医療機関向け
『Office 365』対応セキュリティリファレンス

2017年7月25日
Version 1.1

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11月4日	Version 1.0	初版
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＞ 6.5-11 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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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
6.1-01	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、滅失又は毀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	–	–	対象外	–	–	–	–	–	–	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	–	マイクロソフトはデータセンター所在地を開示しています。当該国にデータを保存することによる法令適用や業務の継続性の影響の有無はお客様による判断が必要です。 マイクロソフト データセンターあるい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、関連するお客様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。 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お客様側で調査することが可能です。 マイクロソフトは、お客様がお客様データの所有者でありアクセス権を保持することを契約書に記載しており、このことはマイクロソフトの経営不安が発生した場合でも継続して保障される事項です。 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。そのためお客様がデータセンターに立ち入ったとしても、お客様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お客様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。 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[66]およびNDA文書では、提供事業者として必要な基本的な事項が規定・明記され、インタビューの結果を含め、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。 また、インタビュー及びNDA文書で確認したところ、日本でMicrosoft Online Servicesの契約をする場合、準拠法は日本法であることが確認できた。 NDA文書を確認したところ、お客様が日本国内でクラウドサービス契約を締結し、日本国内でプレミアサポート契約を締結することで、24時間日本語対応が提供されることを確認した。	要NDA	文献[65]（OST） 文献[66]（SLA）	–	（マイクロソフト社とのNDA により開示）	（マイクロソフト社とのNDAにより開示）	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、滅失又は毀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	–	–	対象外	–	–	–	–	–	–	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	–	–	対象外	–	–	–	–	–	–	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	–	–	対象外	–	–	–	–	–	–	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	–	–	対象外	–	–	–	–	–	–	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	–	–	対象外	–	–	–	–	–	–	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	–	–	対象外	–	–	–	–	–	–	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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．【推奨】） ・各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるよう、定期的にレビュー及び見直しを行うこと。（Ⅱ．4．3．1【基本】） ・情報システム運用責任者を明確に定めて、合意すること。	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、Office 365 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[129]では、マイクロソフトの全てのクラウドインフラストラクチャに対するコンプライアンス責務を負う組織であるMCIO（Microsoft's Cloud Infrastructure and Operations）と、その一部としてクラウドインフラストラクチャのセキュリティプログラムに責任を負う組織であるOSSC（Online Services Security and Compliance team）について言及されている。 文献[01]では、データガバナンスの一環として、Microsoft Online Services 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 Online Services 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。 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[129] 文献[01]「DG-01：データガバナンス - 所有権/管理者責任」 文献[01]「DG-04：データガバナンス - 保持ポリシー」 文献[01]「DG-05：データガバナンス - 安全な廃棄」 文献[01]「DG-06：データガバナンス - 非運用データ」 文献[01]「DG-07：データガバナンス - 情報漏えい」 文献[01]「IS-07：情報セキュリティ - ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「IS-09：情報セキュリティ - ユーザーアクセスの無効化」 文献[01]「IS-10：情報セキュリティ - ユーザーアクセスの確認」 文献[01]「SA-03：セキュリティアーキテクチャ - データのセキュリティ/整合性」 文献[19]「Incident Management Model」	（マイクロソフト社とのNDA により開示）	（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、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	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】） ・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こと。（Ⅲ．4．4．3【基本】） ・受託した個人情報を参照可能な事務室等におけ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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	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 Office 365 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文書を確認したところ、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]「FS-01：施設のセキュリティ - ポリシー」 文献[01]「FS-03：施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDA により開示）	（マイクロソフト社とのNDAにより開示）	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 Online Services 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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項目番	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	
6.3-03					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管理規程を作成すること。	最低限	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．5．3．1【基本】） ・ASP・SaaSサービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・運用しているアクセス管理に関する規程類が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・自社の規程類の情報を医療機関に対して開示する範囲・条件等について、医療機関等と合意すること。	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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。 マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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 Online Services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 Online Services 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 Online Services 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 Online Services 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に通知されます。 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]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-27：情報セキュリティ－資産の返却」 文献[01]「IS-30：情報セキュリティ－診断/構成ポートへのアクセス」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「OP-02：運用管理・文書化」 文献[01]「SA-02：セキュリティアーキテクチャー－ユーザーID資格情報」 文献[01]「SA-03：セキュリティアーキテクチャー－データのセキュリティ/整合性」 文献[131] 文献[01]「IS-18：情報セキュリティ－暗号化」 文献[01]「SA-11：セキュリティ アーキテクチャ－共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	－	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、Office 365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。
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	・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・自社で定める個人情報保護指針等に基づいて、委託業務を実施する皆を、契約内容に含めること。 ・自社で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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要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が含まれていることを確認し、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こと。	マイクロソフトはデータセンター所在地を開示しています。当該国にデータを保存することによる法令適用や業務の継続性の影響の有無はお客様による判断が必要です。 マイクロソフト データセンターあるい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、関連するお客様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。 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お客様側で調査することが可能です。 マイクロソフトは、お客様がお客様データの所有者であり アクセス権を保持することを契約書に記載しており、このことはマイクロソフトの経営不安が発生した場合でも継続して保障される事項です。 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。そのためお客様がデータセンターに立ち入ったとしても、お客様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お客様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。 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[66]およびNDA文書では、提供事業者として必要な基本的な事項が規定・明記され、インタビューの結果を含め、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。 インタビュー及びNDA文書で確認したところ、日本でMicrosoft Online Servicesの契約をする場合、準拠法は日本法であることが確認できた。	要NDA	文献[65](OST) 文献[66](SLA)	－	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、Microsoft Online Services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	・経営陣は、情報セキュリティに関する組織的取組についての基本的な方針を定めた文書を作成すること。また、当該文書には、経営陣が承認の署名等を行い、情報セキュリティに関する経営陣の責任を明確にすること。（Ⅱ．1．1．1【基本】） ・自社で定める情報セキュリティに関する組織的取組における基本方針が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	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 Online Servicesが定める基本方針等が、医療機関等が求めるの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	・医療機関等の体制に対応する事業者の体制を明らかにすることを、医療機関等と合意すること。	－	対象外	－	－	－	－	－	利用者は、Microsoft Online Services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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・マニュアル等の文書管理に関して、開示できる文書等の範囲、事業者の役割等を医療機関等と合意すること。	Microsoft Online Services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 Online Services 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 Online Services 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 Online Services 資産を回復し、Microsoft Online Services のお客様にとって主要なビジネス 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。 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 Online Services 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 Online Services 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、Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services のお主要なビジネス プロセスを再開するための方法が含まれていることが明示されている。	公開文書	文献[01]「OP-02：運用管理・文書化」 文献[01]「RS-01：復元・管理プログラム」 文献[01]「RS-03：復元・ビジネス継続性の計画」	（マイクロソフト社とのNDAにより開示）	－	－	利用者は、Microsoft Online Services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。

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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	
6.3-08					(d) リスクに対する予防、発生時の対応の方法	最低限	・全ての従業員に対し、業務において発見あるいは疑いをもった情報システムのぜい弱性や情報セキュリティインシデント（サービス停止、情報の漏えい・改ざん/破壊・紛失、ウイルス感染等）について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるような手続きを定め、実施を要求すること。報告を受けた後に、迅速に整然と効果的な対応ができるよう、責任体制及び手順を確立すること。（Ⅱ．6．1．1【基本】） ・自社で定める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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	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、Microsoft Online において、電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動などの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プロセスを開発していることが明示されている。 また、不正アクセス検知時およ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。 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および追跡について明示されている。	公開文書	文献[01]「IS-22：情報セキュリティインシデント管理」 文献[01]「SA-14：セキュリティアーキテクチャー - 監査ログ/侵入検出」 文献[01]「RS-03：復元 - ビジネス継続性の計画」 文献[01]「RS-04：復元 - ビジネス継続性のテスト」 文献[130] 文献[65]	—	—	—	利用者は、Microsoft Online Services 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	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】） ・ASP・SaaS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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．2．1．2【基本】） ・自社で定める機器の管理等の運用管理の規程等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。 お客様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	Office 365 および 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 Online Services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]などの公開資料を利用できることを確認した。 文献[01]では、予防的な監査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。	公開文書	文献[03] 文献[01]「OP-03：運用管理 - 容量/リソース計画」	（マイクロソフト社とのNDAにより開示）	—	—	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 Online Services が定める機器の管理等の運用管理の規程等が、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。
6.3-10					(f) 個人情報の記録媒体の管理（保管・授受等）の方法	最低限	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】） ・自社で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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要性から個人情報保護法における運用に準じて取り扱うこと。	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、Office 365 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 Online Services 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者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセス制御も明示されている。 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。	公開文書	文献[01]「DG-01：データガバナンス - 所有権/管理者責任」 文献[01]「DG-04：データガバナンス - 保持ポリシー」 文献[01]「DG-05：データガバナンス - 安全な廃棄」 文献[01]「DG-06：データガバナンス - 非運用データ」 文献[01]「DG-07：データガバナンス - 情報漏えい」 文献[01]「IS-07：情報セキュリティ - ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「IS-09：情報セキュリティ - ユーザーアクセスの無効化」 文献[01]「IS-10：情報セキュリティ - ユーザーアクセスの確認」 文献[01]「SA-03：セキュリティアーキテクチャ - データのセキュリティ/整合性」 文献[19]「Incident Management Model」	—	—	—	利用者は、Microsoft Online Services 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	・医療機関等の管理者が患者等への説明及び同意を得る際に、事業者が提供する情報の範囲、事業者の役割等について医療機関等と合意すること。	—	対象外	—	—	—	—	—	—	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	・連携ASP・SaaS事業者が提供するASP・SaaSサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】） ・ASP・SaaSサービスの提供に用いる情報システムが、情報セキュリティポリシーの要求を遵守していることを確認するため、定期的に点検・監査すること。（Ⅱ．4．3．2【基本】） ・自社において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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・監査記録等を医療機関等に開示する情報の範囲・条件等について合意すること。	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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。 お客様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	Office 365 および 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 Online Services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]などの公開資料を利用できることを確認した。	公開文書	文献[03]	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Microsoft Online Services 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	・ASP・SaaSサービスの提供に支障が生じた場合には、その原因が連携ASP・SaaS事業者に起因するものであったとしても、利用者と直接契約を結ぶASP・SaaS事業者が、その責任において一元的にユーザサポートを実施すること。（Ⅱ．8．1．1【基本】） ・医療機関等の管理者側からの問合せ窓口を設けること、また受付の時間帯等について、医療機関等と合意すること。	マイクロソフトは、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の提供に際して重要な業務を担当する再委託先を開示しています。顧客データへのアクセスを認める再委託先の追加に当たっては14日前に通知する旨を契約書に記載しています。これによりお客様は再委託先が実際の業務に就く前に調査し、問題がある再委託先があった場合の対応を行うことが可能です。 また、クラウドサービスの提供に関わる責任は、再委託先が行う業務範囲を含めてすべてマイクロソフトの責任であることを契約書に記載しています。	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。 NDA文書を確認したところ、お客様が日本国内でクラウドサービス契約を締結し、日本国内でプレミアサポート契約を締結することで、24時間日本語対応が提供されることを確認した。	要NDA	文献[65]（OST）	—	—	（マイクロソフト社とのNDAにより開示）	利用者は、Office 365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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
6.4-01		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競つかの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	・サーバルームやラックの鍵管理を行うこと。（Ⅲ．4．4．6【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】） ・バックアップ媒体も含め、個人情報を含むサーバ以外の機器・媒体等の保管場所を施錠管理すること。	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（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込み物、及び持出し物については、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、アラートがあがったりデータが暗号化されていることで、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]『FS-01：施設のセキュリティ - ポリシー』 文献[01]『FS-03：施設のセキュリティ - 管理されたアクセスポイント』	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	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。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】） ・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅲ．4．4．2【推奨】） ・委託業務に基づき受託する個人情報の内容を参照する必要が生じる場合には、データアクセスが可能な端末が設置されている部屋に対する入退出の施錠管理及び入退出管理を行うこと。	最低限	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お客様のアプリケーションや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。 公開文書	文献[01]『FS-01：施設のセキュリティ - ポリシー』 文献[01]『FS-03：施設のセキュリティ - 管理されたアクセスポイント』	（マイクロソフト社とのNDAにより開示）	–	–	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。
6.4-03				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。	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】）	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文書を確認したところ、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]『FS-01：施設のセキュリティ - ポリシー』 文献[01]『FS-03：施設のセキュリティ - 管理されたアクセスポイント』	（マイクロソフト社とのNDAにより開示）	–	（マイクロソフト社とのNDAにより開示）	利用者は、医療機関等の利用者側の施設について、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。	・サーバルームやラックの鍵管理を行うこと。（Ⅲ．4．4．6【基本】） ・受託する個人情報を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、Office 365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]『FS-01：施設のセキュリティ - ポリシー』 文献[01]『FS-08：施設のセキュリティ - 資産管理』	（マイクロソフト社とのNDAにより開示）	–	–	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。	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】）	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]『FS-01：施設のセキュリティ - ポリシー』 文献[01]『FS-03：施設のセキュリティ - 管理されたアクセスポイント』	（マイクロソフト社とのNDAにより開示）	–	–	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。	・重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。（Ⅲ．4．4．2【推奨】）	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、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]『FS-02：施設のセキュリティ - ユーザーアクセス』	（マイクロソフト社とのNDAにより開示）	–	–	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。	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	最低限	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。 Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。	適合可能	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[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開文書	文献[01]『SA-02：セキュリティアーキテクチャー - ユーザーID資格情報』 文献[17]	–	–	–	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。	・同上	最低限	–	対象外	–	–	–	–	–	–	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	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[17]では、多要素認証として電話による第2要素が使用でき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[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[17] 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で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。	・受託情報を扱う運用端末に、クリアスクリーン等の防止策を講じることを、自社の運用管理規程等に定めること。	最低限	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。	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]『IS-17：情報セキュリティ - 作業領域』	–	–	–	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	第三者認証等から頻推した内容	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	
6.5-05					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	・データベースに格納されたデータの暗号化を行うこと。（Ⅲ．2．2．2【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．3．2．2【推奨】） ・受託した情報の処理に必要な、システムに関する動作確認に際し、原則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こと。 ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化（SSL）、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.7.3）で、"メディアの取り扱い" が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では、トランスポート層、クライアントと Exchange Online 間の暗号化（SSL）、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで暗号化機能が提供されること、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management（IRM）機能やRights Management Services（RMS）機能を用いて暗号化できることが明記されている。 また、文献[01]では、非公開データを運用環境から非運用環境に移動またはコピーすることは、お客様の同意が得られた場合や、マイクロソフトの法務部門の指示による場合を除き、明示的に禁止されていることが明記されている。 文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint Onlineが、ファイル単位の暗号化機能を備えていることが明示されている。 NDAに基づく文書を確認した結果、標準に従って暗号鍵が管理されていることが確認できた。	公開文書	文献[01]「IS-18：情報セキュリティ－ 暗号化」 文献[01]「IS-19：情報セキュリティ－ 暗号化キーの管理」 文献[01]「DG-06：データ ガバナンス － 非運用データ」 文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利した保存データの高度な暗号化」	－	－	（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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・提供するサービスにおいて、医療機関等の利用者の職種、担当業務等に応じたアクセス制御が可能な機能を含めること。 ・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関しては、医療機関等の管理者と協議の上、実際に設定する作業に関する役割も含めて合意すること。 ・医療機関等のアクセス管理に関する運用管理規程の内容に従った運用を行い、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こと。	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 Online Services 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。 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 Online Services 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上で付与されます。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。 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。 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。 Office 365 サービスでは、異なるホスティング サービスの開発スタッフや運用スタッフが、職務分離の原則に従うようにすることができます。ソース コード、ビルド サーバー、および運用環境に対するアクセスは、厳しく制御されています。 例: ☐ Office 365 サービスの運用環境に対するアクセスは運用担当者に制限されます -開発チームとテスト チームには、運用環境内から提供された情報に対してアクセス権が与えられる場合があり、問題のトラブルシューティングに役立てることができます。 ☐ Office 365 サービスのソース コード管理に対するアクセスはエンジニアリング担当者に制限され、運用担当者がソース コードを変更することはできません。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、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、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Microsoft Online Services 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、およ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 Online Services 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[23]では、Office365上のコンテンツに対するエンドユーザのアクセスは、利用者側で設定する権限設定によりコントロールされていることを示している。	公開文書	文献[01]「IS-07：情報セキュリティ－ ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ ユーザーアクセスの確認」 文献[23]	－	－	－	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。
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	・ASP・SaaS 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（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．1．1．5【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】※ベストプラクティス(i)を実施すること。）	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人によるアクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期間は 既定で30日間 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。	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[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 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Lockbox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。	公開文書要NDA	文献[01]「IS-14：セキュリティアーキテクチャー － 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・運用管理者とログのレビュー者のアクセス権を分離する等の、アクセスログの改ざん等に対する措置を講じること。		適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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 Online Services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]では、情報システム監査ツールへのアクセスは、Microsoft Online Services 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できるようにしていることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ/整合性」 文献[01]「IS-29：情報セキュリティ－ 監査ツールへのアクセス」	－	－	－	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	・ASP・SaaS 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（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。（Ⅲ．1．1．5【基本】※ベストプラクティスの(i)～(iv)を実施すること）	Office365 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、Office365 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 Office 365 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 Online Services 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 Online Services 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。	公開文書	文献[01]「SA-12：セキュリティアーキテクチャ － 時刻の同期」	－	－	－	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、外部からの情報受領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	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器についての技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．1．1．6【基本】） ・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．2．2．1【基本】）	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてウイルスがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。関連するサービスの説明やサービス レベル契約（SLA）に、その他の情報が記載されている場合があります。 マイクロソフトは独自のセキュリティ レスポンス センター（MSRC）を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。 詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4）で、"悪意のあるコードからの保護" が規定されています。 Office 365 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。 Office 365 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。 https://www.microsoft.com/en-us/TrustCenter/Security/Office365Security	適合可能	文献[01]には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。 また、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、および教訓の学習）により対応することが明示されている。 文献[10]および文献[11]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。	公開文書	文献[01]「IS-21：情報セキュリティ－ ウイルス/悪意のあるソフトウェアへの対策」 文献[01]「IS-22：情報セキュリティ－ インシデント管理」 文献[10] 文献[11]	（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、利用する端末について、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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
6.5-11					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（最長でも2 ヶ月以内※D.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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限と最小文字数が割り当てられます。Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 【基本】 ・自社において定めた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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・利用者のパスワード発行等に関する手続及び業務範囲について、医療機関等と合意すること。	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。 Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。	適合可能	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[17]では、多要素認証として電話による第2要素が使用できることが明示されている。 またインタビュー等を通じて、以下のソリューションを追加することにより、システム的な制限を追加的に実施できることを確認した。 ・Azure Active Directory (Azure AD) 及び Active Directory Federation Services (AD FS) を使用し、組織が管理するオンプレミスの Active Directory (AD) との間でフェデレーション関係を確立することにより、オンプレミスの組織アカウントによって Microsoft Office 365 Online 上のサービスに対するログインが可能となること ・パスワードの管理ポリシーはオンプレミスのADによって制御可能であること	要NDA	文献[01]「SA-02：セキュリティアーキテクチャー－ユーザーID資格情報」 文献[17]	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、Microsoft Online Services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行うこと。 (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「一般利用者が安心して無線LAN を利用するために」や「企業等が安心して無線LAN を導入・運用するために」を参考にすること。	最低限	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策について、事業者の役割、範囲等について合意すること。	—	対象外	—	—	—	—	—	—	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	—	—	—	—	—	—	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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．4．2．1【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・医療情報について、医療機関等が行う情報資産分類の区分に従い、アクセス制御を行うこと。	—	対象外	—	—	—	—	—	—	利用者及びSI事業者は、情報資産の区分管理を適切に実施する必要がある。
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	・最低限3.と同様の対応を行う。	いずれかの Office 365 Web アプリに認証すると、使用中のブラウザーと Office 365 Web アプリの間でセッションが確立されます。セッションの期間中は、Web アプリを再認証する必要はありません。ユーザーが非アクティブである場合、ユーザーがブラウザーまたはタブを閉じた場合、またはパスワード再設定などのその他の理由により認証トークンが期限切れになった場合に、セッションが期限切れにな る可能性があります。Office 365 のさまざまな Web アプリには、それぞれ異なるセッション タイムアウトが設定されています。既定のタイムアウト値は、アプリの通常時の使用法と合致します。	適合可能	文献[95]では、Office365のサービス毎にセッションタイムアウトの時間が定められていることが明示されている。	公開文書	文献[95]	—	—	—	—
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	・データベースに格納されたデータの暗号化を行うこと。（Ⅲ．2．2．2【推奨】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．3．1．4【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPSの導入等）を講じること。（Ⅲ．3．1．5【推奨】）	データの保存や処理は、Active Directory® 構造と、特にマルチテナント環境の構築、管理、安全確保に役立てるために開発された各種機能によって、同じサービスのお客様の間で論理的に分離されます。 マルチテナント セキュリティ アーキテクチャーにより、共有の Office 365 データ センターに格納されているお客様のデータが、他の組織によってアクセスされたり他の組織に漏えいしたりすることのないようにしています。Active Directory における組織単位 (OU) により、共有システム リソースを介した許可されていない不適の情報転送を制御および防止します。テナントは、Active Directory を介して論理的に適用されるセキュリティ境界（サイロ）に基づいて相互に分離されます。 ISO 27001 規格（具体的には付属文書 A の項 10.6.2）で、“ネットワーク サービスのセキュリティ” 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。 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、Office 365 データ センター内のネットワークは、複数の層別のネットワーク セグメントを作成するように設計されており重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できること、顧客とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されデスクトップとデータ センターの間でデータの機密性や整合性が確保されること、Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケットレベルでのセキュリティが実現でき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。	公開文書	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[27]	—	—	—	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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・自社において定めた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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	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 Online Service 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 Online Services 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、以下の事項を確認した。 ・Azure Active Directory (Azure AD) 及び Active Directory Federation Services (AD FS) を使用し、組織が管理するオンプレミスの Active Directory (AD) との間でフェデレーション関係を確立することにより、オンプレミスの組織アカウントによって Azure 上のサービスに対するログインが可能となること ・パスワードの入力不成功時における挙動はオンプレミスのADによって制御可能であること	要NDA	—	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、Microsoft Online Services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。
6.5-18					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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・採用する認証手段・方式について、医療機関等と合意すること。	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365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。	適合可能	文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開文書	文献[17]	—	—	—	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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	
6.5-19					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	・医療機関等がASP・SaaSの利用に際して無線LANを利用する場合に、医療機関等の無線LANが必要なセキュリティ対策についての、事業者の役割、範囲等について合意すること。	–	対象外	–	–	–	–	–	–	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	–	–	–	–	–	–	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	-	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	(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	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．2【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．5．1．1【基本】）	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、定期健康診断を進んで受ける義務や、健康的な労働環境を確保する事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従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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文書を確認したところ、ISO/IEC 27001のA8.1.2 選考」に準拠する記載があり、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]「HR-02：人的資源のセキュリティ－雇用における合意事項」 文献[01]「IS-11：情報セキュリティ・トレーニング／意識向上」 文献[65](OST)	（マイクロソフト社とのNDAにより開示）	–	（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、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					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	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．5．2．1【基本】）	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなってい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、当社の従業員との契約に機密保持条項を組み込んでいます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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。 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。 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]「HR-02：人的資源のセキュリティ－雇用における合意事項」「IS-11：情報セキュリティ・トレーニング／意識向上」 文献[01]「RS-03：復元－ビジネス継続性の計画」	（マイクロソフト社とのNDAにより開示）	（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、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	・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．5．3．1【基本】）	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に通知されていることが記載されている。	公開文書	文献[01]「IS-27：情報セキュリティ－資産の返却」	–	–	–	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。
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	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・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こと。（Ⅲ．4．4．3【基本】）	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 Office 365 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、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]「FS-01：施設のセキュリティ－ポリシー」 文献[01]「FS-02：施設のセキュリティ－ユーザーアクセス」	–	–	–	–
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	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．2【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．5．1．1【基本】）	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、定期健康診断を進んで受ける義務や、健康的な労働環境を確保する事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従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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。 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。 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]「HR-02：人的資源のセキュリティ－雇用における合意事項」「IS-11：情報セキュリティ・トレーニング／意識向上」 文献[01]「RS-03：復元－ビジネス継続性の計画」	（マイクロソフト社とのNDAにより開示）	–	（マイクロソフト社とのNDAにより開示）	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応						SI事業者・利用者で必要な対応
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	
6.6-06					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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】）	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。 Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されています。可能な場合、独立したプロジェクトごとに、ソース コード ライブラリに対して個別のプロジェクト ワークスペースを確保しています。 Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフは、自身の業務の遂行のためにアクセスする必要があるワークスペースにのみ、アクセス権限が与えられます。ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されます。 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。 Office 365 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。 マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス (代理人による アクセス、共有メールボックスへのアクセスなど) を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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。	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、Microsoft Online Services 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、およ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は自身の業務の遂行のためにアクセスする必要があるワークスペースにのみアクセス権限が与えられることが明示されている。	要NDA	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー－データのセキュリティ/整合性」	－	（マイクロソフト社とのNDAにより開示）	－	－
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	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・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こと。（Ⅲ．4．4．3【基本】）	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 Online 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、Office 365 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。 NDA文書を確認したところ、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]「FS-01：施設のセキュリティ－ポリシー」 文献[01]「FS-02：施設のセキュリティ－ユーザーアクセス」 文献[01]「FS-03：施設のセキュリティ－管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	－	（マイクロソフト社とのNDAにより開示）	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							
評価項目番	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	第三者認証等から頻推した内容	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
6.6-08					④ 委託事業者が再委託を行う旨が否かを明確にし、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	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．2．2．1【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．2．2．2【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．3．1．1【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】） ・外部組織に対して再委託等を行う場合には、事前に医療機関等の管理者に対して説明を行い、契約において体制を明確にすること。 ・外部組織に対して、自社と同等の個人情報保護指針等について遵守させること。 ・外部組織においても表3-9（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におけるASP・SaaS事業者への要求事項）について遵守させること。	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 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 Online Services は契約に基づき、サード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求し、かつ年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求していることが明記されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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 ・Microsoft が下請業者に対して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すること ・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ること 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文書を確認したところ、サードパーティによるサービス、レポート、およ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]『CO-03：コンプライアンス – サードパーティの監査』 文献[02]『顧客データが下請業者に開示される場合』 文献[42] 文献[02]『Microsoft のプライバシー要件』	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–
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	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．2【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．2．2．1【基本】） ・情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。（Ⅱ．2．2．2【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．5．1．1【基本】）		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従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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文書を確認したところ、ISO/IEC 27001のA8.1.2 選考」に準拠する記載があり、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]『HR-02：人的資源のセキュリティ－雇用における合意事項』 文献[01]『IS-11：情報セキュリティ－トレーニング／意識向上』 文献[65](OST)	（マイクロソフト社とのNDAにより開示）	–	（マイクロソフト社とのNDAにより開示）	–
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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．4．2．1【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	–	対象外	–	–	–	–	–	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と、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	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】）	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 Online Services 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。 機器及び破棄手順については、Microsoft Online Services 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	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 Online Services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。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。 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、Microsoft Online Services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。 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およ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。 文献[73]では、連邦法、各国法の法令遵守を含めた行動規範を策定・表明していることが明示されている。	要NDA	文献[01]『DG-05：データ ガバナンス – 安全な廃棄』 文献[06]4.4物理セキュリティ 文献[65](OST)『セキュリティ』 文献[73]	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	SI事業者側では、利用者（ビジネス パートナー）に対して、Microsoft Online Services 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	・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・情報の破棄を実施した場合に、電磁記録媒体の消磁、物理的破壊等、情報の削除方法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こと。								
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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・自社において定めた情報の破棄手順が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。								

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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	
6.8-01		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	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．3．1．1【基本】） ・雇用予定の従業員に対して、機密性・完全性・可用性に係る情報セキュリティ上の要求及び責任の分界点を提示・説明するとともに、この要求等に対する明確な同意をもって雇用契約を締結すること。（Ⅱ．5．1．1【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・受託した情報の処理に必要な、システムの動作確認に際し、原則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こと ・システムに関する動作確認に際し、やむを得ず受託した個人情報を使用する場合には、医療機関等の管理者と十分協議の上、必要な措置を講じて使用すること。	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 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 Online Services は契約に基づき、サード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求し、かつ年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求していることが明記されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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 ・Microsoft が下請業者に対して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すること ・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ること 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文書を確認したところ、サードパーティによるサービス、レポート、およ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 Online Services がスポンサーとなってい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[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 Online Services 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。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。	要NDA	文献[01]「CO-03：コンプライアンス – サードパーティの監査」 文献[01]「DG-05：データ ガバナンス – 安全な廃棄」 文献[01]「HR-02：人的資源のセキュリティ – 雇用における合意事項」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	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模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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	Office 365 サービスでは、異なるホスティング サービスの開発スタッフや運用スタッフが、職務分離の原則に従うようにすることができます。ソース コード、ビルド サーバー、および運用環境に対するアクセスは、厳しく制御されています。 例: □ Office 365 サービスの運用環境に対するアクセスは運用担当者に制限されます。開発チームとテスト チームには、運用環境内から提供された情報に対してアクセス権が与えられる場合があり、問題のトラブルシューティングに役立てることができます。 □ Office 365 サービスのソース コード管理に対するアクセスはエンジニアリング担当者に制限され、運用担当者がソース コードを変更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 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 規格を確認することをお勧めします。 標準的な運用手順が、正式に文書化され、、Microsoft Online Services 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。 スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 · マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。 マイクロソフトは独自のセキュリティ レスポンス センター (MSRC) を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx を参照してください。 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 Online Services 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。 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 Online Services 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。 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。 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、Microsoft Online Services 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、およ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[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[01]にて、Microsoft Online Services では、マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されることを確認した。 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、すべてのサービスおよ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[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 Oniline Services では、トランスポート層、クライアントとExchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで暗号化機能が提供されること、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明記されている 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]「IS-08：情報セキュリティ – ユーザーアクセスの制限/承認」 文献[01]「IS-09：情報セキュリティ – ユーザー アクセスの無効化」 文献[01]「IS-10：情報セキュリティ – ユーザーアクセスの確認」 文献[01]「IS-18：情報セキュリティ – 暗号化」 文献[01]「IS-19：情報セキュリティ – 暗号化キーの管理」 文献[01]「IS-21：情報セキュリティ – ウイルス/悪意のあるソフトウェアへの対策」 文献[01]「SA-02：セキュリティ アーキテクチャ – ユーザー ID 資格情報」 文献[01]「SA-07：セキュリティアーキテクチャ – リモート ユーザーの多要素認証」 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[131] 文献[31] 文献[63] 文献[65](OST)	—	（マイクロソフト社とのNDAにより開示）	—	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。 利用者が使用する端末におけ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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．3．2．1【基本】）	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 Online Services 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。 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 Online Services 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。 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。 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。								

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
6.8-04					保守要員の離職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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．2．2．1【基本】） ・従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。（Ⅱ．5．3．1【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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、内容等について合意すること。	マイクロソフトは独自のセキュリティレスポンス センター (MSRC) を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4) で、"悪意のあるコードからの保護" 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]にて、Microsoft Online Services では年に 1 度、ビジネスへの影響分析として、下記の項目を実施していることが明記されている。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 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。 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]『DG-08：データ ガバナンス – リスク評価』 文献[01]『IS-09：情報セキュリティ – ユーザー アクセスの無効化』 文献[01]『IS-21：情報セキュリティ – ウイルス／悪意のあるソフトウェアへの対策』	–	（マイクロソフト社とのNDAにより開示）	–	利用者が使用する端末におけ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	・サービス提供に必要な保守業務を行うに際して、医療機関等の管理者に対して書面等により作業の事前及び事後に通知を行うこと、及び事前の了解を必要とする作業等について医療機関等と合意すること。								
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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・サービス提供に際して、医療機関等と守秘義務契約を締結すること。	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。	適合可能	文献[01]にて、リスク管理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]『RI-04：リスク管理 – ビジネス／ポリシーの変更の影響』 文献[65](OST)	–	–	–	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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	–	対象外	–	–	–	–	–	–	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。
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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・サービス提供に必要なシステムの保守をリモートメンテナンスで行う場合の医療機関等の管理者に対する報告、承認等について、医療機関等と合意すること。	マイクロソフト データセンターあるい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、関連するお客様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。 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。そのためお客様がデータセンターに立ち入ったとしても、お客様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お客様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。 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 Online Services 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。 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 Online Services 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。 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。 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、Microsoft Online Services 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、およ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[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。 また、インタビュー等を通じて、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていることが確認できた。	要NDA	文献[01]『IS-07：情報セキュリティ – ユーザーアクセスポリシー』 文献[01]『IS-10：情報セキュリティ – ユーザーアクセスの確認』 文献[01]『IS-08：情報セキュリティ – ユーザーアクセスの制限／承認』 文献[01]『SA-14：セキュリティアーキテクチャー – 監査ログ／侵入検出』 文献[131] 文献[65](OST)	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、Microsoft Online Services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	・外部組織が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。（Ⅱ．2．2．1【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携ASP・SaaS 事業者によって確実に実施されることを担保すること。（Ⅱ．3．1．1【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】）	マイクロソフトは、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の提供に際して重要な業務を担当する再委託先を開示しています。顧客データへのアクセスを認める再委託先の追加に当たっては14日前に通知する旨を契約書に記載しています。これによりお客様は再委託先が実際の業務に就く前に調査し、問題がある再委託先があった場合の対応を行うことが可能です。 また、クラウドサービスの提供に関わる責任は、再委託先が行う業務範囲を含めてすべてマイクロソフトの責任であることを契約書に記載しています。	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 Online Services では年に 1 度、ビジネスへの影響分析として、下記の項目を実施していることが明記されている。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 文献[01]によると、Microsoft Online Services は契約に基づき、サード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求し、かつ年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求していることが明記されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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□すること ・下請業者はそれ以外の□的のために顧客データを使□することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対して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すること ・Microsoft によって管理されている施設や機器で業務を□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ること 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。 また、NDA文書を確認したところ、サードパーティによるサービス、レポート、およ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。	公開文書	文献[01]『CO-03：コンプライアンス – サードパーティの監査』 文献[01]『DG-08：データ ガバナンス – リスク評価』 文献[02]『顧客データが下請業者に開□される場合』 文献[02]『Microsoft のプライバシー要件』 文献[42] 文献[65](OST)	–	–	–	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 Microsoft Online Services との連携部分について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						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応						SI事業者・利用者で必要な対応
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	
6.8-10					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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】）	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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。 お客様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	文献[01]では、Microsoft Online Services 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、およ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[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。	要NDA	文献[01]『IS-07：情報セキュリティ－ユーザーアクセスポリシー』 文献[01]『IS-10：情報セキュリティ－ユーザーアクセスの確認』 文献[01]『IS-08：情報セキュリティ－ユーザーアクセスの制限／承認』 文献[01]『SA-14：セキュリティアーキテクチャー－監査ログ／侵入検出』 文献[131] 文献[65](OST)	－	（マイクロソフト社とのNDAにより開示）	－	－
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	・サービス提供に必要な保守業務を医療機関施設内で行う際に、医療機関等の立会いの下で実施する旨を、医療機関等と合意すること。	マイクロソフトは独自のセキュリティ レスポンス センター (MSRC) を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4）で、"悪意のあるコードからの保護" 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	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		－	（マイクロソフト社とのNDAにより開示）	－	－
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	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．2【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】）	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフは、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従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフは、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]『HR-02：人的資源のセキュリティ－雇用における合意事項』 文献[01]『IS-11：情報セキュリティ－トレーニング／意識向上』	－	－	－	－
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	・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・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、医療機関等の管理者による監査の内容、範囲について、医療機関等と合意すること。	マイクロソフト データセンター あるい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、関連するお客様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。 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。そのためお客様がデータセンターに立ち入ったとしても、お客様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お客様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。 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 Online Services 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。 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 Online Services 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。 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、Microsoft Online Services 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、およ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[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。 また、インタビュー等を通じて、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていることが確認できた。	要NDA	文献[01]『IS-07：情報セキュリティ－ユーザーアクセスポリシー』 文献[01]『IS-10：情報セキュリティ－ユーザーアクセスの確認』 文献[01]『IS-08：情報セキュリティ－ユーザーアクセスの制限／承認』 文献[01]『SA-14：セキュリティアーキテクチャー－監査ログ／侵入検出』 文献[131] 文献[65](OST)	－	（マイクロソフト社とのNDAにより開示）	－	－
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	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】）	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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。 お客様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	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、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていることが確認できた。	要NDA	文献[131]	－	（マイクロソフト社とのNDAにより開示）	－	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
6.9-01		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いえる。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時有のリスクである。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。	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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策を適切に実施する必要がある。
6.9-02					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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・情報の持ち出しに関する自社において定めた運用管理規程が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】） ・自社において定めた機器・媒体の盗難、紛失が生じた際の対応についての手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．5．2．1【基本】） ・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．5．2．2【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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6.5 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	・運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。従業員等が用いる運用管理端末の全てのファイルのウイルスチェックを行うこと。技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．5．2．1【基本】） ・受託した情報を可搬媒体により外部に持ち出し、受託情報の処理を行わない旨を、自社の運用管理規程等に含め、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．5．2．1【基本】） ・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．5．2．2【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】）	－	対象外	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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	－	－	－	－	－	－	利用者は、情報および情報機器の持ち出しに関する対策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						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項目番	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	
6.10-01		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 はホ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」に掲げ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 や緊急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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．4．2．1【基本】） ・<u>自社において定めた非常時におけるBCPに関する運用手順等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。</u>	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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。 ・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。 ビジネスの影響分析が適切な間隔で実行され、確認されます。次のような分析を行います。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 標準的な運用手順が、正式に文書化され、Microsoft Online Services 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 Online Services では、Office 365 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、およびトラブルシューティング用の資料を用意しています。 管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 ・ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 ・Exchange 管理者向けのビデオ ・ハイブリッド環境の構成に必要な記事および手順 ・ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki ・停止や問題に関する情報が得られる、サービスの正常性ダッシュボード 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、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。 ビジネスの影響評価、依存関係の分析、およびリスク評価は、少なくとも年に一度、実施または更新されます。お客様は、アプリケーションおよび設計に対する影響を分析し、目標復旧時間 (RTO) と目標復旧時点 (RPO) の要件を満たしていることを確認する責任を負います。	適合可能	文献[01]では、Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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ることが明示されている。 文献[01]では、Microsoft Online Services 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」「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。 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ないことを確認した。 NDA文書を確認したところ、コンティンジェンシープランと同等なBCP対策が規程されており、定期的に検証され、見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]「RS-01：復元・管理プログラム」 文献[01]「RS-03：復元・ビジネス継続性の計画」 文献[01]「RS-04：復元－ビジネス継続性のテスト」	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	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。 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	同上	Microsoft Office 365 のサービスは、高水準のサービスを維持できる回復力の高いシステムで提供されています。サービス継続性のための対策は、Office 365 のシステム設計の一部です。これらの対策により、Office 365 は、ハードウェアやアプリケーションの障害、データ破損、ユーザーに影響を与えるその他のインシデントといった予期せぬイベントから迅速に復旧できます。サービス継続性ソリューションは、重大なサービス停止（たとえば、自然災害やインシデントによって、ある Microsoft のデータ センター全体が使用不能になった場合など）の際にも適用されます。 致命的な障害から復旧した後、データ センターの完全な冗長性がサービスに復元されるまで一定の時間がかかります。たとえば、データ センター 1 に障害が発生すると、サービスがデータ センター 2 のリソースによって復元されます。ただし、データ センター 1 の復元されたリソースまたはデータ センター 3 の新規リソースによって、データ センター 2 のサービスの継続性がサポートされるまで時間がかかります。Office 365サービス レベル契約 (SLA) は、この期間に適用されます。 Office 365 の開発および運用チームは、お客様にビジネス継続性を提供するうえで重要な役割を担う専門の Office 365 サポート組織にサポートされています。サポート スタッフはサービスおよびサービスに関連するアプリケーションに精通しており、Microsoft 社内のアーキテクチャ、開発、テストの専門家と直接やり取りします。 サポート組織は運用および製品開発チームと密接に協力することで、迅速な問題解決を実現し、お客様の声を反映するための窓口になります。お客様からのフィードバックは、計画、開発、運用プロセスに役立てられます。	適合可能	文献[11]では、Microsoft Office365におけるサービス継続性のための対策が取られており、また利用者との窓口として専門のサポート組織が情報提供を行うことが明示されている。	公開文書	文献[11]	–	–	–	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。	・<u>自社において定めた非常時におけるアクセス管理の対応方法の内容（非常時用のユーザアカウントに関する内容含む）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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。</u>	最低限	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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。 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 Office 365 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。 ビジネスの影響分析が適切な間隔で実行され、確認されます。次のような分析を行います。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 標準的な運用手順が、正式に文書化され、Microsoft Online Services 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 Online Services では、Office 365 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、およびトラブルシューティング用の資料を用意しています。 管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 ・ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 ・Exchange 管理者向けのビデオ ・ハイブリッド環境の構成に必要な記事および手順 ・ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki ・停止や問題に関する情報が得られる、サービスの正常性ダッシュボード 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、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。 ビジネスの影響評価、依存関係の分析、およびリスク評価は、少なくとも年に一度、実施または更新されます。お客様は、アプリケーションおよび設計に対する影響を分析し、目標復旧時間 (RTO) と目標復旧時点 (RPO) の要件を満たしていることを確認する責任を負います。	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、Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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ることが明示されている。 文献[01]では、Microsoft Online Services 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」「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。 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]「RS-01：復元・管理プログラム」 文献[01]「RS-03：復元・ビジネス継続性の計画」 文献[01]「RS-04：復元－ビジネス継続性のテスト」	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者が使用する端末については、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						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項目番	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	第三者認証等から頻推した内容	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	
6.10-04					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 サイトが何者かに改ざんされた、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）	・ASP・SaaS 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、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に連絡を通知すること。（Ⅲ．1．1．1【基本】） ・ASP・SaaS 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、情報セキュリティ対策機器、通信機器の障害監視（サービスが正常に動作していることの確認）を行うこと。障害を検知した場合は、利用者に連絡を通知すること。（Ⅲ．1．1．2【基本】） ・ASP・SaaS 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、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．1．1．3【推奨】） ・ASP・SaaS 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（情報セキュリティ対策機器、通信機器等）に係る稼働停止、障害、パフォーマンス低下等について、速報をフォローアップする追加報告を利用者に対して行うこと。（Ⅲ．1．1．8【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．3．2．5【推奨】） ・所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS 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適用が及ぶ場所に設置すること。	最低限	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。 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。 マイクロソフトでは、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、CPU 使用率、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があることが明示されている。 NDA文書で確認したところ、日本でOffice 365の契約をする場合、準拠法は日本法であることが確認できた。 またインタビュー及びNDA文書で確認したところ、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が確認できた。	適合可能	文献[01]では、Microsoft Online において、電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動などの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プロセスを開発していることが明示されている。 また、不正アクセス検知時およ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。 また、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、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があることが明示されている。 NDA文書で確認したところ、日本でOffice 365の契約をする場合、準拠法は日本法であることが確認できた。 またインタビュー及びNDA文書で確認したところ、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が確認できた。	要NDA	文献[01]『IS-22：情報セキュリティインシデント管理』 文献[01]『OP-03：運用管理 – 容量/リソース計画』 文献[130]	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	所管官庁への連絡は利用者側で実施する必要がある。 利用者が使用する端末については、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。
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閉域ネットワークの採用に期待して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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御などなりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．3．1．4【基本】） ・不正な通過パケットを自動的に発見、もしくは遮断する措置（ID/IPSの導入等）を講じること。（Ⅲ．3．1．5【推奨】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．3．2．1【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．3．2．2【推奨】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．3．2．3【基本】） ・医療機関等がASP・SaaSを利用するネットワークにつき、ウイルスや不正なメッセージの混入等による改ざんに対する防止措置についての事業者の役割の範囲について医療機関等と合意すること。	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。 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。 マイクロソフトでは、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、CPU 使用率、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。 ISO 27001 規格（具体的には付属文書 A の項 10.3.1）で、"容量管理" が規定されています。	適合可能	文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 文献[01]では、Microsoft Online Services において、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行されていることが明記されていることを確認した。 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[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 Online Services 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、およ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。 文献[01]にて、Office 365 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 サーバーやストレージ 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、TLS/SSL の使用によりデスクトップとデータ センターの間でデータの機密性や整合性が確保されること、Office 365 サービス ネットワークの終端でルーターをフィルタリングすることによりOffice 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現できることが明記されている。 文献[31]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]『IS-07：情報セキュリティ – ユーザーアクセスポリシー』 文献[01]『IS-08：情報セキュリティ – ユーザーアクセスの制限/承認』 文献[01]『IS-10：情報セキュリティ – ユーザーアクセスの確認』 文献[01]『IS-18：情報セキュリティ – 暗号化』 文献[01]『IS-21：情報セキュリティ – ウイルス/悪意のあるソフトウェアへの対策』 文献[01]『SA-02：セキュリティ アーキテクチャ – ユーザー ID 資格情報』 文献[01]『SA-09：セキュリティ アーキテクチャ – 分離』 文献[31] 文献[31] 文献[63]	–	–	–	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。 端末側で使用する暗号鍵は、第三者に解読されたり漏洩することを、利用者が対策を講じる必要がある。 利用者が使用する端末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SI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。	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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御などなりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．3．2．3【基本】） ・ASP・SaaSを利用するネットワークで用いられる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、医療機関等から事業者までの確認を行うこと（但し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本項の対応を適用せず、別途なりすましを防止する策を講じること）。 ・厚生労働省ガイドライン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を確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化でき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 Online Services 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、およ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。 さらにインタビューにて、Express Routeにて接続される場合であっても、httpsによる通信の暗号化が行われていること、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[01]『IS-07：情報セキュリティ – ユーザーアクセスポリシー』 文献[01]『IS-08：情報セキュリティ – ユーザーアクセスの制限/承認』 文献[01]『IS-10：情報セキュリティ – ユーザーアクセスの確認』 文献[01]『IS-18：情報セキュリティ – 暗号化』 文献[01]『SA-02：セキュリティ アーキテクチャ – ユーザー ID 資格情報』 文献[31] 文献[63]	–	（マイクロソフト社とのNDAにより開示）	–	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。	表3-3参照のこと	最低限	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365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。 スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 ・マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。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。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。	適合可能	文献[17]では、多要素認証として電話による第2要素が使用でき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[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[17] 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	・不正な通過パケットを自動的に発見、もしくは遮断する措置（IDS/IPSの導入等）を講じること。（Ⅲ．3．1．5【推奨】） ・ASP・SaaSを利用するネットワークで用いられるルータ等のネットワーク機器が厚生労働省ガイドラインで求める安全性が確認されているものであること、ASP・SaaSを利用する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、これを経由して医療機関等の施設間を結ぶ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等に関して、事業者の役割、範囲を医療機関等と合意すること。	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出来た。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	–	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応						SI事業者・利用者で必要な対応
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	
6.11-05					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	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．3．2．2【推奨】） ・ASP・SaaSにおいて送受信される データに対して、電子政府推奨の暗号を用いた暗号化等によるセキュリティ対策を講じること。 ・暗号化によるセキュリティ対策が、医療機関等が求める水準を満たすものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	業界標準のトランスポート層セキュリティ（TLS）/SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/ SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。	適合可能	文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。 また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 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]「IS-18：情報セキュリティ－暗号化」	—	（マイクロソフト社とのNDAにより開示）	—	—
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。	最低限	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上遵守な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．3．2．4【基本】） ・通常運用時、緊急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を明確にし、事業者の負う責任の範囲、役割等について、医療機関等と合意すること。 ・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、各種責任に関し、事業者が負う責任の範囲、役割等について、医療機関等と合意すること。	運営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。 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し、SLA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、マイクロソフトはお客様に協力します。お客様による監査について、お客様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、対象となるお客様、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、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。 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 Online Services 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 Online Services 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。 お客様は、Online Service で使用する場合にのみソフトウェアをインストールして使用することができます。Online Service 固有の条件により、お客様が使用できる本ソフトウェアの部数またはお客様が本ソフトウェアを使用できるデバイスの数が制限される場合があります。お客様のソフトウェア使用権は、Online Service のアクティベーション時に開始し、お客様の Online Service の使用権が終了したときに終了します。お客様の本ソフトウェアの使用権が終了した場合、お客様は本ソフトウェアをアンインストールしなければなりません。お客様の本ソフトウェアの使用権が終了した時点で、マイクロソフトはお客様による本ソフトウェアの使用を無効にすることができます。	適合可能	文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。 また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 文献[01]にて、リスク評価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]、文献[66]およびNDA文書では、提供事業者として必要な基本的な事項が規定・明記され、インタビューの結果を含め、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[73]では、連邦法、各国法の法令遵守を含めた行動規範を策定・表明していることが明示されている。 文献[01]では、Microsoft Online Services 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、およ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。 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]、文献[66]およびNDA文書では、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]および文献[66]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、問合せ対応、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]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-18：情報セキュリティ－暗号化」 文献[01]「RI-04：リスク管理 － ビジネス／ポリシーの変更の影響」 文献[01]「SA-14：セキュリティアーキテクチャー－監査ログ/侵入検出」 文献[131] 文献[65](OST) 文献[66](SLA) 文献[73]	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	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、Microsoft Online Services の契約書および使用条件を確認し、Microsoft Online Services 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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．3．1．4【基本】）	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365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。 スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 ・マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。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。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。 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、すべてのサービスおよ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[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 Online Services 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、およ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。 文献[01]にて、Office 365 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 サーバーやストレージ 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、TLS/SSL の使用によりデスクトップとデータ センターの間でデータの機密性や整合性が確保されること、Office 365 サービス ネットワークの終端でルーターをフィルタリングすることによりOffice 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現できることが明記されている。	要NDA	文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」 文献[01]「SA-07：セキュリティアーキテクチャー－リモートユーザーの多要素認証」 文献[01]「SA-02：セキュリティ アーキテクチャ－ ユーザー ID 資格情報」 文献[01]「SA-09：セキュリティアーキテクチャ－分離」 文献[31] 文献[63]	—	（マイクロソフト社とのNDAにより開示）	—	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項番	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	
6.11-08					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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ASP・SaaS 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・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．2．1．4【推奨】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．3．2．4【基本】） ・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、役割等について、医療機関等と合意すること。	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。 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し、SLA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、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。 マイクロソフトでは、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、CPU 使用率、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。 マイクロソフトのセキュリティ レスポンス センター (MSRC) 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 Online Services 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 Online Services 全体で主導します。	適合可能	文献[01]では、Microsoft Online Services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、インタビュー等を通じて、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[66]およびNDA文書では、提供事業者として必要な基本的な事項が規定・明記され、インタービューの結果を含め、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]、文献[66]およびNDA文書では、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[73]では、連邦法、各国法の法令遵守を含めた行動規範を策定・表明していることが明示されている。 文献[65]および文献[66]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、問合せ対応、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]「IS-20：情報セキュリティ－ 脆弱性/更新プログラム管理」 文献[07]「FAQ37」 文献[65](OST) 文献[66](SLA) 文献[73]	―	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	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SSL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の納得できる説明を実施し、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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・外部及び内部からの不正アクセスを防止する措置（ファイアウォール、リバースプロキシの導入等）を講じること。（Ⅲ．3．1．4【基本】） ・患者が情報を閲覧する情報システムの安全性に関する説明責任等において、事業者は責任の範囲、役割等について、医療機関等と合意すること。	暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明書を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.7.3）で、“メディアの取り扱い” が規定されています。 Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。 Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 データの保存や処理は、Active Directory® 構造と、特にマルチテナント環境の構築、管理、安全確保に役立てるために開発された各種機能によって、同じサービスのお客様の間で論理的に分離されます。 マルチテナント セキュリティ アーキテクチャーにより、共有の Office 365 データ センターに格納されているお客様のデータが、他の組織によってアクセスされたり他の組織に漏えいしたりすることのないようにしています。Active Directory における組織単位 (OU) により、共有システム リソースを介した許可されていない不適の情報転送を制御および防止します。テナントは、Active Directory を介して論理的に適用されるセキュリティ境界 (サイロ) に基づいて相互に分離されます。 ISO 27001 規格（具体的には付属文書 A の項 10.6.2）で、“ネットワーク サービスのセキュリティ” が規定されています。 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]によると、Microsoft Oniline Services では、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで暗号化機能が提供されること、保存時（静止状態）には標準 (または暗号化されない) が、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明記されている。 文献[44]では、SharePoint Online が、ファイル単位の暗号化機能を備えてい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[17]では、多要素認証として電話による第2要素が使用できることが明示されている。 文献[01]では、Office 365 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 セグメントを作成するように設計されており重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できること、顧客とマイクロソフト データ センターの間で確立されこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されデスクトップとデータ センターの間でデータの機密性や整合性が確保されること、Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケットレベルでのセキュリティが実現でき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。	公開文書	文献[01]「IS-18：情報セキュリティ－ 暗号化」 文献[01]「IS-19：情報セキュリティ－ 暗号化キーの管理」 文献[44]「ファイル単位の暗号化を利した保存データの高度な暗号化」 文献[01]「SA-02：セキュリティアーキテクチャー－ ユーザーID資格情報」 文献[17] 文献[01]「SA-09：セキュリティアーキテクチャー－ 分離」 文献[27]	―	―	―	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 のみに限定した上で、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クローズド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	―	Azure上に配置された医療情報システムへの接続が伴う場合は、専用線サービスであるExpress Routeの活用、Azureを経由したVPN Gateway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の機能やサービスをご活用いただくことができます。	適合可能	文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 またインタビューにて、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[107]	―	（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、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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．3．2．4【基本】） ・医療機関等の利用者が、医療機関の外部からASP・SaaSを利用する場合に、事業者は、医療機関の利用者が用いる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等の技術導入に関する事業者の役割、前面等を医療機関等と合意すること。	Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモートワーカーから Azure Virtual Network への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Office 365 データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 またインタビューにて、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[107]	―	（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。

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
6.12-01		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して、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。電子署名は紙媒体への署名や記名・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、中長期的には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を考慮し、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。	（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	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子証明書、もしくは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によるものであることを確認し、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こと。	–	対象外	–	–	–	–	–	–	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	同上	–	対象外	–	–	–	–	–	–	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. 「電子署名等に係る地方公共団体情報システム機構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全ての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	同上	–	対象外	–	–	–	–	–	–	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。
6.12-04					（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	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、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こと。	–	対象外	–	–	–	–	–	–	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	同上	–	対象外	–	–	–	–	–	–	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	同上	–	対象外	–	–	–	–	–	–	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	・法令で定められた記名・押印を電子署名で行うものとされた情報に対する電子署名の方式等について、医療機関等と合意すること。 ・合意した電子署名の方式等が、保健医療福祉分野PKI認証局の発行する電子署名もしくはこれと同等の仕様を含むものであることを確認し、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こと。	–	対象外	–	–	–	–	–	–	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）	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ることである。なお、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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規定を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、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[1]では、多要素認証として電話による第2要素が使用できることが明示されている。 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。 Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。	適合可能	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[1]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開文書	文献[01]『SA-02：セキュリティアーキテクチャー－ユーザーID資格情報』 文献[17]	–	–	–	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			「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））		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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・提供する電子カルテシステム等に関するサービスにおいて、医療機関等の職務権限等に応じたアクセス制御が可能であることを含め、仕様内容について、医療機関等と合意すること。	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。 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、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。 文献[23]では、Office365上のコンテンツに対するエンドユーザのアクセスは、利用者側で設定する権限設定によりコントロールされていることを示している。	公開文書	文献[01]『SA-11：セキュリティアーキテクチャー－共有ネットワーク」 文献[23]	–	–	–	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稼動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	・同上	Active Directory Federation Serviceを構築する事で、IPアドレスによる、アクセス制御を実装することは可能。またサードパーティ製のアクセスコントロールソリューションととと組み合わせることで、PC端末制御を行うことも可能。	適合可能	文献[21]では、AD FS(Active Directory Federation Service)と組み合わてOffice 365 を使うことで、IPv4アドレスに基づくアクセス制限が可能であることを示している。 また文献[132]には、Azure AD Premiumを使用することにより、Office 365に対する接続を、特定のIPアドレスからの通信や、特定のドメインに認証された端末からの通信に限定することが可能になることが示されている。 NDA文書より、Microsoft Azure が ISO27001を取得していることから、適切なアクセスコントロールの対策が採られていると考えられる。 またインタビューにて、サードパーティ製のツールと組み合わせることにより、利用可能な端末を制限することができることを確認した。	要NDA	文献[21] 文献[132]	–	（マイクロソフト社とのNDAにより開示）	（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	・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ーフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	Active Directory Federation Serviceを構築する事で、IPアドレスによる、アクセス制御を実装することは可能。またサードパーティ製のアクセスコントロールソリューションととと組み合わせることで、PC端末制御を行うことも可能。	適合可能	文献[21]では、AD FS(Active Directory Federation Service)と組み合わてOffice 365 を使うことで、IPv4アドレスに基づくアクセス制限が可能であることを示している。 また文献[132]には、Azure AD Premiumを使用することにより、Office 365に対する接続を、特定のIPアドレスからの通信や、特定のドメインに認証された端末からの通信に限定することが可能になることが示されている。 またインタビューにて、サードパーティ製のツールと組み合わせることにより、利用可能な端末を制限することができることを確認した。	要NDA	文献[21] 文献[132]	–	（マイクロソフト社とのNDAにより開示）	–	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。

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
7.1-05					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	・同上	利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス (代理人による アクセス、共有メールボックスへのアクセスなど) を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間	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[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 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Lockbox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。	公開文書要NDA	文献[01]『SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出』 文献[17]の『ポリシーの監査と保持』 文献[26]	–	–	–	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、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、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が含まれること。	最低限	・ASP・SaaS 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（情報セキュリティ対策機器、通信機器等）の時刻同期の方法を規定し、実施すること。(Ⅲ．1．1．5【基本】) ・電子データの原本性確保を行うこと。(Ⅲ．5．1．1【推奨】)	Office365 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、Office365 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 Office365 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 Online Services 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 Online Services 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。	公開文書	文献[01]『SA-12：セキュリティ アーキテクチャー – 時刻の同期』	–	–	–	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」を行うに当たり、内容の十分な確認が実施できるようにすること。	最低限	・入力された内容が記録の確定前に作成責任者によって確認できる仕様とすることを、医療機関等と合意すること。	–	対象外	–	–	–	–	–	–	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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。(Ⅱ．2．1．3【基本】) ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。(Ⅱ．3．1．2【基本】) ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。(Ⅲ．2．1．3【基本】) ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。(Ⅲ．2．3．1【基本】)	利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス (代理人による アクセス、共有メールボックスへのアクセスなど) を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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、スタッフまたは契約業者のスタッフによるMicrosoft Online Services の運用環境へのアクセスは、厳しく管理されていることが明示されている。 文献[01]によると、Microsoft Online Services にはレプリケーション機能が含まれていること、利用者は必要に応じて、自社でのデータの抽出およ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[65]には、セキュリティ対策ならびに顧客データにアクセス可能なマイクロソフト担当者の関連手順および責務を規定したセキュリティ関連文書を保持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、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていること、これらのログから更新内容がトレースできることが確認できた。	要NDA	文献[01]『SA-07：セキュリティアーキテクチャー – リモート ユーザーの多要素認証』 文献[01]『DG-04：データ ガバナンス – 保持ポリシー』 文献[65]	–	(マイクロソフト社とのNDAにより開示)	–	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	・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ーフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。	Office365 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、Office365 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 Office365 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 Online Services 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 Online Services 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。	公開文書	文献[01]『SA-12：セキュリティ アーキテクチャー – 時刻の同期』	–	–	–	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。
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	・同上	利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス (代理人による アクセス、共有メールボックスへのアクセスなど) を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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、スタッフまたは契約業者のスタッフによるMicrosoft Online Services の運用環境へのアクセスは、厳しく管理されていることが明示されている。 文献[01]によると、Microsoft Online Services にはレプリケーション機能が含まれていること、利用者は必要に応じて、自社でのデータの抽出およ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[65]には、セキュリティ対策ならびに顧客データにアクセス可能なマイクロソフト担当者の関連手順および責務を規定したセキュリティ関連文書を保持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、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていること、これらのログから更新内容がトレースできることが確認できた。	要NDA	文献[01]『SA-07：セキュリティアーキテクチャー – リモート ユーザーの多要素認証』 文献[01]『DG-04：データ ガバナンス – 保持ポリシー』 文献[65]	–	(マイクロソフト社とのNDAにより開示)	–	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
7.1-14					(3) 更新履歴の保存 1. 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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・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られる機能を含めること。 ・更新管理の仕様について、医療機関等と合意すること。	SharePoint OnLine におけるリストまたはライブラリにおいてバージョン管理を有効にすることにより、リスト内のアイテムやライブラリ内のファイルのすべての変更が保存、トラッキングされ、復元することができます。バージョン管理とその他の設定（チェックアウトなど）を組み合わせると、サイトに投稿されているコンテンツを詳細に管理でき、古いバージョンのアイテムやファイルを参照または復元することも可能となります。	適合可能	文献[01]によると、Office 365 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。 文献[115]によると、SharePoint Onlineのバージョン管理機能を用いることにより、SharePointのドキュメントライブラリ上のファイルの更新履歴を自動的に取得することができ、更新履歴の管理や、更新前ファイルの参照が可能となることが明記されている。	公開文書	文献[01]『DG-04』 文献[115]	—	—	—	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	・同上									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 1. 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	・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こと。（Ⅲ．3．1．2【基本】） ・代行操作を実施するIDや運用方法について、予め医療機関等の管理者と内容を合意すること。	—	対象外	—	—	—	—	—	—	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	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】）	—	対象外	—	—	—	—	—	—	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	・代行操作された際の、データの確定に関する仕様について、医療機関等の管理者と内容を合意すること。	—	対象外	—	—	—	—	—	—	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 1. 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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・機器、ソフトウェア構成について、医療機関等と合意をとること。 ・機器、ソフトウェア構成について文書化を行い、医療機関等の管理者に対して報告できる内容とすること。	Microsoft Online Services では、そ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。Microsoft Online Services 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ます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。	適合可能	文献[01]では、Microsoft Online Services 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 Online Services の提供に使用される資産（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）に関して記録を残していることが明示されている。 また同文献では、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者（Microsoft Online Services とサード パーティ）に対して通知されることが明記されている。	公開文書	文献[01]『FS-08：施設のセキュリティ - 資産管理』 文献[01]『RM-01：リリース管理 - 新規開発/取得』	—	—	—	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	・提供するサービスにおけるシステムの導入プロセスについて、文書化を行うこと。 ・システムの構成管理内容を示す資料の開示内容・範囲・条件について、医療機関等と合意すること。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合） 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 Online Services 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 Online Services の提供に使用される資産（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）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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]『FS-08：施設のセキュリティ - 資産管理』 文献[01]『RM-04：リリース管理 - アウトソース開発」	—	—	—	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	・運用・操作に関する利用者教育における事業者の役割、範囲等について、医療機関等と合意すること。	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなってい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、当社の従業員との契約に機密保持条項を組み込んでいます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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。	公開文書 要NDA	文献[01]『HR-02：人的資源のセキュリティ - 雇用における合意事項』 文献[01]『IS-11：情報セキュリティ - トレーニング/意識向上」 文献[01]『RS-03：復元 - ビジネス継続性の計画」 文献[128]	—	(マイクロソフト社とのNDAにより開示)	—	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定を整備し、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	・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について、事業者の役割、範囲等について医療機関等と合意すること。	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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。お客様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	NDA文書より、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。	要NDA	—	—	—	(マイクロソフト社とのNDAにより開示)	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	・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御などリすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．3．2．3【基本】）	Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモートワーカーから Office 365 への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Office 365 データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[01]では、アクセス制御としてアクセスポリシー、アクセスの許可、最小限の権限、完全性及び秘密保持、認証、ネットワーク設計が含まれることを確認した。文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 さらにインタビューにて、Express Routeにて接続される場合であっても、httpsによる通信の暗号化が行われていること及び、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	公開文書 要NDA	文献[01]『IS-07：情報セキュリティ - ユーザー アクセス ポリシー」 文献[107]	—	(マイクロソフト社とのNDAにより開示)	—	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	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．3．2．1【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．3．2．2【推奨】）	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。 Office 365で、利用者・管理者のクライアント機器とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 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[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、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	公開文書	文献[01]『SA-07：セキュリティアーキテクチャー - リモートユーザーの多要素認証」 文献[01]『SA-11：セキュリティアーキテクチャー - 共有ネットワーク」	—	—	—	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						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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に、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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・ASP・SaaS提供に必要なシステムの保守をリモートメンテナンスで行う場合の、医療機関等への報告対象とするシステムの範囲、そのシステムに対するリモートメンテナンスの実施条件、報告内容等について、医療機関等と合意すること。	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365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。 スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 ・マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。	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。	公開文書	文献[01]「SA-07：セキュリティアーキテクチャー－リモートユーザーの多要素認証」	－	－	－	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、その要否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） 「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)）	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、画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、そのままでは一瞥して判りにくいこと これらに適切に対応することにより、紙の記録と同等と言える見読性を確保しなければならない。 また、何らかのシステム障害が発生した場合においても診療に重大な支障が無い最低限の見読性を確保するための対策も考慮に含める必要がある。 ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、「4.2 責任分界点について」を参考につつ、予め責任を明確化しておき、速やかなる復旧が図られるように配慮しておく必要もある。 これらのことに配慮していても万が一、保存していた情報が き損した場合等は、可能な限り速やかな復旧に努め、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応える見読性の確保を図らなければならない。	（1）情報の所在管理 紙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	・取り扱う各情報資産について、管理責任者を定めると共に、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】）	－	対象外	－	－	－	－	－	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	・見読性を保証するサービス仕様について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－	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	・ASP・SaaS 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、情報セキュリティ対策機器、通信機器の稼働監視（応答確認等）を行うこと。稼働停止を検知した場合は、利用者に速報を通知すること。（Ⅲ．1．1．1【基本】） ・ASP・SaaS 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、ネットワークに対し一定間隔でパフォーマンス監視（サービスのレスポンス時間の監視）を行うこと。また、利用者との取決めに基づいて、監視結果を利用者に通知すること。（Ⅲ．1．1．3【推奨】） ・ASP・SaaS サービスを利用者に提供する時間帯を定め、この時間帯におけるASP・SaaSサービスの稼働率を規定すること。また、アプリケーション、プラットフォーム、サーバ・ストレージの定期保守時間を規定すること。（Ⅲ．2．1．1【基本】） ・見読性を保証するサービス仕様について、医療機関等と合意すること。	－	対象外	－	－	－	－	－	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					（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	・障害等が生じた場合等を想定し、冗長性を確保する仕様等について医療機関等と合意すること。	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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]「RS-03：復元－ビジネス継続性の計画」	－	－	－	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	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	－	対象外	－	－	－	－	－	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	・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	－	対象外	－	－	－	－	－	－	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	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・事業者は、障害等が生じた場合の稼動に関するサービスの品質について医療機関等の管理者と合意する。	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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]「RS-03：復元－ビジネス継続性の計画」	－	－	－	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	・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)をASP・SaaSにおいて含めることについて、医療機関等の管理者と協議し、合意すること。	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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]「RS-03：復元－ビジネス継続性の計画」	－	－	－	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 緊急に必要になると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	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．3．2．4【基本】） ・障害等が生じた場合の責任分界を明確にし、稼動を保証するサービスの品質について医療機関等と合意すること。	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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]「RS-03：復元－ビジネス継続性の計画」	－	－	－	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） 「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）障害等によるデータ保存時の不整合 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 1．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	・ASP・SaaS サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウイルス等に対する対策を講じること。（Ⅲ．2．2．1【基本】）	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてマルウェアがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。関連するサービスの説明やサービス レベル契約 (SLA) に、その他の情報が記載されている場合があります。 マイクロソフトは独自のセキュリティ レスポンス センター (MSRC) を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。 詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4) で、"悪意のあるコードからの保護" が規定されています。 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、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]には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。 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。	公開文書	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	－	－	－	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							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項目番	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	
7.3-02					（2）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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。（Ⅱ．5．2．1【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】）	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなってい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、当社の従業員との契約に機密保持条項を組み込んでいます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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、Microsoft Online において、電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動などの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、マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなってい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 Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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、不正アクセス検知時およ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。 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]『HR-02：人的資源のセキュリティ－雇用における合意事項』 文献[01]『IS-11：情報セキュリティ－トレーニング／意識向上』 文献[01]『IS-22：情報セキュリティインシデント管理』 文献[01]『SA-14：セキュリティアーキテクチャー－監査ログ／侵入検出』	－ （マイクロソフト社とのNDAにより開示）	－ －	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。
7.3-03					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	・取り扱う各情報資産について、管理責任者を定めるとともに、その利用の許容範囲（利用可能者、利用目的、利用方法、返却方法等）を明確にし、文書化すること。（Ⅱ．4．1．1【基本】） ・組織における情報資産の価値や、法的要求（個人情報の保護等）等に基づき、取扱いの慎重さの度合いや重要性の観点から情報資産を分類すること。（Ⅱ．4．2．1【基本】） ・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaS 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、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．1．1．9【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	バックアップの場合、内容がプライマリー 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ます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 Microsoft Online Services では、そ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、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。資産所有者は、その資産に関する情報を常に最新にしておく責任を担います。	適合可能	文献[01]では、Microsoft Online Services 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こと、レプリケーション機能が提供されていることが明示されている。また、利用者自らが自身のデータを抽出してバックアップできることが明示されている。	公開文書	文献[01]『DG-04：データガバナンス － 保持ポリシー』	－	－	－	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	・情報セキュリティ監視（稼働監視、障害監視、パフォーマンス監視等）の実施基準・手順等を定めること。 また、ASP・SaaS 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、ネットワークの運用・管理に関する手順書を作成すること。（Ⅲ．1．1．9【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】） ・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こと。（Ⅲ．4．4．3【基本】）	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 Office 365 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。 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。	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文書を確認したところ、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、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	公開情報 要NDA	文献[01]『FS-01：施設のセキュリティ－ポリシー』 文献[01]『FS-02：施設のセキュリティ－ ユーザーアクセス』 文献[01]『FS-03：施設のセキュリティ－ 管理されたアクセスポイント』	－ 公開情報 要NDA	－ －	（マイクロソフト社とのNDAにより開示）	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	・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】）	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 Online Services の運用環境へのアクセスは、厳しく管理されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。（社内、社外） 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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[62]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。 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[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。	公開文書	文献[01]『SA-14：セキュリティアーキテクチャー－監査ログ／侵入検出』 文献[62] 文献[131]	－	－	－	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含損した時に、バックアップされたデータを用いて含損前の状態に戻せること。もし、含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	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ．2．3．2【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】） ・バックアップのき場箇所の確認に関する仕様、方法等ついて、医療機関等と合意すること	バックアップの場合、内容がプライマリー 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ます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 Microsoft Online Services では、そ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、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。資産所有者は、その資産に関する情報を常に最新にしておく責任を担います。	適合可能	文献[01]によると、Microsoft Online Services 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]『DG-04：データガバナンス － 保持ポリシー』	－	－	－	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	・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaSサービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】）	Microsoft Online Services には、個々のサービスの説明ので定義に従って、お客様がデータ保持ポリシーを適用するための機能が用意されています。バックアップの場合、内容がプライマリー 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ます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。 Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 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。 Office 365 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。	適合可能	文献[01]によると、Microsoft Online Services では、ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されていること、年に 1 度バックアップおよび回復の作業を検証していることが明記されている。 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があることが明示されている。 文献[65]には、セキュリティ対策ならびに顧客データにアクセス可能なマイクロソフト担当者の関連手順および責務を規定したセキュリティ関連文書を保持することが明記されている。	公開文書	文献[01]『DG-04：データガバナンス － 保持ポリシー』 文献[01]『OP-03：運用管理 － 容量/リソース計画』 文献[65]	－	－	－	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	・入出力するデータ項目の形式ついて、標準形式を採用する。標準形式によることができない場合には、妥当なデータ項目の形式について医療機関等と合意すること。	－	対象外	－	－	－	－	－	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	・マスターテーブルの変更に際してのレコード管理方法・とるべき措置等について、移行に際して情報内容の変更が生じない機能及び検証方法を備える。本機能を備えることが困難な場合には、妥当な提案を行い、医療機関等と合意すること。	－	対象外	－	－	－	－	－	－

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
7.3-10					【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	・ASP・SaaSによりデータ保存する際に用いるデータ形式及び転送プロトコルを変更する場合、変更前の方式との互換性の確保等について、医療機関等と合意する。	Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルは暗号化されて保存されています。 業界標準のトランスポート層セキュリティ（TLS）/SSL（Secure Sockets Layer）を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 Office 365ではOutlook、Outlook on the Web（OWA）、EASクライアントにおいて S/MIME によるお客様暗号鍵を使った暗号化、電子署名を行うことが可能です。 Microsoft Online Services 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 Online Services 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。 文献[17]では、電子メールの利用時にS/MIMEによる利用者の暗号鍵を使った暗号化、電子署名が利用可能であることが明示されている。 文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint Onlineが、ファイル単位の暗号化機能を備えてい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。	公開文書要NDA	文献[05] 文献[17] 文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利した保存データの高度な暗号化」	–	（マイクロソフト社とのNDAにより開示）	–	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	・ASP・SaaS 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・ストレージ等の稼働監視、障害監視、パフォーマンス監視の結果を評価・総括して、管理責任者に報告すること。（Ⅲ．1．1．4【推奨】） ・ASP・SaaS 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・ストレージについて、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．2．1．2【基本】） ・ASP・SaaS 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・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．2．1．4【推奨】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	(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。 Microsoft Online Services 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。 マイクロソフトのセキュリティ レスポンス センター（MSRC）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 Online Services 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 Online Services 全体で主導します。	適合可能	文献[01]では、Microsoft Online Services 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があることが明示されている。 また同文献では、Microsoft Online Services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違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。	公開文書	文献[01]「OP-03：運用管理 – 容量/リソース計画」 文献[01]「OP-04：運用管理 – 機器のメンテナンス」 文献[01]「IS-20：情報セキュリティ - 脆弱性/更新プログラム管理」	–	–	–	–
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	・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ．4．4．6【基本】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】）	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。 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境界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、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文書を確認したところ、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。	公開文書要NDA	文献[01]「FS-01：施設のセキュリティ - ポリシー」 文献[01]「FS-02：施設のセキュリティ - ユーザー アクセス」 文献[01]「FS-03：施設のセキュリティ - 管理されたアクセスポイント」	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–
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	・重要な物理的セキュリティ境界（カード制御による出入口、有人の受付等）に対し、個人認証システムを用いて、従業員及び出入りを許可された外部組織等に対する入退室記録を作成し、適切な期間保存すること。（Ⅲ．4．4．1【基本】） ・サーバルームやラックの鍵管理を行うこと。（Ⅲ．4．4．6【基本】）	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]「FS-03：施設のセキュリティ – 管理されたアクセスポイント」	–	–	–	–
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	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） ・バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認すること。（Ⅲ．2．3．2【推奨】） ・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。（Ⅲ．5．3．1【基本】） ・バックアップされたデータに対して、内容が改ざんされていないことを確認できる仕様について、医療機関等と合意すること。	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 Online Services の運用環境へのアクセスは、厳しく制御されています。 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。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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 Online Services では、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていること、これらのログから更新内容がトレースできることが確認できた。	要NDA	文献[01]「DG-04：データガバナンス – 保持ポリシー」 文献[01]「OP-04：運用管理 – 機器のメンテナンス」	–	（マイクロソフト社とのNDAにより開示）	–	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	・医療情報のデータを格納するサーバのディスクの障害対策について、医療機関等と合意する。	Microsoft Online Services には、個々のサービスの説明での定義に従って、お客様がデータ保持ポリシーを適用するための機能が用意されています。バックアップの場合、内容がプライマリー 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ます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。 Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 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。 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 Online Services では、ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されていること、年に 1 度バックアップおよび回復の作業を検証していることが明記されている。 文献[01]によると、Microsoft Online Services 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ることが明示されている。	公開文書	文献[01]「DG-04：データガバナンス – 保持ポリシー」 文献[01]「OP-04：運用管理 – 機器のメンテナンス」	–	–	–	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。

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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
7.3-16					【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 1. 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	ASP・SaaS 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・ストレージに対し、利用者の利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。（Ⅲ．7．2【基本】） ・ASP・SaaSに用いる回線もしくは施設等のサービスレベル維持を満足するための更新計画について、医療機関等と合意すること。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合） Microsoft Online Services 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 Online Services の資産を回復し、Microsoft Online Services 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。 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]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。 文献[01]によると、Microsoft Online Services 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、および定められたしきい値・イベントに基づいた予防的な容量管理の運用プロセスが用意されていることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 – 新規開発/取得」 文献[01]「OP-03：運用管理 – 容量/リソース計画」 文献[01]「OP-04：運用管理 – 機器のメンテナンス」	–	–	–	–
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のも事実である。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。	（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	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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守秘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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
評価項目番	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	
8.1-11					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	・従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。（Ⅱ．5．2．2【基本】） ・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・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すこと。	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。 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し、SLA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、マイクロソフトはお客様に協力します。お客様による監査について、お客様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、対象となるお客様、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、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。 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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、およ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 Online Services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[65]および文献[66]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等の調査に必要となるログ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。 NDA文書を確認したところ、「(10)インシデントが発生した場合の想定損害額とクラウド事業者側が提示する損害賠償・補償上限額とのバランス」について、利用者が直近12か月間にマイクロソフト社に対して支払義務を負ったサービス利用料金を上限とする直接損害に損害賠償が限定されることが確認できた。	要NDA	文献[01]「IS-07：情報セキュリティ - ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ - ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ - ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ - ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー - データのセキュリティ／整合性」 文献[65](OST) 文献[66](SLA)	—	—	(マイクロソフト社とのNDAにより開示)	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	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。（Ⅲ．3．2．1【基本】） ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。（Ⅲ．3．2．2【推奨】） ・第三者が当該事業者のサーバになりすますこと（フィッシング等）を防止するため、サーバ証明書の取得等の必要な対策を実施すること。（Ⅲ．3．2．3【基本】） ・利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル（特に、通信容量とトラヒック変動が重要）及び管理上の要求事項を特定すること。（Ⅲ．3．2．4【基本】） ・外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。（Ⅲ．3．2．5【推奨】） ・ネットワーク回線を含めてASP・SaaS事業者がサービスを提供する場合、そのネットワーク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」を遵守すること。 ・自社で講じるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し、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こと。	6.11に示したとおり。	適合可能	6.11の確認事項のとおり。	—	—	—	—	—	—
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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・ASP・SaaSにおける情報セキュリティ対策ガイドライン（平成20年1月30日総務省）及び本ガイドラインを遵守すること。 ・遵守すべきガイドラインの範囲及びこれを遵守している旨の報告につき、その内容・範囲等を、医療機関等と合意すること。	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、お客様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、ベンダーを通じての個別の検討事項であることを確認した。	要NDA	—	—	(マイクロソフト社とのNDAにより開示)	—	利用者は、標準的な契約書等を確認して、変更要望の有無をベンダ等を通じて示す必要がある。
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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・受託した医療情報を、保守作業に必要な範囲での閲覧を超えて閲覧しないこと。 ・許可されていない受託データの閲覧を禁止することにつき、その方法等を含め、医療機関等と合意すること。	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 Online Services 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 Online Services 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 Online Services 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。 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 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。 マイクロソフトは独自のセキュリティ レスポンス センター（MSRC）を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。 詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4）で、"悪意のあるコードからの保護" が規定されています。 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、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 Online Services 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 Online Services 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。 同文献には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。 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]「OP-02：運用管理・文書化」 文献[01]「IS-07：情報セキュリティ - ユーザー アクセス ポリシー」 文献[01]「IS-21：情報セキュリティ - ウイルス／悪意のあるソフトウェアへの対策」 文献[01]「CO-03：コンプライアンス - サードパーティの監査」 文献[02]「顧客データが下請業者に開示される場合」	—	(マイクロソフト社とのNDAにより開示)	—	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応						SI事業者・利用者で必要な対応
評価項目番	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	
8.1-15					（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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・受託した医療情報は、匿名化されたものを含めて、医療機関との契約に基づくことなく、分析、解析等を実施しないこと。 ・医療機関との契約に基づくことなく、受託したデータの分析・解析を実施しないことにつき、その方法等を含め、医療機関等と合意すること。	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 Online Services 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 Online Services 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 Online Services 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。 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 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。 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。 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。 マイクロソフトは独自のセキュリティレスポンス センター（MSRC）を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。 詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4）で、"悪意のあるコードからの保護" が規定されています。 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、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 Online Services 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 Online Services 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。 同文献には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。 さらに、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[02]では、「Microsoft が顧客データを使用することはなく、宣伝や他の商業上の目的のためにデータから情報を取り出すこともありません」とされている。	要NDA	文献[01]「OP-02：運用管理・文書化」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」 文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」 文献[02]「Azureに保存しているデータのマイクロソフトによる利用」	－	（マイクロソフト社とのNDAにより開示）	－	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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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。 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 Online Services 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 Online Services 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。 さらに、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]「OP-02：運用管理・文書化」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」 文献[01]「CO-03：コンプライアンス－サードパーティの監査」 文献[02]「顧客データが下請業者に開示される場合」 文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	－	（マイクロソフト社とのNDAにより開示）	－	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	・契約に先立ち、医療機関等の管理者から、選定に必要な情報の提供を求められた場合に、速やかに提出すること。	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、お客様の契約内容変更のご要望については、実施可能なものについては変更契約書という形でお受けしています。	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扱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および技術力。 (d)文献[76]から、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経営方針における位置付け、体制、グローバルなバックアップ体制等。	公開文書	文献[01]「IS-01：情報セキュリティ － 管理プログラム」 文献[01]「IS-02：情報セキュリティ － 管理サポート／関与」 文献[01]「IS-03：情報セキュリティ － ポリシー」 文献[75] 文献[76]	－	－	－	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・国民に示す手段として、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	－	－	－	－	－	－	－
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	－	－	－	－	－	－	－
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	・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．3．1．3【基本】）	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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。 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、業務の正当性に基づいて Microsoft Online Services 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、およ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 Online Services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]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」	－	－	－	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。

厚生労働省ガイドラインの評価項目						総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 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	
8.1-21					(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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ネットワーク構成図を作成すること（ネットワークをアウトソーシングする場合を除く）。また、利用者の接続回線も含めてサービスを提供するかどうかを明確に区別し、提供する場合は利用者の接続回線も含めてアクセス制御の責任を負うこと。また、アクセス制御方針を策定し、これに基づいて、アクセス制御を許可又は無効とするための正式な手順を策定すること。（Ⅲ．3．1．1【基本】） ・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こと。（Ⅲ．3．1．2【基本】） ・利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（Ⅲ．9．1．3【基本】） ・システム管理者のデータアクセスの制限の方法について、医療機関等と合意する。	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。（社内、社外） 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 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。	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[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 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Lockbox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]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	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限方法（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 1(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	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・ASP・SaaS サービスの提供及び継続上重要な記録（会計記録、データベース記録、取引ログ、監査ログ、運用手順等）については、法令又は契約及び情報セキュリティポリシー等の要求事項に従って、適切に管理すること。（Ⅱ．7．1．2【基本】） ・利用可能範囲（対象区画・施設、利用が許可される者等）の明示、認可手続の制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。（Ⅱ．7．1．3【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・自社で定める個人情報保護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し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。 ・個人情報保護法の対象に満たない件数(5,000件未満)、対象外（死者に関する情報）等であっても、医療情報の重要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が含まれていることを確認し、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こと。	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。 法的権限を持つ監査当局等の検査等が行われる場合、マイクロソフトはお客様に協力します。お客様による監査については、お客様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、対象となるお客様、被害の状況が判明し次第連絡することとして合意し、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。 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。 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 Online Services 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。 Office 365 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	インタビュー及び公開文書により、個人情報の取扱いについて、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。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 「組織の外部占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[17]の「ポリシーの監査と保持」	–	（マイクロソフト社とのNDAにより開示）	–	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	・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・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、医療機関等と合意すること。	–	対象外	–	–	–	–	–	–	利用者は、個人情報を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。
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必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、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2 1(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	–	–	–	–	–	–	–

厚生労働省ガイドラインの評価項目							総務省ガイドラインの要求事項	ガイドラインに対するMicrosoftの見解	Microsoft Office 365 における対応							SI事業者・利用者で必要な対応
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	
8.4-01		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を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、外部保存を委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）	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。（Ⅱ．7．1．1【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・個人情報は関連する法令に基づいて適切に取り扱うこと。（Ⅲ．5．1．2【基本】） ・機器及び媒体を正式な手順に基づいて廃棄すること。（Ⅲ．5．3．2【基本】） ・事業者の都合により医療機関等に対してASP・SaaSの提供を終了する場合の事前通知の方法、終了が認められる理由、及び終了に向けての対応について、医療機関等と合意すること。 ・情報の破棄の実施に際し、報告の内容・範囲・提出すべき資料等について、医療機関等と合意すること。 ・ASP・SaaSの提供を終了する場合に、受託しているデータ及びこれに関連する資料の内容、範囲、条件等について、医療機関等と合意すること。 ・受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「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こと。	一	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、慣却など）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。 利用者側の運用管理規定については、利用者が主体的に定める必要があります。	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、すべての Microsoft Online Services 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。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。 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[01]「DG-05：データ ガバナンス – 安全な廃棄」 文献[65]（OST）「セキュリティ|物理セキュリティおよび論理セキュリティ	一	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	運用管理規程の整備は利用者側で対応する必要がある。 Microsoft Online Services 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委ね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。

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 Office 365 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	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	
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。	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。 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。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。お客様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。 上記の2点は契約書に記載の事項となっています。 マイクロソフトが提供する上記の第三者監査レポートに重大な不備がありお客様のクラウドサービス利用の継続に支障が出る場合、あるいはセキュリティ対策の不備によってお客様コンテンツの安全性に重大な懸念が生じるような場合、お客様はマイクロソフト専門担当者を通じてお客様がコンプライアンス、法的要件あるいは規制対応に必要となる情報を請求し監査することができます（追加の契約が必要になる場合があります）。	適合可能	文献[01]によると、Office 365及びその基盤となるインフラストラクチャは ISO/IEC 27001:2005 に基づくセキュリティフレームワークを採用し、独立した監査法人によってISO 27001 認定を受けていること、サービスとインフラストラクチャの両方が、年に1回のSSAE16の監査を受け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]「Microsoft Online Services のスタックに対する ISO 認定」	―	（マイクロソフト社とのNDAにより開示）	―	―
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。	―	適合可能	以下の各項目で対応を確認した。	―	―	―	―	―	―
	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		―	―	―	―	―	―
		(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		―	―	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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		―	―	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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		―	―	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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		―	―	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。	医療情報システム上の情報の分類については、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 Online Services では、セキュリティ分類カテゴリーに従って資産を分類し、その後で一連の標準的なセキュリティおよびプライバシー属性を実装することが明示されている。	公開文書	文献[01]「DG-02：データガバナンス-分類」	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。	医療情報システム上の情報の分類については、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、資産所有者は、その資産に関する情報を常に最新にしておく責任を担うことが明示されている。	公開文書	文献[01]「DG-01：データガバナンス - 所有権/管理者責任」	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。

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 Office 365 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	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)	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。	医療情報システム上の情報の分類については、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 Online Services では、年に 1 度ビジネスへの影響分析が実行されること、そこでは、Microsoft Online Services ビジネス環境及びプロセスに関する脅威の特定、脅威の評価、重大な脅威を軽減するための承認された戦略が含まれることが明示されている。	公開文書	文献[01]「DG-08：データガバナンス－リスク評価」	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。	医療情報システム上の情報の分類については、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 Online Services 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およ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およ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。	公開文書	文献[01]「RI-02：リスク管理 － 評価」	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。	医療情報システム上の情報の分類については、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 Online Services では、セキュリティ分類カテゴリーに従って資産を分類し、その後で一連の標準的なセキュリティおよびプライバシー属性を実装することが明示されている。	公開文書	文献[01]「DG-03：データガバナンス－ 処理/ラベリング/セキュリティポリシー」	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。	医療情報システム上の情報の分類については、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 Online Services では、セキュリティ分類カテゴリーに従って資産を分類し、その後で一連の標準的なセキュリティおよびプライバシー属性を実装すること、個々のサービスでの定義に従って顧客がデータ保持ポリシーを適用するための機能が提供されていること、NIST 800-88 準拠の消去ソリューションを使用していること、承認された記憶メディアと廃棄管理サービスを使用すること、職務分離の原則を採用しテスト環境や運用環境へのアクセスをポリシーに応じて制限していること、が明示されている。	公開文書	文献[01](DG-03～06)	―	―	―	利用者及びSI事業者は、自らがMicrosoft Online Services 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。	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 Online Services では全体的な ISMS が設計およ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。	公開文書	文献[01]「IS-01：情報セキュリティ－管理プログラム」	―	―	―	利用者及びSI事業者は、Microsoft Online Services 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。
		(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。	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[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、およ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、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って、現在のお客様の場合はセキュリティ センターを通じて入手できることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス－監査計画」	―	―	―	―
		(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。	適合可能	文献[01]によると、独立した監査法人によるMicrosoft Online Services のレポートおよび認定が提供され、セキュリティおよびコンプライアンスの目標を設定して実現する方法を現していることが明記されている。	公開文書	文献[01]「CO-01：コンプライアンス－監査計画」	―	―	―	―

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 Office 365 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	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	
		(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。	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。 標準的な運用手順が、正式に文書化され、Microsoft Online Services 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 Online Services 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。 Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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 Online Services 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 Online Services およ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。	公開文書	文献[01]「IS-04：情報セキュリティ－基本的な要件」 文献[01]「OP-02：運用管理 － 文書化」 文献[01]「RM-01：リリース管理 － 新規開発/取得」	－	－	－	－
		(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。		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 Online Services の管理者によって承認されていること、Microsoft Online Services 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 Online Services 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[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 Online Services では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 Online 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]によると、Microsoft Online Services では、トランスポート層、クライアントと Exchange Online 間の暗号化（SSL）、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで暗号化機能が提供されること、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management（IRM）機能やRights Management Services（RMS）機能を用いて暗号化できることが明記されている。 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、およ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[121]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。	公開文書	文献[01]「OP-02：運用管理・文書化」 文献[01]「IS-14 情報セキュリティ－管理者による監督」 文献[10] 文献[01]「RI-01：リスク管理 － プログラム」「IS-23：情報セキュリティ－インシデントの報告」 文献[01]「IS-19：情報セキュリティ－暗号化キーの管理」 文献[01]「CO-01：コンプライアンス－監査計画」 文献[121]	－	－	－	－
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。	適合可能	文献[01]によると、Microsoft Online Services 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およ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およ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。	公開文書	文献[01]「RI-02：リスク管理 － 評価」	－	－	－	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。	－	適合可能	以下の各項目で対応を確認した。	－	－	－	－	－	－

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 Office 365 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	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	
		(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（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。	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。	公開文書	文献[01]「FS-03：施設のセキュリティー 管理されたアクセスポイント」	ー	ー	ー	ー
		(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。	適合可能	NDA文書を確認したところ、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	ー	ー	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	ー
		(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。	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。 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。	適合可能	NDA文書を確認したところ、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	ー	ー	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	ー
		(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。	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。	適合可能	NDA文書を確認したところ、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	ー	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	ー

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 Office 365 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	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
	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。	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 お客様のアプリケーションや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]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。	公開文書	文献[01]「FS-01：施設のセキュリティ－ポリシー」 「FS-02：施設のセキュリティ－ユーザーアクセス」 「FS-03：施設のセキュリティ－管理されたアクセスポイント」	―	―	―	―
			・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。		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。	公開文書	文献[01]「FS-01：施設のセキュリティ－ポリシー」 文献[01]「FS-02：施設のセキュリティ－ユーザーアクセス」	―	―	―	―
			・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）。		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。	要NDA	文献[01]「FS-02：施設のセキュリティ－ユーザーアクセス」 文献[01]「FS-03：施設のセキュリティ－管理されたアクセスポイント」	―	―	（マイクロソフト社とのNDAにより開示）	―
			・情報処理事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した情報処理事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、情報処理事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておくこと。	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。	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・記録する出入り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]「FS-01：施設のセキュリティ－ポリシー」	―	（マイクロソフト社とのNDAにより開示）	―	―
			・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。		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。	公開文書	文献[01]「FS-01：施設のセキュリティ－ポリシー」	―	―	―	―

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 Office 365 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	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	
			・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お客様のアプリケーションや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、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。	公開文書	文献[01]「FS-01：施設のセキュリティ – ポリシー」	–	–	–	–
			・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。		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 お客様のアプリケーションや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。	公開文書	文献[01]「FS-02：施設のセキュリティ – ユーザーアクセス」	–	–	–	–
			・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 お客様のアプリケーションや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、アラートがあがったりデータが暗号化されていることで、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]「FS-03：施設のセキュリティ – 管理されたアクセスポイント」	–	（マイクロソフト社とのNDAにより開示）	–	–

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 Office 365 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	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
		(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 お客様のアプリケーションや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。	公開文書	文献[01]「FS-01：施設のセキュリティ－ポリシー」 「FS-02：施設のセキュリティ－ユーザーアクセス」 「FS-03：施設のセキュリティ－管理されたアクセスポイント」	－	－	－	－
			・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、実施されていることが確認できた。	要NDA	－	－	（マイクロソフト社とのNDAにより開示）	－	－
			・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。	Office 365 サービスでは、異なるホスティング サービスの開発スタッフや運用スタッフが、職務分離の原則に従うようにすることができます。ソース コード、ビルド サーバー、および運用環境に対するアクセスは、厳しく制御されています。 マイクロソフトの担当者は、マルチテナント環境の委託が行われる前にサーバーを構築します。サーバーの構築が完了すると、構築チームは自身のアクセス許可を削除します。サーバーを委託した時点から、マイクロソフトの担当者が委託されたサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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、Office 365 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、マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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、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 Online Services 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 Online Services 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]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	－	－

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 Office 365 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	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	
			・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。	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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 Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 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	文献[06]では、FC（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Office 365 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Lockbox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[06]	―	（マイクロソフト社とのNDAにより開示）	―	―
			・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。	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	―	―	（マイクロソフト社とのNDAにより開示）	―	―
		(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。	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お客様のアプリケーションや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。	公開文書	文献[01]「FS-01：施設のセキュリティ－ ポリシー」 「FS-02：施設のセキュリティ－ ユーザーアクセス」 「FS-03：施設のセキュリティ－ 管理されたアクセスポイント」	―	―	―	―
	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 Online Services 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。	公開文書	文献[01]「FS-08：施設のセキュリティ－ 資産管理」	―	―	―	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。

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 Office 365 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	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)	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。	適合可能	文献[01]では、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。	公開文書	文献[01]「RS-06：復元 – 機器の場所」	―	―	―	―
		(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。	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Onlince Services のすべての契約業者のスタッフは、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	インタビュー等を通じて、Office 365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および喫煙が、社内規定により禁止されていることを確認した。	要NDA	―	―	（マイクロソフト社とのNDAにより開示）	―	―
		(7)	医療情報システムを配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮すること。	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。 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災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	―	―	（マイクロソフト社とのNDAにより開示）	―	―

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 Office 365 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	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)	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。	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。	適合可能	文献[01]では、Microsoft Online Services 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。 また、同文献では、無停電電源装置や空調、消火設備などが定期的に保守されていることが明示されている。	公開文書	文献[01]「OP-04：運用管理 – 機器のメンテナンス」 文献[01]「RS-07：復元 – 機器の電源の故障」	–	–	–	–
		(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。	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 Online Services 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 Online Services 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 Online Services 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。	公開文書	文献[01]「OP-04：運用管理 – 機器のメンテナンス」 「DG-05：データ ガバナンス – 安全な廃棄」 文献[65](OST)	–	–	–	–
		(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。	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文書を確認したところ、可搬型の機器等については、盗難や振動による故障に備えて固定されていることが確認できた。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–

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 Office 365 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	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	
			□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。	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およ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]「RS-07: 復元 ― 機器の電源の故障」	―	（マイクロソフト社とのNDAにより開示）	―	―
			□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。 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。	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	―	―	（マイクロソフト社とのNDAにより開示）	―	―
		(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 Online Services 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 Online Services では、記述された物理データ センター コントロール、およびポートへの物理的なアクセスを制御するためのサポート手順を通じて、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	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	―	―	（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。

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 Office 365 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	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	
				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。 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。							
		(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 Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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、およ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。	公開文書	文献[01]「OP-04：運用管理 -装置のメンテナンス」	―	―	―	―

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 Office 365 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	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	
		(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、Office 365 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。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) 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。	適合可能	Microsoft Online Services 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、Office 365 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。	公開文書	文献[01]「SA-04：セキュリティアーキテクチャ – アプリケーションのセキュリティ」 文献[01]「RM-04：リリース管理 – アウトソース開発」	（マイクロソフト社とのNDAにより開示）	ー	ー	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。
	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。	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。 契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。	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。 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およ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[65](OST)	ー	（マイクロソフト社とのNDAにより開示）	ー	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	ー	ー	（マイクロソフト社とのNDAにより開示）	ー	ー

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 Office 365 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	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)	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 Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画 (該当する場合) 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]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 – 新規開発/取得」	ー	ー	ー	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。	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。 契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。	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。 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およ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[65](OST)	ー	（マイクロソフト社とのNDAにより開示）	ー	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。	ー	適合可能	以下の各項目で対応を確認した。	ー	ー	ー	ー	ー	ー
		(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。	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 Online Services 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。	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なわれる場合があることが明示されている。	要NDA	文献[01]「IS-27：情報セキュリティ – 資産の返却」	ー	（マイクロソフト社とのNDAにより開示）	ー	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。		適合可能	文献[01]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。	公開文書	文献[01]「RM-02：リリース管理 – 運用環境の変更」	ー	ー	ー	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 Office 365 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	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	
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。	Microsoft Online Services では、そ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。Microsoft Online Services 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ます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています マイクロソフトでは、Office 365 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）、および脅威モデル（Threat Modeling）によって、マイクロソフトが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の要素を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（具体的には付属文書 A の項 12.5）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。	適合可能	文献[01]では、Microsoft Online Services 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 Online Services の提供に使用される資産（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）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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立（Establish Design Requirements）、攻撃の分析（Analyze Attack Surface）、および脅威モデル（Threat Modeling）によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 文献[01]「DG-01：データ ガバナンス - 所有権/管理者責任」 文献[01]「RM-04：リリース管理 - アウトソース開発」	―	―	―	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。 利用者が使用する端末については、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。		適合可能	文献[01]では、Microsoft Online Services 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 Online Services の提供に使用される資産（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）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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立（Establish Design Requirements）、攻撃の分析（Analyze Attack Surface）、および脅威モデル（Threat Modeling）によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 文献[01]「DG-01：データ ガバナンス - 所有権/管理者責任」 文献[01]「RM-04：リリース管理 - アウトソース開発」	―	―	―	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。 利用者が使用する端末については、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 Online Services 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。 お客様は、お客様コンテンツの所有者であり、いつでもコンテンツをダウンロードし、他のシステムで使用することができます。マイクロソフトまたはマイクロソフトのパートナーはそのためのツールを継続的に提供し続けます。 契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。	適合可能	文献[67]では、Office 365上の電子メールをオンプレミスのExchange Server環境にコピーして再構築可能なことが明示されている。 文献[68]では、Office 365のSharePoint Onlineのデータをオンプレミスの SharePoint環境にコピーして再構築可能なことが明示されている。 また、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使用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	文献[67] 文献[68]	―	（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。

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 Office 365 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	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	
		(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。	Microsoft Online Services 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 Online Services 資産を回復し、Microsoft Online Services 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。 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、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" がそれぞれ規定されています。	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、およ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、および改訂のプロセス 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、および空調（HVAC）、火災検知および抑制システム、電力管理システム等の環境管理を実施していること、Microsoft Online Services 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、火災検知および抑制システムがあること、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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立（Establish Design Requirements）、攻撃の分析（Analyze Attack Surface）、および脅威モデル（Threat Modeling）によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]「RS-03：復元 – ビジネス継続性の計画」 文献[01]「RS-05：復元 – 環境のリスク」 文献[01]「RS-06：復元 – 機器の場所」 文献[01]「RS-07：復元 – 機器の電源の故障」 文献[01]「RM-04：リリース管理 – アウトソース開発」 文献[01]「RM-01：リリース管理 – 新規開発/取得」	–	–	–	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。									
		(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。	Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されています。可能な場合、独立したプロジェクトごとに、ソース コード ライブラリに対して個別のプロジェクト ワークスペースを確保しています。Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフは、自身の業務の遂行のためにアクセスする必要があるワークスペースにのみ、アクセス権限が与えられます。ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されます。 ISO 27001 規格（具体的には付属文書 A の項 11 および 12.4.3）で、"アクセス制御と、プログラム ソース コードに対するアクセス制御" が規定されています。 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、Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されていること、Microsoft Online Services およ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、Microsoft Online Services では年に 1 度、ビジネスへの影響分析として、下記の項目を実施していることが明記されている。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 同文献では、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]「IS-33：情報セキュリティ – ソースコードへのアクセスの制限」 文献[01]「RM-01：リリース管理 – 新規開発/取得」 文献[01]「DG-08：データガバナンス – リスク評価」 文献[01]「LG-02：法律関係 – サードパーティ契約」	–	（マイクロソフト社とのNDAにより開示）	–	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 Office 365 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	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)	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。	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。 マイクロソフトのセキュリティ レスポンス センター (MSRC) 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 Online Services 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 Online Services 全体で主導します。 Microsoft Security Response Center (MSRC) は、毎月第 2 火曜日 (“更新プログラムの火曜日”)、またはゼロデイ攻撃を緩和するための適当な時期に、セキュリティ情報をリリースします。攻撃の可能性に関する概念実証コードが公開された場合や、新しい重要なセキュリティ更新プログラムがリリースされた場合、Microsoft Online Services は、顧客のホスティング環境の脆弱性を修正するために、Microsoft Online Services の対象となるシステムに対して、修正プログラム適用ポリシーに従って修正プログラムを適用する必要があります。	適合可能	文献[01]によると、Microsoft Online Services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、Microsoft Online Services のスタッフおよび契約業者のスタッフは、Microsoft Online Services のすべてのセキュリティ インシデント、脆弱性、および異常動作について迅速に報告し、事前に定義・実装されているポリシーに基づいて規定されている手順に従うことが明示されている。 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、Office 365 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。 文献[05]では、マイクロソフトがセキュリティコミュニティと連携し、セキュリティガイダンスの提供等の対応が明示されている。	公開文書	文献[01]「IS-20：情報セキュリティ－脆弱性/更新プログラム管理」 文献[01]「IS-23：情報セキュリティ－インシデントの報告」 文献[01]「SA-04：セキュリティアーキテクチャ－アプリケーションのセキュリティ」 文献[05] Microsoft Azureのトラストセキュリティセンター	―	―	―	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。 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更なる本人確認 ・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。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 ・計画された変更の特定と文書化 ・変更によって生じる可能性のある影響の評価プロセス ・承認されている非運用環境における変更のテスト ・変更の通知計画 ・変更管理の承認プロセス ・変更の中止と復元計画 (該当する場合) 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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 － 新規開発/取得」 文献[01]「RM-04：リリース管理 － アウトソース開発」	―	―	―	利用者が使用する端末については、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。	Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されています。可能な場合、独立したプロジェクトごとに、ソース コード ライブラリに対して個別のプロジェクト ワークスペースを確保しています。Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフは、自身の業務の遂行のためにアクセスする必要があるワークスペースにのみ、アクセス権限が与えられます。ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されます。 ISO 27001 規格 (具体的には付属文書 A の項 11 および 12.4.3) で、“アクセス制御と、プログラム ソース コードに対するアクセス制御” が規定されています。 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、Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されていること、Microsoft Online Services およ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、Microsoft Online Services では年に 1 度、ビジネスへの影響分析として、下記の項目を実施していることが明記されている。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 同文献では、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]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「RM-01：リリース管理 － 新規開発/取得」 文献[01]「DG-08：データガバナンス－リスク評価」 文献[01]「LG-02：法律関係 － サードパーティ契約」	―	（マイクロソフト社とのNDAにより開示）	―	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 Office 365 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	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	
		(10)	保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。	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。	－	－	－	－	－	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。
	2.6.2.開発施設、試験施設と運用施設の分離	(1)	情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。	マイクロソフトでは、Office 365 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)、および脅威モデル (Threat Modeling) によって、マイクロソフトが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の要素を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 (具体的には付属文書 A の項 12.5) 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。 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。	適合可能	文献[01]では、Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されていること、Microsoft Online Services およ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[11]では、マイクロソフトが開発し、Microsoft Online Services 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。	公開文書	文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「RM-01：リリース管理 － 新規開発/取得」 文献[11]	－	－	－	－
		(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。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 ・計画された変更の特定と文書化 ・変更によって生じる可能性のある影響の評価プロセス ・承認されている非運用環境における変更のテスト ・変更の通知計画 ・変更管理の承認プロセス ・変更の中止と復元計画 (該当する場合) 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]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。 文献[01]では、マイクロソフトがMicrosoft Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトが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の要素を特定されることが明示されている。 文献[01]では、Microsoft Online Services では、非運用環境と運用環境の個別の環境が用意されていること、運用環境へのアクセス権は慎重に制御されること、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明記されている。	公開文書	文献[01]「RM-01：リリース管理 － 新規開発/取得」 文献[01]「RM-04：リリース管理 － アウトソース開発」 文献[01]「SA-06：セキュリティアーキテクチャ － 運用/非運用環境」	－	－	－	－
		(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。									

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 Office 365 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	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	
		(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。	Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されています。可能な場合、独立したプロジェクトごとに、ソース コード ライブラリに対して個別のプロジェクト ワークスペースを確保しています。Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフは、自身の業務の遂行のためにアクセスする必要があるワークスペースにのみ、アクセス権限が与えられます。ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されます。 ISO 27001 規格 (具体的には付属文書 A の項 11 および 12.4.3) で、"アクセス制御と、プログラム ソース コードに対するアクセス制御" が規定されています。	適合可能	文献[01]では、Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されていること、Microsoft Online Services およ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、Microsoft Online Services では年に 1 度、ビジネスへの影響分析として、下記の項目を実施していることが明記されている。 ・Microsoft Online Services ビジネス環境およびプロセスに関連する脅威の特定 ・可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 同文献では、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]「IS-33：情報セキュリティ – ソースコードへのアクセスの制限」 文献[01]「RM-01：リリース管理 – 新規開発/取得」 文献[01]「DG-08：データガバナンス – リスク評価」 文献[01]「LG-02：法律関係 – サードパーティ契約」	–	（マイクロソフト社とのNDAにより開示）	–	–
		(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。	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。 マイクロソフトのセキュリティ レスポンス センター (MSRC) 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 Online Services 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 Online Services 全体で主導します。 Microsoft Security Response Center (MSRC) は、毎月第 2 火曜日 ("更新プログラムの火曜日")、またはゼロデイ攻撃を緩和するための適当な時期に、セキュリティ情報をリリースします。攻撃の可能性に関する概念実証コードが公開された場合や、新しい重要なセキュリティ更新プログラムがリリースされた場合、Microsoft Online Services は、顧客のホスティング環境の脆弱性を修正するために、Microsoft Online Services の対象となるシステムに対して、修正プログラム適用ポリシーに従って修正プログラムを適用する必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 12.6) で、"技術的な脆弱性の管理" が規定されています。 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	文献[01]によると、Microsoft Online Services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、Microsoft Online Services のスタッフおよび契約業者のスタッフは、Microsoft Online Services のすべてのセキュリティ インシデント、脆弱性、および異常動作について迅速に報告し、事前に定義・実装されているポリシーに基づいて規定されている手順に従うことが明示されている。 文献[01]には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。 また、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、および教訓の学習）により対応することが明示されている。 文献[05]では、マイクロソフトがセキュリティコミュニティと連携し、セキュリティガイダンスの提供等の対応が明示されている。	公開文書	文献[01]「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」 文献[01]「IS-21：情報セキュリティ – ウイルス/悪意のあるソフトウェアへの対策」 文献[01]「IS-22：情報セキュリティ – インシデント管理」 文献[01]「IS-23：情報セキュリティ – インシデントの報告」 文献[05] Microsoft Azureのトラストセキュリティセンター	–	–	–	利用者が使用する端末については、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。

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 Office 365 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	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
		(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	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてウイルスがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。関連するサービスの説明やサービス レベル契約 (SLA) に、その他の情報が記載されている場合があります。 マイクロソフトは独自のセキュリティ レスポンス センター (MSRC) を運営しており、すべての範囲のマイクロソフト製品に関する情報を当社のすべてのお客様に提供しています。詳細については、http://www.microsoft.com/ja-jp/security/msrc/default.aspx 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 10.4) で、"悪意のあるコードからの保護" が規定されています。	適合可能	文献[01]には、Microsoft Online Servicesが一般的な悪意のあるソフトウェアから確実に保護されるようにウイルス対策ソフトウェアを複数の層で実行していること、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行していることが明記されている。	公開文書	文献[01]「IS-21：情報セキュリティ－ウイルス/悪意のあるソフトウェアへの対策」	―	―	―	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。									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。	―	対象外	―	―	―	―	―	―	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をすることが考えられる。このような第三者が提供するサービスの利用に関して、以下の管理策を実施すること。	―	適合可能	以下の各項目で対応を確認した。	―	―	―	―	―	―

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 Office 365 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	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	
		(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し、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。	適合可能	文献[65]、文献[66]およびNDA文書では、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。 また、文献[65]および文献[66]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、問合せ対応、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[65](OST) 文献[66](SLA)	―	―	（マイクロソフト社とのNDAにより開示）	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 Online Services 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、およ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。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、Microsoft Online Services 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。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。	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。 文献[01]では、Microsoft Online Services 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。 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]「FS-01：施設のセキュリティ – ポリシー」 文献[01]「OP-04：運用管理 – 機器のメンテナンス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者が使用する端末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。									
		(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。	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、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]「FS-01：施設のセキュリティ – ポリシー」	―	（マイクロソフト社とのNDAにより開示）	―	―

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 Office 365 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	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)	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アプリケーションや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文書を確認したところ、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]「FS-02：施設のセキュリティ – ユーザーアクセス」 文献[01]「FS-03：施設のセキュリティ – 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	ー
		(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 Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合） 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 Online Services 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」を適用していること、セキュリティ開発ライフサイクルにより設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトが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の要素を特定されることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 – 新規開発/取得」 文献[01]「RM-04：リリース管理 – アウトソース開発」	（マイクロソフト社とのNDAにより開示）	ー	ー	利用者が使用する端末については、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。	ー	ー	ー	ー	ー	ー
	2.6.6.ネットワークセキュリティ管理	(1)	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行うこと。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行うこと。	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、Office 365 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 セグメントを作成するように設計されていること、重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できること、。Active Directory における組織単位 (OU) により、共有システム リソースを介した許可されていない不慮の情報転送を制御および防止す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。	公開文書	文献[01]「SA-09：セキュリティアーキテクチャー – 分離」 文献[27] 文献[130]	ー	ー	ー	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、安全性を確保する必要がある。
		(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。）。									

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 Office 365 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	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)	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出来た。	要NDA	―	―	（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。
		(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[01]では、Microsoft Online において、電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動などの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プロセスを開発し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、サービス管理地一宇賀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文書を確認したところ、CSIRTに相当する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。 NDA文書を確認したところ、CSIRTに相当する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]「IS-30：情報セキュリティ－診断/構成ポートへのアクセス」 文献[01]「IS-22：情報セキュリティインシデント管理」 文献[01]「SA-09：セキュリティアーキテクチャー － 分離」 文献[27] 文献[99]インフラストラクチャの保護 文献[130] 文献[131]	―	―	（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、安全性を確保する必要がある。
		(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。									
		(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。									
		(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。									
		(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。									
		(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。

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 Office 365 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	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	
		(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。	お客様は、Online Service で使用する場合にのみソフトウェアをインストールして使用することができます。Online Service 固有の条件により、お客様が使用できる本ソフトウェアの部数またはお客様が本ソフトウェアを使用できるデバイスの数が制限される場合があります。お客様のソフトウェア使用権は、Online Service のアクティベーション時に開始し、お客様の Online Service の使用権が終了したときに終了します。お客様の本ソフトウェアの使用権が終了した場合、お客様は本ソフトウェアをアンインストールしなければなりません。お客様の本ソフトウェアの使用権が終了した時点で、マイクロソフトはお客様による本ソフトウェアの使用を無効にすることができます。	適合可能	文献[65]によると、Microsoft Online Services の使用にあたり、利用者の管理者は必要な適切なサブスクリプション ライセンスを取得し、割り当てる必要があること、及び、Online Services の使用権はOnline Service のアクティベーション時に開始し、お客様の Online Service の使用権が終了したときに終了することが記載されている。	公開文書	文献[65]「標準の条件」	ー	ー	ー	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 Office 365 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	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	
		(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。	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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。 · 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。 · マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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、業務の正当性に基づいて Microsoft Online Services 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、およ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およ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。 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]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「SA-14：セキュリティアーキテクチャー － 監査ログ/侵入検出」 文献[131]	―	（マイクロソフト社とのNDAにより開示）	―	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。 利用者が使用する端末については、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。

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 Office 365 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	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	
		(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。	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 Online Services 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。 · マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。	適合可能	文献[01]では、不正アクセス検知時およ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。 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[62]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。 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]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[131] 文献[62]	ー	（マイクロソフト社とのNDAにより開示）	ー	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。 利用者が使用する端末については、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。	ー	対象外	ー	ー	ー	ー	ー	ー	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。 □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。	Office 365 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 セグメントを作成するように設計されています。このセグメント化により、重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。 データの保存や処理は、Active Directory® 構造と、特にマルチテナント環境の構築、管理、安全確保に役立てるために開発された各種機能によって、同じサービスのお客様の間で論理的に分離されます。 マルチテナント セキュリティ アーキテクチャーにより、共有の Office 365 データ センターに格納されているお客様のデータが、他の組織によってアクセスされたり他の組織に漏えいしたりすることのないようにしています。Active Directory における組織単位 (OU) により、共有システム リソースを介した許可されていない不慮の情報転送を制御および防止します。テナントは、Active Directory を介して論理的に適用されるセキュリティ境界 (サイロ) に基づいて相互に分離されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。	適合可能	文献[01]には、インターネットを介して提供されるサービスに対する顧客のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了し、これらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されること、デスクトップとデータ センターの間でデータの機密性や整合性が確保されることが明示されている。 文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 さらにインタビューにて、Express Routeにて接続される場合であっても、httpsによる通信の暗号化が行われていること及び、Azureに対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[01]「SA-09：セキュリティ アーキテクチャー – 分離」 文献[107]	ー	（マイクロソフト社とのNDAにより開示）	ー	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。

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 Office 365 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	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	
			□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。	Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモート ワーカーから Office 365 への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Office 365 データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[01]では、Office 365 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 セグメントを作成するように設計されており重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できること、顧客とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されデスクトップとデータ センターの間でデータの機密性や整合性が確保されること、Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現できることが明示されている。 またインタビューにて、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー – 分離」	―	（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、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 Online Services 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 Online Services では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。	公開文書	文献[01]「DG-05：データ ガバナンス – 安全な廃棄」	―	―	―	利用者が使用する端末については、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。									
		(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。
		(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 Office 365 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	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)	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。	Microsoft Online Services には、個々のサービスの説明での定義に従って、お客様がデータ保持ポリシーを適用するための機能が用意されています。バックアップの場合、内容がプライマリー 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ます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 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、レプリケーション機能を備えており、ディスクの上長構成から、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されていることが明記されている。	公開文書	文献[01]「DG-04：データ ガバナンス - 保持ポリシー」	―	―	―	利用者が使用する端末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。
		(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 Online Services 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 Online Services では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。	公開文書	文献[01]「DG-05：データ ガバナンス - 安全な廃棄」	―	―	―	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	マイクロソフトは、マイクロソフトのセキュリティ対策ならびに顧客データにアクセス可能なマイクロソフト担当者の関連手順および責務を規定したセキュリティ関連文書を保持します。 マイクロソフトは、パブリック ネットワークから送信される悪質なソフトウェアを含め、悪質なソフトウェアが顧客データに不正アクセスしないようにするためのマルウェア制御機能を備えています。 マイクロソフトは、パブリック ネットワークを介して送信される顧客データを暗号化するか、またはお客様が暗号化できるようにします。	適合可能	文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 文献[65]には、パブリックネットワークを経由して送信されるデータが暗号化されること、通信及び運用管理に関する手順が整備されることが明示されている。	公開文書	文献[01]「IS-18：情報セキュリティ－暗号化」 文献[65]「プライバシーとセキュリティの条件」	―	―	―	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。 利用者が使用する端末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。

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 Office 365 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	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	
		(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。	お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。 マルチテナント セキュリティ アーキテクチャーにより、共有の Office 365 データ センターに格納されているお客様のデータが、他の組織によってアクセスされたり他の組織に漏えいしたりすることのないようにしています。Active Directory における組織単位 (OU) により、共有システム リソースを介した許可されていない不慮の情報転送を制御および防止します。テナントは、Active Directory を介して論理的に適用されるセキュリティ境界 (サイロ) に基づいて相互に分離されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。	適合可能	文献[01]には、インターネットを介して提供されるサービスに対する顧客のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了し、これらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されること、デスクトップとデータ センターの間でデータの機密性や整合性が確保されることが明示されている。 文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 さらにインタビューにて、Express Routeにて接続される場合であっても、httpsによる通信の暗号化が行われていること及び、Azureに対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[01]「SA-09：セキュリティ アーキテクチャー – 分離」	–	（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、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 Office 365 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	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	
		(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。	インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。	適合可能	文献[01]には、インターネットを介して提供されるサービスに対する顧客のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了し、これらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されること、デスクトップとデータ センターの間でデータの機密性や整合性が確保されることが明示されている。 文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 文献[107]では、公共のインターネット回線を利用せず、IP-VPNによる専用のプライベート接続（Express Route）でオンプレミスの環境からMicrosoft Office 365 Online に接続できることが記載されている。 さらにインタビューにて、Express Routeにて接続される場合であっても、httpsによる通信の暗号化が行われていること及び、Azure に対してVPN接続を行い、Azure を経由してOffice 365にアクセスすることにより、オープンネットワークを介した接続を回避する方法も採用できることを確認した。	要NDA	文献[01]「SA-09：セキュリティ アーキテクチャー – 分離」 文献[01]「IS-18：情報セキュリティ – 暗号化」	–	（マイクロソフト社とのNDAにより開示）	–	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。 利用者が使用する端末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。									
			・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。									
			・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。	Exchange Online における電子メールの場合には、未達の際に最終的に NDR が返送される仕組みとなります。SharePoint Online におけるドキュメントライブラリの場合には、アップロード失敗の場合には、その旨画面に表示される仕組みとなります。	適合可能	インタビューにて、Exchange Online のメール送信、及び SharePoint Online のドキュメントアップロードに関して、システム上の障害によりデータ送信に失敗する場合は、その結果を利用者に通知する仕組みが整っていることが確認された。	要NDA	–	–	（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。	マイクロソフトでは、職務分離の原則を採用し、テスト環境や運用環境へのアクセスをポリシーに応じて制限しています。 お客様の非公開データを運用環境から非運用環境に移動またはコピーすることは、お客様の同意が得られた場合や、マイクロソフトの法務部門の指示による場合を除き、明示的に禁止されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.4 および 12.4.2) で、"開発設備、テスト設備、および運用設備の分離とシステム テスト データの保護" が規定されています。	適合可能	文献[01]において、Microsoft Online Services では、非運用環境と運用環境の、個別の環境が用意されており、特定の業務を遂行する権限があり、アクセスを必要とするメンバーにアクセス権を与えるよう、運用環境へのアクセスは慎重に制御されていることが明記されている。 文献[01]では、職務分離の原則を採用し、テスト環境や運用環境へのアクセスをポリシーに応じて制限していること、顧客の非公開データを運用環境から非運用環境に移動またはコピーすることは、顧客の同意が得られた場合や、マイクロソフトの法務部門の指示による場合を除き、明示的に禁止されていることが明記されている。	公開文書	文献[01]「SA-06：セキュリティ アーキテクチャー – 運用/非運用環境」 文献[01]「DG-06：データ ガバナンス – 非運用データ」	–	–	–	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。									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。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画 (該当する場合) 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]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 – 新規開発/取得」	–	–	–	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。

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 Office 365 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	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
		(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。	Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されています。可能な場合、独立したプロジェクトごとに、ソース コード ライブラリに対して個別のプロジェクト ワークスペースを確保しています。Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフは、自身の業務の遂行のためにアクセスする必要があるワークスペースにのみ、アクセス権限が与えられます。ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されます。 ISO 27001 規格 (具体的には付属文書 A の項 11 および 12.4.3) で、"アクセス制御と、プログラム ソース コードに対するアクセス制御" が規定されています。	適合可能	文献[01]では、Microsoft Online Services のソース コード ライブラリへのアクセスは、権限が与えられた Microsoft Online Services のスタッフおよび Microsoft Online Services の契約業者のスタッフに制限されていること、ソース コード ライブラリに対する変更の詳細を記録した監査ログが保持され、定期的な監査中に確認されることが明示されている。	公開文書	文献[01]「IS-33：情報セキュリティ – ソース コードへのアクセスの制限」	–	–	–	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。	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 Online Services 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。 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	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[01]では、Microsoft Online Services 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、およ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。	要NDA	文献[01]「IS-07：情報セキュリティ – ユーザーアクセスポリシー」 文献[01]「IS-10：情報セキュリティ – ユーザーアクセスの確認」 文献[01]「IS-08：情報セキュリティ – ユーザーアクセスの制限/承認」 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」	–	（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。	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。 マイクロソフトのセキュリティ レスポンス センター (MSRC) 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 Online Services 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 Online Services 全体で主導します。 Microsoft Security Response Center (MSRC) は、毎月第 2 火曜日 ("更新プログラムの火曜日")、またはゼロデイ攻撃を緩和するための適当な時期に、セキュリティ情報をリリースします。攻撃の可能性に関する概念実証コードが公開された場合や、新しい重要なセキュリティ更新プログラムがリリースされた場合、Microsoft Online Services は、顧客のホスティング環境の脆弱性を修正するために、Microsoft Online Services の対象となるシステムに対して、修正プログラム適用ポリシーに従って修正プログラムを適用する必要があります。	適合可能	文献[01]によると、Microsoft Online Services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、Microsoft Online Services のスタッフおよび契約業者のスタッフは、Microsoft Online Services のすべてのセキュリティ インシデント、脆弱性、および異常動作について迅速に報告し、事前に定義・実装されているポリシーに基づいて規定されている手順に従うことが明示されている。	公開文書	文献[01]「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」 文献[01]「IS-23：情報セキュリティ – インシデントの報告」	–	–	–	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。									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 Office 365 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	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
		(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。	Active Directory には、アクセスおよびログ活動を制限するメカニズムが備わっています。 ISO 27001 規格 (具体的には付属文書 A の項 11.4.2) で、"外部接続に対するユーザー認証" が規定されています。	適合可能	文献[01]では、Active Directory には、アクセスおよびログ活動を制限するメカニズムが備わっていること、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[17]では、多要素認証として電話による第2要素が使用でき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。	公開文書	文献[01]「IS-34：情報セキュリティ - ユーティリティ プログラム アクセス」 文献[01]「SA-02：セキュリティアーキテクチャー - ユーザーID資格情報」 文献[17] 文献[31]	―	―	―	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。	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。							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。	システム管理者の操作に関する監査ログを取得することができ、システム管理者が万が一不正行為を実施した場合であっても、それを検知することが可能となります。	適合可能	文献[118]にて、Exchange Online におけるシステム管理者による設定の変更の操作を監査ログとして取得できることが明記されている。 また、文献[119]にて、SharePoint Online における、システム管理者を含むユーザによる様々なアクティビティの監査ログを取得し、レポートが可能であることが明記されている。	公開文書	文献[118] 文献[119]	―	―	―	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。	暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格 (具体的には付属文書 A の項 10.8) で、"情報の交換" が規定されています。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 ISO 27001 規格 (具体的には付属文書 A の項 10.7.3) で、"メディアの取り扱い" が規定されています。 お客様とマイクロソフト データ センターの間で確立される接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。	適合可能	文献[01]には、インターネットを介して提供されるサービスに対する顧客のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了し、これらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されること、デスクトップとデータ センターの間でデータの機密性や整合性が確保されることが明示されている。 文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。	要NDA	文献[01]「IS-18：情報セキュリティ - 暗号化」 文献[01]「IS-19：情報セキュリティ - 暗号化キーの管理」 文献[01]「SA-09：セキュリティ アーキテクチャー - 分離」	―	―	―	―
		(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。	保存されているデータについては、Office 365 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。	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。	公開文書	文献[05]	―	―	―	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を適切に選択する必要がある。

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 Office 365 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	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	
		(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 RMS サービスによる暗号化に関しては、マイクロソフトがテナント キーを管理するのではなく、組織に該当する特定の規制に準拠するために、お客様自身でテナント キーを管理する（Bring Your Own Key）ことが可能となります。	適合可能	文献[120]には、Azure Right Management サービスを併用することにより、利用者独自の暗号鍵を持ち込み、Office 365 テナントの暗号鍵を管理することができることが明記されている。	公開文書	文献[120]	―	―	―	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。	Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルは暗号化されて保存されています。 Office 365ではOutlook、Outlook on the Web（OWA）、EASクライアントにおいて S/MIME によるお客様暗号鍵を使った暗号化、電子署名を行うことが可能です。 暗号方式についてはマイクロソフト全体のセキュリティ等活を行う部門が使用を中止すべき方式を決定し、その決定を受けてOffice 365側での設定を変更します。 暗号化技術に特化した情報提供サイトを公開しております。 [参考情報] Microsoft Trust Center https://www.microsoft.com/en-us/TrustCenter/Security/Encryption	適合可能	文献[17]では、電子メールの利用時にS/MIMEによる利用者の暗号鍵を使った暗号化、電子署名が利用可能であることが明示されている。	公開文書	文献[17]	―	―	―	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 Online Services 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 Online Services 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]	―	（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。

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 Office 365 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	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	
	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。	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 Online Services 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 Online Services 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 Online Services 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。 スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 · マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。	適合可能	文献[01]では、不正アクセス検知時およ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。 また、インタビュー等を通じて、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていることが確認できた。	要NDA	文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[131]	ー	（マイクロソフト社とのNDAにより開示）	ー	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。	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 Online Services 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 Online Services 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 Online Services 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 Online Services のセキュリティ制御を検	適合可能	文献[01]では、不正アクセス検知時およ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、およ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、ログ保持期間はExchange Online は90日間、SharePoint Online は30日間としていること、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。	要NDA	文献[01]「IS-23：情報セキュリティ – インシデントの報告」 文献[01]「CO-01：コンプライアンス – 監査計画」 文献[131]	ー	（マイクロソフト社とのNDAにより開示）	ー	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 Office 365 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	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	
				証しています。 Microsoft Online Services のスタッフおよび契約業者のスタッフは、Microsoft Online Services のすべてのセキュリティ インシデント、脆弱性、および異常動作について迅速に報告する必要があります。これらのイベントの報告と処理は、定義され、実装されているポリシーに基づいて規定されている手順に従います。 Microsoft Online 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ます。セキュリティ イベントには、当社の機器や施設内に格納されているお客様のデータへの不法行為によるアクセス、お客様のデータの損失、開示、変更につながる不正アクセスなどが挙げられますが、これら以外にもあります。 ISO 27001 規格 (具体的には付属文書 A の項 13.1.2 および 13.2) で、"セキュリティの脆弱性に関する報告、および責任と手順" が規定されています。							
		(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。	Microsoft Online Services 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 Online Services 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 Online Services 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。	適合可能	文献[01]では、Microsoft Online Services 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 Online Services 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。	公開文書	文献[01]「SA-12：セキュリティアーキテクチャ – 時刻の同期」	(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。		適合可能	文献[01]では、Microsoft Online Services で使用する時刻同期用サーバが、Office 365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。	公開文書	文献[01]「SA-12：セキュリティアーキテクチャ – 時刻の同期」	(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。	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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]「IS-15：情報セキュリティ – 職務分離」 文献[01]「IS-07：情報セキュリティ – ユーザー アクセス ポリシー」	―	―	―	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。	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 Online Services 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 Online Services 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。 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があることが明示されている。 文献[19]では、障害監視およ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。	公開文書	文献[01]「OP-03：運用管理 – 容量/リソース計画」 文献[01]「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」 文献[01]「CO-01：コンプライアンス – 監査計画」 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。

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 Office 365 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	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	
			・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。	情報システム監査ツールへのアクセスは、Microsoft Online Services 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 Online Services 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。	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 Online Services 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できるようにしていることが明示されている。	公開文書	文献[01]「IS-29：情報セキュリティ－監査ツールへのアクセス」	（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。	―	対象外	―	―	―	―	―	―	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。	―	対象外	―	―	―	―	―	―	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。	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 Online Services 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 Online Services 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、およ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 Online Services 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]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ/整合性」	―	―	―	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。
		(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。		適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」	―	―	―	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け、アプリケーションやオペレーションシステムでの権限を設定すること。		適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」	―	―	―	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 Office 365 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	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	
	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。	スタッフおよび契約業者のスタッフによる Microsoft Online Services 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。 · マイクロソフトのユーザーには、リモート アクセス セッションを確立するために、有効な証明書と有効なドメイン アカウントが含まれているスマートカードが Microsoft Online Services から発行されます。 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。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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、およ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 Online Services 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。	公開文書	文献[01]「IS-08: 情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「FS-02: 施設のセキュリティ - ユーザーアクセス」 文献[01]「SA-07: セキュリティアーキテクチャー - リモートユーザーの多要素認証」 文献[31]	ー	ー	ー	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。	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 Online Services 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。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services 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、およ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、およ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 Online Services 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。	公開文書	文献[01]「IS-08: 情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「FS-02: 施設のセキュリティ - ユーザーアクセス」	ー	ー	ー	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。	· 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、業務の正当性に基づいて Microsoft Online Services 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、およ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、およ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 Online Services 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。	公開文書	文献[01]「IS-08: 情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「FS-02: 施設のセキュリティ - ユーザーアクセス」	ー	ー	ー	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 Office 365 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	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	
		(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。	Office 365 サービスでは、異なるホスティング サービスの開発スタッフや運用スタッフが、職務分離の原則に従うようにすることができます。ソース コード、ビルド サーバー、および運用環境に対するアクセスは、厳しく制御されています。 マイクロソフトの担当者は、マルチテナント環境の委託が行われる前にサーバーを構築します。サーバーの構築が完了すると、構築チームは自身のアクセス許可を削除します。サーバーを委託した時点から、マイクロソフトの担当者が委託されたサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 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、Office 365 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、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっている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 Online Services 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 Online Services 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]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」	―	―	―	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。	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。	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 Online Services 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、およ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、およ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。	公開文書	文献[01]「IS-27：情報セキュリティ－資産の返却」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」	―	―	―	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。	ユーザーとプロセスの観点から、違反の防止には、すべてのオペレータ/管理者によるアクセスと操作の監査、サービスにおける管理者の無期限のアクセス許可の不適用、サービスのトラブルシューティングを行うエンジニア特権への "適宜（JIT）アクセスと昇格"（つまり、昇格は必要に応じ、かつ必要時にのみ与える）、および運用アクセス環境と従業員の電子メール環境の分離を実施しています。 また、過去に使用したアカウントの再利用は行っておりません。	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 Office 365 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[17]には、システム管理者としてのアカウントが用意されているわけではなく、必要なタイミングに限定して特権に昇格する運用が行われていることが明示されている。 またインタビューにより、マイクロソフト内部でIDの使いまわしは行っていないことが確認できた。	要NDA	文献[01]「FS-02：施設のセキュリティ－ユーザーアクセス」 文献[17]	―	（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。	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 Online Services 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 Online Services 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 Online Services 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、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっている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 Online Services 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 Online Services 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 Online Services の資産にアクセスする権限の付与されること、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、およ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、およ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。	公開文書	文献[01]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」	―	―	―	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 Office 365 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	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)	特権IDの発行は必要な最小限のものに留めること。	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 Online Services 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 Online Services 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 Online Services 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、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっている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 Online Services 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 Online Services 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]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」	―	（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おけるID管理を適切に実施する必要がある。
		(9)	特権使用者に昇格可能な作業者IDを制限すること。	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 Online Services 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 Online Services 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 Online Services 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、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっている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 Online Services 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 Online Services 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。	公開文書	文献[01]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセス ポリシー」	―	（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 Office 365 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	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	
		(10)	特権の使用時には作業実施内容を記録すること。	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 Online Services 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。 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。 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、Microsoft Online Services 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、およ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。 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。	要NDA	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「SA-14：セキュリティアーキテクチャー－監査ログ/侵入検出」	―	（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。	Microsoft Online Services 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	―	―	（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。	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。 Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。	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は、Microsoft Online Services がスポンサーとなっている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 Online Services 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 Online Services 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]「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-15：情報セキュリティ－職務分離」 文献[01]「IS-07：情報セキュリティ－ユーザー アクセスポリシー」	―	（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 Office 365 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	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	
		(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。	Office 365 のユーザー管理を社内の Active Directory と連携させることができます。社内の管理者は、パスワードポリシー、2 要素認証要件、ロックアウトの制御などの設定を含む、Office 365 利用ユーザーの資格情報ポリシーを管理できます。 Azure Active Directory を使用すると、ユーザーがサービスとしてのソフトウェア (SaaS) アプリケーションへのシングル サインオンを利用できるようになります。たとえば、Microsoft Office 365 ではこのテクノロジが使用されており、Azure やその他のクラウド プラットフォームで実行されるアプリケーションでも使用できます。	適合可能	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。	公開文書	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。
		(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。		適合可能	インタビュー等を通じて、以下の事項を確認した。 ・マイクロソフト社内の作業者についてはマイクロソフト内部のADにより管理されており、定期的なパスワードの変更や一定数世代のパスワード使い回しの禁止などの制限を行っている。 ・SIerなどのサービス提供事業者の作業者については、Azure Active Directory (Azure AD) 及び Active Directory Federation Services (AD FS) を使用し、組織が管理するオンプレミスの Active Directory (AD) との間でフェデレーション関係を確立することにより、オンプレミスの組織アカウントによって Microsoft Office 365 Online 上のサービスに対するログインが可能となり、パスワードの管理ポリシーはオンプレミスのADによって制御可能である。	要NDA	―	―	（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。									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つけない機構とすること。	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 Online Services 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 Online Services 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、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。 また、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]「SA-02：セキュリティアーキテクチャー － ユーザーID資格情報」	―	（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おけるID管理を適切に実施する必要がある。
		(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。		適合可能	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。	公開文書	文献[01]「SA-02：セキュリティアーキテクチャー － ユーザーID資格情報」	―	―	―	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。		適合可能	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。	公開文書	文献[01]「SA-02：セキュリティアーキテクチャー － ユーザーID資格情報」	―	―	―	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。	Microsoft Online Services では、Active Directory を使用して、パスワード ポリシーの適用状況を管理しています。Microsoft Online Services システムは、強制的にユーザーに複雑なパスワードを使用させるように構成されています。パスワードには最長の有効期限と最小文字数が割り当てられます。 Microsoft Online Services が所有されている環境または運用されている環境に関連サービスまたはシステムを導入する場合、その前に契約者提供の既定のパスワードを変更することが、パスワードの取り扱い要件に含まれています。 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。	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	―	―	（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 Office 365 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	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	
		(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。	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。 Office 365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。 Office 365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。	適合可能	文献[01]では、業務の正当性に基づいて Office 365 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、およ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。	公開文書	文献[01]「IS-07: 情報セキュリティ - ユーザーアクセスポリシー」 文献[01]「IS-08: 情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「IS-10: 情報セキュリティ - ユーザーアクセスの確認」 文献[01]「IS-33: 情報セキュリティ - ソースコードへのアクセスの制限」 文献[01]「SA-03: セキュリティアーキテクチャー - データのセキュリティ/整合性」 文献[127]	ー	ー	ー	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。
		(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。	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。	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]「IS-17: 情報セキュリティ - 作業領域」	ー	ー	ー	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 Office 365 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	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	
		(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。	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 Office 365 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。 Office 365 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。 Office 365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。 Office 365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。	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。 また、インタビュー等を通じて、以下の事項を確認した。 ・マイクロソフト社内の作業者についてはマイクロソフト内部のADにより管理されており、一定数のパスワード入力失敗の際にはアカウントをロックアウトするなどの制限を行っている。 ・Slerなどのサービス提供事業者の作業者については、Azure Active Directory (Azure AD) 及び Active Directory Federation Services (AD FS) を使用し、組織が管理するオンプレミスの Active Directory (AD) との間でフェデレーション関係を確立することにより、オンプレミスの組織アカウントによって Azure 上のサービスに対するログインが可能となり、パスワードの入力不成功時における挙動はオンプレミスのADによって制御可能である。	要NDA	文献[01]「SA-02：セキュリティアーキテクチャー – ユーザーID資格情報」 文献[27]	―	（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 Online Services がスポンサーとなっているセキュリティ 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、当社の従業員との契約に機密保持条項を組み込んでいます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する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従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフが、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。	公開文書	文献[01]「HR-02：人的資源のセキュリティ – 雇用における合意事項」 「IS-11：情報セキュリティ – トレーニング/意識向上」	―	―	―	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。

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 Office 365 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	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	
		(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。	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 Office 365 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。 Office 365 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、Microsoft Online Services では、Microsoft Active Directory を使用してパスワード ポリシーの適用状況を管理していること、複雑なパスワードの使用をユーザーに強制するように構成されていること、パスワードには最長の有効期間と最小文字数が割り当てられていることが記載されている。 また、インタビュー等を通じて、以下の事項を確認した。 ・マイクロソフト社内の作業者についてはマイクロソフト内部のADにより管理されており、パスワード漏えいの際にはアカウントをロックアウトするなどの制限を行っている。 ・SIerなどのサービス提供事業者の作業者については、Azure Active Directory (Azure AD) 及び Active Directory Federation Services (AD FS) を使用し、組織が管理するオンプレミスの Active Directory (AD) との間でフェデレーション関係を確立することにより、オンプレミスの組織アカウントによって Azure 上のサービスに対するログインが可能となり、パスワードの管理ポリシーはオンプレミスのADによって制御可能であるこ。	要NDA	文献[01]「SA-02：セキュリティアーキテクチャー – ユーザーID資格情報」	ー	（マイクロソフト社とのNDAにより開示）	ー	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又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。									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。
		(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。	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。	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]「IS-17：情報セキュリティ – 作業領域」	ー	ー	ー	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。

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 Office 365 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	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	
2.7.人的安全対策			医療情報処理を受託する情報処理事業者において医療情報処理に関する管理を的確に行うため、医療情報に触れる機会を持つ情報処理事業者職員は、原則として情報処理事業者の正規職員に限ることを原則とするが、雇用形態が多様化している実態を踏まえ、派遣従業員等の非正規職員についても、秘密保持契約や情報セキュリティ教育等の履行に万全を期し、正規職員のみによる管理と同等レベルの管理が行われることを前提として、認めることとする。	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフは、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従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services 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]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよ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[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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□すること ・下請業者はそれ以外の□的のために顧客データを使□することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対して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すること ・Microsoft によって管理されている施設や機器で業務を□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ること	公開文書	文献[01]「HR-02：人的資源のセキュリティ - 雇用における合意事項」 「IS-11：情報セキュリティ - トレーニング/意識向上」 文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[02] 「Microsoft のプライバシー要件	―	―	―	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。										

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 Office 365 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	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	
		(2)	医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフは、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 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従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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Office 365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]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよ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[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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 ・Microsoft が下請業者に対して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すること ・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ること	公開文書	文献[01]「HR-02：人的資源のセキュリティ - 雇用における合意事項」 「IS-11：情報セキュリティ - トレーニング/意識向上」 文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[02]「顧客データが下請業者に開示される場合」 文献[02] 「Microsoft のプライバシー要件」	―	―	―	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。

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 Office 365 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	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)	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。	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 Online Services 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 Online Services 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 Online Services 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 Online Services 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 Online Services 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。	公開文書	文献[65]「標準のプライバシーとセキュリティの条件 セキュリティ インシデントの通知」	―	―	―	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。
		(4)	医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。	従業員の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]「付録 3 – 標準契約条項（処理者向け）第12条：個人データ処理サービスの終了後の義務」	―	（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。

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 Office 365 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	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	
		(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。	マイクロソフト内の該当するすべての従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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 Online Services のすべての契約業者のスタッフは、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 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従業員は、Microsoft Online Services がスポンサーとなっているセキュリティ 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Office 365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]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよ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 Online Services 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[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・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□すること ・下請業者はそれ以外の□的のために顧客データを使□することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対して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すること ・Microsoft によって管理されている施設や機器で業務を□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ること	公開文書	文献[01]「HR-02：人的資源のセキュリティ - 雇用における合意事項」 「IS-11：情報セキュリティ - トレーニング/意識向上」 文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[01]「IS-06：情報セキュリティ - ポリシーの実施」 文献[02]「顧客データが下請業者に開□される場合」 文献[02]「Microsoft のプライバシー要件」	―	―	―	―
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。	―	―	―	―	―	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。	―	―	―	―	―	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。	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、償却など）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。 利用者側の運用管理規定については、利用者が主体的に定める必要があります。	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、すべてのMicrosoft Online Services 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。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。 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およ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]「DG-05：データ ガバナンス - 安全な廃棄」 文献[65]「付録 3 - 標準契約条項（処理者向け） 第 12 条: 個人データ処理サービスの終了後の義務」	―	（マイクロソフト社とのNDAにより開示）	―	―

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 Office 365 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	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	
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。	Microsoft Online Services およ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ます。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画 (該当する場合) 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]によると、Microsoft Online Services では、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、運用変更の管理手順には、変更によって生じる可能性のある影響の評価プロセス・変更のテスト・承認プロセス・変更の中止と復元計画が含まれていることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 - 新規開発/取得」	―	―	―	利用者及びSI事業者は、使用する端末の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 Office 365 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	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)	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。	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベル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ます。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 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、およ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、および改訂のプロセス 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。 イベント発生時にソリューションが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ます。 ISO 27001 規格 (具体的には付属文書 A の項 14.1.5) で、"ビジネス継続性の計画のテスト、保持、および再評価" が規定されています。	適合可能	文献[01]では、Microsoft Online Services にレプリケーション機能が備えられており、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。 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。	公開文書	文献[01]「DG-04：データ ガバナンス - 保持ポリシー」 文献[01]「RS-03：復元 - ビジネス継続性の計画」 文献[01]「RS-04：復元 - ビジネス継続性のテスト」	ー	ー	ー	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。	ー	対象外	ー	ー	ー	ー	ー	ー	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。	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 Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベル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ます。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 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、およ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、および改訂のプロセス 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。 イベント発生時にソリューションが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ます。 ISO 27001 規格 (具体的には付属文書 A の項 14.1.5) で、"ビジネス継続性の計画のテスト、保持、および再評価" が規定されています。	適合可能	文献[01]では、Microsoft Online Services にレプリケーション機能が備えられており、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。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。 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文書を確認したところ、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]「RS-03：復元 - ビジネス継続性の計画」 文献[01]「RS-04：復元 - ビジネス継続性のテスト」 文献[19]「Incident Management Model」	ー	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	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。		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。	公開文書	文献[01]「RS-03：復元 - ビジネス継続性の計画」 文献[01]「RS-04：復元 - ビジネス継続性のテスト」	ー	ー	ー	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。