医療機関向け
『Microsoft Azure』対応セキュリティリファレンス

2019年 5月 17日
Version 2.0

作成者：
株式会社三菱総合研究所（MRI）
日本ビジネスシステムズ株式会社（JBS）

更新日	版番号	改版内容
2016年2月25日	Version 1.0	初版
2016年4月28日	Version 1.0.1	厚生労働省「医療情報システムの安全管理に関するガイドライン」の第4.2版（平成25年10月）から第4.3版（平成28年3月）への更新内容を確認し、本セキュリティリファレンスの記載内容に変更の必要が無いことを確認した。 加えて、誤字および記載漏れ事項の修正を行った。
2016年11月4日	Version 1.0.2	誤字および記載漏れ事項の修正を行った。
2017年7月25日	Version 1.1	厚生労働省「医療情報システムの安全管理に関するガイドライン」の第5版（平成29年5月）の公開に伴い、要求事項の追加（及びそれに伴う項番の修正）、ならびに下記項目に対する加筆、修正を行った。 ＜加筆・修正＞ 7.2-04 ＜新規追加＞ 6.5-03 6.11-10 また、VPNの接続形態、サードパーティ製ツール、Azure ADについて補足説明を追加した。加えて、誤字脱字の修正を行った。 さらに、参照不可となっている文献について、参照先文献を修正した。
2019年5月17日	Version 2.0	総務省ガイドライン（以下②）の公開に伴い、②の要求事項に対する記載に更新した。 また、①及び③についても記載内容の更新を行った。 ①厚生労働省「医療情報システムの安全管理に関するガイドライン　第5版」（平成29年5月） ②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　第１版」（平成30年7月） ③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　第2版」（平成24年10月）

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から照会した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.1-01	6	6.1	（安全管理措置） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は き損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （従業者の監督） 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。 （委託先の監督） 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。 （個人情報保護法第20 条第21 条第22 条）	「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」において、個人情報保護に関する方針を定め公表することが求められている。本ガイドラインが対象とする情報システムの安全管理も、個人情報保護対策の一部として考えることができるため、この方針の中に情報システムの安全管理についても言及する必要がある。	個人情報保護に関する方針を策定し、公開していること。	最低限	マイクロソフトが利用者（Microsoft Azureを利用するお客様）よりお預かりするデータは（どれが個人情報かどうかも判別できない形で）暗号化された上でデータセンターに保存され、マイクロソフトは（利用者からのご要請がない限り）当該データを閲覧しませんので、利用者がマイクロソフトのクラウドサービスに個人情報を保存することは、個人情報保護法上の「個人情報の取り扱いの委託」には該当しないと考えています。そのため、利用者がマイクロソフトに対し「必要かつ適切な監督」（個人情報保護法22条）を行う必要はなく、そのための個人情報覚書を締結する必要もないと考えております。クラウドサービスへの個人情報の保存は第三者提供にも該当しませんので、本人の同意も不要です。マイクロソフトのクラウドサービスは利用者から信頼いただくため第三者認証機関による認証の取得や、国際基準への適合性の確認を行っています。	適合可能	文献[133]では、お客様自身がデータを所有することが明示され、文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることは無く、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 文献[145]では、Microsoft によって処理される個人データの種類、処理方法、使用目的に関する説明が明示されている。	公開文書	文献[133]文献[134]文献[145]	–	–	–	利用者は、個人情報保護に関する方針を策定・公開を行う必要がある。
6.1-02					個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 利用者のコンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management 万一アカウント不正使用などが疑われる場合、そのアカウント使用に関わる情報は、クラウドサービスの標準的な機能を使用して利用者側で調査することが可能です。 準拠法は日本となります。 品質については、返金保証付のSLAとして規定しています。 指示目的外使用については、お客様コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。	適合可能	文献[65]、文献[141]では、提供事業者として必要な基本的な事項が規定・明記され、実現に向けた対策が講じられていることを確認した。 特筆すべき事項としては、次のとおり。 ・指示目的外使用は、クラウドにおける個人情報保護に関する国際標準「ISO/IEC27018:2014」の認証を取得し、指示目的外使用の禁止を行っている。 文献[144]及び文献[153]にて、Microsoft は、英語では重要度 A 及び B に対して、日本語では重要度 A に対して、24 時間 365日体制でサポートを提供していることが明示されている。	公開文書	文献[65]文献[144]文献[153]	ISO/IEC 27018	–	–	利用者は、個人情報を取り扱う情報システムの安全管理に関する方針を策定する必要がある。
6.2-01		6.2	（安全管理措置） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は き損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （個人情報保護法第20 条）	安全管理を適切に行うための標準的なマネジメントシステムがISO（ISO/IEC27001:2005）ならびにJIS（JIS Q 27001:2006）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。	情報システムで扱う情報をすべてリストアップしていること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、情報システムで扱う情報をすべてリストアップし、情報資産リスト等で管理する必要がある。
6.2-02					リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、情報資産リスト等の情報を常に最新の状態に維持する必要がある。
6.2-03					このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、情報資産リスト等を情報システムの安全管理者が確認できる状態で管理する必要がある。
6.2-04					リストアップした情報に対してリスク分析を実施していること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、情報資産リスト等に基づいてリスク分析を実施する必要がある。
6.2-05					この分析により得られた脅威に対して、6.3 章～6.12 章に示す対策を行っていること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、リスク分析の結果得られた脅威に対して、6.3～6.11 に示す対策を行う必要がある。
6.2-06					上記の結果を文書化して管理していること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview AzureはISO27001の認定を受けています。 https://www.microsoft.com/ja-jp/TrustCenter/Compliance/ISO-IEC-27001	適合可能	文献[148]及び文献[154]にて、Microsoft Azure は、年に 1 回以上、ISO/IEC 27001 及び ISO/IEC 27018 への準拠に関して、第三者の公認認定機関の監査を受けていることが明示されている。	公開文書	文献[148]文献[154]	ISO/IEC 27001 ISO/IEC 27018	–	–	利用者は、実施した対策の結果を文書化して管理する必要がある。
6.3-01		6.3	–	安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。 ① 安全管理対策を講じるための組織体制の整備 ② 安全管理対策を定める規程等の整備と規程等に従った運用 ③ 医療情報の取扱い台帳の整備 ④ 医療情報の安全管理対策の評価、見直し及び改善 ⑤ 情報や情報端末の外部持ち出しに関する規則等の整備 ⑥ 情報端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その情報端末等の管理規程 ⑦ 事故又は違反への対処		情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 Microsoft Azureのデータセンターにおける安全管理については、セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計および実装されています。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることは無く、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 文献[01]では、データガバナンスの一環として、Microsoft Azureサービスの提供に使用される資産の所有者を割り当てるポリシー、データの安全な廃棄、非公開データの非運用環境への移動またはコピーの禁止、情報漏えいを防止する論理制御と物理制御について明示されている。加えて、資産に対するアクセス権を資産の所有者の承認を得た上で付与されること、定期的なアクセスの確認や監査を行うこと、内部または外部の組織とのデータ交換手順の遵行、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスの制限も明示されている。 さらに、文献[19]では、Microsoft Operations Centersにおいて、データ管理も含めて全体の管理を実施していることが明示されている。 NDA文献[N01]にて、情報セキュリティに関する管理者が割り当てられ役割と責任が明確化されていることが確認できた。 加えて、インタビューの結果、管理責任者を中心とした社内ミーティングが行われていることから、管理体制が整備されていると考えられる。	要NDA	文献[01]文献[19]文献[134]文献[135]	–	（本調査で確認した内容に記載の通り）	NDA文献[N01]	利用者及びSI事業者は、それぞれの責任の範囲において、情報システム運用責任者の設置及び担当者の限定を行う必要がある。
6.3-02					個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。	最低限	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなアドに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンターの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。また、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があること、が明記されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。	要NDA	文献[01]	–	–	NDA文献[N01]	利用者は、個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定める必要がある。 利用者は、入退室記録を作成し、適切な期間保存する必要がある。 利用者は、重要な物理的セキュリティ境界からの入退室等を管理するための手順書を作成する必要がある。 利用者は、Microsoft Azureにおいて実施される入退室管理のルールが、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-03					情報システムへのアクセス制限、記録、点検等を定めたアクセス	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 また、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 また、Microsoft Azure の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。 また、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するよう通知されると明示されている。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[01]では、通信時のデータを暗号化するオプションが提供されること、API の呼び出しなどの重要な通信または Microsoft Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があること、暗号鍵の管理主体は原則利用者となることが明示されている。 利用者に提供されるAzureの暗号化機能として、文献[136]にてポイント対サイト接続の暗号化、文献[137]にてサイト間接続の暗号化が明示されている。	公開文書	文献[01]文献[07]文献[131]文献[136]文献[137]	–	–	–	利用者は、情報システムのアクセス管理規程及び運用管理規程を作成する必要がある。 利用者は、ネットワーク構成図を作成する必要がある。 利用者は、情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限する必要がある。 利用者は、Microsoft Azureのアクセス管理の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.3-04					個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。 準拠法は日本となります。 品質については、返金保証付のSLAとして規定しています。 指示目的外使用については、お客様コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。	適合可能	文献[65]、文献[141]及び文献[147]では、提供事業者として必要な基本的な事項が規定・明記されていることを確認した。 文献[141]、文献[151]及び文献[154]では、提供事業者として必要な基本的な事項が規定・明記され、実現に向けた対策が講じられていることを確認した。 特筆すべき事項としては、次のとおり。 ・準拠法は、米国連邦法、ワシントン州法を基本としているが、国別条項において、日本国法が優先適用または付加されることとなっている。 ・指示目的外使用は、クラウドにおける個人情報保護に関する国際標準「ISO/IEC27018:2014」の認証を取得し、指示目的外使用の禁止を行っている。 文献[151]にて、日本でMicrosoft Azureの契約をする場合、準拠法は日本法であることが明示されている。 文献[152]にて、データセンターの所在地の開示についてのマイクロソフト社の情報提供方針及びデータセンターの所在地が明示されている。	要NDA	文献[65]文献[147]文献[151]文献[152]文献[154]	ISO/IEC 27018	–	–	利用者は、Microsoft Azureが定める個人情報保護指針等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-05					運用管理規程等において次の内容を定めること。 (a) 理念（基本方針と管理目的の表明）	最低限	マイクロソフトでは雇用管理の担当者は、マイクロソフトのポリシーに従って、求人、面接、雇用を行う前に職務要件を定めています。職務要件には、職務に関連した主要な責任と仕事、職務の遂行に必要な経歴上の特徴、および必要とされる個人的な能力が含まれます。要件が決定すると、雇用管理の担当者は、職務の概要を示し、求職者の特定に使用される職務内容説明書を作成します。有望な採用候補者が絞られると、面接プロセスを開始して、候補者を評価し、適切な採用決定を行います。 マイクロソフトでは標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。	適合可能	文献[01]では、雇用管理の担当者は、マイクロソフトのポリシーに従って、求人、面接、雇用を行う前に職務要件を定め、職務要件には、職務に関連した主要な責任と仕事、職務の遂行に必要な経歴上の特徴、及び必要とされる個人的な能力が含まれると明示されている。要件が決定すると、雇用管理の担当者は、職務の概要を示し、求職者の特定に使用される職務内容説明書を作成します。有望な採用候補者が絞られると、面接プロセスを開始して、候補者を評価し、適切な採用決定を行うと明示されている。 文献[01]では、標準的な運用手順が、正式に文書化され、Windows Azure の管理者によって承認されると明示されている。また、標準的な運用手順は少なくとも年に一度見直されると明示されている。	公開文書	文献[01]	–	–	–	利用者は、医療情報システムの運用管理規程を定める必要がある。 利用者は、Microsoft Azureが定める基本方針等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-06					(b) 医療機関等の体制	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、Microsoft Azureにおける運用体制が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-07					(c) 契約書・マニュアル等の文書の管理	最低限	利用者(Microsoft Azureを利用する利用者）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 また Azure上に構築された利用者システムにおける正確かつ安全に運用するマニュアルの整備については利用者での管理になります。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていることが明示されている。 また、Microsoft Azure サービスの一環として包括的なガイダンス、ヘルプ、トレーニング、及びトラブルシューティング用の資料を用意していることが明示されている。 また、マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されること、文書化された手順による継続性の計画を含むフレームワークを保持していることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、Microsoft Azureが定める運用管理規程等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-08					(d) リスクに対する予防、発生時の対応の方法	最低限	利用者(Microsoft Azureを利用する利用者）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。 また、インシデント発生時の体制について、インシデントマネージャーやインシデントエンジニアについて、インシデントの処理方法や管理の役割、責任について、及び法務、経営管理者へのエスカレーションとコミュニケーション計画について明示されている。 また、不正アクセス検知時及び発見時の監視について明示されている。さらに、権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 加えて、セキュリティインシデントの対応報告の際のインシデントの特定（システム及びセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[04]では侵入テスト、文献[130]では、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録及び追跡について明示されている。	公開文書	文献[01]文献[04]文献[65]文献[130]	–	–	–	利用者は、Microsoft Azureが定める予防措置及び事故等の発生時の対応等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-09					(e) 機器を用いる場合は機器の管理	最低限	マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	Microsoft Azure 及び GFS が ISO27001を取得していることから、有効なリスク管理態勢を有していると考えられる。 また、Microsoft Azureにおける運用状況については、第三者認証の各種レポートや、文献[03]、文献[06]、文献[07]などの公開資料を利用できることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 文献[01]では、予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを用意していることが明示されている。 また、Windows Azure 環境の主要なハードウェア資産の一覧は保持され、資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担い、資産の所有者は、資産保護を規格に応じて分類し保守する役割も担うと明示されている。また、資産の一覧を検証するために、定期的な監査が実施されると明示されている。	公開文書	文献[01]文献[03]文献[06]文献[07]文献[81]	ISO/IEC 27001	–	–	利用者は、利用者側で管理する機器等（パソコン等端末を含む）については、自ら管理する必要がある。 利用者は、Microsoft Azureが定める機器の管理等の運用管理の境界等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-10					(f) 個人情報の記録媒体の管理（保管・授受等）の方法	最低限	利用者(Microsoft Azureを利用する利用者）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計および実装されています。	適合可能	文献[01]では、データガバナンスの一環として、Microsoft Azureサービスの提供に使用される資産の所有者を割り当てるポリシー、データの安全な廃棄、非公開データの非運用環境への移動またはコピーの禁止、情報漏えいを防止する論理制御と物理制御について明示されている。加えて、資産に対するアクセス権を資産の所有者の承認を得たうえで付与されること、定期的なアクセスの確認や監査を行うこと、内部または外部の組織とのデータ交換手順の遂行、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセス制限も明示されている。 また、同文献では、お客様のデータが損失するのを防ぐレプリケーション、アプリケーションとストレージを管理するサブスクリプション作成等の機能が整備されていることが明示されている。 さらに、文献[19]では、Microsoft Operations Centersにおいて、データ管理も含めて全体の管理を実施していることが明示されている。 加えて、インタビューの結果、管理責任者を中心とした社内ミーティングが行われていることから、管理体制が整備されていると考えられる。	要NDA	文献[01]文献[19]	–	（本調査で確認した内容に記載の通り）	–	利用者は、Microsoft Azureが定める個人情報を記録した媒体の運用管理規程等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-11					(g) 患者等への説明と同意を得る方法	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、患者への説明及び同意を得る主体となる必要がある。
6.3-12					(h) 監査	最低限	利用者(Microsoft Azureを利用する利用者）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。 利用者はマイクロソフトに指示を出すことにより、利用者の監査権を行使しています。利用者はマイクロソフトに与える指示を変更することができます。	適合可能	Microsoft Azure 及び GFS が ISO27001を取得していることから、有効なリスク管理態勢を有していると考えられる。 また、Microsoft Azureにおける運用状況については、第三者認証の各種レポートや、文献[03]、文献[06]、文献[07]などの公開資料を利用できることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。	公開文書	文献[03]文献[06]文献[07]文献[81]	ISO/IEC 27001	–	–	利用者は、Microsoft Azureが実施するシステム監査等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-13					(i) 苦情・質問の受付窓口	最低限	マイクロソフトは利用者からの問い合わせ先としてAzureサポートを提供しています。	適合可能	文献[65]では、マイクロソフトがクラウドサービスの一部を外部業者へ委託している場合、マイクロソフトのクラウドサービス提供に係る責任は全てマイクロソフトにあることを確認した。 文献[144]及び文献[153]にて、Microsoft は、英語では重要度 A 及び B に対して、日本語では重要度 A に対して、24 時間 365日体制でサポートを提供していることが明示されている。	公開文書	文献[65]文献[144]文献[153]	–	–	–	利用者は、Microsoft Azureが実施する受付窓口等の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.4-01	6.4	–	物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて異つかセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。 ① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理） ② 盗難、窃視等の防止 ③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置		個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。また、個人情報を扱う業務端末も利用者の管理となります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていること、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持ち込みみ物、及び持ち出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートの発生やデータの暗号化により、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療機関等の利用者側の施設について、適切な施錠管理を行う必要がある。
6.4-02					個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。 ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	最低限	ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデ	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。	公開文書	文献[01]	–	–	–	利用者は、医療機関等の利用者側の施設について、適切な施錠管理を行う必要がある。

厚生労働省ガイドラインの評価項目								Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.4-03					個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・入退者の記録を定期的にチェックし、妥当性を確認する。	最低限	オ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンターの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。	要NDA	文献[01]	–	–	NDA文献[N01]	利用者は、医療機関等の利用者側の施設における、適切な入退室管理を行う必要がある。
6.4-04					個人情報が存在するPC 等の重要な機器に盗難防止用チェーンを設置すること。	最低限		適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。 また同文献には、Azureサービスの提供に使用される資産には所有者が割り当てられ、資産の一覧が保持されていること、資産の所有者は一覧を最新化する義務を負うこと、資産の一覧を検証するために定期的な監査が実施されることが記載されている。	公開文書	文献[01]	–	–	–	利用者は、医療機関等の利用者側の施設における、適切な端末管理（盗難防止対策）を行う必要がある。
6.4-05					覗き見防止の対策を実施すること。	最低限		適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。	公開文書	文献[01]	–	–	–	利用者は、医療機関等の利用者側の施設における、適切な端末管理（覗き見防止対策）を行う必要がある。
6.4-06					防犯カメラ、自動侵入監視装置等を設置すること。	推奨		適合可能	文献[01]には、バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、及びデータ センター環境への物理アクセスの際の 2 要素認証など、複数の認証とセキュリティプロセスによって、アクセスを適切に制限していることが記載されている。	公開文書	文献[01]	–	–	–	利用者は、医療機関等の利用者側の施設について、適切な監視を行う必要がある。
6.5-01		6.5	–	技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。 しかし、その有効範囲を認識し適切な適用を行えば、技術的な対策は強力な安全対策の手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。 （1）利用者の識別及び認証 （2）情報の区分管理とアクセス権限の管理 （3）アクセスの記録（アクセスログ） （4）不正ソフトウェア対策 （5）ネットワークの上からの不正アクセス	情報システムへのアクセスにおける利用者の識別と認証を行うこと。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview また、利用者がAzureの管理画面を利用する際にはAzure Active Directoryを利用することで識別、認証がなされます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 文献[01]では、Microsoft Azure の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。	公開文書	文献[01]	–	–	–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 利用者は、利用者自身のユーザーによるアクセスを制御し、そのようなアクセスを適切に確認する責任を負う。
6.5-02					本人の識別・認証にユーザID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。	最低限		適合可能	文献[01]では、企業対メインアカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負う。
6.5-03					本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合 、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。"	適合可能	文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。 また文献[126]には、多要素認証として設定している方式が一時的に利用できない場合における代替手段の設定方法が記載されている。	公開文書	文献[31]文献[63]文献[126]	–	–	–	利用者は、多要素認証として設定している手段が利用できない場合であっても業務を停止させないため、その代替手段の設定方法について予め周知しておく必要がある。
6.5-04					入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 技術的な管理および手続き上の管理はマイクロソフトのポリシーの一部であり、その中には一定時間のセッション タイムアウトに関する要件などの分野も含まれます。 ISO 27001 規格（具体的には付属文書 A の項 11.3）で、"ユーザーの責任" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 利用者は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 11.2.1 および 11.2.3）で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、一定時間の無操作時にセッションタイムアウトが設定されることが明示されている。また、利用者が使用するパスワードについて、適切に規定されたパスワードポリシーに準じて管理できることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、医療機関等の利用者側の施設における、適切な端末管理（スクリーンロック等）を行う必要がある。
6.5-05					動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトには、格納域内のデータおよび伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあります。 ISO 27001 規格（具体的には付属文書 A の項 12.3.2）で、"メディアの取り扱い" が規定されています。 Azureにおいて、利用者管理者のクライアント機器とAzureサービスの管理システム間の通信は全てTLSにより暗号化されます。 Azure上で動作するアプリケーションが行う通信と、Azure上に格納するデータの暗号化は利用者アプリケーションによって必要な暗号化を行う必要があります。ここで使用される暗号鍵は利用者管理のものとなります。 データ保存時の暗号化に関しては、利用者のアプリケーション側で対応する必要があります。弊社からは開発者向けに暗号化ライブラリを提供しており、こちらを利用することが可能です。また、暗号化キーの管理についても Azureの標準機能としては提供しておりませんので、利用者にてご用意頂く必要がございます。 Azure上で動作するアプリケーションに関して、（1）、（3）は非該当、7については利用者の責任範囲となります。 128 ビット以上の暗号化キーを使用する TLS により、Microsoft Azure データセンター間および対象のデータセンターのクラスター間で送信される制御メッセージを保護します。エンド ユーザーとユーザーの仮想マシン間のトラフィックを暗号化する事も可能です。 改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 またMicrosoft Azure内部コンポーネント間の全ての通信はSSLで保護され、改ざんを未然に防止しています。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはないと明示されている。 そのため、Microsoftの担当者がテストに本番データを使用することが無いことを確認した。	公開文書	文献[134]文献[135]	–	–	–	利用者及びSI事業者は、医療情報システムの動作確認時に個人情報を使用する際には、適切な漏洩対策を行う必要がある。
6.5-06					医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合 、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、医療情報システム上のアクセス管理を適切に行う必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.5-07					アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。 情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[01]では、Microsoft Azure全体で正確な時刻を維持するために、NTPによる時刻同期が行われていることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、最適化への継続的な取り組みの一環としてPDCAサイクルを採用していることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[138]及び文献[142]では、環境の動作状況を判断するために必要な情報は、Azure Active Directory（Azure AD）レポートで入手できると明示されている。また、マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関するレポートは、契約プランによって7日または30日保持すると明示されている。ユーザー アカウントの正当な所有者ではない人によって行われた可能性があるサインイン試行、及び侵害された可能性があるユーザーアカウントに関するレポートは、契約プランによって7日または30日、90日保持されることが明示されている。	公開文書	文献[01]文献[06]文献[07]文献[131]文献[138]	–	–	–	利用者及びSI事業者は、医療情報システム上のログ管理を適切に行う必要がある。
6.5-08					アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されています。	適合可能	文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、最適化への継続的な取り組みの一環としてPDCAサイクルを採用していることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[138]及び文献[142]では、環境の動作状況を判断するために必要な情報は、Azure Active Directory（Azure AD）レポートで入手できると明示されている。また、マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関するレポートは、契約プランによって7日または30日保持すると明示されている。ユーザー アカウントの正当な所有者ではない人によって行われた可能性があるサインイン試行、及び侵害された可能性があるユーザーアカウントに関するレポートは、契約プランによって7日または30日、90日保持されることが明示されている。	公開文書	文献[01]文献[06]文献[07]文献[131]文献[138]	–	–	–	利用者及びSI事業者は、医療情報システム上のログ管理（保護対策）を適切に行う必要がある。
6.5-09					アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準（PST、GMT、UTC など）を使用しています。可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Microsoft Azure サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格（具体的には付属文書 A の項 10.10.6）で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure全体で正確な時刻を維持するために、NTPによる時刻同期が行われていることが明示されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に行う必要がある。
6.5-10					システム構築時、適切に管理されていないメディア使用時、外部からの情報受信時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。	最低限	マイクロソフトのオンラインサービスの各チームは担当範囲の業務について外部からシステムや機器受け入れを実施する際には、規定に従った手順に従ってセキュリティを含む各種要件が充当されていることを確認する必要があります。 また、Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。	適合可能	文献[01]では、Microsoft Azure において、専門のサポートグループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメータが監視されることが明示されている。 文献[10]及び文献[155]では、マイクロソフトで採用されている「セキュリティ開発ライフサイクル（SDL）」にて、リリース段階における最終的なセキュリティレビューの実施、リリースするコードのアーカイブ、リリース後のレスポンス計画が明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、ウイルスなどのインシデント発生時に、組織的なプロセス（特定、抑制、根絶、復元、及び教訓の学習）により対応することが明示されている。	要NDA	文献[01]文献[10]文献[155]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、Azure上に構築した医療情報システムについて、脆弱性対策およびウィルス対策を適切に行う必要がある。
6.5-11					パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別にIC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長で6.2 ヶ月以内※0.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Microsoftアカウントでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証については利用者の責任範囲です。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。	公開文書	文献[01]文献[63]	–	–	–	利用者は、Microsoft Azureにおけるパスワードポリシーが、医療機関等が求める内容を含むものであることを確認する必要がある。
6.5-12					無線LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。 (2) 不正アクセスの対策を施すこと。少なくともSSID やMAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えばWPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線LAN の適用に関しては、総務省発行の「安心して無線LAN を利用するために」を参考にすること。	最低限	–	対象外	インタビューにて、Azureの構成要素に無線LANの使用が無いことを確認したため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。
6.5-13					13. IoT 機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。 (4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。	最低限	–	対象外	インタビューにて、Azureの構成要素にIoT機器の使用が無いことを確認したため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。
6.5-14					情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報資産の区分管理を適切に実施する必要がある。

厚生労働省ガイドラインの評価項目								Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.5-15					離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。また、個人情報を扱う業務端末も利用者の管理となります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 技術的な管理および手続き上の管理はマイクロソフトのポリシーの一部であり、その中には一定時間のセッション タイムアウトに関する要件などの分野も含まれます。 ISO 27001 規格（具体的には付属文書 A の項 11.3）で、"ユーザーの責任" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、一定時間の無操作時にセッションタイムアウトが設定されることが明示されている。	公開文書	文献[01]	–	–	–	–
6.5-16					外部のネットワークとの接続点やDB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 また、文献[04]では侵入テスト、文献[130]では、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて明示されている。 文献[01]では、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[71]では、仮想マシンとして利用可能なファイアウォールやWAFのイメージがマーケットプレースに多数用意されており、これらを組み合わせて用いることで利用者が必要とするファイアウォール機能やWAF機能が容易に利用可能であることが明示されている。	要NDA	文献[01]文献[04]文献[27]文献[71]文献[130]	–	–	–	利用者は、利用者側の施設等における外部ネットワークとの接続点において、適切なセキュリティ対策を実施する必要がある。
6.5-17					パスワードを利用者識別に使用する場合 以下の基準を遵守すること。 （1）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不応時間を設定すること。 （2）パスワード再入力の失敗が一定回数を超えた場合は再入力を一 定期間受け付けない機構とすること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Microsoftアカウントでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証については利用者の責任範囲です。	適合可能	インタビュー等を通じて、パスワード認証失敗時には適切にそのアカウントが無効化されることを確認した。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、Microsoft Azureにおけるパスワードポリシーが、医療機関等が求める内容を含むものであることを確認する必要がある。 利用者及びSI事業者は、医療情報システムにおけるパスワード認証失敗時には、適切な挙動をとるようにシステムを構築・運用する必要がある。
6.5-18					認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又はIC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI）により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ・ターミナル サービス サーバーは、高度な暗号化設定を使用するように構成されています。 ・Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証（RSA、SecurID）が必要であり、(Azure に接続するために) マイクロソフト企業ネットワーク にリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。 Azure環境への認証については、多要素認証が使用可能となっています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、必要に応じて2要素認証などを導入する必要がある。
6.5-19					無線LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。	推奨	–	対象外	インタビューにて、Azureの構成要素に無線LANの使用が無いことを確認したため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。
6.5-20					IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。	推奨	–	対象外	インタビューにて、Azureの構成要素にIoT機器の使用が無いことを確認したため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。
6.6-01		6.6	–		（1）従業者に対する人的安全管理措置 医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。 1．法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。	最低限	マイクロソフトの全従業員には業務遂行基準の遵守が義務付けられており、その中には機密情報の保護も含まれます。 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1F1gU	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N02]にて、必要な要件を満たした人員の配置を実施していることが確認できた。 文献[65]では、顧客データにアクセス可能なマイクロソフト担当者には秘密保持義務が適用されることが明示されている。	要NDA	文献[01]文献[02]文献[65]	–	–	NDA文献[N02]	利用者及びSI事業者は、自身の管理下にある従業員等については、適切に管理する必要がある。
6.6-02				医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。 医療情報システムに関連する者として、次の5 種類を想定する。 (a) 医師、看護師等の業務で診療に関わる情報を取扱い、法令上の守秘義務のある者 (b) 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取扱い、守秘義務を負う者 (c) システムの保守業者等の雇用契約を結ばずに医療機関等の業務に携わる者 (d) 見舞い客等の医療情報にアクセスする権限を有しない第三者 (e) 診療録等の外部保存の委託においてデータ管理業務に携わる者	2．定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 文献[128]にて、運用及び開発を行う全てのスタッフに対して、セキュリティ及びプライバシーに関する情報提供と、最低1年に1回のセキュリティトレーニングを実施していることが記載されている。 文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。 また、インタビュー等を通して、一般的な防災・防犯訓練は実施していることを確認した。	要NDA	文献[01]文献[128]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、自身の管理下にある従業員等については、適切に教育を実施する必要がある。
6.6-03					3．従業者の退職後の個人情報保護規程を定めること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 従業員の雇用終了プロセスは、Microsoft 米国本社の人事ポリシーによって行われます。 ISO 27001 規格（具体的には付属文書 A の項 8.3）で、"雇用の終了または雇用状態の変更" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、従業員、契約業者、サードパーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するよう通知されると明示されている。	公開文書	文献[01]	–	–	–	利用者及びSI事業者は、従業者の退職後の個人情報保護規程を定める必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目番号	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から展開した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.6-04					サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。	推奨	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 容量管理: 事前予防的な監視により、Microsoft Azure サービス プラットフォームの主要サブシステムのパフォーマンスを、許容されるサービスのパフォーマンスと可用性に対して確立された境界を基準にして継続的に測定します。しきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにします。システム パフォーマンスおよび容量の使用率については、環境を最適化するために事前に計画を立てます。	適合可能	文献[07]では、機密情報のアクセス制御が可能であること(ただし、秘密キーの管理は利用者自身が行う)、また、DC内部の運用管理者であっても、データ内容へのアクセス権限は持っておらず、利用者の承認を得ずに管理者権限に昇格できないことが明示されている。 文献[06]では、マイクロソフトが業界標準のアクセス機構を採用して、Microsoft Azure の物理インフラストラクチャとデータセンター施設を保護していること、データセンターへのアクセス権限とその承認権限はローカルデータセンターのセキュリティ方針に従い、マイクロソフトの運用担当者によって管理されていることが明示されている。 文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していることが明示されている。	公開文書	文献[01]文献[06]文献[07]	–	–	–	–
6.6-05					医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 1）受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 要員の管理についてはマイクロソフト就業規則、労使協定にて定義されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N02]にて、必要な要件を満たした人員の配置を実施していることが確認できた。 文献[65]では、顧客データにアクセス可能なマイクロソフト担当者には秘密保持義務が適用されることが明示されている。	要NDA	文献[01]文献[02]文献[65]	–	–	NDA文献[N02]	利用者は、医療情報システムを提供する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。
6.6-06					② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、特定のプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	–
6.6-07					③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。	最低限	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 容量管理: 事前予防的な監視により、Microsoft Azure サービス プラットフォームの主要サブシステムのパフォーマンスを、許容されるサービスのパフォーマンスと可用性に対して確立された境界を基準にして継続的に測定します。しきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにします。システム パフォーマンスおよび容量の使用率については、環境を最適化するために事前に計画を立てます。	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。 また同文献では、データセンターの施設へのアクセスを制限することが明示されている。	公開文書	文献[01]	–	–	–	利用者は、利用者側の施設等における入退室管理を適切に実施する必要がある。
6.6-08							4) 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Microsoft は、一部のサービス（カスタマー サポートなど）の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Azure の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 NDA文献[N01]にて、対象には孫負業者も含まれていることが確認できた。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。 インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 NDA文献[N02]にて、サードパーティによるサービス、レポート、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることが確認できた。	要NDA	文献[01]文献[02]文献[42]文献[134]	–	（マイクロソフト社とのNDAにより開示）	NDA文献[N01] NDA文献[N02]	–
6.6-09							プログラムの異常等で、保存データを救済する必要があるとき等、やむを えない事情で外部の保守 要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。	推奨	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 要員の管理についてはマイクロソフト就業規則、労使協定にて定義されています。 Microsoft Azureの運用にかかわる従業員はセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N02]にて、必要な要件を満たした人員の配置を実施していることが確認できた。 文献[65]では、顧客データにアクセス可能なマイクロソフト担当者には秘密保持義務が適用されることが明示されている。	要NDA	文献[01]文献[02]文献[65]	–	–	NDA文献[N02]	–
6.7-01		6.7	–		医療に係る電子情報は破棄に関しても安全性を確保する必要がある。破棄は確実に行う必要がある。しかし、例えばデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もあり、注意しなくてはならない。 実際の破棄に備えて、事前に破棄の手順を明確化しておくべきである。	「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。	最低限	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用し、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用すると明示されている。また、同文献にて廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されると明示されている。	公開文書	文献[01]	–	–	–	利用者は、医療に係る電子情報の破棄について、手順等を定める必要がある。
6.7-02					情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うことがし、残存し、読み出し可能な情報がないことを確認すること。	最低限	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。 クラウドサービス上では膨大な数の記憶装置（ハードディスク等）を使用しており、記憶装置の故障や耐用年数期限による交換は定常的に生じるため、個々の記憶装置の故障・交換に際して利用者に通知することはありません。 これらのプロセスは第三者監査の対象となっており、もし異常があった場合にはその解決策とともに第三者監査報告書に記載されますので、利用者による検証が可能です。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶媒メディアと廃棄管理サービスを使用していることが明示されている。 文献[65]では、記憶装置等のコンポーネントを廃棄する際には、不要となったお客様データを消去し、復元できない状態にすること及び、業界標準プロセスを使用し、契約終了後一定期間を経て不要になったデータを消去することを確認した。また、この廃棄手続きは、Azureを使用する際に同意する条項に含まれていることを確認した。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊されますドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないように、このような デバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。 またインタビュー等で確認したところ、記憶装置上の物理的消去及び論理的消去状況については、第三者監査報告書により検証が可能であることが確認できた。	要NDA	文献[01]文献[65]文献[139]	–	（本調査で確認した内容に記載の通り）	–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 SI事業者側では、利用者（ビジネスパートナー）に対して、Microsoft Azureで実施される記憶装置の管理方法及び、契約終了時のデータ削除プロセス等について十分な説明を行う必要がある。
6.7-03					外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策(2)事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。	最低限									

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から展開した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.7-04					運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成	最低限	機器及び破棄手順については、Azureをご利用いただく際に同意いただく「オンラインサービス条項」にも含まれております。 http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46							
6.8-01		6.8	–	医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。 ・個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等 ・真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等 ・見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等 ・保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	最低限	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Microsoft は、一部のサービス (カスタマー サポートなど) の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Azure の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従おう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従おう、契約によって義務付けられています。	適合可能	文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。 インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 NDA文献[N02]にて、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることが確認できた。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員はMicrosoft Azure が開催するセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ管理は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること 文献[150]にて、ディバイスが廃棄される時は、米国の NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。	要NDA	文献[01]文献[02]文献[42]文献[134]	–	（マイクロソフト社とのNDAにより開示）	NDA文献[N02]	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 テストデータ・個人情報の使用については利用者及びSI事業者の責任にて実施する必要がある。
6.8-02					メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を装して操作確認を行うための識別・認証についても同様である。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または決定されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI）により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ・Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証 (RSA、SecurID) が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許可するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、特定のプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行うことが明示されている。 さらに、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。 文献[85]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 文献[01]にて、Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証を用いた利用者認証によるアクセス制御、なりすまし対策を行っていること、またシステム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることを確認した。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]にて、パスワードの長さ、複雑度、有効期限の最小要件はマイクロソフトの企業 Active Directory ポリシーを通じて管理され、すべてのサービス及びインフラストラクチャは、最低でもこの要件を満たす必要があることを確認した。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品 や生体情報による認証の組み合わせが可能であることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されており、外部ネットワークを介した情報交換において、情報の盗聴・改ざん・破壊等から保護するための手順が確立されていることを確認した。 また、インタビュー等を通じて、ログ保持期間は30日間としていることが確認できた。	要NDA	文献[01]文献[06]文献[31]文献[63]文献[65]文献[81]文献[131]	–	（本調査で確認した内容に記載の通り）	–	利用者は、オペレーション実行時の運行状況を確認し、オペレーションを記録する必要がある。 利用者がAzure上で構築するアプリケーションやサービスに対する不正プログラムへの防御対策については、利用者が対策を講じる必要がある。 利用者は、利用者自身のユーザーによるアクセスを制御し、そのようなアクセスを適切に確認するとともに、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。
6.8-03					そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Microsoftアカウントでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。							
6.8-04					保守要員の異動や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 従業員の雇用契約の終了や異動時におけるアクセス権限の無効化に関して、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行っています。	適合可能	文献[01]にて、情報セキュリティ対策の手順として、データガバナンス・設備/施設セキュリティ・暗号化キーの管理・脆弱性ハンドリング・インシデント管理・監視等に関する手順が整備されていること、またそれらのポリシーや手順はリスク評価レポートに基づき決定され、定期的に見直しがなされていることを確認した。 文献[01]にて、Microsoft Azureでは、年に1度リスク評価が実行され、データ、ソフトウェア、ハードウェア等の資産に対する機密性、整合性、及び可用性の影響の評価が行われることを確認した。 文献[01]にて、従業員の雇用契約の終了や異動時におけるアクセス権限の無効化に関して、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査が行われることを確認した。 文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者がAzure上で構築したアプリケーションやサービスに対する不正プログラムへの防御対策については、利用者が対応を講じる必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。
6.8-05					保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	最低限								
6.8-06					保守会社と守秘義務契約を締結し、これを遵守させること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview EA契約およびオンラインサービス条件において、MicrosoftとAzure利用者間の秘密保持に関する項目が明記されています。	適合可能	文献[01]にて、情報セキュリティ対策の手順として、データガバナンス、設備/施設セキュリティ、暗号化キーの管理、脆弱性ハンドリング、インシデント管理・監視等に関する手順が整備されていること、またそれらのポリシーや手順はリスク評価レポートに基づき決定され、定期的に見直しがなされていることを確認した。 文献[65]では、顧客データにアクセス可能なマイクロソフト担当者には秘密保持義務が適用されることが明示されている。	公開文書	文献[01]文献[65]	–	–	–	利用者は、医療情報システムのアプリケーションについては、別途保守会社と守秘義務契約を締結する必要がある。
6.8-07					保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	最低限	マイクロソフトはベストプラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。	適合可能	インタビューにて、マイクロソフトが個人情報を含むデータを組織外に持ち出すことは無いことを確認している。 また、文献[01]では、マイクロソフトはベストプラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用し、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用すると明示されている。また、同文献にて廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されると明示されている。	要NDA	文献[01]	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、保守会社が個人情報を含むデータを持ち出す場合には、運用管理規程等を定めさせ、確認および承認を行う必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.8-08					リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト データセンター あるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連する利用者に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行うことが明示されている。 さらに、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。 文献[65]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 また、インタビュー等を通じて、ログ保持期間は30日間としていることが確認できた。	要NDA	文献[01]文献[06]文献[07]文献[65]文献[81]文献[131]	–	（本調査で確認した内容に記載の通り）	–	利用者は、Azureの運用者に対して保守作業を依頼した場合を含めて、定期的にログを確認する必要がある。
6.8-09					再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview EA契約およびオンラインサービス条件において、MicrosoftとAzure利用者間の秘密保持に関する項目が明記されています	適合可能	文献[65]では、マイクロソフトがクラウドサービス提供の一部を外部業者へ再委託している場合、再委託先の業務範囲も含めてマイクロソフトの責任範囲であることを確認した。 文献[01]にて、Microsoft Azureでは、年に1度リスク評価が実行され、データ、ソフトウェア、ハードウェア等の資産に対する機密性、整合性、及び可用性の影響の評価が行われることを確認した。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。 インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 NDA文献[N02]にて、サードパーティによるサービス、レポート、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることが確認できた。	要NDA	文献[01]文献[02]文献[42]文献[65]文献[134]	–	（マイクロソフト社とのNDAにより開示）	NDA文献[N02]	利用者は、他社のクラウドサービスを組み合わせて使用する場合には、当該クラウドサービスとAzureとの連携部分について対応する必要がある。
6.8-10					詳細なオペレーション記録を保守操作ログとして記録すること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行うことが明示されている。 さらに、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。 文献[65]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。	要NDA	文献[01]文献[06]文献[07]文献[65]文献[81]文献[131]	–	（本調査で確認した内容に記載の通り）	–	–
6.8-11					保守作業時には医療機関等の関係者立会いのもとで行うこと。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。 システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます	適合可能	医療機関等の関係者による保守作業への立会い、また医療機関施設内での保守業務等は実施していないが、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	–
6.8-12					作業員各人と保守会社との守秘義務契約を求めること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの運用にかかわる従業員はセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフおよびGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、さらに従業員との契約に機密保持条項を含めていることが明示されている。	公開文書	文献[01]	–	–	–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
6.8-13					保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。	推奨	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフト データセンターあるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連する利用者に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 利用者コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントは利用者コンテンツへのアクセス権限を有していません。そのため利用者がデータセンターに立ち入ったとしても、利用者コンテンツにアクセスすることはできないため、経営不安等の理由による利用者コンテンツ保全のためのデータセンター立入を受け入れる用意はありません。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 マイクロソフトの資産やデータの保護手順は、論理的なデータや物理的なデータの保護を規定するガイダンスを提供します。これには、移転に関する指示も含まれています。データが格納される場所は、利用者が管理します。詳細については、プライバシーに関する声明（http://www.microsoft.com/windowsazure/legal/）を参照してください。 ISO 27001 規格（具体的には付属文書 A の項 9.2.7 および 10.1.2）で、"資産の除去および変更の管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行うことが明示されている。 さらに、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 情報を外部に持ち出す際のデータの保護に関しては、ガイダンスがあることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。 文献[65]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 また、インタビュー等を通じて、ログ保持期間は30日間としていることが確認できた。	要NDA	文献[01]文献[06]文献[07]文献[65]文献[81]文献[131]	–	（本調査で確認した内容に記載の通り）	–	–
6.8-14					保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 文献[138]及び文献[142]では、環境の動作状況を判断するために必要な情報は、Azure Active Directory (Azure AD) レポートで入手できると明示されている。また、マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関するレポートは、契約プランによって7日または30日保持すると明示されている。ユーザー アカウントの正当な所有者ではない人によって行われた可能性があるサインイン試行、及び侵害された可能性があるユーザーアカウントに関するレポートは、契約プランによって7日または30日、90日保持されることが明示されている。	公開文書	文献[07]文献[81]文献[131]文献[138]	–	–	–	患者情報に対するアクセスの記録は利用者側もしくはSI事業者側にて対応する必要がある。
6.9-01		6.9	–	昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。 一方で、在宅医療、訪問診療等の増加、モバイル端	組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.9-02				末の発展により医療情報を持ち出すニーズや機会が増加していることも事実である。 情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末やCD-R、USBメモリのような情報記録可能媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。 まず重要なことは、「6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」の「6.2.2 取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3 リスク分析」を実施することである。 その上で、医療機関等において把握されている情報もしくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。 一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。 このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要となる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。 ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。	運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-03					情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-04					運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-05					医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-06					情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-07					盗難、置き忘れ等に対応する措置として、情報に対して暗号化したリアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-08					持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LAN はS.5 章C-11 の基準を満たさないことがあるため、利用できない、ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は6.11 章で述べている基準を満たした通信手段を選択すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-09					持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-10					個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は1～5 の対策を行うとともに、管理者の責任において上記の6、7、8、9 と同様の要件を順守させること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-11					外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-12					情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-13					情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-14					スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・BYODは原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。	推奨	–	対象外	インタビューにて、BYODの使用が無いことを確認したため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.10-01	6.10	–		災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（BCP：Business Continuity Plan）と呼ぶ。 我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため適切なBCPの作成と訓練は可能であり、必須の事項と考えられる。 医療機関全体のBCP は本ガイドラインの範疇を超えるため、ここでは「6.2.3 リスク分析」の「7.医療情報システムに関する自然災害やサイバー攻撃によるIT 障害等の非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における医療情報システムのBCP や留意事項について述べる。ただし、医療機関全体のBCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならなければならないことは言うまでもない。 「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非定常状態になる場合がある。前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合である。この際の個人情報保護に関する対応、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。	医療サービスを提供し続けるためのBCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、“ビジネス継続性管理における情報セキュリティの側面” が規定されています。	適合可能	文献[01]では、マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されること、文書化された手順による継続性の計画を含むフレームワークを保持していることが明示されている。 また文献[07]では、DCや各種サポートの稼働状況をポータルから確認できること、障害発生時はRSSで通知を行う機能もあること、契約したインスタンスの稼働状況については専用ポータルから確認できること、API経由でも確認できることが明示されている。さらに、マイクロソフトとの個別サポート契約（有料）を結ぶことにより、障害発生時に一般利用とは異なるレベルの対応が可能となることが明示されている。 文献[01]では、Microsoft Azure の継続性プログラムを主導するフレームワークに「通知、エスカレーション、宣言のプロセス」があることが明示されている。 さらに、インタビュー等を通じて、ガイドラインにて求められる水準の対応がなされていること、委託先が契約通りに委託業務を遂行できないリスクは無いことを確認した。 文献[01]では、Microsoft Azure の継続性プログラムを主導するフレームワークに「文書化された手順による継続性の計画」があること、復元計画は定期的に検証されることが明示されている。 文献[07]では、利用者のインシデントをマイクロソフトのサポート担当が仮想マシンのログを取得し原因究明や解析を行うことが明示されている。 NDA文献[N02]にて、コンティンジェンシープランと同等なBCP対策が規定され、定期的に検証され、是直されることが確認できた。 さらに、インタビュー等を通じて、一般的な障害に対しても、ログ分析等を通じて原因を調査する仕組みが組み込まれていることを確認した。	要NDA	文献[01]文献[02]文献[07]	–	（本調査で確認した内容に記載の通り）	NDA文献[N02]	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 利用者は、地理的な冗長性のためにアプリケーションを複数のデータセンターに展開する責任を負う。 利用者がAzure上で構築した環境については、障害時・災害時に利用者自身が実施すべきコンピュータシステムの復旧手順を明確にする必要がある。 情報資産の管理責任者やその許容範囲、資産価値や法的要求に基づいた資産の分類は利用者側にて実施する必要がある。
6.10-02					正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、正常復帰後のデータ整合性について適切に対応する必要がある。
6.10-03					非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。 ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、“ビジネス継続性管理における情報セキュリティの側面” が規定されています。	適合可能	インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されること、文書化された手順による継続性の計画を含むフレームワークを保持していることが明示されている。 また文献[07]では、DCや各種サポートの稼働状況をポータルから確認できること、障害発生時はRSSで通知を行う機能もあること、契約したインスタンスの稼働状況については専用ポータルから確認できること、API経由でも確認できることが明示されている。さらに、マイクロソフトとの個別サポート契約（有料）を結ぶことにより、障害発生時に一般利用とは異なるレベルの対応が可能となることが明示されている。 文献[01]では、Microsoft Azure の継続性プログラムを主導するフレームワークに「通知、エスカレーション、宣言のプロセス」があることが明示されている。 さらに、インタビュー等を通じて、ガイドラインにて求められる水準の対応がなされていること、委託先が契約通りに委託業務を遂行できないリスクは無いことを確認した。 文献[01]では、Microsoft Azure の継続性プログラムを主導するフレームワークに「文書化された手順による継続性の計画」があること、復元計画は定期的に検証されることが明示されている。 文献[07]では、利用者のインシデントをマイクロソフトのサポート担当が仮想マシンのログを取得し原因究明や解析を行うことが明示されている。 NDA文献[N02]にて、コンティンジェンシープランと同等なBCP対策が規定され、定期的に検証され、是直されることが確認できた。 さらに、インタビュー等を通じて、一般的な障害に対しても、ログ分析等を通じて原因を調査する仕組みが組み込まれていることを確認した。	要NDA	文献[01]文献[02]文献[07]	–	（本調査で確認した内容に記載の通り）	NDA文献[N02]	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 利用者は、地理的な冗長性のためにアプリケーションを複数のデータセンターに展開する責任を負う。 利用者がAzure上で構築した環境については、障害時・災害時に利用者自身が実施すべきコンピュータシステムの復旧手順を明確にする必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.10-04					サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、"非常時"と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先 厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。また、監督官庁への報告は利用者が行う必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureは状態やデータセンター障害の情報を利用者に提供しており、利用者はそれらを監督官庁への報告のために参照することができます。	適合可能	医療情報システムに係る非常事態及び障害は利用者側にて対応する必要があるが、利用者の対応に必要なAzureに関する情報とAzure側の対策として下記が明示されている。 ・文献[01]では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。 ・文献[140]では、Azureサービスの正常性情報が開示されている。 ・文献[01]では、インシデント発生時の体制について、インシデントマネージャーやインシデントエンジニアについて、インシデントの処理方法や管理の役割、責任について、及び法務、経営管理者へのエスカレーションとコミュニケーション計画について明示されている。 ・文献[06]では、各施設は24時間365日稼働するように設計され、停電、物理的な侵入、ネットワークの停止などから運用を保護する様々な手段がとられていることが示されている。このことから、通常の定期保守以上に十分な管理がされていると考えられる。 ・文献[130]では、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて明示されている。 文献[152]にて、データセンターの所在地の開示についてのマイクロソフト社の情報提供方針及びデータセンターの所在地が明示されている。	公開文書	文献[01]文献[06]文献[130]	–	–	–	所管官庁への連絡は利用者側で実施する必要がある。 利用者がMicrosoft Azure上で構築する環境については、利用者が対策する必要がある。また必要に応じて、情報共有機関やセキュリティベンダー等と連携する必要がある。 利用者は、各種資源の能力及び使用状況の確認を行い、システムの性能強化や機能強化、組み合わせの再検討等を行う必要がある。 利用者がAzure上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。
6.11-01		6.11	–	ここでは、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。ここでは、双方向だけではなく、一方向の伝送も含む。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS 型のサービスを利用する、医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する、患者等による外部からのアクセスを許可する、等が考えられる。 医療情報をネットワークを利用して外部と交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない、すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。	ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。 上記を満たす対策として、例えばIPsec とIKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を開始ネットワークの採用に際特にネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。 上記を満たす対策として、例えばIPsec とIKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を開始ネットワークの採用に際特にネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（GSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。また、文献[01]では通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されており、通信の安全性について確認した。 文献[01]では、悪意のあるイベントへの対応を行ううえで、システム上の悪意のある可能性のある動作を識別するために多数の主要なセキュリティ パラメーターを監視すること、パブリック ネットワーク上のレマイクロソフト データ センターとの間で転送されるデータを暗号化するオプションが提供されることが明記されていることを確認した。 文献[01]にて、パスワードの長さ、複雑度、有効期限の最小要件はマイクロソフトの企業 Active Directory ポリシーを通じて管理され、すべてのサービス及びインフラストラクチャは、最低でもこの要件を満たす必要があることを確認した。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 文献[01]にて、Microsoft Azure データ センター内のネットワークは、複数の個別のネットワーク セグメントを持つように設計されており、重要なバックエンド サーバやストレージ デバイスを公開用インターフェイスから分離できること、必要に応じて信頼境界によって論理的に分離されること、複数のネットワーク セグメント間でトラフィックを分離するために、ネットワーク ACL とフィルタが組み込まれていることを確認した。 文献[131]には、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。	公開文書	文献[01]文献[06]文献[31]文献[63]文献[131]	–	–	–	所管官庁への連絡は利用者側で実施する必要がある。 ネットワーク構成図は利用者側にて作成する必要がある。 利用者は、端末側で使用する暗号鍵が第三者によって解読及び漏洩すること防ぐ対策を講じる必要がある。 利用者がAzure上で構築したアプリケーションやサービスで独自に使用する暗号鍵の保護については、利用者が対策する必要がある。 リバースプロキシサーバについては必要に応じて利用者もしくは当事業者にて構築する必要がある。
6.11-02				データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としてはPKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アセットの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクルが要件に挙げられています。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。	適合可能	文献[01]では、パブリック ネットワークを介してマイクロソフト データ センターとの間で転送されるデータを暗号化するオプションが提供されることが明記されていることを確認した。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[01]にて、パスワードの長さ、複雑度、有効期限の最小要件はマイクロソフトの企業 Active Directory ポリシーを通じて管理され、すべてのサービス及びインフラストラクチャは、最低でもこの要件を満たす必要があることを確認した。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 文献[89]では、Azure API Management に相互証明書を使用して API のバックエンド サービスへのアクセスを保護する機能が利用できることが明示されている。 文献[01]では、通信時のデータを暗号化するオプションが提供されること、API の呼び出しなどの重要な通信または Microsoft Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があること、暗号鍵の管理主体は原則利用者となることが明示されている。 また、インタビューにて、インターネットを経由したVPNで接続する場合には、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	文献[01]文献[06]文献[07]文献[31]文献[63]文献[89]	–	（本調査で確認した内容に記載の通り）	–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 利用者は、利用者自身のユーザーによるアクセスを制御し、その アクセスを適切に確認する必要がある。
6.11-03					施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「6.5技術的安全対策」で包括的に述べているので、それを参照すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ・Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証 (RSA、SecurID) が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます (正規の ID バッジをカード リーダーに通します)。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されています。 暗号鍵の不正使用防止は顧客の責任において行う必要があります。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。	公開文書	文献[01]文献[06]文献[31]文献[63]	–	–	–	–
6.11-04					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し、施設内のルータを経由して異なる施設間を結ぶVPN の間で送受信ができないように経路設定されていること、安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureプラットフォームを構成するソフトウェアおよびハードウェアについては、高いセキュリティを確保できる機能を持ったものであることを確認することが、Microsoft社内規定で決められております。	適合可能	インタビュー等を通じて、ネットワーク機器の調達にあたっては、セキュリティ要求に対する充足を含めた、信頼性の高い機器が調達されることが確認出来た。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者は、VPN装置を含む利用者側のネットワーク機器について、安全性が確認出来る機器を利用する必要がある。
6.11-05					送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureにおいて、利用者管理者のクライアント機器とAzureサービスの管理システム間の通信は全てTLSにより暗号化されます。 Azure上で動作するアプリケーションが行う通信と、Azure上に格納するデータの暗号化は利用者アプリケーションによって必要な暗号化を行う必要があります。ここで使用される暗号鍵は利用者管理のものとなります。	適合可能	文献[01]によると、利用者端末とMicrosoft Azureサービスの管理システム間の通信はTLSにより暗号化されることが明示されている。また、文献[01]では、通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は、利用者側アプリケーションの責任で暗号化を実施する必要があることが明示されている。 文献[07]によると、暗号鍵の管理主体は原則利用者となり、公開文書にも明示されている。 インタビューにて、インターネットを経由したVPNで接続する場合には、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	文献[01]文献[06]文献[07]	–	（本調査で確認した内容に記載の通り）	–	–

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.11-06					医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。 そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 ・交換した医療情報等に対する管理責任及び事後責任の明確化。個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。サービスレベル未達の場合には、サービス利用代金の返還を行うことと、SLAに記載しています。 指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 法的権限を持つ監査当局等の検査等が行われる場合、マイクロソフトは利用者に協力します。利用者による監査について、利用者が必要となる情報を提供します。 セキュリティインシデント発生時には、対象となる利用者、被害の状況が判明し次第速やかることとしており、このことは契約書に記載しています。 インシデント発生およびその疑いのある場合の調査協力、情報提供については本調査に必要となるログは標準のサービス機能として提供しているため契約書上への記載は不要としています。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 Azure サービスの使用は、取得されたサービスの契約内容および使用条件に準拠するものとします。Microsoft は、法的条件を単純化し、これらすべての契約を、1 つのオンライン サービス条件に統合しました。これには、利用者の確約内容、詳細なデータ保護条件、エンタープライズ オンライン サービス（Azure、Office 365、および Intune を含む）での欧州連合（EU）標準契約条項の一般的なセットが含まれます。 サブスクリプション（無料試用版を含む）を Microsoft からオンラインで購入または無料利用できる場合、その使用は、マイクロソフト オンライン サブスクリプション契約に準拠するものとします。これには、オンライン サービス条件が含まれています。2014 年 11 月 13 日より前にオンラインで購入された利用者の場合、契約期間が満了するか更新されるまで、その使用は、Microsoft Azure 契約および Microsoft Azure サービス条件に準拠するものとします。 別のボリューム ライセンス契約（エンタープライズ契約など）を通じて購入された利用者の場合、その使用は、購入されたサービスのボリューム ライセンス契約に準拠するものとします。これには、オンライン サービス条件が含まれています。ボリューム ライセンス契約書の写しは、Microsoft アカウントの代表者に連絡するか、ボリューム ライセンスのサイトを通じて入手することができます。 Azure サブスクリプションをお持ちでない場合、Azure サービスの使用は、Microsoft Azure の Microsoft Online Services カスタマー ポータル使用条件に準拠するものとします。 ご不明の点またはその他の質問がある場合は、Microsoft Azure サポートへご連絡ください。 準拠法は日本となります。	最低限	適合可能	文献[65]、文献[141]及び文献[141]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[65]及び文献[141]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。 文献[01]では、パブリック ネットワークを介してマイクロソフト データ センターとの間で転送されるデータを暗号化するオプションが提供されることが明記されていることを確認した。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[03]にて、情報セキュリティ対策の手順として、データガバナンス、設備/施設セキュリティ、暗号化キーの管理、脆弱性ハンドリング、インシデント管理・監視等に関する手順が整備されていること、またそれらのポリシーや手順はリスク評価レポートに基づき決定され、定期的に見直しがなされていることを確認した。 文献[141]、文献[151]及び文献[154]では、提供事業者として必要な基本的な事項が規定・明記され、実現に向けた対策が講じられていることを確認した。 特筆すべき事項としては、次のとおり。 ・準拠法は、米国連邦法、ワシントン州法を基本としているが、国別条項において、日本国法が優先適用または付加されることとなっている。 ・指示目的外使用は、クラウドにおける個人情報保護に関する国際標準「ISO/IEC27018:2014」の認証を取得し、指示目的外使用の禁止を行っている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、サブシステムは契約事業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 利用者に提供されるAzureの暗号化機能として、文献[136]にてポイント対サイト接続の暗号化、文献[137]にてサイト間接続の暗号化が明示されている。	公開文書	文献[01]文献[06]文献[07]文献[65]文献[131]文献[136]文献[137]文献[151]文献[154]	ISO/IEC 27018	–	–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、利用可否を決定する必要がある。 利用者は、Azureの契約書および使用条件を確認し、Azureの責任が及ばない範囲については、自ら対策を施す必要がある。
6.11-07					リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログイン を防止すること。 また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書(SMAPIにより認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証 (RSA、SecurID) が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[01]にて、パスワードの長さ、複雑度、有効期限の最小要件はマイクロソフトの企業 Active Directory ポリシーを通じて管理され、すべてのサービス及びインフラストラクチャは、最低でもこの要件を満たす必要があることを確認した。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]にて、Microsoft Azure データ センター内のネットワークは、複数の個別のネットワーク セグメントを持つように設計されており、重要なバックエンド サーバやストレージ デバイスを公開用インターフェイスから分離できること、必要に応じて信頼境界によって論理的に分離されること、複数のネットワーク セグメント間でトラフィックを分離するために、ネットワーク ACL とフィルタが組み込まれていることを確認した。	公開文書	文献[01]文献[31]文献[63]	–	–	–	ネットワーク構成図は利用者側にて作成する必要がある。
6.11-08					回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。 また上記1 及び4 を満たしていることを確認すること。	最低限	Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。 指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。利用者は、アプリケーションの容量ニーズの監視と計画について責任を負います。 準拠法は日本となります。	適合可能	文献[01]では、Microsoft Azureにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビューにて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。 文献[65]、文献[141]及び文献[147]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[141]、文献[151]及び文献[154]では、提供事業者として必要な基本的な事項が規定・明記され、実現に向けた対策が講じられていることを確認した。 特筆すべき事項としては、次のとおり。 ・準拠法は、米国連邦法、ワシントン州法を基本としているが、国別条項において、日本国法が優先適用または付加されることとなっている。 ・指示目的外使用は、クラウドにおける個人情報保護に関する国際標準「ISO/IEC27018:2014」の認証を取得し、指示目的外使用の禁止を行っている。 文献[65]及び文献[141]及び文献[147]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	要NDA	文献[01]文献[65]文献[147]文献[151]文献[154]	ISO/IEC 27018	（本調査で確認した内容に記載の通り）	–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、利用可否を決定する必要がある。
6.11-09					患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI 個人認証等の技術を用いた対策を実施すること。 また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療情報システムへのアクセスを患者に提供する際には、適切に対応する必要がある。
6.11-10					オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを「TLS1.2 のみに固定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないウィルスやセッションへのアクセス）等による攻撃からの防護について、適切な対策を実施すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者がAzure上に配置された医療情報システムへの接続が行う場合は、閉域網サービスであるExpressRoute機能、VPN Gateway機能の利用によるVPN接続、HTTPS接続時のクライアント証明書要求設定などをご活用いただくことができます。	適合可能	インタビューにて、Azureと利用者の拠点をVPNで接続することが可能であり、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、要求事項を満たすために最適なネットワーク接続の方式を検討し、構築を行う必要がある。
6.11-11					やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境をVPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療情報システムへのリモートアクセスを従業員等に提供する際には、適切に対応する必要がある。
6.12-01		6.12	「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 二 当該情報について改変が行われていないかどうかを確認することができるものであること。 （電子署名及び認証業務に関する法律（平成12 年法律第102 号）第2 条1 項）	平成11 年4 月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」においては、法令で署名または記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていた。 しかし、平成12 年5 月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書等とて、e-文書法令において指定された文書等においては、「A. 制度上の要求事項」に示した電子署名によって、記名・押印にかわり電子署名を施すことで、作成・保存が可能となった。 ただし、医療に係る文書等では一定期間、署名を信頼性を持って検証できることが必要である。電子署名は組織体への署名や記名・押印と異なり、「A. 制度上の要求事項」の一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり失効させた場合は検証ができないという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的によより強固な暗号アルゴリズムへ移行することも求められる。例えば現在、電子署名に一般的に用いられている暗号方式のRSA 1024bitや、ハッシュ関数のSHA1は、政府機関の情報システムからの移行スジュールが決まっており、2008年4月の情報セキュリティ政策会議が決定した「政府機関の情報システム	(1) 厚生労働省の定める準拠性監査基準を満たす健医療福祉分野PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと 1. 保健医療福祉分野PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野PKI 認証局の発行する電子署名を活用することが推奨される。 ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-02							2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-03							3. 「電子署名に係る地方公共団体の認証業務に関する法律」（平成14 年法律第153号）に基づき、平成16 年1 月29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から照会した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.12-04				において使用されている暗号アルゴリズムSHA1及びRSA1024に関わる移行指針」によれば、2014年度以降、RSA 2048bitやSHA2等へ移行される予定となっている。 従って、電子署名を付与する際はこのような点も考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名の検証が継続できる必要がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。近年、デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、JIS規格としても制定された（JIS X 5092:2008 CMS利用電子署名（CAdES）の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名（XAdES）の長期署名プロファイル）。 長期署名方式では、下記により、署名検証の継続を可能としている。 (1) 署名に付与するタイムスタンプにより署名時刻を担保する（署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること）。 (2) 署名当時の検証情報（関連する証明書や失効情報等）を保管する。 (3) 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。	（2）電子署名を含む文書全体にタイムスタンプを付与すること。 1．タイムスタンプは、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16 年11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-05					2．法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-06					3．タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-07					（3）上記タイムスタンプを付与する時点で有効な電子証明書を用いること。 1．当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない 本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対して タイムスタンプを付与する等の対策が必要である。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
7.1-01	7	7.1	電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。 （e-文書法省令第4 条第4 項第2 号） ② 真正性の確保 電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。 「ア) 故意または過失による虚偽入力、書換え、消去及び混同を防止すること。 (イ) 作成の責任の所在を明確にすること。 （施行通知第2 2 (3)②） 「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1 (1)）	真正性とは、正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であり、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を損ったりすることをいう。 また、ネットワークを通じて外部に保存を行う場合、委託元の医療機関から委託先の外部保存施設への転送途中で、診療録等が書き換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。 従って、ネットワークを通じて医療機関の外部に保存する場合には、医療機関等に保存する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。	【医療機関等に保存する場合】 (1) 入力者及び確定者の識別及び認証 a. 電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 1．入力者及び確定者を正しく識別し、認証を行うこと。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療情報システム上のユーザの識別及び認証について、適切に構築する必要がある。
7.1-02					2．システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療情報システム上のユーザの権限管理を適切に実施する必要がある。
7.1-03					3．業務アプリケーションが複数可能な端末を管理し、権限を持たない者からのアクセスを防止すること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療情報システムを利用可能な端末の管理を適切に実施する必要がある。
7.1-04					b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1．装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者側で管理責任者、操作者以外による機器の操作を運用上防止するルールは利用者側で実施する必要がある。
7.1-05					2．当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療情報システムによる電磁的記録が、いつ・誰が行ったかを明確にする仕組みを構築する必要がある。
7.1-06					（2）記録の確定手順の確立と、作成責任者の識別情報の記録 a. 電子カルテシステム等でPC 等の汎用入力端末により記録が作成される場合 1．診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	電子データの原本性確保は利用者側で実施する必要がある。 利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に行う必要がある。
7.1-07					2．「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者及びSI事業者は、医療情報システムにおける電磁的記録の確定において、作成責任者による確認が可能な機能を構築する必要がある。
7.1-08					3.「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者は、記録の確定を、適切な権限を持った確定者が実施するよう業務の設計を行う必要がある。
7.1-09					4．確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	データの履歴バックアップを作成すること。データのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること。仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者側にある。
7.1-10					5．一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用管理規程に明記すること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者は、一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用する必要がある。
7.1-11					6．確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の管理責任者が記録の確定を実施する等のルールを運用管理規程で定め、記録の確定の責任の所在を明確にすること。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者は、確定者が何らかの理由で確定操作ができない場合、代替策の例やルールを運用管理規程で定め、記録の確定の責任の所在を明確にする必要がある。
7.1-12					b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1．運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。	最低限	利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	運用管理規程等に当該装置により作成された記録の確定ルールを利用者側で定義する必要がある。

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1-13					2. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データの履歴バックアップを作成すること、データのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者側にある。
7.1-14					（3）更新履歴の保存 I. 一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データの履歴バックアップを作成すること、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者側にある。 更新履歴を保存し、更新前と更新後の内容を照らし合わせる機能を備える必要がある。
7.1-15					2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データの履歴バックアップを作成すること、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者側にある。 更新履歴について、更新の順序性が識別できるように参照できる機能を備える必要がある。
7.1-16					（4）代行入力の承認機能 I. 代行入力を実施する場合、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	代行操作に関するルールを運用管理規程で定めることは利用者側で行う必要がある。
7.1-17					2. 代行入力が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	代行操作に関する機能の整備は利用者側で行う必要がある。
7.1-18					3. 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われること。この際、内容の確認を行わずに確定操作を行ってはならない。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	代行操作に関する機能の整備は利用者側で行う必要がある。
7.1-19					（5）機器・ソフトウェアの品質管理 I. システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。 Azureプラットフォームを構成するソフトウェアおよびハードウェアについては、高いセキュリティを確保できる機能を持ったものであることを確認することが、Microsoft社内規定で決められております。	適合可能	文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。 文献[07]によると、Azure側がセキュリティパッチの提供等でバージョンを更新した場合は、ポータルにて確認可能であることが明示されている。	公開文書	文献[01]文献[07]	–	–	–	利用者は、医療情報システム全体の機器及びソフトウェアの構成を管理し、文書化する必要がある。
7.1-20					2. 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureプラットフォームに使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。また、Microsoft Azureプラットフォームの提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残しています。 Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、医療情報システム全体の機器及びソフトウェアの構成を管理し、文書化する必要がある。
7.1-21					3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービス や担う役割に応じたトレーニングを受ける必要があることが明示されている。 文献[128]にて、運用及び開発を行う全てのスタッフに対して、セキュリティ及びプライバシーに関する情報提供と、最低1年に1回のセキュリティトレーニングを実施していることが記載されている。 インタビュー等を通じて、運用環境の更新時には、オペレータを対象に操作方法等についての研修を行うことを確認した。 文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。	要NDA	文献[01]文献[128]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療情報システム全体の機器及びソフトウェアの品質管理に関する運用管理規程を整備し、従業員等への教育を実施する必要がある。
7.1-22					4. システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは利用者に代わり、専門の第三者を選定し外部監査を受け、その結果を利用者に利用可能にすることによって、利用者による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	文献[148]より、Microsoft Azure が ISO27001を取得していることから、有効なリスク管理態勢を有していると考えられる。 文献[01]では、マイクロソフトは不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊からお客様のデータを保護できるように、合理的かつ適切で、技術的及び組織的な対策、内部統制、情報セキュリティ ルーチンを実装しており、今後もこれを維持するために年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていると明示されている。	公開文書	文献[01]文献[148]	ISO/IEC 27001	–	–	利用者は、医療情報システム全体の機器及びソフトウェアに関する内部監査を定期的に実施する必要がある。
7.1-23					【ネットワークを通じて医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 （1）通信の相手先が正当であることを認識するための相互認証を行うこと診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者はアプリケーションの構築において、Azure API Management機能を利用し、相互証明書を使用して API のバックエンド サービスへのアクセスを保護することが利用できます。 サービス管理 API は REST API です。すべての API 操作は SSL 上で実行され、X.509 v3 証明書を使用して相互認証されます。	適合可能	文献[01]では、通信時のデータを暗号化するオプションが提供されること、API の呼び出しなどの重要な通信または Microsoft Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があること、暗号鍵の管理主体は原則利用者となることが明示されている。 利用者に提供されるAzureの暗号化機能として、文献[136]にてポイント対サイト接続の暗号化、文献[137]にてサイト間接続の暗号化が明示されている。 文献[89]では、Azure API Management に相互証明書を使用して API のバックエンド サービスへのアクセスを保護する機能が利用できることが明示されている。	公開文書	文献[01]文献[07]文献[89]文献[136]文献[137]	–	–	–	利用者は、医療機関など利用者側の認証が必要な機器等について、適切に設定・管理を行う必要がある。
7.1-24					（2）ネットワーク上で「改ざん」されていないことを保証すること ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。 なお、可逆的な情報の圧縮・解凍並びにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure利用者の管理者のクライアント機器とAzureサービスの管理システム間の通信は全てTLSにより暗号化されます。 Azure上で動作するアプリケーションが行う通信と、Azure上に格納するデータの暗号化は利用者アプリケーションによって必要な暗号化を行う必要があります。ここで使用される暗号鍵は利用者管理のものとなります。	適合可能	文献[01]によると、利用者端末とMicrosoft Azureサービスの管理システム間の通信はTLSにより暗号化されることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があることが明示されている。 文献[07]によると、暗号鍵の管理主体は原則利用者となり、公開文書にも明示されている。	公開文書	文献[01]文献[07]	–	–	–	利用者は、医療機関などの利用者側のネットワーク上での改ざん対策を行う必要がある。

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1-25					(3) リモートログイン機能を制限すること 保守目的等のどうしても必要な場合を除き行うことができないよう、適切に管理されたリモートログインのみに制限する機能を設けなければならない。 なお、これらの具体的要件については、「6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI）により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Azure上に利用者が構成した仮想マシンへのリモート接続は、Azure Security CenterのJust in Time Access機能で特定のユーザーと時間のみに制限することが可能です。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、医療情報システム全体の機器及びソフトウェアに対するリモートアクセスについて、その妥当性を含めて適切に管理する必要がある。
7.2-01		7.2	必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 （e-文書法省令第4 条第4 項第1 号） ① 見読性の確保 必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。 (ア) 情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。 (イ) 情報の内容を必要に応じて直ちに書面に表示できること。 （施行通知第２２(3)①）	電子媒体に保存された内容を、権限保有者からの「診療」「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループットと操作方法で、肉眼で見読可能な状態にできることである。e-文書法の精神によれば、面面上での見読性が確保されていることが求められているが、権限保有者の要求によっては対象の情報の内容を直ちに書面に表示できることが求められることもあるため、必要に応じてこれに対応することを考慮する必要がある。 電子媒体に保存された情報は、紙に記録された情報と違い、以下の理由によりそのままでは見読できない場合がある。 ・電子媒体に格納された情報を見読可能なように画面に呼び出すために何らかのアプリケーションが必要であること ・記録が、他のデータベースやマスター等を参照する形で作成されることが多く、データの作成時点で採用したマスター等に依存しなければ、正しい記録として見読できないこと ・複数媒体に分かれて記録された情報の相互関係が、そのままでは一つの系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。	(1) 情報の所在管理 統管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	電子媒体に関する管理は利用者側で対応する必要がある。
7.2-02					(2) 見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	電子媒体に関する見読化手段の管理は利用者側で対応する必要がある。
7.2-03					(3) 見読目的に応じた応答時間 目的に応じて速やかに検索表示もしくは書面に表示できること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	検索表示に関するアプリケーションの機能は利用者側で確保する必要がある。
7.2-04			「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第２１(1)）	保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。 診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、下記のものが考えられる。 (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等 (2) 不適切な保管・取扱いによる情報の滅失、破壊 (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取り (4) 媒体・機器・ソフトウェアの整合性不備による復元不能 (5) 障害等による電子保存時の不整合 これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。	(4) システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureは利用者が冗長構成を取るために必要となる基本機能（可用性セット、可用性ゾーン、リージョンペアなどの機能）を提供しています。 MicrosoftのAzure運用に関しては、エンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]によると、Microsoft Azure のバックアップ及び冗長性プログラムは、年に 1 度レビューと検証が行われること、障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されることが明示されている。 また同文献によると、継続性プログラムを主導するフレームワークを保持していることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、利用者側のネットワークや端末などの冗長性を確保する必要がある。
7.2-05					【医療機関等に保存する場合】 (1) バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	マイクロソフトではデータ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。	適合可能	文献[01]では、データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義及び維持されています。Windows Azure のバックアップ及び冗長性プログラムは、年に 1 度レビューと検証が行われると明示されている。 また、同文献にてWindows Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されると明示されている。	公開文書	文献[01]	–	–	–	データのバックアップをプラットフォーム以外に保存することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者側にある。
7.2-06					(2) 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データのバックアップをプラットフォーム以外に保存することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者側にある。
7.2-07					(3) 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureは利用者が遠隔地バックアップを取るために必要となる基本機能（Azure Backup, Azure Site Recovery, Geo-redundant Storageなどの機能）を提供しています。	適合可能	文献[01]によると、継続性プログラムを主導するフレームワークを保持していることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、遠隔地へのデータバックアップの要否を含めて、必要最小限の診療録等の見読性を確保する必要がある。
7.2-08					【ネットワークを通じて外部に保存する場合】 医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。 (1) 緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	公開文書	–	–	–	–	データのバックアップをプラットフォーム以外に保存することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者側にある。
7.2-09					(2) 緊急に必要になるまではいえない診療録等の見読性の確保 緊急に必要になるまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureは利用者が災害対策に必要となる基本機能（Azure Backup, Azure Site Recovery, Geo-redundant Storageなどの機能）を提供しています。	適合可能	文献[01]によると、継続性プログラムを主導するフレームワークを保持していることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、遠隔地へのデータバックアップの要否を含めて、必要最小限の診療録等の見読性を確保する必要がある。
7.3-01		7.3	電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。 （e-文書法省令第4 条第4 項第3 号） ③ 保存性の確保 電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。 （施行通知第２２(3)③）	保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。 診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、下記のものが考えられる。 (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等 (2) 不適切な保管・取扱いによる情報の滅失、破壊 (3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取り (4) 媒体・機器・ソフトウェアの整合性不備による復元不能 (5) 障害等による電子保存時の不整合 これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。	【医療機関等に保存する場合】 (1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止 I. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療機関など利用者側の機器等について、セキュリティ対策を適切に行う必要がある。
7.3-02			「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第２１(1)）		(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止 I. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフおよびGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。 文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 また、インタビュー等を通じて、ログ保持期間は30日間としていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療機関など利用者側の機器等について、セキュリティ対策を適切に行う必要がある。

厚生労働省ガイドラインの評価項目							Microsoft Azure における対応							
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
7.3-03					2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトでは、データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure ストレージにはレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合に利用者のデータが損失するのを防ぐことができます。 利用者は、Microsoft Azure上での構成として、冗長化構成を取る事で障害が起きた場合において継続利用をする事が可能です。また、データの履歴のバックアップを作成すること、データのバックアップをAzureプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスを展開すること、仮想マシンの状態のバックアップを作成することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者にあります。 ISO 27001 規格 (具体的には付属文書 A の項 10.5.1) で、"情報のバックアップ" が規定されています。	適合可能	文献[01]では、定期的にプライマリーデータセンターからセカンダリーデータセンターにレプリケートされること、お客様は必要に応じて自社でのデータの抽出及びバックアップの実行を選択できることが明示されている。 文献[38]では、Site Recovery機能を用いることで、仮想マシンのレプリケーションと回復手順が自動化できることが明示されている。 文献[06]では、利用者が地理的に分散した第2のストレージアカウントを作成することで、ホット・フェールオーバー機能が利用できることが明示されている。 文献[38]では、Site Recovery機能を用いることで、仮想マシンのレプリケーションと回復手順が自動化できることが明示されている。	公開文書	文献[01]文献[06]文献[38]	–	–	–	利用者は、運用管理規程の作成および運用の周知徹底を行う必要がある。
7.3-04					3. 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。	最低限	マイクロソフトでは、アクセスは職務によって制限しており、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなアプに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データ センターの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書(OST)に記載しています。	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。 文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。 文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持ち込みみ物、及び持ち出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートの発生やデータの暗号化により、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	NDA文献[N01]	利用者は、医療機関など利用者側の機器等について、セキュリティ対策を適切に行う必要がある。
7.3-05					4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書(SMAPI)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[138]及び文献[142]では、環境の動作状況を判断するために必要な情報は、Azure Active Directory (Azure AD) レポートで入手できると明示されている。また、マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関するレポートは、契約プランによって7日または30日保持すると明示されている。ユーザー アカウントの正当な所有者ではない人によって行われた可能性があるサインイン試行、及び侵害された可能性があるユーザーアカウントに関するレポートは、契約プランによって7日または30日、90日保持されることが明示されている。	公開文書	文献[01]文献[138]	–	–	–	利用者は、医療機関など利用者側の機器等について、セキュリティ対策を適切に行う必要がある。
7.3-06					5. 各保存場所における情報が き損した時に、バックアップされたデータを用いて き損前の状態に戻せること。もし き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure ストレージにはレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合に利用者のデータが損失するのを防ぐことができます。 利用者は、Microsoft Azure上での構成として、冗長化構成を取る事で障害が起きた場合において継続利用をする事が可能です。また、データの履歴のバックアップを作成すること、データのバックアップをAzureプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスを展開すること、仮想マシンの状態のバックアップを作成することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任は利用者にあります。	適合可能	文献[01]によると、Microsoft Azure にはレプリケーション機能が含まれており、お客様のデータが損失するのを防ぐことが明示されている。	公開文書	文献[01]	–	–	–	文献[01]によると、利用者のデータの履歴バックアップを作成すること、利用者のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者にある。
7.3-07					(3) 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 1. 記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。	最低限	Azureのストレージは冗長化し持続性を担保するように運用されています。ローカル冗長ストレージは、オブジェクトに年間 99.999999999% (9 が 11 個) 以上の持続性が提供されます。 https://docs.microsoft.com/ja-jp/azure/storage/common/storage-redundancy-lrs	適合可能	文献[01]によると、Microsoft Azure のバックアップ及び冗長性プログラムは、年に 1 度レビューと検証が行われること、障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されることが明示されている。 文献[01]では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。 文献[06]では、各施設は24時間365日稼働するように設計され、停電、物理的な侵入、ネットワークの停止などから運用を保護する様々な手段がとられていることが示されている。このことから、通常の定期保守以上に十分な管理がされていると考えられる。	公開文書	文献[01]文献[06]	–	–	–	文献[01]によると、利用者のデータの履歴バックアップを作成すること、利用者のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者にある。
7.3-08					(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 1. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データ形式の選択・設定は、利用者が対応する必要がある。
7.3-09					2. マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	文献[01]によると、利用者はMicrosoft Azure内で利用者がホスティングするアプリケーションに対する責任を負う。
7.3-10					【ネットワークを通じて医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 (1) データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureの仮想ネットワークゲートウェイはIPSecなど一般的なプロトコルを利用可能で、利用者はVPN接続時に利用できます。	適合可能	文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。 インタビューを通じて、通信の暗号化については、国際標準への準拠や、暗号化の強化のために仕様の変更が行われること、さらに変更が行われる場合には事前に顧客に通知していることが確認した。	要NDA	文献[05]	–	（本調査で確認した内容に記載の通り）	–	利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。 利用者は、医療情報システムで使用するデータ形式及び転送プロトコルについて、バージョン管理と継続性の確保を行う必要がある。
7.3-11					(2) ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。	最低限	Microsoft Azure利用者はゲストOS、ソフトウェア及びアプリケーションをコントロールし、利用者の機器に対する管理を行う事ができます。またその管理は利用者の責任となります。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。利用者は、アプリケーションの容量ニーズの監視と計画について責任を負います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていること、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。	公開文書	文献[01]	–	–	–	–
7.3-12					【医療機関等に保存する場合】 (1) 不適切な保管・取扱いによる情報の滅失、破壊の防止 1. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。	推奨	医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。 なお、Azureに関しては、利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview	適合可能	文献[06]では、マイクロソフトが業界標準のアクセス機構を採用して、Microsoft Azure の物理インフラストラクチャとデータ センター施設を保護すること、アクセスはごく少数の運用担当者に限定される必要があり、かつ担当者は管理アクセス用の資格情報を定期的に変更する必要があること、データ センターへのアクセス権限とその承認権限は、ローカル データ センターのセキュリティ方針に従い、マイクロソフトの運用担当者によって管理されていることが明示されている。 文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。また、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。 インタビューの結果、日本国内ではみ部に面したガラス部分には容易な破壊を防止する強度のものを採用し、あわせて侵入センサー、もしくは監視カメラ等を設置している。また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階窓部分への接近を防止、もしくは検知する仕組みを採用している。これらの対策により、必要な防犯措置が講じられていると考えられる。	要NDA	文献[01]文献[06]	–	（本調査で確認した内容に記載の通り）	NDA文献[N01]	–

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.3-13					2. サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。	公開文書	文献[01]	–	–	–	–
7.3-14					3. 診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	適合可能	文献[01]によると、Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されていることが明示されている。 文献[06]によると、Microsoft Azure 内でファブリックの 3 つの異なるノードに複製され、ハードウェア障害の影響を最小限に抑えることが明示されている。	公開文書	文献[01]文献[06]	–	–	–	利用者は、データのバックアップに対する改ざん等を確認する機能を備える必要がある。
7.3-15					(2) 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 若しくはRAID-6 相当以上のディスク障害に対する対策を行うこと。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	適合可能	文献[01]によると、Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発及びメンテナンス プロセスが用意されていることが明示されている。 文献[06]によると、Microsoft Azure では、顧客データの整合性を確保するため、VMのアーキテクチャ、構成ファイル、ストレージアカウント等を用いた方法でデータ保護を実現していることが明示されている。	公開文書	文献[01]文献[06]	–	–	–	利用者は、医療機関など利用者側の施設等で管理する記憶媒体の劣化対策を行う必要がある。
7.3-16					【ネットワークを通じて医療機関等の外部に保存する場合】 (1) ネットワーク中や外部保存を受託する機関の設備の互換性を確保すること I. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。	推奨	Microsoft Azureプラットフォームでは、サービス継続性の管理 (SCM) の開発およびメンテナンス プロセスが用意されています。このプロセスには、Microsoft Azure の資産を回復し、Microsoft Azure の主要なビジネス プロセスを再開するための方法が含まれています。継続性ソリューションによって、サービスの運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されます。利用者は、地理的な冗長性のためにアプリケーションを複数の場所に展開する責任を負います。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.4) で、"機器のメンテナンス" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]によると、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。 文献[01]によると、Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発及びメンテナンス プロセスが用意されていることが明示されている。 文献[06]によると、スイッチ、ルーター、ロード バランサーなどのネットワーク デバイスの構成と管理は、認証されたマイクロソフトの運用担当者によって、通常、大きな変更 (データ センター自体の再構成など) があった場合にのみ実施されるが、これらのデバイスはMicrosoft Azure ファブリックにより仮想化されているため、事実上顧客からは変更が認識できないことが明示されている。	公開文書	文献[01]文献[06]	–	–	–	–
8.1-01	8	8.1	電気通信回線を通じて外部保存を行う場合にあっては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第1条の5 第1 項に規定する病院又は同条第2 項に規定する診療所その他これに準ずるものとして医療法人等が適切に管理する場所、行政機関等が開設したデータセンター等、及び医療機関等が民間事業者等との契約に基づいて確保した安全な場所に置かれるものであること。 （外部保存改正通知第2 1 (2)）	ネットワークを通じて医療機関等以外の場所に診療録等を保存することができれば、システム堅牢性の高い安全な情報の保存場所の確保によるセキュリティ対策の向上や災害時の危機管理の推進、保存コストの削減等により医療機関等において診療録等の電子保存が推進されることが期待できる。しかし、外部保存には保存機関の不適切な情報の取り扱いにより患者等の情報が瞬時に大量に漏えいする危険性も存在し、その場合、漏えいした場所や責任者の特定が困難になる可能性がある。そのため、常にリスク分析を行いつつ万全の対策を講じなければならず、医療機関等の責任が相対的に大きくなる。さらには、情報の保存を受託する機関等もしくは従業者による、利益を目的とした不当利用の危惧がある点も事実である。その一方で金融情報、信用情報、通信情報は実態として保存・管理を当該事業者以外の外部事業者に委託しており、合理的に運用されている。金融・信用・通信に関わる情報と医療に関わる情報を一概に同様に扱うことはできないが、一般に実績あるデータセンター等の情報の保存・管理を受託する事業者は慎重で十分な安全対策を講じており、医療機関等が自ら管理することに比べても厳重に管理されていることが多い。 本来、医療に関連した個人情報の漏えいや不当な利用等により、個人の権利利益が侵害された場合には、被害者の苦痛や権利回復が困難であることが多く、医療機関等や関係各者に対し、法律や各種ガイドライン等により格別の安全管理措置を講じることが求められている。従って、診療録等のネットワークを通じた医療機関等以外の場所での外部保存については、通常求められる安全管理上の体制と同等以上の体制を確保した上で、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることが原則である。 上記に対応するためには「C. 最低限のガイドライン」で定める、「(2)行政機関等が開設したデータセンター等に保存する場合」と「3.医療機関等が民間事業者等との契約に基づいて確保した安全な場所」に該当する機関を選定する場合には、「C. 最低限のガイドライン」で定める事項を厳守し、また、データセンター等の情報処理関連事業者が経済産業省が定めた「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」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 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」の要求事項を満たしていることを確認の上、契約等でその遵守状況を明らかにしなくてはならない。	(1) 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (ア) 病院や診療所の内部で診療録等を保存すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-02					(イ) 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-03					(ウ) 病院、診療所等であっても、保存を受託した診療録等について分析等を行う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-04					(エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取り扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-05					(オ) 情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-06					(カ) 情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-07					2) 行政機関等が開設したデータセンター等に保存する場合 (ア) 法律や条例により、保存業務に従事する個人もしくは従事していた個人に対して、個人情報の内容に係る秘匿義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-08					(イ) 適切な外部保存に必要な技術及び運用管理能力を有すること を、システム監査技術者及びCertified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-09					(ウ) 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-10					(エ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないようにさせること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-11					3) 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。サービスレベル未達の場合には、サービス利用代金の返還を行うことと、SLAに記載しています。 指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 法的権限を持つ監査当局等の検査等が行われる場合、マイクロソフトは利用者に協力します。利用者による監査について、利用者が必要となる情報を提供します。 セキュリティインシデント発生時には、対象となる利用者、被害の状況が判明し次第連絡することとしており、このことは契約書に記載しています。 インシデント発生およびその疑いのある場合の調査協力、情報提供についてはその調査に必要となるログは標準のサービス機能として提供しているため契約書上への記載は不要としています。 マイクロソフトは全社で共通となる業務遂行基準 (SBC) を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書 (OST) 記載済み。 準拠法は日本となります。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[65]及び文献[141]及び文献[147]では、報告・連絡等の運営ルール、セキュリティインシデント発生時の対応が規定・明記されている。また、セキュリティインシデントの調査に必要となるログ出力などの基本的な機能は、標準サービスで提供されていることを確認した。また、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。 文献[151]では、「6 責任制限 a.制限」にて、本契約に基づくすべての請求についての各当事者の責任範囲は、請求原因が発生する前の12か月間に本契約に基づきオンライン サービスについて支払われた金額を上限とする直接損害に限定されることが確認できた。	公開文書	文献[01]文献[07]文献[65]文献[147]文献[151]	–	–	–	利用者は、医療情報システム提供事業者との間で、守秘に関連した事項や違反した場合のペナルティを含む委託契約を締結し、情報の取り扱いに関する監督を行う必要がある。
8.1-12					(イ) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。	最低限	6.11に示したとおり。	適合可能	6.11の確認事項のとおり。	–	–	–	–	–	–

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.1-13					(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「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」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 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」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。	最低限	クラウドサービスに係る契約は、弊社の標準的な契約書（MBSA、EA、OST、SLA、加入契約など）に基づいて行うため変更できませんが、利用者の契約内容変更のご要望については、必要に応じて導入ベンダー様と相談のうえ対応を検討させていただきます。	適合可能	総務省ガイドラインについては、本セキュリティリファレンスに確認結果を記載した。 経済産業省ガイドラインについては、別途作成したセキュリティリファレンスに記載した。 インタビュー等を通じて、当該ガイドラインに対応して、契約内容が変更できるかどうかは、ベンダを通じての個別の検討事項であることを確認した。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者は、標準的な契約書等を確認し、ベンダを通じて変更要望の有無を示す必要がある。
8.1-14					(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。	最低限	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 利用者コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントは利用者コンテンツへのアクセス権限を有していません。そのため利用者がデータセンターに立ち入ったとしても、利用者コンテンツにアクセスすることはできないため、経営不安等の理由による利用者コンテンツ保全のためのデータセンター立入を受け入れる用意はありません。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 マイクロソフトの資産やデータの保護手順は、論理的なデータや物理的なデータの保護を規定するガイダンスを提供します。これには、移転に関する指示も含まれています。データが格納される場所は、利用者が管理します。詳細については、プライバシーに関する声明（http://www.microsoft.com/windowsazure/legal/）を参照してください。 ISO 27001 規格（具体的には付属文書 A の項 9.2.7 および 10.1.2）で、"資産の除去および変更の管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、 Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 「6.8情報システムの改造と保守」については、当該項目の確認事項のとおり。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保守作業に必要な範囲を超えた閲覧の禁止に関して確認する必要がある。
8.1-15					(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保存した情報の分析、解析の禁止に関して確認する必要がある。
8.1-16					(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等が起こらないようにさせること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、外部保存を受託する事業者が保存された情報の提供を行わないよう確認する必要がある。
8.1-17					(キ) 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の4 点について確認すること。 (a) 医療情報等の安全管理に係る基本方針・取扱規程等の整備 (b) 医療情報等の安全管理に係る実施体制の整備 (c) 実績等に基づく個人データ安全管理に関する信用度 (d) 財務諸表等に基づく経営の健全性	最低限	マイクロソフトはTrust Centerにて、コンプライアンス、セキュリティ、プライバシー、透明性への取り組みを公開しています。	適合可能	本項目は基本的に医療機関側で実施すべき事項である。 ただし、確認すべき事項については、以下を確認できた。 (a)文献[01]から、情報セキュリティに係る基本方針及び取り扱い規定等を整備していること。 (b)文献[01]から、情報セキュリティに係る実施体制を整備していること。 (c)文献[75]から、「クラウド利用を想定する業務に係る実績、技術力」について、マイクロソフト社のエンタープライズ向けクラウドサービスの実績及び技術力。 (d)文献[149]から、財務諸表を公表していること。	公開文書	文献[01]文献[75]文献[149]	–	–	–	利用者は、外部保存を受託する事業者の選定基準を定める必要がある。
8.1-18					(ア)「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、保存を受託した機関全体としてのより一層の自助努力を患者へ説明に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークやISMS 認定等の第三者による認定を取得すること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-19					(イ)「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、（ア）で述べた第三者による認定を受けること。	推奨	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1-20					(ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法としては、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure ストレージにはレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合に利用者のデータが損失するのを防ぐことができます。 マイクロソフトでは、指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨を契約書に記載しています。	適合可能	文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。	公開文書	文献[06]	–	–	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等を確認する必要がある。
8.1-21					(エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。	推奨	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトでは、指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨を契約書に記載しています。	適合可能	文献[06]では、「機密データに対する厳格なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。	公開文書	文献[06]	–	–	–	利用者は、医療情報システム提供事業者による個人情報の管理方法やアクセスの制御方法（非常時の運用を含む）について確認し、システム提供事業者と合意する必要がある。
8.2-01		8.2	患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。 （外部保存改正通知第2 (3)）	ネットワークを通じて外部に保存する場合、医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設や通信事業者にも及ぶために、より一層、個人情報の保護に配慮が必要となる。 なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮される必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。	(1) 診療録等の外部保存委託先の事業者内における個人情報保護 ① 適切な委託先の監督を行うこと 診療録等の外部保存を受託する事業者内の個人情報保護については本ガイドライン6 章を参照し、適切な管理を行う必要がある。	最低限	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。サービスレベル未達の場合には、サービス利用代金の返還を行うことと、SLAに記載しています。 指示目的外使用については、利用者コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 法的権限を持つ監査当局等の検査等が行われる場合、マイクロソフトは利用者に協力します。利用者による監査について、利用者が必要となる情報を提供します。 セキュリティインシデント発生時には、対象となる利用者、被害の状況が判明し次第連絡することとしており、このことは契約書に記載しています。 インシデント発生おようその疑いのある場合の調査協力、情報提供についてはその調査に必要となるログは標準のサービス機能として提供しているため契約書上への記載は不要としています。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 準拠法は日本となります。	適合可能	インタビュー及び公開文書により、個人情報の取り扱いについて、マイクロソフト社が「分野における個人情報保護に関するガイドラインの安全措置等についての実務指針」の旨に定める「個人データ保護に関する委託先選定の基準」の医療機関の評価作業に十分な情報を提供していることを確認した。 文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 「組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について」は、本ガイドライン6.11項にて記述している。	要NDA	文献[07]	–	（本調査で確認した内容に記載の通り）	–	利用者は、サービス利用廃止時に責任をもってデータ削除を実施する必要がある。
8.2-02					(2) 外部保存実施に関する患者への説明 診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。 ① 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。	最低限	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、個人情報の外部保存を行っている旨を患者に説明し理解を得た上で診療を開始する必要がある。

厚生労働省ガイドラインの評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	章	節	制度上の要求事項	考え方（抜粋）	ガイドライン	分類		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.2-03					2）患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は、意識が回復した時点で事後に説明をし、理解を得る必要がある。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者は、意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は、意識が回復した時点で事後に説明をし、理解を得る必要がある。
8.2-04					3）患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。	最低限	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	利用者は、乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。
8.3-01		8.3	外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。 また、事故等が発生した場合における責任の所在を明確にしておくこと。 （外部保存改正通知第２１(４)）	本項の記載は、「4 電子的な医療情報を扱う際の責任のあり方」及び「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」へ考え方を集約したため、それらを参照されたい。	－	－	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	－
8.4-01		8.4	外部保存を行う病院、診療所等の管理者は、運用管理規程を定め、これに従い実施すること。 （外部保存改正通知第３１）	外部保存に係る運用管理規程を定めることが求められており、考え方及び具体的なガイドラインは、「6.3 組織的安全管理対策」の項を参照されたい。 また、その際の責任のあり方については、「4 電子的な医療情報を扱う際の責任のあり方」を参照されたい。 なお、すでに電子保存の運用管理規程を定めている場合には、外部保存に対する項目を適宜修正・追加等すれば足りると考えられる。	診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査しなくてはならない、また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。 これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記しておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。 これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければならない。 ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。 また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を受託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。 （厚労省ガイドラインでは「B.考え方」の枠に記載されている内容だが、総務省ガイドラインでは要求事項として扱われているためここに記載）	－	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 デバイスが廃棄されるときは、米国の NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われます。	適合可能	文献[65]によると、マイクロソフト社のクラウドサービスでは、業界標準プロセスを使用し、契約終了後一定期間を経て不要になったデータを消去することが明示されている。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[65]	－	（本調査で確認した内容に記載の通り）	－	運用管理規程の整備は利用者側で対応する必要がある。 Azure上のデータの操作はユーザとなる医療機関が自ら行うのみで、通常運用においてマイクロソフト側が操作することはないため、医療機関側で管理する必要がある。 ■消去証明書の受領 SI事業者側では、利用者（ビジネスパートナー）に対して、消去証明書の発行に関する説明および第三者監査報告書等について十分な説明を行う必要がある。 ■データ消去プロセスの簡略化 利用者側では、あらかじめ利用者のリスク管理ポリシーを十分認識の上、機密情報を扱わない業務をクラウドサービスに変わる場合においてのみ、契約終了時のデータ消去プロセスを簡略化することが可能である。

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.1-01	3	3.2.1	上述のように組織的安全管理対策においては、 ・組織・体制の整備 ・運用管理規程の整備 ・運用管理規程に基づく文書類の整備 等が求められる。 これらの観点から、クラウドサービス事業者への要求事項として、以下の対応を行うことが求められる。	（ア） 組織・体制の整備についての要求事項 本項は、組織的安全管理対策を講じるための組織・体制の整備に関する要求事項を示す。 組織・体制の整備 ① サービスの提供についての管理責任を有する責任者を設置する。 ② 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。 ③ サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④ ①から③に掲げた責任者の任命・解任等のルールを策定する。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、セキュリティを重視したサービスを運用し、セキュリティに関する絶対的な安心感をお客様にお約束することが、マイクロソフトの目標です。マイクロソフトは不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊からお客様のデータを保護できるように、合理的かつ適切で、技術的及び組織的な対策、内部統制、情報セキュリティルールを実装しており、今後もこれを維持していきます。年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていると明示されている。 NDA文献[N01]にて、Azureは、サービスの約束とシステムの要件、及びシステム内の効果的な管理を設計、実装、及び運用して、Azureのサービスの約束とシステムの要件が達成されたことを合理的に保証する責任があると明示されていることを確認した。	要NDA	文献[01]	―		NDA文献[N01]	利用者及びSI事業者は、医療情報システムで取り扱う医療情報の安全管理に関する組織・体制を整備する必要がある。	―
3.2.1-02				（イ） クラウドサービスの提供契約についての要求事項 1.守秘義務 ① サービスに係る情報及び受託した情報に関する守秘義務について、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management EA契約およびオンラインサービス条件にて秘密保持に関する項目を含む、その他は必要に応じて個別対応。 マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8) で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[65]では、「担当者は、顧客データに関する秘密保持義務を負い、かかる義務は当該担当者の任用の終了後も継続する」ことが明記されている。 また、インタビュー等を通じて、すべての従業員が適切な含意書にサインして、Microsoft社の雇用ポリシーを受け入れる必要があることを確認した。 文献[01]では、セキュリティの違反、または情報セキュリティポリシーの違反が疑われるMicrosoft Azureサービスのスタッフは、調査プロセスの対象となり、該当する懲戒措置（最も重い場合は雇用終了も含む）が実施されること、セキュリティの違反、または情報セキュリティ ポリシーの違反が疑われる契約業者のスタッフは、正式な調査の対象となり、関連する契約に該当する措置が実施される（契約の終了となる可能性もある）ことが明示されている。 文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられている。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化すること、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[65]文献[134]	―	（本調査で確認した内容に記載の通り）	―	利用者は、医療情報システムを提供する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。 利用者及びSI事業者は、自身の管理下にある従業員等については、適切に管理する必要がある。	―
3.2.1-03				2.運用規定等の遵守 ① サービス提供に係る契約において、次項（ウ）1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、基本的なセキュリティ要件はISMS フレームワーク全体の一部として継続的に確認、向上、実装されることが明示されている。 また、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、標準的な運用手順は少なくとも年に一度見直されること、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、Microsoft Azure のスタッフは全員、情報セキュリティポリシー文書内のすべてのポリシーを確認し、それに従うことに同意した旨を表明すること、Microsoft Azure の契約業者のスタッフは全員、このポリシー内の関連するポリシーに従うことに同意することが明示されている。 文献[06]によると、マイクロソフトが業界標準のアクセス機構を採用して、Microsoft Azure の物理インフラストラクチャとデータ センター施設を保護していることが明示されている。 ISO/IEC 27001の付属文書A6.2.2「顧客対応におけるセキュリティ」、A6.2.3「第三者との契約におけるセキュリティ」を遵守している。 文献[06]及び文献[10]では、システム開発・変更について、開発ライフサイクルを通じたセキュリティ対応の取り組みが明示されている。 文献[01]では、Microsoft Azure サービスがISO の計画 (Plan)、実行 (Do)、評価 (Check)、改善 (Act) プロセスを使用して、継続的にリスク管理フレームワークを保守し強化していること、Microsoft Azure ではインシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発していることが明示されている。 文献[07]によると、障害発生時の対応についてはマイクロソフトとの個別サポート契約（有料）を結ぶことにより、一般利用とは異なるレベルの対応が可能であることが明示されている。 文献[01]では、格納域内のデータ及び伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあることが明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。 文献[06]によると、Microsoft Azure には、監視、ログ、レポートの機能が複数のレベルで実装されており、顧客の可視性を高めていることが明示されている。 文献[93]によると、医療機関からの問い合わせ窓口については、専用のサポートプランによって選択可能であることが明示されている。	公開資料	文献[01]文献[06]文献[07]文献[10]文献[93]	ISO/IEC 27001		―	利用者及びSI事業者は、医療情報システムの運用管理規程を定め遵守する必要がある。	―
3.2.1-04				3 関係ガイドラインの遵守 ① サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。 ② ①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な限り具体的に行う（例えば、総務省が定める「ASP・SaaS（医療情報取扱いサービス）の安全・信頼性に係る情報開示指針」（平成29年3月31日）に定める事項に準じた情報の提供を行う等）		利用者(Microsoft Azureを利用する医療機関などのお客様、サービス提供事業者）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview サービス提供に関わる契約は、医療機関などとサービス提供事業者の間にて締結されますので、マイクロソフトは関与いたしません。 各ガイドラインに対する Microsoft Azure の適合に関しては、各セキュリティリファレンス（総務省・厚生労働省・経産省版）シートをご参照ください。	適合可能	本項目は、セキュリティリファレンス（厚生労働省・経産省版）シートを参照する。	公開資料	―	―		―	利用者及びSI事業者は、医療情報システムの運用管理規程を定め遵守する必要がある。	―
3.2.1-05				（ウ） 運用管理規程についての要求事項 本項は、安全管理対策を講じるための運用管理規程の整備に関する要求事項を示す。厚生労働省ガイドライン第 5 版では、運用管理規程において含めるべき内容について 9 項目を定めている。ここではこれらの項目に従って、クラウドサービス事業者において、自社の運用管理規程の策定や、医療機関との合意等において、対応すべき要求事項を示す。 1.基本方針と管理目的の表明 ① 経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ② ①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③ ①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④ 情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤ 情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。 ⑥ 情報セキュリティポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。	・組織的取組における基本方針	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、セキュリティとプライバシーに関する業界のベストプラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計及び実装されていること、お客様向けバージョンの情報セキュリティポリシーは、要求に応じて入手できると明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 文献[01]では、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。 セキュリティ及び運用上の理由により、Microsoft Azure では、マイクロソフトの Microsoft Azure プラットフォーム サービスに対してお客様自身が監査を行うことを許可していないが、お客様は事前に承認を得ることにより、お客様自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。 文献[01]では、基本的なセキュリティ要件はISMS フレームワーク全体の一部として継続的に確認、向上、実装されることが明示されている。 また、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、標準的な運用手順は少なくとも年に一度見直されること、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。	公開資料	文献[01]	ISO/IEC 27001		―	利用者及びSI事業者は、個人情報保護に関する方針を策定・公開を行う必要がある。 利用者及びSI事業者は、個人情報を取り扱う情報システムに関して情報セキュリティポリシー等の安全管理に関する方針を策定する必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.1-06				2.サービス提供先の体制 ① サービスの提供に係る体制を、緊急時の対応も含めて明確にする。 ② サービスの提供に係る体制等に関する情報（再委託による体制に関する情報を含む）の開示等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス提供に係る体制等に関する情報の開示	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 Microsoft は、一部のサービス（カスタマー サポートなど）の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Azure の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[01]では、セキュリティを重視したサービスを運用し、セキュリティに関する絶対的な安心感をお客様に約束することが、マイクロソフトの目標です。マイクロソフトは不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊からお客様のデータを保護できるように、合理的かつ適切で、技術的及び組織的な対策、内部統制、情報セキュリティ ルーチンを実装しており、今後もこれを維持していきます。年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていると明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。 NDA文献[N02]にて、サードパーティによるサービス、レポート、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることを確認した。 NDA文献[N01]にて、Azureは、サービスの約束とシステムの要件、及びシステム内の効果的な管理を設計、実装、及び運用して、Azureのサービスの約束とシステムの要件が達成されたことを合理的に保証する責任があると明示されていることを確認した。	要NDA	文献[01]文献[02]文献[134]	—		NDA文献[N01] NDA文献[N02]	利用者及びSI事業者は、医療情報システムで取り扱う医療情報の安全管理に関する組織・体制を整備する必要がある。 利用者は、Microsoft Azure及びSI事業者の体制が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-07				3.契約書・マニュアル等の文書の管理 ① 情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。 ② サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。 ③ サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療情報の管理状況に関係する資料の提供 ・サービス提供に係る運用管理規程の開示等の有無、範囲、条件等	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 また Azure上に構築されたお客様システムにおける正確かつ安全に運用するマニュアルの整備についてはお客様での管理になります。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、特定のプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていることが明示されている。 また、Microsoft Azure サービスの一環として包括的なガイダンス、ヘルプ、トレーニング、及びトラブルシューティング用の資料を用意していることが明示されている。 また、マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されること、文書化された手順による継続性の計画を含むフレームワークを保持していることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者は、医療情報システムで取り扱う医療情報の安全管理に関する文書を管理する必要がある。 利用者は、Microsoft Azure及びSI事業者の規模類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-08				4.リスクの発現の予防、発生時の対応の方法 ① サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。 ② サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・受託する医療情報に係るリスク分析の結果と対応措置 ・リスク等に対する予防措置及び事故等の発生時の対応等（自社の規程）	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、特定のプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]では、Microsoft Azure では、年に 1 度リスク評価が実行されること、そこでは、資産に対する機密性、整合性、及び可用性の影響が評価されることが明示されている。 文献[01]では、Microsoft Azure に関するリスク評価プロセスでは、まずリスクを特定し、続いて発生の可能性及び影響を判定することによってリスク レベルを確立し、最後にリスクの影響を許容可能なレベルまで引き下げる制御及び保護措置を特定すること、手段に応じて、可能な限りリスクを軽減するため推奨事項と制御が用意されていることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、Microsoft Azure のスタッフは全員、情報セキュリティポリシー文書内のすべてのポリシーを確認し、それに従うことに同意した旨を表明すること、Microsoft Azure の契約業者のスタッフは全員、このポリシー内の関連するポリシーに従うことに同意することが明示されている。 文献[06]によると、マイクロソフトが業界標準のアクセス機構を採用して、Microsoft Azure の物理インフラストラクチャとデータ センター施設を保護していることが明示されている。 ISO/IEC 27001の付属文書A6.2.2「顧客対応におけるセキュリティ」、A6.2.3「第三者との契約におけるセキュリティ」を遵守している。 文献[06]及び文献[10]では、システム開発・変更について、開発ライフサイクルを通じたセキュリティ対応の取り組みが明示されている。 文献[01]では、Microsoft Azure サービスがISO の計画 (Plan)、実行 (Do)、評価 (Check)、改善 (Act) プロセスを使用して、継続的にリスク管理フレームワークを保守し強化していること、Microsoft Azure ではインシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発していることが明示されている。 文献[07]によると、障害発生時の対応についてはマイクロソフトとの個別サポート契約（有料）を結ぶことにより、一般利用とは異なるレベルの対応が可能であることが明示されている。 文献[01]では、格納域内のデータ及び伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあることが明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。 文献[06]によると、Microsoft Azure には、監視、ログ、レポートの機能が複数のレベルで実装されており、顧客の可視性を高めていることが明示されている。 文献[93]によると、医療機関からの問い合わせ窓口については、専用のサポートプランによって選択可能であることが明示されている。	公開資料	文献[01]文献[06]文献[07]文献[10]文献[93]	ISO/IEC 27001		—	利用者及びSI事業者は、医療情報システムが係るリスクを分析し事故等の発生時における対応を定める必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-09				5.機器を用いる場合の機器等の管理 ① 機器等の管理方法について、文書化を行う。 ② 機器等について、台帳管理等により所在確認等を行う旨を定める。 ③ 機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・機器の管理等の運用（自社の規程）	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフトはお客様に代わり、専門の第三者を選定し外部監査を受け、その結果をお客様に利用可能にすることによって、お客様による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	文献[01]では、Microsoft Azure 環境の主要なハードウェア資産の一覧は保持されていること、資産の一覧を検証するために、定期的な監査が実施されていることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者側で管理する機器等（パソコン等端末を含む）については、自ら管理する必要がある。 利用者は、Microsoft Azure及びSI事業者の規模類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.1-10				8.個人情報の記録媒体の管理方法 ① 個人情報を記録した媒体の管理等に関する運用規程を策定する。 ② 個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・個人情報を記録した媒体の運用	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計および実装されています。 マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 文献[01]では、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。 セキュリティ及び運用上の理由により、Microsoft Azure では、マイクロソフトの Microsoft Azure プラットフォーム サービスに対してお客様自身が監査を行うことを許可していないが、お客様は事前に承認を得ることにより、お客様自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。	公開資料	文献[01]	ISO/IEC 27001		—	利用者及びSI事業者は、記録媒体の管理方法に関する運用規程を定める必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-11				7.患者等への説明と同意を得る方法 ① 医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、患者への説明及び同意を得る主体となり対応する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-12				8.監査 ① サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ② 第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③ 監査実施について記録し、当該記録の保存・管理方法を明確にする。 ④ 自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ 医療機関等に開示する監査記録等の範囲・条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・自社において実施するシステム監査等の状況及びその記録の提示条件・範囲等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management 災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS)に属するOnline Services Security and Compliance（OSSC)の情報セキュリティ管理システム（ISMS)によりレビュープロセスが確立されています。使用する統制策(ISO27001/27005、SAS70 TypeIおよび II、SOX,PCI DSS, FISMA等)の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。 Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 また Azure上に構築されたお客様システムにおける正確かつ安全に運用するマニュアルの整備については お客様での管理になります。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 なお、Microsoft Azure には専用のサポートプランがいくつかございます。実際の運用に合わせてご選択ください。 https://azure.microsoft.com/ja-jp/support/options/	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 文献[01]では、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。 セキュリティ及び運用上の理由により、Microsoft Azure では、マイクロソフトの Microsoft Azure プラットフォーム サービスに対してお客様自身が監査を行うことを許可していないが、お客様は事前に承認を得ることにより、お客様自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。	公開資料	文献[01]	ISO/IEC 27001		—	利用者及びSI事業者は、医療情報システム全体の監査方針を定める必要がある。 利用者は、Microsoft Azure及びSI事業者の監査方針及び関連する文書等が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-13				9.苦情・質問の受け付け窓口の設置 ① 医療機関等の管理者からの問合せ窓口を設ける。また受付の時間帯等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化する。	・医療機関等の管理者側からの問合せ窓口における受付の時間帯等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Azureサポートサポートプランへのご加入でお問合せ窓口がご利用可能です。 WEBからお問合せいただいた内容は担当によって記録され、履歴として共有されます。 https://azure.microsoft.com/ja-jp/support/plans/	適合可能	文献[93]によると、医療機関からの問い合わせ窓口については、専用のサポートプランによって選択可能であることが明示されている。 Azureに関しては文献[143]及び文献[144]、プライバシーに関しては文献[145]及び文献[146]にて問い合わせ窓口が設置されていることを確認した。	公開資料	文献[93]文献[143]文献[144]文献[145]文献[146]	—		—	利用者は、問合せ窓口を設置する必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.1 資産台帳】 【7.3 組織的安全管理策（体制、運用管理規程）】
3.2.1-14				(エ) 運用管理規程に基づく文書類の整備についての要求事項 本項は、運用管理規程に基づく文書類の整備に関する要求事項を示す。厚生労働省ガイドライン第 5 版では、個人情報が参照可能な施設等の入退管理に関する規程等や、アクセス管理規程、委託契約において含めるべき内容について定めている。ここではこれらの項目に従って、クラウドサービス事業者が対応すべき要求事項を示す。 1.アクセス管理規程の策定 ① クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びにアクセス管理の運用状況に関する定期的なレビューの実施等を内容とするアクセス管理規程を策定する。 ② サービスの提供に係るアクセス記録（外部からのアクセス、利用者によるアクセス等を含む）の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データに アクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間 (最長 6 か月) 使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 また、Microsoft Azure の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者は、医療情報システムのアクセス管理規程を作成する必要がある。	【7.2.2 情報の分類】
3.2.1-15				2.委託契約に含めるべき事項 ① 医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、医療情報システム提供事業者（SI事業者等）との間で、医療情報の取り扱いに関する委託契約を定める必要がある。	【7.2.2 情報の分類】
3.2.2-01	3.2.2		(1)を踏まえ、クラウドサービス事業者が行うべき要求事項について以下に記述する。 (ア) サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項 (イ) 個人情報が参照可能な運用端末等の設置場所等における物理的安全管理対策としての要求事項 (ウ) 個人情報が格納されている機器や媒体に対する物理的安全管理対策としての要求事項 なお、本項では、厚生労働省ガイドライン第5版6.4章に対応する要求事項について記載するが、一部、厚生労働省ガイドライン第5版7.3章「保存性の確保について」で示される要求事項のうち、物理的安全管理対策に関するに対応する要求事項も含めることとする。そのため、厚生労働省ガイドライン第5版6.4章では、個人情報の取扱いを対象としているが、ここでは「医療情報を取り扱うサービス」に供する情報全般（例えばサービス提供上の設定データ等、情報が保存されている媒体及び機器の適切な保管・取扱いに必要な情報）を対象としている。	(ア) サービスに供する機器、媒体等の設置場所等における物理的安全管理対策としての要求事項 本項は、サービスに供する機器、媒体等の設置場所に対して、物理的な安全対策を求めるものである。具体的には、機器等の設置場所の施錠管理とアクセス管理（不正なアクセスの防止とそのための管理・監視措置）を内容とする。 1.施錠管理 ① サービスに供する機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。 ② サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③ サービスに供する媒体等を格納するキャビネット等について、施錠管理を行う。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management ISO 27001 規格（具体的には付属文書 A の項 9）で、"バプリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされただアなどで制限されていること、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ複数を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。	公開資料	文献[01]	—		—	利用者及びSI事業者側で管理する機器等（パソコン等端末を含む）については、自ら施錠管理する必要がある。	【7.5.1 医療情報処理施設の建物に関する要求事項】 【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】 【7.5.3 情報処理装置のセキュリティ】 【7.6.5 第三者が提供するサービスの管理】 【7.6.12 ログの取得及び監査】 【7.6.13 アクセス制御方針】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.2-02				2.アクセス制御 ① サービスに供する機器や媒体の設置場所については、許可された者のみが入退できるように制限する。 ② サービスに供する機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。 ③ サービスに供する機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退 者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を適単位で行う等、入退者を特定しうる方策を講じる。 ④ サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤ サービスに供する機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。 ⑥ サービスに供する機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。 ⑦ ①～⑥につき、運用管理規程等に規定する。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management ISO 27001 規格（具体的には付属文書 A の項 9）で、"パブリック アクセス、配送、荷物の積み込み領域、および物理的 /環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を数設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。また、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また同文献には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があること、が明記されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持ち出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートの発生やデータの暗号化により、情報の持ち出しが困難であることが確認できた。 インタビューの結果、日本国内では外部に面したガラス部分には容易な破壊を防止する強度のものを採用し、あわせて侵入センサー、もしくは監視カメラを設置している。また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階定部分への接近を防止、もしくは検知する仕組みを採用している。これらの対策により、必要な防犯措置が講じられていると考えられる。	要NDA	文献[01]	—	（本調査で確認した内容に記載の通り）	NDA文献[N01]	利用者及びSI事業者は、個人情報が参照可能な場所においては、来訪者の記録と識別、入退の制限等の入退管理ルールを定める必要がある。また、入退室記録は、適切な期間保存する必要がある。 利用者及びSI事業者は、情報システムのアクセス管理規程及び運用管理規程を作成する必要がある。	【7.5.1 医療情報処理施設の建物に関する要求事項】 【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】 【7.5.3 情報処理装置のセキュリティ】 【7.6.5 第三者が提供するサービスの管理】 【7.6.12 ログの取得及び監査】 【7.6.13 アクセス制御方針】
3.2.2-03				3.サービスに供する機器や媒体を保存する施設 ① サービスに供する機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐える機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。 ② ①の施設を設置する建築物は、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス提供に使用する機器等が格納されている建物種別（建物名）・地域 ・上記建物における物理的安全管理措置の概要（耐災害のための措置（火災対策、水害対策、落雷雷対策、熱対策等）、入退管理等）	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフトは、ビジネス継続性に関する ISO 22301 認証を取得した最初の超大規模クラウド サービス プロバイダーです。独立した認証機関による、事業継続性のプロセスに関するすべての要素を対象とした厳格な監査を経て、Microsoft Azure、Microsoft Azure Government、Microsoft Cloud App Security、Microsoft Intune、Microsoft Power BI がこの認証を取得しました。この監査では、これら対象サービスのほか、Azure 管理機能、Azure Portal、対象サービスの監視、操作、更新に使用するシステムが審査されました。 ISO 22301:2012 は、ビジネス継続性の確保をサポートする管理システムについての初めての国際規格です。ISO 22301 はビジネス継続性に関する重要規格であり、破壊的な出来事の予防、緩和、対応、回復を図るための厳格な手順（プラクティス）などを認定するものとなります。 https://www.microsoft.com/ja-jp/trustcenter/compliance/iso-22301 災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS）に属するOnline Services Security and Compliance（OSSC）の情報セキュリティ管理システム（ISMS）によりレビュープロセスが確立されています。使用する統制策（ISO27001/27005、SAS70 TypeIおよびII、SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。 Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。	適合可能	文献[01]では、データ センターを保護するために、以下を含む環境の管理を実施しています。 ・温度管理 ・冷暖房、換気、及び空調（HVAC） ・火災検知及び抑制システム ・電力管理システム 文献[01]では、データ センターには、以下の項目を監視するための専用の施設運用センターがあると明示されている。 ・電力システム。発電機、切り替えスイッチ、メインの分電装置、電力管理モジュール、無停電電源装置など、すべての重要な電気コンポーネントを含む。 ・冷暖房、換気、空調（HVAC）システム。データ センター内の空間温度と湿度、空間の与圧、外部の空気の取り込れを管理及び監視します。 また、すべてのデータ センターに火災検知及び抑制システムが存在し、データ センター内の様々な場所に可搬式消火器が設置されています。施設及び環境保護機器について、定期的な保守が行われていると明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者側で管理する機器等（パソコン等端末を含む）において、適切な場所で管理する必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.1 医療情報処理施設の建物に関する要求事項】 【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】 【7.5.3 情報処理装置のセキュリティ】 【7.6.5 第三者が提供するサービスの管理】 【7.6.12 ログの取得及び監査】 【7.6.13 アクセス制御方針】
3.2.2-04				4.カメラによる監視 ① サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 ② 防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。 ③ サービスに供する機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 容量管理: 事前予防的な監視により、Microsoft Azure サービス プラットフォームの主要サブシステムのパフォーマンスを、許容されるサービスのパフォーマンスと可用性に対して確立された境界を基準にして継続的に測定します。しきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにします。システム パフォーマンスおよび容量の使用率については、環境を最適化するために事前に計画を立てます。	適合可能	文献[01]には、バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、及びデータセンター環境への物理アクセスの際の 2 要素認証など、複数の認証とセキュリティプロセスによって、アクセスを適切に制限していることが記載されている。 NDA文献[N01]にて、セキュリティ監視データセンター監視システムは、データセンターのメインの出入り口、データセンターのコロケーションの出入り口、ケージ、施設された キャビネット、通路、出荷及び受け入れエリア、重要な環境、周辺エリア、駐車場などの重要なデータセンターエリアを監視し、監視記録は90日間または現地の法律で定められているとおり保存されていることが確認できた。	要NDA	文献[01]	—		NDA文献[N01]	利用者及びSI事業者側で管理する施設において、適切な監視を行う必要がある。	【7.5.1 医療情報処理施設の建物に関する要求事項】 【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】 【7.5.3 情報処理装置のセキュリティ】 【7.6.5 第三者が提供するサービスの管理】 【7.6.12 ログの取得及び監査】 【7.6.13 アクセス制御方針】
3.2.2-05				（イ）個人情報が参照可能な運用端末等に対する物理的安全管理対策としての要求事項 本項は、個人情報が参照可能な運用端末等に対する物理的な安全管理対策を求めるものである。具体的には、覗き見等の防止を内容とする。 1.覗き見等の防止 ① 個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。 ② 運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、適切な端末管理（のぞき見防止対策）を行う必要がある。	-
3.2.2-06				（ウ）個人情報が格納されている機器、媒体に対する物理的安全管理対策としての要求事項 本項は、個人情報が物理的に保存されている機器、媒体の盗難・紛失等を避けるための物理的措置を講じることを求めるものである。 1.機器・媒体等の盗難・紛失防止 ① 個人情報が物理的に保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。 ② 個人情報が存在するPC 等の重要な機器には、盗難防止用チェーンを取り付ける。 ③ 受託する個人情報を運用や保守に用いる端末に保存しない旨、自社の運用管理規程等に定める。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Online Services の機器は、盗難や、火事、煙、水、ほこり、振動、地震、電子的な干渉などの環境的なリスクから保護された環境に配置されています。 ISO 27001 規格（具体的には付属文書 A の項 9.1.4 および 9.2.1）で、"外部および環境による脅威に対する保護、および機器の配置に関する保護" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 文献[01]では、Windows Azure では、Windows Azure サービスの提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Windows Azure 環境の主要なハードウェア資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されると明示されている。	公開資料	文献[01]文献[134]文献[135]	—		—	利用者及びSI事業者は、適切な端末管理（盗難防止対策、端末上への情報保存の禁止策）を行う必要がある。	【7.5.3 情報処理装置のセキュリティ】
3.2.3-01	3.2.3		（1）を踏まえ、クラウドサービス事業者は技術的安全管理対策として、 ・利用者の識別及び認証 ・情報の区分管理とアクセス権限の管理 ・アクセスの記録（アクセスログ） ・不正ソフトウェア対策 ・サービス利用に係る機器等（無線 LAN、IoT 機器）のセキュリティ対策等が求められる。 これに加えて、「e-文書法の対象となる医療情報を含む文書等の作成における真正性の確保」、「ソフトウェア・機器の品質管理」、「応答時間に関する対応」、「医療情報等の保存」に関する要求事項も、技術的安全管理対策に含めている。 厚生労働省ガイドライン第 5 版では「e-文書法の対象となる医療情報を含む文書等の作成における真正性の確保」、「ソフトウェア・機器の品質管理」は、「7.1 真正性の確保について」、「応答時間に関する対応」は「7.2 見読性の確保について」、「医療情報等の保存」は「7.3 保存性の確保について」で対策が示されている。いずれも外部保存を行うための追加的な要件として示されているものであるが、クラウドサービスにおいては、外部保存による対応ができるものが中心であることから、技術的安全管理対策として規定した。 以上を踏まえて、クラウドサービス事業者が医療情報を取り扱うサービスを提供する上で対応すべき内容、医療機関等と合意すべき内容について要求事項として整理する。		（ア） 利用者の識別及び認証に対する要求事項 本項は、利用者認証に関する要求事項について記載する。厚生労働省ガイドライン第 5 版では、医療情報システムの不正な利用（なりすまし）を防止する観点から、利用者を特定・識別するための認証を求めている。認証方法としては、ID 及びパスワードの組み合わせ以外の認証方法を推奨しているが、ID 及びパスワードの組み合わせによる認証による場合にとるべき対策、複数要素認証による場合の対応策等についても示している。これに対応するクラウドサービス事業者に対するの具体的な要求事項を以下に示す。 1.利用者の識別 ① 情報システムの利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者によるIDの共同利用は行わない。ただし当該情報システムが他の情報システムを利用するためのID（non interactive ID）は除く。 ② 利用者のなりすまし等を防止するための認証を行う。 ③ 利用者には、医療機関等においてサービスを利用する者のほか、情報システムの運用若しくは開発に従事する者又は管理者権限を有する者も含める。 ④ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行う。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の適用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュ	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者は、医療情報システムにおけるアカウント管理を適切に行う必要がある。	【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】 【7.6.6 ネットワークセキュリティ管理】 【7.6.10 アプリケーションに対するセキュリティ要求事項】 【7.6.14 作業者アクセス及び作業者ID の管理】 【7.6.15 作業者の責任及び周知】

総務省ガイドラインの評価項目						Microsoft Azure における対応							
評価項目番号	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
						リティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 Microsoft Azureの開発者および、運用担当者はWindows Live IDおよび自己署名付き証明書（SMAP)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ・ターミナル サービス サーバーは、高度な暗号化設定を使用するように構成されています。 ・Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証（RSA、SecurID）が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。 マイクロソフトは、顧客データを含む情報システムへのアクセスおよび使用をログに記録し、またはお客様がログに記録できるようにし、アクセス ID、時刻、許可または拒否された認証、および関連する活動を登録します。	適合可能						
3.2.3-02			2.本人識別のためにパスワードを設定する時のルール ① 本人の識別・認証に、ユーザ ID とパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと情報システムにアクセスできないようにする。 ・初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。 ・パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。 ② パスワード認証に係る以下のルールを実現する措置を講じる。 ・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。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③ パスワードには十分な安全性を満たす有効期間を設定する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。 ④ 認証に際してID及びパスワードにかならない場合でも、上記と同等以上の安全性を確保する。	・パスワードポリシー	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID/ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 ※オンラインサービス条件 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSITT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 11.2.1 および 11.2.3）で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[63]では、複数要素を用いた認証には、パスワード以外に、ユーザーの所持品や生体情報による認証の組み合わせが可能であることが明示されている。 文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 インタビュー等を通じて、パスワード認証失敗時には適切にそのアカウントが無効化されることを確認した。	要NDA	文献[01]文献[63]	―	（マイクロソフト社とのNDAにより開示）	―	利用者及びSI事業者は、承認されていない第三者にパスワードが開示されないようにする責任を負う。 利用者及びSI事業者は、医療情報システムにおけるパスワードを管理し、認証失敗時には、適切な挙動をとるようにシステムを構築・運用する必要がある。 利用者及びSI事業者は、ID及びパスワード以外の認証方式を採用する場合であっても、要求事項に応じた安全性の確保が必要である。	【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】 【7.6.6 ネットワークセキュリティ管理】 【7.6.10 アプリケーションに対するセキュリティ要求事項】 【7.6.14 作業者アクセス及び作業者ID の管理】 【7.6.15 作業者の責任及び周知】
3.2.3-03			3.パスワードの管理 ① 利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理する。 ② サービスを提供する製品等の導入に際しては、初期パスワードを変更するだけでなく、アカウントの棚卸しを行い、不要なものについては削除を行う。 ③ 利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。 ④ パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。 ⑤ パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知したとて、当該パスワードを無効化し、変更できるような対応を講じる。 ⑥ 利用者が設定するパスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、これに基づく運用を行う。 ⑦ 利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。 ⑧ 利用者のパスワードポリシーについて、サービス仕様適合開示書に基づき、医療機関等と合意する。	・パスワードポリシー	利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID/ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 ※オンラインサービス条件 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSITT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 11.2.1 および 11.2.3）で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[127]には、Azure AD Identity Protection チームは、よく使用され、侵害されたパスワードを継続的に調査し、グローバル禁止パスワード リストに含まれるあまりにも一般的と見なされるパスワードをブロックすると明記されている。 文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 文献[01]では、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。 セキュリティ及び運用上の理由により、Microsoft Azure では、マイクロソフトの Microsoft Azure プラットフォーム サービスに対してお客様自身が監査を行うことを許可していないが、お客様は事前に承認を得ることにより、お客様自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。 また、インシデント発生時の体制について、インシデントマネージャーやインシデントエンジニアについて、インシデントの処理方法や管理の役割、責任について、及び法務、経営管理者へのエスカレーションとコミュニケーション計画について明示されている。 また、不正アクセス検知時及び発見時の監視について明示されている。さらに、権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 加えて、セキュリティインシデントの対応報告時のインシデントの特定（システム及びセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。	公開資料	文献[01]文献[127]	ISO/IEC 27001		―	利用者及びSI事業者は、医療情報システムにおけるアカウントとパスワードを適切に管理し、失念および漏えい時の対応を定める必要がある。 利用者及びSI事業者は、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負う。 ※エントロピーは文字列と記号の混沌具合を意味する 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【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】 【7.6.6 ネットワークセキュリティ管理】 【7.6.10 アプリケーションに対するセキュリティ要求事項】 【7.6.14 作業者アクセス及び作業者ID の管理】 【7.6.15 作業者の責任及び周知】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.3-04				4.複数要素認証への対応 ① 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、2要素認証以上の認証強度のある方法による。 ② 利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の ID・パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。 ④ 利用者の認証に際して、何らかの物理的な媒体・身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段・手順を事前に定める。 ⑤ 代替的手段・手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。 ⑥ 代替的手段・手順により、情報システム利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。 ⑦ その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・利用者の認証で採用する認証手段・方式、一時的な利用者の認証方法	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID/ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 ※オンラインサービス条件 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSIT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 11.2.1 および 11.2.3）で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者は、必要に応じて2要素認証などを導入する必要がある。 利用者は、認証情報に採用している物理的な媒体および身体情報等が利用できない場合であっても、業務を停止させないため、その代替手段の設定方法について予め周知する必要がある。 利用者は、SI事業者が提供する認証方式および対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【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】 【7.6.6 ネットワークセキュリティ管理】 【7.6.10 アプリケーションに対するセキュリティ要求事項】 【7.6.14 作業者アクセス及び作業者ID の管理】 【7.6.15 作業者の責任及び開知】
3.2.3-05				(イ) 情報の区分管理とアクセス権限の管理に対する要求事項 本項は、医療情報を取り扱うクラウドサービスにおける情報システム上の利用権限に関する要求事項について示す。厚生労働省ガイドライン第 5 版では、医療情報に対して、医療従事者の資格に応じたアクセス権限の設定を厳格に行えるようにするための対応策等について示している。 クラウドサービス事業者の対応として、受託する情報のほか、医療情報を取り扱うクラウドサービスに係る情報も含めて、情報区分を設定し、それぞれについて適切な権限設定・付与を行うこと等に対応するための要求事項を示す。 1.情報管理区分 ① 医療情報とそれ以外の情報を区分できる措置を講じる。 ② 医療情報については、情報区分に従ってアクセス制御を行えるようにする。 ③ 仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。 ④ 医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等による情報資産の区分の設定、アクセス制御の設定の状況	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、情報資産の区分管理を適切に行いアクセスを制御する必要がある。 利用者及びSI事業者は、医療情報システムにおけるアクセス管理を適切に行う必要がある。 利用者は、SI事業者が提供するアクセス制御方法が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.13 アクセス制御方針】
3.2.3-06				2.権限設定 ① サービスには、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含める。 ② 医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。資料の提供に係る条件等については、サービス仕様適合開示書に基づき、医療機関等と合意する。	・利用者の職種等に応じたアクセス制御の設定の可否及びその仕様、提供の範囲・条件等 ・運用管理規程に基づくアクセス管理状況に関する資料・提供の可否等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management ID管理、認証認可を行うことのできるAzureADの活用でアクセス権限・範囲等のアクセス制御をしていただくことが可能 アクセス権限や範囲についてはAzure Monitorといった機能で実現いただくことも可能 https://azure.microsoft.com/ja-jp/services/monitor/	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 文献[01]では、Microsoft Azure の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。	公開資料	文献[01]	—		—	利用者は、医療情報システムにおけるアクセス管理およびアクセス制御を適切に行う必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）との間で、アクセス制御の設定内容および作業の役割分担を定める必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.13 アクセス制御方針】
3.2.3-07				3.アクセス対象の設定 ①サービスには、受託する医療情報を患者等ごとに管理できる機能を含める。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、医療情報を患者等ごとに管理する機能を含める必要がある。	【7.6.13 アクセス制御方針】
3.2.3-08				(ウ) e-文書法の対象となる医療情報を含む文書等の作成における真正性の確保に対する要求事項 (a) 入力者及び確定者の識別及び認証に関する安全管理対策 I.PC 等の汎用入力端末により記録が作成される場合 ① e-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様	e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、作成者の識別及び認証に関する仕様	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、医療情報システムにおけるアクセス管理およびアクセス制御を適切に行う必要がある。	【7.6.10 アプリケーションに対するセキュリティ要求事項】
3.2.3-09				2.臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 ① e-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・サービスとの連携におけるインタフェースの構築に関する役割分担	e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・提供するサービスに関連する臨床検査システム、医用画像ファイリングシステム等との連携におけるインタフェースの構築に関し、事業者の役割、範囲	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、医療情報システムと特定の装置等との連携におけるインタフェースの構築に関する役割分担を定める必要がある。	【7.6.10 アプリケーションに対するセキュリティ要求事項】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目番号	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.3-10				(b) 記録の確定手順の確立と、作成責任者の識別情報の記録に関する安全管理対策 1.PC 等の汎用入力端末により記録が作成される場合 ①) e-文書法の対象となる医療情報を含む文書等の作成にPC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様 ・入力された内容についての記録確定前における確認の可否等についての仕様 ・記録の確定権限に関する仕様 ・確定した記録の追記・削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様	e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・確定された登録情報（作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に係る仕様 ・入力された内容についての記録確定前における作成責任者による確認の可否等についての仕様 ・確定した記録に関する追記・削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定の機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療情報システムにおける記録の確定手順と作成責任者の識別が可能な機能を構築する必要がある。	-
3.2.3-11				(c) 更新履歴の保存に関する安全管理対策 1.更新履歴比較機能 ① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等 が保存される等、更新前後の内容を照らし合せることができる機能を含める。	e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・一旦確定した診療録等を更新した場合、更新前と更新後に係るデータの保存、若しくは更新履歴等の保存を行うことにより、更新前後の内容を照らし合せられる機能に関する仕様	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データの更新履歴を保存し、更新前と更新後の内容を照らし合わせる機能を備える必要がある。	-
3.2.3-12				2.更新順序識別機能 ① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。	e-文書法の対象となる医療情報を含む文書等の作成を目的とする、PC 等の汎用入力端末を利用するサービスにおける以下の仕様 ・一旦確定した診療録等を更新した場合、更新履歴を保存し、更新の順序性が識別できる機能に関する仕様	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データ更新履歴について、更新の順序性が識別できるように参照できる機能を備える必要がある。	-
3.2.3-13				(d) 代行入力の承認機能に関する安全管理対策 ① 真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能を含める。 ③ 真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作(承認)に関する機能を含める。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、代行操作に関する機能及び運用方法を整備する必要がある。	-
3.2.3-14				(エ) アクセス記録（アクセスログ）に対する要求事項 本項は、医療情報を取り扱うクラウドサービスを提供する情報システムへのアクセス記録に関する要求事項を示す。アクセス記録が、不正な情報システムの利用や情報漏洩が生じた場合の原因究明に必須の記録であることを踏まえ、厚生労働省ガイドライン第 5 版では、その証拠となる記録の正確性に関する対応策等について示している。 この目的を達するのに必要な保存期間やアクセス記録に対する機密性、完全性、可用性の観点から対応すべき要求事項を示す。 1.アクセス記録の取得 ① 情報システムへのアクセスを記録し、一定期間保存する。 ② アクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める。 ③ アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するアクセス記録又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。 ⑤ ④で定める法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。 ⑥ 情報システムの運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。 ⑦ ⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・アクセス記録の取得（有無、対象（時間、データ、利用者等）取得方法）、取得していない場合の代替措置 ・システム管理者・運用者・保守担当者等におけるアクセス管理の状況等の情報開示、運用状況の開示 ・受託した医療情報の法定年限経過後の保存期間・対応・管理方法 ・法定年限が定められていない医療情報の保存期間・対応・管理方法	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[01]では、Windows Azure のセキュリティを高め、イベント ログ、及びプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準（PST、GMT、UTC など）を使用し、可能な場合は、Windows Azure 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Windows Azure サーバの時計がネットワーク タイム プロトコルを通じて同期されると明示されている。 文献[142]では、環境の動作状況を判断するためにAzure Active Directory ポータルの監査アクティビティ レポートが取得できると明示されている。 文献[138]では、Azure AD にデータが保存される期間としてアクティビティ レポートは30日間、セキュリティ シグナルは契約プランによって30日及び90日であることが明示されている。	公開資料	文献[01]文献[138]	–		–	利用者及びSI事業者は、医療情報システム上のログ管理（保存期間）を適切に行い、取得したログは定期的に確認する必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.2.2 情報の分類】 【7.6.6 ネットワークセキュリティ管理】 【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】 【7.6.12 ログの取得及び監査】
3.2.3-15				2.アクセス記録の保全のための要件 ① アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。 ② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。 ③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management インタビューにて回答	適合可能	文献[01]では、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。また、文献[156]では、Azure では、セキュリティ関連イベントに対する信頼性の高い認証済みのログ記録を行い、改ざん対策が組み込まれたこのログ記録から監査証跡を生成することもできると明示されている。 文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていること、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。 文献[142]では、環境の動作状況を判断するためにAzure Active Directory ポータルの監査アクティビティ レポートが取得できると明示されている。 文献[138]では、Azure AD にデータが保存される期間としてアクティビティ レポートは30日間、セキュリティ シグナルは契約プランによって30日及び90日であることが明示されている。	公開資料	文献[01]文献[138]文献[156]	–		–	利用者及びSI事業者は、医療情報システム上のログ管理（保護対策）を適切に行う必要がある。	【7.2.2 情報の分類】 【7.6.6 ネットワークセキュリティ管理】 【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】 【7.6.12 ログの取得及び監査】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.3-16				3.時刻の設定 ①アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure ホストは内部の Microsoft タイム サーバーに同期されています。このサーバーでは、GPS アンテナを使用して、Microsoft が所有する Stratum 1 デバイスから時刻を取得します。 Azure の仮想マシンでは、そのホストに依存して正確な時刻 (ホスト時刻) を VM に渡すことも、VM でタイム サーバーから直接時刻を取得することも、あるいはこれらの両方を組み合わせることもできます。 スタンドアロン ハードウェアでは、Linux OS によって、起動時にホスト ハードウェア クロックのみが読み取られます。その後、クロックは、Linux カーネルの割り込みタイマーを使用して維持されます。この構成では、クロックは時間の経過と共に誤差が生じます。 Azure の新しい Linux ディストリビューションでは、VM で VMICTimeSync プロバイダーを使用できます。このプロバイダーは LIS (Linux Integration Services) に含まれており、ホストからより頻繁にクロック更新についてクエリを実行するためのものです。 Microsoft Azure のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用しています。可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Microsoft Azure サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.10.6) で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure のすべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用し、可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、NTPを通じて同期されることが明示されている。 文献[01]では、Microsoft Azure で使用する時刻同期用サーバが、Microsoft Azure環境全体で正確な時刻を維持するために使用されていることが明示されている。	公開資料	文献[01]	―		―	利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に行う必要がある。	【7.2.2 情報の分類】 【7.6.6 ネットワークセキュリティ管理】 【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】 【7.6.12 ログの取得及び監査】
3.2.3-17				(オ) 端末等に表示される医療情報の漏洩に対する要求事項 本項は、参照権限を有しない者が端末を使って医療情報を閲覧することへの防止策に関する要求事項を内容とする。厚生労働省ガイドライン第 5 版では、主にクリアスクリーン等、医療機関等における利用者の端末の対応策等について示されている。 クラウドサービス事業者における運用等の端末への対応のほか、医療機関等における利用者の端末への適用に関する要求事項を以下に示す。 1.端末表示からの漏洩対策 ① サービスの運用・保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。 ② サービスの運用・保守端末等を設置している区域は監視カメラ等により適切に監視を行う。 ③ 医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断する、あるいは強制ログオフを行うことができるようにする。 ⑤ 医療機関等における利用者端末への④の措置の具体的な適用について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等における利用者端末に対するクリアスクリーン等の対策の責任関係 ・医療機関等における利用者端末に対するセッションの遮断、強制ログオフ機能の有無、対応状況、責任関係	-		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者及びSI事業者は、適切な端末管理（スクリーンロック等）を行う必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.14 作業者アクセス及び作業者ID の管理】 【7.6.15 作業者の責任及び周知】
3.2.3-18				(カ) 情報漏洩対策等に対する要求事項 本項は、情報漏洩対策等に関する要求事項について示す。厚生労働省ガイドライン第 5 版では、情報システム構築時における対応や動作確認における対応、外部からの不正アクセスへの防護措置等について示している。なお動作確認における個人情報の利用については、3．2．6に統合する。 これらを踏まえて、情報漏洩対策等に関する要求事項を以下に示す。 1.ウイルスやマルウェア等への対策 ①情報システムの構築に際しては、ウイルスやマルウェア等の混入が生じないようにするための手順を策定し、これに則って構築する。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新のウイルス対策ソフト等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。 ⑤ 情報システムの脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 PaaS およびプラットフォームとなる Microsoft Azure のデータセンターにおけるウイルスやマルウェア等はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure のウイルス／マルウェア対策、セキュリティパッチ適用については、SOC 2 レポートをご参照ください。 Microsoft Azure ではセキュリティ監視サービスがあり、攻撃を受けた場合やMicrosoft Azure サービスに影響がある場合は、利用者に通知する機能があります。	適合可能	文献[01]では、Microsoft Azure において、専門のサポートグループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメータが監視されることが明示されている。 文献[10]及び文献[155]では、マイクロソフトで採用されている「セキュリティ開発ライフサイクル（SDL）」にて、リリース段階における最終的なセキュリティレビューの実施、リリースするコードのアーカイブ、リリース後のレスポンス計画が明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、ウイルスなどのインシデント発生時に、組織的なプロセス（特定、抑制、根絶、復元、及び教訓の学習）により対応することが明示されている。 文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。	要NDA	文献[01]文献[10]文献[155]	―	（本調査で確認した内容に記載の通り）	―	利用者及びSI事業者は、医療情報システムのウイルスやマルウェア対策を適切に行う必要がある。 利用者及びSI事業者は、医療情報システムが攻撃を受けた際を想定した対応（関係者への周知）を定める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.6 ネットワークセキュリティ管理】 【7.6.7 電子媒体の取扱】 【7.6.8 情報交換に関するセキュリティ】 【7.6.10 アプリケーションに対するセキュリティ要求事項】
3.2.3-19				2.外部からの攻撃等への対策 ① 外部のネットワークと医療情報を格納する機器との接続に際しては、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。 ② 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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③ 侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。 ④ ホスティングの利用時等、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。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[71]では、仮想マシンとして利用可能なファイアウォールやWAFのイメージがマーケットプレースに多数用意されており、これらを組み合わせて用いることで利用者が必要とするファイアウォール機能やWAF機能が容易に利用可能であることが明示されている。	公開資料	文献[01]文献[27]文献[71]文献[130]文献[131]	―		―	利用者及びSI事業者は、要求事項を満たすために最適なネットワーク接続の方式を検討し、構築を行う必要がある。 利用者は、利用者側の施設等における外部ネットワークとの接続点において、適切なセキュリティ対策を実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.6 ネットワークセキュリティ管理】 【7.6.7 電子媒体の取扱】 【7.6.8 情報交換に関するセキュリティ】 【7.6.10 アプリケーションに対するセキュリティ要求事項】
3.2.3-20				(キ) 応答時間に関する要求事項 ① 医療機関等がサービスを利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス提供に際しての利用者側の応答速度等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview また、Azureの基盤からはメトリックが提供されておりAzure利用者はシステムの基盤のパフォーマンスの監視を行うことができます。 https://docs.microsoft.com/ja-jp/azure/azure-monitor/platform/data-platform-metrics	適合可能	応答時間に影響するAzureの可用性に関して、文献[141]では、Microsoft の稼働時間の保証とダウンタイムのクレジット ポリシーが明示されている。 文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。	公開資料	文献[134]文献[135]	―		―	利用者は、検索表示に関するアプリケーション機能（応答時間）を確保する必要がある。	-
3.2.3-21				(ク) 医療情報等の保存に対する要求事項 本項は、医療情報を取り扱うクラウドサービスを提供する情報システム等の保存場所及びバックアップに関する要求事項や内容とする。厚生労働省ガイドライン第 5 版では、外部保存の対象となるデータについて、「7.3 保存性の確保について」において、バックアップ等に関する対応策等を示している。クラウドサービスでは、外部保存は原則としてどのサービスでも生じうることから、本ガイドラインでは一般的な技術的な対応策として規定することとした。情報システムの保存領域管理に関する内容のほか、バックアップのルールや採用すべき手法等に関する要求事項を以下に示す。 1.保存管理 ① 各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。 ② 医療機関等がサービスを利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 情報システムが情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。 ④ ③において、他の事業者が提供するクラウドサービスを利用する場合においても、同様の情報を収集して、対応する。仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。 ⑤ ③により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。 ⑥ サービスに係る委託先に対しても、③の運用管理規程に定める管理方法への対応等を求める。	・サービス利用に際して利用可能な保存可能量/サイズ・利用可能期間、リスク、バックアップ頻度、バックアップ方法等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview なお、マイクロソフトのAzureの運用については下記のとおりです。 データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。 Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格 (具体的には付属文書 A の項 10.5.1) で、"情報のバックアップ" が規定されています。 Microsoft Azure上での構成として、冗長化構成を取る事で、障害が起きた場合において継続利用をする事が可能です。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 Microsoft Azure 及び GFS が ISO27001を取得しているとから、有効なリスク管理態勢を有していると考えられる。 また、Microsoft Azureにおける運用状況については、第三者認証の各種レポートや、文献[03]、文献[06]、文献[07]などの公開資料を利用できることを確認した。 文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 文献[01]では、予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを用意していることが明示されている。	公開資料	文献[01]文献[03]文献[06]文献[07]文献[81]文献[134]文献[135]	ISO/IEC 27001		―	利用者は、医療情報を適切に保存管理し、管理方法に関する教育を従業員に行う、また、運用管理規程等に含める必要がある。 利用者は、各種資源の能力及び使用状況の確認を行い、システムの性能強化や機能強化、組み合わせの再検討等を行う必要がある。 利用者は、SI事業者が提供する利用可能な資源に係る情報が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.7 電子媒体の取扱】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
				等の整備方法一般の記載等を含める。											
3.2.3-22				2.バックアップルール ① 3. 2. 1（2）（ウ）4. ①において実施するリスク分析結果に基づき情報システムのバックアップを取得する。バックアップの取得対象、取得頻度、保存方法（媒体、管理方法等を定め、その内容を運用管理規程等に含める。 ② ①に従い取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改ざん・破壊等がないことを確認する。 ③ 記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの別、容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。 ④ ③の対象となるバックアップの記録媒体につき、使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。 ⑤ ①～④の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。 ⑥ バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・バックアップルール	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureは、利用者がシステムやデータのバックアップを取ることを可能にするサービス（Azure Backup）を提供しています。	適合可能	文献[01]では、Microsoft Azure の環境に向けた、サービス継続性の管理（SCM）の開発及びメンテナンス プロセスが用意されていることが明示されている。また、継続性プログラムを主導するフレームワークを保持していることが明示されている。 文献[01]では、Microsoft Azure のバックアップ 及び冗長性プログラムは、年に 1 度レビューと検証が行われること、障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されることが明示されている。 文献[01]では、Windows Azure にはレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができると明示されている。また、お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任はお客様にあると明示されている。 文献[151]では、Azure Backup の各機能を提供しオンプレミスでは、転送中のデータは、オンプレミスのマシン上で AES256 を使用して暗号化、オンプレミスから Azure へのバックアップでは、Azure 上のデータは、ユーザーがバックアップを設定するときに指定したパスフレーズを使用して暗号化されて保存され、この暗号化パスフレーズまたはキーは、転送されたり Azure に保存されたりすることはないと明示されている。また、Azure VM の場合、データは Storage Service Encryption（SSE）を使用して暗号化されて保存されると明示されている。 また、同文献にてAzure Backup では、Azure クラウドの基盤となる機能と無制限のスケールを使用して、高可用性を実現しると明示されている。	公開資料	文献[01]文献[151]	―		―	利用者及びSI事業者は、医療情報システムのバックアップルールを定め従業員等及び再委託業者に対して教育を行う、また、運用管理規程等に含める必要がある。 利用者及びSI事業者は、医療情報システムのバックアップに対する改ざん等を確認する機能を備える必要がある。 利用者は、Microsoft Azure及びSI事業者のバックアップ対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.7 電子媒体の取扱】
3.2.3-23				3 冗長化措置 ① 情報システム、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。 ② 診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。 ③ ①を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス継続性を保証するための水準・冗長化対策の状況 ・障害時等でも診療等を継続するための代替措置等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureは、利用者が冗長構成を取ることを可能にするサービス（可用性セット、可用性ゾーン、Azure Site Recovery）を提供しています。	適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、及びプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。 文献[01]では、レプリケーション機能を備えており、当該機能を使用することでデータがリカバリ可能であることが明示されている。 文献[06]では、利用者が地理的に分散した第2のストレージアカウントを作成することで、ホット・フェールオーバー機能が利用できることが明示されている。 文献[32]にて、Microsoft Azureストレージサービスの機能として、同一施設内における3回のデータ複製、他リージョンに対するデータ複製など、複数方式のレプリケーションによる持続性と高可用性が維持されていることが確認できた。	公開資料	文献[01]文献[06]文献[32]	―		―	利用者及びSI事業者は、医療情報システムの冗長化措置および利用者及びSI事業者側のネットワークや端末等の冗長性を確保する必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.7 電子媒体の取扱】
3.2.3-24				4.毀損した情報の取扱い ① 情報が毀損した場合、速やかに回復するための措置を講じ、その内容・手順等について、運用管理規程等に含める。 ② ①に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。 ③ ②で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・障害等により毀損した情報に関する責任の範囲、免責条件等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Microsoft Azureでは各装置における障害対応として以下を実施しております。 Azureのストレージは冗長化されており、特定のハードウェアの故障が起こっても問題にならないよう、持続性が担保されています。	適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、及びプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。 また同文献によると、継続性プログラムを主導するフレームワークを保持していることが明示されている。 文献[01]では、Microsoft Azure のバックアップ 及び冗長性プログラムは、年に 1 度レビューと検証が行われること、障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されることが明示されている。 文献[01]では、Microsoft Azure の環境に向けた、サービス継続性の管理（SCM）の開発及びメンテナンス プロセスが用意されていることが明示されている。 文献[06]によると、Microsoft Azure では、顧客データの整合性を確保するため、VMのアーキテクチャ、構成ファイル、ストレージアカウント等を用いた方法でデータ保護を実現していることが明示されている。	公開資料	文献[01]文献[06]	―		―	利用者は、情報の履歴バックアップの取得等、情報が毀損した場合の対応を運用管理規程に定める必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）との間で、医療情報が毀損した場合の役割等を定める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.7 電子媒体の取扱】
3.2.3-25				5.保存データの見読性確保 ① 医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。 ② 受託する医療情報を格納する機器・媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。 Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格（具体的には付属文書 A の項 10.5.1）で、"情報のバックアップ" が規定されています。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。	適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、及びプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。 文献[01]では、Microsoft Azure のバックアップ及び冗長性プログラムは、年に 1 度レビューと検証が行われること、障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されることが明示されている。 文献[01]では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。	公開資料	文献[01]	―		―	利用者にて、医療情報に関する見読性を確保し維持する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.7 電子媒体の取扱】
3.2.3-26				（ケ）ソフトウェア・機器等の品質管理に対する要求事項 本項は、医療情報を取り扱うクラウドサービスを提供する情報システムにおけるソフトウェアの品質管理に関する要求事項を内容とする。厚生労働省ガイドライン第 5 版では、外部保存の対象となる情報について、「7.1 真正性の確保について」において、ソフトウェア・機器等の品質管理に関する対応策等を示している。ソフトウェア、機器の品質管理に関する要求事項を以下に示す。 1.情報システムに関するドキュメント作成 ① 情報システムにおける機器及びソフトウェアの構成図を作成する。 ② 情報システムのネットワーク構成図を作成する。 ③ ①、②で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。 ④ 情報システムを構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。 ⑤ ①～④で策定した資料等を医療機関等の求めに応じて提出することについて、サービス仕様適合開示書に基づき、開示内容、範囲、条件等を医療機関等と合意する。	・システムに関するドキュメントの提供の有無・範囲・条件等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者はAzure上のネットワークのマップを表示する機能やv利用者のAzureサービスの操作に関するアクティビティログを提供する機能を利用可能です。	適合可能	文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。 文献[07]によると、Azure側がセキュリティパッチの提供等でバージョンを更新した場合は、ポータルにて確認可能であることが明示されている。 文献[01]では、Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開資料	文献[01]文献[07]	―		―	利用者及びSI事業者は、医療情報システム全体の機器及びソフトウェアの構成を管理し、文書化する必要がある。 利用者は、Microsoft Azure及びSI事業者の資料提示、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.2 開発施設、試験施設と運用施設の分離】 【7.6.3 悪意のあるコードに対する管理策】 【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】 【7.9 医療情報システムの改造と保守】
3.2.3-27				2.品質管理に関する運用 ① サービスに供する機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。 ② サービスに供する機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。 ③ サービスに係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。 ④ システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残しています。 Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。 Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。 マイクロソフトはお客様に代わり、専門の第三者を選定し外部監査を受け、その結果をお客様に利用可能にすることによって、お客様による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。	適合可能	文献[01]では、Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。 文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 また、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[128]にて、運用及び開発を行う全てのスタッフに対して、セキュリティ及びプライバシーに関する情報提供と、最低1年に1回のセキュリティトレーニングを実施していることが記載されている。 インタビュー等を通じて、運用環境の更新時には、オペレータを対象に操作方法等についての研修を行うことを確認した。	要NDA	文献[01]文献[128]	―	（本調査で確認した内容に記載の通り）	NDA文献[N01]	利用者及びSI事業者は、医療情報システムが係る機器及びソフトウェアの品質管理に関する運用管理規程を整備し、従業員等への教育を実施する必要がある。 利用者及びSI事業者は、医療情報システム全体の機器及びソフトウェアに関する内部監査を定期的に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.2 開発施設、試験施設と運用施設の分離】 【7.6.3 悪意のあるコードに対する管理策】 【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】 【7.9 医療情報システムの改造と保守】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
						の設定を行うべきである。								
3.2.3-28				（コ） 無線 LAN・IoT 機器の利用に対する要求事項 本項は、無線 LAN 及び IoT 機器の利用に対する要求事項を内容とする。無線LANや、IoT 機器の利用については、クラウドサービス事業者が提供した機器等を利用する場合のほか、医療機関等が管理する機器等を利用する場合等、いくつかのケースが挙げられる。クラウドサービス事業者が、これらについてどこまでをサービスや責任の範囲にするのかを明確にすることが重要である。 厚生労働省ガイドライン第 5 版では、医療機関等が無線 LAN や IoT 機器を利用する場合に講じるべき技術的な対策について定めている。 クラウドサービス事業者においては、自社が提供するサービスとの関係や医療機関等との間での責任分界や、（自社が提供するか否かを問わず）サービスに利用される IoT 機器に対して技術的な観点から講じるべき安全対策についての要求事項を以下に示す。 1.医療機関等における無線 LANの利用 ① 医療情報を取り扱うサービスの利用に際して、医療機関等が無線 LAN を利用する場合に必要なセキュリティ対策について、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等が無線 LAN を導入する場合のセキュリティ上の責任関係、情報提供	Azureに関してマイクロソフトと利用者の責任分界点については下記に明記されています。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関の無線LANの管理に関しては、無線LANの管理者が責任を負う必要があります。	対象外	インタビューにて、Azureの構成要素に無線LAN及びIoT機器の使用が無いことを確認したため、本項目は対象外とする。	–	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。	–
3.2.3-29				2.IoT 機器を利用したサービス提供時 ① IoT機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システムへのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。 ③ IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。	・IoT 機器の利用を含むサービスを提供する場合の医療機関等との責任分界	Azureに関してマイクロソフトと利用者の責任分界点については下記に明記されています。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview	対象外	インタビューにて、Azureの構成要素にIoT機器の使用が無いことを確認したため、本項目は対象外とする。	–	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。	–
3.2.4-01	3.2.4		クラウドサービス事業者は、厚生労働省ガイドライン第 5 版における「委託事業者」に当たることから、これを踏まえたクラウドサービス事業者における対応策は、 ・クラウドサービス事業者の従業者等に対する人的安全管理措置 ・再委託事業者における人的安全管理措置 の 2 つの内容に整理できる。この2つに関する要求事項以下にを示す。	（ア） 従業者等に対する守秘義務等に関する対応 1.就業開始時における対応 ① サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。		Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。	適合可能	文献[65]では、「担当者は、顧客データに関する秘密保持義務を負い、かかる義務は当該担当者の任用の終了後も継続する」ことが明記されている。 また、インタビュー等を通じて、すべての従業員が適切な合意書にサインして、Microsoft社の雇用ポリシーを受け入れる必要があることを確認した。 文献[65]では、顧客データにアクセス可能なマイクロソフト担当者には秘密保持義務が適用されることが明示されている。 文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 また、同文献にて、セキュリティの違反、または情報セキュリティポリシーの違反が疑われるMicrosoft Azureサービスのスタッフは、調査プロセスの対象となり、該当する懲戒措置（最も重い場合は雇用終了も含む）が実施されること、セキュリティの違反、または情報セキュリティ ポリシーの違反が疑われる契約業者のスタッフは、正式な調査の対象となり、関連する契約に該当する措置が実施される（契約の終了となる可能性もある）ことが明示されている。 文献[134]では、Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること、下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されることが明示されている。	要NDA	文献[01]文献[65]文献[134]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、自身の管理下にある従業員等について、適切に管理する必要がある。	【7.7 人的安全対策】
3.2.4-02				2.就業時における教育等 ① サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。 ② この教育・訓練は就業開始時及び就業後定期的に行う。		Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 文献[128]にて、運用及び開発を行う全てのスタッフに対して、セキュリティ及びプライバシーに関する情報提供と、最低1年に1回のセキュリティトレーニングを実施していることが記載されている。 文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。 また、インタビュー等を通じて、一般的な防災・防犯訓練は実施していることを確認した。	要NDA	文献[01]文献[128]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、自身の管理下にある従業員等について、適切に管理する必要がある。	【7.7 人的安全対策】
3.2.4-03				3.退職後の守秘義務等 ① サービスの提供に従事する要員が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。 ② サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。 ③ サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記2における教育・訓練に含める。		Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。	適合可能	文献[01]では、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するよう通知されると明示されている。 文献[65]では、「担当者は、顧客データに関する秘密保持義務を負い、かかる義務は当該担当者の任用の終了後も継続する」ことが明記されている。 また、インタビュー等を通じて、すべての従業員が適切な合意書にサインして、Microsoft社の雇用ポリシーを受け入れる必要があることを確認した。	要NDA	文献[01]文献[65]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、自身の管理下にある従業員等について、適切に管理する必要がある。	【7.7 人的安全対策】
3.2.4-04				4.守秘義務違反者への対応措置 ① 上記1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。		Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。	適合可能	文献[01]では、セキュリティの違反、または情報セキュリティポリシーの違反が疑われるMicrosoft Azureサービスのスタッフは、調査プロセスの対象となり、該当する懲戒措置（最も重い場合は雇用終了も含む）が実施されること、セキュリティの違反、または情報セキュリティ ポリシーの違反が疑われる契約業者のスタッフは、正式な調査の対象となり、関連する契約に該当する措置が実施される（契約の終了となる可能性もある）ことが明示されている。 文献[134]では、Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること、下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されることが明示されている。	公開資料	文献[01]文献[134]	–		–	利用者は、医療情報システムを提供する事業者(SI事業者等)に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。	【7.7 人的安全対策】
3.2.4-05				5.従業者等への教育状況・守秘義務等の状況 ① サービスの提供に従事する要員に対する教育・訓練の実施状況や、守秘義務等への対応状況等に関して、サービス仕様適合開示書に基づき、医療機関等と合意する。	・教育・訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供	Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 また、同文献にてセキュリティの違反、または情報セキュリティポリシーの違反が疑われるMicrosoft Azureサービスのスタッフは、調査プロセスの対象となり、該当する懲戒措置（最も重い場合は雇用終了も含む）が実施されること、セキュリティの違反、または情報セキュリティ ポリシーの違反が疑われる契約業者のスタッフは、正式な調査の対象となり、関連する契約に該当する措置が実施される（契約の終了となる可能性もある）ことが明示されている。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられている。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	公開資料	文献[01]文献[134]	–		–	利用者及びSI事業者は、自身の管理下にある従業員等について、適切に管理する必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.7 人的安全対策】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.4-06				（イ） 再委託先に対する人的安全管理措置 1.委託契約に含めるべき事項 ① 情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、当該再委託に係る契約において体制を明確にする。 ② 再委託先には、自社と同等の個人情報保護指針等を遵守させる。 ③ 再委託に係る契約に、委託業務に係る守秘義務を含める。 ④ 再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。 ⑤ 再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは、オンラインサービス部門は外部委託に当たってマイクロソフトとお客様の契約と同等のセキュリティ事項を含む契約によって外部委託を行い、その中には、お客様データの目的外使用の禁止、セキュリティ対策の実施と管理、セキュリティ実施状況の監査と報告あるいはマイクロソフトによる監査の受け入れ、外部委託先による再委託の際の手続と要件、インシデント対応の手順などを含めています。 https://www.microsoft.com/ja-jp/trustcenter/security/designopsecurity	適合可能	文献[01]では、年に１度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。 文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられている。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化すること、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[134]	–		NDA文献[N01]	利用者は、医療情報システム提供事業者（SI事業者等）との間で、守秘に関連した事項や違反した場合のペナルティを含む委託契約を締結し、情報の取り扱いに関する監督を行う必要がある。	【7.6.5 第三者が提供するサービスの管理】
3.2.5-01		3.2.5	厚生労働省ガイドライン第 5 版における規定に対応した要求事項を以下に示す。	（ア） 情報の破棄に関する安全管理対策 1.情報の破棄の保証 ① サービスに供する情報を格納する機器、媒体等を破棄する手順に、不可逆的な破壊・抹消等により元のデータを復元できなくする措置を含める。 ② 情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁・物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。 ③ ①で挟じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・情報の廃棄に関する手順・消去方法等の情報提供・廃棄証明の提供の条件	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスでは契約終了後、一定の期間はお客様管理者がデータにアクセスすることができる状態になります。この期間は、お客様がデータ移行後の確認および万一移行漏れがあった場合の回復手段とするために用意されています。この期間終了後、お客様コンテンツの削除が開始され、お客様によるお客様コンテンツのアクセスや回復は行うことができなくなります。削除処理が完了するとお客様コンテンツは回復不可能な状態となります。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶媒メディアと廃棄管理サービスを使用していること、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用し破壊の記録は保持されることが明示されている。 文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶媒メディアと廃棄管理サービスを使用していること、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用し破壊の記録は保持されることが明示されている。 「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。 文献[65]では、データ処理サービスの提供終了時にユーザーから移転されたすべての個人データ及びこれのコピーを返却するか、または全ての個人データを破棄しその旨を証明することが明示されている。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[01]文献[65]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療に係る電子情報の破棄について、手順等を定める必要がある。 SI事業者は、利用者（ビジネスパートナー）に対して、医療情報システム及びMicrosoft Azureで実施される記憶装置の管理方法及び、契約終了時のデータ削除プロセス等について十分な説明を行う必要がある。	【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】 【7.6.7 電子媒体の取扱】 【7.8 情報の破棄】
3.2.5-02				2.情報破棄手順の文書化 ① 運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、サービス提供上の要否の確認を定期的に行うこと。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・サービス提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置（事前に破棄の基準等を告知する等）。 ② 情報の破棄手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・情報の廃棄に関する手順・消去方法等の情報提供・廃棄証明の提供の条件	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分" が規定されています。 「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。 マイクロソフトのエンタープライズ向けクラウドサービスでは契約終了後、一定の期間はお客様管理者がデータにアクセスすることができる状態になります。この期間は、お客様がデータ移行後の確認および万一移行漏れがあった場合の回復手段とするために用意されています。この期間終了後、お客様コンテンツの削除が開始され、お客様によるお客様コンテンツのアクセスや回復は行うことができなくなります。削除処理が完了するとお客様コンテンツは回復不可能な状態となります。	適合可能	文献[65]では、データ処理サービスの提供終了時にユーザーから移転されたすべての個人データ及びこれのコピーを返却するか、または全ての個人データを破棄しその旨を証明することが明示されている。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[65]	–	（本調査で確認した内容に記載の通り）	–	利用者は、医療に係る電子情報の破棄について、手順等を定める必要がある。 SI事業者は、利用者（ビジネスパートナー）に対して、医療情報システム及びMicrosoft Azureで実施される記憶装置の管理方法及び、契約終了時のデータ削除プロセス等について十分な説明を行う必要がある。	【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】 【7.6.7 電子媒体の取扱】 【7.8 情報の破棄】
3.2.6-01		3.2.6	厚生労働省ガイドライン第 5 版が示すように情報システムの改造と保守に関する安全管理対策においては、6.8 章に示すように ・保守に用いるアカウント管理 ・保守の実施に関する管理（実施記録の管理・監督関係） ・保守等における個人情報の利用制限等が求められる。 これに加えて、本項では、（エ）において、「保守における整合性・継続性確保のための安全管理対策」に関する要求事項も含めている。これは厚生労働省ガイドライン第 5 版では 7.2 章「見読性の確保について」で対策が示され、外部保存を行うための追加的な要件として示されているものである。 以上を踏まえた要求事項を以下に示す。	（ア） 保守に用いるアカウント管理に関する安全管理対策 1.保守用のアカウント ① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で当該情報システムにアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。 ② ①で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[142]では、環境の動作状況を判断するためにAzure Active Directory ポータルの監査アクティビティ レポートが取得できると明示されている。 文献[138]では、Azure AD にデータが保存される期間としてアクティビティ レポートは30日間、セキュリティ シグナルは契約プランによって30日及び90日であることが明示されている。	公開資料	文献[01]文献[138]	–		–	利用者及びSI事業者は、医療情報システムの保守用のアカウント管理を適切に行い、アクセスログを記録する必要がある。	【7.6.7 電子媒体の取扱】 【7.6.14 作業者アクセス及び作業者ID の管理】
3.2.6-02				2.保守用のアカウントの管理 ① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、適用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するよう通知されると明示されている。	公開資料	文献[01]文献[31]	–		–	利用者及びSI事業者は、医療情報システムの保守用のアカウント管理を適切に行う必要がある。	【7.6.7 電子媒体の取扱】 【7.6.14 作業者アクセス及び作業者ID の管理】
3.2.6-03				（イ） 保守実施に関する安全管理対策 1.リモートメンテナンス ① リモートメンテナンス（により保守業務を行う場合の手順を策定するとともに、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。 ②リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。 ③ サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、医療機関等と合意する。	・システムのリモートメンテナンスに関する事項	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview なお、マイクロソフトのAzureの運用については下記のとおりです。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[142]では、環境の動作状況を判断するためにAzure Active Directory ポータルの監査アクティビティ レポートが取得できると明示されている。 文献[138]では、Azure AD にデータが保存される期間としてアクティビティ レポートは30日間、セキュリティ シグナルは契約プランによって30日及び90日であることが明示されている。	公開資料	文献[01]文献[138]	–		–	利用者及びSI事業者は、医療情報システムのリモートメンテナンス手順を策定し、保守作業の記録及びアクセスログを確認する必要がある。 利用者は、Microsoft Azure及びSI事業者の規模類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【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】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける追加安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.6-04				2.ログによる保守結果のレビュー ① 情報システムの保守において実施した操作結果について、操作ログ等により記録し、管理する。 ② 取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureのサービスに対する利用者の行った操作に関してのアクティビティログを提供し、利用者はそれを確認することができます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[142]では、環境の動作状況を判断するためにAzure Active Directory ポータルの監査アクティビティ レポートが取得できると明示されている。 文献[138]では、Azure AD にデータが保存される期間としてアクティビティ レポートは30日間、セキュリティ シグナルは契約プランによって30日及び90日であることが明示されている。	公開資料	文献[01]文献[138]	―		―	利用者及びSI事業者は、医療情報システムの保守作業の記録及びアクセスログを管理する必要がある。 利用者は、医療情報へのアクセスログを確認する必要がある。	【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【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】
3.2.6-05				3.医療機関等内における保守対応 ① 情報システムの保守業務を医療機関等の施設内で行う際の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等施設内でサービス提供に必要な保守業務を行う際の対応等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは、Azureのサービスについて返金保証付きのSLAを提供しています。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者及びSI事業者は、医療機関等の施設内における保守業務について、対応内容を定める必要がある。	【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【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】
3.2.6-06				4.保守業務の実施報告 ① 情報システムの保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② ①における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。 ③ 保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。 ④ ③に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ ④で示された手順について、医療機関等が対応すべき事項がある場合、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑥ 保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure Service HealthはAzureのサービスの正常性やメンテナンス情報を提供します。 https://docs.microsoft.com/ja-jp/azure/service-health/service-health-overview	適合可能	文献[01]では、Windows Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立され、このプロセスには以下のものが含まれていると明示されている。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、及びシナリオの特定 (製品の計画時) ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV (開発)、INT (統合テスト)、STAGE (運用前)、PROD (運用) 環境それぞれに応じた開始/終了条件に基づくテスト、認証、及び変更管理 文献[01]では、Windows Azure プラットフォーム内の基盤となるオペレーティング システム (OS) に対する変更は、運用環境に移る前に、品質、パフォーマンス、他のシステムへの影響、復旧目標、及びセキュリティ機能に関して、少なくともレビューとテストが行われ、変更は、運用環境に展開される前に、様々なテスト環境でテストされ、承認されると明示されている。 文献[147]では、ネットワーク、ハードウェア、または本サービスの保守もしくはアップグレードに関する、ダウンタイム開始の少なくとも 5 日前までに通知を公開するかお客様に通知すると明示されている。	公開資料	文献[01]文献[147]	―		―	利用者及びSI事業者は、保守会社が事前申請提出を義務付け、責任者が承認する必要がある。 利用者及びSI事業者は、保守業務における影響範囲や保守作業手順を、運用管理規程に含める必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【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】 【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【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】
3.2.6-07				(ウ) 保守に用いるデータの取扱いに関する安全管理対策 1.保守で用いるデータ ① 情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ② 情報システムの動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、3．2．4で示す守秘義務が課された委員・委託先等により動作確認を行う旨を含めた手順を定める。 ③ 情報システムの動作確認に際し、受託した個人情報をやむを得ず使用する場合について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・受託した個人情報をやむを得ず保守・動作確認で使用する場合の対応	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management マイクロソフトがお客様のデータをテストに利用することはありません。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 そのため、Microsoftの担当者がテストに本番データを使用することは無いことが確認できた。	公開資料	文献[134]文献[135]	―		―	利用者及びSI事業者は、保守業務において扱うデータや保守作業手順を定める必要がある。 テストデータ・個人情報の使用については、守秘義務が課された利用者及びSI事業者の責任にて実施する必要がある。	【7.6.2 開発施設、試験施設と運用施設の分離】 【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】 【7.6.10 アプリケーションに対するセキュリティ要求事項】
3.2.6-08				2.保守目的での医療情報の持ち出し ① 医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療 機関等又はクラウドサービス事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。 ② ①で定める手順及び情報の提供条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療情報を組織外に持ち出す手順及びこれに関する情報提供の条件	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊される。ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Meda Sanitation に従ってデータ消去または破壊が行われると明示されている。 また、インタビューにて機器を修理し再設置することはなく必ず廃棄するため、持ち出しは廃棄時のみであることが確認できた。	要NDA	文献[01]文献[139]	―	（本調査で確認した内容に記載の通り）	―	利用者は、保守会社が個人情報を含むデータを持ち出す場合には、運用管理規程等を定めさせ、確認および承認を行う必要がある。	【7.6.2 開発施設、試験施設と運用施設の分離】 【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】 【7.6.10 アプリケーションに対するセキュリティ要求事項】
3.2.6-09				(エ) 保守における整合性・継続性確保のための安全管理対策 1.データ項目の標準形式の採用 ① 診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。 ② 厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、サービス仕様適合開示書に基づき、医療機関等と合意する。	・標準形式を採用していない項目の場合のデータ項目の形式、標準形式への変換等への対応	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者は、データの形式の選択・設定を行う必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【7.9 医療情報システムの改造と保守】
3.2.6-10				2.レコード管理方法等 ① 医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を情報システムに備える。 ② ①に示す機能等を備えることが困難な場合の情報システム更新・移行の手順について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・マスターテーブルの変更における レコード管理方法・移行対応への支援	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者は、医療情報に係るマスターテーブルの変更管理を定め、必要な機能を備える必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【7.9 医療情報システムの改造と保守】
3.2.6-11				3.データ形式及び転送プロトコルのバージョン管理と継続性の確保 ① データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。 ② ①の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。 ③ ②は、他の情報システムとのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ データ形式・転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、3．4に示す対策を講じる。	・データ形式の変更等における互換性確保への方針・対応支援措置	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure には AES-256 をはじめとする幅広い種類の暗号化機能が用意されており、利用者は自分のニーズに最適なソリューションを選択できます。 Microsoft Azure は国際的な情報セキュリティ基準である ISO 27001 認証を取得しており、準拠状況の監査を毎年実施しています。その他国際標準などの準拠のため、あるいはセキュリティや暗号化の強化のために、仕様の変更が行われる場合は事前にお客様に案内が行われます。	適合可能	文献[01]では、Windows Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立され、このプロセスには以下のものが含まれていると明示されている。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、及びシナリオの特定 (製品の計画時) ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV (開発)、INT (統合テスト)、STAGE (運用前)、PROD (運用) 環境それぞれに応じた開始/終了条件に基づくテスト、認証、及び変更管理 文献[01]では、Windows Azure プラットフォーム内の基盤となるオペレーティング システム (OS) に対する変更は、運用環境に移る前に、品質、パフォーマンス、他のシステムへの影響、復旧目標、及びセキュリティ機能に関して、少なくともレビューとテストが行われ、変更は、運用環境に展開される前に、様々なテスト環境でテストされ、承認されると明示されている。 文献[147]では、ネットワーク、ハードウェア、または本サービスの保守もしくはアップグレードに関する、ダウンタイム開始の少なくとも 5 日前までに通知を公開するかお客様に通知すると明示されている。 文献[01]では、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。 文献[01]では、Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発及びメンテナンス プロセスが用意されていることが明示されている。	公開資料	文献[01]文献[147]	―		―	利用者にて、医療情報システムで使用するデータ形式及び転送プロトコルについて、バージョン管理と継続性の確保を行う必要がある。 SI事業者は、利用者（ビジネスパートナー）に対して、データ形式や転送プロトコル等の変更による影響等について十分な説明を行う必要がある。 利用者は、Microsoft Azure及びSI事業者が提供する情報が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【7.9 医療情報システムの改造と保守】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける追加安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.6-12				4.サービスに供する機器の劣化対策 ① サービスに供する情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。 ② サービスに供する情報システムについて、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。 ③ サービスに供する情報システムについて、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ④ ③においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・機器・ソフトウェアのバージョンアップ等に伴うサービス提供の一部停止・終了時の対応方針・支援措置	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていること、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。	公開資料	文献[01]	―		―	利用者は、医療機関など利用者側の施設等で管理する機器やソフトウェアの劣化対策を行う必要がある。 SI事業者は、利用者（ビジネスパートナー）に対して、機器やソフトウェア等サポート終了による影響及び対応について十分な説明を行う必要がある。 利用者は、Microsoft Azure及びSI事業者の対応等が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【7.9 医療情報システムの改造と保守】
3.2.6-13				5.サービスに供する情報システムの互換性確保や他の事業者のサービスとの関係 ① 医療情報を取り扱うサービスに供する情報システムに関する機器及びソフトウェア]については、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。 ② 他のクラウドサービス事業者が提供するクラウドサービスを用いて、サービスを提供する場合には、他のクラウドサービス事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他のクラウドサービス事業者のクラウドサービスの停止・変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、「4.サービスに供する機器の劣化対策」②～④に示す対応策を講じる。 ③ 医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他のクラウドサービス事業者のクラウドサービスの変更を行う場合には、①、②を考慮して行う。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者はデータや仮想マシンのディスクを任意のタイミングでAzureからダウンロードすることが可能です。また、重要な機能の削除またはサービスの停止について 12 か月前までに通知することを契約書（オンラインサービス条件）に記載しています。 https://azure.microsoft.com/ja-jp/support/legal/	適合可能	文献[01]では、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。 文献[01]では、Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発及びメンテナンス プロセスが用意されていることが明示されている。	公開資料	文献[01]	―		―	利用者及びSI事業者は、医療情報システムに係る機器及びソフトウェア等の変更によるリスクを検討する必要がある。 他のクラウドサービス事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を講じる必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】 【7.9 医療情報システムの改造と保守】
3.2.6-14				(オ) 保守の体制・再委託に関する安全管理対策 1.保守体制の変更 ① 情報システムの保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・保守体制の変更における報告の有無、範囲等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview また、マイクロソフトは問い合わせ窓口としてAzureサポートを提供しています。 https://azure.microsoft.com/ja-jp/support/options/	適合可能	Azureに関しては文献[143]及び文献[144]、プライバシーに関しては文献[145]及び文献[146]にて問い合わせ窓口が設置されていることを確認した。 委託先に関しては、文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。 NDA文献[N02]にて、サードパーティによるサービス、レポート、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることを確認した。	要NDA	文献[01]文献[02]文献[134]文献[143]文献[144]文献[145]文献[146]	―		NDA文献[N02]	利用者及びSI事業者は、医療情報システムの保守等の体制変更時の対応を定めておく必要がある。 利用者は、Microsoft Azure及びSI事業者の体制変更時の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】
3.2.6-15				2.再委託先の体制 ① 情報システムの保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。 ② ①の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[65]では、マイクロソフトがクラウドサービス提供の一部を外部業者へ再委託している場合、再委託先の業務範囲も含めてマイクロソフトの責任範囲であることを確認した。 文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられている、副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている、このプログラムの目的は、データの取り扱い方法を標準化し強化すること、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。 インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 NDA文献[N02]にて、サードパーティによるサービス、レポート、及び提供記録を定期的に監視・レビューし、監査を定期的に実施していることを確認した。	要NDA	文献[01]文献[02]文献[42]文献[65]文献[134]	―	（マイクロソフト社とのNDAにより開示）	NDA文献[N02]	利用者及びSI事業者は、外部保守事業者が個人情報にアクセスする際は、守秘契約等の秘密保持締結や運用管理規程及び安全管理措置を確認する必要がある。 利用者及びSI事業者は、外部保守事業者を適切に管理し、定期的に確認する必要がある。	【7.6.1 情報処理装置及びソフトウェアの保守】 【7.6.5 第三者が提供するサービスの管理】
3.2.7-01	3.2.7	クラウドサービス事業者への要求事項について、厚生労働省ガイドライン第 5 版が示す内容を踏まえ、 ・運用管理規程等に関する安全管理対策 ・機器・媒体の台帳管理 ・情報機器等の持ち出しにおける漏洩対策に関する安全管理対策 について整理する。クラウドサービス事業者への要求事項を以下に示す。	(ア) 運用管理規程等に関する安全管理対策 1.機器・媒体の持ち出しに関する方針策定 ① サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等を、運用管理規程に定める。 ② ①における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。 ③ ①で定める内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.6 および 10.7.2) で、"機器の安全な処分または再使用とメディアの処分" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスクドライブを交換または修理のために製造元に返却する前に、ディスクドライブは確実に消去または破壊される、ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。	公開資料	文献[01]文献[139]	―		―	利用者及びSI事業者は、情報および機器・媒体の持ち出しに関する対応を適切に実施する必要がある。 利用者は、Microsoft Azure及びSI事業者の規程類が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.5.5 情報処理装置の外部への持ち出しに関する要求事項】 【7.6.8 情報交換に関するセキュリティ】
3.2.7-02				2.サービスに供する記録媒体・記録機器に関する対応 ① サービスに供する記録媒体・記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体・記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器・媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器・媒体等の盗難・紛失（持ち出し時の機器・媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応 ・外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））	・クラウドサービス事業者における運用管理規程に示す情報の社外持ち出しのルール、従業員等における対応	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスクドライブを交換または修理のために製造元に返却する前に、ディスクドライブは確実に消去または破壊される、ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。	公開資料	文献[01]文献[139]	―		―	利用者及びSI事業者は、情報および機器・媒体の持ち出しに関するセキュリティ対策を、運用管理規程に含める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.5.5 情報処理装置の外部への持ち出しに関する要求事項】 【7.6.8 情報交換に関するセキュリティ】

総務省ガイドラインの評価項目						Microsoft Azure における対応							
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
3.2.7-03				3.従業員等及び委託先に対する対応 ① 「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ② 上記の運用管理規程については、再委託先に対しても遵守等を求める。	・クラウドサービス事業者における運用管理規程に示す情報の社外持ち出しのルール、従業員等における対応	Microsoft Azureの運用にかかわる従業員はセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、Microsoft が下請業者に対してMicrosoft のベンダプライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、及び定期的なプライバシー トレーニングの受講を要求すること、また、Microsoft によって管理されている施設や機器で業務を行う下請業者はMicrosoft のプライバシー基準に従うよう契約によって義務付けられていること、その他のすべての下請業者はMicrosoft社と同等のプライバシー基準に従うよう契約によって義務付けられていることが明示されている。 文献[65]では、「担当者は、顧客データに関する秘密保持義務を負い、かかる義務は当該担当者の任用の終了後も継続する」ことが明記されている。 また、インタビュー等を通じて、すべての従業員が適切な合意書にサインして、Microsoft社の雇用ポリシーを受け入れる必要があることを確認した。 文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があると明示されている。 また、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。	要NDA	文献[01]文献[65]文献[134]	―	（本調査で確認した内容に記載の通り）	NDA文献[N01]	利用者及びSI事業者は、情報および機器・媒体の持ち出しに関する教育を従業員に行う必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）や外部保守事業者等との間で、医療情報および機器・媒体の持ち出しに関する事項を含む委託契約を締結する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.5.5 情報処理装置の外部への持ち出しに関する要求事項】 【7.6.8 情報交換に関するセキュリティ】
3.2.7-04				4.医療機関等との合意 ①「2.サービスに供する記録媒体・記録機器に関する対応」、「3.従業員等及び委託先に対する対応」に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。		利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊される。ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 文献[01]では、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。	公開資料	文献[01]文献[139]	ISO/IEC 27001		―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しに関する対応を適切に実施する必要がある。 利用者は、Microsoft Azure及びSI事業者の規模額が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.5.5 情報処理装置の外部への持ち出しに関する要求事項】 【7.6.8 情報交換に関するセキュリティ】
3.2.7-05				(イ) 機器・媒体の台帳管理 ① サービスに関する情報を格納する機器・媒体等については、台帳管理等を行い、定期的に所在確認を行う。		利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management 利用者は、情報の格納先となる Azure サービスを把握する責任があります。 Microsoft Azure プラットフォームにおけるマイクロソフト管理者のアクセスは、特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（オンラインサービス条件）記載されています。	適合可能	文献[01]では、Windows Azure では、Windows Azure サービスの提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実施しています。Windows Azure 環境の主要なハードウェア資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されると明示されている。	公開資料	文献[01]	―		―	利用者及びSI事業者は、情報を格納する機器・媒体を適切に管理し定期的に所在を確認する必要がある。	【7.6.7 電子媒体の取扱】
3.2.7-06				(ウ) 情報機器等の持ち出しにおける漏洩対策に関する安全管理対策 1.起動パスワードの設定 ① サービスに供する機器等については、起動パスワードの設定を行う。 ② 起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。 ③ サービスに関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。		利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。Microsoft Azureの開発者および、運用担当者は2要素認証による不正なアクセスの使用防止、アクセス権限確認を講じています。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 インタビュー等を通じて、自動ログインのためにパスワードが保管してはならないことが規則で定められていることを確認した。 インタビュー等を通じて、起動時パスワードについても適切に設定されていることを確認した。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。 さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 インタビュー等を通じて、ベンダにより付与されたデフォルトパスワードは、適切なパスワードに変更されることを確認した。	要NDA	文献[01]	―	（本調査で確認した内容に記載の通り）	―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しによる情報漏洩対策（アクセス制御）を適切に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.14 作業者アクセス及び作業者 ID の管理】
3.2.7-07				2.機器を持ち出す場合の手順 ① サービスに関する情報を格納する機器・媒体等を持ち出す場合の手順には、機器・媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。		利用者(Microsoft Azureを利用するお客様）のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊される。ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。	公開資料	文献[01]文献[139]	―		―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しによる情報漏洩対策（暗号化）を適切に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.14 作業者アクセス及び作業者 ID の管理】
3.2.7-08				3.持ち出し機器等におけるアプリケーション ① サービスに関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。 ② サービスに関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。		利用者(Microsoft Azureを利用するお客様）はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者はゲストOS、ソフトウェア及びアプリケーションをコントロールし、利用者の機器に対する管理を行う事ができます。またその管理は利用者の責任となります。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[139]では、保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊される。ドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにし、このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われると明示されている。	公開資料	文献[01]文献[139]	―		―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しによる情報漏洩対策を適切に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.14 作業者アクセス及び作業者 ID の管理】
3.2.7-09				4.BYODへの対応 ① サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは禁止する。 ② 利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、医療機関等と合意する。 なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏えい等を防止する観点から、例えば、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。	・医療機関等における利用者が個人所有する機器によりサービス利用する場合の責任分界、必要な対応策に関する情報提供	-	対象外	インタビューにて、BYODの使用が無いことを確認したため、本項目は対象外とする。	―	―	―	（本調査で確認した内容に記載の通り）	―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しによる情報漏洩対策を適切に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.14 作業者アクセス及び作業者 ID の管理】
3.2.7-10				5.公衆無線LAN の利用禁止 ① 業務上、サービスに関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。		-	対象外	インタビューにて、公衆無線LANの使用が無いことを確認したため、本項目は対象外とする。	―	―	―	（本調査で確認した内容に記載の通り）	―	利用者及びSI事業者は、情報を格納する機器・媒体の持ち出しによる情報漏洩対策を適切に実施する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.14 作業者アクセス及び作業者 ID の管理】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.2.8-01		3.2.8	厚生労働省ガイドライン第 5 版が示す内容を踏まえ、 ・BCP 等への対応 ・非常時に実施すべき代替措置と、その復旧方法 ・サイバー攻撃等への対応策 等について、要求事項を以下に示す。	(ア) 障害時における見読性確保に関する安全管理対策 1.障害時の責任分界 ① 障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・障害等が生じた場合の責任分界、稼動を保証するサービスの品質	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure プラットフォームが提供する各サービスの SLA については下記に記載しています。 https://azure.microsoft.com/ja-jp/support/legal/sla/	適合可能	文献[65]、文献[141]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[65]及び文献[141]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	公開資料	文献[65]	―		―	利用者にて、電子媒体に関する見読性の可用性及び責任範囲を定める必要がある。	【7.10.1 要求事項の識別】
3.2.8-02				2.医療機関への情報提供 ① 医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・障害時における見読性確保のための、医療機関等側で講じうる方策に関する情報提供	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure プラットフォームが提供する各サービスの SLA については下記に記載しています。 https://azure.microsoft.com/ja-jp/support/legal/sla/	適合可能	文献[65]、文献[141]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[65]及び文献[141]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	公開資料	文献[65]	―		―	利用者にて、電子媒体に関する見読性に関して対応する必要がある。	【7.10.1 要求事項の識別】
3.2.8-03				3.外部ファイル等の出力 ① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者にて、電子媒体に関する見読性に関して対応する必要がある。	【7.10.1 要求事項の識別】
3.2.8-04				4.遠隔地のバックアップに関する見読性 ① 医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・遠隔地に保存するバックアップデータにつき、その利用方法のための機能、利用に必要な情報の提供、条件等	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者にて、電子媒体に関する見読性に関して対応する必要がある。	【7.10.1 要求事項の識別】
3.2.8-05				5.見読性の確保の支援機能 ① 緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等）をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・緊急時の医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―		―	利用者にて、電子媒体に関する見読性に関して対応する必要がある。	【7.10.1 要求事項の識別】
3.2.8-06				(イ) 災害等の非常時の対応に関する安全管理対策 1.BCP 等の策定 ① サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ② ①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。 ③ ①で策定したBCP及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・BCP 及びコンテンジェンシープランに基づくサービス内容	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure プラットフォーム インフラストラクチャの各層は、障害発生時にも運用を継続できるように設計されています。また、Microsoft Azure のストレージにはレプリケーション機能が備わっており、Microsoft データセンター内で障害が発生した場合に利用者のデータが損失するのを防ぐ仕組みとなっています。 利用者は、データの履歴バックアップを作成すること、データのバックアップを Azure の異なるリージョンのデータセンターに保存すること、Azure プラットフォーム以外に保存すること、仮想マシンの状態のバックアップを作成することなど、追加の手順を実施することが可能です。また、利用者は、Microsoft Azure上構築するシステムを冗長化構成とする事で、障害が起きた場合においても継続利用をする事が可能です。	適合可能	文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。 また同文献には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。 文献[19]では、Microsoft Operations Center(MOC)にて、防災管理も含めて全体の管理を実施していることが明示されている。 NDA文献[N01]にて、情報セキュリティに関する管理者が割り当てられ役割と責任が明確化されていること、災害などに備えた事業継続のためのプロセスが定められていることが確認できた。 文献[01]には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。 文献[01]では、ビジネス継続性の計画として、業界及びマイクロソフトのベストプラクティスに合致するフレームワークが保持されていることを確認した。フレームワークには以下が含まれている。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、及び回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、及び改訂のプロセス	要NDA	文献[01]文献[19]	―		NDA文献[N01]	利用者がMicrosoft Azure上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。 利用者は、扱う情報の資産価値及び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の優先順位に基づいて、BCP及びコンテンジェンシープランを策定する必要がある。 利用者及びSI事業者は、医療情報システムの冗長化展開やフォールトトレランス等の非常時の対応と復旧手順を定める必要がある。 利用者及びSI事業者側のネットワークや端末などの冗長性を確保する必要がある。 利用者は、Microsoft Azure及びSI事業者の非常時の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.14 作業者アクセス及び作業者ID の管理】 【7.10.1 要求事項の識別】 【7.10.2 事業継続計画の立案及びレビュー】
3.2.8-07				2.非常時のサービスの運用 ① 非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。 ③ 非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。 ④ 非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。	・非常時に用いる利用者のアカウント及び非常時用機能の有効化のための措置	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。 また同文献には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。 文献[19]では、Microsoft Operations Center(MOC)にて、防災管理も含めて全体の管理を実施していることが明示されている。 NDA文献[N01]にて、情報セキュリティに関する管理者が割り当てられ役割と責任が明確化されていること、災害などに備えた事業継続のためのプロセスが定められていることが確認できた。 文献[01]には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。	要NDA	文献[01]文献[19]	―		NDA文献[N01]	利用者は、扱う情報の資産価値及び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の優先順位に基づいて、BCP及びコンテンジェンシープランを策定する必要がある。 利用者及びSI事業者は、非常時に際したサービス提供内容を定める必要がある。	【7.6.14 作業者アクセス及び作業者ID の管理】 【7.10.1 要求事項の識別】 【7.10.2 事業継続計画の立案及びレビュー】
3.2.8-08				3.サイバー攻撃等への対応 ① サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。 ② ①の場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。 ③ ①の場合において、医療機関等が行う必要のある所管官庁への連絡・報告のために提供する資料の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関と合意する。 ④ ③で定める、医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の執行が及ぶ場所に設置する。	・サイバー攻撃的等が生じた際に医療機関等が行う必要のある、所管官庁への連絡・報告について、医療機関等への提出資料の範囲、条件等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。また、業務端末も利用者の管理となります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 利用者は、システムを構成する Azure の各サービスに対する稼働状態、操作やイベントのログを保存・確認することができます。 また、利用者はアプリケーション、仮想マシン、ストレージ等を 日本国内の Azure リージョンに配置することができます。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。	適合可能	文献[01]では、Microsoft Azure サービスがISO の計画 (Plan)、実行 (Do)、評価 (Check)、改善 (Act) プロセスを使用して、継続的にリスク管理フレームワークを保守し強化していること、Microsoft Azure ではインシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発していることが明示されている。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策及び態勢が整備されていることが明示されている。インシデント発生時の体制について、インシデントマネージャーやインシデントエンジニアについて、インシデントの処理方法や管理の役割、責任について、及び法務、経営管理者へのエスカレーションとコミュニケーション計画について明示されている。 また、不正アクセス検知時及び発見時の監視について明示されている。さらに、権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 加えて、セキュリティインシデントの対応報告時のインシデントの特定（システム及びセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や模倣、再発防止策について明示されている。 文献[65]では、顧客データへの違法なアクセス、または当該機器または施設への不正アクセスが顧客データの紛失、開示、または改変につながったことについて知った場合、速やかに、(1) セキュリティ インシデントについてお客様に通知し、(2) セキュリティ インシデントを調査して詳細情報をお客様に提供し、(3) セキュリティ インシデントにより生じる影響を緩和しそれにより生じる損害を最小限に抑えるための合理的な手段を講じること、が明示されている。	公開資料	文献[01]文献[65]	ISO/IEC 27001		―	利用者及びSI事業者は、サイバー攻撃の対応手順と関係する報告先を定める必要がある。 医療情報に関しては、利用者が所管官庁への連絡を行う必要がある。 利用者は国内法の執行が及ぶ場所に医療情報システムに係る機器及びデータ等を設置する必要がある。	【7.6.14 作業者アクセス及び作業者ID の管理】 【7.10.1 要求事項の識別】 【7.10.2 事業継続計画の立案及びレビュー】

総務省ガイドラインの評価項目						Microsoft Azure における対応								
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容	ガイドラインに対するMicrosoftの見解	ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける追加安全管理対策の記述内容
3.2.8-09				4.サービス回復後のデータ整合性の確保 ① 非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定・検証方法の確認等）を講じる。		-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムに係るバックアップからの回復等データの整合性を確保する必要がある。 医療情報に関しては、利用者がデータの履歴バックアップの作成、データの保存場所の選定等を行い、データ整合性の確保する必要がある。	【7.6.14 作業者アクセス及び作業者ID の管理】 【7.10.1 要求事項の識別】 【7.10.2 事業継続計画の立案及びレビュー】
3.2.9-01		3.2.9	クラウドサービス事業者への要求事項については、厚生労働省ガイドライン第 5 版の 6.11 章に示す内容に加えて、7.2 章「真正性の確保について」で示されている「通信の相手先が正当であることを認識するための相互認証」を（ア）「ネットワークに関する安全管理対策」に含めて規定する。 以上を踏まえて、クラウドサービス事業者が医療情報を取り扱うクラウドサービスを提供するとて対応すべき内容、医療機関等と合意すべき内容について、要求事項として示す。	（ア） ネットワークに関する安全管理対策 I.ネットワーク経路における全般的な安全管理対策 ①ネットワークに於いて、情報の盗聴、改ざん、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準・手順等の整備、通信の暗号化等）を行う。 ② アクセス先のなりすましやセッション乗っ取り、フィッシング等）抜けクラウドサービスを提供するとて対応すべき内容、医療機関等と合意すべき内容について、要求事項として示す。 ③ 経路の安全性確保のため、IPSec + IKEへの対応や閉域ネットワークへの対応等及びその条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ ネットワーク経路におけるウイルスや不正なメッセージの混入等の改ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ 医療機関等がチャネル・セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・経路の安全性確保のための措置（IPSec + IKE への対応や閉域ネットワークへの対応）、情報提供等（閉域性の範囲等） ・改ざんに対する防止措置（ウイルスや不正なメッセージの混入等への対応措置）、情報提供 ・チャネル・セキュリティの確保のための閉域ネットワークの範囲に関する情報の提供	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理は下記のようにマイクロソフトが実施しています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通じて関係者との共有を進めています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 なお、Azure上で動作するアプリケーションが行う通信と、Azure上に格納するデータの暗号化は利用者アプリケーションによって必要な暗号化を行う必要があります。ここで使用される暗号鍵は利用者管理のものとなります。	適合可能	文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 また、文献[04]では侵入テスト、文献[130]では複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて明示されている。 文献[01]では、利用者端末とMicrosoft Azureサービスの管理システム間の通信はTLSにより暗号化されることが明示されている。 文献[01]では、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[01]では通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されている。 文献[71]では、仮想マシンとして利用可能なファイアウォールやWAFのイメージがマーケットプレースに多数用意されており、これらを組み合わせて用いることで利用者が必要とするファイアウォール機能やWAF機能が容易に利用可能であることが明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[131]には、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。	公開資料	文献[01]文献[04]文献[06]文献[27]文献[71]文献[130]文献[131]	–		–	利用者及びSI事業者は、医療情報システムにおけるネットワークについて、なりすまし等の防止や通信の暗号化、経路の安全確保等適切に、セキュリティ対策を行う必要がある。 利用者及びSI事業者側の施設における外部ネットワークとの接続点において、適切なセキュリティ対策を実施する必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）との間で、ネットワークの安全対策に係る役割の範囲を定める必要がある。 利用者は、Microsoft Azure及びSI事業者の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-02				2.医療機関等からのネットワーク経路の確認 ① 医療機関等からクラウドサービス事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で経路の確認を行う。 ② ①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認証を行う。 ③ ①について、事業者が保守業務を再委託している場合には、事業者と再委託先との接続では、別途なりすましを防止する策を講じる。 ④ 厚生労働省ガイドライン第5版6.11 c)項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等が採用する通信方式認証手段の厚生労働省ガイドラインとの適合性に関する確認	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、および(シナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、Microsoft Azure 上で利用者がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、パブリック ネットワークを介してマイクロソフト データ センターとの間で転送されるデータを暗号化するオプションが提供されると明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[01]では、通信時のデータを暗号化するオプションが提供されること、API の呼び出しなどの重要な通信またはMicrosoft Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われることが明示されている。	公開資料	文献[01]文献[06]	–		–	利用者は医療機関等からクラウドサービス事業者までのネットワーク経路を適切に管理する必要がある。 また、医療情報システム等クラウド事業者が提供するサーバとの認証方式についても管理する必要がある。 利用者及びSI事業者は、医療情報システムにおけるアクセス管理およびアクセス制御を適切に行う必要がある。 利用者は、SI事業者が提供する認証方式および対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-03				3.ネットワーク経路対応に用いる機器 ① ルータ等のネットワーク機器は、ISO15408で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。 ② ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関するクラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等の施設内のルータにより経路設定されている場合のサービス提供上の責任分界・必要な対応措置、条件等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureプラットフォームを構成するソフトウェアおよびハードウェアについては、高いセキュリティを確保できる機能を持ったものであることを確認することが、Microsoft社内規定で決められております。 医療機関等との通信経路や VPN 構成については、利用者側にて設計・構成・運用する必要があります。	適合可能	インタビュー等を通じて、ネットワーク機器の調達にあたっては、セキュリティ要求に対する充足を含めた、信頼性の高い機器が調達されることが確認出来た。 医療機関等の施設内のルータについては、利用者にて対応が必要である。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者側の施設等におけるネットワーク機器を適切に管理し調達する必要がある。 利用者は、医療情報ステム提供事業者（SI事業者等）との間で、VPNの設定に関する役割を定める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-04				4.暗号化対策 ① 送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。 ② サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。 ③ ②のほか、医療機関等がメールの暗号化（S/MIME等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・メール・ファイルに対する暗号化措置への対応の可否、対応可能な暗号化手法、条件等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview なお、利用者が使用する管理クライアント機器と、Azureサービスの管理システム間の通信は全てTLS 1.2 により暗号化されます。	適合可能	文献[01]では、利用者端末とMicrosoft Azureサービスの管理システム間の通信はTLSにより暗号化されることが明示されている。また、文献[01]では、通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されている。 文献[157]及び文献[158]では、TLS 1.2以降の使用推奨に関する取り組みと、ブラウザーのセキュリティ設定にて、[TLS 1.2 の使用]をオンにすることを求める記述を確認した。 文献[07]では、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は、利用者側アプリケーションの責任で暗号化を実施する必要があることが明示されている。また同文献にて、暗号鍵の管理主体は原則利用者となることが明示されている。	公開資料	文献[01]文献[06]文献[07]文献[157]文献[158]	–		–	利用者及びSI事業者は、通信の暗号化対策を行う必要がある 利用者は、SI事業者が提供する暗号化対策が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-05				5.通信経路の暗号化対策 ① オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。 ② SSL-VPNは、原則として使用しない。 ③ サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。 ④ 医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策に関する情報提供を行う。情報提供の範囲、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・ソフトウェア型のIPsec 又はTLS1.2 への対応における医療機関等側に対する、クラウドサービス事業者からの要請事項、責任分界等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 医療機関等との通信暗号化や VPN 構成については、利用者側にて設計・構成・運用する必要があります。 なお、利用者が使用する管理クライアント機器と、Azureサービスの管理システム間の通信は全てTLS 1.2 により暗号化されます。	適合可能	文献[01]では、利用者端末とMicrosoft Azureサービスの管理システム間の通信はTLSにより暗号化されることが明示されている。また、文献[01]では、通信時のデータを暗号化するオプションが提供されること、文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されている。 文献[157]及び文献[158]では、TLS 1.2以降の使用推奨に関する取り組みと、ブラウザーのセキュリティ設定にて、[TLS 1.2 の使用]をオンにすることを求める記述を確認した。 文献[07]では、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は、利用者側アプリケーションの責任で暗号化を実施する必要があることが明示されている。また同文献にて、暗号鍵の管理主体は原則利用者となることが明示されている。	公開資料	文献[01]文献[06]文献[07]文献[157]文献[158]	–		–	利用者及びSI事業者は、医療情報システムにおけるネットワークについて、TLSの設定や通信の暗号化、経路の安全確保等、適切にセキュリティ対策を行う必要がある。 利用者は、Microsoft Azure及びSI事業者の対策が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-06				6.回線の品質等 ① 回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービスを提供する際に用いる回線の管理責任、品質等に対する事業者の責任の範囲、役割等	Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。 また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 準拠法は日本となります。 https://azure.microsoft.com/ja-jp/support/legal/	適合可能	文献[65]、文献[141]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[65]及び文献[141]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	公開資料	文献[65]	–		–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、サービスの利用可否を決定する必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）との間で、医療情報システムにおけるネットワークの責任範囲等を定める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.9-07				7.医療機関等の外部からのサービス利用 ① 医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するためのクラウドサービス事業者の役割分担等につき、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス利用に際して医療機関等の利用者が利用する仮想デスクトップ等におけるクラウドサービス事業者の役割・責任分界等	-	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システム提供事業者（SI事業者等）との間で、医療機関等の利用者側で管理するPC（作業環境）に対するサービス及び責任範囲等を定める必要がある。	【7.5.3 情報処理装置のセキュリティ】 【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.6 ネットワークセキュリティ管理】 【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.9-08				(イ) 保守における通信上の安全管理対策 ① リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理は下記のようにマイクロソフトが行います。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証 (RSA、SecurID) が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます (正規の ID バッジをカード リーダーに通します)。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されます。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。 文献[01]では、Microsoft Azure のすべてのスタッフおよびGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するよう通知されると明示されている。	公開資料	文献[01]文献[31]	–		–	利用者及びSI事業者は、医療情報システムにおける保守作業の環境に関して、ネットワーク経路の安全確保やアクセス管理等、適切にセキュリティ対策を行う必要がある。 利用者及びSI事業者は、医療情報システムにおけるアクセス管理を適切に行う必要がある。	–
3.2.9-09				(ウ) 医療機関等との責任分界に関する取り決め 1.通信経路に関する責任分界 ① 通常運用時及び非常時の医療機関等と事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項のIoTで定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等からクラウドサービス事業者に至る通信経路に関する責任分界の考え方、クラウドサービス事業者の責任の範囲、医療機関等における責任の内容 ・医療機関等とクラウドサービス事業者において交換する情報の機密レベル ・医療機関等の管理者において発生する患者等に対する説明責任、管理責任等、各種責任におけるクラウドサービス事業者の対応方針等、対応措置、条件等	Azureプラットフォームの提供品質については、返金保証付のSLAとして規定しています。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性については それぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。 また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 また、サービス契約および使用条件に責任範囲、役割について記載しています。 準拠法は日本となります。 https://azure.microsoft.com/ja-jp/support/legal/	適合可能	文献[65]、文献[141]では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献[65]及び文献[141]では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。 文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と承認しない目的に限定されると明示されている。	公開資料	文献[65]文献[134]文献[135]	–		–	利用者は、医療情報システム提供事業者（SI事業者等）との間で、医療情報システムにおけるネットワークの責任範囲や扱う情報等を定める必要がある。	【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.8 情報交換に関するセキュリティ】
3.2.9-10				2.患者等が閲覧する場合の手続・責任分界 ① サービスにより管理する医療情報を患者等の閲覧に供する場合に、クラウドサービス事業者において対応すべきセキュリティ上の措置の条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・サービス提供上想定されるネットワーク上の脅威に対する責任分界の考え方、クラウドサービス事業者の責任・対応の範囲 ・医療情報を患者（患者の家族等、患者が閲覧を同意した等の者を含む）の閲覧に供する場合のセキュリティ条件、情報提供の範囲等	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性については それぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。 また、利用者向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 また、サービス契約および使用条件に責任範囲、役割について記載しています。 準拠法は日本となります。 https://azure.microsoft.com/ja-jp/support/legal/	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者は、医療情報システムへのアクセスを患者に提供する際は、適切なアクセス管理及び情報管理を行う必要がある。 利用者は、患者への説明を行う主体となる必要がある。	【7.6.3 悪意のあるコードに対する管理策】 【7.6.4 ウェブブラウザを使用する際の要求事項】 【7.6.8 情報交換に関するセキュリティ】
3.2.10-01	3.2.10		厚生労働省ガイドライン第 5 版では、法令で定められた記名・押印を電子署名で行うことについての安全管理対策について ・医療情報の作成において付与する電子署名で用いる電子証明書 ・タイムスタンプの付与 ・タイムスタンプと電子証明書の関係 を規定しており、これに対応する必要がある。 そこで上記の分類に従い、クラウドサービス事業者への要求事項を以下に示す。	(ア) 電子証明書による電子署名 ① 法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合に、保健医療福祉分野PKI 認証局の発行する署名用電子証明書へ対応することの可否を、医療機関等に対して明らかにする。 ② 保健医療福祉分野PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律（平成12 年法律第102 号）」第2 条1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・電子署名法における認定特定認証事業者が発行する電子証明書を用いないで、法令で定められた記名・押印を電子署名で行うサービスを提供する場合の本人確認・検証方法 ・公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合の、公的個人認証サービスに係る電子証明書の検証方法等	–	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。	【7.6.8 情報交換に関するセキュリティ】 【7.6.11 暗号による管理策】
3.2.10-02				(イ) タイムスタンプの付与 ① 電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容・検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・タイムスタンプの付与に関する内容・検証方法等 ・法定保存年限内の期間におけるタイムスタンプの有効性検証の方法等 ・タイムスタンプを付した情報の長期保存における対応措置	–		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。	【7.6.8 情報交換に関するセキュリティ】
3.2.10-03				(ウ) タイムスタンプを付与する時点で有効な電子証明書の使用 ① タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・タイムスタンプを付した場合の電子証明書の執行前の有効性担保にかかる対応等	–		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。	【7.6.11 暗号による管理策】
3.3.6-01	3.3.6		厚生労働省ガイドライン第 5 版が示す対策のうち、契約に盛り込むべき内容（守秘義務違反への対応、各種ガイドライン遵守義務等）については、本ガイドライン3．2．1における契約内容に対する項目で示す。 本項で示すクラウドサービス事業者への要求事項については、 ・医療機関等によるサービス選択のための事業者情報の提供 ・受託医療情報の無断閲覧禁止 ・受託情報の解析及び第三者提供の制限等について整理する。	(ア) 医療機関等によるサービス選択のための事業者情報の提供 ① サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。 ・医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況 ・医療情報等の安全管理に係る実施体制の整備状況 ・実績等に基づく個人データ安全管理に関する信用度 ・財務諸表等に基づく経営の健全性		利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azureプラットフォームのサービス提供品質については、返金保証付のSLAとして規定しています。また、サービス契約および使用条件に責任範囲、役割について記載しています。 準拠法は日本となります。 https://azure.microsoft.com/ja-jp/support/legal/ 下記にて各種情報を提供しています。 ・第三者監査レポート https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide ・財務諸表 https://www.microsoft.com/en-us/investor	適合可能	文献[01]では、セキュリティとプライバシーに関する業界のベストプラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計及び実装されていること、お客様向けバージョンの情報セキュリティポリシーは、要求に応じて入手できると明示されている。 文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。 また、外部認証に関する監査レポートは文献[148]、財務諸表に関しては文献[149]にて明示されている。	公開資料	文献[01]文献[148]文献[149]	ISO/IEC 27001		–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、サービスの利用可否を決定する必要がある。	【7.1.1 ISMS 認証取得時の考慮事項】 【7.3 組織的安全管理策（体制、運用管理規程）】

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.3.6-02				（イ） 受託情報に対する閲覧制限 1.保守・運用における受託情報の閲覧制限 ① 受託した医療情報を保守・運用を行うために閲覧するのは必要最小限とする。 ② ①の閲覧が必要な場合には、緊急時を除き、システム管理者の事前・事後の承認により実施する。 ③ 受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。 ④ ①～③における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また、③により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。	・受託した医療情報の閲覧に係る範囲、手順等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Azure プラットフォームでは、運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（オンラインサービス条件）記載されています。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]文献[134]文献[135]	—	（本調査で確認した内容に記載の通り）	—	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保守作業に必要な範囲を超えた閲覧の禁止に関して確認する必要がある。	—
3.3.6-03				2.受託情報の閲覧制限のための機能 ① 予定された保守・運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。 ② システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。		利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 Azure プラットフォームでは、運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（オンラインサービス条件）記載されています。	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Azure の管理者によって承認されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントは特定のプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。 文献[01]では、通信時のデータを暗号化するオプションが提供されること、API の呼び出しなどの重要な通信は Microsoft Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われることが明示されている。 文献[07]によると、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があること、暗号鍵の管理主体は原則利用者となることが明示されている。	要NDA	文献[01]文献[07]文献[134]文献[135]	—	（本調査で確認した内容に記載の通り）	—	利用者は、情報資産の区分管理を適切に行いアクセスを制御する必要がある。 利用者及びSI事業者は、医療情報システムにおけるアクセス管理を適切に行う必要がある。 利用者は、SI事業者が提供するアクセス制御方法が、医療機関等が求める内容を含むものであることを確認する必要がある。	—
3.3.6-04				（ウ） 受託情報の解析及び第三者提供制限 1.受託情報の解析等の制限等 ① 受託した医療情報の解析・分析は、サービス提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。 ② 受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。		–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		—	利用者は、医療情報に関して第三者提供を含め適切に管理する必要がある。	–
3.3.6-05				2.受託情報の解析等の第三者提供制限 ① 受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。 ② ①の内容を、サービス提供に係る契約に含める。 ③ 医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧・取得できないように、3．2．3及び3．2．9に示す対応策を講じる。 ④ ③により、第三者提供（閲覧）を行う場合には、閲覧・取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更・削除できる対応を行う。 ⑤ 医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。 ⑥ ①～⑤により第三者提供及びその報告を行うための条件、範囲等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・受託情報の第三者提供及びその報告範囲、条件等	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		—	利用者は、医療情報に関して第三者提供を含め適切に管理する必要がある。 利用者は、医療情報システムにおけるアクセス管理およびアクセス制御を適切に行う必要がある。	–
3.3.7-01	3.3.7	個人情報の保護に関する要求事項は、3．2．1ないし3．2．7、及び3．2．9においてそれぞれ示しているが、厚生労働省ガイドライン第 5 版に従い、それらの要求事項に加えて、クラウドサービス事業者に求める事項を以下に示す。	（ア） 診療録等の外部保存委託先の事業者内における個人情報保護 ① 個人情報保護対応策を、サービス仕様適合開示書に基づき、医療機関等と合意する。	・クラウドサービス事業者における個人情報保護対応策	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 品質については、返金保証付のSLAとして規定しています。 指示目的外使用については、お客様コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 準拠法は日本となります。 マイクロソフトは全社で共通となる業務遂行基準（SBC）を定め、公開しており、この中で法令順守を強く表明しています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（オンラインサービス条件）記載されています。	適合可能	インタビュー及び公開文書により、個人情報の取り扱いについて、マイクロソフト社が「分野における個人情報保護に関するガイドラインの安全管理等についての実務指針」の II に定める「個人データ保護に関する委託先選定の基準」の医療機関の評価作業に十分な情報を提供していることを確認した。	要NDA	—	—	（本調査で確認した内容に記載の通り）	—	利用者は、外部保存を受託する事業者の選定基準を定める必要がある。	【7.3 組織的安全管理策（体制、運用管理規程）】
3.3.7-02			イ） 外部保存実施に関する患者への説明 ① 医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		—	利用者は、個人情報の外部保存を行っている旨を患者に説明し理解を得た上で診療を開始する必要がある。	–

総務省ガイドラインの評価項目						ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応	経済産業省ガイドラインにおける当該安全管理対策の記述内容
評価項目項番	章	節	総務省ガイドラインの要求事項	総務省ガイドラインの要求事項2	サービス仕様適合開示書により情報提供される内容		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
3.4.1-01		3.4.1	医療機関等がクラウドサービスの利用による医療情報の外部保存を終了するケースとしては、 ・クラウドサービス事業者側の都合による終了 ・医療機関等側における都合による利用の終了 の 2 つが考えられる。前者の場合には、医療機関等においては、必ずしも利用中のサービスが停止することを予定していないため、委託していた医療情報の利用が不能になるリスクが生じる。そのため、事前の取り決めを十分に行うことが求められる。 いずれの場合にも、クラウドサービス事業者は、 ・受託したデータの返却 ・受託したデータの削除 についての対応策を講じる必要がある。 また、クラウドサービス事業者の都合により、サービス内容の大きな変更が生じる場合も考えられる。 その場合には、クラウドサービス事業者は、医療機関等に対して、十分な告知期間の設定することや、終了等に伴う移行支援等の内容について、予め医療機関等に示し、医療情報の利用の停止を防止するための対応策を講じることが求められる。クラウドサービス事業者への要求事項を以下に示す。	① サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、サービスを利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。 ② ①の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式）、返却方法、条件については、サービス仕様適合開示書に基づき、医療機関等と合意する。また医療機関等のサービス利用開始後に、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。 ③ ②におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機関等と合意する。なお、返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合の対応策を講じる。 ④ ①において、サービスの変更を含むサービスの一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、②の対応は除く）、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ 医療機関等の都合により医療機関等のサービス利用が終了する場合も、②、③ に示す対応策を講じる。 ⑥ サービス提供の停止又は医療機関等におけるサービス利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。 ⑦ ⑥に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑧ ①～⑦についての手順等を、運用管理規程等に含める。	・サービス提供終了時の医療機関等へのデータ返却におけるデータの範囲（データ種類、期間等）、データ形式（データ項目、項目の詳細、ファイル形式）、返却方法、条件 ・返却するデータに、クラウドサービス事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合の対応 ・サービス提供終了時における医療機関等へのデータ返却以外の対応内容（移行支援等）、条件等 ・サービス終了後にクラウドサービス事業者が管理する情報の範囲等	利用者(Microsoft Azureを利用するお客様)のデータは利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management Microsoft Azureのデータセンターにおける安全管理については下記のとおりです。 契約書（オンラインサービス条件）にて、マイクロソフトは利用者クラウドサービスの利用を停止したときやサブスクリプションが失効したときの具体的なプロセスを契約上確約しています。これには、利用者データをマイクロソフト管理下のシステムから削除することも含まれます。 また、保管用のディスク ドライブにハードウェア障害が発生した場合は、マイクロソフトがそのディスク ドライブを交換または修理のために製造元に返却する前に内容が消去されるか破壊され、ドライブ上のデータは完全に上書きされるので、そのデータはどのような手段でも回復できなくなると明示されている。 文献(65)では、サービスまたは機能の廃止に関して、セキュリティ、法令またはシステム パフォーマンスに関する要因によって迅速な削除が必要となる場合を除き、マイクロソフトはお客様に対し、重要な機能の削除またはサービスの停止について 12 か月前までに通知すると明示されている。	適合可能	文献(150)では、サービス利用終了時のお客様のデータに関して、お客様がクラウド サブスクリプションを終了したときやサブスクリプションが失効した場合は（無料試用を除く）、お客様がデータを抽出するかサブスクリプションを更新するための時間を確保するために、Microsoft はお客様の顧客データを機能限定アカウントに 90 日間（「保持期間」）保管し、この 90 日間の保持期間が終了すると、Microsoft はアカウントを無効化して顧客データを削除すると明示されている。 また、同文献にて保管用のディスクドライブにハードウェア障害が発生した場合は、Microsoft がそのディスクドライブを交換または修理のために製造元に返却する前に内容が消去されるか破壊され、ドライブ上のデータは完全に上書きされるので、そのデータはどのような手段でも回復できなくなると明示されている。 文献(65)では、サービスまたは機能の廃止に関して、セキュリティ、法令またはシステム パフォーマンスに関する要因によって迅速な削除が必要となる場合を除き、マイクロソフトはお客様に対し、重要な機能の削除またはサービスの停止について 12 か月前までに通知すると明示されている。	公開資料	文献(65)文献(150)	—		—	利用者及びSI事業者は、他のクラウドサービス事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を講じる必要がある。 利用者及びSI事業者は、サービスを停止時の告知や情報の取り扱い等の対応について定める必要がある。 利用者は、Microsoft Azure及びSI事業者のサービス停止・変更に関する対応が、医療機関等が求める内容を含むものであることを確認する必要がある。 SI事業者は、Microsoft Azureのサービス停止・変更に関する対応が、医療機関等が求める内容を含むものであることを確認する必要がある。	【7.6.7 電子媒体の取扱】
3.5.2-01		3.5.2	3．5．1で示した医療機関に対するオンライン診療におけるセキュリティ情報の要求事項を踏まえ、オンライン診療システムを提供するクラウドサービス事業者の要求事項を以下に示す。	① オンライン診療システムにおいて、医療情報システムとの接続がある場合には、本ガイドラインの「3．2」～「3．4」の要求事項を、オンライン診療システムを提供するクラウドサービス事業者にも適用する。 ② 患者側端末で利用するオンライン診療システムの機能には、オンライン診療の実施中に医療情報システムと接続する機能等を含まないこと、及びこれに関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。	・患者側端末において提供されるオンライン診療システムの機能において、医療情報システムへの接続がないこと及びこれに関する情報提供 ・オンライン診療システムを利用する場合の医療機関とオンライン診療システムを提供するクラウドサービス事業者との責任分界	-		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、医療情報システムがオンライン診療システムと接続する場合の機能及び責任範囲等について定める必要がある。 利用者は、医療情報システム提供事業者（SI事業者等）との間で、オンライン診療システムと接続する場合の機能及び責任範囲等を定める必要がある。	-	-

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
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			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。	Microsoft クラウド サービスのセキュリティは、パートナーシップに基づくものであり、お客様と Microsoft が責任を共有するモデルです。 お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、および自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持ちます。Microsoft は、セキュリティ制御や、データとアプリケーションを保護するための機能をお客様に提供します。お客様のセキュリティの責任の度合いは、クラウド サービスの種類に応じて決まります。詳細は下記URLもご覧ください。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 準拠法は日本となります。 品質については、返金保証付のSLAとして規定しています。 指示目的外使用については、お客様コンテンツをサービス提供以外の目的で使用しない旨、契約書に記載しています。 監査コンプライアンス マイクロソフトは、顧客データおよび個人データの処理に使用されるコンピューター、コンピューティング環境および物理的なデータ センターのセキュリティの監査を以下のように実施します。 ・標準またはフレームワークにおいて監査の実施が規定されている場合、かかる制御標準またはフレームワークに関する監査は、少なくとも年 1 回実施されるものとします。 ・各監査は、適用される各制御標準またはフレームワークについて、規制機関または認定機関の標準および規則に従って実施されるものとします。 ・各監査は、当社が選択した適格の独立した第三者のセキュリティ監査人によって、当社の費用負担により実施されるものとします。 実施される監査ごとに、監査レポート（以下「マイクロソフト監査レポート」）が作成されます。この監査レポートは、https://servicetrust.microsoft.com/ またはマイクロソフトが指定した場所に提供されます。マイクロソフト監査レポートは、マイクロソフトの秘密情報であり、監査人によって重要な知見が見つかった場合は明確に開示されます。 当社は、マイクロソフト監査レポートで提起された問題を、監査人が満足するように速やかに修正するものとします。 お客様から要求があった場合には、お客様に各マイクロソフト監査レポートを提供します。マイクロソフト監査レポートには、当社および監査人の非開示および頒布に関する制限が適用されます。 お客様がマイクロソフトと標準契約条項を締結した場合、または GDPR 条件が適用される場合、お客様は、オンラインサービス条件に規定するとおり、監査の実行をマイクロソフトに指示することによってその監査権を行使することに同意するものとします。この指示の変更を希望する場合、お客様は、標準契約条項および GDPR 条件に規定するとおり、この指示を変更する権利を有します。変更の要求は書面にて行うものとします。 標準契約条項が適用される場合、標準契約条項の第 5 条 f 項および第 12 条 2 項に本項が追加されます。 オンラインサービス条件のいずれの規定も、標準契約条項または GDPR 条件を変更するものではなく、また、標準契約条項または GDPR に基づく監督当局の権利またはデータ主体の権利に影響を及ぼすものでもありません。Microsoft Corporation は、本条項の第三者受益者です。	適合可能	文献[01]によると、Microsoft Azure のコア サービス（コンピューティング、ストレージ、及び仮想ネットワーク）は ISO/IEC 27001:2005 の認証を取得しており、プラットフォームの残りの機能についてもこの認証の取得が予定されていること、CDN 以外のすべての Microsoft Azure サービスが稼働する GFS の物理インフラストラクチャが、ISO 27001 認証を取得していることが明示されている。 インタビューの結果、クラウドにおける個人情報保護に関する国際標準「ISO/IEC27018:2014」の認証を取得し、指示目的外使用の禁止を行っていることが確認できた。	要NDA	文献[01]	ISO/IEC 27001 ISO/IEC 27018	（本調査で確認した内容に記載の通り）	–	–
2.2.情報資産管理			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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	–
	2.2.1 資産台帳	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	–
		(2)	預託された情報の全てを資産台帳に記録すること。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等を資産台帳により適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等を資産台帳により適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等を資産台帳により適切に管理する必要がある。
	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類に基づいたリスク管理を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類に基づいたリスク管理を適切に実施する必要がある。
		(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、実施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）。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類に基づいたリスク管理を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らがMicrosoft Azure にアップロード・格納したデータ等の分類に基づいたリスク管理を適切に実施する必要がある。
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。	医療情報システム上の医療情報の安全管理に関する方針の策定は、利用者側で対応する必要があります。 Azure インフラストラクチャは、ISO 27001、HIPAA、FedRAMP、SOC 1、SOC 2 など、国際的かつ業界固有の広範なコンプライアンス標準に適合するように設計および管理されています。また、オーストラリアの IRAP、英国の G-Cloud、シンガポールの MTCS など、国に固有の標準にも適合します。British Standards Institute が行うようなサード パーティによる厳正な監査により、これらの基準に定められている厳密なセキュリティ管理要件を満たしていることが証明されています。 実施される監査ごとに、監査レポート（以下「マイクロソフト監査レポート」）が作成されます。この監査レポートは、https://servicetrust.microsoft.com/ またはマイクロソフトが指定した場所に提供されます。マイクロソフト監査レポートは、マイクロソフトの秘密情報であり、監査人によって重要な知見が見つかった場合は明確に開示されます。 当社は、マイクロソフト監査レポートで提起された問題を、監査人が満足するように速やかに修正するものとします。 お客様から要求があった場合には、お客様に各マイクロソフト監査レポートを提供します。マイクロソフト監査レポートには、当社および監査人の非開示および頒布に関する制限が適用されます。	適合可能	文献[01]によると、セキュリティとプライバシーに関する業界のベストプラクティスに対応するため、Microsoft Azure では全体的な ISMS が設計及び実装されていること、お客様向けバージョンの情報セキュリティポリシーは、要求に応じて入手できるようになっていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、Microsoft Azure上に構築する医療情報システムで取り扱う医療情報の安全管理に関する方針を策定する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	Microsoft クラウド サービスのセキュリティは、パートナーシップに基づくものであり、利用者(Microsoft Azureを利用するお客様)と マイクロソフトが責任を共有するモデルです。 お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、および自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持ちます。Microsoft は、セキュリティ制御や、データとアプリケーションを保護するための機能をお客様に提供します。お客様のセキュリティの責任の度合いは、クラウド サービスの種類に応じて決まります。詳細は下記URLもご覧ください。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト の顧客データのプライバシーに対するコミットは、世界初のクラウド プライバシーの国際実施基準である ISO/IEC 27018 の採用で裏付けられています。信頼できる独立第三者監査機関により、適用される Microsoft エンタープライズ クラウド サービスが、パブリック クラウド内の個人識別情報の保護に関する ISO 27018 実施基準に準拠していることが検証されています。この順守によって、マイクロソフト のデータセンター内にお客様が格納した個人情報の返却、転送および削除に関する マイクロソフト のポリシーの透明性も確約されます。 お客様は自身の顧客データの格納場所を把握します 顧客データへのアクセスはお客様が管理します サービスの利用停止時はお客様が顧客データを管理します https://www.microsoft.com/ja-jp/trustcenter/Privacy/You-are-in-control-of-your-data	適合可能	文献[01]によると、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていること、Microsoft Azure 及びGFSの ISO 27001 認定については、マイクロソフトの外部 ISO 監査法人である BSI グループの Web サイトから、その他の監査情報は、新規のお客様の場合は NDA に基づいて請求することにより入手できることが明示されている。	公開資料	文献[01]	ISO/IEC 27001		–	–
		(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。	医療情報システム上の個人情報の保護に関しては、利用者側で対応する必要があります。 Microsoft クラウド サービスのセキュリティは、パートナーシップに基づくものであり、利用者(Microsoft Azureを利用するお客様)と マイクロソフトが責任を共有するモデルです。 お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、および自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持ちます。Microsoft は、セキュリティ制御や、データとアプリケーションを保護するための機能をお客様に提供します。お客様のセキュリティの責任の度合いは、クラウド サービスの種類に応じて決まります。詳細は下記URLもご覧ください。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト の顧客データのプライバシーに対するコミットは、世界初のクラウド プライバシーの国際実施基準である ISO/IEC 27018 の採用で裏付けられています。信頼できる独立第三者監査機関により、適用される Microsoft エンタープライズ クラウド サービスが、パブリック クラウド内の個人識別情報の保護に関する ISO 27018 実施基準に準拠していることが検証されています。この順守によって、マイクロソフト のデータセンター内にお客様が格納した個人情報の返却、転送および削除に関する マイクロソフト のポリシーの透明性も確約されます。 お客様は自身の顧客データの格納場所を把握します 顧客データへのアクセスはお客様が管理します サービスの利用停止時はお客様が顧客データを管理します https://www.microsoft.com/ja-jp/trustcenter/Privacy/You-are-in-control-of-your-data	適合可能	文献[01]によると、個々のお客様による監査を許可する代わりに、独立した監査法人による Microsoft Azure のレポート及び認定がお客様と共有されることが明示されている。 セキュリティ及び運用上の理由により、Microsoft Azure では、マイクロソフトの Microsoft Azure プラットフォーム サービスに対してお客様自身が監査を行うことを許可していないが、お客様は事前に承認を得ることにより、お客様自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。	公開資料	文献[01]	–		–	–
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS)に属するOnline Services Security and Compliance（OSSC)の情報セキュリティ管理システム（ISMS)によりレビュープロセスが確立されています。使用する統制策（ISO27001／27005、SAS70 TypeIおよび II、 SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。 Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 また Azure上に構築されたお客様システムにおける正確かつ安全に運用するマニュアルの整備についてはお客様での管理になります。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 · ガバナンス · 影響の許容範囲 · ビジネスの影響分析 · 依存関係の分析（非技術面および技術面） · 戦略 · 計画 · テスト · トレーニングおよび意識向上 ISO 27001 規格で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 なお、Microsoft Azure には専用のサポートプランがいくつかございます。実際の運用に合わせてご選択ください。 https://azure.microsoft.com/ja-jp/support/options/	適合可能	文献[01]によると、基本的なセキュリティ要件はISMS フレームワーク全体の一部として継続的に確認、向上、実装されることが明示されている。 また、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、標準的な運用手順は少なくとも年に一度見直されること、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。	公開資料	文献[01]	–		–	–
		(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。	災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS)に属するOnline Services Security and Compliance（OSSC)の情報セキュリティ管理システム（ISMS)によりレビュープロセスが確立されています。使用する統制策（ISO27001／27005、SAS70 TypeIおよび II、 SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。 Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 また Azure上に構築されたお客様システムにおける正確かつ安全に運用するマニュアルの整備についてはお客様での管理になります。 マイクロソフト向けのエンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 · ガバナンス · 影響の許容範囲 · ビジネスの影響分析 · 依存関係の分析 (非技術面および技術面) · 戦略 · 計画 · テスト · トレーニングおよび意識向上 ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。 なお、Microsoft Azure には専用のサポートプランがいくつかございます。実際の運用に合わせてご選択ください。 https://azure.microsoft.com/ja-jp/support/options/	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Azure の管理者によって承認されていること、Microsoft Azure のスタッフは全員、情報セキュリティポリシー文書内のすべてのポリシーを確認し、それに従うことに同意した旨を表明すること、Microsoft Azure の契約業者のスタッフは全員、このポリシー内の関連するポリシーに従うことに同意することが明示されている。 文献[06]によると、マイクロソフトが業界標準のアクセス機構を採用して、Microsoft Azure の物理インフラストラクチャとデータ センター施設を保護していることが明示されている。 ISO/IEC 27001の付属文書A6.2.2f 顧客対応におけるセキュリティ」、A6.2.3f 第三者との契約におけるセキュリティ」を遵守している。 文献[06]及び文献[10]では、システム開発・変更について、開発ライフサイクルを通じたセキュリティ対応の取組が明示されている。 文献[01]では、Microsoft Azure サービスがISO の計画 (Plan)、実行 (Do)、評価 (Check)、改善 (Act) プロセスを使用して、継続的にリスク管理フレームワークを保守し強化していること、Microsoft Azure ではインシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発していることが明示されている。 文献[07]によると、障害発生時の対応についてはマイクロソフトとの個別サポート契約（有料） を結ぶことにより、一般利用とは異なるレベルの対応が可能であることが明示されている。 文献[01]によると、格納域内のデータ及び伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあることが明示されている。 文献[01]によると、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。 文献[06]によると、Microsoft Azure には、監視、ログ、レポートの機能が複数のレベルで実装されており、顧客の可視性を高めていることが明示されている。 文献[93]によると、医療機関からの問い合わせ窓口については、専用のサポートプランによって選択可能であることが明示されている。	公開資料	文献[01]文献[06]文献[07]文献[10]文献[93]	ISO/IEC 27001		–	–
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。	医療情報の伝達経路に関するリスク評価に関しては、利用者側で対応する必要があります。 マイクロソフトは外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Azure では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Server and Tools Business (STB) 全体で主導します。 ISO 27001 規格 で、"技術的な脆弱性の管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]によると、Microsoft Azure に関するリスク評価プロセスでは、まずリスクを特定し、続いて発生の可能性及び影響を判定することによってリスク レベルを確立し、最後にリスクの影響を許容可能なレベルまで引き下げる制御及び保護措置を特定すること、手段に応じて、可能な限りリスクを軽減するため推奨事項と制御が用意されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるデータ等の伝送経路のリスク評価を適切に実施する必要がある。
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ことを確認すること。	–	–	–	公開資料	–	–		–	–
		(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。	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、データセンター内の重要なシステムが設置されている部屋は、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。	公開資料	文献[01]	–		–	–

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施錠可能な棚”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターを保護するために、以下を含む環境の管理を実施しています。 · 温度管理 · 冷暖房、換気、および空調 (HVAC) · 火災検知および抑制システム · 電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、“外部および環境による脅威に対する保護” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 ビデオ カメラでは施設周辺や建物の玄関、すべてのサーバー ラックの前方と後方を監視しています。データセンターの各階を退出するときに、再び全身の金属検査によるスクリーニングを通過する必要があります。データセンターを退館するには、詳細なセキュリティ スキャンに合格する必要があります。 https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security	適合可能	NDA文献[N01]にて、建物への不法侵入や破壊行為を防止する為の措置（アクセス管理、警報、監視カメラ、24時間の警備員常駐）が行われていることが確認できた。 インタビューの結果、日本国内では外壁には強度のあるPCコンクリート等で施工されており、破壊行為等への対策が講じられていると考えられる。 インタビューの結果、日本国内では外部に面したガラス部分には容易な破壊を防止する強度のものを採用し、あわせて侵入センサー、もしくは監視カメラ等を設置している。また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階窓部分への接近を防止、もしくは検知する仕組みを採用している。これらの対策により、必要な防犯措置が講じられていると考えられる。	要NDA	文献[01]	—	（本調査で確認した内容に記載の通り）	NDA文献[N01]	—
		(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。	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施錠可能な棚”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターを保護するために、以下を含む環境の管理を実施しています。 · 温度管理 · 冷暖房、換気、および空調 (HVAC) · 火災検知および抑制システム · 電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、“外部および環境による脅威に対する保護” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 アクセスの申請と承認。データセンターに到着する前にアクセスの申請を行う必要があります。コンプライアンスや監査目的など、訪問について有効な業務上の妥当性を提示することが求められます。すべての申請は、Microsoft の社員によって、アクセスの必要性に基づいて承認されます。アクセスの必要性に基づくことで、データセンターでタスクを完了するために必要な個人の数を最小限に保つことができます。Microsoft が入館許可を付与すると、個人は、承認された業務上の妥当性に基づいて、データセンターの必要な個別の領域にのみ入館できます。入館許可は、一定の期間に制限されており、その後失効します。 施設の周辺。データセンターに到着すると、明確に定義されたアクセス ポイントを通過することを求められます。通常は、スチールやコンクリートでできた高いフェンスが、周辺を 1 インチごとに取り囲んでいます。データセンターの周辺にはカメラが設置され、セキュリティ チームがビデオを常時監視しています。 建物の玄関。データセンターの玄関には、厳格な研修と経歴のチェックを受けたプロのセキュリティ担当者が常駐しています。これらのセキュリティ担当者は、データセンターを定期的に巡回し、データセンター内部にあるカメラのビデオも常時監視しています。 建物の内部。建物に入った後、データセンター内で移動を続けるには、生体認証による 2 段階認証に合格する必要があります。ID が検証済みになると、データセンターの入館が承認された部分にのみ入ることができます。承認された時間帯のみ、その場所に滞在できます。 https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security	適合可能	NDA文献[N01]にて、建物への不法侵入や破壊行為を防止する為の措置（アクセス管理、警報、監視カメラ、24時間の警備員常駐）が行われていることが確認できた。 インタビューの結果、日本国内では外壁には強度のあるPCコンクリート等で施工されており、破壊行為等への対策が講じられていると考えられる。 インタビューの結果、日本国内では外部に面したガラス部分には容易な破壊を防止する強度のものを採用し、あわせて侵入センサー、もしくは監視カメラ等を設置している。また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階窓部分への接近を防止、もしくは検知する仕組みを採用している。これらの対策により、必要な防犯措置が講じられていると考えられる。	要NDA	文献[01]	—	（本調査で確認した内容に記載の通り）	NDA文献[N01]	—
		(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。	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施錠可能な棚”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターを保護するために、以下を含む環境の管理を実施しています。 · 温度管理 · 冷暖房、換気、および空調 (HVAC) · 火災検知および抑制システム · 電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、“外部および環境による脅威に対する保護” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	NDA文献[N01]にて、各種災害（窃盗、火災、爆発、煙、水、ちり、振動、地震、有害な化学物質、電気干渉、停電、電気障害、放射線など）に対する考慮がなされていることが確認できた。 ISO 27001の管理策「外部及び環境の脅威からの保護」並びに「装置の設置及び保護」で求められている要件を考慮すると、要求事項は満たしていると考えられる。	要NDA	文献[01]	ISO/IEC 27001		NDA文献[N01]	—
	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 ・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。	Microsoft は、承認されていないユーザーがデータおよびデータセンター リソースへの物理アクセス権を取得するリスクを低減させるために、物理的なセキュリティを階層化する手法を採用しています。Microsoft によって管理されるデータ センターには、何層ものセキュリティ保護が用意されています。具体的には、施設の周辺、建物の周辺、建物の内部、およびデータセンターの各階で、アクセスの承認を行います。物理的なセキュリティのレイヤーを次に示します。 アクセスの申請と承認。データセンターに到着する前にアクセスの申請を行う必要があります。コンプライアンスや監査目的など、訪問について有効な業務上の妥当性を提示することが求められます。すべての申請は、Microsoft の社員によって、アクセスの必要性に基づいて承認されます。アクセスの必要性に基づくことで、データセンターでタスクを完了するために必要な個人の数を最小限に保つことができます。Microsoft が入館許可を付与すると、個人は、承認された業務上の妥当性に基づいて、データセンターの必要な個別の領域にのみ入館できます。入館許可は、一定の期間に制限されており、その後失効します。 施設の周辺。データセンターに到着すると、明確に定義されたアクセス ポイントを通過することを求められます。通常は、スチールやコンクリートでできた高いフェンスが、周辺を 1 インチごとに取り囲んでいます。データセンターの周辺にはカメラが設置され、セキュリティ チームがビデオを常時監視しています。 建物の玄関。データセンターの玄関には、厳格な研修と経歴のチェックを受けたプロのセキュリティ担当者が常駐しています。これらのセキュリティ担当者は、データセンターを定期的に巡回し、データセンター内部にあるカメラのビデオも常時監視しています。 建物の内部。建物に入った後、データセンター内で移動を続けるには、生体認証による 2 段階認証に合格する必要があります。ID が検証済みになると、データセンターの入館が承認された部分にのみ入ることができます。承認された時間帯のみ、その場所に滞在できます。 データセンターの各階。入場が承認された間にのみ許可されます。入館者は、全身の金属検査によるスクリーニングに合格する必要があります。未承認のデータが把握されないままデータセンターを入退館するリスクを低減するために、データセンターの各階には、承認されたデバイスしか持ち込みできません。さらに、ビデオ カメラはすべてのサーバー ラックの前方と後方を監視しています。データセンターの各階を退出するときに、再び全身の金属検査によるスクリーニングを通過する必要があります。 データセンターを退館するには、詳細なセキュリティ スキャンに合格する必要があります。 訪問者は、マイクロソフトの施設を退出する前に、バッジを返却するよう求められます。 https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限すること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。	公開資料	文献[01]	—		—	—

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
			・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。	Microsoft は、承認されていないユーザーがデータおよびデータセンター リソースへの物理アクセス権を取得するリスクを低減させるために、物理的なセキュリティを階層化する手法を採用しています。Microsoft によって管理されるデータ センターには、何層ものセキュリティ保護が用意されています。具体的には、施設の周辺、建物の周辺、建物の内部、およびデータセンターの各階で、アクセスの承認を行います。物理的なセキュリティのレイヤーを次に示します。 アクセスの申請と承認。データセンターに到着する前にアクセスの申請を行う必要があります。コンプライアンスや監査目的など、訪問について有効な業務上の妥当性を提示することが求められます。すべての申請は、Microsoft の社員によって、アクセスの必要性に基づいて承認されます。アクセスの必要性に基づくことで、データセンターでタスクを完了するために必要な個人の数を最小限に保つことができます。Microsoft が入館許可を付与すると、個人は、承認された業務上の妥当性に基づいて、データセンターの必要な個別の領域にのみ入館できます。入館許可は、一定の期間に制限されており、その後失効します。 施設の周辺。データセンターに到着すると、明確に定義されたアクセス ポイントを通過することを求められます。通常は、スチールやコンクリートでできた高いフェンスが、周辺を 1 インチごとに取り囲んでいます。データセンターの周辺にはカメラが設置され、セキュリティ チームがビデオを常時監視しています。 建物の玄関。データセンターの玄関には、厳格な研修と経歴のチェックを受けたプロのセキュリティ担当者が常駐しています。これらのセキュリティ担当者は、データセンターを定期的に巡回し、データセンター内部にあるカメラのビデオも常時監視しています。 建物の内部。建物に入った後、データセンター内で移動を続けるには、生体認証による 2 段階認証に合格する必要があります。ID が検証済みになると、データセンターの入館が承認された部分にのみ入ることができます。承認された時間帯のみ、その場所に滞在できます。 データセンターの各階。入場が承認された階にのみ許可されます。入館者は、全身の金属検査によるスクリーニングに合格する必要があります。未承認のデータが把握されないままデータセンターを入退館するリスクを低減するために、データセンターの各階には、承認されたデバイスしか持ち込みできません。さらに、ビデオ カメラはすべてのサーバー ラックの前方と後方を監視しています。データセンターの各階を退出するときに、再び全身の金属検査によるスクリーニングを通過する必要があります。 データセンターを退館するには、詳細なセキュリティ スキャンに合格する必要があります。 訪問者は、マイクロソフトの施設を退出する前に、バッジを返却するよう求められます。 https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していることが明示されている。	公開資料	文献[01]	–		–	–
			・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）。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データ センターの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]には、マイクロソフトの全ての建物へのアクセスはカードリーダーによって制限されること、データセンターへの入室は生体認証によって制限されること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明記されている。 また同文献には、データセンターに対するアクセスリストは定期的に監査され、その結果として適切な処置が行われることが記載されている。	公開資料	文献[01]	–		–	–
			・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載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。	マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。受付の職員は、ID カードを携帯していない正社員（FTE）や契約業者を積極的に監視する必要があります。職員は常に ID バッジを着用する必要があり、バッジを着用していない人物の身元を確認したり報告を行ったりする必要があります。すべてのゲストは、ゲスト バッジを着用し、権限を与えられたマイクロソフトの従業員によってエスコートされる必要があります。 ISO 27001 規格（具体的には付属文書 A の項 9.1.3）で、"セキュリティが確保されたオフィス、部屋、および施設" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]によると、職員は常に ID バッジを着用する必要があること、すべてのゲストは、ゲスト バッジを着用し、権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。 また、インタビューの結果、日本国内では入退室者を識別・記録する出入管理設備が設置されており、入館には事前申請と顔写真入りの身分証明書が必要であることから、不法侵入を防止する措置が講じられていると考えられる。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	–
			・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。	Microsoft は、承認されていないユーザーがデータおよびデータセンター リソースへの物理アクセス権を取得するリスクを低減させるために、物理的なセキュリティを階層化する手法を採用しています。Microsoft によって管理されるデータ センターには、何層ものセキュリティ保護が用意されています。具体的には、施設の周辺、建物の周辺、建物の内部、およびデータセンターの各階で、アクセスの承認を行います。物理的なセキュリティのレイヤーを次に示します。 アクセスの申請と承認。データセンターに到着する前にアクセスの申請を行う必要があります。コンプライアンスや監査目的など、訪問について有効な業務上の妥当性を提示することが求められます。すべての申請は、Microsoft の社員によって、アクセスの必要性に基づいて承認されます。アクセスの必要性に基づくことで、データセンターでタスクを完了するために必要な個人の数を最小限に保つことができます。Microsoft が入館許可を付与すると、個人は、承認された業務上の妥当性に基づいて、データセンターの必要な個別の領域にのみ入館できます。入館許可は、一定の期間に制限されており、その後失効します。 施設の周辺。データセンターに到着すると、明確に定義されたアクセス ポイントを通過することを求められます。通常は、スチールやコンクリートでできた高いフェンスが、周辺を 1 インチごとに取り囲んでいます。データセンターの周辺にはカメラが設置され、セキュリティ チームがビデオを常時監視しています。 建物の玄関。データセンターの玄関には、厳格な研修と経歴のチェックを受けたプロのセキュリティ担当者が常駐しています。これらのセキュリティ担当者は、データセンターを定期的に巡回し、データセンター内部にあるカメラのビデオも常時監視しています。 建物の内部。建物に入った後、データセンター内で移動を続けるには、生体認証による 2 段階認証に合格する必要があります。ID が検証済みになると、データセンターの入館が承認された部分にのみ入ることができます。承認された時間帯のみ、その場所に滞在できます。 データセンターの各階。入場が承認された階にのみ許可されます。入館者は、全身の金属検査によるスクリーニングに合格する必要があります。未承認のデータが把握されないままデータセンターを入退館するリスクを低減するために、データセンターの各階には、承認されたデバイスしか持ち込みできません。さらに、ビデオ カメラはすべてのサーバー ラックの前方と後方を監視しています。データセンターの各階を退出するときに、再び全身の金属検査によるスクリーニングを通過する必要があります。 データセンターを退館するには、詳細なセキュリティ スキャンに合格する必要があります。 訪問者は、マイクロソフトの施設を退出する前に、バッジを返却するよう求められます。 https://docs.microsoft.com/ja-jp/azure/security/azure-physical-security	適合可能	文献[01]によると、データ センターの受付の職員は、ID カードを携帯していない正社員（FTE）や契約業者を積極的に監視する必要があること、職員は常に ID バッジを着用する必要があり、バッジを着用していない人物の身元を確認したり報告を行ったりする必要があることが明示されている。	公開資料	文献[01]	–		–	–
			・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。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・ マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・ アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・ マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、データ センターの受付職員が、ID カードを携帯していない正社員（FTE）や契約業者を積極的に監視する必要があること、職員は常に ID バッジを着用する必要がありバッジを着用していない人物の身元を確認したり報告を行ったりする必要があること、すべてのゲストは、ゲスト バッジを着用し、権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。	公開資料	文献[01]	–		–	–
			・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。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・ マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・ アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・ マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられること、物理的なアクセス権限では、複数の認証とセキュリティのプロセスを利用すること、データセンター内の様々なドアに取り付けられた物理的な入室管理装置などにより物理的なアクセスを許可された従業員、契約業者、訪問者のみに入室が限定されることが明示されている。	公開資料	文献[01]	–		–	–
			・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。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持ち出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートの発生やデータの暗号化により、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	–

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	情報又は答等の開示レベル	確認した公開文書	第三者認証等から推奨した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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 ・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。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限すること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。	公開資料	文献[01]	—		—	—
			・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。	マシン室およびすべての物理的なセキュリティコントロールは、適切なアクセスコントロールが保証されるように設計され、実施されています。マイクロソフトは国際的に通用する厳密なベストプラクティスに基づいて運用をしており、IOS/IEC27001:2005 認定や SSAE 16/ISAE 3403 SOC 1, AT101 SOC 2 認証を含む国際標準によって自身のみならず、第三者によっても評価しています。証明書や評価レポートは参照いただけます。	適合可能	インタビューの結果、マシン室及びすべての物理的なセキュリティコントロールは、適切なアクセスコントロールが保証されるように設計され、実施されていることが確認できた。	要NDA	—	—	（本調査で確認した内容に記載の通り）	—	—
			・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。	運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。 また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 ISO 27001の管理策「接続時間の制限」で求められている要件を考慮すると、要求事項は満たしていると考えられる。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	ISO/IEC 27001	（本調査で確認した内容に記載の通り）	—	—
			・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。	Microsoft Azureでは特定のラックが特定の利用者のシステムに依存しないように構成されており、原則として特定のラックの問題発生時には利用者のシステムを別のラックに再配置するため、ラック等の物理的なアクセスが利用者のシステムには影響しません。 物理的な問題が利用者のシステムに影響を与える場合には事前にメンテナンスの通知を行います。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/maintenance-and-updates アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 文献[06]では、FCI（ファブリックコントローラー）における一連の資格情報（キーやパスワード）の転送、保持、使用を行うための仕組みがMicrosoft Azure の開発者、管理者、バックアップ サービス/担当者等に機密情報を公開しないように設計されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]文献[06]	—	（本調査で確認した内容に記載の通り）	—	—
			・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。	Microsoft Azureでは特定のラックが特定の利用者のシステムに依存しないように構成されており、原則として特定のラックの問題発生時には利用者のシステムを別のラックに再配置するため、ラック等の物理的なアクセスが利用者のシステムには影響しません。よってシステムを顧客別にラベリングするようなことはなく、外部からの状態では医療情報システムであることを判断することはできません。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビューの結果、日本国内ではコンピュータ室、データ保管室等の名称は表示されていないため、侵入や破壊、機密情報漏洩等の防止措置がとられていると考えられる。	要NDA	—	—	（本調査で確認した内容に記載の通り）	—	—
		(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 ・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。	(1),(2)に記載の通り、安全性が確保されている	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限すること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。	公開資料	文献[01]	—		—	—
	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・維持すること。	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に関しては、利用者側で対応する必要があります。	適合可能	文献[01]によると、Microsoft Azure 環境の主要なハードウェア資産の一覧は保持されていること、資産の一覧を検証するために、定期的な監査が実施されていることが明示されている。	公開資料	文献[01]	—		—	利用者及びSI事業者は、自らの医療情報システムで使用する情報処理装置のリストの作成・維持を適切に行う必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、医療情報システムに用いる装置に必要のないアプリケーション等をインストールしないように権限管理やルールの設定を行う必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、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必要がある。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必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、医療情報が端末上に保存されないように措置を講じる必要がある。
		(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。	データ センターを保護するために、以下を含む環境の管理を実施しています。 - 温度管理 - 冷暖房、換気、および空調（HVAC） - 火災検知および抑制システム - 電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、"外部および環境による脅威に対する保護" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure サービスの機器は、盗難や、火事、煙、水、ほこり、振動、地震、電子的な干渉などの環境的リスクから保護された環境に配置されていることが明示されている。	公開資料	文献[01]	—		—	—
		(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。	社内規定にて情報処理設備の周辺では飲食や喫煙を行うことが禁止されています。 マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビュー等を通じて、Microsoft Azureを含むオンラインサービスを実行している資産付近での飲食及び喫煙が、社内規定により禁止されていることを確認した。	要NDA	—	—	（本調査で確認した内容に記載の通り）	—	—

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	情報又は参考の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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など、装置に悪影響を及ぼさないよう配慮すること。	Microsoft Online Services の機器は、盗難や、火事、煙、水、ほこり、振動、地震、電子的な干渉などの環境的なリスクから保護された環境に配置されています。 ISO 27001 規格（具体的には付属文書 A の項 9.1.4 および 9.2.1）で、"外部および環境による脅威に対する保護、および機器の配置に関する保護" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターを保護するために、以下を含む環境の管理を実施しています。 ・温度管理 ・冷暖房、換気、および空調 (HVAC) ・火災検知および抑制システム ・電力管理システム	適合可能	インタビューの結果、日本国内では建築基準法に規定する不燃材料及び消防法に規定する防炎性能を有するものを使用しており、内装等の防炎対策が講じられていると考えられる。 また、日本国内では内装等は不燃材及び防炎性能を有するものを使用しており、防炎対策が施されていると考えられる。 さらに、日本国内ではコンピュータ室内に什器・備品を常設しておらず、什器・備品に関するリスクは存在しないと考えられる。	要NDA	–	–	(本調査で確認した内容に記載の通り)	–	–
		(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。	ISO 27001 規格（具体的には付属文書 A の項 9.2.4）で、"機器のメンテナンス" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。	公開資料	文献[01]	–		–	–
		(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。	保存用のディスク ドライブにハードウェア障害が発生した場合、マイクロソフト がそのディスク ドライブを交換または修理のために製造元に返却する前に、ディスク ドライブは確実に消去または破壊されますドライブ上のすべてのデータは完全に上書きされ、どのような手段をもってもデータを回復できないようにします。 このようなデバイスが廃棄される場合、NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われます。 https://www.microsoft.com/ja-jp/trustcenter/Privacy/You-are-in-control-of-your-data ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分 " が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて確実あるいは消去を行います。	適合可能	文献[01]では、Microsoft Azureの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 文献[01]では、マイクロソフトがベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していることが明示されている。 また、文献[65]では、記憶装置等のコンポーネントを廃棄する際には、不要となったお客様データを消去し、復元できない状態にすることを確認した。	公開資料	文献[01]文献[65]	–		–	–
		(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。	データ センターを保護するために、以下を含む環境の管理を実施しています。 ・温度管理 ・冷暖房、換気、および空調 (HVAC) ・火災検知および抑制システム ・電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、"外部および環境による脅威に対する保護" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビューの結果、日本国内では建物自体が免震構造であり、ラックへの耐震措置も講じられていることから、コンピュータ機器や什器に対する耐震措置が講じられていると考えられる。 NDA文献[N01]にて、許可されていない物理的なサイトへのアクセス及び盗難、損傷、紛失、及び操作の失敗に対する保護対策が講じられていることが確認できた。	要NDA	文献[01]	–	(本調査で確認した内容に記載の通り)	NDA文献[N01]	–
			・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。	データ センターには、専用の 24 時間年中無休で稼働する無停電電源装置 (UPS) および緊急電源サポート (発電機など) が装備されています。UPS と発電機の両方について定期的な保守が行われています。データ センターでは、緊急時の燃料供給のための調整が行われています。 データ センターには、以下の項目を監視するための専用の施設運用センターがあります。 ・電力システム、発電機、切替スイッチ、メインの分電装置、電力管理モジュール、無停電電源装置など、すべての重要な電気コンポーネントを含む。 ・冷暖房、換気、空調 (HVAC) システム。データ センター内の空間温度と湿度、空間の与圧、外部の空気の取り入れを制御および監視します。 すべてのデータ センターに火災検知および抑制システムが存在します。 また、データ センター内のさまざまな場所に可搬式消火器が設置されています。施設および環境保護機器について、定期的な保守が行われています。 ISO 27001 規格（具体的には付属文書 A の項 9.1.4 および 9.2.2）で、"外部および環境による脅威に対する保護、およびサポート ユーティリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビューの結果、日本国内では空調設備を、全利用時の発熱見合いに対してn+1台以上の構成で設計されており、空調設備の能力に余裕があると考えられる。 文献[01]では、データセンターの空調システムにより、空間温度と湿度、空間の与圧、外部の空気の取り入れを制御及び監視されていることが明示されている。 インタビューの結果、日本国内ではコンピュータ室専用の空調設備を設置しており、的確な温湿度制御が可能であると考えられる。	要NDA	文献[01]	–	(本調査で確認した内容に記載の通り)	–	–
			・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。	ISO 27001 規格（具体的には付属文書 A の項 9）で、"パブリック アクセス、配送、荷物の積み込み領域、および物理的/環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な柵"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビューの結果、日本国内では出入口扉は十分な強度を有した建具とし、施錠付きとしていることから、防犯・防災対策が施されていると考えられる。	要NDA	–	–	(本調査で確認した内容に記載の通り)	–	–
		(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。	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり、正式な確認および更新のプロセスが適用されます。Microsoft Azure の資産に対するアクセス権は、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 ・資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいて付与されます。 ・適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 ・物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 Microsoft Azure では、データ センターの物理的な コントロールを通じて診断ポートおよび構成ポートへの物理的なアクセスを制御します。診断ポートおよび構成ポートへのアクセスは、サービス/資産の所有者と、アクセスを必要としているハードウェア/ソフトウェアのサポート担当者の間の申し合わせによって初めて可能になります。ポート、サービス、およびコンピューターやネットワーク機器にインストールされている同様の機能の中で、ビジネス機能において特に必要とされないものは、無効にされるか削除されます。" ISO 27001 規格（具体的には付属文書 A の項 10.6.1、11.1.1、および 11.4.4）で、"ネットワーク制御とアクセス制御" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。	適合可能	インタビュー等を通じて、起動時パスワードについても適切に設定されていることを確認した。	要NDA	–	–	(本調査で確認した内容に記載の通り)	–	利用者及びSI事業者は、医療情報システムに使用する端末等について、使用するパスワードを適切に管理する必要がある。
		(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。	Microsoft Azureでは各装置における障害対応として以下を実施しております。 ・H/W死活 Azure 側で監視し障害時は別 H/W へ自動切替 ・ネットワーク死活 経路冗長化により自動切替 ・OS死活 Azure 側で監視し障害時は再起動、又は別 H/W へ自動切替 ・プロセス IIS 等 Windows 提供プロセスは Azure 側で監視し障害時は 再起動 お客様アプリケーションで起動する別プロセス（アプリケーション個別プロセス）はお客様側で監視頂きます。	適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、及びプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。	公開資料	文献[01]	–		–	–
		(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	マイクロソフトでは、Microsoft Azure サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威のモデリング (Threat Modeling) によって、サービス実行中の潜在的な脅威、攻撃を受けやすいサービスの箇所儘な側面などの要素をマイクロソフトが特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格で、"開発におけるセキュリティとサポート プロセス" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	Microsoft Azureの運用環境では、ISO 27001の管理策「ネットワークにおける装置の識別」で求められている要件を考慮すると、登録されたネットワークアドレスとの整合性に関する要求事項は満たしていると考えられる。 文献[01]によると、Security Development Lifecycle（セキュリティ開発ライフサイクル）: マイクロソフトでは、Microsoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスの制御や不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができること、不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らせることが明示されている。	公開資料	文献[01]	ISO/IEC 27001		–	利用者及びSI事業者は、医療機関などの施設で使用する端末等の情報処理装置について、ネットワークに不正な装置が接続されないように対策を講じる必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機関又は等の開示レベル	確認した公開文書	第三者認証等から推察した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
	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。	利用終了時には、一定期間の猶予の後、お客様コンテンツは回復不可能な状態に削除されます。また、このことは契約書に記載しています。 また、お客様管理の鍵による暗号化を行い、契約終了時に暗号鍵を無効化することで復号化されたデータの読み出しを防止することができます。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。 マイクロソフトのエンタープライズ向けクラウドサービスで使用する記憶装置は、マイクロソフト データセンター内で厳重な管理下に置かれて運用されています。記憶装置の故障、利用年数の経過などの理由によりセキュリティ管理領域外に記憶装置を移動する場合、記憶装置の状態に合わせて破棄あるいは消去を行います。 クラウドサービス上では膨大な数の記憶装置（ハードディスク等）を使用しており、記憶装置の故障や耐用年数期限による交換は定常的に生じるため、個々の記憶装置の故障・交換に際してお客様に通知することはありません。 これらのプロセスは第三者監査の対象となっており、もし異常があった場合にはその解決策とともに第三者監査報告書に記載されますので、お客様による検証が可能です。 マイクロソフトのエンタープライズ向けクラウドサービスでは契約終了後、一定の期間はお客様管理者がデータにアクセスすることができる状態になります。この期間は、お客様がデータ移行後の確認および万一移行漏れがあった場合の回復手段とするために用意されています。この期間終了後、お客様コンテンツの削除が開始され、お客様によるお客様コンテンツのアクセスや回復は行うことができなくなります。削除処理が完了するとお客様コンテンツは回復不可能な状態となります。	適合可能	文献[65]では、データ返却、消去等の対応が規定・明記されていること、記憶装置等のコンポーネントを廃棄する際には、不要となったお客様データを消去し、復元できない状態にすることを確認した。 文献[66]によると、Microsoft Azureで使用する記憶装置はマイクロソフト データセンター内で厳重な管理下に置かれて運用されていること、役割を終えたシステムについては、マイクロソフトの運用担当者が厳格なデータ処理手順とハードウェア廃棄手順に従って処理することが明示されている。 またインタビュー等で確認したところ、記憶装置上の物理的消去及び論理的消去状況については、第三者監査報告書により検証が可能であることが確認できた。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[06],文献[65]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにて使用する端末を一時的に外部からレンタルして調達するような場合は、利用者及びSI事業者は、確実な方法でデータを消去する必要がある。
		(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。	BIOSの堅牢化を含む、お客様のご利用になられる環境に対してのプラットフォームの堅牢化とセキュリティ対策を施しています。	適合可能	インタビュー等を通じて、BIOSの堅牢化を含むセキュリティ対策が施されていることを確認した。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	–
		(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。	Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]によると、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていること、このプロセスには「全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー、DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、及び変更管理」が含まれることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムで使用する端末でリムーバブルハードディスクを利用する場合、利用者及びSI事業者は、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必要がある。
		(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。	保管用のディスクドライブにハードウェア障害が発生した場合は、マイクロソフトがそのディスクドライブを交換または修理のために製造元に返却する前に内容が消去されるか破壊されます。ドライブ上のデータは完全に上書きされるので、そのデータはどのような手段でも回復できなくなります。 このようなデバイスが廃棄されるときは、米国の NIST 800-88 Guidelines for Media Sanitation に従ってデータ消去または破壊が行われます。 https://www.microsoft.com/ja-jp/trustcenter/privacy/data-management	適合可能	文献[65]では、データ返却、消去等の対応が規定・明記されていること、記憶装置等のコンポーネントを廃棄する際には、不要となったお客様データを消去し、復元できない状態にすることを確認した。 文献[66]によると、Microsoft Azureで使用する記憶装置はマイクロソフト データセンター内で厳重な管理下に置かれて運用されていること、役割を終えたシステムについては、マイクロソフトの運用担当者が厳格なデータ処理手順とハードウェア廃棄手順に従って処理することが明示されている。 またインタビュー等で確認したところ、記憶装置上の物理的消去及び論理的消去状況については、第三者監査報告書により検証が可能であることが確認できた。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[06],文献[65]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにて使用する端末を一時的に外部からレンタルして調達するような場合は、利用者及びSI事業者は、確実な方法でデータを消去する必要がある。
	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。	–	–	–	公開資料	–	–		–	–
		(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。	Microsoft Azure利用者はゲストOS、ソフトウェア及びアプリケーションをコントロールし、利用者の機器に対する管理を行う事ができます。またその管理は利用者の責任となります。 データセンターが適切に Azure のセキュリティ要件に対応していることを保証するために、設備の物理的なセキュリティの確認が定期的に実施されます。データセンターのホスティング プロバイダーの担当者は、Azure サービスの管理は行いません。この担当者は、Azure システムにサインインできず、Azure 併置の部屋と区画への物理アクセス権を保有しません。 Microsoft では、NIST 800-88 コンプライアンスのベスト プラクティスの手順とワイプ ソリューションを採用しています。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。 システムの寿命がくると、Microsoft 運用担当者は、データを格納しているハードウェアが信頼できない第三者の手に渡らないよう、厳格なデータ処理およびハードウェア廃棄の手続きを実行します。セキュリティで保護された消去アプローチは、それをサポートしているハード ドライブに使用されます。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。すべての Azure サービスは、承認済みのメディア ストレージと破棄管理サービスを利用します。 Azure インフラストラクチャは、ISO 27001、HIPAA、FedRAMP、SOC 1、SOC 2 など、国際的かつ業界固有の広範なコンプライアンス標準に適合するように設計および管理されています。また、オーストラリアの IRAP、英国の G-Cloud、シンガポールの MTCS など、国に固有の標準にも適合します。British Standards Institute が行うようなサード パーティによる厳正な監査により、これらの基準に定められている厳密なセキュリティ管理要件を満たしていることが証明されています。	適合可能	インタビュー等を通じて、重要な情報処理装置が許可なく持ち出される可能性が極めて低いことを確認した。 また、文献[01]によると、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するように通知されること、契約業者またはサード パーティのインフラストラクチャから、すべての電子メディアを削除する必要があること、データが適切に削除されていることを確認するため、マイクロソフトによって監査が行われる場合があることが明示されている。	要NDA	文献[01]	–	（マイクロソフト社とのNDAにより開示）	–	利用者及びSI事業者は、医療情報システムにて使用する端末の持ち出し・再設置に関する適切な手順を策定する必要がある。
		(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。	Microsoft Azure利用者はゲストOS、ソフトウェア及びアプリケーションをコントロールし、利用者の機器に対する管理を行う事ができます。またその管理は利用者の責任となります。 Microsoft では、NIST 800-88 コンプライアンスのベスト プラクティスの手順とワイプ ソリューションを採用しています。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。 システムの寿命がくると、Microsoft 運用担当者は、データを格納しているハードウェアが信頼できない第三者の手に渡らないよう、厳格なデータ処理およびハードウェア廃棄の手続きを実行します。セキュリティで保護された消去アプローチは、それをサポートしているハード ドライブに使用されます。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。すべての Azure サービスは、承認済みのメディア ストレージと破棄管理サービスを利用します。 Azure インフラストラクチャは、ISO 27001、HIPAA、FedRAMP、SOC 1、SOC 2 など、国際的かつ業界固有の広範なコンプライアンス標準に適合するように設計および管理されています。また、オーストラリアの IRAP、英国の G-Cloud、シンガポールの MTCS など、国に固有の標準にも適合します。British Standards Institute が行うようなサード パーティによる厳正な監査により、これらの基準に定められている厳密なセキュリティ管理要件を満たしていることが証明されています。	適合可能	文献[01]によると、Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスが確立されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにて使用する端末の持ち出し・再設置に関する適切な手順を策定する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残しています。 Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていること、変更が運用環境に展開される前に様々なテスト環境でテストされ承認されることが明示されている。	公開資料	文献[01]	—		—	利用者は、自らの資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を負い、資産保護を規格に応じて分類し、保守する役割を担う。 利用者は、自身のデータの管財人としての責任を負う。 利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残しています。 Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていること、変更が運用環境に展開される前に様々なテスト環境でテストされ承認されることが明示されている。	公開資料	文献[01]	—		—	利用者は、自らの資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を負い、資産保護を規格に応じて分類し、保守する役割を担う。 利用者は、自身のデータの管財人としての責任を負う。 利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。	Microsoft Azure は国際的な情報セキュリティ基準である ISO 27001 認証を取得しており、準拠状況の監査を毎年実施しています。その他国際標準などの準拠のため、あるいはセキュリティや暗号化の強化のために、仕様の変更が行われる場合は事前にお客様に案内が行われます。	適合可能	インタビューを通じて、通信の暗号化については、国際標準への準拠や、暗号化の強化のために仕様の変更が行われること、さらに変更が行われる場合には事前に顧客に通知していることを確認した。	要NDA	—	—	（本調査で確認した内容に記載の通り）	—	利用者及びSI事業者は、医療情報システムで使用する古いデータ形式の互換性について、適切に対応する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview エンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発およびメンテナンス プロセスが用意されています。このプロセスには、Microsoft Azure の資産を回復し、Microsoft Azure の主要なビジネス プロセスを再開するための方法が含まれています。継続性ソリューションによって、サービスの運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されます。お客様は、地理的な冗長性のためにアプリケーションを複数の場所に展開する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 9.2.4）で、"機器のメンテナンス" が規定されています。	適合可能	文献[01]では、ビジネス継続性の計画として、業界及びマイクロソフトのベストプラクティスに合致するフレームワークが保持されていることを確認した。フレームワークには以下が含まれている。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、及び回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、及び改訂のプロセス 文献[01]では、ビジネス継続プログラムオフィスにおいて継続性プログラムを主導するフレームワークを保持していること、データ センターを保護するために温度管理、冷暖房、換気、及び空調（HVAC）、火災検知及び抑制システム、電力管理システム等の環境管理を実施していること、Microsoft Azureサービスの機器が、盗難や、火事、煙、水、ほこり、振動、地震、電子的な干渉などの環境的リスクから保護された環境に配置されていることが明示されている。 文献[01]では、データ センターに、電力システム、冷暖房、換気、空調（HVAC）システムを監視するための専用の施設運用センターや、火災検知及び抑制システムがあること、施設及び環境保護機器について定期的な保守が行われていること、専用の24時間年中無休で稼動する無停電電源装置（UPS）と発電機があり、緊急時の燃料供給のための調整が行われていることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。	公開資料	文献[01]	—		—	利用者は、医療情報システムのアプリケーション等の保守を適切に実施する必要がある。 利用者は、地理的な冗長性のためにアプリケーションを複数のデータセンターに展開する責任を負う。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview エンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析（非技術面および技術面） ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 Microsoft Azure の環境に向けた、サービス継続性の管理 (SCM) の開発およびメンテナンス プロセスが用意されています。このプロセスには、Microsoft Azure の資産を回復し、Microsoft Azure の主要なビジネス プロセスを再開するための方法が含まれています。継続性ソリューションによって、サービスの運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されます。お客様は、地理的な冗長性のためにアプリケーションを複数の場所に展開する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 9.2.4）で、"機器のメンテナンス" が規定されています。 AzureのVMについて再起動を伴うメンテナンスが行われる場合、メンテナンスの予定日時が知らされます。このような場合は、都合に応じて自分自身でメンテナンスを開始できる時間枠が与えられます。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/maintenance-notifications	適合可能	文献[01]では、ビジネス継続性の計画として、業界及びマイクロソフトのベストプラクティスに合致するフレームワークが保持されていることを確認した。フレームワークには以下が含まれている。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、及び回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、及び改訂のプロセス 文献[01]では、ビジネス継続プログラムオフィスにおいて継続性プログラムを主導するフレームワークを保持していること、データ センターを保護するために温度管理、冷暖房、換気、及び空調（HVAC）、火災検知及び抑制システム、電力管理システム等の環境管理を実施していること、Microsoft Azureサービスの機器が、盗難や、火事、煙、水、ほこり、振動、地震、電子的な干渉などの環境的リスクから保護された環境に配置されていることが明示されている。 文献[01]では、データ センターに、電力システム、冷暖房、換気、空調（HVAC）システムを監視するための専用の施設運用センターや、火災検知及び抑制システムがあること、施設及び環境保護機器について定期的な保守が行われていること、専用の24時間年中無休で稼動する無停電電源装置（UPS）と発電機があり、緊急時の燃料供給のための調整が行われていることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。	公開資料	文献[01]	—		—	—
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格（具体的には付属文書 A の項 10.5.1）で、"情報のバックアップ" が規定されています。 ネットワークの高速且つ、信頼性の高い接続性を確保する為に、複数のネットワーク経路により、3テラビット以上のバックボーン、2000以上のネットワークを組み合わせ、高信頼のネットワーク接続性、キャパシティを提供しています。 修正プログラムは弊社で作成したもので、お客様に提供するパッチと同様、電子署名がつけられたものを使用します。また、社外から入手する際には、信頼できる提供元から入手し、ハッシュ値などの確認を行うこととしています。	適合可能	文献[01]では、ソースコードライブラリへのアクセスが権限を与えられたスタッフまたは契約業者のスタッフに制限されていること、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスが厳しく制御されていること、Microsoft Azure 及びシステム変更に関して運用変更の管理手順が定められていることが明示されている。 文献[01]では、データ・ソフトウェア・ハードウェアを対象とした資産に対する機密性、整合性、可用性に関するリスクの評価が年に1回行われていることが明示されている。また、機密資産をマイクロソフト外の関係者と交換する場合は必ず正式な手順を踏むように定めていることを確認した。 また、インタビュー等を通じて、修正プログラムには電子署名が付けられていることが確認できた。	要NDA	文献[01]	—	（本調査で確認した内容に記載の通り）	—	利用者は、プログラムファイルの管理方法を定める必要がある。 利用者は、契約や規定により接続相手先の本人確認や端末確認の方法を明確にし、適切な管理を行う必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機関又は省等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	サービス利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview プロビジョニングされた後、環境を管理して保守する責任はお客様にあります（つまり、ユーザー アクセス管理 や、規制要件に準拠した適切なポリシーおよび手順など）が、Microsoft Azureとして不正なアクセスを予防する為に、認証やマルウェア対策、侵入テスト等の対策を講じています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]によると、Microsoft Azure はマイクロソフト セキュリティ レスポンス センター（MSRC）とGFSから通知された脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを主導すること、Microsoft Azure ではセキュリティインシデント、脆弱性、及び異常動作について報告し処理する手順があること、お客様のデータのセキュリティが侵害されまたは不正アクセスを受けたと Microsoft Azure の担当者が判断した場合、お客様に通知することが明示されている。 文献[06]では、マイクロソフトが標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが明示されている。 文献[07]では、利用者のインシデントについてマイクロソフト側で原因分析を行うことが明示されている。	公開資料	文献[01]文献[06]文献[07]	–		–	利用者は、オープンネットワークを利用したサービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設ける必要がある。 仮想マシン(VM)ロールの場合、お客様は仮想マシンを評価して更新する責任を負う。 加えて、下記のいずれについても、SI事業者あるいは利用者が対応する必要がある。 ・通常とは異なる取引が行われた時等、取引のリスクに応じた要なる本人確認 ・利用者機器（パソコンなど）のシステム環境チェック機能 ・取引内容をモニタリングし、疑わしい取引や異常を検知した場合は取引を一時的に中断する仕組み ・ハードウェアトークン等を利用したトランザクション認証
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。また、Microsoft Azureサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残しています。 Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 · 計画された変更の特定と文書化 · ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） · 機能/コンポーネント設計の仕様決定 · 全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー · DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していることが明示されている。この「セキュリティ開発ライフサイクル」により、攻撃の分析や脅威のモデリングが行われ、設計、開発、または実装の段階で潜在的な脅威が特定された場合に、サービスを制限したり不要な機能を削除したりすることによりリスクを最小限に抑えていることが確認できた。 また、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。	公開資料	文献[01]	–		–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格（具体的には付属文書 A の項 10.5.1）で、"情報のバックアップ" が規定されています。 ネットワークの高速且つ、信頼性の高い接続性を確保する為に、複数のネットワーク経路により、3テラビット以上のバックボーン、2000以上のネットワークを組み合わせ、高信頼のネットワーク接続性、キャパシティを提供しています。 修正プログラムは弊社で作成したもので、お客様に提供するパッチと同様、電子署名がつけられたものを使用します。また、社外から入手する際には、信頼できる提供元から入手し、ハッシュ値などの確認を行うこととしています。	適合可能	文献[01]では、ソースコードライブラリへのアクセスが権限を与えられたスタッフまたは契約業者のスタッフに制限されていること、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスが厳しく制御されていること、Microsoft Azure 及びシステム変更に関して運用変更の管理手順が定められていることが明示されている。 文献[01]では、データ・ソフトウェア・ハードウェアを対象とした資産に対する機密性、整合性、可用性に関するリスクの評価が年に1回行われていることが明示されている。また、機密資産をマイクロソフト外の関係者と交換する場合は必ず正式な手順を踏むように定めていることを確認した。 さらに、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていること、また変更については、運用環境に展開される前に、様々な テスト環境でテストされ、承認されることが明示されている。 また、インタビュー等を通じて、修正プログラムには電子署名が付けられていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、プログラムファイルの管理方法を定める必要がある。 利用者は、契約や規定により接続相手先の本人確認や端末確認の方法を明確にし、適切な管理を行う必要がある。
		(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、「6.6.5 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。	上記(1)～(9)にて記載しました。	適合可能	上記(1)～(9)にて確認した。	公開資料	–	–		–	利用者およびSI事業者は、外部事業者の選定及び医療機関への報告を適切に行う必要がある。
	6.6.2 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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格（具体的には付属文書 A の項 10.5.1）で、"情報のバックアップ" が規定されています。 Microsoft Azure は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）ガイドラインと完全に統合されています。このガイドラインは、ソフトウェア対策プログラムのモデルとして世界的に認知されています。 Microsoft Azure アプリケーション開発時のセキュリティベストプラクティスにより詳細がございます。 http://www.windowsazure.com/ja-jp/support/trust-center/security/ お客様開発アプリケーションおよび、他社パッケージソフトウェアにおける開発についてはお客様が責任を負います。 Azure 上で追加されるサービスは原則SDLに則って開発がされていきます。	適合可能	文献[01]では、ソースコードライブラリへのアクセスが権限を与えられたスタッフまたは契約業者のスタッフに制限されていること、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスが厳しく制御されていること、Microsoft Azure 及びシステム変更に関して運用変更の管理手順が定められていることが明示されている。 文献[10]及び文献[155]では、マイクロソフトが開発し、Azureに展開されるあらゆるソフトウェアが「セキュリティ開発ライフサイクル（SDL）」に従うことが明示されており、テスト段階にてコードインスペクションの実施やファジングテストの実施や、リリース段階にて最終的なセキュリティレビューの実施、リリースするコードのアーカイブ、リリース後のレスポンス計画が明示されている。 文献[01]にて、マイクロソフトでは、Windows Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。また、設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスの制御や不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします と明示されている。 文献[10]及び文献[11]にて、SDLのベストプラクティスが明示されている。	公開資料	文献[01]文献[10]文献[11]文献[155]	–		–	利用者は、プログラムファイルの管理方法を定める必要がある。 利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 · 計画された変更の特定と文書化 · ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） · 機能/コンポーネント設計の仕様決定 · 全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー · DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]にて、Microsoft Azureでは、開発環境、統合テスト環境、運用前環境、運用環境の間で論理的及び物理的な分離が維持され、環境間での資産の交換用に形式化された手順が用意されていることが確認できた。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。 文献[01]では、Microsoft Azure プラットフォーム内の基盤となるオペレーティング システム（OS）に対する変更は、運用環境に移る前に、品質、パフォーマンス、他のシステムへの影響、復旧目標、及びセキュリティ機能に関して、少なくともレビューとテストが行われること、変更は運用環境に展開される前に様々なテスト環境でテストされ承認されることが明示されている。	公開資料	文献[01]	–		–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 · 計画された変更の特定と文書化 · ビジネスの目標、優先度、およびシナリオの特定 (製品の計画時) · 機能/コンポーネント設計の仕様決定 · 全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー · DEV (開発)、INT (統合テスト)、STAGE (運用前)、PROD (運用) 環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.2) で、"変更管理" が規定されています。	適合可能	文献[01]にて、Microsoft Azureでは、開発環境、統合テスト環境、運用前環境、運用環境の間で論理的及び物理的な分離が維持され、環境間での資産の交換用に形式化された手順が用意されていることが確認できた。 文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。 文献[01]では、Microsoft Azure プラットフォーム内の基盤となるオペレーティング システム (OS) に対する変更は、運用環境に移る前に、品質、パフォーマンス、他のシステムへの影響、復旧目標、及びセキュリティ機能に関して、少なくともレビューとテストが行われること、変更は運用環境に展開される前に様々なテスト環境でテストされ承認されることが明示されている。	公開資料	文献[01]	–		–	–
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure には以下に説明するレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールトトレランスを提供するための追加の手順を実施する責任はお客様にあります。 ISO 27001 規格 (具体的には付属文書 A の項 10.5.1) で、"情報のバックアップ" が規定されています。	適合可能	文献[01]では、ソースコードライブラリへのアクセスが権限を与えられたスタッフまたは契約業者のスタッフに制限されていること、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスが厳しく制御されていること、Microsoft Azure 及びシステム変更に関して運用変更の管理手順が定められていることが明示されている。 文献[01]では、データ・ソフトウェア・ハードウェアを対象とした資産に対する機密性、整合性、可用性に関するリスクの評価が年に1回行われていることが明示されている。また、機密資産をマイクロソフト外の関係者と交換する場合は必ず正式な手順を踏むように定めていることを確認した。 さらに、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていること、また変更については、運用環境に展開される前に、様々なテスト環境でテストされ、承認されることが明示されている。 また、インタビュー等を通じて、修正プログラムには電子署名が付けられていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者は、プログラムファイルの管理方法を定める必要がある。 利用者は、契約や規定により接続相手先の本人確認や端末確認の方法を明確にし、適切な管理を行う必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者は、医療情報システム上で取り扱う医療情報を適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者は、医療情報システム上で取り扱う医療情報を適切に管理する必要がある。
	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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview サービスがプロビジョニングされた後、環境を管理して保守する責任はお客様にあります（つまり、ユーザー アクセス管理や、規制要件に準拠した適切なポリシーおよび手順など）が、Microsoft Azureとして不正なアクセスを予防する為に、認証やマルウェア対策、侵入テスト等の対策を講じています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、プロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]によると、マイクロソフトのセキュリティレスポンスセンター（MSRC）が外部のセキュリティ脆弱性の通知サイトを定期的に監視し、Microsoft Azure はMSRCとGFSから通知された脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを主導すること、インシデントの発生時に脆弱性が確認された場合は製品エンジニアリングチームにエスカレーションすることが明示されている。また、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていること、及びウイルスなどのインシデント発生時に、組織的なプロセス（特定、抑制、根絶、復元、及び教訓の学習）により対応することを確認した。 文献[06]では、マイクロソフトが標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが明示されている。	公開資料	文献[01]文献[06]	–		–	利用者がMicrosoft Azure上で構築する環境については、利用者のサイバーセキュリティ等の運用等に則り対策する必要がある。
		(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	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
	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。	–	–	–	公開資料	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
		(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。）。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーションソフトウェアや端末ソフトウェアのセキュリティ対策を適切に行う必要がある。
	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。	–	–	–	公開資料	–	–		–	–

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	情報又は書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	サービスレベル未達の場合には、サービス利用代金の返還を行うことと、SLAに記載しています。 (1)可用性については、SLAに記載の上、返金保証対象としています。 性能については、該当する項目についてSLAに記載し、返金保証対象としています。 拡張性についてはそれぞれのサービス仕様で規定しています。 (2)障害対応については可用性を保証するSLAに含まれていると考えております。 問い合わせ対応については、お問い合わせの内容により処理所要時間が変わってくるためSLAとして規定していません。また、お客様向けに優先対応を行う有償のサポートプログラムを用意しています。 (3)データが不正アクセス等により改ざんされるような場合にはセキュリティインシデントとして扱うことを契約書に記載しています。 (4)再委託先を含む統制環境の構築と維持については契約書に記載しています。 セキュリティ対策・管理やサービスレベルについて「オンライン サービス条件」に記載[文献65]	適合可能	文献(65)、文献(141)及び文献(147)では、サービスレベル未達の対応が、サブスクリプション単位で規定・明記されていることを確認した。 文献(65)及び文献(141)では、システム運用の保証（可用性、障害等に伴うシステムの停止時間、計画停止期間、信頼性、性能、拡張性、稼働時間、ネットワークを含む管理体制、など）、サポートの保証（障害対応、問い合わせ対応、など）、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	公開資料	文献(65)文献[147]	–		–	利用者は、対象業務の重要度、要求事項と提供されるサービスレベルを照らし合わせ、利用可否を決定する必要がある。
		(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。	当社の独立した監査と認定は、個々のお客様の監査に代わって、お客様と共有されます。これらの認定と認証は、当社のセキュリティおよび準拠の目標を設定および達成する方法を正確に表しており、すべてのお客様に対する約束を検証するための実用的なメカニズムとして機能します。数千にものぼるお客様に当社のサービスの監査を許可することは現実的ではなく、それによってセキュリティとプライバシーが侵害される可能性があります。当社の独立した第三者の検証プログラムには 1 年ごとに実施される監査が含まれており、それによって、Microsoft Azure のセキュリティ制御を検証しています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開資料	文献[01]	–		–	利用者は、Microsoft Azure 及びGFSのISO27001認定については BSIグループのWebサイトを参照することができる。新規の利用者の場合、NDAに基づいて請求することでその他の監査情報を請求することにより入手できる。 利用者は、事前に承認を得ることにより、利用者自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。
		(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。	マイクロソフトの運用とサポートの担当者は世界各地に配置されています。このことは、24 時間 365 日、適切な人員が稼働している状態を確保するのに役立っています。サービス運用の大半は自動化されているため、人間の介入が必要になる部分はごくわずかです。 マイクロソフトのエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはありません。代わりに、必要なときにのみ、管理者の監視下でアクセス権が付与されます。 マイクロソフトの担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されます。たとえば、トラブルシューティングや機能の向上（たとえばマルウェアからの保護）です。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていること、職員は常にIDバッジを着用する必要があり着用していない人物の身元確認・報告が義務付けられていること、すべてのゲストはゲストバッジを着用し、マイクロソフトの従業員によってエスコートされることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者がAzure上で構築したアプリケーションやサービスに対する不正プログラムへの防御対策については、利用者が対応を講じる必要がある。
		(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。	処理者の守秘義務に関する確約事項 マイクロソフトは、顧客データおよび個人データの処理に従事するマイクロソフトの担当者が、(i) 当該データをお客様からの指示でのみ処理すること、および (ii) 処理の終了後も顧客データおよび個人データの守秘義務と安全性の保持が義務付けられていることを保証します。 下請処理者の使用に関する通知および規制 マイクロソフトは、一部のサービスまたは補助的なサービスを第三者に委託することができます。お客様は、かかる第三者およびマイクロソフトの関連会社を下請処理者として契約することに同意するものとします。標準契約条項または GDPR 条件の下で上記の同意が要求される場合、この承認は、マイクロソフトが顧客データおよび個人データの処理を下請業者に委託することに対するお客様の事前の書面による同意を構成します。 マイクロソフトは、その下請処理者が本 OST のマイクロソフトの義務を遵守することに責任を負います。マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。マイクロソフトは、本 OST がマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。 マイクロソフトは、随時、新しい下請処理者と契約できるものとします。マイクロソフトは、新規に契約した下請処理者に顧客データまたは個人データへのアクセスを許可する 14 日前までに、ウェブサイトを更新し、かかる更新を知る方法をお客様に提供することにより、新規業者についてお客様に通知します。ただし、コア オンライン サービスに関しては、新規の下請処理者に顧客データへのアクセスを許可する 6 か月前までに、ウェブサイトを更新し、かかる更新を知る方法をお客様に提供することにより、新規業者についてお客様に通知します。 新しい下請処理者を承認しない場合、お客様は、当該通知期間が終わる前に、不承認の理由を記載した解除通知を書面で交付することによって、影響を受ける Online Service のサブスクリプションを違約金なしで解約することができます。影響を受ける Online Service がスイート（またはサービスの 1 回の購入）の一部である場合、解約はスイート全体に適用されます。解約後、マイクロソフトは、お客様またはそのリセラーに対する以降の請求書から、解約した Online Service のサブスクリプションに対する支払義務を削除します。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていること、職員は常にIDバッジを着用する必要があり着用していない人物の身元確認・報告が義務付けられていること、すべてのゲストはゲストバッジを着用し、マイクロソフトの従業員によってエスコートされることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）		
		(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。	施設への物理アクセス: マイクロソフトは、顧客データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に制限します。 データセンター内で移動を続けるには、生体認証による 2 段階認証に合格する必要があります。ID が検証済みになると、データセンターの入館が承認された部分にのみ入ることができます。承認された時間帯のみ、その場所に滞在できます。	適合可能	文献[01]では、職員は常にIDバッジを着用する必要があり着用していない人物の身元確認・報告が義務付けられていること、すべてのゲストはゲストバッジを着用し、マイクロソフトの従業員によってエスコートされることが明示されている。 インタビューの結果、日本国内では入退室者を識別・記録する出入管理設備が設置されており、入館には事前申請と顔写真入りの身分証明書が必要であることから、不法侵入を防止する措置が講じられていると考えられる。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	–
		(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。	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	文献[01]では、データセンターへの入室は生体認証で制限していること、データセンター内は入室管理装置があること、マイクロソフトのデータセンター管理組織でアクセスを許可された従業員、契約業者、訪問者のみに限定するための運用上の手順を導入していること、IDカードを携帯していない人物はゲストバッジが与えられ権限を与えられたマイクロソフトの従業員によってエスコートされる必要があることが明示されている。 NDA文献[N01]にて、入退室の監視が行われており、またその記録が四半期に一度の監査対象となっていることが確認できた。	要NDA	文献[01]	–		NDA文献[N01]	–
		(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 では、主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 · 計画された変更の特定と文書化 · ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） · 機能/コンポーネント設計の仕様決定 · 全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー · DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 お客様は、Microsoft Azure 内でお客様がホスティングするアプリケーションに対する責任を負います。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。	適合可能	文献[01]では、マイクロソフトがMicrosoft Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Azureの主要な変更の実装を制御するためのソフトウェア開発及びリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、及び変更管理」が含まれていることが明示されている。	公開資料	文献[01]	–		–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。	「セキュリティリファレンス（厚生労働省・総務省版）」の6.8節を参照。	適合可能	「セキュリティリファレンス（厚生労働省・総務省版）」の6.8節を参照。	公開資料	–	–		–	–
	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、独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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。	公開資料	文献[01]文献[27]文献[130]	–		–	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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。）。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能		公開資料	–				
		(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。	手配するソフトウェアおよびハードウェアについては、セキュリティに妥協することのない機能を持ったものであることを確認することが、社内規定で決められております。	適合可能	インタビュー等を通じて、ネットワーク機器の調達にあたっては、セキュリティ要求に対する充足を含めた、信頼性の高い機器が調達されることが確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療機関などの施設で使用するネットワーク機器等について、安全性が確保された機器を選定する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機関又は省等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[99]には、Azure環境内のデバイスによって生成される大量の情報は監視・相関関係の特定・分析を行う中央システムによって管理されること、サービス管理チームが継続的に状況把握しアラートに適宜対応することが記載されている。また、セキュリティ更新プログラムにより既知の脆弱性からシステムを保護していることが記載されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 NDA文献[N01]にて、インシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]文献[27]文献[99]文献[130]文献[131]	–		NDA文献[N01]	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[99]には、Azure環境内のデバイスによって生成される大量の情報は監視・相関関係の特定・分析を行う中央システムによって管理されること、サービス管理チームが継続的に状況把握しアラートに適宜対応することが記載されている。また、セキュリティ更新プログラムにより既知の脆弱性からシステムを保護していることが記載されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 NDA文献[N01]にて、インシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]文献[27]文献[99]文献[130]文献[131]	–		NDA文献[N01]	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[99]には、Azure環境内のデバイスによって生成される大量の情報は監視・相関関係の特定・分析を行う中央システムによって管理されること、サービス管理チームが継続的に状況把握しアラートに適宜対応することが記載されている。また、セキュリティ更新プログラムにより既知の脆弱性からシステムを保護していることが記載されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 NDA文献[N01]にて、インシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]文献[27]文献[99]文献[130]文献[131]	–		NDA文献[N01]	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[99]には、Azure環境内のデバイスによって生成される大量の情報は監視・相関関係の特定・分析を行う中央システムによって管理されること、サービス管理チームが継続的に状況把握しアラートに適宜対応することが記載されている。また、セキュリティ更新プログラムにより既知の脆弱性からシステムを保護していることが記載されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 NDA文献[N01]にて、インシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]文献[27]文献[99]文献[130]文献[131]	–		NDA文献[N01]	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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。	外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、データセンターの物理的なコントロールを通じて診断ポート及び構成ポートへの物理的なアクセスを制御していること、コンピュータやネットワーク機器にインストールされている同様の機能の中で、ビジネス上必要とされていないものは無効にされるか削除されること、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[99]には、Azure環境内のデバイスによって生成される大量の情報は監視・相関関係の特定・分析を行う中央システムによって管理されること、サービス管理チームが継続的に状況把握しアラートに適宜対応することが記載されている。また、セキュリティ更新プログラムにより既知の脆弱性からシステムを保護していることが記載されている。 文献[130]には、複数のネットワークレイヤーにおける異なるセキュリティ対策によって外部からの不正なアクセスを防止する多層防御のアプローチについて記載されている。また、多層防御アプローチの一環として、外部からの不正なアクセスを防止するためにIDS/IPSやファイアウォールが導入されていることが明記されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 NDA文献[N01]にて、インシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]文献[27]文献[99]文献[130]文献[131]	–		NDA文献[N01]	利用者は、不正侵入を防止するためには、適切にネットワークACLを設定する必要がある。 利用者は、ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などの必要性を判断して構成する必要がある。
		(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）	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのインターネット接続に関するポリシーや構成等を検討し、適切に実装する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおける同時アクセスユーザ数を適切に設定する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview サービス、ユーザー、セキュリティイベントのログは一元的に保持されます。イベントログ安全なインフラストラクチャにアーカイブされ180日間保持されます。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約事者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格で、"アクセス制御" が規定されています。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 · Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。 マイクロソフトは、顧客データを含む情報システムへのアクセスおよび使用をログに記録し、またはお客様がログに記録できるようにし、アクセス ID、時刻、許可または拒否された認証、および関連する活動を登録します。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。さらに、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 また、文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。	公開資料	文献[01]文献[07]文献[131]	–		–	利用者は、利用者自身のユーザによるアクセスを制御し、そのようなアクセスを適切に確認する責任を負う。 利用者は、オペレーション実行時の遂行状況を確認し、オペレーションを記録する必要がある。 利用者は、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 利用者がAzure上で構築したアプリケーションやサービスのアクセス履歴については、利用者が適切にログの蓄積および確認を行う必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview サービス、ユーザー、セキュリティイベントのログは一元的に保持されます。イベントログ安全なインフラストラクチャにアーカイブされ180日間保持されます。ID管理・侵入検知ツールはAzure環境内に実装されています。早期警告システムが運用環境内のセキュリティイベントの分析をサポートしています。監視エージェントとアラート及びインシデント管理システムはシステムを危険にさらす可能性のあるイベントにほぼリアルタイムでアラートを生成します。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 · Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[138]では、ID管理に Azure Active Directory Premiumを契約して使用することで、高度なセキュリティレポートが利用可能であることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 文献[138]及び文献[142]では、環境の動作状況を判断するために必要な情報は、Azure Active Directory (Azure AD) レポートで入手できると明示されている。また、マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関するレポートは、契約プランによって7日または30日保持すると明示されている。ユーザー アカウントの正当な所有者ではない人によって行われた可能性があるサインイン試行、及び侵害された可能性があるユーザーアカウントに関するレポートは、契約プランによって1日または30日、90日保持されることが明示されている。	公開資料	文献[01]文献[131]文献[138]	–	–	–	利用者は、利用者自身のユーザによるアクセスを制御し、そのようなアクセスを適切に確認する責任を負う。 利用者は、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 利用者がAzure上で構築したアプリケーションやサービスのアクセス履歴については、利用者が適切にログの蓄積および確認を行う必要がある。
		(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。	–	対象外	インタビューにて、Azureの構成要素に無線LANの使用が無い事を確認したため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムに無線ネットワークを使用する場合は、無線ネットワーク上で医療情報を扱わない等、適切に管理する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Virtual Network Gateway を使用してリージョン内の VPN を企業ネットワークにインターネット経由で接続している場合、この通信の暗号化には、既定で AES-256 などの標準が使用されます。ただし、構成は企業ネットワークの Site-to-Site VPN ゲートウェイに依存します。 リージョン内の仮想プライベート ネットワークが Azure ExpressRoute などの直接接続テクノロジを使用して企業ネットワークに接続している場合、このトラフィックは MPLS ネットワーク上の ISP を経由するため、一般的に安全性がより高いと考えられます。追加のセキュリティ要件に対応する必要があるお客様の場合は、仮想ハード ディスク (VHD) ファイルを移動する際に、IPsec、TLS、または BitLocker などのその他のアプリケーション レベルの暗号化技術を使用して通信を暗号化することを推奨します。 Microsoft従業員がリモートアクセスを行う際はポリシーに沿った厳密なアクセス管理、認証の下でVPN接続を実施します。リモートアクセスサービスに事前承認されている必要があり、ADドメインに接続されているか、AzureADに接続、認証した上で接続を行います。リモートVPNアクセスは全てAES-256 などの標準技術で暗号化されます。	適合可能	インタビューにて、インターネットを経由したVPNで接続する場合には、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、医療機関側のネットワーク装置等を適切に管理する必要がある。
			・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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Virtual Network Gateway を使用してリージョン内の VPN を企業ネットワークにインターネット経由で接続している場合、この通信の暗号化には、既定で AES-256 などの標準が使用されます。ただし、構成は企業ネットワークの Site-to-Site VPN ゲートウェイに依存します。 リージョン内の仮想プライベート ネットワークが Azure ExpressRoute などの直接接続テクノロジを使用して企業ネットワークに接続している場合、このトラフィックは MPLS ネットワーク上の ISP を経由するため、一般的に安全性がより高いと考えられます。追加のセキュリティ要件に対応する必要があるお客様の場合は、仮想ハード ディスク (VHD) ファイルを移動する際に、IPsec、TLS、または BitLocker などのその他のアプリケーション レベルの暗号化技術を使用して通信を暗号化することを推奨します。 Microsoft従業員がリモートアクセスを行う際はポリシーに沿った厳密なアクセス管理、認証の下でVPN接続を実施します。リモートアクセスサービスに事前承認されている必要があり、ADドメインに接続されているか、AzureADに接続、認証した上で接続を行います。リモートVPNアクセスは全てAES-256 などの標準技術で暗号化されます。	適合可能	文献[01]にて、ネットワークを制御するために、API の呼び出しなどの重要な通信または Windows Azure 内の通信については、SSL などのプロトコルを使用して暗号化、認証、整合性の制御が行われると明示されている。	公開資料	文献[01]	–	–	–	利用者及びSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、医療機関側のネットワーク装置等を適切に管理する必要がある。
			・インターネット上のトラフィックがVPNチャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しないこと。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、医療機関側のネットワーク装置等を適切に管理する必要がある。
			・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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、医療機関側のネットワーク装置等を適切に管理する必要がある。
	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、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。	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し (つまり切断する)、情報の回復を不可能にする (分解、切断、粉砕、焼却など) 破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.6 および 10.7.2) で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していること、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用し破壊の記録は保持されることが明示されている。	公開資料	文献[01]	–		–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。			文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していること、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用し破壊の記録は保持されることが明示されている。	公開資料	文献[01]	–		–	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。
		(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。	(データの冗長性)マイクロソフトはデータが確実に保護されることを支援します。 ローカル冗長ストレージでは、データのコピーが 3 つ保持されます。LRS は、1 つのリージョンの 1 つの施設内で 3 回複製されます。LRS では、データは通常のハードウェア障害から保護されますが、1 つの施設の障害からは保護されません。 ゾーン冗長ストレージ (ZRS): ゾーン冗長ストレージでは、データのコピーが 3 つ保持されます。ZRS は 2 ～ 3 の施設間で 3 回複製され、LRS よりも高い持続性を提供します。レプリケーションは、単一のリージョン内または 2 つのリージョン間で発生します。ZRS は、1 つのリージョン内のデータの持続性が確保されることを支援します。 geo 冗長ストレージ (GRS):geo 冗長ストレージは、ストレージ アカウントの作成時に、そのアカウントに対して既定で有効になっています。GRS では、データのコピーが 6 つ保持されます。GRS を使用すると、データがプライマリ リージョン内で 3 回複製されます。また、プライマリ リージョンから数百マイル離れたセカンダリ リージョンでも、データは 3 回複製されます。そのため、最も優れたレベルの持続性が実現されます。プライマリ リージョンで障害が発生すると、Azure Storage はセカンダリ リージョンにフェールオーバーします。GRS は、2 つのリージョン内のデータの持続性を確保することを支援します。 https://docs.microsoft.com/ja-jp/azure/security/azure-protection-of-customer-data	適合可能	文献[01]では、レプリケーション機能を備えており、当該機能を使用することでデータがリカバリ可能であることが明示されている。 文献[06]では、利用者が地理的に分散した第2のストレージアカウントを作成することで、ホット・フェールオーバー機能が利用できることが明示されている。 文献[32]にて、Microsoft Azureストレージサービスの機能として、同一施設内における3回のデータ複製、他リージョンに対するデータ複製など、複数方式のレプリケーションによる持続性と高可用性が維持されていることが確認できた。	公開資料	文献[01]文献[06]文献[32]	–		–	利用者がAzure上で構築するアプリケーションやサービスの障害の早期発見および早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。 ホット・フェールオーバー機能を用いるためには、利用者が第2のストレージアカウントを作成して構成する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。
		(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。	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 Microsoft Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Azureのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していること、データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用し破壊の記録は保持されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、自らが使用する電子媒体を適切に管理する必要がある。
	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。 ・情報を電子媒体に記録して交換する際の手順 ・情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	SI事業者側では、利用者（ビジネスパートナー）に対して、利用者のリスクに対応した適切なアプリケーションを提供し実装する必要がある。 暗号鍵の管理主体は原則利用者であるが、SI事業者側では利用者（ビジネスパートナー）の必要に応じて、利用者のリスクに対応した適切な暗号鍵の管理方法を提案する必要がある。 利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。 アプリケーション上の情報伝達手段、ファイル交換手段、電子署名やタイムスタンプの方式は利用者側で決定する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、VPNを使用する場合は、VPNの構成や使用する暗号鍵、医療機関側のネットワーク装置等を適切に管理する必要がある。 利用者及びSI事業者は、医療情報システムのアプリケーション上で情報交換をする場合は、送信者及び受信者の認証および記録を適切に行う必要がある。
			・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止策を行うこと。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーション上で情報交換する場合は、否認防止策を講じる必要がある。
			・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。）。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーション上で情報交換する場合は、交換する情報の機密レベルを送信側及び受信側で合意する必要がある。
			・交換された情報に悪意のあるコードが含まれていないことを確実とすること。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムのアプリケーション上で情報交換する場合は、交換する情報に関するセキュリティ対策（悪意のあるコードなどの混入防止等）を適切に行う必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
			・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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
			・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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムにおける物理的な情報の搬送について、適切に取り扱う必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	SI事業者側では、利用者（ビジネスパートナー）に対して、利用者のリスクに対応した適切なアプリケーションを提供し実装する必要がある。 暗号鍵の管理主体は原則利用者であるが、SI事業者側では利用者（ビジネスパートナー）の必要に応じて、利用者のリスクに対応した適切な暗号鍵の管理方法を提案する必要がある。 利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。 アプリケーション上の情報伝達手段、ファイル交換手段、電子署名やタイムスタンプの方式は利用者側で決定する必要がある。
			・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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	SI事業者側では、利用者（ビジネスパートナー）に対して、利用者のリスクに対応した適切なアプリケーションを提供し実装する必要がある。 暗号鍵の管理主体は原則利用者であるが、SI事業者側では利用者（ビジネスパートナー）の必要に応じて、利用者のリスクに対応した適切な暗号鍵の管理方法を提案する必要がある。 利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。 アプリケーション上の情報伝達手段、ファイル交換手段、電子署名やタイムスタンプの方式は利用者側で決定する必要がある。
			・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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－	－	－	SI事業者側では、利用者（ビジネスパートナー）に対して、利用者のリスクに対応した適切なアプリケーションを提供し実装する必要がある。 暗号鍵の管理主体は原則利用者であるが、SI事業者側では利用者（ビジネスパートナー）の必要に応じて、利用者のリスクに対応した適切な暗号鍵の管理方法を提案する必要がある。 利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。 アプリケーション上の情報伝達手段、ファイル交換手段、電子署名やタイムスタンプの方式は利用者側で決定する必要がある。
			・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムのアプリケーション上での情報の送受信について、エラー時の再送設定やエラー原因の特定などを適切に行う必要がある。
	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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムを適切に管理する必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムを適切に管理する必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムを適切に管理する必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムを適切に管理する必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、医療情報システムを適切に管理する必要がある。
	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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、アプリケーションを適切に管理する必要がある。
		(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。	－	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	－	－	－		－	利用者及びSI事業者は、アプリケーションを適切に管理する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	保証文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、アプリケーションを適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、アプリケーションを適切に管理する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、アプリケーションを適切に管理する必要がある。
	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。	マイクロソフトには、格納域内のデータおよび伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあります。 ISO 27001 規格（具体的には付属文書 A の項 12.3.2）で、"メディアの取り扱い" が規定されています。 Azureにおいて、お客様管理者のクライアント機器とAzureサービスの管理システム間の通信は全てTLSにより暗号化されます。 Azure上で動作するアプリケーションが行う通信と、Azure上に格納するデータの暗号化はお客様アプリケーションによって必要な暗号化を行う必要があります。ここで使用される暗号鍵はお客様管理のものとなります。 データ保存時の暗号化に関しては、利用者のアプリケーション側で対応する必要があります。弊社からは開発者向けに暗号化ライブラリを提供しており、こちらを利用することが可能です。 128 ビット以上の暗号化キーを使用する TLS により、Microsoft Azure データセンター間および対象のデータセンターのクラスター間で送信される制御メッセージを保護します。エンド ユーザーとユーザーの仮想マシン間のトラフィックを暗号化する事も可能です。 改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 またMicrosoft Azure内部コンポーネント間の全ての通信はSSLで保護され、改ざんを未然に防止しています。データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。 暗号鍵の不正使用防止は利用者(Microsoft Azureを利用するお客様)責任において行う必要があります。 Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI)により認証を行い、2要素認証に不正なアクセスの使用防止、アクセス権限確認を講じています。	適合可能	文献[01]では、通信時のデータを暗号化するオプションが提供されることが明示されている。 文献[06]では、証明書や秘密鍵の安全な送信方法及びAzure上での安全な保存方法などが明示されている。 文献[07]では、蓄積・伝送データの暗号化については、Microsoft Azure上で動作する利用者側アプリケーションと利用者端末との通信は利用者側アプリケーションの責任で暗号化を実施する必要があることが明示されている。 文献[07]では、暗号鍵の管理主体は原則利用者となり、公開文書にも明示されている。 文献[07]では、データ保存時の暗号化に、暗号化ライブラリが提供されていることが明示されている。	公開資料	文献[01]文献[06]文献[07]	–		–	–
		(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。	保存データの暗号化、転送中のデータの暗号化、Azure Key Vault を使用した キー管理など、Azure は AES-256 までのさまざまな暗号化機能を提供するので、ニーズに最適なソリューションを自由に選択できます。 https://docs.microsoft.com/ja-jp/azure/security/security-azure-encryption-overview	適合可能	文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。	公開資料	文献[05]	–		–	利用者及びSI事業者は、医療情報システムに使用する暗号化アルゴリズムを適切に選択する必要がある。
		(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。	Azure Key Vault を使用すると、キーや（パスワードなどの）小規模の秘密情報を、ハードウェア セキュリティ モジュール（HSM）に格納されたキーで暗号化できます。さらに安心感を高めたい場合には、FIPS 140-2 レベル 2 規格への準拠が検証済みの HSM でキーをインポートまたは生成すれば、キーを HSM の境界内にとどめることができます。Key Vault は、マイクロソフトがキーを確認または抽出しないように作られています。キーの使用について、Azure ログを使用して監視と監査を行えます。	適合可能	文献[87]では、Azure Key Vault を使用することでクラウドのアプリケーションやサービスの暗号化鍵を保護できること、鍵はハードウェア セキュリティ モジュールを使用して、Azure によってセキュリティで保護されていることが明示されている。 また、同文献にてAzure Key Vaultを使用することで、暗号鍵の作成・取り消し・削除、使用状況の監視が行えることが明示されている。	公開資料	文献[87]	–		–	利用者及びSI事業者は、医療情報システムにおける暗号鍵の漏洩対策を講じる必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureで購入できる証明書はX.509 v3（Microsoft Azure発行）です。または、別の信頼された証明機関によって発行された証明書を利用することもできます。	適合可能	文献[88]では、Azure で使用される証明書は x.509 v3 証明書であり、別の信頼された証明書によって署名することも、自己署名することもできることが明示されている。	公開資料	文献[88]	–		–	利用者及びSI事業者は、必要に応じて信頼された証明書を使用する必要がある。
		(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。	Microsoft Azure には AES-256 をはじめとする幅広い種類の暗号化機能が用意されており、お客様は自分のニーズに最適なソリューションを選択できます。 Microsoft Azure は国際的な情報セキュリティ基準である ISO 27001 認証を取得しており、準拠状況の監査を毎年実施しています。その他国際標準などの準拠のため、あるいはセキュリティや暗号化の強化のために、仕様の変更が行われる場合は事前にお客様に案内が行われます。	適合可能	文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。 インタビューを通じて、通信の暗号化については、国際標準への準拠や、暗号化の強化のために仕様の変更が行われること、さらに変更が行われる場合には事前に顧客に通知していること確認した。	要NDA	文献[05]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムで使用する暗号化アルゴリズムの危殆化について、対策を講じる必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、公開鍵証明書の真正性の確認を適切に実施する必要がある。
	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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書（SMAPI)により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書によるニ要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。	公開資料	文献[01]文献[131]	–		–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。 当社の独立した監査と認定は、個々のお客様の監査に代わって、お客様と共有されます。これらの認定と認証は、当社のセキュリティおよび準拠の目標を設定および達成する方法を正確に表しており、すべてのお客様に対する約束を検証するための実用的なメカニズムとして機能します。数千にものぼるお客様に当社のサービスの監査を許可することは現実的ではなく、それによってセキュリティとプライバシーが侵害される可能性があります。当社の独立した第三者の検証プログラムには 1 年ごとに実施される監査が含まれており、それによって、Microsoft Azure のセキュリティ制御を検証しています。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、プロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]では、不正アクセス検知時及び発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。 文献[01]では、年に１度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、及びコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。 文献[131]には、マイクロソフトはサービスに関連するすべてのシステムを継続的に監視することにより、悪意ある行為を予測し、脅威を示している可能性のある例外イベントを監視し、潜在的な脅威を特定することが明記されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。	要NDA	文献[01]文献[131]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるログの監査などを適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機能又は参考の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure ホストは内部の Microsoft タイム サーバーに同期されています。このサーバーでは、GPS アンテナを使用して、Microsoft が所有する Stratum 1 デバイスから時刻を取得します。Azure の仮想マンシでは、そのホストに依存して正確な時刻 (ホスト時刻) を VM に渡すことも、VM でタイム サーバーから直接時刻を取得することも、あるいはこれらの両方を組み合わることもできます。 スタンドアロン ハードウェアでは、Linux OS によって、起動時にホスト ハードウェア クロックのみが読み取られます。その後、クロックは、Linux カーネルの割り込みタイマーを使用して維持されます。この構成では、クロックは時間の経過と共に誤差が生じます。Azure の新しい Linux ディストリビューションでは、VM で VMICTimeSync プロバイダーを使用できます。このプロバイダーは LIS (Linux Integration Services) に含まれており、ホストからより頻繁にクロック更新についてクエリを実行するためのものです。 Microsoft Azure のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用しています。可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Microsoft Azure サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.10.6) で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure のすべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用し、可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、NTPを通じて同期されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure ホストは内部の Microsoft タイム サーバーに同期されています。このサーバーでは、GPS アンテナを使用して、Microsoft が所有する Stratum 1 デバイスから時刻を取得します。Azure の仮想マンシでは、そのホストに依存して正確な時刻 (ホスト時刻) を VM に渡すことも、VM でタイム サーバーから直接時刻を取得することも、あるいはこれらの両方を組み合わることもできます。 スタンドアロン ハードウェアでは、Linux OS によって、起動時にホスト ハードウェア クロックのみが読み取られます。その後、クロックは、Linux カーネルの割り込みタイマーを使用して維持されます。この構成では、クロックは時間の経過と共に誤差が生じます。Azure の新しい Linux ディストリビューションでは、VM で VMICTimeSync プロバイダーを使用できます。このプロバイダーは LIS (Linux Integration Services) に含まれており、ホストからより頻繁にクロック更新についてクエリを実行するためのものです。 Microsoft Azure のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用しています。可能な場合は、Microsoft Azure 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Microsoft Azure サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.10.6) で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure で使用する時刻同期用サーバが、Microsoft Azure環境全体で正確な時刻を維持するために使用されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおける時刻同期を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.3) で、"職務の分離" が規定されています。	適合可能	文献[01]では、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。 また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。
			・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを用意していることが明示されている。 文献[01]では、Microsoft Azureにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処出来るようにしていることが明示されている。 文献[01]では、「予防的な容量管理」や各種指標による「ハードウェア監視」の運用プロセスがあることが示されている。 文献[01]では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンス及び可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェア及びソフトウェアサブシステムなどの運用プロセスがあることが明示されている。 文献[19]では、障害監視及び対応が世界中の複数のMicrosoft Operations Center(MOC) で行われていることを示している。	公開資料	文献[01]文献[19]	–		–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。
			・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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 情報システム監査ツールへのアクセスは、Microsoft Azure で権限が与えられた担当者のみに制限されます。 委任管理モデルにより、管理者は特定のタスクを実行するのに必要なアクセス権だけを持ち、エラーの可能性を抑えて、必要な場合に限りシステムや機能にアクセスできるようにします。Microsoft Azure には正式な監視プロセスがあり、標準的な運用手順の確認頻度や、監視のプロセスおよび手順の確認などが含まれます。 ISO 27001 規格 (具体的には付属文書 A の項 15.3.2 および 10.10.3) で、"情報システム監査ツールの保護とログ情報の保護" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、情報システム監査ツールへのアクセスは、Microsoft Azure で権限が与えられた担当者のみに制限されていることが明示されている。また、管理者は特定のタスクを実行するのに必要なアクセス権だけを持ち、エラーの可能性を抑えて、必要な場合に限りシステムや機能にアクセス出来るようにしていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるログ管理を適切に実施する必要がある。
	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.	Microsoft Azureはクラウドセキュリティやプライバシー保護で最先端の技術が利用されています。マイクロソフトはサイバーセキュリティに年間10億ドルを費やしており、この大部分がAzureを信頼できるプラットフォームにする改善に利用されています。セキュリティに重点を置いているため、業界標準の必要性も認識しています。Open Compute Project (OCP)、Project Olympus・Cerberusなどのオープンな開発を通じてハードウェア開発レイヤーで必要なセキュリティ対策を規定、追加すると同時に、Azureへ採用することでセキュリティ向上を実現しています。 https://azure.microsoft.com/ja-jp/global-infrastructure/hardware-innovation/ セキュリティとプライバシーは Azure プラットフォームに組み込まれ、セキュリティ開発ライフ サイクル (SDL) から開始します。SDL はすべての開発段階でセキュリティに対応し、安全性をより一層高めるよう Azure が継続的に更新されます。運用セキュリティ保証 (OSA) を SDL の知識上に構築し、クラウドベースのサービスにおけるライフサイクルを通じて、安全な操作のためのフレームワークを提供します。 https://www.microsoft.com/ja-jp/TrustCenter/security/azure-security	適合可能	インタビューにて、ネットワーク機器の調達にあたっては、セキュリティ要求に対する充足を含めた、信頼性の高い機器が調達されることが確認できた。 文献[148]では、Azureのプラットフォームが ISO 27001 認証対象であることが明示されている。 文献[01]によると、Microsoft Azure のコア サービス (コンピューティング、ストレージ、及び仮想ネットワーク) は ISO/IEC 27001:2005 の認証を取得しており、プラットフォームの残りの機能についてもこの認証の取得が予定されていること、CDN 以外のすべての Microsoft Azure サービスが稼働する GFS の物理インフラストラクチャが、ISO 27001 認証を取得していることが明示されている。 また、基盤となっている主要なネットワーク インフラストラクチャは現在、GFS によって管理されています。サービス プロバイダーまたは機器製造業者に対する SLA は、GFS の ISO 27001 認定の対象であると明示されている。	要NDA	文献[01]文献[148]	ISO/IEC 27001	（本調査で確認した内容に記載の通り）	–	利用者は、医療情報システムに対するセキュリティ要求事項を適切に整理する必要がある。
		(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.	マイクロソフトでは、Microsoft Azure サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を (基盤のレベルにおいても) 十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威のモデリング (Threat Modeling) によって、サービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面などの要素をマイクロソフトが特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。https://www.microsoft.com/en-us/securityengineering/sdl/	適合可能	文献[01]では、マイクロソフトでは、Windows Azure サービスの設計、開発、及び実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用し、セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を (基盤のレベルにおいても) 十分に確保するうえで役立つと明示されている。	公開資料	文献[01]	–		–	利用者は、医療情報システムに対するセキュリティ要求事項を適切に整理する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Azure には、情報セキュリティ ポリシーを含む、適切な企業および組織のセキュリティ ポリシーが導入されています。このポリシーはAzure の担当者において、承認、公開、および伝達済みです。情報セキュリティ ポリシーでは、業務の正当性に基づいてAzure の資産にアクセスする権限の付与が必要になります。このアクセス権は、資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されます。さらに、このポリシーでは、アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるアクセス権限の管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	情報又は参考の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Windows Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Windows Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Windows Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格をご確認ください。 予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるアクセス権限の管理を適切に実施する必要がある。
		(5)	業務内容を考慮した必要最小限のアクセス権限を設計、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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Windows Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Windows Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Windows Azure 環境に職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格をご確認ください。 予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。お客様は、アプリケーションの容量ニーズの監視と計画について責任を負います。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるアクセス権限の管理を適切に実施する必要がある。
	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。	Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 · Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます (正規の ID バッジをカード リーダーに通します)。また、データ センターへの入室は生体認証によって制限されます。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書によるニ要素認証を実施しています。 また、特権の利用は記録され、監査されています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 · マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 · アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 · マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[31]では、ID基盤にAzure Active Directoryを使用することで、様々な認証オプションが利用でき、IDの不正使用防止機能を有することが明示されている。	公開資料	文献[01]文献[31]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 · Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます (正規の ID バッジをカード リーダーに通します)。また、データ センターへの入室は生体認証によって制限されます。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書によるニ要素認証を実施しています。 また、特権の利用は記録され、監査されています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 · マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 · アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 · マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azureの開発者および、運用担当者はMicrosoftアカウントおよび自己署名付き証明書により認証を行い、不正なアクセスの使用防止、アクセス権限確認を講じています。 スタッフおよび契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 · Microsoft Azure では、ネットワーク レベルのコンポーネントへのアクセスには 2 要素認証が必要であり、(Azure に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは、2 要素認証によってセットアップされる直接アクセスを使用します。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます (正規の ID バッジをカード リーダーに通します)。また、データ センターへの入室は生体認証によって制限されます。 上記の通り、マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書によるニ要素認証を実施しています。また、特権の利用は記録され、監査されています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 · マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 · アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 · マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。 文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Windows Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Windows Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Windows Azure 環境に職務の分離が実装されています。 アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するように通知されます。また、契約業者またはサード パーティのインフラストラクチャから、すべての電子メディアを削除する必要があります。また、データが適切に削除されていることを確認するため、マイクロソフトによって監査が行われる場合があります。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するように通知されます。また、契約業者またはサード パーティのインフラストラクチャから、すべての電子メディアを削除する必要があります。また、データが適切に削除されていることを確認するため、マイクロソフトによって監査が行われる場合があります。 ISO 27001 規格 で、"資産の返却" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するように通知されます。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 ※オンラインサービス条件 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSIT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格 で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小特権の原則に基づいて付与されることが明示されている。さらに、情報セキュリティポリシーに、アクセスの準備、認証、アクセスの承認、アクセス権の削除、及び定期的なアクセスの確認が含まれることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(8)	特権IDの発行は必要な最小限のものに留めること。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間（最長 6 か月）使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.3) で、"職務の分離" が規定されています。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機能又は参考等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(9)	特権使用者に昇格可能な作業者IDを制限すること。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間 (最長 6 か月) 使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.3) で、"職務の分離" が規定されています。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(10)	特権の使用時には作業実施内容を記録すること。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 処理活動の記録 マイクロソフトは、GDPR 第 30 条 (2) 項で義務付けられているすべての記録を保持し、お客様に代わって行う個人データの処理に該当する場合には、要請に応じてお客様にかかる記録を提供するものとします。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 サービス、ユーザー、セキュリティイベントのログは一元的に保持されます。イベントログ安全なインフラストラクチャにアーカイブされ180日間保持されます。ID管理・侵入検知ツールはAzure環境内に実装されています。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、プロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていること、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。が確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft の運用担当者が顧客データに定期的にアクセスする操作は、既定で拒否される設定になっています。顧客データへのアクセス権を付与する場合、リーダーの承認が必要になり、アクセスは慎重に管理されて、ログに記録されます。アクセス制御の要件は、次のような Azure セキュリティ ポリシーによって確立されています。 既定では、顧客データへのアクセス権はない。 お客様の仮想マシン (VM) に関するユーザー アカウントまたは管理者アカウントはない。 タスク (監査とログ アクセスの要求) を完了するために必要な最低限の特権を付与する。 Azure のサポート担当者には、Microsoft によって一意の Corporate Active Directory アカウントが割り当てられます。Azure は、重要な情報システムへのアクセスを制御するために、Microsoft Information Technology (MSIT) によって管理されている Microsoft Corporate Active Directory に依存しています。多要素認証が必要であり、アクセスは安全なコンソールからのみ許可されます。 すべてのアクセス試行が監視され、基本的な一連のレポートを使用して表示できます。 Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、プロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	インタビュー等を通じて、保守作業に必要な特権アカウントはプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSIT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格 (具体的には付属文書 A の項 11.2.1 および 11.2.3) で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Azure のすべてのスタッフ及びGFSのスタッフが提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があること、不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure環境に職務の分離が実装されていることが明示されている。また、Microsoft Azure の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。 インタビュー等を通じて、ベンダにより付与されたデフォルトパスワードは、適切なパスワードに変更されることを確認した。	要NDA	文献[01]	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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付けない機構とすること。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書(OST)記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Live IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証についてはお客様の責任範囲です。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機能又は書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 なお、利用可能な認証サービスのAzureActiveDirectoryは最初のログオン時にパスワードを強制的に変更させる機能を持っています。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Live IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証についてはお客様の責任範囲です。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Live IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証についてはお客様の責任範囲です。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSIT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格 (具体的には付属文書 A の項 11.2.1 および 11.2.3) で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビュー等を通じて、自動ログインのためにパスワードが保管してはならないことが規則で定められていることを確認した。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Live IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証についてはお客様の責任範囲です。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、及び最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Azureの運用環境へのアクセスが厳しく制御されていることが明示されている。 文献[127]には、Azure ADではよく使用されているパスワードを動的に禁止する仕組みや、パスワードハッシュをクラッキングするためのレインボーテーブルへの対策が行われていることが記載されている。	公開資料	文献[01]文献[127]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機密文書等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview アクセス ポリシー: マイクロソフトは、顧客データにアクセス可能な個人のセキュリティ権限の記録を保持します。 アクセスの許可 -マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 -マイクロソフトは、一定期間 (最長 6 か月) 使用されていない認証資格情報を無効にします。 -マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 -顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID /ログインを割り当てます。 最小限の権限 -テクニカル サポート担当者は、必要な場合に限り、顧客データへのアクセスを許可されます。 -マイクロソフトは、顧客データへのアクセスを、職務を履行するためにかかるアクセスを必要とする個人にのみ制限します。 企業ドメイン アカウント向けのパスワード ポリシーは、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されます。一時パスワードは、MSIT が確立したプロセスを使用してユーザーに通知されます。 すべてのサービスおよびインフラストラクチャは、最低でも MSIT の要件を満たす必要があります。ただし、社内組織は独自の裁量でセキュリティ ニーズに合わせて、この標準を超えて強度を高めることができます。 お客様は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負います。 ISO 27001 規格 (具体的には付属文書 A の項 11.2.1 および 11.2.3) で、"ユーザー パスワードの管理およびユーザー登録" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビュー等を通じて、一定時間を経過すると強制ログオフされることを確認した。	要NDA	–	–	(本調査で確認した内容に記載の通り)	–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 Microsoft Azure環境への認証として、ActiveDirectoryでの認証、クレームベースの認証、Live IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。 Azure環境への認証については、強いパスワードのみが使用可能となっています。 Azure環境上で動作するアプリケーションの認証についてはお客様の責任範囲です。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。 文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。	公開資料	文献[01]文献[27]	–		–	利用者及びSI事業者は、医療情報システムにおけるID管理を適切に実施する必要がある。
	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。	マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、自社の作業者の教育を適切に実施する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、自社の作業者のアカウント管理を適切に実施する必要がある。
		(2)	システムに許可なくアクセスされた疑いがあるとき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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 -マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 -マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 認証 -マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 -認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 -マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 -マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 -マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 -マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[01]では、企業ドメイン アカウント向けのパスワード ポリシーが、パスワードの長さ、複雑度、有効期限の最小要件を規定するマイクロソフトの企業 Active Directory ポリシーを通じて管理されることが明示されている。	公開資料	文献[01]	–		–	利用者及びSI事業者は、自社の作業者のアカウント管理を適切に実施する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機関又は等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
				少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。								
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 完全性および秘密保持 ・マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。 ・マイクロソフトはパスワードを、当該パスワードが有効である間はそれらが判読できなくなるような方法で保存します。 組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	インタビュー等を通じて、アイドル時間を経過した後には端末ロックされ、解除にはパスワード入力が必要であることを確認した。	要NDA	–	–	（本調査で確認した内容に記載の通り）	–	利用者は、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必要がある。
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方全を期し、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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8) で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[34]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示している。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられている。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けている。このプログラムの目的は、データの取り扱い方法を標準化し強化すること、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[134]	–		NDA文献[N01]	利用者及びSI事業者は、医療情報を操作する可能性のある職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8) で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けています。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[134]	–		NDA文献[N01]	利用者及びSI事業者は、医療情報を操作する可能性のある職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める必要がある。
		(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。	マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8) で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。 Microsoft は、一部のサービス (カスタマー サポートなど) の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Azure の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けています。このプログラムの目的は、データの取り扱い方法を標準化し強化することと、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[134]	–		NDA文献[N01]	利用者及びSI事業者は、医療情報を操作する可能性のある職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定する必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview インシデント エンジニア、インシデント マネージャー、コミュニケーション マネージャー、および機能チームに対して、インシデントの処理方法、管理の役割、および責任が定義されています。 Windows Azure のオペレーション マネージャーは、その他の担当者のサポートを受けて、セキュリティおよびプライバシーに関するインシデントの調査と解決を監督する責任を負います。インシデントの調査と分析を行うために、他の担当者にエスカレーションして依頼するプロセスが確立されています。 セキュリティ インシデントの発生時に、プライバシー、法務、または経営管理者に通知するエスカレーションおよびコミュニケーション計画が確立されています。 マイクロソフトのプロセスは、特定、抑制、根絶、復元、および教訓の学習の手順で構成されています。 ISO 27001 規格 (具体的には付属文書 A の項 13.2) で、"セキュリティ インシデントの対応計画" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格をご確認ください。 ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格 (具体的には付属文書 A の項 11) で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、そのプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 運用システムに対して意図しないアクセスや変更または承認されていないアクセスや変更が行われるリスクを最小限に抑えるため、Microsoft Azure 環境内の重要な機能については職務が分離されています。職務と責任は、Microsoft Azure の運用チーム間で分離および定義されています。資産の所有者または管理者は、運用環境内で異なるアクセスおよび権限を承認します。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Azure 環境に職務の分離が実装されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.3) で、"職務の分離" が規定されています。	適合可能	文献[65]では、顧客データへの違法なアクセス、または当該機器または施設への不正アクセスが顧客データの紛失、開示、または改変につながったことについて知った場合、速やかに、(1) セキュリティ インシデントについてお客様に通知し、(2) セキュリティ インシデントを調査して詳細情報をお客様に提供し、(3) セキュリティ インシデントにより生じる影響を緩和しそれにより生じる損害を最小限に抑えるための合理的な手段を講じること、が明示されている。	公開資料	文献[65]	–		–	利用者及びSI事業者は、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必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	機関又は省等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 従業員、契約業者、サード パーティのユーザーは、雇用または契約の期間中にマイクロソフトから提供されたすべての物理的な資料を適切に破棄するかまたは返却するように通知されます。また、契約業者またはサード パーティのインフラストラクチャから、すべての電子メディアを削除する必要があります。また、データが適切に削除されていることを確認するため、マイクロソフトによって監査が行なわれる場合があります。 ISO 27001 規格（具体的には付属文書 A の項 8.3.2）で、"資産の返却" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 従業員の雇用終了プロセスは、Microsoft 米国本社の人事ポリシーによって行われます。 ISO 27001 規格（具体的には付属文書 A の項 8.3）で、"雇用の終了または雇用状態の変更" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[65]では、「担当者は、顧客データに関する秘密保持義務を負い、かかる義務は当該担当者の任用の終了後も継続する」ことが明記されている。 また、インタビュー等を通じて、すべての従業員が適切な合意書にサインして、Microsoft社の雇用ポリシーを受け入れる必要があることを確認した。	要NDA	文献[65]	—	（本調査で確認した内容に記載の通り）	—	利用者及びSI事業者は、医療情報を操作する職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておく必要がある。 利用者及びSI事業者は、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必要がある。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。 Microsoft は、一部のサービス（カスタマー サポートなど）の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Azure の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。 Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Azure または GFS が開催するセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Azureのすべての契約業者のスタッフ及びGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 NDA文献[N01]にて、対象には請負業者も含まれていることが確認できた。 文献[01]では、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 セキュリティの違反、または情報セキュリティポリシーの違反が疑われるMicrosoft Azureサービスのスタッフは、調査プロセスの対象となり、該当する懲戒措置（最も厳しい場合は雇用終了も含む）が実施されること、セキュリティの違反、または情報セキュリティポリシーの違反が疑われる契約業者のスタッフは、正式な調査の対象となり、関連する契約に該当する措置が実施される（契約の終了となる可能性もある）ことが明示されている。 文献[01]によると、Microsoft Azure では契約により、下請業者に対し重要なプライバシー及びセキュリティ要件を満たすよう求めることが明示されている。 文献[134]では、データへのアクセスを必要とする作業を Microsoft が外部の会社に委託する場合は、その会社が副処理者と見なされ、Microsoft は、この副処理者のリストを開示しています。また、副処理者は、Microsoft からの委託の対象であるオンライン サービスを提供するためだけにデータにアクセスでき、その他の目的でデータを使用することは禁じられています。副処理者には、このデータの機密保持が義務付けられ、Microsoft がお客様に契約上確約したのと同等またはそれよりも厳格なプライバシー要件を満たすことが契約上義務付けられると明示されている。 また、Microsoft は副処理者に、Microsoft Supplier Security and Privacy Assurance Program への参加を義務付けています。このプログラムの目的は、データの取り扱い方法を標準化し強化すること、サプライヤーのビジネス プロセスとシステムが Microsoft のものと整合していることを保証することを要求すると明示されている。	要NDA	文献[01]文献[134]	—		NDA文献[N01]	—
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。	『2.6.7.電子媒体の取扱』を参照。	適合可能	『2.6.7.電子媒体の取扱』を参照。	公開資料	—	—		—	利用者は、医療情報システムの利用に当たり外部電子媒体を使用する場合、『2.6.7.電子媒体の取り扱い』に準拠した対応を行う必要がある。
		(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	『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。	適合可能	『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。	公開資料	—	—		—	利用者は、医療情報システムの利用に当たりリムーバブルハードディスク等を使用する場合、『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』に準拠した対応を行う必要がある。
		(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。	オンライン サービス条件の中で、Microsoft はお客様がクラウド サービスの利用を停止したときやサブスクリプションが失効したときの具体的なプロセスを契約上確約しています。これには、顧客データを Microsoft 管理下のシステムから削除することも含まれます。 お客様がクラウド サブスクリプションを終了したときやサブスクリプションが失効した場合は（無料試用を除く）、Microsoft はお客様の顧客データを機能限定アカウントに 90 日間（『保持期間』）保管します。これは、お客様がデータを抽出するかサブスクリプションを更新するための時間を確保するためです。この期間内に、Microsoft は通知を複数回行います。したがって、お客様はデータ削除の予告を十分に受けることになります。 この 90 日間の保持期間が終了すると、Microsoft はアカウントを無効化して顧客データを削除します。これには、キャッシュやバックアップとして複製されたものも含まれます。対象範囲内サービスについては、この削除は保持期間終了後 90 日以内に行われます（対象範囲内サービスは、オンライン サービス条件の『データ処理条件』の項で定義されています）。 顧客データが Microsoft の法人向けクラウド サービスのマルチテナント環境でホストされているときは、慎重な手段を講じて顧客データを論理的に分離します。このことは、ある利用者のデータが漏えいして別の利用者のデータと混在するのを防ぐのに役立つほか、ある利用者の削除済みデータに他の利用者がアクセスできないようにするのに役立ちます。 マイクロソフトのエンタープライズ向けクラウドサービスでは契約終了後、一定の期間はお客様管理者がデータにアクセスすることができる状態になります。この期間は、お客様がデータ移行後の確認および万一移行漏れがあった場合の回復手段とするために用意されています。この期間終了後、お客様コンテンツの削除が開始され、お客様によるお客様コンテンツのアクセスや回復は行うことができなくなります。削除処理が完了するとお客様コンテンツは回復不可能な状態となります。	適合可能	文献[65]では、データ処理サービスの提供終了時にユーザーから移転されたすべての個人データ及びこれのコピーを返却するか、または全ての個人データを破棄しその旨を証明することが明示されている。 インタビュー等で確認したところ、消去証明書の発行は行っていないが、第三者監査報告書により消去プロセスが検証可能であることが確認できた。	要NDA	文献[65]	—	（本調査で確認した内容に記載の通り）	—	—
2.9.医療情報システムの改造と保守			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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、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、試験結果を確認する必要がある。
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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、医療情報処理に関わる業務プロセスを識別する必要がある。 利用者及びSI事業者は、医療情報処理に関わる情報処理設備等について識別する必要がある。
		(2)	業務プロセス間の相互関係を評価すること。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、業務プロセス間の相互関係を評価する必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、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必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、SI事業者との連携の元、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必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者は、SI事業者との連携の元、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必要がある。
		(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—		—	利用者及びSI事業者は、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、方策を検討する必要がある。

経済産業省ガイドラインの評価項目				ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
節	項	項番	要求事項		ガイドラインへの適合性	本調査で確認した内容	情報又は参考等の開示レベル	確認した公開文書	第三者認証等から推測した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview Microsoft Azure上での構成として、冗長化構成を取る事で、障害が起きた場合において継続利用をする事が可能です。 また Microsoft Azure にはレプリケーション機能が含まれており、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができます。 お客様のデータの履歴バックアップを作成すること、お客様のデータのバックアップをプラットフォーム以外に保存すること、冗長性のあるコンピューティング インスタンスをデータ センター全体に展開すること、仮想マシンの状態とデータのバックアップを作成することなど、その他のフォールト トレランスを提供するための追加の手順を実施する責任はお客様にあります。 Microsoft Azure プラットフォーム インフラストラクチャの各層は、障害発生時にも運用を継続できるように設計されています。	適合可能	文献[01]では、レプリケーション機能を備えており、当該機能を使用することでデータが1カ所以上で可能であることが明示されている。 また、ビジネス継続のための復旧計画を立て、手順を確立すること、計画した手順が有効であることを定期的に検証することが明示されている。 文献[06]では、利用者が地理的に分散した第2のストレージアカウントを作成することで、ホット・フェールオーバー機能が利用できることが明示されている。 文献[38]では、Site Recovery機能を用いることで、仮想マシンのレプリケーションと回復手順が自動化できることが明示されている。	公開資料	文献[01]文献[06]文献[38]	–		–	利用者及びSI事業者は、医療情報システムを用いた業務継続性を考慮し、必要に応じた冗長構成を検討する必要がある。
	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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは、ビジネス継続性に関する ISO 22301 認証を取得した最初の超大規模クラウド サービス プロバイダーです。独立した認証機関による、事業継続性のプロセスに関するすべての要素を対象とした厳格な監査を経て、Microsoft Azure、Microsoft Azure Government、Microsoft Cloud App Security、Microsoft Intune、Microsoft Power BI がこの認証を取得しました。この監査では、これら対象サービスのほか、Azure 管理機能、Azure Portal、対象サービスの監視、操作、更新に使用するシステムが審査されました。 ISO 22301:2012 は、ビジネス継続性の確保をサポートする管理システムについての初めての国際規格です。ISO 22301 はビジネス継続性に関する重要規格であり、認定されると、破壊的な出来事の予防、緩和、対応、回復を図るための厳格な手順（プラクティス）となります。 https://www.microsoft.com/ja-jp/trustcenter/compliance/iso-22301	適合可能	文献[135]では、お客様は、自分のデータと ID を所有し、それらとオンプレミス リソースのセキュリティ、及び自分が制御しているクラウド コンポーネントのセキュリティを保護する責任を持つと明示されている。 文献[134]では、Microsoft のエンジニアには、クラウドの顧客データに対する既定のアクセス権が与えられることはなく、Microsoft の担当者が顧客データを使用するのは、契約で定めたサービスの提供と矛盾しない目的に限定されると明示されている。 Microsoft Azureにおいては文献[01]にて、ビジネス継続性プログラム オフィスでは、すべてのレベルにおいて継続性プログラムを主導する、業界及びマイクロソフトのベスト プラクティスに合致するフレームワークを保持し、フレームワークには以下のものが含まれると明示されている。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、及び回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、及び改訂のプロセス お客様は、地理的な冗長性のためにアプリケーションを複数のデータ センターに展開する責任を負います。	公開資料	文献[01]文献[134]文献[135]	–		–	利用者は、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必要がある。
		(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。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview 災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS）に属するOnline Services Security and Compliance（OSSC）の情報セキュリティ管理システム（ISMS）によりレビュープロセスが確立されています。使用する統制策（ISO27001/27005、SAS70 TypeIおよび II、SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。 マイクロソフト内の該当するすべての従業員は、Microsoft Azure が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。また、マイクロソフトは、従業員との契約に機密保持条項を含めています。 Microsoft Azure のすべての契約業者のスタッフおよび GFS のスタッフは、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8）で、"役割と責任、および情報セキュリティの意識向上、教育、トレーニング" が規定されています。	適合可能	文献[01]では、ビジネス継続性プログラムを主導するフレームワークに「該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニングプログラム」があることが明示されている。 また同文献には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。 文献[19]では、Microsoft Operations Center(MOC)にて、防災管理も含めて全体の管理を実施していることが明示されている。 NDA文献[N01]にて、情報セキュリティに関する管理者が割り当てられ役割と責任が明確化されていること、災害などに備えた事業継続のためのプロセスが定められていることが確認できた。	要NDA	文献[01]文献[19]	–	–	NDA文献[N01]	利用者は、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必要がある。
		(3)	事業継続計画について定期的に見直しを行うこと。	利用者(Microsoft Azureを利用するお客様)はアプリケーションおよびデータとそのアクセス権を利用者自身が管理する仕組みになっており、利用者による安全管理を実施いただく必要があります。 プラットフォームとなるMicrosoft Azureのデータセンターにおける安全管理はマイクロソフトが行います。 https://docs.microsoft.com/ja-jp/azure/security/security-management-and-monitoring-overview マイクロソフトは、ビジネス継続性に関する ISO 22301 認証を取得した最初の超大規模クラウド サービス プロバイダーです。独立した認証機関による、事業継続性のプロセスに関するすべての要素を対象とした厳格な監査を経て、Microsoft Azure、Microsoft Azure Government、Microsoft Cloud App Security、Microsoft Intune、Microsoft Power BI がこの認証を取得しました。この監査では、これら対象サービスのほか、Azure 管理機能、Azure Portal、対象サービスの監視、操作、更新に使用するシステムが審査されました。 ISO 22301:2012 は、ビジネス継続性の確保をサポートする管理システムについての初めての国際規格です。ISO 22301 はビジネス継続性に関する重要規格であり、認定されると、破壊的な出来事の予防、緩和、対応、回復を図るための厳格な手順（プラクティス）となります。 https://www.microsoft.com/ja-jp/trustcenter/compliance/iso-22301	適合可能	文献[01]には、ビジネス継続性プログラムにおけるソリューションが、イベント発生時に有効であることを保証するため、復元計画は業界のベストプラクティスに従って定期的に検証されること、ビジネス継続性プログラムにはテスト・メンテナンス・改定のプロセスが含まれていることが記載されている。	公開資料	文献[01]	–		–	利用者は、事業継続計画について定期的に見直しを行う必要がある。