医療情報システム向け
使えるクラウドバックアップ
利用リファレンス

(経済産業省版)

2019年12月2日版

使えるねっと株式会社

長野本社：〒380-0836 長野県長野市南県町1082 KOYO南県町ビル3階

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
1	2 医療情報を受託管理する情報処理事業者における安全管理上の要求事項	2.1 医療情報に係る情報処理事業を受託する上で必須される認証及び認定				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。	弊社は、ISO27001を取得しております。 登録番号：2015/2238 弊社ホームページ(https://www.tsukaeru.net/) に登録ロゴを掲載しております。" 情報セキュリティマネジメントシステムの国際規格であるISO27001を認証取得しており、第三者機関から定期的な監査を受けることでサービス品質の担保と日々の改善を行っております。
2		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。	(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。	弊社が提供するバックアップシステムで医療機関から預かる情報は、お客様情報(住所、名前、メールアドレス以下顧客情報)、およびバックアップデータとなります。 すべてのデータはコントロールパネルを通じて弊社データセンター内にあり、バックアップを格納するサーバ群は弊社が管理しております。 顧客情報はマルチテナント型で管理され、コントロールパネルを通じでアクセスすることが可能である。 また、顧客情報については弊社プライバシーポリシーに則り管理されます。 弊社保管データについてはお客様が所有・管理されるものであり、弊社は、保管データの内容を把握することはできず、 お客様との契約に基づく明確な指示又は法令上効力と拘束力のある要請がない限り、保管データにアクセスすることはしません。
3					(2)	預託された情報の全てを資産台帳に記録すること。	顧客情報はコントロールパネル配下で一元管理され、電子媒体として記録されております。バックアップデータにおいてはお客様自身でコントロールパネルを通じして管理していただきます。
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。	顧客情報はコントロールパネル配下で一元管理されており、電子媒体として管理され、許可された管理者が速やかに検索および集計することが可能となります。
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。	顧客情報はコントロールパネル配下で一元管理されており、特定の管理者のみが操作可能であり、バックアップデータには管理者が接触することはない
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。	コントロールパネルへのアクセスは記録されます。これらの記録はいつでも閲覧することが可能である
7			2.2.2.情報の分類		(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。	顧客情報においては弊社プライバシーポリシーに則り管理されております。 バックアップデータにおいては、原則そのお客様のみがアクセス可能な仕組みになっており、お客様側で管理していただく仕組みとなります。
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。	同上
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。	ISO27001の認証されております弊社で定めたISMSマニュアルに基づき、リスク分析を実施しております。
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。	同上
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）。	顧客情報についてはレベルを分類せずに一律重要方法として管理するようにしております。また、その顧客情報については弊社プライバシーポリシーに則り管理されております。なお、バックアップデータについては管理画面を通じてお客様側で管理するようにしております。
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。	同上
13		2.3.組織的安全管理策（体制、運用管理規程）			(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。	バックアップデータについてはお客様にて管理いただきます。一方、弊社における個人情報の取り扱いやその他データの保護規則については「プライバシーポリシー」や、情報セキュリティー基本方針にて定義され、運用されております。その詳細については以下を参照ください。 https://www.tsukaeru.net/privacy https://www.tsukaeru.net/security
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。	同上
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。	同上

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	弊社ではISO27001に準拠して設計・構築・運用することでサービス品質を確保しております。 登録時に入力されたお客様情報は、弊社およびAcronis社が定めた「プライバシーポリシー」に則り、保護されております。また、バックアップシステムに保存されておりますお客様のデータも原則弊社から閲覧することはありません。ただし、法律に基づき裁判所や警察等の公的機関から要請があった場合、法令に特別の規定がある場合、お客様や公衆の生命・健康・財産を損なうおそれがある場合、また法律や弊社のご利用規約に反する行為により、当社の権利、財産またはサービスを保護する必要がある場合には、この限りではありません。
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組方針、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。	同上
18		2.4.医療情報の伝達経路におけるリスク評価				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。	医療情報機器から弊社バックアップサーバ の経路は、TLS通信およびAcronis社のソフトウェアによる暗号化により安全性を確保しております。 初期バックアップの容量が大きい場合シャトル便(USB HDD)を使用してローカルでバックアップしたものを宅配便で配送することがありますが、バックアップする際も暗号化することで配送経路で問題が発生してもデータを開くことができない仕様となっております。
19		2.5.物理的安全対策	2.5.1.医療情報処理施設の建物に関する要求事項	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	(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。	弊社のデータセンターは、従業員のみの入室で、セキュリティカード+暗証番号により施錠管理されております。 外来者は、従業員の立ち合いのもとで入室とし、サーバ機器への不正アクセスを防止しております。
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。	弊社のデータセンターは、監視カメラで常時監視および記録を保存しております。
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。	弊社データセンターの入口および各部屋の入口は、ALSOKの施錠管理システムで管理し、不正な物理的な侵入を抑止しております。
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。	弊社データセンターの建物は、2008年建築基準法の耐震基準で建築されております。 また、火災への対策としてコンピュータへの影響を考慮し、早期煙検知装置及消化ガスシステムを導入しております。
23			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	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	(1)	・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。	弊社データセンターの入退館はALSOKの施錠システムで管理し、セキュリティカード+暗証番号により入退室者の確実な認証を行っております。
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。	弊社データセンターへの外来者の入館時は、従業員の立ち合いとなり、受付も従業員が実施しております。
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）。	弊社データセンターへの外来者の入館時は、誓約書へ記名して頂き、誓約書の履歴を保存しております。 従業員の入館時はセキュリティカードによる履歴を保存しております。
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。	弊社データセンターへの入館は、従業員のみに制限されており、外来者の入館時は従業員が立ち合いとなります。
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。	弊社データセンターへの入館は、従業員のみに制限されており、外来者の入館時は従業員が立ち合いとなります。
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。	弊社データセンターへの入館に使用するセキュリティカードの紛失時は、管理者へ連絡して対象のセキュリティカードを無効化しております。また、セキュリティカードを所有しております従業員の退職時はセキュリティカードを回収しております。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	弊社データセンターへの外来者の入館時間は、従業員が立ち合いできる時間内に限定して調整しております。
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。	弊社データセンターへ個人所有物の持込が必要な際は申請を必要とし、「持出持込記録」にて管理しております。
31				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	(2)	・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	弊社データセンターへの入館は、従業員に限定されており、外来者の入館時は従業員が立ち会うことにより不正操作に対する安全性が確保されております。
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。	弊社のデータセンターへの入館は、従業員のみに限定しており、セキュリティカードは従業員のみに配布しております。 また、入館時はセキュリティカードごとに、従業員各自の暗証番号が必要となるため、不特定多数の者がセキュリティカードを扱うことができないようにしております。
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、作業終了時刻、作業内容等について記録すること。	弊社データセンターへの外来者の入館時は、誓約書へ記名して頂きます。 誓約書に入館時間、退館時間、入館理由の記載が必要となります。
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。	データセンターは自社で所有しており、外部事業者に作業を依頼する場合は、対象サーバーをサービスから切り離した上で、従業員の立ち合いの元で作業を実施してもらおります。 作業内容については事前に確認し、作業内容に変更があった場合はその都度報告をうけることで、システムへの影響がないことを確認しております。
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。	医療情報を取り扱っておりますシステムは、バックアップシステムとなっており、どのようなデータのバックアップを扱っておりますかを識別できるようなラベルは掲示していません。
36				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	(3)	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。	弊社占有のデータセンターで運用さております。
37			2.5.3.情報処理装置のセキュリティ		(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Øの維持すること。	医療情報を扱っておりますバックアップシステムについては、サーバー機器のリストを作成し管理しております。
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	バックアップサービスのサーバ群へ必要がないアプリケーションをインストールすることはございません。 特定の管理者のみがアプリケーションのインストールやパッケージの操作が可能であり、そのインストールされておりますアプリケーションについては管理ツールを利用して適切に管理されております。
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。	弊社の使えるクラウドバックアップは、データが医療情報であるかにかかわらず、バックアップデータの中身について閲覧することはございません。 医療機関等からの依頼により確認が必要な場合は、アクセス権限のないものが閲覧できない場所で作業をする手順としております。
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。	同上
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。	弊社データセンターの消火設備は、コンピュータに損傷を与えないよう水の代わりに消火ガスシステムを導入しております。 また、人体にも影響を与えないよう二酸化炭素ではなく「窒素＋アルゴン」の混合ガスを採用しております。
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。	弊社データセンターは禁煙となっております。 また、飲食はオペレーションルーム内のみとなります。
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。	弊社データセンターへの火器、危険物等の持込みは原則禁止としております。 工事等によりやむを得ない場合は、禁止事項に該当する作業として報告を受け、サーバー室内の装置に影響がないよう、養生等をした上で持込となります。
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。	装置は監視システムにより障害を検知し、物理的な障害が発生した場合は、障害部品の交換を実施しております。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	障害対応は、弊社データセンター内で実施します。 HDDなどの障害で交換した場合は、情報記録媒体の処分手順に従い処理し、外部に情報が漏洩しないよう配慮しております。
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。	・サーバーラックはコンクリート床に耐震固定した架台に固定することで転倒を防止しております。 ・サーバーラックの熱対策としては、ラックの前面床下から冷気を送ることにより、サーバーが冷気を吸気できるようにし、背面からの排熱が空調設備に循環されるようにしております。 空調設備はサーバー室に冗長用を含め3台設置され、十分な冷気をフリーアクセスフロアーに送っております。 ・サーバーラックの扉については、自社データセンターのためサーバー室への入退管理により鍵管理としております。
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。	弊社サービス提供において使用される情報処理機器は常時稼働状態であるため、起動パスワードを設定する必要性がございません。
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。	バックアップシステムの障害発生時においても業務を継続できるよう冗長化で構成されております。 HDD, 電源, Network は各サーバー内で冗長化されており、サーバーが1台停止しても、残りのサーバーで運用できるようサーバー単位でも冗長化されております。 また、途中経路のNetwork機器や電源系統についても冗長化されております。
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。	弊社のネットワークに接続する端末機器は、指定のウイルススキャンソフトにより集中管理しており、不適切な機器が接続されないよう整備しております。 また、無線LANの利用については、MACアドレス制限により指定された端末機器のみアクセスを許可しております。
50			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		(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。	ハードディスク等を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おりますことを確認するよう適切な管理を行っております。
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。	サーバー等の廃棄の際は、工場出荷時の設定にリセットすることにより、設定されたパスワードを消去しております。
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。	ハードディスクを機器に接続する際は、事前に検査機で動作確認及びデータ消去を実施しております。
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。	ハードディスクの廃棄時は、情報記録媒体の処分手順に従い処理しております。 廃棄した機器については、廃棄リストに記載しております。
54			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。	(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。	情報処理装置を持ち出す場合は、ISO申請書により申請し、持出持込管理の台帳で管理しております。 持出機器は紛失が発生しないよう定期的にチェックしております。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	バックアップおよびリストアデータの物理搬送する際に外付けHDDを利用する(このサービスを以下シャトル便とする) 顧客から戻ってきたシャトル便の情報記録媒体は、ネットワークに接続されていないPCでウイルススキャンチェック後、サーバー機へ接続しております。
56		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		(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。	弊社バックアップサーバ、クライアントソフトウェアは予め指定されております手順に沿って、影響を評価しております。
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。	悪影響が生じる可能性がある変更を実施する場合においても、予め指定されております手順に沿ってデータの保存を保証するような方策を検討し、実施いたします。その場合、一時的なサービスの停止や通信断が発生することがありますが、変更を実施する前に利用者へメール等でその影響を周知して変更を実施いたします。
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。	弊社サービスの変更を行う場合がありますが、以前のデータ形式を維持いたします。この場合のお客様に対する通知ポリシー等はサービス利用規約に則って運用されます。
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。	弊社バックアップサーバにおいて保守作業が実施される場合はメンテナンス日時を事前にアナウンスし、停止時間を最小限にとどめて保守作業を実施しております。
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。	同上
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。	弊社バックアップサーバにおいては監視ツールにより常時モニタリングしており、何か改ざんがあれば検知する仕組みです。クライアントソフトウェアについても適切にパッケージが管理されており、定期的に悪意のある変更がないかチェックしております。
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。	弊社バックアップサーバにおいては弊社ISMSで定められた手順および管理手法に沿って、技術的な脆弱性を定期的にレビューしており、脆弱性の重要度/危険度に応じて実施を検討いたします。
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。	同上
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。	同上
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。	原則、弊社バックアップサーバにおいては保守作業を外部委託することはありません。
66			2.6.2.開発施設、試験施設と運用施設の分離		(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。	クライアントおよびサーバサイドともにAcronis社が開発したアプリケーションを用おります。 事前に弊社ルールに基づいた検証により安全性を確認しております。 同様にAcronis社側でも十分に検証してアプリケーションを展開しております。
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。	開発そのものはAcronis社で実施されており、開発環境と本番環境は別環境であり直接接続されておりません。 Acronis社によりすべてのコードはセキュリティレビューが実施され、又、パッチまたはコードはすべてテストが実施され、信頼できるリポジトリからリリースされる仕組みとなります。
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。	同上
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。	同上
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。	開発環境と本番環境は接続されてないため、直接コピーはできません。また、本番環境のデータを開発環境で利用することは禁止されております。
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。	同上

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
72			2.6.3.悪意のあるコードに対する管理策		(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。	弊社の保守端末は ウイルススキャンソフトにより集中管理されており、定期的に問題が発生していないかチェックしております。 問題が発生した場合は、状況により対策を実施しております。
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	弊社で使用しております機器に導入しておりますウイルススキャンソフトでは、下記が有効となっております。 ・リアルタイムファイルシステム保護 ・ドキュメント保護 ・HIPS(ホスト侵入防止システム) ・アンチステルス(ルートキット対策) ・Webアクセス保護 ・電子メールクライアント保護 ・フィッシング対策保護 また、定義ファイルの自動更新が有効となっております。 尚、一般ユーザには管理者権限が付与されていないため、アンインストール不可となっております。
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。	弊社で使用しております機器に導入しておりますウイルススキャンソフトは集中管理されており、定期的に問題が発生していないかチェックしております。定義ファイルの更新などで問題が発生しております場合は、状況により対策を実施しております。
75			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	(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。	医療情報を扱っておりますバックアップシステムのサーバーは、CLI 環境のためウェブブラウザは利用できません。
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。）。	同上
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。	同上
78			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。	(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。	弊社の使えるバックアップサービスはAcronisが提供する技術を利用していますが、サービスの管理は、社内運用規定において実施、運用、維持に関する定期的な内部監査を行っております。 また、作業の実施においても項目ごとに事前のレビュー、事後の報告を行うフローに沿って運用されております。 その安全管理およびサービスレベルはISO27001の認証を取得し、定期的に第三者評価を受けることでその品質を確保しております。
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。	同上
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。	同上
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。	弊社データセンターへの入館は、従業員のみに制限されており、外来者の入館時は従業員が立ち合いとなります。
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。	弊社データセンターへの入館は、従業員のみに制限されており、外来者の入館時は従業員が立ち合いとなります。 弊社はデータセンター内での作業者やお客様会社名等の個人情報保護の観点から、顔写真入りのIDカード等の携行を必須としておりません。データセンタ内では入館カードをカードケースに入れ色分けされたストラップにて首からかけ、第三者に見えるように携行するようにしております。
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。	同上
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。	サービス変更に関しては重要度によって区別された社内規定によるプロセス、有識者承認フローを介して決定されております。
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。	原則、弊社バックアップサーバにおいては保守作業を外部委託することはありません。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
86			2.6.6.ネットワークセキュリティ管理		(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。	弊社バックアップサーバにおいてはゲートウェイサーバーを経由してアクセスする仕組みとなっております。 また、作業においては弊社の運用ルールに沿って実施されております。
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。）。	弊社バックアップサーバでは、そのゲートウェイにおいて2要素認証が採用されており、悪意のある第三者が侵入できない仕組みです.
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。	弊社が管理するルータ及びネットワーク機器は冗長化しており、また、適切な機器が利用されておりますので、安全性が担保されております。
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。	弊社データセンターへの入館は、特定の従業員に限定されており、利用していないネットワークポートへの物理的な配線をすることは制限されております。
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	弊社基盤の入り口機器にはFirewallが設置され必要なポートのみ通しており、異常なトラフィックを検知した場合は調査し対応しております。
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。	弊社基盤のセキュリティパッチは常に最新化を図るようにしております。 また、Networkに関する異常が検出された場合、攻撃・不正アクセス等がないか調査し対応しております。
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。	弊社では事業継続管理を規定しており、非常時における規定も含まれております。 ISO 27001 に準拠して規定には「非常時におけるエスカレーション」、「関連部門への周知と指示」、「特別体制の整備」、「公的機関との連携」、「対象者への通知」が規定されております。
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。	弊社基盤に対する不正アクセスに対し、これらのアクセスをモニタリングし問題に迅速に対応する為、ロギング、モニタリングを実施した内容を保管しております。
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）	バックアップシステムにおいては、左記に限定される範囲で接続管理を実施しております。
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。	弊社の端末において同時ログオンの上限については、接続できるアカウントを制限して接続できるようになっております。
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。	弊社基盤に対するアクセスログは常に記録されており、定期的に不審な活動が行われてないかチェックしております。
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。	同上
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 。	弊社のバックアップサーバが接続しているネットワークでは無線LANは利用しておりません。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
99					(14)	VPN接続を行う場合には以下の事項に従うこと。 Ⅰ接続時にVPN装置間で相互に認証を行うこと。 Ⅰ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。 Ⅰ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。 Ⅰ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。	弊社の端末は、ゲートウェイを通してバックアップサーバーへ接続しております。 医療機関等からの接続については、TSL1.2を使用しておりますが、バックアップストレージの接続オプションとしてVPN接続を提供することが可能となっております。その場合、適切な暗号技術を用い、医療機関ごとにチャンネルを分けることが可能となっております。
100			2.6.7.電子媒体の取扱		(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、DVD－R等）を用い、情報交換作業終了後、電子媒体を(9)に示す方式にて確実に廃棄処分すること。	電子媒体(CD-R, DVD-R) を持ち出す場合は、ISO申請書により申請し、持出持込管理の台帳で管理しております。 持出機器は紛失が発生しないよう定期的にチェックしております。
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。	大容量のHDDをシャトル便として顧客へ送る際は、前回書き込まれたバックアップデータを消去した上で利用しております。 顧客のBackupデータはパスワード付きで暗号化しており、消去したデータを復元しても、パスワードがなければ、データの中身を見ることはできないようになっております。
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。	CD-R/DVD-Rの電子媒体は、CD/DVD管理台帳にて管理しております。 定期的にチェックし、紛失がないことを確認しております。 CD-R/DVD-Rの廃棄後も記録は保持しております。
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。	CD-R/DVD-Rの電子媒体は、ブランクメディアを鍵付きのキャビネットで保管し、鍵は管理部にて保管しております。 また、ブランクメディアはISO事務局の管理となり、使用する際は申請が必要となります。
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	CD-R/DVD-Rへ書き込むデータは、情報喪失のリスクのある用途には使用いたしません。
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。	同上
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。	バックアップデータはRAID6以上の信頼線のある Storage Clusterに保存されており、ディスク障害等の耐障害性が非常に高い構成で管理されております。
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	CD-R/DVD-Rへ書き込むデータは、機密情報を扱わないようにしております。
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。	CD-R/DVD-Rを廃棄する場合は、シュレッダーにより裁断しております。
109			2.6.8.情報交換に関するセキュリティ		(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。 Ⅰ情報を電子媒体に記録して交換する際の手順 Ⅰ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 Ⅰ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	バックアップおよびリストアデータは交換時の通信は常時AES256およびTLS1.2により暗号化され、完全性、機密性を担保いたします。 コントロールパネルとの接続もTLS1.2が利用されております。
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。	同上 および送受信者のログ取得および認証を実施しております

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	物理搬送が必要な場合は、指定された信頼でき追跡可能な配送業者を利用し、適切なコンテナで媒体を保管して、その媒体の中に保存されるデータは暗号化してあります。
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。	バックアップおよびリストアデータは交換時、常時AES256およびTLS1.2により暗号化され、完全性、機密性を担保します。 また、利用機器とクラウドは証明書により認証されており、なおかつ、暗号化されております。
113			2.6.9.医療情報システムに対するセキュリティ要求事項		(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。	サーバサイドにおいて本番環境に開発ツールはありません。更新する場合にはあらかじめ決められたルールおよび自動化ツールにより更新を実施します。クライアントソフトウェアにおいても開発ツールは同梱されておりません。
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。	サーバサイドにおいて運用上不必要なファイルは設置しておりません、また、接続できるのは許可された管理者のみであり、その操作は記録されております。
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。	アプリケーションの部分においてはAcronis社が十分な試験を実施し、それを弊社側で導入する際にもあらかじめ定められた手順により検証し、導入を実施しております。
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に必要なログを取得すること。	同上
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。	サーバ側の設定ファイルについてはバージョン管理ツールで管理されており、クライアント側のソフトウェアにおいてはAcronis側で十分に管理されております。
118			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		(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。	定期的にアプリケーションの脆弱性診断を実施して、その結果によって対策を実施しております。
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。	弊社サービスにおいては最新の脆弱性情報を参照し、迅速に対応しております。
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。	特定の管理者のみが特定のユーザを利用し、特権の操作を実施します。その操作は記録されており、問題発生時に分析可能となります。
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。	弊社のサービスについては、十分な強度を持ったハッシュ値関数を利用しております。
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。	利用ユーザは権限に応じたアクセス権を付与することが可能でありますが。その権限の付与については医療機関で管理する仕組みとなっております。
123			2.6.11.暗号による管理策	アプリケーション及び情報処理装置で暗号を利用する場合には、以下の管理策を適用すること。	(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必須暗号リスト等を用いること。	バックアップのデータの暗号化においてはAES256が利用できる。通信においてはTLS1.2が利用され、また、暗号化においては同じくAES256が採用されております。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	鍵が漏洩した場合は、漏洩した鍵での認証を即時に無効化し、新しい鍵を提供する仕組みとしております。
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。	電子証明書は信頼できる組織によって発行されたものを使用しております。
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。	弊社運用については暗号鍵の危殆化に備えた暗号化の方針を定めており、また、電子政府推奨暗号リストの利用を定めております。
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おります。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おりますため、データの改ざんや漏洩のリスクは最小限化されております。
128			2.6.12.ログの取得及び監査		(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。	操作は記録されており、参照が可能です。 また、弊社基盤に対する各種ログについては、社内規定のもと適切に収集/管理されております。その品質は、ISO27001に準拠しております。
129					(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こと。	弊社運用においては、不正なアクセス等に対するログを常時監視しており、万がーインシデントが発生した場合は予め規定されたルールに沿ってエスカレーションが実施される仕組みとなります。
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。	弊社基盤のNTPサーバは、適切な参照先が設定されており、時刻同期されております。
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。	同上
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。	弊社基盤の管理者、作業者については必要最低限のアカウント払い出しを行い、台帳管理を行って運用しております。各作業者等の異動や退職等にも迅速に対応するべく、定期的にレビューがなされており、その品質はISOにおいて定期的に第三者評価を受けております。
133			2.6.13.アクセス制御方針		(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。	弊社の機器においては定期的にセキュリティや脆弱性の見直しがされており、必要に応じてパッチを適用することで安全性を確保しております。 又、ISO27001等、ITシステム運用に必要な認証を取得し、定期的に外部監査を受けることでその品質を確保しております。
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。	同上
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。	弊社インフラについてのアクセス権の登録・変更・廃棄に関するプロセスはISO27001等、ITシステム運用に必要な認証を取得し、定期的に外部監査を受けることでその品質を確保しております。
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。	同上
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。	同上
138			2.6.14.作業者アクセス及び作業者IDの管理		(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。	作業者ごとにユニークなアカウントを利用しており、そのアカウントの操作については記録されております
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。	同上
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。	複数作業者で共有するための共有ID及びグループのIDの利用は禁止されております。 設定されたID情報は、ユニークなユーザIDとしてサービス利用責任の範囲で管理されております。
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。	同上
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。	弊社保守運用業務に関わる担当者のIDは文書化された運用定義書の中で管理されており、定期的にチェックを行っております。このプロセスに基づき作業者の変更、退職等においては利用停止いたします。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
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。	弊社保守運用業務に関わる担当者のIDは文書化された運用定義書の中で管理されており、1名ずつ個別に払い出されます。このため、過去に使われたものを流用することはありません。
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。	弊社保守運用業務に関わる担当者のIDは文書化された運用定義書の中で管理されており、不要なIDについても定期的にチェックを行っております。
145					(8)	特権IDの発行は必要な最小限のものに留めること。	弊社保保守運用業務に関わる担当者、役割分担は文書化された運用定義書の中で管理されております。この役割分担の中で特権IDは必要分のみ申請フロー発行される運用となっております。
146					(9)	特権使用者に昇格可能な作業者IDを制限すること。	弊社保保守運用業務に関わる担当者、役割分担は文書化された運用定義書の中で管理されております。この役割分担の中で特権IDは必要分のみ申請フロー発行される運用となっております。
147					(10)	特権の使用時には作業実施内容を記録すること。	弊社保守運用業務についてのすべての作業実施内容は文書化されたワークフローにおいて定義され、事前にレビューされます。また、実際の作業実施に関わるログについては取得し管理しております。
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。	弊社保守運用業務におけるサービス機器へのアクセスはリモートアクセスを原則としており、予め定義された居室、端末およびネットワークを介して接続されます。これらの機器等以外からのアクセスを行うことは禁じられております。
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。	弊社に実装される機器やソフトウェアは予め自社内で検証作業が実施され、必要のないアカウント等情報は削除されます。また、サービス環境への実装後のアクセスに関しては予め文書化されたルールに基づき、アカウントを払い出された職員のみがアクセスできる運用を行っております。ログイン等のログ情報は全て管理され、異常検知時はアラート通知がなされることになっております。
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。	2要素認証を利用しており、パスワードは利用しておりません。
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。	同上
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。	同上
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。	同上
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。	同上
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。	同上
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。	同上
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。	同上
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、あるいは強制オフを行うこと。	作業者の機器はスクリーンロックの設定をしてあるため、5分以内に画面がロックされ不正に利用されるリスクを低減しております。
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。	弊社バックアップサービスへのログインが不成功になった場合は再入力が一定時間ブロックされる仕組みとなります。 また、警告メッセージはシステム管理者に通知される仕組みを導入しております。
160			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	(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。	弊社では毎年全従業員に対し、自身のパスワードを他人に漏らさず安全な管理を徹底する等のセキュリティ研修を実施し,パスワード等の管理にかかる厳密性を徹底しております。

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
161				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	(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。	弊社運用環境に対するアクセスに関しては文書化された運用定義書によってログ取得を義務付けており、不審なアクセス等について定期的なレビューが行われております。また、万が一のインシデント等発生時の対応プロセス、体制、手順を定めており、迅速かつ適切な対応を徹底しております。
162					(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。	弊社で使用される機器は一定時間操作されないものに関して自動的に端末ロックが行われる運用になっており、第三者による利用を未然に防いでおります。
163		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。	(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。	弊社の従業員は入社時に「入社時誓約書」「秘密保持および個人情報に関する誓約書」に署名しております。 また、入社時にISO教育としてセキュリティ関連の教育を行い、その後定期的にセキュリティ意識向上のため教育を実施し、教育訓練記録管理台帳にて管理しております。
164					(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。	同上
165					(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。	万が一のインシデント等発生時の対応プロセス、体制、手順を定めており、迅速かつ適切な対応を徹底しております。
166					(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。	従業員の退職時は、資産貸出返却リストにより貸与された情報資産をすべて返却できるよう管理しております。 また、退職後の守秘義務へ合意してもらうため、退職時誓約書に署名してもらおります。
167					(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。	弊社の従業員は入社時に「入社時誓約書」「秘密保持及び個人情報に関する誓約書」にサインをしております。 また、ISOで定めたセキュリティ教育を実施することで、各従業員のセキュリティ意識向上を図っております。 懲罰規定については、就業規則に定めております。
168		2.8.情報の破棄			(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。	CD-R/DVD-Rを廃棄する場合は、シュレッダーにより裁断しております。 また、CD・DVD管理台帳にてステータスを廃棄に変更して管理しております。
169					(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。	ハードディスク等の廃棄については、情報記録媒体の処分手順に従い処理しております。
170					(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 。	医療機関等からバックアップデータの削除依頼があった場合は、削除を行った記録を提出いたします。
171		2.9.医療情報システムの改造と保守			(1)	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。	弊社運用では、技術的脆弱性に対するパッチや設定変更等対応については社内規定に則って集中管理され、リスク評価と分析を行った上で迅速かつ適切に管理されております。
172		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		(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。	弊社で取り扱う医療情報はバックアップとなるため、障害が医療業務に直接与える影響はございません。 また、使えるクラウドバックアップサービスでは、保管場所/サイクルは自由に選択でき、災害時には国内施設から海外施設に変更して頂く事で再度利用できるようにしております。 弊社ではISO 27001 に準拠して事業継続管理規程を設けており、非常時における規程も含まれております。規程には「非常時におけるエスカレーション」、「関連部門への周知と指示」、「特別体制の整備」、「公的機関との連携」、「対象者への通知」が規定されております。
173					(2)	業務プロセス間の相互関係を評価すること。	同上
174					(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。	同上
175					(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。	同上
176					(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。	同上

Seq	「医療情報を受託管理する情報処理事業者向けガイドライン第2版」で必要とされる実施事項						
	章	節	段	概要	番号	要求事項	対応状況
177					(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 。	同上
178					(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。	同上
179			2.10.2.事業継続計画の立案及びレビュー		(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。	弊社で取り扱う医療情報はバックアップとなるため、障害が医療業務に直接与える影響はございません。 また、使えるクラウドバックアップサービスでは、保管場所/サイクルは自由に選択でき、災害時には国内施設から海外施設に変更して頂く事で再度利用できるようにしております。 弊社ではISO 27001 に準拠して事業継続管理規程を設けており、非常時における規程も含まれております。規程には「非常時におけるエスカレーション」、「関連部門への周知と指示」、「特別体制の整備」、「公的機関との連携」、「対象者への通知」が規定されております。
180					(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。	弊社ではISO 27001 に準拠して事業継続管理規程を設けており、定期的にチェックを行い業務フローや手順等の見直しを実施しております。
181					(3)	事業継続計画について定期的に見直しを行うこと。	同上