3	1		1	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社で定める情報セキュリティに関する組織的取組における基本方針が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・情報セキュリティに関する組織的取組における基本方針等を作成しているか ・情報セキュリティに関する組織的取組における基本方針等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		2	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等の体制に対応する事業者の体制を明らかにすることを、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・体制図を作成しているか ・体制図が、医療機関等の体制に対応しているか ・体制図について、、医療機関等の合意を得ているか
3	1		3	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	マニュアル等の文書管理に関して、開示できる文書等の範囲、事業者の役割等を医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・文書管理に関して、開示する範囲・条件を定めているか ・開示範囲等について医療機関等の合意を得ているか
3	1		4	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社で定めるリスク等に対する予防措置及び事故等の発生時の対応等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・リスク等に対する予防措置及び事故等の発生時の対応等が定めてあるか ・リスク等に対する予防措置及び事故等の発生時の対応等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		5	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社で定める機器の管理等の運用管理の規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・機器の管理等の運用管理の規程等が定めてあるか ・機器の管理等の運用管理の規程等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		6	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社で定める個人情報を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・個人情報を記録した媒体の運用管理規程等が定めてあるか ・個人情報を記録した媒体の運用管理規程等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		7	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	個人情報保護法の対象に満たない件数(5,000 件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱うこと。	総務省医療ASP−GL	3.2.1	・件数に関わらず、個人情報保護法における運用に準じることになっているか
3	1		8	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等の管理者が患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・医療機関等の管理者が患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等が定めてあるか ・提供範囲等について医療機関等の合意を得ているか
3	1		9	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社において実施するシステム監査等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・システム監査等を実施しているか ・システム監査等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		10	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	監査記録等を医療機関等に開示する情報の範囲条件等について合意すること。	総務省医療ASP−GL	3.2.1	・監査記録等を作成しているか ・監査記録等を開示する範囲・条件を定めているか ・開示範囲等について医療機関等の合意を得ているか
3	1		11	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等の管理者側からの問合せ窓口を設けること。また受付の時間帯等について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.1	・医療機関等に対する問い合わせ窓口を設けているか ・問い合わせ窓口の受付時間について医療機関等の合意を得ているか
3	1		12	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	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関しては、医療機関等の管理者と協議の上、実際に設定する作業に関する役割も含めて合意すること。	総務省医療ASP−GL	3.2.3	・アクセス制御機能のグループの権限や適用範囲について、医療機関等と合意を得ているか ・グループに所属するユーザについて、医療機関等と合意を得ているか
3	1		13	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等のアクセス管理に関する運用管理規程の内容に従った運用を行い、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP−GL	3.2.3	・運用管理規程等を定めているか ・運用管理規程等にアクセス制御に関する項目が存在するか ・運用管理規程等を遂行する際に、証跡を残すように定めてあるか ・医療機関等の求めに応じ、証跡を提出できるようにしてあるか
3	1		14	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	運用管理者とログのレビュー者のアクセス権を分離する等の、アクセスログの改ざん等に対する措置を講じること。	総務省医療ASP−GL	3.2.3	・アクセスログに対するアクセス権を設定しているか ・運用管理者とログのレビュー者のアクセス権を分離しているか
3	1		15	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.3	・パスワードポリシーが定めてあるか ・パスワードポリシーについて、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		16	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	利用者のパスワード発行等に関する手続及び業務範囲について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.3	・パスワード発行等の手続き・範囲等が規定されているか ・規定されたパスワード発行等の手続き・範囲等について、医療機関等と合意を得ているか
3	1		17	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等がASPSaaS の利用に際して無線LAN を利用する場合に、医療機関等の無線LAN が必要なセキュリティ対策について、事業者の役割、範囲等について合意すること。	総務省医療ASP−GL	3.2.3	・ASP・SaaS の利用のために使用する無線LANについて、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・無線LANの責任範囲に事業者が含まれる場合、無線LAN が必要なセキュリティ対策を施しているか ・無線LANの責任範囲に事業者が含まれる場合、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		18	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	推奨	自社において定めたパスワードポリシーが、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP−GL	3.2.3	・パスワードポリシーが定めてあるか ・パスワードポリシーについて、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		19	3. 契約・合意・説明に関する事項　1）内部運用に関する条	推奨	採用する認証手段方式について、医療機関等と合意すること。	総務省医療ASP−	3.2.3	・採用する認証手段や方式について、医療機関等と合意を得ているか
3	1		20	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	推奨	医療機関等がASPSaaS の利用に際して無線LAN を利用する場合に、医療機関等の無線LAN が必要なセキュリティ対策についての、事業者の役割、範囲等について合意すること。	総務省医療ASP−GL	3.2.3	・ASP・SaaS の利用のために使用する無線LANについて、事業者の責任範囲を明確にして、医療機関等と合意を得ているか ・無線LANの責任範囲に事業者が含まれる場合、無線LAN が必要なセキュリティ対策を施しているか ・無線LANの責任範囲に事業者が含まれる場合、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	1		21	3. 契約・合意・説明に関する事項　1）内部運用に関する条	必須	・サービス提供に際して、医療機関等と守秘義務契約を締結すること。	総務省医療ASP−	3.2.6	・医療機関等と守秘義務契約を取り交わしているか
3	1		22	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	「ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと」という旨の事項が委託契約事項に定められていること	経産省医療外部保存−GL	4.2	・「ハードウェア及びソフトウェアの仕様書、運用計画書、事業継続計画文書等を求めに応じて提出可能な状態におくこと」という旨の事項が標準委託契約様式または既委託契約書の契約事項に定められているか
3	1		23	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	「定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告についても、提出可能な状態におくこと」という旨の事項が委託契約事項に定められていること	経産省医療外部保存−GL	4.2	・「定期的な情報セキュリティ監査、システム監査等、第三者監査の実施、結果及び是正措置報告についても、提出可能な状態におくこと」という旨の事項が標準委託契約様式または既委託契約書の契約事項に定められているか
3	1		24	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	発生しうる事態を想定した説明責任の分担を契約事項として含めること	経産省医療外部保存−GL	4.3	・発生しうる事態を想定した説明責任の分担が契約事項として含められていること
3	1		25	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	発生した事態に関する責任については医療機関等との契約において第一義に情報処理事業者が負うこと	経産省医療外部保存−GL	4.3	・再委託の場合、発生した事態に関する責任については医療機関等との契約において委託先の責任にせず第一義に情報処理事業者が負うことが規定されているか
3	1		26	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等と情報処理事業者、回線事業者の責任について、想定される障害等のそれぞれについて契約に明示すること	経産省医療外部保存−GL	4.4	・医療機関等と情報処理事業者、回線事業者の責任について、想定される障害等のそれぞれについて契約書に明示されているか
3	1		27	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	インターネットVPNを利用する場合には、「直接の契約関係にない回線事業者で発生したインターネットVPN 上の障害についての責任を誰かに負わせることはできない。」というリスクを契約上考慮すること	経産省医療外部保存−GL	4.4	・インターネットVPNを利用する場合には、「直接の契約関係にない回線事業者で発生したインターネットVPN 上の障害についての責任を誰かに負わせることはできない。」というリスクを踏まえて契約上責任分界が決められているか
3	1		28	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	推奨	医療情報安全管理ガイドラインの基準に従っていることを、適用している安全管理策を適用宣言書の形で整理しておくこと	経産省医療外部保存−GL	8.1	・医療情報安全管理ガイドラインの基準に従っていることを明文化しているか
3	1		29	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	原則として、機密管理の観点から受託管理する医療情報の全体を情報処理事業者が閲覧・処理を行わないこと。	経産省医療外部保存−GL	3	・原則として受託管理する医療情報の全体を情報処理事業者が閲覧・処理を行わない為の方策をとっているか。
3	1		30	3. 契約・合意・説明に関する事項　1）内部運用に関する条件	必須	医療機関等が求めるサービスの実現のために閲覧が必要な場合は、医療情報安全管理ガイドラインにおける記述を踏まえつつ、医療情報の秘匿性の高さに十分配慮して、適切なアクセス管理を実施した上で行うこと。	経産省医療外部保存−GL	3	・医療機関等が求めるサービスの実現のために閲覧が必要な場合は、適切なアクセス管理を実施した上で行っているか。

項番 大分類	中分類	小分類	要件	分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
3	1		31	3. 契約・合意・説明に関する事項 1）内部運用に関する条件	必須	扱う情報として、法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすること。	経産省医療外部保存-GL	3	・扱う情報として、法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実としているか。
3	1		32	3. 契約・合意・説明に関する事項 1）内部運用に関する条件	必須	ネットワーク経由の交換手順について医療機関等と合意し、手順書として双方で管理すること	経産省医療外部保存-GL	3.4	・ネットワーク経由の交換手順について医療機関等と合意し、手順書として双方で管理しているか
3	1		33	3. 契約・合意・説明に関する事項 1）内部運用に関する条件	必須	アプリケーション入力による医療情報の交換手順について医療事業者と合意し、手順書として双方で管理すること。	経産省医療外部保存-GL	3.5	・アプリケーション入力による医療情報の交換手順について医療事業者と合意し、手順書として双方で管理しているか
3	1		34	3. 契約・合意・説明に関する事項 1）内部運用に関する条件	必須	ASP・SaaS事業者においては、プライバシーマークを取得することが強く求められる。また不足なく適用範囲を定めた適用宣言書に基づくISMS 認定の取得を考慮することも求められる。	総務省医療ASP-GL	2.4	・ASP・SaaS事業者においては、プライバシーマークを取得することを配慮しているか。また不足なく適用範囲を定めた適用宣言書に基づくISMS 認定の取得を考慮しているか。
3	2		1	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	・外部組織に対して再委託等を行う場合には、事前に医療機関等の管理者に対して説明を行い、契約において体制を明確にすること。	総務省医療ASP-GL	3.2.4	・体制図を作成しているか ・体制図について、再委託先まで記載されているか ・体制図について、契約において医療機関等の合意を得ているか
3	2		2	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	・外部組織に対して、自社と同等の個人情報保護指針等について遵守させること。	総務省医療ASP-GL	3.2.4	・再委託先に対して守秘義務契約を交わしているか ・再委託先に対して自社と同等の個人情報保護指針等を遵守させているか ・再委託先に対して自社と同等の個人情報保護指針等の教育を実施しているか
3	2		3	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	・外部組織においても個人情報を交換する場合の安全管理に関する要求事項を遵守させること。	総務省医療ASP-GL	3.2.4	・再委託先に対しても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におけるASP・SaaS 事業者への要求事項を順守させているか
3	2		4	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	再委託先の事業者に対して互いの責任の範囲について合意し、再委託先との契約で明記しておくこと	経産省医療外部保存-GL	4.3	・再委託先の事業者に対して互いの責任の範囲について合意し、再委託先との契約で明記にされているか
3	2		5	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	第三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されていること。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、第三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することが定められているか。 ・リスク評価結果報告書に上記の内容が記録されており、内容が妥当か。
3	2		6	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	サービスの実施、運用、維持について定期的に検証されていること。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、サービスの実施、運用、維持について定期的に検証するように定められているか。 ・検証結果報告書が存在し、その内容が妥当か。
3	2		7	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	サービス実施について事前、事後報告を義務づけ、報告内容が点検確認されていること。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、サービス実施について事前、事後報告が義務付けられているか。 ・サービス実施結果報告書が存在し、その内容が妥当か。 ・サービス実施結果報告書の内容が点検確認されているか。
3	2		8	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	サービス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ていないこと。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、サービスを実施する人員の届け出が定められているか。 ・サービス実施結果報告書が存在し、その内容が妥当か。
3	2		9	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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させてこと。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、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させることが定められているか。
3	2		10	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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、職員の入室、退室手順に準ずること。	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、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、職員の入室、退室手順に準ずる内容が定められているか。
3	2		11	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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	経産省医療外部保存-GL	7.6.5	・運用手順書の中で、サービス変更時に引き続き安全性が維持されることについて適切な検証を行うことが定められているか。 ・検証結果報告書が存在し、その内容が妥当か。
3	2		12	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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ているか。
3	2		13	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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を求めているか。 ・保守作業の委託契約の中で、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のことを求めているか。
3	2		14	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	3. 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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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ているか。
3	2		15	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	4. 保守要員の離職や担当変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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、保守要員の離職や担当変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ているか。 ・運用手順書の中で、それに応じるアカウント管理体制を整えているか。
3	2		16	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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と、終了時の速やかな作業報告書の提出を求めているか。 ・運用手順書の中で、それらの書類を事業者の責任者が逐一承認することが定められているか。
3	2		17	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、守秘義務契約を締結しているか。 ・運用手順書の中で、委託業者が守秘義務を遵守していることを定期的に確認することが定められているか。
3	2		18	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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を定めることを求めているか。 ・運用手順書の中で、その内容を事業者の責任者が逐一承認することを定めているか。
3	2		19	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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提出することを求めているか。 ・運用手順書の中で、その内容を事業者の責任者が確認することを定めているか。
3	2		20	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	必須	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。	経産省医療外部保存-GL	7.6.5	・保守作業の委託契約の中で、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が定められているか。
3	2		21	3. 契約・合意・説明に関する事項 2）再委託先の管理・監督	推奨	外部事業者がサービスを実施する際は、情報処理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。	経産省医療外部保存-GL	7.6.5	・外部事業者がサービスを利用する際の作業者が情報処理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するよう規定されているか
3	3	1	1	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	下記の項目は医療機関等の手順であることを明確にし医療機関等に説明すること (1) 医療情報を外部保存することに関する内部申請及び承認プロセスを実施する。 (2) 情報処理事業者受け取り後の真正性検証のため、外部保存対象の電子ファイルについて電子署名を付与等の対策を実施する。 (3) 医療機関等と情報処理事業者を接続するネットワーク上の機器に電子ファイルを複写する（なお、医療機関等の内部ネットワークと電子ファイル転送用のネットワークが接続されている場合は不要な通信が行われないよう適切な安全管理対策、アクセス制御を適用すること）。 (4)ネットワークを経由して情報処理事業者の受入れ機器に電子ファイルを複写する。 (5) 情報処理事業者に送出完了を通知する。	経産省医療外部保存-GL	3.4	・左記項目が医療機関等で実施すべき手順であることを明確にして医療機関等に説明し、実施を要請しているか
3	3	1	2	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	下記の項目は医療機関等の手順であることを明確にし医療機関等に説明すること (1) 情報処理事業者からの定時報告を確認、検証する。 (2) 不審な点があれば、ただちに確認を行う。	経産省医療外部保存-GL	3.4	・左記項目が医療機関等で実施すべき手順であることを明確にして医療機関等に説明し、実施を要請しているか
3	3	1	3	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS 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適用が及ぶ場所に設置すること。	総務省医療ASP-GL	3.2.8	・ASP・SaaS 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適用が及ぶ場所に設置しているか ・所管官庁に対して提出する法令に基づく資料を円滑に提出できるようにしているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
3	3	1	4	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・障害等が生じた場合等を想定し、冗長性を確保する仕様等について医療機関等と合意すること	総務省医療ASP-GL	3.3.3	・冗長性に対するサービス仕様が明確になっているか ・サービス仕様が障害等が生じることを想定しているか ・冗長性に対するサービス仕様について、医療機関等と合意を得ているか
3	3	1	5	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	推奨	・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	総務省医療ASP-GL	3.3.3	・障害等が生じた際のサービス品質が明確になっているか ・障害等が生じた際のサービス品質について、医療機関等と合意を得ているか
3	3	1	6	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・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すこと。	総務省医療ASP-GL	3.3.5	・委託契約の際に、守秘義務契約を取り交わしているか ・守秘義務契約に違反した場合のペナルティについて記載されているか
3	3	1	7	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・自社で講じるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP-GL	3.3.5	・ASP・SaaS を利用するネットワークについて、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしているか ・医療機関等の求めに応じ、基準を満たしていることの証跡について、提出できるようにしてあるか
3	3	1	8	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等を、医療機関等と合意すること。	総務省医療ASP-GL	3.3.5	・遵守すべきガイドラインが明確になっているか ・遵守すべきガイドラインに対して、遵守していることについて証跡を残しているか ・証跡の内容や範囲等について、医療機関等と合意を得ているか
3	3	1	9	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと。	総務省医療ASP-GL	3.3.5	・守秘義務契約を取り交わしているか ・保守作業で取り扱う領域を定めているか ・保守作業で領域を超えて閲覧していないことが確認されているか
3	3	1	10	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・許可されていない受託データの閲覧を禁止することにつき、その方法等を含め、医療機関等と合意すること。	総務省医療ASP-GL	3.3.5	・受託データで許可されていない範囲の閲覧を禁止しているか ・閲覧の禁止方法を含め、医療機関等と合意を得ているか
3	3	1	11	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・受託した医療情報は、匿名化されたものを含めて、医療機関との契約に基づくことなく、分析、解析等を実施しないこと。	総務省医療ASP-GL	3.3.5	・受託した医療情報について、医療機関との契約に基づくことなく、分析、解析等を実施していないか
3	3	1	12	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と合意すること。	総務省医療ASP-GL	3.3.5	・受託した医療情報について、契約外の分析、解析等を防ぐ方策について明確になっているか ・契約外の分析、解析等を防ぐ方策について、医療機関等と合意を得ているか
3	3	1	13	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。	総務省医療ASP-GL	3.3.5	・契約前に、サービス選定に必要な情報(安全管理の基本方針・規定・体制、実績に基づく信用度、経営の健全性等)について整理してあるか ・サービス選定に必要な情報について、提供が求められた場合提出できるようにしてあるか
3	3	1	14	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	推奨	・システム管理者のデータアクセスの制限の方法について、医療機関等と合意する。	総務省医療ASP-GL	3.3.5	・システム管理者にデータアクセス制限を行っているか ・システム管理者に対するアクセス制御について、医療機関等と合意を得ているか
3	3	1	15	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・自社で定める個人情報保護を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.5	・個人情報保護指針等を作成しているか ・個人情報保護指針等について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか
3	3	1	16	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱う旨が含まれていることを確認し、医療機関等の求めに応じて資料を提出できるようにすること。	総務省医療ASP-GL	3.3.5	・件数に関わらず、個人情報保護法における運用に準じることになっているか ・運用方式について医療機関に提出できるようにしているか
3	3	1	17	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ①事業者から利用者に説明する事項	必須	・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、役割分担等について、医療機関等と合意すること。	総務省医療ASP-GL	3.3.5	・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対する責任範囲を明確にして、医療機関等と合意を得ているか ・外部保存に関する説明の責任範囲に事業者が含まれる場合、説明に必要な資料を提供しているか
3	3	2	1	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ②サービス提供終了時の要求事項	必須	・事業者の都合により医療機関等に対してASP・SaaS の提供を終了する場合の事前通知の方法、終了が認められる理由、及び終了に向けての対応について、医療機関等と合意すること。	総務省医療ASP-GL	3.4.2	・ASP・SaaS の提供を終了する場合の対応について定めてあるか ・終了に対する事前通知の方法、告知期限について定めてあるか ・終了理由、終了への対応について、医療機関等と合意を得ているか
3	3	2	2	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ②サービス提供終了時の要求事項	必須	・情報の破棄の実施に際し、報告の内容・範囲・提出すべき資料等について、医療機関等と合意すること。	総務省医療ASP-GL	3.4.2	・情報の破棄手順について定めてあるか ・情報の破棄手順について、医療機関等の求める内容を踏まえ、協議を行った上で合意を得ているか ・実施内容に情報の削除方法について記録してあるか ・実施内容を記録した破棄記録等を医療機関に提出しているか
3	3	2	3	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ②サービス提供終了時の要求事項	必須	・ASP・SaaS の提供を終了する場合に、受託しているデータ及びこれに関連する資料の内容、範囲、条件等について、医療機関等と合意すること。	総務省医療ASP-GL	3.4.2	・ASP・SaaS の提供を終了する場合の受託データや関連資料について、対応について明確にしているか ・対応内容について、医療機関等と合意を得ているか
3	3	2	4	3. 契約・合意・説明に関する事項　3）医療情報の保存／取扱いをする場合の要求事項 ②サービス提供終了時の要求事項	必須	・受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「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こと。	総務省医療ASP-GL	3.4.2	・受託データを医療機関に引き渡す際に、厚労省ガイドラインに従ったデータ形式で渡すこととしているか ・引き渡しの方法や形式について、医療機関等と合意を得ているか

項番				分類	必須／推奨	対策項目	対象GL	GLでの参照箇所	確認項目
大分類	中分類	小分類	要件						
3	3	3	1	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	推奨	ASP・SaaSにおいて使用するデータの形式等についても、将来的な移行を視野に入れた対応をすることが望ましい	総務省医療ASP-GL	3.4.3	・入出力するデータ項目の形式について、将来的な移行について検討されているか
3	3	3	2	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	入出力するデータ項目の形式等について、標準形式を採用し、標準形式によることができない場合には、妥当な対応を行う旨を医療機関等と協議する、等の対応を図ることが求められる	総務省医療ASP-GL	3.4.3	・入出力するデータ項目の形式が標準形式であるか ・入出力するデータ項目の形式が標準形式でない場合、代替となるデータ形式が妥当なものであるかについて、医療機関等と合意を得ているか
3	3	3	3	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5情報の相互運用性と標準化について」に従って行うことが求められる。	総務省医療ASP-GL	3.4.3	・受託データを医療機関に引き渡す際に、厚労省ガイドラインに従ったデータ形式で渡すこととしているか
3	3	3	4	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	医療情報を作成する医療従事者及び医療機関等が真正性を確保することができるよう、情報記録者が誰であるのか（責任の所在）について電磁的記録として認識できるよう、文書フォーマット等について医療機関等と十分な合意を形成しておくこと。	経産省医療外部保存-GL	6.1	・医療情報を作成する医療従事者及び医療機関等が真正性を確保することができるよう、情報記録者が誰であるのか（責任の所在）について電磁的記録として認識できるよう、文書フォーマット等について医療機関等と十分な合意を形成するための準備がなされているか
3	3	3	5	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	それぞれの情報に求められる見読可能となるまでの時間的要求について、医療機関等と合意しておくこと	経産省医療外部保存-GL	6.2	・それぞれの情報に求められる見読可能となるまでの時間的要求について、医療機関等と合意しているか／合意の為の案を提示しているか
3	3	3	6	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	医療情報安全管理ガイドラインの「8. 診療録及び診療諸記録を外部に保存する際の基準」の要求事項その他、全ての要件を満たしていること	経産省医療外部保存-GL	8.1	・医療情報安全管理ガイドラインの「8. 診療録及び診療諸記録を外部に保存する際の基準」の要求事項を満たしているか
3	3	3	7	3. 契約・合意・説明に関する事項 3）医療情報の保存／取扱いをする場合の要求事項 ③電子保存の要求事項	必須	情報処理事業者による医療情報の閲覧が禁止されていること	経産省医療外部保存-GL	8.1	・情報処理事業者による医療情報の閲覧が禁止しているか