『Reckoner』ガイドライン対応リファレンス

経済産業省版

2020 年 10 月 1 日

株式会社スリーシェイク

改訂履歴

版数	発行日	改訂内容
第 1 版	2020 年 10 月 1 日	初版発行

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定	7.1.1 ISMS 認証取得時の考慮事項	1	プライバシーマーク認定・ISMS 認証等の公正な第三者の認定を取得。	当社は、第三者認定として ISMS の取得に向けて取り組みをしています。	適合可能
	7.2.1 資産台帳	2	医療機関等から預かる情報を管理するための管理台帳の整備について文書化しての管理。	医療情報の保存は当社の環境では行っておらず、Google 提供のクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、Google のセキュリティに関するホワイトペーパー（https://cloud.google.com/security/overview/whitepaper?hl=ja、以下『Google Cloud Platform』対応セキュリティリファレンス）をご参照ください。	対象外
		3	預託された情報の全てを資産台帳に記録。		対象外
		4	必要に応じて資産台帳の閲覧が速やかに行うことができる状態での管理。		対象外
		5	資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限。		対象外
		6	資産台帳等を電磁的記録として管理する場合、資産台帳等へのアクセス制限を侵害する行為についての記録。		対象外
	7.2.2 情報の分類	7	情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を実施。	当社は医療情報を扱わず、接続情報のみ管理しています。接続情報について重要度や管理方法を定義し、情報所有者や管理責任者が適切に扱えるように社内向け機密情報保護規定にて規定しています。	適合可能
		8	情報の所有者、管理責任者は情報の分類が正しく行われていることの定期的な確認。	当社は医療情報を扱わず、接続情報のみ管理しています。運用ルールに従って適切に管理されていることを開発責任者が定期的に確認することで、品質を管理しています。	適合可能
		9	預託される情報に対して分類にもとづいたリスク分析を実施。	当社サービスにおいて、預託される情報はデータソースに対する接続情報のみであり、それに対して重要度を定義しリスク分析を実施しています。詳細は社内向け機密情報保護規定にて記載しています。	適合可能
		10	リスク分析の結果に応じてリスク低減に必要な管理策を実施。	当社サービスにおいて、預託される情報はデータソースに対する接続情報のみであり、それに対して重要度を定義し必要な対策を実施しています。詳細は社内向け機密情報保護規定にて記載しています。	適合可能
		11	分類がわかるように情報にラベルをつける（電磁的記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得る）。	当社サービスにおいて、預託される情報はデータソースに対する接続情報のみであり、それに対して分類及び対策を実施しています。詳細は社内向け機密情報保護規定にて記載しています。	適合可能
		12	各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定める。	当社サービスにおいて、預託される情報はデータソースに対する接続情報のみであり、それに対して必要な対策を実施しています。詳細は社内向け機密情報保護規定にて記載しています。	適合可能
7.3 組織的安全管理策（体制、運用管理規程）		13	医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる 状態にしておく。	医療情報の保存は当社の環境では行っておらず、Google 提供のクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		14	個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておく。	個人情報の保存は当社の環境では行っておらず、Google 提供のクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		15	個人情報保護に関しては、医療機関等の監督の下で実施。		対象外
		16	情報処理の安全管理に関わる手順書、運用管理規程の整備。	当社サービスに係る情報処理の安全管理は、以下の経済産業省及び総務省によるガイドラインに準拠し、その内容は本文書類にて開示する通りです。 ・経済産業省「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」 ・総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」 当社は医療情報を受託管理するクラウドサービス事業者として、上記の２省２ガイドラインの要求事項への対応を図っており、その内容は本文書を含め、いつでも医療機関等の担当者が確認できるようにホ	適合可能
		17	運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内 の体制及び施設、医療機関等及び清掃事業者等の外部事業者との契約書の管理、情 報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リ スク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による 情報セキュリ		適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			ティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等 についての記載。	ームページ上に開示しています。これにより、医療機関等の担当者の方々が自院の運用管理規程を踏まえ、当社サービスをどのように利用・管理するかという観点より、手順書の策定、または現行の運用管理規程の見直しを行えるようにしています。	
7.4 医療情報の伝達経路におけるリスク評価		18	医療情報の取扱に際しては高い機密性が求められていることへの配慮。機密性を確保するためには、医療情報の移動する範囲を限定することが必要。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価の実施。	社内向け機密情報保護規定にて規定済です。	適合可能
7.5 物理的安全対策		情報処理事業者の専有する領域に医療情報システムを設置する場合には、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の確認			
	7.5.1 医療情報処理施設の建物に関する要求事項	19	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、鍵管理の実施。	医療情報の保存は当社の環境では行っておらず、Google 提供のクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		20	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。		対象外
		21	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の導入。		対象外
		22	自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施。		対象外
	7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項	情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合			
		23	医療情報システムを設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証の実施。	当社サービスは Google 提供のクラウド基盤 Google Cloud Platform に構築しているため、実質的に当該システムの設置先は外部事業者である Google が運営するデータセンターとなり、当社の直接的な主管範囲外となります。よって、医療情報処理施設への入退館、入退室等に関する事項への対応状況は【外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等を利用する場合】に係る項目をご参照ください。	対象外
		24	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の利用。		対象外
		25	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の確認（履歴の保全については「7.6.12 ログの取得及び監査」を参照）。		対象外
		26	情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理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、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。		対象外
		27	情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理事業者の 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。		対象外
		28	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、情報処理事業者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実施。		対象外

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		29	情報処理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。		対象外
		30	医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを認めないこと。		対象外
		外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合			
		31	データセンターを運営する外部事業者が、①と同等な安全管理策を実施する等、情報処理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の確認。	当社サービスはGoogle提供のクラウド基盤Google Cloud Platformに構築しているため、実質的に当該システムの設置先は外部事業者であるGoogleが運営するデータセンターとなり、当社の直接的な主管範囲外となります。よって、医療情報処理施設への入退館、入退室等に関する事項への対応状況は【外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等を利用する場合】に係る項目をご参照ください。	対象外
		32	医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理事業者の職員以外が鍵を扱わないよう、確実な鍵管理を実施。		対象外
		33	情報処理事業者が医療情報システムの設置されるサーバラックを解錠して行う作業について、作業者、作業開始時刻、作業終了時刻、作業内容等についての記録。		対象外
		34	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム、医療情報に影響を与えないことの確認。		対象外
		35	医療情報システムであることが同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしない。		対象外
		外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合			
		36	サーバ環境を運営する外部事業者が①及び②と同等な安全管理策を実施する等、情報処理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の確認。	当社サービスはGoogle提供のクラウド基盤Google Cloud Platformに構築しているため、実質的に当該システムの設置先については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
	7.5.3 情報処理装置のセキュリティ	37	不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストの作成・維持。	当社サービスはGoogle提供のクラウド基盤Google Cloud Platformを利用しています。当社サービスで利用している情報処理上のリソースリストはGoogle Cloud Platformの管理画面（Cloud Console）で一覧化されており、不正なリソース利用の発生があれば適時に対応可能な体制としています。	対象外
		38	医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。	システム構築は運用保守担当者の中でも、一部の特権を持っている管理者のみが行うことができます。実際にシステム構築する際は、クラウドインフラストラクチャオーケストレーションツールやプロビジョニングツールでシステム構築を自動化しており、意図しないアプリケーションがインストールされた場合でも、適時に検知可能にしています。	対象外
		39	医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを実施。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を実施。	当社サービスの接続情報などは全て暗号化された状態で保存されており、端末画面で暗号化されていない情報を表示することはありません。外部での作業時には、覗き見防止用フィルターなどを設置する対策を講じています。	対象外
		40	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。	当社サービスはクラウド型でWebブラウザを利用する型式で提供しており、接続する端末に医療情報と個人情報が保存されないようにしています。社内の保守運用では、医療情報が端末で保存されることがないよう、サーバ上で業務が完結するように運用しています。上記の通り、利用者の端末に加え当社の保守運用作業においても、サーバのみでデータ管理することを可能とすることで、想定外のデータ保存が発生することのない仕組みを整備しています。	対象外
		41	火災発生時の消火設備が機器に損傷を与えないような配慮。	本項目は当社サービスのクラウド基盤を提供しているGoogleの対応事項となるため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		42	医療情報システムを配置する室内での喫煙、飲食の禁止。		対象外

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		43	医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないような配慮。		対象外
		44	それぞれの装置は製造元または供給元が指定する間隔及び仕様に従って保守点検を行い、必要に応じて交換を実施。		対象外
		45	保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。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。		対象外
		医療情報システムを設置するサーバラックについては以下の安全管理策の実施			
		46	震災時に転倒することが無いよう確実に設置。	本項目は当社サービスのクラウド基盤を提供しているGoogleの対応事項となるため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		47	熱による障害を防ぐため十分な空調設備を保有し、サーバラック内の十分な換気。		対象外
		48	扉に十分な安全強度を持つ物理的施錠装置を設け、鍵管理についての十分な配慮。		対象外
		49	起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードの設定。設定されるパスワードの品質、管理については「7.6.14 作業者アクセス及び作業者 ID の管理」に従うこと。		対象外
		50	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。		対象外
		51	不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みの整備運用を実施。	本項目は当社サービスのクラウド基盤を提供しているGoogleの対応事項となるため、『Google Cloud Platform』対応セキュリティリファレンスにおける本項目をご参照ください。	適合可能
	7.5.4 情報処理装置の廃棄及び再利用に関する要求事項	52	ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、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の確認。	本項目は当社サービスのクラウド基盤を提供しているGoogleの対応事項となるため、『Google Cloud Platform』対応セキュリティリファレンスにおける本項目をご参照ください。社内での保守運用では、医療情報が端末で保存されることがないようサーバ上で業務が完結するように運用しています。よって、当社執務室内の当社サービスへアクセスするための端末に医療情報が残存することはありません。	適合可能
		53	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。		適合可能
		54	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。		適合可能
		55	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に整備。		適合可能
	7.5.5 情報処理装置の外部への持ち出しに	56	情報処理装置が設置されている室内及び情報処理事業者の管理領域から持ち出す場合に備え、適切な持ち出し手順を策定。	クラウド上の情報は操作PC及び外部記録媒体にコピーできないようにアクセス制御がされています。	対象外
		57	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。		対象外

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
	関する要求事項				
7.6 技術的安全対策	7.6.1 情報処理装置及びソフトウェアの保守	58	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実施。	当社サービスのソフトウェアを更新（リリース）する際は、事前に社内でテスト（結合テストならびに総合テスト）を行っており、更新時の思わぬ影響がでないように確認評価しています。また、更新するに当たり医療機関であるユーザに悪影響を及ぼす可能性がある事象があった際は、更新の中止・延期を行い、対応した上での更新を行っています。	適合可能
		59	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討。	社内で業務に利用する端末にはセキュリティソフトを導入しており、常にセキュリティソフトで端末内を監視するようにしています。	適合可能
		60	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポート。	当社サービスはクラウド型でWebブラウザを通じて利用するサービスのため、データ形式やプロトコルが変更するようなときは、事前にサーバ側でデータを変換ないし対応をした上でリリースをおこなっています。そのため、利用している医療機関はデータ形式やプロトコルの変更があった際も、そのことを意識することなくソフトウェアをシームレスに利用することができます。	適合可能
		61	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。	保守作業におけるダウンタイムが必要最低限となるよう、事前に計画書の作成・レビュー体制の構築を実施して品質管理をしています。	適合可能
		62	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。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。	保守作業に伴うリリース手順書について、レビュー体制を構築し品質管理をしています。システム停止を伴う作業の場合は、１週間前に事前に通知し承認を受けた上で実施しています。	適合可能
		63	不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施。	当社サービスの不正な改ざんを防止する方法として下記の２つを実施しています。１つ目は、本番環境を更新するときは事前にテスト環境で動作テストならびにソースコードのレビューを行っています。そこで、意図しないプログラムがはいっていないかを確認しています。２つ目は、本番環境のリリース時は継続的インテグレーションツールで本番環境のリリースを自動化しており、手作業による操作ミスや特定の管理者以外が不適切なプログラムを入れることができないようにしています。	適合可能
		64	医療情報システムに関連する技術的脆弱性について、台帳等を利用しての管理。	プラットフォーム診断/ペネトレーションテストを定期に実施しており、台帳にて脆弱性の管理を行っています。	適合可能
		65	潜在的な技術的脆弱性が特定された場合、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。	定期的な脆弱性診断で特定された問題について、セキュリティ担当によってリスク分析と対策を検討した上で必要な処置を実施しています。	適合可能
		66	修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証。	修正パッチ含めてソフトウェアを本番環境にリリースするときは、事前にテスト環境で動作テストならびにソースコードのレビューを実施し、意図しないプログラムがはいっていないかを確認しています。	適合可能
		67	保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「7.6.5 第三者が提供するサービスの管理」の管理策を実施。選定した外部事業者について医療機関等に報告し、合意を得る。	保守作業は外部事業者に委託していません。	対象外
	7.6.2 開発施設、試験施設と運用施設の分離	68	情報処理に供するアプリケーションについては、情報処理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。	外部開発者事業者が開発したアプリケーションについては、事前に試験を実施して安全性を検証した上で使用しています。	適合可能
		69	ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設を用いて実施。	当社サービスの開発は本番環境とは物理的に別の開発環境を用いており、運用施設（医療機関）に影響がないようにしています。	適合可能
		70	開発施設では悪意のあるコード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	開発施設（社内）で用いる端末はインターネットに接続していますが、セキュリティソフトを導入して	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			場合には「7.6.3 悪意のあるコードに対する管理策」に従う。	悪意あるコードやプログラムが入ることがないようにしています。	
		71	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ざん防止、検知策を実施。	当社サービスはクラウド上の本番環境を更新することで医療機関等が利用する本番環境（サービス）も更新されます。本番環境にリリースする際は、継続的インテグレーションツールで本番環境のリリースを自動化しており、手作業による操作ミスや特定の管理者以外が不適切なプログラムを入れることができず、仮に混入していたとしても適時に検知できるプロセスとしています。	適合可能
		72	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。	医療情報の保存は当社の環境では一切行っておりません。クラウド上の情報は操作 PC 及び外部記録媒体にコピーできないようにアクセス制御しています。	対象外
		73	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、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用する。	医療情報の保存は当社の環境では一切行っておりません。	対象外
	7.6.3 悪意のあるコードに対する管理策	74	最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認。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。	開発・保守を実施する全ての端末にセキュリティ対策ソフトを導入しています。	適合可能
		悪意のあるコード対策ソフトウェアにおいて次の設定を実施			
		75	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）。	セキュリティ対策ソフトで悪意のあるコードに対する対策を実施しています。また、セキュリティ管理者による定期的な点検作業で安全性を担保しています。	適合可能
		76	リスク評価の結果として必要であれば定期的にスキャンを実施。電子媒体へのデータ書き出し・読み込み時におけるオンデマンド。		適合可能
		77	定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新。		適合可能
		78	管理者以外による設定変更やアンインストールの禁止。		適合可能
		79	一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、ス キャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策を実施。	セキュリティ対策ソフトで対策を実施しています。また、セキュリティ管理者による定期的な点検作業によって安全性を担保しています。本番環境は社内のネットワーク経由で管理者しか接続できないよう対策を実施しています。	適合可能
	7.6.4 ウェブブラウザを使用する際の要求事項	80	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。	本番環境の仮想サーバ OS にはウェブブラウザはインストールしていません。	適合可能
		81	ウェブブラウザの設定で、認可していないサイトから ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する）。		適合可能
		82	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「7.6.3 悪意のあるコードに対する管理策」に即して検査する。		適合可能
	7.6.5 第三者が提供するサービスの管理	83	第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認。	当社サービス提供に大きく影響を受ける第三者サービスは、Google Cloud Platform（クラウド基盤）です。Google Cloud Platform とは各サービスに対して SLA を確認した上でサブスクリプション契約しており、サービスレベルや品質の担保について取り決めをした上で利用しています。	適合可能
		84	サービスの実施、運用、維持について定期的に検証する。	いずれの第三者サービスの場合も、問題や不具合などの発覚時には原因調査と改善策を依頼し、問題解決や再発防止に向けて取り組んでいます。	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		85	サービス実施について事前、事後報告を義務づけ、報告内容の点検確認。	Google Cloud Platform に関して、メンテナンスなどサービス影響のある変更がある場合は事前に通知をもらい、影響を最小限にするようにしています。	適合可能
		86	サービスを実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。	当社サービスの提供に際して、サービス提供システム等に再委託先の要員が直接アクセスする可能性のある業務範囲は、Google Cloud Platform によるデータセンターの管理・運営業務のみとなります。Google による本事項への対応状況は、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		87	サービス実施中に第三者が管理区域に立ち入る場合、顔写真を券面に入れた身分証明を携帯する。		適合可能
		88	サービス実施にともなう処理施設内への立ち入り手順に関しては、情報処理事業者 職員の入室、退室手順に準ずること。		適合可能
		89	サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を実施。	Google Cloud Platform に関しては、メンテナンス等の当社サービスに影響がある変更が行われる場合、事前に通知を行わせた上でサービスへの影響を最小限化するための取り組みを行っています。	適合可能
		90	医療情報システムの保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関するガイドライン第 4.1 版」6.8 章 C 項の管理策を実施。	保守作業は外部事業者に委託していません。	対象外
	7.6.6 ネットワークセキュリティ管理	91	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実施。	本番環境に関するセキュリティゲートウェイは、当社サービスを構築・運用するクラウド基盤を提供する Google の主管となります。Google による本事項への対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。Google によるセキュリティ対策に加え、クラウド基盤上での当社サービス固有の取り組みとして、ファイアウォールによるポートや接続制限を実施しています。	適合可能
		92	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）。		適合可能
		93	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。	当社の本番環境（物理サーバ層）におけるネットワークセキュリティ対策は、ファイアウォールの設置以外は上記の項目の理由により Google が主管しています。Google による本事項への対応状況は『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		94	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。		適合可能
		95	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実施。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、同様の制御を実施。		適合可能
		96	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実施。		適合可能
		97	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ように設定。		適合可能
		98	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を含める。		適合可能
		医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定。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			
		99	外部からの医療情報システムの稼働監視・遠隔保守。	当社サービス（仮想層）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は、サービス提供に必要不可欠のものに限定した上で接続管理を実施しています。当社サービスで利用	適合可能
		100	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。		適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		101	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。	している情報処理上のリソースのリストは、Google が機能提供する Google Cloud Platform の管理画面（Cloud Console）で一覧化されており、オープンネットワークとの未許可の接続等が発生した場合は、適時に検知可能です。	適合可能
		102	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。		適合可能
		103	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。		適合可能
		104	時刻同期のための時刻配信サーバへのアクセス。		適合可能
		105	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）。		適合可能
		106	その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医 療情報データベース等）。		適合可能
		107	医療情報システムのサーバ機器等への同時ログオンユーザ数（OS アカウント等）に適切な上限を設ける。	当社サービスは医療情報を扱っておりません。	対象外
		108	ネットワーク接続ログ（認証ログ及び接続ログ）の記録。	当社の本番環境（物理サーバ層）におけるネットワークセキュリティ対策は Google の主管範囲となるため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。Google のセキュリティ対策に加え、当社のシステム環境において設置するファイアウォールにおいても、以下の取り組みを実施することで、よりセキュアなネットワーク管理に向けた対策を実施しています。 ・ネットワーク接続のログに関しては、ファイアウォールで取得しており、また各サーバもアクセスログを取得して、ログを管理しているストレージに保存している。 ・ログに関しては、通常とは異なるアクセスパターンの有無を確認しており、不正なアクセスがあった際は検証を実施している。	適合可能
		109	ネットワーク接続ログを定期的に検証し不審な活動が行われていないことの検証。		適合可能
		110	医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しない。	本項目は当社サービス提供のクラウド基盤（物理サーバ）を主管する Google の対応事項となるため、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		111	VPN 接続を行う場合には以下の事項に従う。	当社サービスはオプションとして VPN 接続サービスを提供しております。提供の際は事業者ごとにインターネットと隔離されたプライベートネットワークを構築し、暗号化された通信によって接続しています。	適合可能
		112	接続時に VPN 装置間で相互に認証を実施。		適合可能
		113	傍受、リプレイ等のリスクを最小限に抑えるために、「7.6.11 暗号による管理策」に従い、適切な暗号技術を利用する。		適合可能
		114	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。		適合可能
		115	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。		適合可能
	7.6.7 電子媒体の取扱	116	電子媒体について情報処理事業者施設外への不要な持ち出しを行わない。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を No127 に示す方式にて確実に廃棄処分。	社内向け機密情報保護規定に則り、重要情報持ち出しの際は暗号化（GPG 暗号化）し持ち出すように徹底しています。	適合可能
		117	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。		適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		118	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の維持。		適合可能
		119	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、鍵管理についての十分に配慮。		適合可能
		120	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。		適合可能
		121	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、他媒体に複写。		適合可能
		122	情報を保管する為にハードディスク装置を用いる場合、RAID-1 もしくは RAID-6 相当以上のディスク障害に対する対策の実施。	本項目は当社サービスをクラウド上で提供する際のシステムの物理 OS 層を主管する Google の主管範囲となります。『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		123	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実施。	社内向け機密情報保護規定に則り、重要情報持ち出しの際は暗号化（GPG 暗号化）し持ち出すように徹底しています。	適合可能
		124	電子媒体を廃棄する場合、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の確認。		適合可能
	7.6.8 情報交換に関するセキュリティ	次の情報交換方法について予めの合意			
		125	情報を電子媒体に記録して交換する際の手順。	個人情報および医療情報の保存は当社の環境では一切行っておらず、Google が提供するクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google（外部事業者）が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		126	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。		対象外
		127	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。		対象外
		128	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。		対象外
		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実施			
		129	発送者、受領者を識別し記録。	個人情報および医療情報の保存は当社の環境では一切行っておらず、Google が提供するクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google（外部事業者）が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		130	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、否認防止対策を実施。		対象外
		131	交換する情報の機密レベルに関して合意（受領側で機密レベルが低くならないこと）。		対象外
		132	交換された情報に悪意のあるコードが含まれていないことを確実とする。		対象外
		物理的に情報を搬送する際には以下の対策を実施			
		133	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。	個人情報および医療情報の保存は当社の環境では一切行っておらず、Google が提供するクラウド基盤 Google Cloud Platform に限定しています。本項目に関する Google（外部事業者）が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	対象外
		134	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。		対象外
		135	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。		対象外
		136	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。		対象外
		137	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。		対象外
		138	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。		対象外
		電子的に情報を転送する際には以下の対策を実施			
		139	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。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	個人情報および医療情報の保存は当社の環境では一切行っておらず、Google が提供するクラウド基盤 Google Cloud Platform に限定しています。本項目に	対象外

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			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。	関する Google（外部事業者）が運用するデータセンター及びサーバ環境に係る物理的な安全対策状況については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	
		140	送受信する経路を適切な方法で傍受のリスクからの保護。		対象外
		141	受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じる。		対象外
		142	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。		対象外
	7.6.9 医療情報システムに対するセキュリティ要求事項	143	運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類を運用システム上に置かない。	当社サービスの本番環境では、プログラム実行に最小限のソフトウェアで運用しています。そのため、不必要なファイルやコンパイラ等の開発ツールは本番環境にはありません。本番環境を更新する際は継続的インテグレーションツールで自動化しているため、本番環境のサーバで人が作業することがなく、運用ミスも起きないようにしており、仮に障害等が発生した場合も常時の監視体制のもとで適時の復旧を可能にしています。	適合可能
		144	情報処理に不必要なファイル等を運用システム上に置かない。		適合可能
		145	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。	当社サービスのソフトウェアを更新（リリース）する際は、事前に社内でテスト（結合テストならびに総合テスト）を行っており、更新時の思わぬ影響がでないように確認評価しています。このテスト環境は本番環境とオペレーティングシステムやミドルウェアの環境を同じにしており、その環境でテストを行うことで OS やミドルウェアレイヤーの検証も実施しています。	適合可能
		146	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、監査に必要なログを取得。	システムに必要なライブラリの更新や変更などの管理はライブラリ管理ツールを用いており、管理ツールの変更履歴などはログで取得保存しています。	適合可能
		147	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、監査証跡とするためにログを取得。	当社サービスの本番環境での設定やファイルは、全て定期的なバックアップとログ取得をしています。本番環境に影響がある作業時は、事前に作業内容をログとして保管するプロセスとしています。	適合可能
	7.6.10	148	提供するアプリケーションについて、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実施。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。	社内セキュリティチームにより、プラットフォーム診断/ペネトレーションテストを定期実施しています。	適合可能
		149	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、公開される最新の脆弱性情報を参照し、迅速に対応策を実施。	社内でセキュリティ対策チームを設置し、脆弱性に対する品質管理を実施しています。	適合可能
		150	アプリケーションにて情報の登録、編集、削除等を行う際、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実施。	当社サービスの本番環境に影響がある作業は、一部の特権がある担当者のみが行うことができるようにしています。そのような作業をするときは、事前の承認プロセスで何をするのかを把握したうえで操作ログを取得しており、問題発生時に分析できるようにしています。	適合可能
		151	アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存。	クラウド上の認証情報は暗号化されてデータベース/ストレージに保管されており、パスワードは全てハッシュ化されて保存されています。	適合可能
		152	アプリケーションによる情報操作について、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止。	職務権限に応じて情報操作が可能なメンバーを管理することができます。	適合可能
	7.6.11 暗号による管理策	153	暗号アルゴリズムは十分な安全性を有するものを使用。選択基準としては電子政府推奨暗号リスト 42 等を用いる。	十分な安全性を有する一方向ハッシュ関数（SHA-256 など）を使用しています。	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		154	暗号鍵が漏洩した場合に備えた対応策を策定。	インシデントが発生した場合、直ちにセキュリティ担当及び開発責任者による承認フローを得た上で対応策を実施する運用ルールを策定しています。	適合可能
		155	電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとする。	サーバ証明書は WebTrust 規準を満たした認証局が発行する証明書を利用しています。クライアント証明書は、ユーザの存在を当社で確認するため、当社が発行した証明書を利用しています。	適合可能
		156	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。	IPA が発信するセキュリティ情報を基準に暗号化レベルを見直し、必要に応じて切り替えるプロセスとしています。	適合可能
		157	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。	当社サービスと医療機関がデータをやりとりする際は、ネットワークで通信を暗号化して実施しています。その暗号化はサーバ証明書とクライアント証明書の双方で認証しているため、データの改ざんや漏洩のリスクは最小限化されています。	適合可能
	7.6.12 ログの取得及び監査	158	作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成して管理。	アクセスログはクラウド上で 9 ヶ月保管しています。	適合可能
		159	監査ログを定期的に検証して不正な行為、システムの異常等を検出。	仮想層のアクセスログ、エラーログ、パフォーマンスログは常に監視しており、異常時には通知をトリガーに調査するような運用をしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		160	ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期。	仮想層で稼働しているすべてのサーバは NTP サーバと同期して運用しています。そのときのセキュリティ対策として、各サーバのゲートウェイとなる入り口にファイアウォールを設置しており、外部からの通信は遮断するようにしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		161	標準時刻に同期する時刻提供元は信頼できる機関を利用。	仮装層においては Google が提供する Google Public NTP を使用しています。	適合可能
		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			
		162	ログデータにアクセスする作業者及び操作を制限。	仮想層では下記の対策をしています。 （１）ログ自体が改ざんされるリスクについては、ログデータは限られたシステム管理者しかアクセスできないようにしており、さらに特権管理者以外は閲覧のみできる状態です。特権管理者のみが編集削除できるようにしており、担当者によるログ改ざんリスクを最小限にしています。 （２）データ増加によりログが保存できなくなるリスクについてはディスクの空き容量を監視しており、定期メンテナンス時に必要に応じて容量を追加する運用をしています。物理層における本取り組みは、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	適合可能
		163	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実施。		適合可能
		164	ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施す。		適合可能
	7.6.13 アクセス制御方針	165	情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理。	社内向け機密情報保護規定にて規定済です。	適合可能
		166	情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理。		適合可能
		167	アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定。	仮想層（当社管理）アカウントの登録変更破棄プロセスは下記の通り運用しています。 （１）アカウント発行は特権を持っている管理者のみが発行できます。アカウントを発行する際は、その担当者が行う業務を確認したうえで操作できる権限を限定した形で発行しています。 （２）アカウントの削除や変更については、月に 1 度アカウントのクリーニングを実施しております。その際に、各アカウントの使用有無、退職の有無、業務内容の変更有無を確認し、変更があるアカウントについては変更または削除を行います。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		168	それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグ	仮想層（当社管理）のアカウントを発行する際は、そのアカウントを利用する担当の業務に応じて最小限の権限を付与しています。データアクセスについ	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
			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実施。	ては、閲覧する範囲とその範囲において閲覧のみか編集もするかというマトリックスでグルーピングして権限を付与しています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	
		169	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。		適合可能
	7.6.14 作業者アクセス及び作業者 ID の管理	170	作業者を情報処理装置上にてユニークな作業者 ID により識別。	当社が管理する仮想層の本番環境に係るアカウントは、担当ごとに全てユニークなアカウントを利用しており、開発環境については GSuite でアカウントをユニークに付与しています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		171	作業者 ID を発行する際に、既存の ID との重複を排除する仕組みを導入。	本番環境で利用しているシステムの設定により、当社が管理する仮想層で重複する ID は発行できません。ID 発行申請に際して重複有無の検証を必ず行うプロセスとしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		172	複数作業者で共用するためのグループ ID の利用は原則として行わず、業務上必要であればログ上で操作の実施者が特定できるように、作業者 ID でログオンしてからグループ ID に変更する仕組みを利用。	当社が管理する仮想層の本番環境の ID 使い回しやグループ ID は使用しておらず、すべてユニークな ID で作業をしています。当社サービスの本番環境での作業はすべてログを取得しており、どのアカウントでどういう操作をしたのかが把握できるようにしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		173	作業者 ID の発行は医療情報システムの管理に必要な最小限の人数に留める。	当社が管理する仮想層の本番環境では、当社サービスの開発保守をする最低限にしか付与していません。その運用に際しては、アカウント発行時に特権を持っている管理者と責任者の承認確認ののちアカウント付与を実施しています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		174	作業者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とする。	当社が管理する仮想層の本番環境では、担当が変更あるいは退職した時点で ID の利用停止を実施しています。ID の変更削除については、月に 1 度アカウントのクリーニングを実施しています。各アカウントの使用有無、退職の有無、業務内容の変更有無を確認し、変更があるアカウントについては、変更または削除を行います。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		175	監視ログの監査時に作業者を確実に特定するため、作業者 ID は過去に使われたものを再利用しない。	当社が管理する仮想層の本番環境における作業者 ID を特定できるようにするため、作業者 ID の使い回し（共有）は禁止しています。当社サービスの本番環境に影響ある作業時は、事前に作業者が作業内容を申請して承認の後に実施するため、誰が何をしたかを適時にトレースできるようにしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		176	不要な作業者 ID が残っていないことを定期的に確認。	当社が管理する仮想層の本番環境の作業者 ID の変更削除については、毎月月末にアカウントのクリーニング作業をしています。各 ID 保有者の利用状況や業務内容の変更有無、離職の有無を確認し、変更がある ID は変更削除を実施しています。物理層における本取り組みは『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		177	特権 ID の発行は必要な最小限のものに留める。	特権 ID は開発責任者の承認（ワークフロー）を得た上で発行しています。	適合可能
		178	特権使用者に昇格可能な作業者 ID を制限。	特権使用者に昇格可能な作業者 ID は開発責任者の承認（ワークフロー）を得た上で発行しています。	適合可能
		179	特権の使用時には作業実施内容を記録。	特権の使用は作業内容を定義した上で、かつ開発責任者の承認も得た上で実施しています。作業内容は開発管理アプリケーションにて管理しています。	適合可能
		180	管理端末以外からの特権 ID による直接ログオンの禁止。	特権 ID によるログインは、社内の限定したネットワーク経由のみのアクセスに制限しています。	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		181	情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについて削除あるいはパスワード変更の実施。	当社が管理する仮想層の本番環境にて、当社作業員が担当する当社サービスで利用しているシステムはすべてGoogle Cloud Platformのクラウド基盤上にあるサービスを利用しており、それ以外の機器・装置は利用していません。クラウド上で利用しているサーバやソフトウェアについては、アカウントは最小限にして運用しており、初期時のアカウントや必要ないアカウントは削除しています。毎月アカウントはクリーニング作業しており、そこで不必要なアカウントが発生していた場合は削除するようにしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		182	医療情報システムへのログオン用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の情報保管。	パスワードは全てハッシュ化され保存されています。	適合可能
		183	医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者へ強制。	パスワードは定期的に変更する運用ルールを制定し、定期的に遵守しているかどうかを管理者が確認する仕組みを導入しています。	適合可能
		184	医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにする。	社内でパスワードポリシーを規定しています。	適合可能
		185	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。		適合可能
		186	パスワード発行時、乱数から生成した仮の医療情報システム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。	仮想層の本番環境において作業者IDのパスワードを利用者に変更してもらうようにアナウンスしています。特権IDについては、限られた管理者が5世代前以外のパスワードを変更時に設定する運用となっています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		187	パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とする。	仮想層の本番環境における特権ID、及び作業者IDのパスワードルールは以下の通りです。 ＜技術的な対応＞ ・8文字以上 ・半角英数字を混在 ・記号を含める ＜運用面の対応＞ ・定期的なパスワードの変更 ・パスワードを複雑にするよう依頼 ・パスワードを使い回さないよう依頼 物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		188	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底。	仮想層の本番環境ならびに開発テスト環境では、個々人の端末を利用しているため、第三者が利用するケースは一切ありません。よって、パスワードの自動記憶による権限のない第三者によるシステムへのアクセスのリスクは極小化されていると考えています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		189	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。また、一般の作業者による閲覧を制限。	パスワードに関するデータは全て暗号化されて上で保持しています。	適合可能
		190	端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを実施。	仮想層の本番環境のログインID（作業者ID）は、一定時間の未使用時には強制的にセッション遮断、またはログオフする設定となっています。	適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		191	パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とする。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入。	パスワード入力が不成功に終わった場合の再入力に対して、一定の不応時間の設定は行なっておりませんが、定期的にアクセスログの監視を行い不正なアクセスを検知できる対応を実施しています。	適合可能
	7.6.15 作業者の責任及び周知	192	各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護。	セキュリティ教育について記載する物理層における本取り組みは、『Google Cloud Platform』 対応セキュリティリファレンスをご参照ください。	適合可能
		193	システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合、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。	仮想層の本番環境システムへのアクセスログ等、各種ログで不正や疑いがあったとき、またはパスワードが第三者に漏れた可能性がある場合、該当アカウントを停止してその経由の原因調査ならびに再発防止策を行うプロセスを実施しています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		194	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。	仮想層の本番環境へアクセスする端末が設置された執務室からの離席時・退社時は、ログオフないしシャットダウンを行うよう周知しています。端末の複数人での利用は原則禁止しており、万が一のために一定時間でログオフする設定にしています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
7.7 人的安全対策		195	医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として、秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。	従業員全員に対して、採用時に機密保持契約を締結しています。	適合可能
		196	医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対して情報セキュリティに関する一定水準の知識の理解を持つ、 あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行う。	2ヶ月に1度、セキュリティ教育訓練を実施しています。	適合可能
		197	情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証。	社員、業務委託の関係者による不正と思われる行為を検知した場合、直ちにアクセス権を停止し、開発管理者によって影響範囲の特定、データの改竄、破壊などが行われてないかどうか検証します。	適合可能
		198	医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。	取り扱う業務は全てクラウド上で保管され、退職または委託終了時はPCを返却し、全ての情報に対するアクセス権を停止します。	適合可能
		199	医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設ける。	医療機関等との委託契約は実施しません。全ての従業員及び業務委託について機密保持契約を締結し、定期的にセキュリティ教育を実施しています。	対象外
7.8 情報の破棄		200	CD-R 等の廃棄については「7.6.7 電子媒体の取扱」を参照すること。	情報記録電子媒体にコピーできないようにアクセス制御がされています。	適合可能
		201	ハードディスク等の廃棄については「7.5.4 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。		適合可能

医療情報を受託管理する情報処理事業者における安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対するスリーシェイクの見解	ガイドラインへの適合性
		202	情報処理事業者は医療情報安全管理ガイドラインに従って情報の破棄を行った記録を提出。		適合可能
7.10 医療情報処理に関する事業継続計画	7.10.1 要求事項の識別	203	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。	当社が所管する仮想層における当社サービスの開発/保守・運用に求められるシステム構成環境（端末、ネットワーク、機器・装置等）に係る情報は漏れなく当社内で台帳等により一元的に管理しています。これらの構成環境を用いて医療機関等へ安定的且つ継続的にサービス提供するための開発/保守管理・運用管理プロセスは当社内マニュアル・手順書として整備され、日々の保守・運用をする中で必要に応じた見直しを行うプロセスとなっています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		204	業務プロセス間の相互関係を評価。	当社が所管する仮想層における当社サービスの開発/保守・運用管理業務は、手順書・マニュアルとして文書化・整備され、各業務がどのように関連するかという相互関係は可視化されています。物理層における本取り組みは、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
		205	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。	事業継続計画を策定し運用することで問題発生時には適時に復旧できるようにしています。詳細は事業継続計画に記載しています。	適合可能
		206	医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別。	医療情報を扱わないため、対象外となります。	対象外
		207	医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別。		対象外
		208	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見 読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を検討。	システムを停止させずに安定的かつ継続的に稼働させるために、システムの冗長化や拡張性の高いアーキテクチャーを採用しています。データベースの冗長化をはじめ、基盤のダウンタイムを最小に抑える仕組みやリアルタイムの監視システムなど、システムの可用性を高める対策を実施しています。	適合可能
		209	医療機関等に提供する情報処理サービス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、情報処理サービス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本ガイドラインで提示する物理的安全対策を施す。	当社サービスは Google が提供するクラウド基盤 Google Cloud Platform のもとで運営を行っており、物理的なシステム環境は Google の主管範囲となります。情報処理施設等の代替・バックアップ施設等、ファシリティ面の物理的な冗長化対策については、『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。	適合可能
	7.10.2 事業継続計画の立案及びレビュー	210	医療情報システムのサービス提供における業務プロセス及び医療情報システムの優先順位にもとづいて、医療情報処理に関する事業継続計画を策定。	当社では Google が提供するクラウド基盤 Google Cloud Platform にてサービス提供を行っているため、物理層の主管は Google となることから、物理的なシステム環境が利用不可となる事態、あるいは悪意ある外部者によるプラットフォームを標的とするサイバー攻撃を想定した事業継続計画は独自では策定していません。本内容については、Google による『Google Cloud Platform』対応セキュリティリファレンスをご参照ください。当社所管の仮想層を対象とした当社サービスの事業継続計画には、次の事項を含めて文書化、及び関係者間の認識共有を図っており、当社の所管範囲で事業継続に影響のないようにしています。 ・障害発生時の全体フロー ・障害発生時の障害レベル判断手順 ・障害発生時の関係者の共有、対応人員の配置 ・一次対応手順 ・恒久対応手順 ・障害発生時の医療機関への周知フロー ・各所関係者への連絡フロー	適合可能

医療情報を受託管理する情報処理事業者における 安全管理ガイドライン（平成２４年１０月）				対応状況	
項目番号		No	要求事項	ガイドラインに対する スリーシェイクの見解	ガイドライン への適合性
		211	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のレビュー。	当社所管の仮想層では、障害レベルの大小含めた日々のなかで起きるトラブルの中で実務的に検証を重ねており、問題発生の度に問題箇所の原因追求や再発防止策、ならびにこのプロセスの振り返りを行い、常に具体的な業務フローや手順等の見直しを実施しています。よって、特定の時点で模擬試験を行い、事業継続のプランを見直すのではなく、日々の業務のなかで継続的な見直しを行うという方式を採用しています。	適合可能
		212	事業継続計画について定期的に見直しを実施。		適合可能