

Acronis Cyber Protect Cloud を 使用した医療情報の安全管理に関する ガイドライン

本書では、経済産業省（METI）および総務省（MIC）によって策定された「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（2023 年 8 月改訂版 v 1.1）に基づき、Acronis が情報開示要件の一環として導入したセキュリティ管理対策について概説する。¹ 本文書で説明されている Acronis の制御は、第三者監査コンプライアンスプログラムである ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018 および ISO 9001 によって認証済みである。詳細な情報は、SOC-2 Type II 報告書より取得することができる。

Acronis のユーザごとに異なる「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」で必要とされる「情報の流れ」については、状況に応じた対応を提示することが困難である。このため、Acronis は「別紙 2 別紙2 統合前ガイドラインにおける対策項目一覧と医療情報安全管理ガイドライン6.0版の対応表」に沿って本文書を作成した。² 上記の別紙 2 で採用された番号付けと関連する「要求事項の内容」に加えて、Acronis による準拠の方法、および関連する前述の ISO の制御との対応が追加されている。



¹ https://www.soumu.go.jp/main_content/000891033.pdf

² https://www.soumu.go.jp/main_content/000891035.pdf

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1. 人的・組織的対策				
1.1. 規程・手順の 策定	① アクセス 管理規程の策定	①-1	医療情報システム等へのアクセス制限、記録、点検等を定めたアクセス管理規程を作成し、医療機関等の求めに応じて提出できる状態にしておく。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御は、Acronis の ISO/IEC 27001 および SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis では以下のように 2 種類のデータを区別している。</p> <ul style="list-style-type: none"> ・サービスの提供（製品の使用状況など）と Acronis のサービス管理に必要なデータ。 Acronis がサービスを提供するために、データ管理者として収集および処理するデータ。このようなデータには、アカウント名、メールアドレスとその他の連絡先情報、請求の詳細、およびサービスを通じて自動収集された一部の情報が含まれる場合があり、個人情報が含まれる可能性がある。詳細については、Acronis の個人情報保護方針を参照のこと。 https://www.acronis.com/company/privacy/ ・カスタマーのコンテンツデータ。カスタマーが Acronis のサービスを利用する際に Acronis がデータ処理者（復処理者）として処理する可能性があるデータ。情報は、バックアップアーカイブ、ファイル、仮想マシンなどの特定の製品の使用時にカスタマーから提供される。この種類のデータに関しては、カスタマーが Acronis を通じて保管する情報のカテゴリや内容を Acronis が管理することはない。 <p>Acronis は、ロールベースで厳格に職務分掌し、特権アクセスを付与する。Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-2	<p>アクセス管理規程には以下の内容を含める。</p> <ul style="list-style-type: none"> ・アクセス権限、アカウント管理における登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセス ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・アクセス管理の運用状況に関する定期的なレビューの実施。 	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） ・「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御は、Acronis の ISO/IEC 27001 および SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、自社のニーズに応じてアクセス管理を含む環境の設定と管理に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② 持ち出した機器の外部のネットワークに接続する場合の対策の策定	②-1	持ち出した機器を外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） ・「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） ・「ネットワークセキュリティ」（ISO27K1:2013 A.13.1、ISO27K1:2022 A.8.20、A.8.22） ・「データ漏洩防止」（27K1:2022 8.12） <p>Information security oversight and management controls, including logical access 論理アクセス制御を含む情報セキュリティ監査および管理制御は、Acronis の ISO/IEC 27001 および SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
	③ 情報の廃棄対応	③-1	CD-R 等の廃棄手順について定める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」（27K1:2013 A.8.3.2、27K1:2022 A.7.10） ・「装置の安全な処分または再利用」（27K1:2013 A.11.2.7、27K1:2022 A.14） ・「資産の移動」（27K1:2013 A.11.2.5、27K1:2022 A.7.10） ・「設備の保守」（27K1:2013 A.11.2.4、27K1:2022 A.13） ・「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御は、Acronis の ISO/IEC 27001 および SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis のハードディスクには、保存時のデータを保護するために、フルディスク暗号化（FDE）やドライブブロック機構などの技術が組み込まれている。</p> <p>Acronis は、データセンターのコロケーションにおいて、現地の有資格のサードパーティを使用してドライブが物理的に処分されることを保証する。</p>
		③-2	ハードディスク等の廃棄手順について定める。	
		③-3	破棄手順に、不可逆的な破壊・抹消等により元のデータを復元できなくする措置を含める。	
		③-4	ハードディスク等を医療情報システム等内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認する。	
		③-5	サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		⑤-6	ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「マルウェア対策」(27K1:2013 A.12.2、27K1:2022 8.7) ・「技術的脆弱性の管理」(27K1:2013 A.12.6.1、A.18.2.3、27K1:2022 A.8.8) <p>Acronis は、市販のツールと独自に開発したツールを組み合わせた包括的な脆弱性管理プログラムを実装し、セキュリティ脅威を事前対応的に特定するとともに、厳格な自動化および手動の侵入テスト、品質保証対策、ソフトウェアセキュリティ評価、外部監査を実施している。脆弱性の監視と対処の責任は、Acronis のサイバーセキュリティチームが負う。チームはこれらの課題を入念に特定および追跡し、是正が確認されるまで定期的にフォローアップを行う。さらに、Acronis は脆弱性報奨金制度を実施することで、セキュリティ独立研究者との強固な関係を構築している。</p> <p>脆弱性管理に関する管理については、Acronis の SOC 2 Type II 報告書のために第三者監査人による レビューおよび検証も行われている。</p> <p>Acronis のサイバーセキュリティ体制に関する詳細情報は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		⑤-7	ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) <p>メディアセキュリティを含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis のハードディスクには、保存時のデータを保護するために、フルディスク暗号化 (FDE) やドライブロック機構などの技術が組み込まれている。</p> <p>Acronis は、独自の消失訂正アルゴリズムを使用し、カスタマーのデータをセキュリティを保って削除するソフトウェア定義ストレージソリューションを採用している。Acronis Cyber Infrastructure のドライブや機器が故障、修理のために交換、または廃止された場合、Acronis は NIST SP 800-88rev1 に従って、ディスクからデータを消去し、機器の内部メモリから残留データを削除する措置を講じる。情報を消去（削除）できない場合、そのようなデータを読み取る（復元する）ことができないように、機器を物理的に破壊する。</p> <p>Acronis は、データセンターのコロケーションにおいて、現地の有資格のサードパーティを使用してドライブが物理的に処分されることを保証する。</p> <p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		⑤-8	<p>物理的な破壊措置については受託事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等にし外部委託の了承を得ておく。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。</p> <p>なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式 (NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等) も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施することが望ましい。</p>	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) <p>メディアセキュリティを含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis のハードディスクには、保存時のデータを保護するために、フルディスク暗号化 (FDE) やドライブロック機構などの技術が組み込まれている。</p> <p>Acronis は、独自の消失訂正アルゴリズムを使用し、カスタマーのデータをセキュリティを保って削除するソフトウェア定義ストレージソリューションを採用している。Acronis Cyber Infrastructure のドライブや機器が故障、修理のために交換、または廃止された場合、Acronis は NIST SP 800-88rev1 に従って、ディスクからデータを消去し、機器の内部メモリから残留データを削除する措置を講じる。情報を消去 (削除) できない場合、そのようなデータを読み取る (復元する) ことができないように、機器を物理的に破壊する。</p> <p>Acronis は、データセンターのコロケーションにおいて、現地の有資格のサードパーティを使用してドライブが物理的に処分されることを保証する。</p> <p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>
		⑤-9	電子媒体を廃棄する場合には、物理的な破壊措置 (高温による融解、裁断等) を適用し、情報の読み出しが不可能であることを確認する。	
		⑤-10	<p>運用管理規程に以下の内容を定める。</p> <ul style="list-style-type: none"> ・管理する個人情報又はこれを格納する媒体等について、医療情報システム等提供上の要否の確認を定期的に行うこと。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置 (事前に破棄の基準等を告知する等)。 	
		⑤-11	情報の破棄手順について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	④ 情報や機器の 組織外への持出に 対する対策	④-1	受託する個人情報を運用や保守に用いる端末に原則保存しない旨、自社の運用管理規程等に定める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「機器の設置および保護」(27K1:2022 A.11.2.1、27K1:2022 A.7.8) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「構外にある機器および資産のセキュリティ」(27K1:2013 A.11.2.6、27K1:2022 A.7.9) ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) <p>Acronis のカスタマーのコンテンツデータは、従業員によって直接アクセスすることはできず、端末デバイスにエクスポートすることもできない。</p>
		④-2	医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又は受託事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。	
		④-3	④-2で定める手順及び情報の提供条件について、医療機関等と合意する。	
		④-4	持ち出した機器を再度設置するための適切な検証手順を策定する。	
		④-5	保守点検で障害不良等が発見された際の対応作業等を行う際には受託事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出す。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「機器の設置および保護」(27K1:2022 A.11.2.1、27K1:2022 A.7.8) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「構外にある機器および資産のセキュリティ」(27K1:2013 A.11.2.6、27K1:2022 A.7.9) ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) <p>Acronis の内部ポリシーでは、損傷したハードウェアを再利用または修理することはない。損傷したハードウェアは廃棄される。</p> <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		④-6	<p>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。</p> <ul style="list-style-type: none"> ・ 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ・ 申請承認プロセス ・ 返却確認プロセス、等。 	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		④-7	返却時の検証手順に含まれる事項には次のようなものが考えられる。 <ul style="list-style-type: none"> ・ 装置の動作確認 ・ 盗聴装置等、情報の安全性を脅かす装置の有無 ・ 悪意のあるプログラムの検出作業 ・ 収められている情報の検証作業（不正な改竄等）、等。. 	
	⑤ 持ち出した機器や 媒体の管理手順の 策定	⑤-1	サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「設備の配置と保護」（27K1:2013 A.11.2.1、27K1:2022 A.7.8） ・ 「構外にある機器および資産のセキュリティ」（27K1:2013 A.11.2.6、27K1:2022 A.7.9） ・ 「媒体の処分」（27K1:2013 A.8.3.2、27K1:2022 A.7.10） ・ 「装置の安全な処分または再利用」（27K1:2013 A.11.2.7、27K1:2022 A.14） ・ 「資産の移動」（27K1:2013 A.11.2.5、27K1:2022 A.7.10） ・ 「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） ・ 「資産利用の許容範囲」（27K1:2013 A.8.1.3、27K1:2022 A.5.10） ・ 「ネットワークセキュリティ」（27K1:2013 A.13.1.1、27K1:2022 A.8.20） ・ 「情報のバックアップ」（27K1:2013 A.12.3.1、27K1:2022 A.8.13） <p>Acronis は、データが Acronis または Acronis の代理の直接の管理下でない外部の境界を通過する際に、1 つ以上のネットワーク層にまたがって転送されるすべてのデータが暗号化され、認証されるよう保証する。</p> <p>大容量の電子メディアは、初回バックアップのためにカスタマーが物理的なデータ配送サービスを要求した場合のみ使用される。Physical Data Shipping サービスに関する詳細情報は、次のページを参照のこと。https://www.acronis.com/support/providers/physical-data-shipping/</p> <p>Acronis のハードディスクには、保存時のデータを保護するために、フルディスク暗号化（FDE）やドライブロック機構などの技術が組み込まれている。Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		⑤-2	⑤-1における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。	
		⑤-3	⑤-1で定める内容について、医療機関等と合意する。	
		⑤-4	電子媒体について受託事業者施設外への不要な持ち出しを行わない。CD、DVD、MO 等。	
		⑤-5	情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行う。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行う。	
		⑤-6	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「情報の分類」（27K1:2013 A.8.2.1、27K1:2022 A.5.12） ・ 「情報のラベル付け」（27K1:2013 A.8.2.2、27K1:2022 A.5.13） <p>カスタマーは、Acronis Cyber Protect Cloud に保存されている情報に独自のデータラベルを適用できる。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		⑤-7	記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。 <ul style="list-style-type: none"> 管理体制及び管理方法記録媒体・記録機器の取扱い サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器 媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失（持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業員等における誤送信等を含む。））が起きた場合の対応。 	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） 「情報セキュリティの意識向上、教育および訓練」（27K1:2013 A.7.2.2、27K1:2022 A.6.3） <p>Acronisは、ISO 27001 規格に準拠する情報セキュリティ管理システム (ISMS) を採用し、包括的な内部文書を維持している。すべての文書は、システムに保管され、複製とバックアップが行われる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p> <p>Acronis の契約社員はすべて、入社時にセキュリティ訓練を受講し、Acronis での在籍中にも継続して訓練を受講する。新規契約社員は、オリエンテーションの一環として、カスタマー情報を安全に保護する当社の献身を重視し、当社の行動規範に従うことを誓約する。特定のロールに基づいて、特定のセキュリティの側面に関する追加の訓練を受ける場合がある。例えば、情報セキュリティチームは新しいエンジニアに対して、セキュアコーディングの実践、製品設計、および自動脆弱性テストツールの使用に関するトレーニングを提供する。</p> <p>セキュリティ意識と訓練の管理を含む情報セキュリティの監視と管理制御については、Acronis の SOC 2 Type II 報告書のために第三者の監査人によるレビューおよび検証も行われている。</p>
		⑤-8	⑤-7の内容に関する教育を従業員等に対して行う。	
		⑤-9	⑤-7の内容を含む運用管理規程については、再委託先に対しても遵守等を求める。	
	⑥ 機器・ソフトウェアの品質管理に係る手順の策定	⑥-1	情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。	Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「変更管理」（27K1:2013 A.12.1.2、27K1:2022 A.8.32） 「システムの取得、開発および保守」（27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32） 「製品およびサービスの設計・開発」（9001:2015 8.3） <p>Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。</p>
		⑥-2	機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等を含める。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		⑥-3	機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。	<p>Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) ・「製品およびサービスの設計・開発」(9001:2015 8.3) <p>Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。</p>
		⑥-4	医療情報システム等に係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。	
		⑥-5	<p>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。</p> <ul style="list-style-type: none"> ・ 変更についての影響が及び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。 	
1.2. 個人情報を含まないテストデータの利用	① 個人情報を含むデータの利用に対する対策	①-1	医療情報を開発及び試験用データとして直接利用しない。利用する場合には、個人を識別できる情報等の削除及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等にし、了解を得た上で利用する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27018 の認証を取得している。</p> <ul style="list-style-type: none"> ・「開発、テストおよび運用環境の分離」(27K1:2013 A.12.1.4、27K1:2022 A.8.31、27K18:2019 12.1.4) ・「開発およびサポートプロセスにおけるセキュリティ」(27K1:2013 A.14.2、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定と管理に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.3. 守秘義務に係る 契約	① 医療情報システム 等提供に係る職員 全てとの守秘義務 に係る契約締結	①-1	医療情報を操作する可能性のある受託事業者の職員全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める。派遣従業員については守秘義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求める。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> ・「選考」(27K1:2013 A.7.1.1、27K1:2022 A.6.1) ・「雇用条件」(27K1:2013 A.7.1.2、27K1:2022 A.6.2) ・「情報セキュリティの意識向上、教育および訓練」(27K1:2013 A.7.2.2、27K1:2022 A.6.3) ・「懲戒手続」(27K1:2013 A.7.2.3、27K1:2022 A.6.4) ・「資産利用の許容範囲」(27K1:2013 A.8.1.3、27K1:2022 A.5.10) ・「秘密保持契約または守秘義務契約」(27K1:2013 A.13.2.4、27K1:2022 A.6.6) ・「リモートワーク」(27K1:2013 A.6.2.2、27K1:2022 A.6.7)
		①-2	医療情報を操作する可能性のある受託事業者の職員（派遣従業員含む）については、守秘義務に関する内容を就業規則等を含める。	
		①-3	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続を予め規定しておく。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める。	Acronis は、新規採用者に対して、現地の法律で許可される範囲で身辺調査を実施する。 情報セキュリティの監視および管理制御（Acronis の機密保持の約束、採用慣行の制御、セキュリティ意識および訓練の管理を含む）について、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等を含める。	利用規約 https://www.acronis.com/support/platform-terms-conditions/
		①-5	上記に違反した受託事業者（派遣従業員含む）の職員に対して、適切な懲戒手続を課すことを、雇用契約又は派遣契約に含めるか、就業規則等を含める。定めた懲戒手続については各職員に周知し、理解したことの確認を行う。	個人情報保護方針 https://www.acronis.com/company/privacy/
		①-6	医療情報を操作する受託事業者の職員（派遣従業員含む）に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、医療機関等と合意する。	Acronis エンドユーザライセンス契約 https://www.acronis.com/support/eula/

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② 医療機関等や再委託先との守秘義務を含めた契約の締結	②-1	医療情報システム等に係る情報及び受託した情報に関する守秘義務について、医療情報システム等提供に係る契約に含める。契約には、守秘義務に違反した受託事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。	Acronis は、クラウドプロバイダー向けの ISO/IEC 27017 規格の認証を取得している。Acronis の情報セキュリティ監視および管理制御 (Acronis の機密保持のコミットメントを含む) については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 利用規約 https://www.acronis.com/support/platform-terms-conditions/ 個人情報保護方針 https://www.acronis.com/company/privacy/ Acronis エンドユーザライセンス契約 https://www.acronis.com/support/eula/
		②-2	医療情報システム等の動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、守秘義務が課された要員・委託先等により動作確認を行う旨を含めた手順を定める。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-3	医療情報システム等の動作確認に際し、受託した個人情報をやむを得ず使用する場合について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
1.4. 教育訓練の実施	① 医療情報システム等提供に係る教育訓練の実施	①-1	医療情報を操作する可能性のある受託事業者の職員の全てに個人情報保護及び情報セキュリティに関する教育を行い、一定水準の理解を得た職員だけを業務に従事させる。	Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。 ・「情報セキュリティの意識向上、教育および訓練」(27K1:2013 A.7.2.2、27K1:2022 A.6.3) ・「組織的知識」、「能力」、「意識向上」(9001:2015 7.1.6、7.2、7.3) ・「雇用の終了後または変更後の責任」(27K1:2013 A.7.3.1、27K1:2022 A.6.5)
		①-2	派遣従業員に関しては、派遣元に対し、個人情報保護及び情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行う。	Acronis の契約社員はすべて、入社時にセキュリティ訓練を受講し、Acronis での在籍中にも継続して訓練を受講する。新規契約社員は、オリエンテーションの一環として、カスタマー情報を安全に保護する当社の献身を重視し、当社の行動規範に従うことを誓約する。特定のロールに基づいて、特定のセキュリティの側面に関する追加の訓練を受ける場合がある。例えば、情報セキュリティチームは新しいエンジニアに対して、セキュアコーディングの実践、製品設計、および自動脆弱性テストツールの使用に関するトレーニングを提供する。
		①-3	この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行う。	
		①-4	医療情報を操作する受託事業者の職員(派遣従業員含む)の退職時又は契約終了時以降の守秘義務について、教育・訓練に含める。	セキュリティ意識と訓練の管理を含む情報セキュリティの監視と管理制御については、Acronis の SOC 2 Type II 報告書のために第三者の監査人によるレビューおよび検証も行われている。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.5. 運用状況の モニタリング	① 医療情報システム 等提供に係る 閲覧・操作内容の モニタリング	①-1	受託事業者の職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改竄又は破壊等の行為が行われていないことを検証する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「情報セキュリティインシデント管理の計画および準備」(27K1:2013 A.16.1.1、27K1:2022 A.5.24) ・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) ・「情報セキュリティインシデントへの対応」(27K1:2013 A.16.1.5、27K1:2022 A.5.26) ・「情報セキュリティ事象の報告」(27K1:2013 A.16.1.2、27K1:2022 A.6.8) <p>Acronis は、システムまたはデータの機密性、完全性、可用性を損なう可能性のあるセキュリティインシデントへの対処に特化した厳格なインシデント管理プロセスを維持する。セキュリティインシデントが特定されると、Acronis のセキュリティチームはインシデントを速やかにログ記録し、重大度に応じて分類する。カスタマーに直接影響を及ぼすインシデントには最優先で対応する。このプロセスには、特定のアクション、通知およびエスカレーション手順、緩和手順、文書化手順の詳細を記載する。</p> <p>特に機密性の高いカスタマーデータを含むシステムに重点を置いた、インシデント対応計画の定期的なテストを実施している。これらのテストは、内部リスクやソフトウェアの脆弱性を含むさまざまな脅威シナリオを対象とし、チームの準備度を確認する。</p> <p>セキュリティ侵害がカスタマーのデータに関係する場合、Acronis とそのパートナーは、被害を受けたカスタマーに速やかに通知し、調査プロセスを通じて包括的なサポートを提供する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、不正アクセスを検出し、最終的に緩和措置を講じることができるよう、環境を構成、管理および保護するすべての権利と責任を保持する。</p>
		①-2	医療情報システム等の保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、医療機関等と合意する。	<p>Acronis Cyber Protect Cloud サービスは、マネージドサービスプロバイダー (MSP) と提携して提供される。MSP は、メンテナンス時にカスタマーに通知する機能を有効化できる。</p> <p>最終的なカスタマーが通知機能を利用できない場合、最終的なカスタマーは自分の運用に影響を及ぼす可能性のあるメンテナンス期間について通知を受けられるよう、自分の MSP に通知機能を有効にするように依頼する必要がある。</p>
		①-3	保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、医療機関等と合意する。	<p>詳細については、http://www.acronis.co.jp を参照のこと。</p> <p>https://kb.acronis.com/content/70368</p> <p>https://www.acronis.com/ja-jp/support/</p> <p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部分としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-4	医療情報システム等の保守業務を医療機関等の施設内で行う際の対応について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
	② 機器や媒体の 定期的な所在確認	②-1	電子媒体は台帳を作成して管理する。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証する。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「資産に対する責任」(27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「オペレーティングシステムへのソフトウェアのインストール」(ISO27K1:2013 A.12.5.1、ISO27K1:2022 A.8.19) <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のハードディスクには、保存時のデータを保護するために、フルディスク暗号化 (FDE) やドライブロック機構などの技術が組み込まれている。Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		②-2	情報を格納する機器・媒体等については、台帳管理等を行い、定期的に所在確認を行う。	
		②-3	個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。	
	③ システム構成や ソフトウェアの 動作状況に関する 内部監査の実施	③-1	システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。	<p>Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) ・「製品およびサービスの設計・開発」(9001:2015 8.3) <p>Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.6. 物理的に情報を搬送する場合の対策	① 組織外に持出する情報に対する暗号化等の対策	①-1	<p>物理的に情報を搬送する際には以下の対策を実施する。</p> <ul style="list-style-type: none"> 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択する。 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐ。 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認する。 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用する。 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さない。 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施す。 	<p>データを保管するために使用される媒体は、Acronis のデータセンター外には移転されない。</p> <p>Acronis のカスタマーに対し、初回バックアップ用の物理メディアを発送する可能性がある。このプロセスに関する詳細情報は、https://www.acronis.com/support/providers/physical-data-shipping/ を参照のこと。</p>
1.7. 解析及び第三者提供の制限	① 受託した医療情報の解析及び第三者提供の制限	①-1	受託した医療情報を保守・運用を行うために閲覧するのは必要最小限とする。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) 「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) 「ネットワークセキュリティ」(ISO27K1:2013 A.13.1.1、A.13.1.3; ISO27K1:2022 A.8.20、A.8.22) 「データ漏洩防止」(27K1:2022 8.12) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-2	①-1の閲覧が必要な場合には、緊急時を除き、システム管理者の事前・事後の承認により実施する。	
		①-3	受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。	
		①-4	①-1～①-3における閲覧に係る範囲、手順等について、医療機関等と合意する。また①-2、①-3により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-5	受託した医療情報の解析・分析は、医療情報システム等提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。	<p>該当なし。これはカスタマーの責任で対応する必要がある。カスタマーのデータは、常に契約に基づいて処理される。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/</p>
		①-6	受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。	
		①-7	受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。	<p>Acronis は、クラウドプロバイダー向けの ISO/IEC 27017 および ISO/IEC 27018 規格の認証を取得している。Acronis の情報セキュリティ監視および管理制御（Acronis の機密保持のコミットメントを含む）については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/</p>
		①-8	①-7の内容を、医療情報システム等提供に係る契約に含める。	
		①-9	医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように対応策を講じる。	
		①-10	①-9により、第三者提供（閲覧）を行う場合には、閲覧・取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応を行う。	<p>N該当なし。これはカスタマーの責任で対応する必要がある。カスタマーのデータは、常に契約に基づいて処理される。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/company/privacy/ https://www.acronis.com/support/platform-terms-conditions/ https://www.acronis.com/support/eula/</p>
		①-11	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。	
		①-12	①-7～①-11により第三者提供及びその報告を行うための条件、範囲等について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.8. 情報の破棄に係る記録の提出	① 情報の破棄に係る実施記録の取得及び医療機関等への提出	①-1	情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁・物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」（27K1:2013 A.8.3.2、27K1:2022 A.7.10） ・「装置の安全な処分または再利用」（27K1:2013 A.11.2.7、27K1:2022 A.14） ・「資産の移動」（27K1:2013 A.11.2.5、27K1:2022 A.7.10） ・「設備の保守」（27K1:2013 A.11.2.4、27K1:2022 A.13） ・「操作手順書」（27K1:2013 A.12.1.1、27K1:2022 A.5.37） <p>メディアセキュリティを含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis は、独自の消失訂正アルゴリズムを使用し、カスタマーのデータをセキュリティを保って削除するソフトウェア定義ストレージソリューションを採用している。Acronis Cyber Infrastructure のドライブや機器が故障、修理のために交換、または廃止された場合、Acronis は NIST SP 800-88rev1 に従って、ディスクからデータを消去し、機器の内部メモリから残留データを削除する措置を講じる。情報を消去（削除）できない場合、そのようなデータを読み取る（復元する）ことができないように、機器を物理的に破壊する。</p> <p>Acronis は、データセンターのコロケーション内で、現地の資格のある第三者を使用してディスクの物理的廃棄を行う。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/support/platform-terms-conditions/</p> <p>https://www.acronis.com/company/privacy/</p> <p>https://www.acronis.com/support/eula/</p>
		①-2	物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については受託事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得る。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。	
		①-3	①-1で講じる措置及び資料を提供するのに必要な条件等について、医療機関等と合意する。	
		①-4	医療情報システム等提供の停止又は医療機関等における医療情報システム等利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。	
		①-5	①-4に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.9. 再委託を行う 場合の再委託先 の管理	① 再委託を行う場合 の医療機関等への 情報提供と再委託 先の適切な監督	①-1	情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、合意を得る。また、当該再委託に係る契約において体制を明確にする。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 の認証を取得している。</p> <ul style="list-style-type: none"> ・「供給者関係」(27K1:2013 A.15、27K1:2022 A.5.19、A.5.20、A.5.21、A.5.22、27K17 15) <p>ベンダのセキュリティ慣行を含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、第三者サプライヤーをオンボーディングする前に、これらのサプライヤーが導入しているセキュリティおよびプライバシー対策の徹底的な評価を行う。この評価により、サプライヤーが契約したデータアクセスレベルと提供するサービス範囲に合致するセキュリティおよびプライバシー標準を維持していることが保証される。Acronis による第三者サプライヤーのリスク評価が行われた後、サプライヤーは、セキュリティ、機密性、およびプライバシーに関する特定の契約条件に同意することが求められる。</p> <p>Acronis のデータ保護に関する補遺は、カスタマーが復処理者の変更に興議を申し立てるための条件と手順を記載している。</p>
		①-2	再委託先には、自社と同等の個人情報保護指針等を遵守させる。	
		①-3	再委託に係る契約に、委託業務に係る守秘義務を含める。	
		①-4	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。	
		①-5	医療情報システム等の保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、医療機関等と合意する。	<p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部分としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>
		①-6	医療情報システム等の保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。	
		①-7	①-6の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 の認証を取得している。</p> <ul style="list-style-type: none"> ・「供給者関係」(27K1:2013 A.15、27K1:2022 A.5.19、A.5.20、A.5.21、A.5.22、27K17 15) <p>ベンダのセキュリティ慣行を含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、第三者サプライヤーをオンボーディングする前に、これらのサプライヤーが導入しているセキュリティおよびプライバシー対策の徹底的な評価を行う。この評価により、サプライヤーが契約したデータアクセスレベルと提供するサービス範囲に合致するセキュリティおよびプライバシー標準を維持していることが保証される。Acronis による第三者サプライヤーのリスク評価が行われた後、サプライヤーは、セキュリティ、機密性、およびプライバシーに関する特定の契約条件に同意することが求められる。</p> <p>第三者ベンダに関するリスク評価に基づき、Acronis はベンダ自体のセキュリティ状況を定期的に再評価する。</p> <p>Acronis は、カスタマーデータにアクセスする可能性のある第三者の復処理者との契約において、データ保護に関する補遺 (DPA) を含める。本 DPA は、復処理者がカスタマーデータの保護に関する Acronis のコミットメントを満たすために実施する必要があるセキュリティおよびプライバシー上の責任を明示する。</p>
		①-8	再委託先により提供される医療情報システム等の安全管理策及びサービスレベルが十分であることを確認する。	
		①-9	再委託先による医療情報システム等の実施、運用、維持について定期的に検証する。	
		①-10	再委託先による医療情報システム等の実施、運用、維持について定期的サービス実施について事前、事後報告を義務づけ、報告内容を点検確認する。	
		①-11	再委託先による医療情報システム等を実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-12	医療情報システム等の実施中に再委託先が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) 物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。
		①-13	再委託先による医療情報システム等の実施にともなう処理施設内への立ち入り手順に関しては、受託事業者の職員の入室、退室手順に ¹	
		①-14	再委託先による医療情報システム等の変更時には、引き続き安全性が維持されていることについて適切な検証を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 の認証を取得している。 ・「供給者関係」(27K1:2013 A.15、27K1:2022 A.5.19、A.5.20、A.5.21、A.5.22、27K17 15) ベンダのセキュリティ慣行を含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-15	医療情報システム等の保守点検作業を外部事業者に委託する場合には、医療情報システムの安全管理に関するガイドライン システム運用編「10. 医療情報システム・サービス事業者による保守対応等に対する安全管理措置」に従い管理策を実施する。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-16	外部事業者が医療情報システム等を実施する際は、受託事業者又は外部事業者の正規職員が管理している状況で作業を行うことが望ましい。	Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 の認証を取得している。 ・「供給者関係」(27K1:2013 A.15、27K1:2022 A.5.19、A.5.20、A.5.21、A.5.22、27K17 15) ベンダのセキュリティ慣行を含む情報セキュリティの監視および管理制御については、Acronis SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。

¹ 以降、文末切れ(000891035.pdf)

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.10. 非常時に備えた 対応	① 医療情報システム 等の提供に係る 事業影響度分析の 実施	①-1	医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」（27K1:2013 A.17.1、27K1:2022 A.5.39） ・「事業継続のための ICT 準備度」（27K1:2022 A.5.30） ・「情報のバックアップ」（27K1:2013 A.12.3.1、27K1:2022 A.8.13） ・「情報処理施設の冗長性」（27K1:2013 A.17.2.1、27K1:2022 A.8.14） <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-2	業務プロセス間の相互関係を評価する。	
		①-3	事業を継続するための業務プロセスの優先順位を明確にする。	
		①-4	医療情報システム等に発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別する。	
		①-5	医療情報システム等に発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② 医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-1	医療情報システム等の提供における医療機関等が想定する医療の継続性の観点を入れて、医療情報処理に関する事業継続計画を策定する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>事業継続計画は、オフィスとデータセンターのコロケーションの両方に対して設計され、定期的の実施される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p> <p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>
		②-2	策定した事業継続計画について模擬試験を含めた適切な方法でレビューする。	
		②-3	事業継続計画について定期的に見直しを行う。	
		②-4	<p>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。</p> <ul style="list-style-type: none"> ・ 事前準備計画 ・ 「非常時」判断手順 ・ 関係者の召集、対応本部の設置 ・ 機器及び作業員の縮退措置及び代替施設の手配措置 ・ バックアップ施設等、代替施設への切替え措置 ・ 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） ・ 障害の拡大範囲に関する判断手順、基準 ・ 正常復帰の判断手順、基準 ・ 正常復帰後の医療情報システム等の点検手順（不正侵入、情報改竄、情報破損等の検出等） ・ 所管官庁への連絡体制、等。 	
		②-5	策定した事業継続計画に基づくサービス内容について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	③ 医療情報システム 等復旧後における 整合性確保	③-1	非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の規定等）を講じる。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」（27K1:2013 A.17.1、27K1:2022 A.5.39） ・「事業継続のための ICT 準備度」（27K1:2022 A.5.30） ・「情報のバックアップ」（27K1:2013 A.12.3.1、27K1:2022 A.8.13） ・「情報処理施設の冗長性」（27K1:2013 A.17.2.1、27K1:2022 A.8.14） <p>Acronis Cyber Protect Cloud を使用するカスタマーは、事業継続およびディザスタリカバリ戦略の策定を含む、環境の設定および管理に関するすべての権利と責任を保持する。</p>
	④ 非常時用の利用者 アカウントや 機能の管理手順の 策定	④-1	非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」（27K1:2013 A.17.1、27K1:2022 A.5.39） ・「事業継続のための ICT 準備度」（27K1:2022 A.5.30） ・「情報のバックアップ」（27K1:2013 A.12.3.1、27K1:2022 A.8.13） ・「情報処理施設の冗長性」（27K1:2013 A.17.2.1、27K1:2022 A.8.14） <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		④-2	非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。	
		④-3	非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。	
		④-4	非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.11. サイバー攻撃等 による障害発生 時の対応	① サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-1	サイバー攻撃等により、サービスの提供に支障が生じた場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「情報セキュリティインシデント管理の計画および準備」（27K1:2013 A.16.1.1、27K1:2022 A.5.24） ・「情報セキュリティ事象の評価および決定」（27K1:2013 A.16.1.4、27K1:2022 A.5.25） ・「情報セキュリティインシデントへの対応」（27K1:2013 A.16.1.5、27K1:2022 A.5.26） ・「情報セキュリティ事象の報告」（27K1:2013 A.16.1.2、27K1:2022 A.6.8） <p>インシデント管理手順を含む情報セキュリティの監視および管理コントロールについては、Acronis の SOC 2 Type II 報告書のために第三者監査人によってレビューおよび検証されている。</p> <p>Acronis は、システムまたはデータの機密性、完全性、可用性を損なう可能性のあるセキュリティインシデントへの対処に特化した厳格なインシデント管理プロセスを維持する。セキュリティインシデントが特定されると、Acronis のセキュリティチームはインシデントを速やかにログ記録し、重大度に応じて分類する。カスタマーに直接影響を及ぼすインシデントには最優先で対応する。このプロセスには、特定のアクション、通知およびエスカレーション手順、緩和手順、文書化手順の詳細を記載する。</p> <p>特に機密性の高いカスタマーデータを含むシステムに重点を置いた、インシデント対応計画の定期的なテストを実施している。これらのテストは、内部リスクやソフトウェアの脆弱性を含むさまざまな脅威シナリオを対象とし、チームの準備度を確認する。</p> <p>セキュリティ侵害がカスタマーのデータに関係する場合、Acronis とそのパートナーは、被害を受けたカスタマーに速やかに通知し、調査プロセスを通じて包括的なサポートを提供する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
	② サイバー攻撃等による原因調査のためのログ等の記録の保全	①-2	サイバー攻撃等により、サービスの提供に支障が生じた場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、医療機関と合意する。サイバー攻撃、その他医療機関等における危機管理対応時において、対象事業者が医療機関等と医療情報システム等に関して委託契約を締結している場合、対象事業者は、医療機関等への危機管理対応内容に応じて構築すべき体制（事業者内の危機対応体制の構築の要否や責任者等）やその内容（情報提供方法、役割分担の設定の必要性の判断等）等を運用管理規程に定める。	
		①-3	医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバストレージ等は国内法の執行が及ぶ場所に設置する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「ログ取得」（27K1:2013 A.12.4、27K1:2022 A.8.15） ・「監視活動」（27K1:2022 A.8.16） <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
	② サイバー攻撃等による原因調査のためのログ等の記録の保全	②-1	サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「ログ取得」（27K1:2013 A.12.4、27K1:2022 A.8.15） ・「監視活動」（27K1:2022 A.8.16） <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
1.12. ネットワーク上の 責任範囲・役割 の合意	① 外部と医療情報を 交換する際の責任 範囲・役割の合意	①-1	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「マルウェアからの保護」(27K1:2013 A.12.2、27K1:2022 A.8.7) ・「監視活動」(27K1:2022 A.8.16) ・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) ・「情報セキュリティインシデントへの対応」(27K1:2013 A.16.1.5、27K1:2022 A.5.26) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p>
		①-2	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	
		①-3	ネットワークで用いられる医療機関等の施設内のルータについて、これを經由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関する受託事業者の役割分担について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>このデータを保管または処理するシステムへのアクセスは、最小特権の原則に従って付与される。システムやネットワークデバイスへのアクセスには、ユーザ ID、パスワード、セキュリティキー、および/または証明書による認証が必要となる。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-4	回線の管理、品質等に対する受託事業者の管理責任の所在や管理方法について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「通信セキュリティ」(27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6) ・「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(27K1:2013 A.14.1.2、27K1:2022 A.8.26) <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-5	通常運用時及び非常時の医療機関等と受託事業者との起点から終点までの通信手順、その他医療情報システムの安全管理に関するガイドライン システム運用編「13. ネットワークに関する安全管理措置」に定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、受託事業者の負う管理責任の所在や管理方法について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「通信セキュリティ」(27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6) ・「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(27K1:2013 A.14.1.2、27K1:2022 A.8.26) <p>Acronis の ISO/IEC 27017 および ISO/IEC 27018 規格の認証は、クラウドサービスのセキュリティとクラウドに送信する個人情報の安全な取り扱いに対する Acronis のコミットメントを保証する。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/support/platform-terms-conditions/</p> <p>https://www.acronis.com/company/privacy/</p> <p>https://www.acronis.com/support/eula/</p>
		①-6	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	
		①-7	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う管理責任の所在や管理方法について、医療機関等と合意する。	<p>カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。</p>
		①-8	サービスにより管理する医療情報を患者等の閲覧に供する場合に、受託事業者において対応すべきセキュリティ上の措置の条件、内容等について、医療機関等と合意する。	<p>該当なし。これはカスタマーの責任で対応する必要がある。</p>
		①-9	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「通信セキュリティ」(27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6) ・「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(27K1:2013 A.14.1.2、27K1:2022 A.8.26) <p>Acronis の ISO/IEC 27017 および ISO/IEC 27018 規格の認証は、クラウドサービスのセキュリティとクラウドに送信する個人情報の安全な取り扱いに対する Acronis のコミットメントを保証する。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/support/platform-terms-conditions/</p> <p>https://www.acronis.com/company/privacy/</p> <p>https://www.acronis.com/support/eula/</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-10	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う管理責任の所在や管理方法について、医療機関等と合意する。	カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。
1.13. 機器・ソフトウェアの品質管理	① 医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-1	医療情報システム等における機器及びソフトウェアの構成図を作成する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) ・「資産に対する責任」(27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。
		①-2	医療情報システム等のネットワーク構成図を作成する。	
		①-3	①-1、①-2で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。	
		①-4	医療情報システム等を構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。	
		①-5	①-1～①-4で策定した資料等を医療機関等の求めに応じて提出することについて、開示内容、範囲、条件等を医療機関等と合意する。	
	② 機器・ソフトウェアの導入や変更における事前検証の実施	②-1	保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行う。	Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。 ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) ・「製品およびサービスの設計・開発」(9001:2015 8.3) Acronis は、設計から配置に至るまで、複数のソフトウェアセキュリティチェックを保証するためにセキュリティ開発ライフサイクル (SDLC) を確立している。独立したセキュリティ研究者を参加させるべく脆弱性報奨金制度を実施している。 変更管理およびソフトウェア開発を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。
		②-2	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため影響を最小限に抑える方策	
		②-3	情報処理に供するアプリケーションについては、受託事業者自身で開発したアプリケーションを用いる。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いる。	
		②-4	ソフトウェアに不正プログラムが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施することが望ましい。	
		②-5	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	③ 本番環境と 開発環境の分離	③-1	ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。	<p>Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「開発環境、試験環境および運用環境の分離」(27K1:2013 A.12.1.4、27K1:2022 A.8.31) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.31、A.8.32) ・「製品およびサービスの設計・開発」(9001:2015 8.3) <p>Acronis は、設計から配置に至るまで、複数のソフトウェアセキュリティチェックを保証するためにセキュリティ開発ライフサイクル (SDLC) を確立している。独立したセキュリティ研究者を参加させるべく脆弱性報奨金制度を実施している。</p> <p>変更管理およびソフトウェア開発を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		③-2	開発施設では不正プログラムが混入することを避けるため、不特定多数が利用するネットワーク (インターネット等) と接続を持つ場合には不正プログラムへの対策を行う。	
		③-3	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしない。	
		③-4	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かない。	
		③-5	情報処理に不必要なファイル等を運用システム上におかない。	
1.14. 変化に伴う 医療機関等への 影響の最小化	① 医療情報システム 等に用いる機器や ソフトウェアの サポート	①-1	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自社の事業継続およびディザスタリカバリ戦略に従って、自社のデータを保管する場所を単独で選択する責任を負う。利用可能な場合、地理的冗長性の追加サービスを有効化できる。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-2	受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合 (媒体の劣化、読取装置等のサポート切れ等)、速やかに代替的な措置を講じ、見読性確保のための対応を行う。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-3	それぞれの装置は製造元又は供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) <p>メディアセキュリティを含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p>
		①-4	情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。	<p>Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) ・「製品およびサービスの設計・開発」(9001:2015 8.3) <p>変更管理およびソフトウェア開発を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-5	医療情報システム等について、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。	<p>契約上の責任および合意事項に関する Acronis のプラットフォームサービス契約条件詳細については、https://www.acronis.com/en-us/support/platform-terms-conditions/ の第 14 および 15 条を参照のこと。</p>
		①-6	医療情報システム等について、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	
		①-7	①-6においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② 保守作業に伴う 医療情報システム 等停止時間の 最小化	②-1	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・「資産の移動」(27K1:2013 A.11.2.5、27K1:2022 A.7.10) ・「設備の保守」(27K1:2013 A.11.2.4、27K1:2022 A.13) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>システムの可用性およびインテグリティに関連する制御を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p>
		②-2	保守業務における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。	
		②-3	保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。	
		②-4	②-3に定めた手順を医療機関等に示し、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、医療機関等と合意する。	
		②-5	②-3で示された手順について、医療機関等が対応すべき事項がある場合、医療機関等と合意する。	
	③ 医療情報システム 等の停止や 仕様変更時の対応	③-1	サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、医療情報システム等を利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	<p>契約上の責任および合意事項に関する Acronis のプラットフォームサービス契約条件詳細については、https://www.acronis.com/en-us/support/platform-terms-conditions/ の第 14 および 15 条を参照のこと。</p>
		③-2	③-1の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式）、返却方法、条件については、医療機関等と合意する。また医療機関等のサービス利用開始後に、医療機関等と合意した内容を変更する場合には、③-1に準じた対応策を講じる。	
				<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「資産の返却」(27K1:2013 A.8.1.4、27K1:2022 A.5.11) ・「クラウドサービスのカスタマー資産の移動」(27K17:2015 CLD.8.1.5) <p>契約上の責任および合意事項に関する Acronis のプラットフォームサービス契約条件詳細は、https://www.acronis.com/support/platform-terms-conditions/ 第 9.7 条を参照のこと。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		③-3	③-2におけるデータの返却については、医療情報システムの安全管理に関するガイドライン システム運用編「5. 1 医療情報システム等における情報の相互運用性と標準化の重要性」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、受託事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、医療機関等と合意する。	
		③-4	③-1においてサービスの変更を含む医療情報システム等の一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、③-2の対応は除く）、条件等について、医療機関等と合意する。	
		③-5	医療機関等の都合により医療機関等の医療情報システム等利用が終了する場合も、③-2、③-3に示す対応策を講じる。	
		③-6	③-1～③-5についての手順等を、運用管理規程等に含める。	
2. 物理的対策				
2.1. 入退管理	① 機器や媒体の 設置場所への 認証や入退管理	①-1	機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） <p>物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis のデータセンターのセキュリティ体制についての詳細は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		①-2	機器や媒体の設置場所については、許可された者のみが入退できるように制限する。	
		①-3	医療情報システム等を設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行う。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-4	有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用する。	
		①-5	有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認する。	
		①-6	受託事業者の職員の業務に応じて執務室内に滞在できる時間を指定する。	
		①-7	機械式の認証装置で利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号 (PIN)、パスワード等の記憶要素、生体情報 (バイオメトリクス) 等を組み合わせることが望ましい。	
		①-8	機器や媒体の設置場所への入退状況の管理 (入退記録のレビュー含む) は定期的に行う。	
2.2. 施錠管理・ 鍵管理	① サーバラックや キャビネットの 施錠管理・鍵管理	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境 (専有サーバ、仮想プライベートサーバ等) を利用する場合においても、同等の措置がとられていることを確認する。 ・ 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・ 「物理的および環境的セキュリティ」 (27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) ・ 「機器の設置および保護」 (27K1:2022 A.11.2.1、27K1:2022 A.7.8) ・ 「資産に対する責任」 (27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) 共有データセンターの物理的セキュリティは、各データセンター施設と責任を共有する。
		①-2	機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。	Acronis は、世界中で多数の共有データセンター施設を運用するパートナーシップを確立している。これらの施設は、設備、電力、冷却に関する厳格な基準とコンプライアンス要件に適合している。この手法により、最適な条件とアップタイムを維持し、ミッションクリティカルなデータを保護する。Acronis はさらに、最も一般的な障害事象の発生率を低下または排除するために、データセンターの設置場所に厳格な要件を設けている。Acronis は各契約期間中、第三者のセキュリティ制御、サービス提供、契約要件の遵守の定期的な監視およびレビューを行う。
		①-3	サーバ等を格納するラック等について、施錠管理を行う。	物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。
		①-4	媒体等を格納するキャビネット等について、施錠管理を行う。	Acronis のデータセンター のセキュリティポリシーについての詳細は、 https://www.acronis.com/trust-center/ を参照のこと。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-5	電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) ・「機器の設置および保護」(27K1:2022 A.11.2.1、27K1:2022 A.7.8) ・「資産に対する責任」(27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) <p>共有データセンターの物理的セキュリティは、各データセンター施設と責任を共有する。</p> <p>Acronis は、世界中で多数の共有データセンター施設を運用するパートナーシップを確立している。これらの施設は、設備、電力、冷却に関する厳格な基準とコンプライアンス要件に適合している。この手法により、最適な条件とアップタイムを維持し、ミッションクリティカルなデータを保護する。Acronis はさらに、最も一般的な障害事象の発生率を低下または排除するために、データセンターの設置場所に厳格な要件を設けている。Acronis は各契約期間中、第三者のセキュリティ制御、サービス提供、契約要件の遵守の定期的な監視およびレビューを行う。</p> <p>物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis のデータセンター のセキュリティポリシーについての詳細は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		①-6	データセンターを運営する外部事業者が、自社専有の建物と同等な安全管理策を実施する等、受託事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認する。	
		①-7	医療情報システム等の設置されるサーバラックには施錠を行い、定められた受託事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行う。	
		①-8	受託事業者が医療情報システム等の設置されるサーバラックを解錠して行う作業については、作業者、作業開始時刻、作業終了時刻、作業内容等について記録する。	
		①-9	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム等、医療情報に影響を与えないことを確認する。	
		①-10	医療情報システム等であることが、同じデータセンター内に立ち入る他事業者にはわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしない。	
		①-11	医療情報システム等の設置されるサーバラックの施錠装置については、ハードウェアトークン又は ICカード等の認証デバイス、暗証番号 (PIN)、パスワード等の記憶要素、生体情報 (バイオメトリクス) 等を組み合わせることが望ましい。	
		①-12	受託事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認する。	
		①-13	機器や媒体の保存場所 (ラック、保管庫含む) の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。	
		①-14	①-1～①-13につき、運用管理規程等に規定する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
2.3. 不正な侵入の 監視	① 防犯カメラ等によ る医療情報を処理 する施設内への 侵入監視	①-1	<p>受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。</p> <ul style="list-style-type: none"> ・ 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施す。 ・ 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入する。 	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） <p>物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis のデータセンターのセキュリティ体制についての詳細は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		①-2	防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。	
		①-3	機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がいないことを確認する。	
		①-4	サービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視を行う。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② 受託事業者の 職員に対する 職員証等の着用の 義務付け	②-1	受託事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した受託事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、受託事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) 「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) 「事業継続のための ICT 準備度」(27K1:2022 A.5.30) 「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) 「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) 事業継続慣行と物理セキュリティ管理を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。
		②-2	受託事業者の職員は、受託事業者の専有する領域にて、受託事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認する。	Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。 Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自身の事業継続およびディザスタリカバリ戦略に従って、自分のデータを保管する場所を単独で選択する責任を負う。利用可能な場合、地理的冗長性の追加サービスを有効化できる。
		②-3	職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、受託事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行う。	Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。 Acronis のデータセンターのセキュリティ体制についての詳細は、 https://www.acronis.com/trust-center/ を参照のこと。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
2.4. バックアップ施設 における対策	① バックアップ施設 に対する物理的 安全対策の実施	①-1	医療機関等に提供する医療情報システム等の継続に必要であれば、受託する医療情報のバックアップ施設等、医療情報システム等を継続するための代替情報処理施設を設置し、それらの施設に対しても物理的安全対策を施す。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) 「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) 「事業継続のための ICT 準備度」(27K1:2022 A.5.30) 「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) 「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行と物理セキュリティ管理を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自身の事業継続およびディザスタリカバリ戦略に従って、自分のデータを保管する場所を単独で選択する責任を負う。利用可能な場合、地理的冗長性の追加サービスを有効化できる。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p> <p>Acronis のデータセンターのセキュリティ体制についての詳細は、 https://www.acronis.com/trust-center/ を参照のこと。</p>
2.5. 個人所有物の 持ち込み制限	① 医療情報を処理 する施設内への 個人所有物の 持ち込み制限	①-1	医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを制限する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) 「構外にある機器および資産のセキュリティ」(27K1:2013 A.11.2.6、27K1:2022 A.7.9) 「資産利用の許容範囲」(27K1:2013 A.8.1.3、27K1:2022 A.5.10)
		①-2	機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。	<p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
2.6. 機器の盗難への対策	① 重要な機器への盗難防止用チェーン等の取付	①-1	個人情報が存在するPC 等の重要な機器には、盗難防止用チェーン等を取り付ける。	<p>Acronis is certified to the ISO/IEC 27001 Standard, which regulates:</p> <p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） ・「構外にある機器および資産のセキュリティ」（27K1:2013 A.11.2.6、27K1:2022 A.7.9） ・「資産利用の許容範囲」（27K1:2013 A.8.1.3、27K1:2022 A.5.10） <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
2.7. 覗き見への対策	① 覗き見防止対策	①-1	医療情報等が表示される端末画面等がアクセス権限の無いものが視野に入らないような対応（室内の機器レイアウト等）を行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） ・「構外にある機器および資産のセキュリティ」（27K1:2013 A.11.2.6、27K1:2022 A.7.9） ・「資産利用の許容範囲」（27K1:2013 A.8.1.3、27K1:2022 A.5.10） <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p>
		①-2	個人情報の表示中の覗き見を予防するために、端末に覗き見対策のシートを貼る等の対策を行う。	<p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
2.8. 災害等への対策	① 地震、水害、落雷、 火災等、及び、 それに伴う停電等 への対策	①-1	機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等、及び、それに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） <p>共有データセンターの物理的セキュリティは、各データセンター施設と責任を共有する。</p> <p>Acronis は、世界中で多数の共有データセンター施設を運用するパートナーシップを確立している。これらの施設は、設備、電力、冷却に関する厳格な基準とコンプライアンス要件に適合している。この手法により、最適な条件とアップタイムを維持し、ミッションクリティカルなデータを保護する。Acronis はさらに、最も一般的な障害事象の発生率を低下または排除するために、データセンターの設置場所に厳格な要件を設けている。Acronis は各契約期間中、第三者のセキュリティ制御、サービス提供、契約要件の遵守の定期的な監視およびレビューを行う。</p> <p>物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis のデータセンターのセキュリティ体制についての詳細は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		①-2	①-1の施設を設置する建築物について、医療機関等と合意する。	
		①-3	火災発生時の消火設備が機器に損傷を与えないよう配慮する。	
		①-4	医療情報システム等を配置する室内での喫煙、飲食を禁止する。	
		①-5	医療情報システム等を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮する。	
		①-6	<p>医療情報システム等を設置するサーバラックについては以下の安全管理策を実施する。</p> <ul style="list-style-type: none"> ・震災時に転倒することが無いよう確実に設置する。 ・熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されている。 ・扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。 	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3. 技術的対策				
3.1. 利用者認証の 実装	① 利用者を一意に 識別する方式の 採用	①-1	医療情報システム等にて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は厳格に職務分掌し、ロールベースで特権アクセスを付与しており、Acronis の従業員はカスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-2	医療情報システム等の利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者によるIDの共同利用は行わない。ただし当該医療情報システム等が他の医療情報システム等を利用するためのID (noninteractive ID) は除く）。	
		①-3	利用者のなりすまし等を防止するための認証を行う。	
		①-4	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行う。	
	② 一時的な 認証手段の用意	②-1	利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		②-2	代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。	
		②-3	代替的手段・手順により、医療情報システム等利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。	
		②-4	その他、一時的な利用者の認証方法について医療機関等と合意する。	
	③ 長時間離席時の 対策	③-1	離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐ。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「無人状態にある利用者装置」(27K1:2013 A.11.2.8、27K1:2022 A.8.1) ・「データ漏洩防止」(27K1:2022 8.12) <p>Acronis は、資産利用の許容範囲に関する特定のポリシーと手順を策定し、従業員に対して、デスクや画面上に機密データを保管せず、退席時には端末をロックするように義務付けている。一定期間アクティビティがないとユーザのマシンをブロックする技術的な対策が実装されている。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		③-2	サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。	<ul style="list-style-type: none"> Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 「クリアデスクおよびクリアスクリーン」(27K1:2013 A.11.2.9、27K1:2022 A.7.7) 「データ漏洩防止」(27K1:2022 8.12)
		③-3	医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「クリアデスクおよびクリアスクリーン」(27K1:2013 A.11.2.9、27K1:2022 A.7.7) 「データ漏洩防止」(27K1:2022 8.12) <p>Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、運用手順やガイドラインの策定を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		③-4	端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「無人状態にある利用者装置」(27K1:2013 A.11.2.8、27K1:2022 A.8.1) 「データ漏洩防止」(27K1:2022 8.12)
		③-5	離席の場合のクローズ処理の具体的な適用について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「無人状態にある利用者装置」(27K1:2013 A.11.2.8、27K1:2022 A.8.1) 「データ漏洩防止」(27K1:2022 8.12) <p>Acronis は、エンドユーザのコンピューターに対して、非アクティブ状態が 15 分間続いた後にトリガされるパスワード保護されたスクリーンセーバーの形で、セッションロックを実装している。このスクリーンセーバーは、ユーザがコンピューターに再度サインインするまでロックされたままとなる。さらに、Acronis は、中間者攻撃やアイドル状態のセッションの乗っ取りを効果的に阻止するべく、本番環境への接続に暗号化セッションを適用している。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	④ 安全なパスワード 要件の定義	④-1	パスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とする。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17) ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「アイデンティティ管理」(27K1:2013 A.9.2.1、27K1:2022 A.5.16) ・「認証情報」(27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「セキュリティ保護された認証」(27K1:2013 A.9.4.2、27K1:2022 A.8.5) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis の従業員のパスワードは、脆弱なパスワードや漏洩したパスワードを発見するために、定期的に自動ツールで監査される。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis のカスタマーのパスワードが漏洩した証拠を検出するために、脅威インテリジェンスシステムが実行されている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		④-2	パスワードポリシーについて、医療機関等と合意する。	
		④-3	パスワードには有効期限の設定を行い、定期的な変更を強制する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。	
		④-4	パスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。	
		④-5	パスワード発行時には、乱数から生成した仮の医療情報システム等へのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施する。	
		④-6	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう利用者に徹底する。	
		④-7	利用者がパスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、利用者が設定しようとする品質の低いパスワードを認めないシステムの導入等を行う。	
		④-8	本人の識別・認証に用いる情報は、本人しか知り得ない状態に保つよう対策を行う。	
		④-9	利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと医療情報システム等にアクセスできないようにする。	
		④-10	初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。	
		④-11	パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		④-12	利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」（27K1:2013 A.9.4.3、27K1:2022 A.5.17） ・「アクセス制御」（27K1:2013 A.9.1、27K1:2022 A.5.15） ・「アイデンティティ管理」（27K1:2013 A.9.2.1、27K1:2022 A.5.16） ・「認証情報」（27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17） ・「アクセス権」（27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18） ・「セキュリティ保護された認証」（27K1:2013 A.9.4.2、27K1:2022 A.8.5） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis の従業員のパスワードは、脆弱なパスワードや漏洩したパスワードを発見するために、定期的に自動ツールで監査される。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis のカスタマーのパスワードが漏洩した証拠を検出するために、脅威インテリジェンスシステムが実行されている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		④-13	パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とする。	
		④-14	パスワード入力不成功に終わった場合の再入力に対して一定の不応時間を設定する。連続してログオンが失敗した場合は再入力を一定期間受けつけない機構とする。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入する。	
	⑤ 多要素認証方式の採用	⑤-1	ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号 (PIN) 又はパスワード等の記憶要素、生体情報 (バイオメトリクス) 等を組み合わせた多要素認証とすることが望ましい。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」（27K1:2013 A.9.4.3、27K1:2022 A.5.17） ・「アクセス制御」（27K1:2013 A.9.1、27K1:2022 A.5.15） ・「アイデンティティ管理」（27K1:2013 A.9.2.1、27K1:2022 A.5.16） ・「認証情報」（27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17） ・「アクセス権」（27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18） ・「セキュリティ保護された認証」（27K1:2013 A.9.4.2、27K1:2022 A.8.5） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		⑤-2	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、多要素認証とする。	
		⑤-3	利用者の認証で採用する認証方式について、医療機関等と合意する。	
		⑤-4	利用者の認証において、ID・パスワードによる認証方式を採用している場合には、ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、医療情報システムの安全管理に関するガイドラインにおいては、同ガイドライン 第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.2. アクセス権限の 管理.	① 必要最小限と なるような アクセス権限の 管理	①-1	医療情報システム等の操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、閲覧、編集、削除等を防止する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17) ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「アイデンティティ管理」(27K1:2013 A.9.2.1、27K1:2022 A.5.16) ・「認証情報」(27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「セキュリティ保護された認証」(27K1:2013 A.9.4.2、27K1:2022 A.8.5) ・「情報セキュリティの独立したレビュー」(27K1:2013 A.18.2.1、27K1:2022 A.5.35) ・「情報の分類」(27K1:2013 A.8.2.1、27K1:2022 A.5.12) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与している。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-2	医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。	
		①-3	医療情報システム等の構成要素（情報処理装置、ソフトウェア）それぞれのアクセス管理に係るセキュリティ要求事項を整理する。	
		①-4	それぞれの情報にアクセスする権限を持つ利用者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行う。	
		①-5	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定する。	
		①-6	定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。	
		①-7	予定された保守・運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。	
		①-8	システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。	
	② 医療情報に対する アクセス制御	②-1	医療情報とそれ以外の情報を区分できる措置を講じる。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-2	医療情報については、情報区分に従ってアクセス制御を行えるようにする。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-3	仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-4	医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.3. ID・パスワードの 管理	① 利用者アクセス 及びIDの管理・ 運用	①-1	利用者は医療情報システム等上においてユニークな利用者ごとのIDにより識別する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17) ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「アイデンティティ管理」(27K1:2013 A.9.2.1、27K1:2022 A.5.16) ・「認証情報」(27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「セキュリティ保護された認証」(27K1:2013 A.9.4.2、27K1:2022 A.8.5) ・「情報セキュリティの独立したレビュー」(27K1:2013 A.18.2.1、27K1:2022 A.5.35) ・「情報の分類」(27K1:2013 A.8.2.1、27K1:2022 A.5.12) ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) ・「特権的なユーティリティプログラムの使用」(27K1:2013 A.9.4.4、27K1:2022 A.8.18) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		①-2	利用者のIDを発行する際に、既存のIDとの重複を排除する仕組みを導入する。	
		①-3	複数利用者で共用するためのグループIDの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、利用者ごとのIDでログオンしてからグループIDに変更する仕組みを利用する。	
		①-4	利用者のIDの発行は医療情報システム等の管理に必要な最小限の人数に留める。	
		①-5	監視ログの監査時に利用者を実際に特定するため、利用者のIDは過去に使われたものを再利用しない。	
		①-6	アクセスを許可された利用者のIDによるアクセス可能範囲が許可された通りとなっていること(不正に変更されていないこと)を定期的に確認することが望ましい。	
		①-7	不正なアカウントの利用又は試みが行われたことを利用者自身で検出するため、利用者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗 ¹	
		①-8	不正なアカウントの利用を防ぐため、利用者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。	
		①-9	認可されていない利用者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると当該IDが存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。	
		①-10	緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。	
		①-11	医療情報システム等に許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知する。	

¹ 以降、文末切れ(000891035.pdf)

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-12	利用者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とする。	
		①-13	不要な利用者の ID が残っていないことを定期的に確認する。	
	② 特権IDの最小限の利用及び作業実施内容の記録	②-1	特権 ID の発行は必要な最小限のものに留める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17) ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「アイデンティティ管理」(27K1:2013 A.9.2.1、27K1:2022 A.5.16) ・「認証情報」(27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「セキュリティ保護された認証」(27K1:2013 A.9.4.2、27K1:2022 A.8.5) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>
		②-2	特権使用者に昇格可能な利用者の ID を制限する。	
		②-3	特権の使用時には作業実施内容を記録する。	
		②-4	管理端末以外からの特権 ID による直接ログオンを禁止する。	
		②-5	特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限することが望ましい。	
		②-6	医療情報システム等の機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改竄、削除など不正な行為を防止することが望ましい。	
	③ パスワードの管理・運用	③-1	各利用者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17) ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「アイデンティティ管理」(27K1:2013 A.9.2.1、27K1:2022 A.5.16) ・「認証情報」(27K1:2013 A.9.2.4、A.9.3.1、A.9.4.3; 27K1:2022 A.5.17) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「セキュリティ保護された認証」(27K1:2013 A.9.4.2、27K1:2022 A.8.5) <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、厳格な職務分掌を維持し、ゼロトラストインフラストラクチャを介して、必須の多要素認証方式を使用し、ロールベースで特権アクセスを付与する。</p> <p>Acronis Cyber Protect Cloud では、ユーザが多要素認証を設定できるが、ユーザが必要に応じて有効にする責任を負う。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		⑤-2	医療情報システム等及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等の棚卸を行い、必要のないアカウントに ¹	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「設定管理」(27K1:2022 A.8.9) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		⑤-3	パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「パスワード管理システム」(27K1:2013 A.9.4.3、27K1:2022 A.5.17)
		⑤-4	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用する。また、一般の作業による閲覧を制限する。	・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		⑤-5	パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。 ・「情報セキュリティインシデント管理の計画および準備」(27K1:2013 A.16.1.1、27K1:2022 A.5.24)
		⑤-6	パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。	・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) ・「情報セキュリティインシデントへの対応」(27K1:2013 A.16.1.5、27K1:2022 A.5.26) ・「情報セキュリティ事象の報告」(27K1:2013 A.16.1.2、27K1:2022 A.6.8) Acronis は、システムまたはデータの機密性、完全性、可用性を損なう可能性のあるセキュリティインシデントへの対処に特化した厳格なインシデント管理プロセスを維持する。セキュリティインシデントが特定されると、Acronis のセキュリティチームはインシデントを速やかにログ記録し、重大度に応じて分類する。カスタマーに直接影響を及ぼすインシデントには最優先で対応する。このプロセスには、特定のアクション、通知およびエスカレーション手順、緩和手順、文書化手順の詳細を記載する。 特に機密性の高いカスタマーデータを含むシステムに重点を置いた、インシデント対応計画の定期的なテストを実施している。これらのテストは、内部リスクやソフトウェアの脆弱性を含むさまざまな脅威シナリオを対象とし、チームの準備度を確認する。 セキュリティ侵害がカスタマーのデータに関係する場合、Acronis とそのパートナーは、被害を受けたカスタマーに速やかに通知し、調査プロセスを通じて包括的なサポートを提供する。 Acronis Cyber Protect Cloud を使用するカスタマーは、不正アクセスを検出し、最終的に緩和措置を講じることができるよう、環境を構成、管理および保護するすべての権利と責任を保持する。

¹ 以降、文末切れ(000891035.pdf)

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.4. ログの取得と 検証	① ログの取得と検証	①-1	利用者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録したログを作成し、一定期間保存する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) <p>論理アクセス制御、ログ取得、監視を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、侵入試行およびその他のセキュリティ関連イベントを特定するために、独自のセキュリティ情報およびイベント管理システムを使用し、監査ログを継続的に監視している。事前に定義されたしきい値に基づいて、さらなる調査のためにセキュリティアラートが生成される。これらの監視ツールは、セキュリティ担当者に自動的にアラートを発する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、ログ管理や監視活動を含む環境の設定、管理、保護に関するすべての権利と責任を保持する。</p>
		①-2	ログを定期的に検証して不正な行為、システムの異常等を検出する。	
		①-3	<p>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。</p> <ul style="list-style-type: none"> ・ 利用者情報（利用者の ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス） ・ ファイル及びデータへのアクセス、変更、削除記録（利用者の ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） ・ データベース操作記録（利用者の ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）修正パッチの適用作業（利用者の ID、変更されたファイル） ・ 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容） ・ システム起動、停止イベント ・ ログ取得機能の開始、終了イベント外部デバイスの取り外し ・ IDS・IPS 等のセキュリティ装置のイベントログ <p>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）</p>	
		①-4	ログを集中させ問題の検出を一箇所で確実にを行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理する。	
		①-5	運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得する。	
		①-6	システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証拠とするためにログを取得する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-7	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) <p>論理アクセス制御、ログ取得、監視を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、侵入試行およびその他のセキュリティ関連イベントを特定するために、独自のセキュリティ情報およびイベント管理システムを使用し、監査ログを継続的に監視している。事前に定義されたしきい値に基づいて、さらなる調査のためにセキュリティアラートが生成される。これらの監視ツールは、セキュリティ担当者に自動的にアラートを発する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やアクティビティの監視を含む環境の構成、管理、保護に関するすべての権利と責任を保持する。</p>
		①-8	①-7に関する情報の医療機関等への提供について、医療機関等と合意する。	
		①-9	ログの取得機能を有しない場合には、医療機関等と合意する。	
		①-10	医療情報システム等の保守に従事する者及び管理者権限を有する者が、その業務の目的で当該医療情報システム等にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。	
		①-11	①-10で定めるアカウントで行った作業等は、アクセスした個人情報 that 特定できる形で、ログ等により記録し、保存する。	
		①-12	医療情報システム等の保守において実施した操作結果について、操作ログ等により記録し、管理する。	
		①-13	取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。	
		①-14	ログを検証するため、利用者がアクセスした医療情報等を迅速に確認できるよう、利用者のIDと、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「特権的なユーティリティプログラムの使用」(27K1:2013 A.9.4.4、27K1:2022 A.8.18) <p>論理アクセス制御、ログ取得、監視を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、侵入試行およびその他のセキュリティ関連イベントを特定するために、独自のセキュリティ情報およびイベント管理システムを使用し、監査ログを継続的に監視している。事前に定義されたしきい値に基づいて、さらなる調査のためにセキュリティアラートが生成される。これらの監視ツールは、セキュリティ担当者に自動的にアラートを発する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やアクティビティの監視を含む環境の構成、管理、保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② ログの改竄や 削除を防止する ためのアクセス 制限や外部保存	②-1	<p>ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用する。</p> <ul style="list-style-type: none"> ・ ログデータにアクセスする利用者及び操作を制限する。 ・ 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとる。 ・ ログデータに対する不正な改竄及び削除行為に対する検出・防止策を施す。 	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・ 「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・ 「監視活動」(27K1:2022 A.8.16) ・ 「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・ 「特権的なユーティリティプログラムの使用」(27K1:2013 A.9.4.4、27K1:2022 A.8.18) <p>論理アクセス制御、ログ取得、監視を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、侵入試行およびその他のセキュリティ関連イベントを特定するために、独自のセキュリティ情報およびイベント管理システムを使用し、監査ログを継続的に監視している。事前に定義されたしきい値に基づいて、さらなる調査のためにセキュリティアラートが生成される。これらの監視ツールは、セキュリティ担当者に自動的にアラートを発する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やアクティビティの監視を含む環境の構成、管理、保護に関するすべての権利と責任を保持する。</p>
	③ 時刻の 標準時刻への同期	③-1	<p>ログを利用して正確に事故原因等を検証するため、医療情報システム等のすべてのサーバ・機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておく。</p>	<ul style="list-style-type: none"> ・ Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・ 「クロックの同期」(27K1:2013 A.12.4.4、27K1:2022 A.8.17)
		③-2	<p>医療情報システム等のすべてのサーバ・機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証することが望ましい。</p>	
		③-3	<p>ログの時刻の信頼性を確保するために、医療情報システム等の時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。</p>	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	④ リモートメンテナ ナンスにおける 不正な侵入防止と ログの取得・検証	④-1	リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、医療情報システム等への不正な侵入が生じないように安全管理措置を講じる。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9.1、27K1:2022 A.5.15) ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) ・「アクセス権」(27K1:2013 A.9.2.2、A.9.2.5、A.9.2.6、27K1:2022 A.5.18) ・「特権的なユーティリティプログラムの使用」(27K1:2013 A.9.4.4、27K1:2022 A.8.18) <p>論理アクセス制御、ログ取得、監視を含む情報セキュリティ監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、侵入試行およびその他のセキュリティ関連イベントを特定するために、独自のセキュリティ情報およびイベント管理システムを使用し、監査ログを継続的に監視している。事前に定義されたしきい値に基づいて、さらなる調査のためにセキュリティアラートが生成される。これらの監視ツールは、セキュリティ担当者に自動的にアラートを発する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やアクティビティの監視を含む環境の構成、管理、保護に関するすべての権利と責任を保持する。</p>
		④-2	リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。	
		④-3	サービス提供に必要な医療情報システム等の保守をリモートメンテナンスで行う場合、医療機関等と合意する。	
	⑤ 取り扱う医療情報 の法定保存年限に 基づくログの保存 期間の設定	⑤-1	取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するログ又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。	該当なし。これはカスタマーの責任で対応する必要がある。
		⑤-2	法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、医療機関等と合意する。なお、本項におけるログの管理方法について保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。	該当なし。これはカスタマーの責任で対応する必要がある。
3.5. 不正プログラム への対策	① 不正プログラム 対策ソフトウェア の導入と管理	①-1	最新の脅威についての情報収集に努め、導入している不正プログラム対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認する。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「マルウェアからの保護」(27K1:2013 A.12.2.1、27K1:2022 A.8.7) ・「情報セキュリティインシデント管理の計画および準備」(27K1:2013 A.16.1.1、27K1:2022 A.5.24) ・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) ・「情報セキュリティインシデントへの対応」(27K1:2013 A.16.1.5、27K1:2022 A.5.26) ・「情報セキュリティ事象の報告」(27K1:2013 A.16.1.2、27K1:2022 A.6.8) <p>Acronis は、独自に開発した製品を使用してマルウェアの脅威を処理し、エンドポイントレベルでの保護を保証する。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		①-2	不正プログラム対策ソフトウェアにおいて次の設定を行う。 <ul style="list-style-type: none"> ・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 	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-3	一定期間、不正プログラムのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとる。	
		①-4	医療情報システム等の構築に際しては、不正プログラム等の混入が生じないようにするための手順を策定し、これに則って構築する。	
		①-5	不正プログラム対策ソフトウェアのパターン定義ファイルを常に最新のものに更新する。	
		①-6	医療情報システム等の構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新の不正プログラム対策ソフトウェア等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。	
		①-7	医療情報システム等利用環境がウイルス等による攻撃を受けた場合に、医療情報システム等提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。	
3.6. 端末やサーバの 堅牢化	① 端末やサーバの 堅牢化	①-1	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにする。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） <p>論理アクセス制御を含む情報セキュリティ監査および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p> <p>Acronis は、ロールベースで厳格に職務分掌し、特権アクセスを付与する。Acronis の従業員は、カスタマーのコンテンツデータにアクセスすることはできない。カスタマーのコンテンツデータは、いかなる理由においても Acronis の従業員の端末からエクスポートされることはない。</p> <p>Acronis のストレージは保存時に AES-256 によって暗号化される。使用する製品によっては、カスタマーはデータを Acronis Cyber Cloud Storage に送信する前に、自分の側で暗号化を有効にすることもできる。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、アクセス管理やデータの暗号化を含む、環境の設定と管理に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-2	ウェブブラウザの接続するサーバを業務上必要なサーバに限定する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「マルウェアからの保護」(27K1:2013 A.12.2.1、27K1:2022 A.8.7) ・「Web フィルタリング」(27K1:2022 A.8.23) <p>Acronis は、独自に開発した製品を使用してマルウェアの脅威を処理し、エンドポイントレベルでの保護を保証する。</p> <p>Webフィルタリングはエンドユーザのデバイスで有効化され、脅威インテリジェンスの結果に基づいて、疑わしい IP アドレスと URL をブロックする。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		①-3	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash等のプログラムコードをダウンロード及び実行することができない設定とする(管理ソフトウェアが実行されるサーバのみを認可する)。	
		①-4	認可したサイトからダウンロードされるコードについても不正プログラム対策ソフトウェアにより検査する。	
		①-5	ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な確認なしに起動されないよう設定を行うことが望ましい。	
		①-6	医療情報システム等のサーバ機器等への同時ログオンユーザ数(OS アカウント等)に適切な上限を設ける。	<ul style="list-style-type: none"> ・ Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・ 「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2)
		①-7	医療情報システム等に用いる装置には、必要のないアプリケーション等をインストールしない。	
		①-8	医療情報システム等に関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「資産に対する責任」(27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) ・ 「媒体の処分」(27K1:2013 A.8.3.2、27K1:2022 A.7.10) ・ 「装置の安全な処分または再利用」(27K1:2013 A.11.2.7、27K1:2022 A.14) ・ 「運用システムへのソフトウェアのインストール」(ISO27K1:2013 A.12.5.1、A.12.6.2、ISO27K1:2022 A.8.19)
		①-9	医療情報システム等に関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。	
3.7. 機器・ソフトウェアの脆弱性への対応	① 安全性が確認できるネットワーク機器の利用	①-1	ルータ等のネットワーク機器は、安全性が確認できる機器を利用する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「ICT サプライチェーンにおける情報の管理」(27K1:2013 A.15.1.3、27K1:2022 A.5.21) ・ 「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) ・ 「資産に対する責任」(27K1:2022 A.8.1、27K1:2022 A.5.9、A.5.10、A.5.11) <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		①-2	ルータ等のネットワーク機器は、ISO/IEC15408で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	② パッチ適用等の実施	②-1	医療情報システム等に関連する技術的脆弱性については台帳等を利用して管理する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「技術的脆弱性の管理」(27K1:2013 A.12.6.1、A.18.2.3、27K1:2022 A.8.8) ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) <p>Acronis は、市販のツールと独自に開発したツールを組み合わせた包括的な脆弱性管理プログラムを実装し、セキュリティ脅威を事前対応的に特定するとともに、厳格な自動化および手動の侵入テスト、品質保証対策、ソフトウェアセキュリティ評価、外部監査を実施している。脆弱性の監視と対処の責任は、Acronis のサイバーセキュリティチームが負う。チームはこれらの課題を入念に特定および追跡し、是正が確認されるまで定期的にフォローアップを行う。さらに、Acronis は脆弱性報奨金制度を実施することで、セキュリティ独立研究者との強固な関係を構築している。</p> <p>脆弱性管理および変更管理に関連する制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis のサイバーセキュリティ体制に関する詳細情報は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		②-2	潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定する。	
		②-3	修正パッチの適用前にパッチが改竄されていないこと及び有効性を検証する。	
		②-4	オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システム等に対する影響を評価し、試験結果を確認してから実施する。	
	③ 医療情報システム等への脆弱性診断の実施	③-1	提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行う。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「技術的脆弱性の管理」(27K1:2013 A.12.6.1、A.18.2.3、27K1:2022 A.8.8) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) <p>Acronis は、市販のツールと独自に開発したツールを組み合わせた包括的な脆弱性管理プログラムを実装し、セキュリティ脅威を事前対応的に特定するとともに、厳格な自動化および手動の侵入テスト、品質保証対策、ソフトウェアセキュリティ評価、外部監査を実施している。脆弱性の監視と対処の責任は、Acronis のサイバーセキュリティチームが負う。チームはこれらの課題を入念に特定および追跡し、是正が確認されるまで定期的にフォローアップを行う。設計から配置まで、複数のソフトウェアセキュリティチェックを実施するために、セキュリティ開発ライフサイクル (SDLC) が確立されている。独立したセキュリティ研究者を参加させるべく脆弱性報奨金制度を実施している。</p> <p>脆弱性管理に関する管理については、Acronis の SOC 2 Type II 報告書のために第三者監査人による レビューおよび検証も行われている。</p> <p>Acronis のサイバーセキュリティ体制に関する詳細情報は、https://www.acronis.com/trust-center/ を参照のこと。</p>
		③-2	アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。	
		③-3	開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的な脆弱性検査を行う。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
	④ 最新の脆弱性に関する情報の収集	④-1	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「ICT サプライチェーンにおける情報の管理」（27K1:2013 A.15.1.3、27K1:2022 A.5.21） 「技術的脆弱性の管理」（27K1:2013 A.12.6.1、A.18.2.3、27K1:2022 A.8.8） 「システムの取得、開発および保守」（27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32） <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		④-2	医療情報システム等の脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「脅威インテリジェンス」（27K1:2022 A.5.7）
	⑤ IoT機器に関する情報収集及び脆弱性への対応	⑤-1	IoT機器の利用を含むサービスを提供する場合、医療機関等との役割分担について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		⑤-2	IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。	該当なし。これはカスタマーの責任で対応する必要がある。
3.8. ネットワーク上のアクセス制御。	① ネットワークのアクセス制御。	①-1	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> 「通信セキュリティ」（27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6） 「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」（27K1:2013 A.14.1.2、27K1:2022 A.8.26） 「ログ取得」（27K1:2013 A.12.4、27K1:2022 A.8.15） 「監視活動」（27K1:2022 A.8.16） <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
		①-2	セキュリティゲートウェイでは、不正な IP アドレスを持つトラフィックが通過できないように設定する（接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等）。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-3	<p>医療情報システム等において、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定する。他に必要なサービスがある場合には、医療機関等の合意を得てから利用する。</p> <ul style="list-style-type: none"> ・ 外部からの医療情報システム等の稼動監視・遠隔保守 ・ セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ・ オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード ・ 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・ ファイアウォール、IDS・IPS などのセキュリティ機器に対する不正アクセス監視 ・ 時刻同期のための時刻配信サーバへのアクセス ・ これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等） ・ その他の医療情報システム等の稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等） 	
	② なりすましの防止	②-1	<p>次の情報交換方法について予め合意しておく。</p> <ul style="list-style-type: none"> ・ 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 	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・ 「通信セキュリティ」（27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6） ・ 「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」（27K1:2013 A.14.1.2、27K1:2022 A.8.26） <p>Acronis の ISO/IEC 27017 および ISO/IEC 27018 規格の認証は、クラウドサービスのセキュリティとクラウドに送信する個人情報の安全な取り扱いに対する Acronis のコミットメントを保証する。</p> <p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/support/platform-terms-conditions/</p> <p>https://www.acronis.com/company/privacy/</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		②-2	情報交換手順では搬送の形態によらず次の事項を確実にする。 発送者、受領者を識別し記録する。 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行う。 交換する情報の機密レベルに関して合意する（受領側で機密レベルが低くならないようにする）。 交換された情報に悪意のあるコードが含まれていないことを確実にする。	
		②-3	電子的に情報を転送する際には以下の対策を実施する。 <ul style="list-style-type: none">送信者、受信者は相互に電子的に認証を行って相手の正当性を検証する。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。送受信する経路は適切な方法で傍受のリスクから保護されている。受信した情報について経路途中での損傷、改竄が無いことを検証する対策を講じる。送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施する。	
		②-4	医療機関等から受託事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。	
		②-5	②-4において、医療機関等が外部接続するサーバ等と受託事業者のサーバとの間の相互認証を行う。	
				AAcronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none">「通信セキュリティ」（27K1:2013 A.13、27K1:2022 A.8.20、A.8.21、A.8.22、A.5.14、A.6.6）「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」（27K1:2013 A.14.1.2、27K1:2022 A.8.26） Acronis のセキュリティチームは、Acronis のネットワークインフラストラクチャを保護する堅牢な境界を維持することに注力している。さまざまな種類の侵入テストにより、ネットワーク境界の内部継続テストを厳格に実施する。さらに、Acronis は、資格と認定を受けた侵入テスト担当者を活用し、外部のサードパーティによる侵入テストを調整する。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		②-6	②-4について、受託事業者が保守業務を再委託している場合には、受託事業者と再委託先との接続では、別途なりすましを防止する策を講じる。	
		②-7	医療情報システムの安全管理に関するガイドライン システム運用編「13. ネットワークに関する安全管理措置第④項における医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、医療機関等と合意する。	
	③ ネットワーク ポートへの不正な 装置の接続制限	③-1	ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) ・「機器の設置および保護」(27K1:2022 A.11.2.1、27K1:2022 A.7.8) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。
		③-2	不正な装置を識別するため、医療情報システム等内で利用する情報処理装置を登録したリストを作成・維持する。	
		③-3	不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあ ¹	
	④ 無線LAN利用時の 対策、	④-1	医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、医療情報システム等事業者の役割分担等について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		④-2	業務上、医療情報システム等に関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。	
3.9. 不正な通信の 検知や遮断	① ネットワーク上の 不正な通信の 検知や遮断	①-1	医療機関等との接続ネットワーク境界には侵入検知システム (IDS)、侵入防止システム (IPS) 等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行う。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「ログ取得」(27K1:2013 A.12.4、27K1:2022 A.8.15) ・「監視活動」(27K1:2022 A.8.16) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) ・「ネットワークおよびネットワークサービスへのアクセス」(27K1:2013 A.9.1.2、27K1:2022 A.5.15) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。

¹ 以降、文末切れ(000891035.pdf)

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-2	侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。	
		①-3	侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。	
		①-4	侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定とする。	
		①-5	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る。	
		①-6	医療情報システム等から、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視することが望ましい。	
		①-7	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。	
				該当なし。これはカスタマーの責任で対応する必要がある。
3.10. 外部へ持ち出す 機器や情報の 管理	① 持ち出しを行う 機器の認証	①-1	機器等については、起動パスワードの設定を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） ・「構外にある機器および資産のセキュリティ」（27K1:2013 A.11.2.6、27K1:2022 A.7.9） ・「機器の設置および保護」（27K1:2022 A.11.2.1、27K1:2022 A.7.8） ・「設備の保守」（27K1:2013 A.11.2.4、27K1:2022 A.13） 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている
		①-2	起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。	
		①-3	医療情報システム等に関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせで行う。	
	② 搬送する情報に対する対策	②-1	情報を格納する機器・媒体等を持ち出す場合の手順には、機器・媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。	
				Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「アクセス制御」（27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2） ・「構外にある機器および資産のセキュリティ」（27K1:2013 A.11.2.6、27K1:2022 A.7.9）

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.11. 仮想デスクトップ やMDM・MAMに よる情報漏洩へ の対策	① 個人所有の機器の 管理	①-1	<p>利用者が個人所有する機器による医療情報システム等利用に関する対応策について、医療機関等と合意する。 なお具体的には以下の内容を参考にする。</p> <ul style="list-style-type: none"> 利用者が所有する機器からの情報漏洩等を防止する観点から、例えば、仮想デスクトップを用いて OS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント (MDM) やモバイルアプリケーションマネジメント (MAM) 等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。 	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> 「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) 「構外にある機器および資産のセキュリティ」(27K1:2013 A.11.2.6、27K1:2022 A.7.9) 「リモートワーク」(ISO27K1:2013 A.6.2.2、ISO27K1:2022 A.6.7) <p>Acronis の従業員は、業務目的で Acronis のマシンとモバイルデバイスを使用する。また、Acronis は、ユーザ所有のデバイス上で Acronis の完全管理型アプリケーションを業務活動に使用することを許可している。</p>
		①-2	サービスの提供に係る目的 (開発、保守、運用含む) で従業員等の個人所有の機器を利用することは原則禁止とする。	
	② 端末側に情報を残さない技術の導入	②-1	医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するための受託事業者の役割分担等につき、医療機関等と合意する。	
3.12. 未登録の 電子媒体の 接続制限	① サーバ等への 未登録の 電子媒体の 接続制限	①-1	医療情報システム等においてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除する。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。	<p>Acronisは、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 の認証を取得している。</p> <ul style="list-style-type: none"> 「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) 「設定管理」(27K1:2022 A.8.9) 「仮想マシンの強化」(27K17:2015 CDL.9.5.2) <p>Acronis Cyber Cloud Infrastructure は、信頼性が高い検証済みのベースラインから展開されるコードベースのインフラストラクチャである。さらに、ツールを使用して、本番環境のマシン上で事前に定義されたオペレーティングシステム (OS) 構成との差異を特定し、自動的に修正する。</p>
		①-2	不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.13. 暗号化・ 電子署名の利用	① 安全性が 確認された 暗号化・電子署名 の利用	①-1	ネットワークにおいて、情報の盗聴、改竄、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」（27K1:2013 A.10.1、27K1:2022 A.8.24） ・「ネットワークセキュリティ」（27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22） 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-2	アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置（サーバ証明書の導入等）を行う。	Acronis は、Acronis または Acronis の代理の管理下でない物理的な境界を越えてデータを転送する場合は必ず、1 つ以上のネットワーク層を介して送信されるすべてのデータに対して暗号化と認証を実装している。Acronis のセキュリティに関する詳細情報については、 https://www.acronis.com/trust-center/ 参照のこと。
		①-3	経路の安全性確保のため、IPsec + IKEへの対応や閉域ネットワークへの対応等及びその条件等について、医療機関等と合意する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」（27K1:2013 A.10.1、27K1:2022 A.8.24） ・「ネットワークセキュリティ」（27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22） ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-4	情報伝送に用いるケーブル類については直接の傍受リスクについて配慮することが望ましい。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」（27K1:2013 A.10.1、27K1:2022 A.8.24） ・「ネットワークセキュリティ」（27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22） ・「物理的および環境的セキュリティ」（27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6） 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-5	暗号アルゴリズムは十分な安全性を有するものを使用する。選択基準としては電子政府推奨暗号リスト 等を用いる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」（27K1:2013 A.10.1、27K1:2022 A.8.24） ・「ネットワークセキュリティ」（27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22） 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。
		①-6	送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。	Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。.
		①-7	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」（27K1:2013 A.10.1、27K1:2022 A.8.24） ・「ネットワークセキュリティ」（27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22） Acronis は、オープンな暗号化手法の採用を推奨し、すべての認証トラフィックに TLS を使用することを義務付けている。カスタマーデータは、保存時、転送時、および Acronis の内部ネットワークの通過時に暗号化される。
		①-8	①-7のほか、医療機関等がメールの暗号化（S/MIME等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-9	VPN 接続を行う場合には以下の事項に従う。 接続時に VPN 装置間で相互に認証を行う。 傍受、リプレイ等のリスクを最小限に抑えるために、適切な暗号技術を利用する。 インターネット上のトラフィックが VPNチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しない。 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPN チャンネルを医療機関等別に構築する等の対策を実施する。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) ・「公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮」(27K1:2013 A.14.1.2、27K1:2022 A.8.26) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。
		①-10	オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22)
		①-11	SSL-VPNは、原則として使用しない。	Acronis は、オープンな暗号化手法の採用を推奨し、すべての認証トラフィックに TLS を使用することを義務付けている。カスタマーデータは、保存時、転送時、および Acronis の内部ネットワークの通過時に暗号化される。
		①-12	サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。	
		①-13	医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、医療機関等と合意する。	
	② 暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-1	暗号鍵が漏洩した場合に備えた対応策を策定しておく。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) ・「データ漏洩防止」(27K1:2022 8.12) ・「情報セキュリティインシデント管理の計画および準備」(27K1:2013 A.16.1.1、27K1:2022 A.5.24) ・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		②-2	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。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) ・「ネットワークセキュリティ」(27K1:2013 A.13.1、27K1:2022 A.8.20、A.8.21、A.8.22) Acronis は、認証の完全性を保証するために証明書を使用する。
		②-3	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。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24) ・「データ漏洩防止」(27K1:2022 8.12) ・「情報セキュリティインシデント管理の計画および準備」(27K1:2013 A.16.1.1、27K1:2022 A.5.24) ・「情報セキュリティ事象の評価および決定」(27K1:2013 A.16.1.4、27K1:2022 A.5.25) 情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。
		②-4	医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証する。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-5	暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-6	暗号鍵の生成は耐タンパー性を有する ICカード、USB トークンデバイスといった安全な環境で実施することが望ましい。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24)
		②-7	暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。	<ul style="list-style-type: none"> ・ Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) ・「暗号の利用」(27K1:2013 A.10.1、27K1:2022 A.8.24)。
		②-8	電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できるようにすることが望ましい。	該当なし。これはカスタマーの責任で対応する必要がある。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.14. リモート メンテナンスの アクセス管理	① リモート メンテナンスの 不必要なログイン を防止するための アクセス管理	①-1	リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 <ul style="list-style-type: none"> ・「アクセス制御」(27K1:2013 A.9、27K1:2022 A.5.15、A.5.16、A.5.17、A.5.18、A.8.2) ・「変更管理」(27K1:2013 A.12.1.2、27K1:2022 A.8.32) ・「システムの取得、開発および保守」(27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32) <p>情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis Cyber Protect Cloud を使用するカスタマーは、環境の設定、管理および保護に関するすべての権利と責任を保持する。</p>
3.15. 電子署名を 利用する場合の 管理	① 信頼できる第三者 機関が発行した 電子証明書の利用	①-1	医療情報システム等において電子署名を利用する場合、保健医療福祉分野PKI 認証局の発行する署名用電子証明書等の信頼できる第三者機関が発行した電子証明書を利用する。	該当なし。これはカスタマーの責任で対応する必要がある。
	② 電子署名を 施す場合のタイム スタンプの付与	②-1	電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容・検証方法について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-2	タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		②-3	タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
	③ タイムスタンプを 付与する時点で 有効な電子証明書 の使用。	③-1	タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.16. 改竄防止・ 検知策の実装	① ソフトウェアの 改竄防止・検知策 の実装	①-1 ①-2	不正な改竄を受けていないことを検証するため、定期的にソフトウェアの整合性検査（改竄検知）を実施する。 不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改竄防止、検知策を実施する。	Acronis は、次の規定に基づいて、ISO 9001 および ISO/IEC 27001 規格の認証を取得している。 ・「変更管理」（27K1:2013 A.12.1.2、27K1:2022 A.8.32） ・「システムの取得、開発および保守」（27K1:2013 A.14、27K1:2022 A.8.25、A.8.26、A.8.27、A.8.28、A.8.29、A.8.32） ・「製品およびサービスの設計・開発」（9001:2015 8.3） Acronis は、設計から配置に至るまで、複数のソフトウェアセキュリティチェックを保証するためにセキュリティ開発ライフサイクル（SDLC）を確立している。独立したセキュリティ研究者を参加させるべく脆弱性報奨金制度を実施している。 変更管理およびソフトウェア開発を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。 Acronis Cyber Protect Cloud を使用するカスタマーは、変更管理およびシステム開発手順を含む環境の設定と管理に関するすべての権利と責任を保持する。
3.17. 患者ごとの 情報の管理	① 患者ごとに情報を 管理する機能の 実装	①-1	医療情報システム等には、受託する医療情報を患者等ごとに管理できる機能を含める。	該当なし。これはカスタマーの責任で対応する必要がある。
3.18. 利用目的に 応じた応答時間 の確保	① 医療情報システム 等の利用目的に 応じた応答時間の 確保	①-1	医療機関等が医療情報システム等を利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.19. 冗長化による 障害対策	① 医療情報システム 等の停止に備えた 冗長化	①-1	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-2	医療情報システム等、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。	
		①-3	①-2を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、医療機関等と合意する。	
		①-4	障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、医療機関等と合意する。	
	② ディスク障害対策	②-1	診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.20. システム障害時の 措置.	① 医療情報 システム等障害時 における機能の 実装	①-1	医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、医療機関等と合意する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-2	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え汎用のブラウザ等で閲 ¹	
		①-3	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、医療機関等と合意する。	
		①-4	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、医療機関等と合意する	
		①-5	緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)をサービスに含め、これに必要なセキュリティ等の情報提供について、医療機関等と合意する。	
		①-6	障害等が生じた場合の役割分担を明確にした上で、稼働を保証するサービスの範囲について、医療機関等と合意する。	
3.21. バックアップ及び リストアの管理	① バックアップや リストア等の 情報の管理	①-1	電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「物理的および環境的セキュリティ」(27K1:2013 A.11、27K1:2022 A.7.1、A.7.2、A.7.3、A.7.4、A.7.5、A.7.6) <p>物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。</p>

¹ 以降、文末切れ(000891035.pdf)

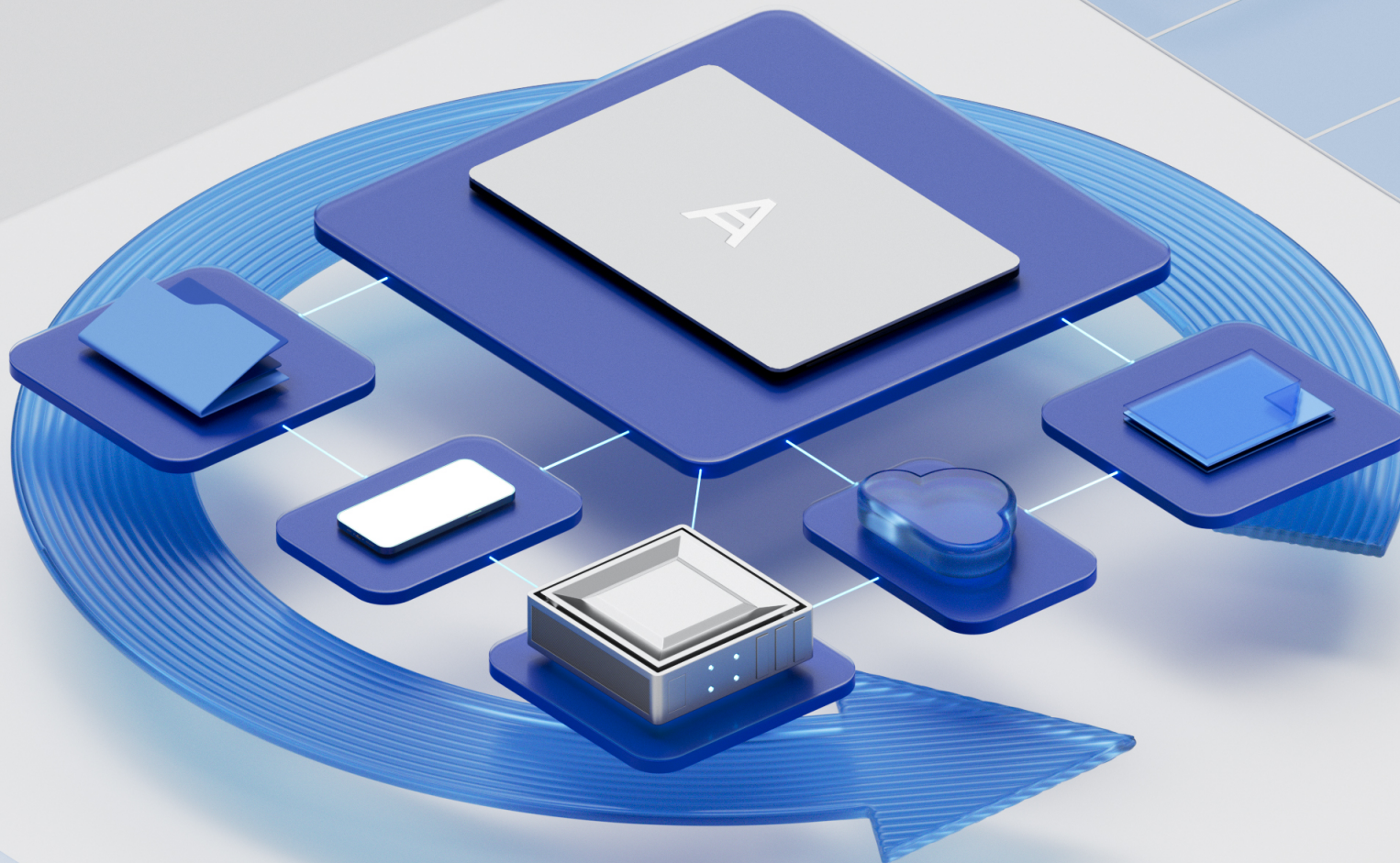
カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-2	各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。 ・「容量の管理」(27K1:2013 A.12.1.3、27K1:2022 A.8.6、27K17 12.1.3)
		①-3	医療機関等が医療情報システム等を利用する際に、利用可能な資源に係る情報(保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等)について、医療機関等と合意する。	
		①-4	医療情報システム等が情報を保存する場所(内部、可搬媒体)、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。	Acronis is certified to the ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 Standards, Acronisは、次の規定に基づいて、ISO/IEC 27001、ISO/IEC 27017 および ISO/IEC 27018 規格の認証を受けている。 ・「容量の管理」(27K1:2013 A.12.1.3、27K1:2022 A.8.6、27K17:2015 12.1.3) ・「関係当局との連絡」(27K1:2013 A.6.1.3、27K1:2022 A.5.5、27K17:2015 6.1.3) ・「個人情報の地理的所在」(27K18:2019 A.12.1) ・「仮想環境における分離」(27K17:2015 CLD.9.5.1) 物理的セキュリティ管理手順を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われる。
		①-5	①-4において、他の事業者が提供する医療情報システム等を利用する場合においても、同様の情報を収集して、対応する。仮想化技術による医療情報システム等を利用する場合には、受託事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。	
		①-6	①-4により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。	Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。 ・「操作手順書」(27K1:2013 A.12.1.1、27K1:2022 A.5.37) ・「情報セキュリティの意識向上、教育および訓練」(27K1:2013 A.7.2.2、27K1:2022 A.6.3) Acronisは、ISO 27001 規格に準拠する情報セキュリティ管理システム(ISMS)を採用し、包括的な内部文書を維持している。すべての文書は、システムに保管され、複製とバックアップが行われる。 Acronis の契約社員はすべて、入社時にセキュリティ訓練を受講し、Acronis での在籍中にも継続して訓練を受講する。新規契約社員は、オリエンテーションの一環として、カスタマー情報を安全に保護する当社の献身を重視し、当社の行動規範に従うことを誓約する。特定のロールに基づいて、特定のセキュリティの側面に関する追加の訓練を受ける場合がある。 セキュリティ意識と訓練の管理を含む情報セキュリティの監視と管理制御については、Acronis の SOC 2 Type II 報告書のために第三者の監査人によるレビューおよび検証も行われている。
		①-7	医療情報システム等に係る委託先に対しても、①-4の運用管理規程に定める管理方法への対応等を求める。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-8	情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p>
		①-9	①-8に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。	<p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、 https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-10	①-9で示す場合の、毀損した情報に関する管理責任の所在、免責条件等について、医療機関等と合意する。	<p>契約の義務と合意事項を概説した以下の文書を参照のこと。</p> <p>https://www.acronis.com/support/platform-terms-conditions/</p> <p>https://www.acronis.com/company/privacy/</p> <p>https://www.acronis.com/legal/</p> <p>https://www.acronis.com/support/eula/</p>

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-11	リスク分析結果に基づき医療情報システム等のバックアップを取得する。バックアップの取得対象、取得頻度、保存方法・媒体、管理方法等を定め、その内容を運用管理規程等に含める。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。</p> <p>Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		①-12	取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改竄・破壊等がないことを確認する。	
	② バックアップに 用いる記録媒体の 管理	②-1	記録媒体に格納するバックアップについては、その媒体の特性（テープ/ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。	<p>Acronis は、次の規定に基づいて、ISO/IEC 27001 規格の認証を取得している。</p> <ul style="list-style-type: none"> ・「障害時の情報セキュリティ」(27K1:2013 A.17.1、27K1:2022 A.5.39) ・「事業継続のための ICT 準備度」(27K1:2022 A.5.30) ・「情報のバックアップ」(27K1:2013 A.12.3.1、27K1:2022 A.8.13) ・「情報処理施設の冗長性」(27K1:2013 A.17.2.1、27K1:2022 A.8.14) <p>事業継続慣行を含む情報セキュリティの監視および管理制御については、Acronis の SOC 2 Type II 報告書のために第三者監査人によるレビューおよび検証も行われている。</p> <p>Acronis は、プラットフォームの要素を高い冗長性で設計しており、少なくとも N+1 パラダイムが採用されている。このアプローチは、そのサーバのアーキテクチャ、データストレージ慣行、ネットワークとインターネット接続、および提供されるソフトウェアサービスにおいて顕著に表れている。この「あらゆる側面における冗長性」戦略により、エラー管理がシステムに組み込まれ、単一のサーバ、データセンター、ネットワーク接続に依存しないソリューションが提供される。</p> <p>Acronis は、カスタマーのコンテンツデータを複製しない。Acronis Cyber Protect Cloud を使用する各カスタマーは、自分のデータを保管する場所を独自に選択し、利用可能な場合は、事業継続およびディザスタリカバリ戦略に従って、地理的冗長性の追加サービスを有効化する責任を負う。Acronis はカスタマーに対し、3-2-1 バックアップ戦略の採用を強く推奨する。3-2-1 バックアップ戦略についての詳細は、https://www.acronis.com/blog/posts/backup-rule/ を参照のこと。</p>
		②-2	バックアップの記録媒体の使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複製する。	
		②-3	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、別の媒体等に複製する。	
		②-4	②-1～②-3の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。	
		②-5	バックアップに係る情報の提供について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
3.22. システム更改に 備えた互換性 確保。	① データ形式・ プロトコルの 互換性の確保	①-1	診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-2	厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-3	医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を医療情報システム等に備える。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-4	①-3に示す機能等を備えることが困難な場合の医療情報システム等更新・移行の手順について、医療機関等と合意する。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-5	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルを利用をサポートする。	Acronis では以下のように 2 種類のデータを区別している。 サービス提供（製品使用など）および Acronis のサービス管理に必要なデータ。Acronis がサービスを提供するために、データ管理者として収集および処理するデータ。このようなデータには、アカウント名、メールアドレスとその他の連絡先情報、請求の詳細、およびサービスを通じて自動収集された一部の情報が含まれる場合があり、個人情報が含まれる可能性がある。詳細については、Acronisの個人情報保護方針を参照のこと。 https://www.acronis.com/company/privacy/
		①-6	データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。	カスタマーのコンテンツデータカスタマーが Acronis のサービスを利用する際に Acronis がデータ処理者（復処理者）として処理する可能性があるデータ。この情報は、特定の製品（バックアップアーカイブ、ファイル、または仮想マシンなど）を利用する際に、カスタマーによって提供される。この種類のデータに関しては、カスタマーが Acronis を通じて保管する情報のカテゴリや内容を Acronis が管理することはない。
		①-7	①-6の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。	カスタマーは自身の法的義務とコンプライアンス義務を評価および維持することについて全責任を負う。Acronis はコンテンツデータの一部としてどのようなデータが提供されるか不明であるため、カスタマーは特定の要件を満たす必要がある場合、Acronis に確認する必要がある。Acronis は、適用可能なデータ保護制度の下でかかる義務を負うカスタマーと標準的なデータ処理契約を結ぶことができる。
		①-8	①-7は、他の医療情報システム等とのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、医療機関等と合意する。	

カテゴリ	サブカテゴリ	No.	要求事項の内容	Acronis のコンプライアンス
		①-9	データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、見読性確保の対策を講じる。	Acronis は、次の規定に基づいて、ISO/IEC 27001 および ISO/IEC 27017 規格の認証を取得している。 <ul style="list-style-type: none"> ・「資産の返却」(27K1:2013 A.8.1.4、27K1:2022 A.5.11) ・「クラウドサービスのカスタマー資産の移動」(27K17:2015 CLD.8.1.5) 契約上の責任および合意事項に関する Acronis のプラットフォームサービス契約条件詳細は、 https://www.acronis.com/support/platform-terms-conditions/ 第 9.7 条を参照のこと。
		①-10	医療情報システム等に関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。	該当なし。これはカスタマーの責任で対応する必要がある。
		①-11	他の事業者が提供する医療情報システム等を用いて、サービスを提供する場合には、他の事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他の事業者のサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、機器の劣化対策を講じる。	変更点については、3.3.1 条の同じ問題に関する注記を参照のこと。
		①-12	医療情報システム等に係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他の事業者のサービスの変更を行う場合には、①-10、①-11を考慮して行う。	該当なし。これはカスタマーの責任で対応する必要がある。



Acronis

詳細はwww.acronis.comをご覧ください

Copyright © 2002–2024 Acronis International GmbH. 無断複製禁止。Acronis および Acronis ロゴは、Acronis International GmbH の米国および/またはその他の国における登録商標です。その他の商標または登録商標はそれぞれの所有者に帰属します。事前の予告なく技術的な変更や図の変更が行われる場合があります。品質には万全を期していますが、誤りが含まれている場合があります。2024年 9 月