『きりんカルテ』ガイドライン対応リファレンス

経済産業省版

2019 年 7 月 26 日
2019 年 8 月 26 日改正
きりんカルテシステム株式会社

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
2.1 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		1	医療情報に係る情報処理事業を受託する機関においては、医療情報の安全確保を目的として、合理的・客観的な基準による公正な第三者認証を取得すること。	当社は、第三者認定としてプライバシーマークを取得しています。登録番号は、第10824469（02）号です。ホームページ上（https://xirapha.jp/privacy-policy/）にも掲載しています。	○
2.2 情報資産管理	2.2.1 資産台帳	医療情報が完全な状態にあることを保証するために、資産台帳等を適切に維持管理することを目的として、以下の管理策を適用すること。なお、資産台帳等の媒体は、紙文書、電子ファイルのいずれでも良いが、媒体特有の脅威について把握し、適切な管理策を追加すること。			
		2	（１）医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。	当社が提供する電子カルテシステム（以下、「当社サービス」という。）にて医療機関等から預かる情報は、患者の個人情報、医療情報があります。メインの情報は、患者の個人情報ならびに医療情報です。その他、医療機関の情報や、当社のサービス開始時の他社からの移行データ、アンケート等があります。これらの情報については、JIS Q 15001が規定している個人情報保護マネジメントシステム（以下、「PMS」という。）に則り、個人情報を保護する体制を整備しています。文書化については、個人情報保護方針、個人情報保護規則、個人情報安全管理規則を定めており、そのなかで個人情報管理台帳の整備について明文化しています。	○
		3	（２）預託された情報の全てを資産台帳に記録すること。	医療機関等から預かる情報は、すべて個人情報管理台帳に取得目的ごとに記入して管理しています。個人情報管理台帳は、原本を紙でファイリングしてPMSの管理事務局（以下、「PMS事務局」という。）が一元管理しています。	○
		4	（３）必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。	個人情報管理台帳は、紙でファイリングしてPMS事務局が一元管理しており、社内の所定の場所で管理し、PMS事務局はすぐに閲覧・編集することができるようにしています。	○
		5	（４）資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。	個人情報管理台帳は、社内の所定の場所でPMS事務局が管理しています。他のメンバーの閲覧が必要なときは事務局への申請ならびに承認を必須としており、PMS事務局が承認しないメンバーが台帳へ自由にアクセスすることができないようにしています。	○
		6	（５）資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。	個人情報管理台帳は紙にて管理しています。該当の紙資料はPMS事務局が所定の施錠可能なキャビネットにて管理し、当該キャビネットの鍵はPMS事務局の権限者が保管しているため、本来権限のないメンバーがアクセスすることはありません。	○
	2.2.2 情報の分類	7	（１）情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。	当社では氏名や一部情報だけであっても、情報のレベルを分類せずに一律重要情報として管理するようにしています。医療機関等から預かる情報は全て重要なものと当社は考えます。個人情報ならびに医療情報は、たとえ氏名や一部情報だけであっても漏洩すれば患者や医療機関のプライバシー問題、医療機関や会社への信頼問題に発展する恐れがあります。そのため情報のレベル分類は一律重要情報として管理しています。	○
		8	（２）情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。	社内で扱う個人情報、医療情報はすべて目的ごとに個人情報管理台帳で管理しています。定期的な確認という観点では、まず情報を扱う前に、管理者、所有者を管理台帳上で明記し承認するプロセスがあります。また管理台帳を定期的（半期ごと）に見直しクリーニングを行っており、その際に各管理台帳の業務ならびに責任者、所有者を確認しています。	○
		9	（３）預託される情報に対して分類にもとづいたリスク分析を実施すること。	個人情報ならびに医療情報を扱う場合は、個人情報管理台帳に記載するとともに、リスク分析表を事前に記載し、情報管理の責任者とPMS事務局が承認するというプロセスを取っています。リスク分析表では、取得入力、移送送信、利用加工、保管バックアップ、削除破棄の観点で起こりうるリスクとそのリスク低減に対する管理策を事前に取り決めています。また、実際の業務開始以降は、作業者はリスク分析表に則ってリスク低減に必要な管理策を実施し、管理者がそのプロセスを点検確認するように運用しています。	○
		10	（４）リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。		
		11	（５）分類がわかるように情報にラベルをつけること（電磁的な記録にラベルをつけ	当社では氏名や一部情報だけであっても、情報のレベルを分類せずに一律重要情報として管理するようにし	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
			る方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。	ています。その上で、医療機関から預かる情報のうち電子カルテシステム当社サービスの個人情報、医療情報については、すべてMicrosoft Corporationが提供するクラウド基盤Microsoft Azureで管理しており、その承諾は当社が定める当社サービスのService Level Objective（以下、「SLO」という。）にて明記しています。医療機関には、サービス申し込み前にこのSLOを確認いただき同意していただくようにしています。	
		12	（６） 各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。	ラベルではなく、情報取得の目的ごとに、取得入力、移送送信、利用加工、保管バックアップ、削除破棄を定めています。基本的な方針は、その目的で作業する作業者のみが情報にアクセスできるようにしており、Microsoft Azure上の情報については、特定のシステム管理者のみがアクセスできるようにしています。	○
2.3 組織的安全管理策（体制、運用管理規程）		13	（１）医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	安全管理に関する方針は、当社で個人情報保護規則を定めています。医療情報の安全管理に関する方針については、本リファレンスに記載しており、内部の管理体制・プロセスの変更に伴い、適宜更新を行い、最新の方針をいつでも医療機関等が確認できるようにしています。	○
		14	（２）個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	個人情報保護に関する方針は、個人情報保護方針を定めています。ホームページ上に「個人情報保護方針（https://xirapha.jp/privacy-policy/）」ならびに「個人情報の取り扱いについて（https://xirapha.jp/privacy-policy/handling/）」を掲載しており個人情報の利用等について明示しています。	○
		15	（３）個人情報保護に関しては、医療機関等の監督の下に行うこと。	No14で記述する通り、当社の個人情報保護に関する方針はホームページ上に公開しており、医療機関等の監督責任担当者が自機関のポリシーに合致するか否かをいつでも確認可能としています。これにより、医療機関等にとって、当社が実施する個人情報保護に関する取り組みを可視化し、管理監督を円滑且つ効果的に行えるようにしています。	○
		16	（４）情報処理の安全管理に関わる手順書、運用管理規程を整備すること。	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ており、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。	○
		17	（５）運用管理規程には、情報セキュリティに対する組織的取り組み方針、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。		
2.4.医療情報の伝達経路におけるリスク評価		18	医療情報の取扱いに際しては高い機密性が求められていることに配慮しなければならない。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である。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うこと。	医療情報の取扱に関してのリスク評価は、PMS（JIS Q 15001）を前提に、リスク評価と対策を行っています。この要求にある項目に関しては、情報の入り口は当社サービスを利用する医療機関からのみで、ネットワークは暗号化しており、漏洩や改ざんなどがおきないようにしています。またデータの保存管理については、Microsoft Corporationが提供するクラウド基盤Microsoft Azureを利用しており、第三者や不正、災害などの想定しうるリスクについて機密性、完全性、可用性が保てるようにシステム構築・運用保守を行っています。	○
2.5 物理的安全対策	2.5.1 医療情報処理	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こと。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認すること。			

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
	施設の建物に関する要求事項	19	（１）医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理が行われていること。	医療情報の保存は当社の環境では一切行っておらず、Microsoft Corporationが提供するクラウド基盤Microsoft Azureに限定しています。本項目に関するMicrosoft Corporation（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、株式会社三菱総合研究所および日本ビジネスシステムズ株式会社が実施した医療機関向け『Microsoft Azure』対応セキュリティリファレンス（https://www.mri.co.jp/service/201602_021630.html、以下『Microsoft Azure』対応セキュリティリファレンス）をご参照ください。	○
		20	（２）傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては、十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施すこと。		
		21	（３）建物、部屋に対する不正な物理的な侵入を抑止するため、侵入検知装置を導入すること。		
		22	（４）自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。		
	2.5.2．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	（１）	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を行うこと。	当社サービスは、Microsoft Corporationが提供するクラウド基盤Microsoft Azure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Microsoft Corporation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、【（３） 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。	○
		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を利用すること。		
		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を確認すること（履歴の保全については「2.6.12.ログの取得及び監査」を参照）。		
		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こと。		
		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、身分を確認すること。		
		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こと。		
		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すること。		
		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。		
		（２）	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を確認すること。	当社サービスは、Microsoft Corporationが提供するクラウド基盤Microsoft Azure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Microsoft Corporation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、【（３） 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。	○
		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、確実な鍵管理を行うこと。		
		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は、作業者、作業開始時刻、作業		

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
			終了時刻、作業内容等について記録すること。		
		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を確認すること。		
		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こと。		
		（３）	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を確認すること。	当社サービスは、Microsoft Corporationが提供するクラウド基盤Microsoft Azureに構築しているため、実質的には当該システムの設置先は外部事業者であるMicrosoft Corporation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。本項目については、Microsoft Corporationによる『Microsoft Azure』対応セキュリティリファレンスをご参照ください。なお、当社サービスへリモートでアクセスする端末を設置する自社の執務室は、Felicaカードによる認証と暗証番号による認証の２重化を行っており、防犯カメラによる24時間の監視ログ取得を行っており、自社環境においても確実な入退室管理を徹底しています。	○
	2.5.3 情報処理装置のセキュリティ	37	（１）不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。	当社サービスは、Microsoft Corporationが提供するクラウド基盤Microsoft Azureを利用しています。当社サービスにて利用している情報処理上のリソースのリストはMicrosoft Azureの管理画面（Azureポータル）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。	○
		38	（２）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。また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。	○
		39	（３）医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。	医療情報ならびに個人情報を扱う業務はすべて執務室内で行い、執務室外や社外では行えないようにしています。また、医療情報ならびに個人情報を扱うエリアを定めており、そのエリア内はカメラやスマートフォンなどの持ち込みを禁止しています。執務室内は、業務委託や部外者は立ち入りできないようにしています。上記の取り組みにより、本来、医療情報へアクセスする権限のない者が万が一にも医療情報へアクセスすることを未然防止しています。	○
		40	（４）医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにすること。	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ならびに個人情報が保存されないようにしています。また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。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。	○
		41	（５）火災発生時の消火設備が機器に損傷を与えないよう配慮すること。	本項目は、当社サービスのクラウド基盤を提供しているMicrosoft Corporationの対応事項となるため、『Microsoft Azure』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。	
		42	（６）医療情報システムを配置する室内での喫煙、飲食を禁止すること。		
		43	（７）医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。		○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		44	（８）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こと。		
		45	（９）保守点検で障害不良等が発見された際の対応作業等を行う際には情報処理事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにすること。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出すこと。記憶装置等、障害により情報の消去が不可能となっている装置については、補修ではなく物理的な破壊を行ってから廃棄を選択すること。		
		46	（１０）医療情報システムを設置するサーバラックについては、以下の安全管理策を実施すること。 ・震災時に転倒することが無いよう確実に設置すること。 ・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こと。 ・扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。		
		47	（１１）起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「2.6.14.作業者アクセス及び作業者ＩＤの管理」に従うこと。		
		48	（１２）情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。	本項目は、当社サービスのクラウド基盤を提供しているMicrosoft Corporationの対応事項となるため、『Microsoft Azure』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。なお、当社においても、ミドルウェアやアプリケーションにおける対策として、データの冗長化と定期的なバックアップを行っています。Microsoft Corporationのデータセンター災害時にも、医療機関等のデータを復元したうえで迅速に当社サービスを復旧できる対策をしています。	○
		49	（１３）不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。	本項目は、当社サービスのクラウド基盤を提供しているMicrosoft Corporationの対応事項となるため、『Microsoft Azure』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。	○
	2.5.4 情報処理装置の廃棄及び再利用に関する要求事項	50	（１）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を確認すること。	本項目は、当社サービスのクラウド基盤を提供しているMicrosoft Corporationの対応事項となるため、『Microsoft Azure』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。なお、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。	○
		51	（２）サーバ等のＢＩＯＳパスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。		
		52	（３）ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。		

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		53	（４）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こと。		
	2.5.5. 情報処理装置の外部への持ち出しに関する要求事項	利用中の情報処理装置を外部に持ち出す行為は原則として禁止するが、製造元でのみ可能な補修が必要な場合など、止むを得ない事情により外部への持ち出しを行う場合には、以下の管理策を適用すること。			
		54	（１）情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。	医療情報はサーバのみに保存しており、端末には保存されないようにしています。また、社内の医療情報の有無を問わずすべての端末に対して、執務室から持ち出す時は管理台帳への記入と管理者が承認するフローを運用しており、不適切な持ち出しが起こらないようにしています。	○
		55	（２）持ち出した機器を再度設置するための適切な検証手順を策定すること。	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。また、USBメモリなどの外部記憶媒体は使用を禁止しています。また万が一接続した場合も、セキュリティソフトでスキャンされるため、不正プログラムなどの検知ができるようにしています。	○
2.6.技術的安全対策	2.6.1. 情報処理装置及びソフトウェアの保守	56	（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こと。	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。	○
		57	（２）変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。	No56と同様に、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。	○
		58	（３）医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。	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。	○
		59	（４）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立てて実施すること。	当社サービスのリリースや保守作業が発生する場合は、深夜0:00～6:00の間に行っており、医療機関が業務をする時間を避けた上で保守を行っています。	○
		60	（５）情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。	当社サービスをリリースする際は、リリース手順書を事前に作成しており、実施の際はその手順書に基づいて担当者と管理者が手順の検証を都度行っています。また、システム停止を伴うメンテナンスを行う際は、実施の７日前までに事前に利用者にアナウンスし、業務影響がないように行っています。	○
		61	（６）不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。	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	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
				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。	
		62	（７）医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。	当社サービスの脆弱性については、脆弱性スキャナーツールでの巡回と、定期的に第三者のセキュリティレビューを受けています。そこで発見された脆弱性については、脆弱性の重要度／危険度に応じてレベル分けを行い、対応時期を決めた上で対応実施するように管理しています。	○
		63	（８）潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。		
		64	（９）修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。	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。	○
		65	（１０）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、「2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。	保守ならびに開発を外部事業者に一部再委託をしています。ただし、再委託先においても、上記No56から64の要件を満たすよう契約を求めており、それに基づく運用を行っています。また、利用者に関しては利用規約にて委託の条項を設けており、当社サービスの利用開始時に同意をいただいています。上記の取り組みを通して、再委託に伴う管理品質の低下を防止するとともに、利用者（医療機関等）にとって、どのような体制のもとで当社サービスを提供しているかについて説明責任を果たすプロセスとしています。なお、再委託先との契約にかかわらず、医療機関等へのサービス提供における責任はすべて当社が担っています。	○
	2.6.2.開発施設、試験施設と運用施設の分離	66	（１）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こと。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こと。	当社サービスは、カルテは自社開発、レセプトコンピュータは日本医師会ORCA管理機構が提供するORCAを利用しています。自社開発ならびにORCAも含めて、当社サービスの本番環境のリリース時は、事前に結合テスト、総合テストを行っており、安全性や問題がないことを確認した上でリリースをしています。	○
		67	（２）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（以下、「開発施設」という。）を用いて行うこと。	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行っています。	○
		68	（３）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）と接続を持つ場合には「2.6.3.悪意のあるコードに対する管理策」に従うこと。	開発施設（社内）で用いる端末はインターネットに接続をしていますが、セキュリティソフトを導入しており、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。	○
		69	（４）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、検知策を実施すること。	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。	○
		70	（５）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こと。	本番環境と開発環境は物理的にデータも含めて別れており、開発環境ならびにテスト環境では、ダミーのデータを利用して開発・テストを行っており、医療データをそのまま開発・テスト環境で使うことは禁止されています。	○
		71	（６）医療情報を開発及び試験用データとして直接、利用しないこと。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に示し、了解を得た上で利用すること。		
	2.6.3.悪意のあるコードに対する管理策	72	（１）最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木	開発環境に用いる端末にはセキュリティソフトを導入しており、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）等の検知ができるようにしています。本番環境の仮想層は、開発したプログラムと特定のライブラリ・サーバソフト	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
			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。	しか導入しておらず、悪意のあるソフトウェア等の混入は開発環境で未然防止する体制のため、特にセキュリティソフト等の対策は行っておりませんが、常時本番環境上のログモニタリングを行うことで、悪意のあるコードやソフトウェアの挙動有無を監視する取り組みを補完的に実施しています。なお、物理サーバ層のセキュリティ対策はMicrosoft Corporationの主管範囲となります。そのため、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	
		73	（２）悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ・リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信） ・リスク評価の結果として必要であれば定期的にスキャンを実施 ・電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン ・定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ・管理者以外による設定変更やアンインストールの禁止	開発環境の端末でのセキュリティソフトは、当社の特定の管理者のみが管理できるようにしており、管理者以外は設定変更やアンインストールできないようにしています。その上でセキュリティソフトの設定でリアルタイムスキャン、定期的なファイルスキャン、外部記憶装置のスキャン、自動アップデートを行っております。本番環境における物理サーバ層に係る本項目の対応状況は、Microsoft Corporationの主管範囲となるため、『Microsoft Azure』対応セキュリティリファレンスの本項目をご参照ください。	○
		74	（３）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又は隔離措置をとるといった対策が行われていること。	開発環境におけるセキュリティソフトは、当社管理者のみが設定を変更できるようにしており、インターネットに接続された時点で定義ファイル等は更新されるようになっています。そのうえで、施設内のネットワークに接続した段階で該当端末はインターネット経由で定義ファイルなどがアップデートされるようになっています。またOSのアップデートやパッチも、ネットワーク接続時にアップデートを行うようにしています。本番環境における物理サーバ層に係る本項目の対応状況は、Microsoft Corporationの主管範囲となるため、『Microsoft Azure』対応セキュリティリファレンスの本項目をご参照ください。	○
	2.6.4.ウェブブラウザを使用する際の要求事項	医療情報システム内で必要とする、ネットワーク監視ソフトウェア、サーバ制御ソフトウェア等でユーザインタフェースとしてウェブブラウザを使用する場合は、以下の要求事項を満足する体制を確立すること。			
		75	（１）ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること。	当社執務室からアクセス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。また、No37に記載の通り、当社サービスにて利用している情報処理上のリソースのリストはMicrosoft Azureの管理画面（Azureポータル）で一覧化されており、ウェブブラウザのインストール等、不正なリソース利用の発生があれば適時に検知可能です。本番環境における物理サーバ層に係る本項目の対応状況は、Microsoft Corporationの主管範囲となるため、『Microsoft Azure』対応セキュリティリファレンスの本項目をご参照ください。	○
		76	（２）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。）。		
		77	（３）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「2.6.3.悪意のあるコードに対する管理策」に即して検査されること。		
	2.6.5.第三者が提供するサービスの管理	医療情報システムが設置される領域において、有人監視、機械監視、保守点検作業、清掃作業等については、外部の事業者に作業依頼をすることが考えられる。このような第三者が提供するサービスの利用に関して、以下の管理策を実施すること。			
		78	（１）第三者により提供されるサービスの安全管理策及びサービスレベルが十分であることを確認すること。	当社サービスを提供するうえで、サービス提供に大きく影響を受ける第三者サービスは下記です。 （１）Microsoft Azure（クラウド基盤） （２）ORCA（日本医師会ORCA管理機構が提供する日医標準レセプトソフト） （１）のMicrosoft Azureとは、サブスクリプション契約、各サービスに対してSLAを確認した上で契約しており、サービスレベル、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。（２）のORCAに関しては、使用許諾契約に同意の上利用していますが、ORCAがオープンソース・ソフトウェアのため、利用前に動作や品質などの検証をおこなったうえで、利用をしています。	○
		79	（２）サービスの実施、運用、維持について定期的に検証すること。	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、その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。	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		80	（３）サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。	Microsoft Azureに関しては、メンテナンスなどサービスに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。ORCAに関しては、ソフトウェアの更新など変更があった場合は、その変更内容を社内で検証しています。	○
		81	（４）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こと。	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、Microsoft Corporationによるデータセンターの管理・運営業務のみとなります。Microsoft Corporationによる本事項への対応状況は、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		82	（５）サービス実施中に第三者が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯すること。		
		83	（６）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、情報処理事業者の職員の入室、退室手順に準ずること。		
		84	（７）サービスの変更時には、引き続き安全性が維持されていることについて適切な検証を行うこと。	Microsoft Azureに関しては、メンテナンス等、当社サービスに影響がある変更が行われる場合は、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。ORCAに関しては、ソフトウェアの更新等の変更があった場合は、変更に伴う当社サービスへの影響有無について必ず社内で検証する体制としています。	○
		85	（８）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（厚生労働省、平成22年２月）」６．８章C項の管理策を実施すること。	当社サービスの保守点検作業のうち、ソフトウェアの改修ならびに障害時の対応は、外部事業者からの派遣メンバーで対応を図っていますが、これらのメンバーは当社常駐型で当社の監督のもとで業務を行っています。その意味で、外部事業者へ業務の一部を外部委託する方式は当社では採用していません。なお、外部事業者/派遣メンバーについても、当社社員同様、会社間ならびに該当する個人と守秘義務契約を締結しています。また、これらのメンバーには、担当範囲以外のシステムの操作が出来ないようにしており、且つ、作業内容の点検、ならびにログの取得もあわせておこなっています。	○
	2.6.6. ネットワークセキュリティ管理	86	（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こと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。	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Microsoft Corporationの主管となります。Microsoft Corporationによる本事項への対応状況は、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。なお、Microsoft Corporation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行っています。また、医療機関等が当社サービスにアクセスする際は、TLS1.2での接続及びクライアント証明書を必須にしており、クライアント証明書が認証された端末からのみアクセス可能としています。	○
		87	（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こと（接続機器類のＩＰアドレスをプライベートアドレスとして設定して、ファイアウォール、ＶＰＮ装置等のセキュリティゲートウェイを通過しようとするトラフィックをＩＰアドレスベースで制御する等。）。		
		88	（３）ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。	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、No86、No87の理由によりMicrosoft Corporationが主管しています。Microsoft Corporationによる本事項への対応状況は、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。なお、Microsoft Corporationによる物理サーバ層の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、仮想層にて以下を実施することで、利用者が安全安心してサービスを利用できるようにしています。 ・ログ監視を通して、異常検出をした際は、管理者にメールで通知が行われる仕組みの採用 ・異常検出した際は、原因分析、再発防止を検討した上で、システム上の対応を行うフローの整備	○
		89	（４）ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限すること。		
		90	（５）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（以下、「ＩＤＳ」という。）及び侵入防止システム（以下、「ＩＰＳ」という。）を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行うこと。		

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		91	（６）侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行うこと。		
		92	（７）侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。		
		93	（８）侵入検知の記録には不正アクセス等の事後処理に必要な項目が含まれていること。		
		94	（９）医療情報システムにおいて、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定すること。他に必要なサービスがある場合には、医療機関等の合意を得てから利用すること。 ・外部からの医療情報システムの稼働監視・遠隔保守 ・セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ・オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード ・電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・ファイアウォール、ＩＤＳ・ＩＰＳなどのセキュリティ機器に対する不正アクセス監視 ・時刻同期のための時刻配信サーバへのアクセス ・これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等） ・その他の医療情報システムの稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）	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行っています。また、No37に記載の通り、当社サービスで利用している情報処理上のリソースのリストは、Microsoft Corporationが機能提供するMicrosoft Azureの管理画面（Azureポータル）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。	○
		95	（１０）医療情報システムのサーバ機器等への同時ログオンユーザ数（ＯＳアカウント等）に適切な上限を設けること。	当社サービスでは、医療機関等のユーザによるインターネット経由のアクセスを管理するシステムIDを介して、当社サービスへアクセスする仕組みを採用しています。これにより、複数のユーザ（ID)が同時にシステムへアクセスすることによるパフォーマンス劣化を未然防止しています。	○
		96	（１１）ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。	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No86、No87の通り、Microsoft Corporationの主管範囲となるため、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。なお、Microsoft Corporation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行う	
		97	（１２）ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。		○
		98	（１３）医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないこと。	本項目は、当社サービスを提供するクラウド基盤（物理サーバ）を主管するMicrosoft Corporationの対応事項となります。『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		99	（１４）ＶＰＮ接続を行う場合には以下の事項に従うこと。 ・接続時にＶＰＮ装置間で相互に認証を行うこと。 ・傍受、リプレイ等のリスクを最小限に抑えるために、「2.6.11.暗号による管理策」に従い、適切な暗号技術を利用すること。 ・インターネット上のトラフィックがＶＰＮチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。 ・複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためＶＰＮチャンネルを医療機関等別に構築する等の対策を実施すること。	当社ではTLS1.2による接続方式を採用しており、VPNによる接続方式は採用していないため、本項目は該当しません。	－ （当社提供サービスに含まれない事項のため、Microsoft Azureによる対応状況の対象外）
	2.6.7.電子媒体の取扱	100	（１）電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。ＣＤ、ＤＶＤ、ＭＯ等の電子媒体については、追記のできない光学メディア（ＣＤ－Ｒ、ＤＶＤＲ等）を用い、情報交換作業終了後、電子媒体を（９）に示す方式にて確実に廃棄処分すること。	当社ではCD、DVD、USBメモリ等の可搬型電子媒体の利用は運用上、一切禁止しており、その旨を社員/派遣社員へ周知徹底しています。なお、プログラム・データのやり取りは、Microsoft Corporationが提供するOffice 365等、全てインターネット上のクラウドツールを介して行っており、業務端末のローカルに個人情報を保管しない業務運用としています。	○
		101	（２）情報交換目的やバックアップ目的でＭＴ、ＤＡＴ、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行うこと。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行うこと。		
		102	（３）電子媒体は台帳を作成して管理すること。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証すること。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持すること。		
		103	（４）電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮すること。		
		104	（５）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媒体の製造者により指定される保管環境にて保管すること。		
		105	（６）製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、他媒体に複写すること。		
		106	（７）情報を保管するためにハードディスク装置を用いる場合には、ＲＡＩＤ－１もしくはＲＡＩＤ－６相当以上のディスク障害に対する対策を取ること。	本項目は、本サービスをクラウド上で提供するに際したシステムの物理OS層を主管するMicrosoft Corporationの主管範囲となります。『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		107	（８）全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行うこと。	※No100～No105をご参照ください。	○
		108	（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こと。		
	2.6.8.情報交換に関するセキュリティ	109	（１）医療機関等と情報処理事業者間の情報交換に関して、次の事項を予め合意しておくこと。 ・情報を電子媒体に記録して交換する際の手順 ・情報をネットワーク経由で文書ファイル	個人情報ないし医療情報を交換するケースは、サービス利用時のレセプトコンピュータの移行データを受け取る場合があります。このような機密情報を交換する場合には、当社サービス上もしくはセキュアファイル交換サービス（NRIセキュアテクノロジーズ株式会社が提供する「クリプト便」）の利用をする運用をして	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
			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	います。セキュアファイル交換サービスを利用する場合は、ファイルにパスワードをかけたうえで、セキュアファイル交換サービスを介して、ファイルの授受を行っています。緊急時も同様に運用しています。セキュアファイル交換サービスを使うことで、通信を暗号化した上で安全にファイルをやりとりすることができるため、データの完全性、機密性を担保しています。	
		110	（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こと。 ・発送者、受領者を識別し記録すること。 ・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止策を行うこと。 ・交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと。）。 ・交換された情報に悪意のあるコードが含まれていないことを確実とすること。	機密情報の授受時は、セキュアファイル交換サービスを利用しています。そのサービス上で、 ・発送者受領者のログ取得 ・発送者の認証 を行っています。また、このサービスを介してやりとりすることで、受領側の機密レベルも高い基準を担保するようにしています。受け取ったデータは、セキュリティソフトがある端末でリアルタイムスキャンをしているため、悪意のあるコードやプログラムが入っていないことを確保しています。	○
		111	（３）物理的に情報を搬送する際には以下の対策を実施すること。 ・医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。 ・配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。 ・配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。 ・配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。 ・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。 ・電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。	当社は物理的な情報搬送には対応していないため、本項目は該当しません。	－ （当社提供サービスに含まれない事項のため、Microsoft Azureによる対応状況の対象外）
		112	（４）電子的に情報を転送する際には以下の対策を実施すること。 ・送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 ・送受信する経路は適切な方法で傍受のリスクから保護されていること。 ・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。 ・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。	機密情報を交換する際は、NRIセキュアテクノロジーズ株式会社が提供する「クリプト便」というセキュアファイル交換サービスを利用しています。そのサービスでは、送信者は当社が指定したメールアドレス経由のみでファイル送信可能にすることでの身元確認をおこなっています。サービス利用時にユーザ認証することで、関係者以外がファイルにアクセスできないようにしています。本サービスでは、通信経路を暗号化したうえで利用するため、改ざんや傍受されることはない旨がNRIセキュアテクノロジーズ株式会社により保証されています。また本サービスでは、利用・操作のログも取得できるため、当社においても問題発生時には原因追求できる体制としています。	○
	2.6.9.医療情報システムに対するセキュリティ	113	（１）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こと。	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のみで運用しています。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。また、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	○
		114	（２）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こと。		

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
	要求事項			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。	
		115	（３）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こと。	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おこなっています。	○
		116	（４）運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。	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。	○
		117	（５）システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。	当社サービスの本番環境での設定やファイルは、すべて定期的なバックアップとログの取得をしています。また、本番環境に影響がある作業を行うとき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。	○
	2.6.10.アプリケーションに対するセキュリティ要求事項	118	（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こと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。	仮想層における当社サービスの脆弱性については、脆弱性スキャナーツールでの巡回と、定期的に第三者のセキュリティレビューを受けています。そこで発見された脆弱性については、脆弱性の重要度／危険度に応じてレベル分けを行い、対応時期を決めた上で対応実施するように管理しています。データ送受信の際の完全性については、通信をTLS1.2でクライアント証明書を入れることで暗号化しており、改ざんや傍受防止をしています。なお、物理OS層におけるセキュリティ対策は、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		119	（２）アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。	仮想層における第三者のソフトウェアについては、各ソフトウェアの脆弱性の重要度に応じて、ライブラリ管理ツールないしは、ソースコードを更新して対応しています。なお、物理OS層におけるセキュリティ対策は、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		120	（３）アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。	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。また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。	○
		121	（４）アプリケーションにて医療事業者側の作業者を認証する情報（ＩＤ／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。	当社サービスを医療機関が利用する際の認証情報（パスワード）は、プログラム上で、CRYPTRECによる「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」が推奨するハッシュ関数を用いてデータベースに保存しています。	○
		122	（５）アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。	当社サービスを利用するためには、医療機関内で利用するアカウントが必要で、そのアカウントがないと情報にアクセスができません。またそのアカウントは、医療機関の職務ごとに権限をわけており、操作できる対象を変えています。現状設定できる権限は、医師、看護師、クラーク、その他であり、カルテ確定は権限を設定したアカウントでしかできないようにしています。	○
	2.6.11.暗号による管理策	123	（１）暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。	データを保存しているデータベースの暗号化は、データベースソフトウェアが提供するAES暗号化方式を採用しており、鍵長も十分長いものを使用しています。ネットワークの暗号化は、IPAの「SSL/TLS暗号設定ガイドライン」での高セキュリティ型に準拠しており、TLS1.2の暗号化は、RSA・AES暗号で鍵長も長いものを使用しています。	○
		124	（２）暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。	ネットワークの暗号鍵が漏洩した場合は、漏洩した鍵での認証を無効化して新たに鍵の再発行をするプロセスとしています。またデータの暗号鍵が漏洩した場合は、暗号鍵を変更してデータの移行を行うプロセスとしています。ただし、データの暗号鍵につては漏洩しても直接的に利用者や第三者にデータが開示される状	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
				態にはないため、ネットワークの暗号鍵が漏洩した場合よりもリスクが低く、漏洩範囲やそのときのリスク分析の評価に応じた適切な対応を行います。	
		125	（３）電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。	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。	○
		126	（４）暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。	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。	○
		127	（５）医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。	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おこなっています。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。	○
	2.6.12.ログの取得及び監査	128	（１）作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し管理すること。	当社サービスの本番環境（仮想層）で取得しているログは下記です。 ・Webサーバのアクセスログ ・アプリケーションのエラーログ ・医療機関の操作ログ ・データベースサーバの実行ログ ・各種パフォーマンスログ このうち、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。なお、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。	○
		129	（２）監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。	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。なお、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。	○
		130	（３）ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。	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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		131	（４）標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。	仮想層では大手機関（Google Public NTP）が提供しているNTPサーバを利用しています。物理OS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。	○
		132	（５）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こと。 ・ログデータにアクセスする作業者及び操作を制限すること。 ・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。 ・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。	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。	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
	2.6.13.アクセス制御方針	133	（１）情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること。	当社サービスにおける仮想層で用いているソフトウェアのセキュリティ要件は、下記の通りです。 （１）OSについては、最新のOSのセキュリティ情報を確認しながら必要に応じてセキュリティパッチやアップデートを行っています。また、よりクラウドのマネージドされた環境を利用するために、PaaSへの移行を進めています。 （２）DBMSについては、Microsoft AzureのPaaSサービスを利用しているため、ミドルウェアレイヤーのセキュリティはMicrosoft Azureが対応しています。データベースのデータは個人情報が含まれる箇所は暗号化して保存しています。 （３） アプリケーションについては、利用するライブラリはセキュリティ情報を確認しながら必要に応じてセキュリティパッチやアップデートを行っています。また、定期的に脆弱性スキャナー、第三者の脆弱性検査を受けることで、セキュリティリスクの低減を行っています。 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。	○
		134	（２）情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること。		
		135	（３）アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。	仮想層（当社管理）のアカウントの登録変更破棄のプロセスは下記の通り運用しています。 （１）アカウントの発行は、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。その時点で各アカウント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て、変更があるアカウントは変更削除を行っています。 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。	○
		136	（４）それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。	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権限をグルーピングしており、権限を付与しています。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。	○
		137	（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こと。		
	2.6.14.作業者アクセス及び作業者ＩＤの管理	138	（１） 作業者は情報処理装置上においてユニークな作業者ＩＤにより識別されること。	当社が管理する仮想層の本番環境に係るアカウントは、担当ごとにすべ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Microsoft Active Directory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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		139	（２）作業者ＩＤを発行する際に、既存のＩＤとの重複を排除する仕組みを導入すること。	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。また、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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		140	（３）複数作業者で共用するためのグループＩＤの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者ＩＤでログオンしてからグループＩＤに変更する仕組みを利用すること。	当社が管理する仮想層の本番環境のIDの使い回しや、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。また、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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		141	（４）作業者ＩＤの発行は医療情報システムの管理に必要な最小限の人数に留めること。	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。また、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	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
				ト付与を行っています。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。	
		142	（５）作業者が変更あるいは退職した際には、ただちに当該作業者ＩＤを利用停止とすること。	当社が管理する仮想層の本番環境では、作業者IDは、担当が変更になった離職した時点で、IDの利用停止をおこなっています。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。その時点で各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て、変更があるIDは変更削除を行っています。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。	○
		143	（６）監視ログの監査時に作業者を確実に特定するため、作業者ＩＤは過去に使われたものを再利用しないこと。	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。また、当社サービスの本番環境に影響ある作業を行うときは、事前に作業者が作業内容を申請して承認の後実施するため、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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		144	（７）不要な作業者ＩＤが残っていないことを定期的に確認すること。	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。その時点で各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て、変更があるIDは変更削除を行っています。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。	○
		145	（８）特権ＩＤの発行は必要な最小限のものに留めること。	当社が管理する仮想層の本番環境にて、全ての操作を行うことが可能な特権IDは原則利用禁止としており、パスワードも当社の限られた管理者のみが把握している状況です。本番環境へのアクセスは基本的に、権限を制限したIDにより行うこととしており、通常時に特権IDを利用するシステム運用は一切ありません。なお、緊急時において特権IDを利用する必要が生じた場合は、管理者が担当者にパスワードを通知した上で、作業終了後に、作業内容を検証し、本来行うべきでない作業を行っていないかを点検しています。また、作業終了後には、管理者がパスワードを適時に変更することで、不適切な特権IDの利用が発生しないようにしています。当社作業員が、権限制限されたIDにより、当社サービスの本番環境（サーバやDBMS含む）で作業するときは、特定のクラウド上の踏み台サーバを経由してログインするようにしており、この踏み台サーバ以外からはアクセスできないようにしています。また、この踏み台サーバも社内のネットワークからのみアクセスできるようにしており、本番環境へのアクセス方法自体も多重に制限を行っています。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。	○
		146	（９）特権使用者に昇格可能な作業者ＩＤを制限すること。		
		147	（１０）特権の使用時には作業実施内容を記録すること。		
		148	（１１）管理端末以外からの特権ＩＤによる直接ログオンを禁止すること。		
		149	（１２）情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。	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Microsoft Azure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を行っており、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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		150	（１３）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情報を保管すること。	当社が管理する仮想層の本番環境にて、当社サービスで用いるOSやDBMS、その他Microsoft Azureのサービスは、それぞれが提供する認証機構を利用しており、標準機能としてパスワードは復元できない形で保存されています。物理層における本取り組みは、『Mic	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
				rosoft Azure』対応セキュリティリファレンスをご参照ください。	
		151	（１４）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に強制すること。	仮想層の本番環境へログインできるIDは、特権ID、及び作業用途に応じて限定された作業者IDのみとなります。作業者IDについては定期的にパスワードを変更する運用としています。特権IDについてはNo145～No148の内容をご参照ください。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。	○
		152	（１５）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こと。	仮想層の本番環境へログインできるIDは、特権ID、及び作業用途に応じて限定された作業者IDともに、パスワード変更時には、5世代前までと同様のパスワードは利用しない運用としています。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。	○
		153	（１６）パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。	仮想層の本番環境におけるIDについて、パスワードを変更する際は、変更前のパスワードの確認を必須にしており、そのアカウントの所有者しかパスワードを変更できない運用としています。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。	○
		154	（１７）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こと。	仮想層の本番環境において作業者IDの初期パスワードは、ランダムのパスワードを発行しており、そのあと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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		155	（１８）パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。	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＞ ・半角英数字の混在したパスワードを求める ・パスワードの文字列数は最低8文字以上 ＜運用面の対応＞ ・定期的なパスワードの変更のアナウンス ・パスワード使い回し禁止のアナウンス ・パスワードの複雑さのアナウンス 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。	○
		156	（１９）パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。	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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		157	（２０）パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。	仮想層の本番環境のIDのパスワードは、サーバ内部でCRYPTREC「電子政府における調達のために参照すべき暗号のリスト 」が推奨するハッシュ関数を用いて保存しており、パスワードを第三者が容易に解読することは困難な設計となっています。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。	○
		158	（２１）端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。	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。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。	○
		159	（２２）パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセー	仮想層の本番環境のIDにはパスワード誤入力時の一定の時間経過を必要とする設定（パスワード総当たり攻撃や辞書攻撃等の不正アクセス対策）は行っていませんが、本番環境へのアクセス経路自体に多重的な制限を施しており、且つ、本番環境を常にモニタリング・監視することにより、仮に不正アクセス攻撃が発生し	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
			ジをシステムの管理者に送出する仕組みを導入すること。	た場合も適時に検知が可能な体制としています。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。	
	2.6.15. 作業者の責任及び周知	各作業者に対しては、自己の責任範囲を認識し、責任を果たすことを周知することが必要である。以下の管理策について作業者に対し周知し、理解したことを確認すること。			
		161	（１）各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。	当社では、業務アサイン時にセキュリティ教育ならびにセキュリティテストを実施しており、パスワードの機密性についての啓発を行う説明会を定期的に開催しています。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。	○
		162	（２）システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。	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は、該当するアカウントを停止し、その経緯	○
		163	（３）離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。	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。また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を行っています。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。	○
2.7.人的安全対策		医療情報処理を受託する情報処理事業者において医療情報処理に関する管理を的確に行うため、医療情報に触れる機会を持つ情報処理事業者職員は、原則として情報処理事業者の正規職員に限ることを原則とするが、雇用形態が多様化している実態を踏まえ、派遣従業員等の非正規職員についても、秘密保持契約や情報セキュリティ教育等の履行に万全を期し、正規職員のみによる管理と同等レベルの管理が行われることを前提として、認めることとする。			
		164	（１）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。	当社サービスの開発保守にかかわる従業員のうち、医療情報ならびに個人情報にアクセスする可能性がある従業員は、派遣社員も業務委託も含めて、秘密保持契約を結んでいます。	○
		165	（２）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、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。	当社サービスの開発保守にかかわる従業員は、医療情報ならびに個人情報のアクセスの可能性の有無を問わず、セキュリティ教育、セキュリティテストを実施しており、情報セキュリティならびに医療情報の扱いに一定の知識と理解をもったうえで業務に取り組むようにしています。また、このテストは年に１回実施しており、定期的に教育をしています。	○
		166	（３）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すること。	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は、 ・各種アカウントを停止 ・該当するログの詳細を確認 ・本人による事情聴取 をすることで行為の確認と影響範囲を特定します。データの信頼性は、DBMSの実行ログならびに当社サービスの本番環境にアクセスする踏み台サーバのログを見ることで発見できます。サービスレベル水準は、ネットワーク構成やサーバなどのログから変更履歴を確認できるので、そこから状況を把握できます。	○
		167	（４）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。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。	社員ならびに業務委託の退職・離職の場合は、返却物などのチェックリストを用意しており、ヌケモレがないように行っています。退社後の機密情報の管理は、秘密保持契約が退社後も有効になるようにしています。	○

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		168	（５）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こと。	当社サービスを利用する医療機関には、「利用規約」ならびに「個人情報の取り扱いについて」で、当社の個人情報の扱いについて明記しており、事前にその同意の上で利用いただくようにしています。	○
2.8.情報の破棄		169	（１）ＣＤ－Ｒ等の廃棄については「2.6.7.電子媒体の取扱」を参照すること。	N100～No105に記載の通り、当社ではCD、DVD、USBメモリ等の可搬型電子媒体の利用は一切禁止しています。なお、物理的なハードディスク等の主管はMicrosoft Corporationの主管範囲となるため、No169～No171の項目については、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
		170	（２）ハードディスク等の廃棄については「2.5.4.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。		
		171	（３）情報処理事業者は「医療情報システムの安全管理に関するガイドライン」に従って情報の破棄を行った記録を提出すること。		
2.9.医療情報システムの改造と保守		172	オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。	仮想層では、当社サービスのOSやセキュリティパッチを更新（リリース）する際は、ソフトウェアの更新時と同様に、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。なお、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。	○
2.10.医療情報処理に関する事業継続計画	2.10.1.要求事項の識別	173	（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）、情報処理設備等について識別すること。	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。また、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を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のマニュアル・手順書として整備されて、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。なお、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。	○
		174	（２）業務プロセス間の相互関係を評価すること。	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、及び運用管理業務は、手順書・マニュアルとして文書化・整備されており、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。なお、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。	○
		175	（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こと。	事業を継続するための業務の優先順位を決める上で、大切なことは「医療機関がいかなるときも診療行為を継続できること」であり、その観点より、No174に記す通り、開発/保守・運用管理プロセスの相互関係の整理に加え、重要度評価を行っています。当社が所管する仮想層において特に重要度の高い業務プロセスは、以下の３つと考えており、重点的な対応を行うようにしています。 （１）システムを停止させず安定的且つ継続的に稼働させるための管理業務（常にシステムを監視し、問題発生時には適時に復旧できるようにするための運用管理業務） （２）問題発生時に適切に当社サービスのアプリケーションを更新するための管理業務（診療報酬改定等に応じたシステム更新等の、保守管理業務） （３） 医療機関からの問い合わせやトラブルに迅速に対応するための管理業務（ユーザサポートに係る運用管理業務） 特に（１）、つまり障害復旧の観点からは、当社サービスで障害が発生した場合、影響（あるいは障害の予兆がある場合どのような事象が現れるか）について整理を行い、当社メンバーが漏れなく共有できる仕組み	○
		176	（４）医療情報システムに発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別すること。		
		177	（５）医療情報システムに発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別すること。		

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	仮想層に係る当社の対応状況	物理層に係るMicrosoft Azureの管理対象範囲有無
		178	（６）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すること。	を講じています。これにより、特定の担当者のみしか障害復旧または予兆監視の対応ができなくなるという属人性のない環境で、迅速かつプロアクティブに医療機関のユーザを保護できるようにしています。上記に加えて機能面でもユーザ保護の観点より様々な施策を講じています。例えば、当社サービスまたはネットワークに障害がおきたときのために、当社サービスにはPDFダウンロードという機能を提供しています。この機能を使うことで、その医療機関での医療情報をその指定した端末にPDFで常にバックアップを取ることができ、当社サービスが使えない状況でも、医療機関で診療行為が継続できるようにしています。なお、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。	
		179	（７）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こと。	当社サービスはMicrosoft Corporationが提供するクラウド基盤Microsoft Azureのもとで運営を行っており、物理的なシステム環境はMicrosoft Corporationの主管範囲となります。よって、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、『Microsoft Azure』対応セキュリティリファレンスをご参照ください。	○
	2.10.2.事業継続計画の立案及びレビュー	180	（１）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として策定すること。	当社ではMicrosoft Corporationが提供するクラウド基盤Microsoft Azureにてサービス提供を行っているため、物理層の主管はMicrosoft Corporation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、Microsoft Corporationによる『Microsoft Azure』対応セキュリティリファレンスをご参照ください。なお、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	○
		181	（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こと。	当社所管の仮想層では、No180で記した障害復旧のプロセスは、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。	○
		182	（３） 事業継続計画について定期的に見直しを行うこと。		