医療機関向け
『Teams』対応セキュリティリファレンス

2020年 07月30日
Version 1.1

作成者：
株式会社三菱総合研究所（MRI）

Copyright (C) MRI All Rights Reserved.

更新日	版番号	改版内容
2020年6月26日	Version1.0	初版
2020年7月30日	Version1.1	第1.1版

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.1-01	6.情報システムの基本的な安全管理	6.1 方針の制定と公表	（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ドライン」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。	C. 最低限のガイドライン	1. 個人情報保護に関する方針を策定し、公開していること。	マイクロソフトではサービスにおけるセキュリティ対策の契約書への明記やマイクロソフト トラストセンターなどにて幅広く情報を公開しています。 また、ISO 27001など90以上のコンプライアンス認証に対応しており、SOCなど第三者機関による監査も定期的に実施しています。 定期的に情報はアップデートされますので、最新情報はWebサイトをご確認ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products https://www.microsoft.com/ja-jp/trust-center/ https://docs.microsoft.com/ja-jp/microsoftteams/teams-security-guide Microsoft がお客様の顧客データを使用するのは、お客様との間で合意したサービスを提供するため、およびそのサービスの提供と矛盾しない目的に限られます。 Microsoft の広告主によってサポートされるサービスとの間でお客様のデータを共有することはなく、マーケティングや広告を目的としてマイニングすることもありません。 お客様がサービスの利用を終了する場合、Microsoft は、お客様がデータの所有権を引き続き確実に保持できるように必要な手段を取ります。 https://www.microsoft.com/ja-jp/trust-center/privacy/data-management https://privacy.microsoft.com/ja-jp/privacystatement?culture=ja-jp&country=JP	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、個人情報保護に関する方針を策定・公開する必要がある。
6.1-02					C. 最低限のガイドライン	2. 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。	マイクロソフトラスト センターにてセキュリティ、プライバシー、コンプライアンスに関する詳細な情報(お客様のデータの場所、お客様のデータに誰がアクセスできるかなど)を公開しています。 https://www.microsoft.com/ja-jp/trust-center/privacy/data-management またオンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策において物理セキュリティおよび論理セキュリティなどさまざまな対策を明記しています。	適合可能	文献[08]にて、サービス提供事業者として、個人情報の取り扱いについて以下が明示されている。 ・マイクロソフトは、お客様の情報のセキュリティを保護するために努めています。マイクロソフトは、不慮の、不正なまたは違法なアクセス、開示、改変、滅失または破壊から顧客データを保護するために、適切な技術的および組織的な対策を講じており、これを維持しこれに従います。 ・顧客データは、Microsoft Online Serviceの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・無料試用版を除き、マイクロソフトは、お客様のサブスクリプションの満了または終了後90日間、Microsoft Online Serviceに保存されたお客様の顧客データを機能が限定されたアカウントに保持し、お客様がデータを抽出できるようにします。90 日の保持期間の終了後、マイクロソフトはお客様のアカウントを無効にして顧客データを削除します。 ・マイクロソフトがプライバシーまたはセキュリティに関する確約事項を遵守していないとお考えの場合、お客様は、カスタマー サポートまで連絡するか、http://go.microsoft.com/?linkid=9846224 にあるマイクロソフトのプライバシー Web フォームを使用することができます。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	—	—	—	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 医療機関等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		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。	C. 最低限のガイドライン	1. 情報システムで扱う情報を全てリストアップしていること。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データ保護条件 – データ処理の性質（権利の帰属）にて「マイクロソフトは、本条でお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。」が明記されています。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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					C. 最低限のガイドライン	2. 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。	同上 (6.2-01)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、情報資産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					C. 最低限のガイドライン	3. 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。	同上 (6.2-01)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、情報資産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					C. 最低限のガイドライン	4. 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。	同上 (6.2-01)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、情報資産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					C. 最低限のガイドライン	5. 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。	同上 (6.2-01)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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					D. 推奨されるガイドライン	1. 上記の結果を文書化して管理していること。	同上 (6.2-01)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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 組織的安全管理対策（体制、運用管理規程）		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	C. 最低限のガイドライン	1. 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。	公開サイト「トラストセンター」に基づく運用を実施し、公開サイト・コミュニティーなど様々な手段を通じて情報公開を行っています。 https://www.microsoft.com/ja-jp/trust-center またオンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策 – 情報セキュリティの構築においてセキュリティ責任者の役割を明確化しています。	適合可能	文献[08]及び文献[25]にて、マイクロソフトはセキュリティ規則および手順の調整と監視を担当する1人以上のセキュリティ責任者を任命していることが明示されている。 文献[14]にて、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やのセキュリティプログラムに責任を負う組織であるOSSC（Microsoft Online Service Security and Compliance team）について明示されている。 インタビューにて、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が確認できた。このことから管理体制についても整備されていると考えられる。	要NDA	文献[08] 文献[14] 文献[25]	—	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が確認でき、このことから管理体制についても整備されている。	—	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					C. 最低限のガイドライン	2. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策において「施設への物理的アクセス。当社は、顧客データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に限定します。」と明記しています。	適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、物理的な侵入対策を講じていることが明示されている。 文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。 また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[01] 文献[37]	—	—	—	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 Service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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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					C. 最低限のガイドライン	3. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御 (アクセスポリシー、アクセスの許可、最小限の権限など)の対策が明記しています。	適合可能	文献[08]にて、アクセス制御のポリシーを定めていることが明示されている。 また、情報システムへのアクセス制限のルールについて以下が明示されている。 ・マイクロソフトは、顧客データが保管されているマイクロソフト システムへのアクセスを許可されている担当者の記録を保持し、更新します。 ・マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 ・顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID/ログインを割り当てます。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用可能であることが明示されている。	公開文書	文献[08] 文献[25] 文献[26]	–	–	–	利用者は、情報システムのアクセス管理規程及び運用管理規程を作成する必要がある。 利用者は、ネットワーク構成図を作成する必要がある。 利用者は、情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限する必要がある。 利用者は、Microsoft Teams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					C. 最低限のガイドライン	4. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データ保護条件 – 下請け処理者の使用に関する通知および規制において明確化しています。 マイクロソフトは、その下請処理者が本 DPA のマイクロソフトの義務を遵守することに責任を負います。マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。マイクロソフトは、本 DPA がマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。マイクロソフトは、これらの契約上の義務が確実に満たされるように下請処理者を監督することに同意します。	適合可能	文献[25]にて、個人情報の安全管理について以下が明示されている。 ・マイクロソフトは、送信、保存、またはその他の方法で処理された個人データの偶発的または違法な破壊、損失、変更、不正開示、またはアクセスから顧客データおよび個人データを保護するために、適切な技術的および組織的対策を講じ、維持します。これらの対策は、マイクロソフト セキュリティ ポリシーに規定するものとします。 ・マイクロソフトは、当該セキュリティ ポリシーを、Microsoft Online Service について確立されているセキュリティ制御手段の内容ならびに当社のセキュリティ規定およびポリシーに関してお客様が合理的に要求した他の情報と共にお客様に提供します。 なお、上記事項については文献[08]でも一部同様の事柄が明示されている。 インタビューにて、Microsoftとしてデータ保護条件を定めており、お客様と安全管理に関する事項を含んだ契約を締結していることが確認できた。	要NDA	文献[08] 文献[25]	–	Microsoftとしてデータ保護条件を定めており、お客様と安全管理に関する事項を含んだ契約を締結している。	–	利用者は、Microsoft Online Service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					C. 最低限のガイドライン	5. 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）	公開サイト「トラストセンター」に基づく運用を実施し、公開サイト・コミュニティーなど様々な手段を通じて情報公開を行っています。 https://www.microsoft.com/ja-jp/trust-center またオンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策 – 通信および運用管理において運用ポリシーなどについて明確化しています。	適合可能	文献[36]にて、Microsoft Teamsにおけるプライバシー、データ保護等に関する宣言事項が明示されている。 文献[19]、及び文献[32]にて、Microsoft Teamsではプライバシー、コンプライアンス、セキュリティに対する様々な対策がなされ、ISO27001等の各種認証を取得済みであることが明示されている。	公開文書	文献[19] 文献[32] 文献[36]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中に理念を記載する必要がある。 利用者は、Microsoft Online Serviceが定める基本方針等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-06					C. 最低限のガイドライン	(b) 医療機関等の体制	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中に医療機関等の体制を記載する必要がある。 利用者は、Microsoft Online Service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. 最低限のガイドライン	(c) 契約書・マニュアル等の文書の管理	契約書はこちらに公開しています。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。 またオンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策 – 通信および運用管理において運用ポリシー、事業継続性の管理において緊急対応計画などについて明確化しています。	適合可能	NDA文献[N04]、及びインタビューにて、ドキュメントにおけるリテンションポリシーが定められていることが確認できた。	要NDA	–	–	ドキュメントにおけるリテンションポリシーが定められている。	NDA文献[N04]	利用者は、医療情報システムの運用管理規程を定め、その中で文書管理について定める必要がある。 利用者は、Microsoft Online Serviceが定める運用管理規程等が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.3-08					C. 最低限のガイドライン	(d) リスクに対する予防、発生時の対応の方法	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策において情報セキュリティインシデント管理 「インシデント対応プロセス –マイクロソフトは、違反の内容、期間、違反の影響、報告者の名前、違反の報告先、データの回復手順を含む、セキュリティ違反の記録を保持します。 –セキュリティ インシデントとなる各セキュリティ違反について、マイクロソフトは、上記の「セキュリティ インシデントの通知」の規定に従い、過度の遅滞なく、かつ、いかなる場合も 72 時間以内に通知を行います。 –マイクロソフトは、開示されたデータ、データの開示先および開示時刻を含む、顧客データの開示を追跡するか、または お客様が追跡できるようにします。 サービス監視。マイクロソフトのセキュリティ担当者は、少なくとも 6 か月ごとに記録を確認し、必要な場合は改善のための取り組みを提案します。」と明記されています。 インフラ全体の構成と変更管理などはこちらをご参照ください https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure-monitoring	適合可能	文献[18]にて、Teams はMicrosoft 365 (Office 365 含む)サービスの一部として徹底的な防御によるサービスレベルのセキュリティ、サービス内の顧客コントロール、セキュリティ強化、運用上のベスト プラクティスなど、すべてのセキュリティ ベスト プラクティスとプロシージャに従っていることが明示されている。 また、Teams は、Microsoft セキュリティ開発ライフサイクル (Security Development Lifecycle: SDL) に記載されている「Microsoft 信頼できるコンピューティングのセキュリティ開発ライフ サイクル」に準拠して設計、開発されていることが明示されている。 さらに、Teamsサービスのセキュリティに対するより一般的な脅威（ウイルス、盗聴、中間者攻撃等）と、Microsoftがそれらの脅威の軽減に用いる方法を明らかにしていることが明示されている。 文献[08]にて、マイクロソフトは、マイクロソフトの機器またはマイクロソフトの施設内に保管された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、セキュリティ インシデントについての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、セキュリティ インシデント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[08] 文献[18]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中でリスクに対する予防、発生時の対応方法について定める必要がある。 利用者は、Microsoft Online Service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					C. 最低限のガイドライン	(e) 機器を用いる場合は機器の管理	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策においてアセット管理、通信および運用管理について明記しています。	適合可能	文献[04]にて、Microsoft Operations Centersでは専門家チームが配置されており、サービス全体の監視、プロセスの自動化、インフラストラクチャの運用を担当していることが明示されている。 文献[23]にて、ISO27001等の第三者認証を取得、維持していること と、新しい監査レポートとアーカイブ済みの監査レポートが明示されていることから、有効なリスク管理態勢を有していると考えられる。	公開文書	文献[04] 文献[23]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中で機器の管理方法について定める必要がある。 利用者は、Microsoft Online Service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					C. 最低限のガイドライン	(f) 個人情報の記録媒体の管理（保管・授受等）の方法	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策においてアセット管理 「アセット一覧。マイクロソフトは、顧客データが保管されているすべてのメディアの一覧を保持します。かかるメディアの一覧へのアクセスは、かかるアクセスを書面で許可されている当社担当者に制限されます。 アセットの取り扱い –マイクロソフトは顧客データを分類して、識別しやすくするとともに、かかるデータへのアクセスを適切に制限できるようにします。 –マイクロソフトは、顧客データの印刷に制限を課し、顧客データを含む印刷物の廃棄手順を定めています。 –マイクロソフトの担当者は、顧客データを携帯用デバイスに格納し、顧客データにリモート アクセスし、または顧客データをマイクロソフトの施設以外で処理する前に、マイクロソフトの許可を得る必要があります。」と明記しています。	適合可能	文献[08]にて、マイクロソフトは顧客データが保管されているすべてのメディアの一覧を保持し、かかるメディアの一覧へのアクセスは、かかるアクセスを書面で許可されているマイクロソフト担当者に制限されていることが明示されている。 また、これらの取り扱いルールとして以下が明示されている。 ・マイクロソフトは、顧客データを分類して、識別しやすくすると共に、かかるデータへのアクセスを適切に制限できるようにします。 ・マイクロソフトは、顧客データの印刷に制限を課し、顧客データを含む印刷物の廃棄手順を定めています。 ・マイクロソフト担当者は、顧客データを携帯用デバイスに格納し、顧客データにリモートアクセスし、または顧客データをマイクロソフトの施設以外で処理する前に、マイクロソフトの許可を得る必要があります。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中で個人情報の記録媒体の管理方法について定める必要がある。 利用者は、Microsoft Online Service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					C. 最低限のガイドライン	(g) 患者等への説明と同意を得る方法	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 個人データの処理(GDPR)において「お客様とマイクロソフトは、お客様が個人データの管理者であり、マイクロソフトが当該データの処理者であることに合意するものとします。」と明記しています。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中で患者への説明と同意を得る方法について定める必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.3-12					C. 最低限のガイドライン	(h) 監査	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データセキュリティ – 監査コンプライアンスにおいて 「マイクロソフトは、顧客データおよび個人データの処理に使用されるコンピューター、コンピューティング環境および物理的なデータ センターのセキュリティの監査を以下のように実施します。 ・標準規格または枠組みにおいて監査の実施が規定されている場合、かかる管理基準またはフレームワークに関する監査は、少なくとも年 1 回実施されるものとします。 ・各監査は、適用される各管理基準またはフレームワークについて、規制機関または認定機関の標準および規則に従って実施されるものとします。 ・各監査は、当社が選択した適格の独立した第三者のセキュリティ監査人によって、当社の費用負担により実施されるものとします。」 と明記しています。	適合可能	文献[08]にて、マイクロソフトは各Microsoft Online Serviceについて、顧客データ（個人データを含む）の処理に使用されるコンピューター、コンピューティング環境、および物理的なデータ センターのセキュリティの監査を以下のように実施していると明示されている。 ・標準またはフレームワークにおいて監査の実施が規定されている場合、かかる制御標準またはフレームワークに関する監査は、各Microsoft Online Serviceについて少なくとも年 1 回実施されるものとします。 ・各監査は、適用される各制御標準またはフレームワークについて、規制機関または認定機関の標準および規則に従って実施されるものとします。 ・各監査は、マイクロソフトが選択した適格の独立した第三者のセキュリティ監査人によって、マイクロソフトの費用負担により実施されるものとします。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 文献[23]にて、ISO27001等の第三者認証を取得、維持していることと、新しい監査レポートとアーカイブ済みの監査レポートが明示されていることから、有効なリスク管理態勢を有していると考えられる。	公開文書	文献[08] 文献[23] 文献[25]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中で監査方法について定める必要がある。 利用者は、Microsoft Online Service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					C. 最低限のガイドライン	(i) 苦情・質問の受付窓口	サポートに関してはこちらに情報を公開しています。 https://docs.microsoft.com/ja-jp/office365/servicedescriptions/office-365-platform-service-description/support 認証された管理者は、Microsoft 365 管理センターを使用して、サービス要求をオンラインで送信し、アクセスサポートの電話番号を、開いているすべてのサービス要求を表示することができます。管理センターで送信されるサービス要求は、要求がクローズされてから最大14日間、再度開くことができます。手順については、「Microsoft 365 for business サポートへのお問い合わせ」を参照してください。 Microsoft 365 テクニカル サポート チームは、Microsoft 365 および Office 365 に関連する問題のトラブルシューティングのみを行います。お客様のネットワークで発生する問題は、サポートの範囲外にあります。この場合、お客様はネットワーク チームまたはMicrosoft のネットワーク チームに協力を要請する必要があります。	適合可能	文献[24]にて、以下のような質問の受付が可能であることが明示されている。 ・Microsoftアカウントにサインインできない、またはアカウントがハッキングされた ・マイクロソフトの製品、サービス、またはデバイスに技術的な問題がある ・詐欺を報告したい ・デバイスにウイルス、スパイウェア、マルウェアがある ・不審なメールを受け取った ・プライバシーに関する質問や懸念がある	公開文書	文献[24]	–	–	–	利用者は、医療情報システムの運用管理規程を定め、その中で苦情・質問の受付窓口について定める必要がある。 利用者は、Microsoft Online Serviceが実施する受付窓口等の対応が、医療機関等が求める内容を含むものであることを確認する必要がある。
6.4-01		6.4 物理的安全対策		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幾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。 ・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） ・盗難、窃視等の防止 ・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	C. 最低限のガイドライン	1. 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。	マイクロソフトラスト センターにてセキュリティ、プライバシー、コンプライアンスに関する詳細な情報(お客様のデータの場所、お客様のデータに誰がアクセスできるかなど)を公開しています。 https://www.microsoft.com/ja-jp/trust-center/privacy/data-management https://privacy.microsoft.com/ja-jp/privacystatement?culture=ja-jp&country=JP またオンライン サービス データ保護追加契約 (DPA) 付属文書 A – セキュリティ対策（アセット管理、物理セキュリティおよび論理セキュリティ、アクセス制御など）を明記しています。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products	適合可能	文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[37]	–	–	–	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					C. 最低限のガイドライン	2. 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でき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得る手段がある場合はこの限りではない。		適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、物理的な侵入対策を講じていることが明示されている。 文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。 文献[08]及び文献[25]にて、施設への物理アクセスとして、マイクロソフトは顧客データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に制限していることが明示されている。 また、コンポーネントへの物理アクセスとして、マイクロソフトはメディアの種類、許可された送付者/受信者、日付および時刻、メディアの数ならびに含まれる顧客データの種類を含め、顧客データを収録したメディアの出入りを記録していることが明示されている。	公開文書	文献[01] 文献[08] 文献[25] 文献[37]	–	–	–	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					C. 最低限のガイドライン	3. 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。		適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、物理的な侵入対策を講じていることが明示されている。 文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。 また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[01] 文献[37]	–	–	–	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					C. 最低限のガイドライン	4. 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。		適合可能	文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[37]	–	–	–	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					C. 最低限のガイドライン	5. 覗き見防止の対策を実施すること。		適合可能	文献[37]にて、データセンターには、"最小特権"の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。 文献[38]にて、自動化されたプロセスにより、多くのセキュリティ侵害の原因となる人為的エラーを削減できるよう対策を講じていることが明示されている。	公開文書	文献[37] 文献[38]	–	–	–	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.4-06					D. 推奨されるガイドライン	1. 防犯カメラ、自動侵入監視装置等を設置すること。		適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、建物、コンピュータルームには監視カメラを設置していることが明示されている。 また、24時間常駐の警備員を配置していることが明示されている。 文献[37]にて、データセンターには、“最小特権”の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[01] 文献[37]	—	—	—	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 技術的安全対策		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 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	C. 最低限のガイドライン	1. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御 (アクセスポリシー、アクセスの許可、最小限の権限などの対策を明記しています。	適合可能	文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 加えて、NDA文献[N03]にて、Azure AD Premium 2ライセンスを利用することで、AzureADを通して不審なサインインや資格情報の漏洩などに対する多要素認証の強制やパスワードリセット等が行えることが確認できた。	要NDA	文献[33]	—	—	NDA文献[N03]	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					C. 最低限のガイドライン	2. 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 (6.5-01)	適合可能	文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 加えて、NDA文献[N03]にて、Azure AD Premium 2ライセンスを利用することで、AzureADを通して不審なサインインや資格情報の漏洩などに対する多要素認証の強制やパスワードリセット等が行えることが確認できた。	要NDA	文献[33]	—	—	NDA文献[N03]	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、事実と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					C. 最低限のガイドライン	3. 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。	同上 (6.5-01)	適合可能	文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 文献[13]にて、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明示されている。	公開文書	文献[13] 文献[33]	—	—	—	利用者は、多要素認証として設定している手段が利用できない場合であっても業務を停止させないため、その代替手段の設定方法について予め周知しておく必要がある。
6.5-04					C. 最低限のガイドライン	4. 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おそれがある場合には、クリアスクリーン等の防止策を講じること。	同上 (6.5-01)	適合可能	文献[10]にて、Office 365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。 また、文献[34]にて、Microsoft Teamsに対し、Azure Active Directory (Azure AD) によって発行されたトークンの有効期間を指定できることが明示されている。	公開文書	文献[10] 文献[34]	—	—	—	利用者は、医療機関等の利用者側の施設における、適切な端末管理（スクリーンロック等）を行う必要がある。
6.5-05					C. 最低限のガイドライン	5. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策において物理セキュリティおよび論理セキュリティなどさまざまな対策を明記しています。 Microsoft Teams などはMicrosoft Security Development Lifecycleに基づいて設計、開発されています。 https://www.microsoft.com/en-us/securityengineering/sdl/ セキュリティ要件の定義など12のプラクティスを実践しています	適合可能	文献[08]にて、マイクロソフトは、お客様の情報のセキュリティを保護することに努め、不慮の、不正なまたは違法なアクセス、開示、改変、滅失または破壊から顧客データを保護するために、適切な技術的および組織的な対策を講じており、これ維持することが明示されている。 顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Serviceの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 また、顧客データにアクセス可能な担当者に対しては、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適用し、運用管理においてセキュリティ対策を実施していることが明示されている。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 NDA文献[N03]にて、利用者側が行える対策として、Azure AD Premium 2ライセンスを利用することで、Teamsで共有されたファイルの自動分類 (ラベリング) および暗号を実施できることが確認できた。	要NDA	文献[08] 文献[25]	—	—	NDA文献[N03]	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					C. 最低限のガイドライン	6. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御の対策を明記しています。 また、Microsoft Teamsのセキュリティガイドもご参照ください。 https://docs.microsoft.com/ja-jp/microsoftteams/teams-security-guide	適合可能	文献[05]にて、Azure Active Directory (Azure AD) を使用して、Microsoft Teams を管理するために必要な、異なるレベルのアクセス権限を持つ管理者を指定可能であることが明示されている。 また、Teamsの管理者ロールには4種類あり、Teamsサービス管理者、Teams通信管理者、Teams通信サポートスペシャリスト、およびTeams通信サポートエンジニアが含まれ、それぞれのロールに許可されている操作内容が明示されている。 加えて、NDA文献[N03]にて、Azure AD Premium1ライセンスを利用することで、IPアドレス制御等の条件付きアクセスが実施できることが確認できた。	要NDA	文献[05]	—	—	NDA文献[N03]	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。 また、医療情報システムの運用管理規程を定め、その中でアクセス権限の見直しについて定める必要がある。
6.5-07					C. 最低限のガイドライン	7. 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、並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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策を明記しています。 また利用者含めたアクセス、操作ログの確認が可能です。 https://docs.microsoft.com/ja-jp/azure/active-directory/reports-monitoring/concept-sign-ins https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide	適合可能	文献[06]にて、Teamsを含むMicrosoft 365サービスで利用可能な主な監査レポートが明示されている。 文献[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行 文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用可能であることが明示されている。	公開文書	文献[06] 文献[26] 文献[28]	—	—	—	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					C. 最低限のガイドライン	8. 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。		適合可能	文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用可能であることが明示されている。 文献[27]にて、ユーザーが特定のドキュメントを表示したかどうか、またはメールボックスからアイテムを削除したかどうか等について、セキュリティ コンプライアンス センターを使用して統合監査ログを検索し、組織内のユーザーと管理者のアクティビティを確認できることが明示されている。 文献[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	公開文書	文献[26] 文献[27] 文献[28]	—	—	—	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確推した内容	マイクロソフト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	
6.5-09					C. 最低限のガイドライン	9. 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。	時刻同期については以下の情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/windows/time-sync	適合可能	文献[41]にて、Azureホストは内部のMicrosoftタイムサーバーに同期されており、このサーバーでは、GPSアンテナを使用してMicrosoftが所有するStratum1デバイスから時刻を取得していることが明示されている。 また、文献[32]、及びインタビューにて、各種認証を取得済みであることと、サービス提供において正確な時刻同期が行われていることが確認できた。	要NDA	文献[32] 文献[41]	—	各種認証を取得済みであることと、サービス提供において正確な時刻同期が行われている。	—	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。
6.5-10					C. 最低限のガイドライン	10. システム構築時、適切に管理されていないメディア使用時、外部からの情報受信時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	インフラ全体のセキュリティ対策においては以下で情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure セキュリティ更新管理を行うことにより、システムを既知の脆弱性から保護できます。Azure では、統合されたデプロイ システムを使用して、Microsoft ソフトウェアのセキュリティ更新プログラムの記布とインストールを管理します。Azure は、Microsoft セキュリティ レスポンス センター（MSRC）のリソースを利用することもできます。MSRC は、毎日 24 時間体制で、セキュリティ インシデントおよびクラウドの脆弱性を識別、監視、対応、および解決しています。	適合可能	文献[02]にて、セキュリティ開発ライフサイクル（SDL）は、セキュリティの保証とコンプライアンスの要件をサポートする一連のプラクティスで構成されており、SDLは、開発コストを削減しながら、ソフトウェアの脆弱性の数と重大度を低減することが明示されている。 文献[18]にて、Teams は、Microsoft 365サービスおよびOffice 365サービスの一部として徹底的な効率によるサービス レベルのセキュリティ、サービス内の顧客コントロール、セキュリティ強化、運用上のベスト プラクティスなど、すべてのセキュリティ ベスト プラクティスとプロシージャに従っていることが明示されている。 また、Teams は、Microsoft セキュリティ開発ライフサイクル（Security Development Lifecycle: SDL）に記載されている「Microsoft 信頼できるコンピューティングのセキュリティ開発ライフ サイクル」に準拠して設計、開発されていることが明示されている。 さらに、Teamsサービスのセキュリティに対するより一般的な脅威（ウイルス、盗聴、中間者攻撃等）と、Microsoft がそれらの脅威の軽減に用いる方法を明らかにしていることが明示されている。	公開文書	文献[02] 文献[18]	—	—	—	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。
6.5-11					C. 最低限のガイドライン	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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御の対策を明記しています。 利用者のパスワードポリシーはこちらで公開しています。 https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-sspr-policy	適合可能	文献[08]にて、パスワードポリシーについて以下が明示されている。 ・マイクロソフトは、業界標準の規定を使用して、情報システムへのアクセスを試みるユーザーを特定し、認証します。 ・認証メカニズムがパスワードに基づいている場合、マイクロソフトはパスワードの定期更新を義務付けます。 ・認証メカニズムがパスワードに基づいている場合、マイクロソフトは 8 文字以上のパスワードの設定を義務付けます。 ・マイクロソフトは、無効になったまたは有効期限の切れた ID を他の個人が使用できないようにします。 ・マイクロソフトは、無効なパスワードを使用して情報システムに繰り返しアクセスしようとする行為を監視するか、または顧客が監視できるようにします。 ・マイクロソフトは、破られた、または不注意で開示されたパスワードを無効にするために、業界標準の手順を保持します。 ・マイクロソフトは、割り当て時、頒布時、および保管中にパスワードの機密性と完全性を維持するために設計された、業界標準のパスワード保護規定を使用します。 文献[20]にて、利用できる各ユーザーアカウントに応じたパスワードポリシーが明示されている。 文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。	公開文書	文献[08] 文献[20] 文献[33]	—	—	—	利用者は、ガイドラインが求めるパスワード管理方法を実装する必要がある。また、システムを利用する従業員、患者等に適切なパスワードの使用・管理を求める必要がある。 利用者は、Microsoft Online Service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					C. 最低限のガイドライン	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。	—	対象外	無線LANの利用がないため、本項目は対象外とする。	—	—	—	—	—	—	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。
6.5-13					C. 最低限のガイドライン	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と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。	—	対象外	IoT機器の利用ががないため、本項目は対象外とする。	—	—	—	—	—	—	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。
6.5-14					D. 推奨されるガイドライン	1. 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。	情報の秘密度に応じたラベル付けやデータ損失防止(DLP)暗号化など適切な電子情報の管理が必要であり、これらコンプライアンスを管理する機能が提供されています。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/?view=o365-worldwide	適合可能	文献[35]の情報保護の管理にて、Office 365 Advanced Complianceを利用することで、データ損失防止 (DLP)機能により情報へのアクセス管理が行えることが明示されている。	公開文書	文献[35]	—	—	—	利用者は、情報資産の区分管理を適切に実施する必要がある。
6.5-15					D. 推奨されるガイドライン	2. 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）。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御の対策「マイクロソフトは、マイクロソフトが管理する施設を離れる場合、または他に管理者がいない状態でコンピューターの側を離れる場合には、管理セッションを無効にするようマイクロソフト担当者に指示します。」を明記しています。 利用者セッションのタイムアウトはこちらで公開しています。 https://docs.microsoft.com/ja-jp/office365/enterprise/session-timeouts	適合可能	文献[10]にて、Office 365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[10]	—	—	—	利用者は、離席する場合の処置（クリアスクリーン）を行う必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から裏付した内容	マイクロソフト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	
6.5-16					D. 推奨されるガイドライン	3. 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。	インフラ全体のセキュリティ対策においては以下で情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure ネットワークアーキテクチャをご参照ください。 また、Microsoft Teamsのセキュリティガイドにも対策を公開しています。 https://docs.microsoft.com/ja-jp/microsoftteams/teams-security-guide	適合可能	文献[25]にて、通信のセキュリティ対策として、パブリック ネットワークから送信される悪意のあるソフトウェアを含め、悪意のある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ることが明示されている。 文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル（SRTP）、およびその他の業界標準暗号化技術（256 ビットの Advanced Encryption Standard (AES) 暗号化など）を使用することにより、すべてのTeamsデータがネットワーク上で保護されていることが明示されている。 NDA文献[N03]にて、Azure AD Premium1ライセンスを利用することで、IPアドレス制御等の条件付きアクセスが実施できることが明示されている。	要NDA	文献[18] 文献[25]	―	―	NDA文献[N03]	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					D. 推奨されるガイドライン	4. 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。	認証に利用するAzure Active Directoryではスマートロックアウト機能を提供しています。 https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/howto-password-smart-lockout 既定のスマート ロックアウトでは、10 回試行に失敗した後、アカウントによるサインインの試行が 1 分間ロックされます。後続のサインインの試行が失敗するたびに、アカウントは再度ロックされます。最初は 1 分間、後続の試行ではより長い時間ロックされます。	適合可能	文献[21]にて、すべてのユーザー アカウントは、その作成方法に関わらず、Azure AD DS の既定のパスワード ポリシーによって次のアカウントロックアウトポリシーが適用されることが明示されている。 ・アカウントのロックアウト期間: 30 ・許可される失敗したログオン試行回数: 5 ・失敗したログオン試行回数のカウントがリセットされるまでの時間: 30 分 ・パスワードの有効期間: 90 日間 インタビューにて、以下の事項を確認した。 ・Azure Active Directory (Azure AD) 及び Active Directory Federation Service (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	文献[21]	―	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。 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。	―	利用者は、Microsoft Online Service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					D. 推奨されるガイドライン	5. 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I2 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・端末利用時を合わ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。	Microsoft 365では、デバイスや電話を使った二要素認証の標準的なサポートを行っています。また、場所や人、アプリケーションによって二要素認証の動作を変えることも可能であり、例えば院外でスマートホストを利用する場合のニ要素認証の強制などの条件付きアクセスが可能です。https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/overview	適合可能	文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 加えて、NDA文献[N03]にて、Azure AD Premium 2ライセンスを利用することで、AzureADを通して不審なサインインや資格情報の漏洩などに対する多要素認証の強制やパスワードリセット等が行えることが明示されている。	要NDA	文献[33]	―	―	NDA文献[N03]	利用者及びSI事業者は、必要に応じて2要素等の多要素認証を導入する必要がある。
6.5-19					D. 推奨されるガイドライン	6. 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。	―	対象外	無線LANの利用がないため対象外とする。	―	―	―	―	―	利用者及びSI事業者は、無線LANの管理を適切に行う必要がある。
6.5-20					D. 推奨されるガイドライン	7. 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。	―	対象外	IoT機器の利用がないため対象外とする。	―	―	―	―	―	利用者及びSI事業者は、IoT機器の管理を適切に行う必要がある。
6.6-01		6.6 人的安全対策		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	C. 最低限のガイドライン	(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。	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提供する事が規定されています。また、従業員等に関しては契約によりデータの秘密保持と安全性保持を義務付けています。	適合可能	文献[08]、及び文献[25]にて、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。 NDA文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれていることが確認できた。	要NDA	文献[08] 文献[25]	―	Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	利用者及びSI事業者は、自身の管理下にある従業員等については、適切に管理する必要がある。
6.6-02					C. 最低限のガイドライン	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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策にてセキュリティトレーニングを明記しています。 マイクロソフトはマイクロソフト担当者に、関連するセキュリティ手順およびそれぞれの役割について通知します。また、マイクロソフトは、マイクロソフト担当者に、セキュリティ規則および手順に対する違反により生じ得る結果についても通知します。マイクロソフトは、トレーニングにおいては匿名データのみを使用します。 またデータ保護条件 – 下請け処理者の使用に関する通知および規制において明確化しています	適合可能	文献[25]にて、マイクロソフトは、適用されるデータ保護要件および業界標準に従い、顧客データおよび個人データにアクセスするマイクロソフトの従業員に対し、データ プライバシーおよびセキュリティに関する必須のトレーニングを定期的に実施していることが明示されている。 文献[02]にて、Microsoft SDLのプラクティスの中には、開発者、サービスエンジニア等向けのセキュリティに関するトレーニングが盛り込まれていることが明示されている。 インタビューにて、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が確認できた。 また、一般的な防災・防犯訓練について実施していることが確認できた。	要NDA	文献[02] 文献[25]	―	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。 一般的な防災・防犯訓練について実施している。	―	利用者及びSI事業者は、自身の管理下にある従業員等については、適切に教育を実施する必要がある。
6.6-03					C. 最低限のガイドライン	3. 従業者の退職後の個人情報保護規程を定めること。	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	NDA文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員の退職後の個人情報保護に関する事柄については、就業契約に盛り込まれていることが確認できた。	要NDA	―	―	Microsoft従業員の退職後の個人情報保護に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.6-04					D. 推奨されるガイドライン	1. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策を明記しています。 また、Microsoft 365 E5に含まれるCustomer Lockboxの仕組みを利用すると Microsoft側がデータを参照する際に利用者の事前承認が可能となります。	適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、コンピュータルームには カメラを設置していることが明示されている。 文献[37]にて、データセンターには、“最小特権”の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。 また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。 文献[08]にて、従業員への管理について以下が明示されている。 ・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、顧客データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に制限します。	公開文書	文献[01] 文献[08] 文献[37]	–	–	–	利用者及びSI事業者は、重要区画においては従業者のモニタリングを行う必要がある。
6.6-05					C. 最低限のガイドライン	(2) 事務取扱委託業者の監督及び守秘義務契約 1. 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付けられた守秘契約を締結すること	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。また、従業員等に関しては契約によりデータの秘密保持と安全性保持を義務付けています。	適合可能	NDA文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員の罰則に関する事柄については、就業契約に盛り込まれていることが確認できた。	要NDA	–	–	Microsoft従業員の罰則に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	利用者は、SI事業者との間で包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。
6.6-06					C. 最低限のガイドライン	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。	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。 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。 Microsoft 365 E5に含まれるeDiscovery and Audtを利用するとログの保有期間を1年間に延長することができます。	適合可能	文献[37]にて、データセンターではコンピューター化されたメンテナンスシステムがすべてのスケジュールと作業指示を管理しているとともに、メンテナンス時にはデータセンター管理担当者による作業開始前の承認、及び完了を示すために最終承認が行われることが明示されている。 インタビューにて、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は監視されていることが確認できた。	要NDA	文献[37]	–	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は監視されている。	–	利用者は、SI事業者が行うシステム保守作業について、作業者・作業内容・作業結果を確認する必要がある。
6.6-07					C. 最低限のガイドライン	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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策（物理セキュリティおよび論理セキュリティなど）を明記しています。	適合可能	文献[37]にて、データセンターには、“最小特権”の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。 また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。	公開文書	文献[37]	–	–	–	利用者は、利用者側の施設等における入退室管理を適切に実施する必要がある。
6.6-08					C. 最低限のガイドライン	④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データ保護条件 – 下請け処理者の使用に関する通知および規制において明確化しています。 マイクロソフトは、その下請処理者が本 DPA のマイクロソフトの義務を遵守することに責任を負います。マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。マイクロソフトは、本DPA がマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。マイクロソフトは、これらの契約上の義務が確実に満たされるように下請処理者を監督することに同意します。	適合可能	文献[25]にて、委託に関する事項について以下が明示されている。 ・マイクロソフトは、一部のサービスまたは補助的なサービスを第三者に委託することができます。 ・標準契約条項または GDPR 条件の下で上記の同意が要求される場合、この承認は、マイクロソフトが顧客データおよび個人データの処理を下請業者に委託することに対するお客様の事前の書面による同意を構成します。 ・マイクロソフトは、その下請処理者が本DPAのマイクロソフトの義務を遵守することに責任を負います。 ・マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。 ・マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。 ・マイクロソフトは、本DPAがマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。 ・マイクロソフトは、これらの契約上の義務が確実に満たされるように下請処理者を監督することに同意します。 なお、上記事項については文献[08]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	–	–	–	利用者は、SI事業者に対して再委託先の適切な管理を求め、それを契約条件とする必要がある。
6.6-09					D. 推奨されるガイドライン	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。		適合可能	文献[08]にて、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。 顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Servicesの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 NDA文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれていることが確認できた。	要NDA	文献[08] 文献[25]	–	Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	利用者は、SI事業者との間で包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結する必要がある。
6.7-01		6.7 情報の破棄		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。	C. 最低限のガイドライン	1. 「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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.7-02					C. 最低限のガイドライン	2. 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し、残存し、読み出し可能な情報がないことを確認すること。	物理的なセキュリティ対策を以下のサイトで公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/physical-security データ関連のデバイス Microsoft では、NIST 800-88 コンプライアンスのベスト プラクティスの手順とワイプ ソリューションを採用しています。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。 機器の廃棄 システムの寿命がくると、Microsoft 運用担当者は、データを格納しているハードウェアが信頼できない第三者の手に渡らないよう、厳格なデータ処理およびハードウェア廃棄の手続きを実行します。セキュリティで保護された消去アプローチは、それをサポートしているハード ドライブに使用されます。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。すべての Azure サービスは、承認済みのメディア ストレージと破棄管理サービスを利用します。	適合可能	文献[08]にて、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 Serviceを使用する際に同意する条項に含まれていることを確認した。 文献[37]にて、資産が使用停止されると、データセンターではメディアのサニタイズに関する NIST SP 800-88ガイドラインに従ってメディアをサニタイズし、適切な廃棄方法は資産の種類によって決定されることが明示されている。また、安全な過程管理に従った手順が踏まれ、破壊証明書の発行と適切な保管がなされることが明示されている。	公開文書	文献[08] 文献[37]	—	—	—	利用者は、契約終了時のデータ削除プロセス等について把握する必要がある。 また、契約終了時には SI事業者を通じて読み出し可能な情報が残存していないことを確認する必要がある。
6.7-03					C. 最低限のガイドライン	3. 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。		適合可能	文献[08]にて、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 Serviceを使用する際に同意する条項に含まれていることを確認した。 文献[37]にて、資産が使用停止されると、データセンターではメディアのサニタイズに関する NIST SP 800-88ガイドラインに従ってメディアをサニタイズし、適切な廃棄方法は資産の種類によって決定されることが明示されている。また、安全な過程管理に従った手順が踏まれ、破壊証明書の発行と適切な保管がなされることが明示されている。	公開文書	文献[08] 文献[37]	—	—	—	利用者は、契約終了時のデータ削除プロセス等について把握する必要がある。 また、契約終了時には SI事業者を通じて読み出し可能な情報が残存していないことを確認する必要がある。
6.7-04					C. 最低限のガイドライン	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		適合可能	文献[08]にて、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 Serviceを使用する際に同意する条項に含まれていることを確認した。 文献[37]にて、資産が使用停止されると、データセンターではメディアのサニタイズに関する NIST SP 800-88ガイドラインに従ってメディアをサニタイズし、適切な廃棄方法は資産の種類によって決定されることが明示されている。また、安全な過程管理に従った手順が踏まれ、破壊証明書の発行と適切な保管がなされることが明示されている。	公開文書	文献[08] 文献[37]	—	—	—	利用者は、医療情報システムの運用管理規程を定め、その中で不要になった個人情報を含む媒体の破棄について定める必要がある。
6.8-01		6.8 情報システムの改造と保守		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	C. 最低限のガイドライン	1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データの移転と場所 - 処理者の守秘義務に関する種約事項を明確化しています	適合可能	文献[08]にて、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 Service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。	公開文書	文献[08]	—	—	—	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					C. 最低限のガイドライン	2. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御 (アクセスポリシー、アクセスの許可、最小限の権限など)の対策を明記しています。	適合可能	文献[16]にて、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示されている。 文献[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行 文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。	公開文書	文献[16] 文献[28] 文献[33]	—	—	—	利用者は、SI事業者がメンテナンスを行う際に適切なアカウントを使用するように求める必要がある。 SI事業者は、メンテナンスに際して個人情報にアクセスする必要がある場合は、作業者を特定できるように作業記録を残す必要がある。
6.8-03					C. 最低限のガイドライン	3. 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。	同上 (6.8-02)	適合可能	文献[22]にて、アカウントの不正防止について、Microsoft はアカウントのセキュリティを優先し、他のユーザーがお客様の許可なくサインインできないようにしており、新しい場所やデバイスからのサインインがあった場合、メール メッセージと SMS でアラートを送信してアカウントを保護することが明示されている。 文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。	公開文書	文献[22] 文献[33]	—	—	—	利用者及びSI事業者は、メンテナンスに使用するアカウントを適切に管理する必要がある。
6.8-04					C. 最低限のガイドライン	4. 保守要員の離職や担当替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。	同上 (6.8-02)	適合可能	インタビューにて、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	—	—	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。	—	利用者は、保守要員の変更を速やかに報告するようSI事業者に義務付ける必要がある。 また、報告を受けた際には関連するアカウントの登録・変更・削除を速やかに実施する必要がる。
6.8-05					C. 最低限のガイドライン	5. 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。		適合可能	文献[43]、及びインタビューにて、利用者はMicrosoft 365における計画済みのメンテナンスや、その他重要なアナウンスを含む今後の変更について、管理センター内のメッセージセンターにて状況を追跡できることが確認できた。 文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用可能であることが明示されている。	要NDA	文献[26] 文献[43]	—	利用者はMicrosoft 365における計画済みのメンテナンスや、その他重要なアナウンスを含む今後の変更について、管理センター内のメッセージセンターにて状況を追跡できる	—	利用者は、SI事業者に対してメンテナンス作業の事前申請と完了 報告の提出を求める必要がある。
6.8-06					C. 最低限のガイドライン	6. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データの移転と場所 - 下請処理者の使用に関する通知および規制を明確化しています	適合可能	文献[08]、及び文献[25]にて、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[08] 文献[25]	—	—	—	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					C. 最低限のガイドライン	7. 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。	同上 (6.8-02)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.8-08					C. 最低限のガイドライン	8. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御の対策が明記されています。 利用者含めたアクセス、操作ログの確認が可能です。 https://docs.microsoft.com/ja-jp/azure/active-directory/reports-monitoring/concept-sign-ins https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide	適合可能	文献[16]にて、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示されている。 インタビューにて、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[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	要NDA	文献[16] 文献[28]	–	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。	–	利用者は、Microsoft Online Service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					C. 最低限のガイドライン	9. 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。	同上 (6.8-06)	適合可能	文献[25]にて、委託に関する事項について以下が明示されている。 ・マイクロソフトは、一部のサービスまたは補助的なサービスを第三者に委託することができます。 ・標準契約条項または GDPR 条件の下で上記の同意が要求される場合、この承認は、マイクロソフトが顧客データおよび個人データの処理を下請業者に委託することに対するお客様の事前の書面による同意を構成します。 ・マイクロソフトは、その下請処理者が本DPAのマイクロソフトの義務を遵守することに責任を負います。 ・マイクロソフトは、下請処理者に関する情報をマイクロソフトのウェブサイト上に提供します。 ・マイクロソフトは、下請処理者と契約を締結する際、書面による契約書を交わすことにより、下請処理者がマイクロソフトから委託されたサービスを提供するためにのみ顧客データまたは個人データにアクセスして使用し、それ以外の目的には当該データを使用しないことを保証します。 ・マイクロソフトは、本DPAがマイクロソフトに求めるものと同等以上のデータ保護対策を講じるよう書面に規定し、下請処理者に義務付けます。 ・マイクロソフトは、これらの契約上の義務が確実に満たされるように下請処理者を監督することに同意します。 なお、上記事項については文献[08]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	–	–	–	利用者は、SI事業者に対して再委託先に対しても同等の対応を行うよう求める必要がある。
6.8-10					D. 推奨されるガイドライン	1. 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。	同上 (6.8-08)	適合可能	インタビューにて、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[16]にて、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示されている。 また、インタビューにて、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[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	要NDA	文献[16] 文献[28]	–	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。	–	–
6.8-11					D. 推奨されるガイドライン	2. 保守作業時には医療機関等の関係者立会いの下で行うこと。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアクセス制御の対策が明記されています。	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、インタビューにて、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	–	–	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。	–	–
6.8-12					D. 推奨されるガイドライン	3. 作業員各人と保守会社との守秘義務契約を求めること。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データの移転と場所 – 処理者の守秘義務に関する雛形事項および下請処理者の使用に関する通知および規制を明確化しています	適合可能	NDA文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれていることが確認できた。	要NDA	–	–	Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	–
6.8-13					D. 推奨されるガイドライン	4. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアセット管理の対策が明記されています。	適合可能	文献[08]にて、マイクロソフトは、マイクロソフの施設外へ持ち出されるメディア内の顧客データへのアクセスを（暗号化を通じてなど）制限していることが明示されている。 また、運用管理において、マイクロソフトは、顧客データを含む情報システムへのアクセスおよび使用をログに記録し、またはお客様がログに記録できるようにし、アクセス ID、時刻、許可または拒否された認証、および関連する活動を登録していることが明示されている。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 文献[16]にて、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示されている。 また、インタビューにて、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[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	要NDA	文献[08] 文献[16] 文献[25] 文献[28]	–	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。	–	–
6.8-14					D. 推奨されるガイドライン	5. 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。	利用者含めたアクセス、操作ログの確認が可能です。 https://docs.microsoft.com/ja-jp/azure/active-directory/reports-monitoring/concept-sign-ins https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide	適合可能	文献[16]にて、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示されている。 文献[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	公開文書	文献[16] 文献[28]	–	–	–	–
6.9-01		6.9 情報及び情報機器の持ち出しについて		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。	C. 最低限のガイドライン	1. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.9-02				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搬媒体が考えられる。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特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。 従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。	C. 最低限のガイドライン	2. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-03					C. 最低限のガイドライン	3. 情報を格納した可搬媒体若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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-04					C. 最低限のガイドライン	4. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-05					C. 最低限のガイドライン	5. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-06					C. 最低限のガイドライン	6. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-07					C. 最低限のガイドライン	7. 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り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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-08					C. 最低限のガイドライン	8. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-09					C. 最低限のガイドライン	9. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-10					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-11					D. 推奨されるガイドライン	1. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-12					D. 推奨されるガイドライン	2. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-13					D. 推奨されるガイドライン	3. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.9-14					D. 推奨されるガイドライン	4. 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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、情報および情報機器の持ち出しに関する対応を適切に実施する必要がある。
6.10-01		6.10 災害、サイバー攻撃等の非常時の対応		災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（BCP：Business Continuity Plan）と呼ぶ。 我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため適切なBCPの作成と訓練は可能であり、必須の事項と考えられる。 医療機関全体のBCP は本ガイドラインの範疇を超えるため、ここでは「6.2.3 リスク分析」の「7.医療情報システム」に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 や留意事項について述べる。ただし、医療機関全体のBCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならなければならないことは言うまでもない。 「通常の状態で使用できない」とは、システム自体が異常動作又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。	C. 最低限のガイドライン	1. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における通信および運用管理や事業継続性の対策 「– 当社は、顧客データを処理する当社情報システムが設置されている施設について緊急時対応計画を保持しています。 ・マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データを再構築することを試みるように設計されています。」を明記しています。 また可用性については情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure-availability	適合可能	文献[12]にて、Microsoft のデータ センター内のハードウェアやソフトウェアの障害、お客様とMicrosoft間のネットワーク接続の障害、あるいは火災、洪水、その他の地域災害によるデータ センターの重大な被害などのインシデントが発生した場合、Microsoftからお客様へメンテナンス通知を行うことが明示されている。 文献[08]、及び文献[25]にて、マイクロソフトは、顧客データを処理するマイクロソフト情報システムが設置されている施設について緊急時対応計画を保持していることが明示されている。 文献[37]にて、データセンターは中断が発生した場合に重要なデータセンタープロセスの継続的運用および再開をテストする必要があるとした上で、重要な各サービスには文書化されたビジネス継続性計画を設けられており、定義された回復時間および目標回復時刻内にシステムを回復するための役割、責任、詳細な手順が決められていることが明示されている。また、テスト中に特定された問題は解決され、継続的改善のために目標が設定され、それに応じてビジネス継続性計画が更新されることが明示されている。	公開文書	文献[08] 文献[12] 文献[25] 文献[37]	–	–	–	利用者は、災害時における医療サービスのBCPを定める必要がある。その一環として、“非常時”判断の基準、非常時システムへの切り替え手順、正常復帰時の手順、それらの実行を判断する責任者を定める必要がある。
6.10-02					C. 最低限のガイドライン	2. 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。	同上(6.10-01)に加えてデータ保護についても公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/protection-customer-data	適合可能	文献[39]にて、データ損失から回復するための対応（データの整合性確認を含む）について明示されている。 また、文献[09]にて、Microsoft Teamsにおけるサービスレベル（SLA）が明示されている。	公開文書	文献[09] 文献[39]	–	–	–	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
6.10-03					C. 最低限のガイドライン	3. 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て、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。 ・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。	同上(6.10-01)に加えてインシデント管理についても公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure-monitoring	適合可能	インタビューにて、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[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン：マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ：ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン：ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	要NDA	文献[28]	—	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。	—	利用者及びSI事業者は、非常時システムが正常時に悪用されないように適切な管理を行う必要がある。
6.10-04					C. 最低限のガイドライン	4. 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）	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策の明記およびさまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure	適合可能	文献[08]にて、インシデント対応プロセスについて以下が明示されている。 ・マイクロソフトは、違反の内容、期間、違反の影響、報告者の名前、違反の報告先、データの回復手順を含む、セキュリティ違反の記録を保持します。 ・セキュリティ インシデントとなる各セキュリティ違反について、マイクロソフトは、上記の「セキュリティ インシデントの通知」の規定に従い、不当な遅滞なく、かつ、いかなる場合も 30 暦日以内に通知を行います。 ・マイクロソフトは、開示されたデータ、データの開示先および開示時刻を含む、顧客データの開示を追跡するか、またはお客様が追跡できるようにします。	公開文書	文献[08]	—	—	—	利用者は、サイバー攻撃による被害が生じた場合には所管官庁に連絡を行う必要がある。
6.11-01		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		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。	C. 最低限のガイドライン	1. 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。 無線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。	同上 (6.10-04)	適合可能	文献[15]にて、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。また、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示されている。 文献[18]にて、盗聴対策として以下が明示されている。 ・Teams では、Microsoft 365 (Office 365 含む)内でのサーバー通信に相互 TLS (MTLS) を使用し、また、クライエントからサービスへの通信に TLS を使用しているため、特定の会話が攻撃される可能性のある時間内にこの攻撃が目的を達成することは非常に困難です。 ・TURN プロトコルは、リアルタイム メディア通信に使用されます。TURN プロトコルでは、トラフィックの暗号化は必須ではなく、送信する情報は、メッセージの整合性によって保護されます。 盗聴にさらされているにもかかわらず、パケットのソースと宛先のアドレスを見るだけで、送信する情報 (つまり、IP アドレスとポート) を直接抽出できます。Teams サービスは、クリア テキストで送信されることのない TURN パスワードをはじめとするいくつかのアイテムから得られるキーを使用して、メッセージのメッセージ整合性を確認することにより、データが有効であることを確保します。メディア トラフィックには SRTP を使用し暗号化されています。	公開文書	文献[15] 文献[18]	—	—	—	利用者及びSI事業者は、通信経路におけるセキュリティ対策についてMicrosoft Online Serviceに含まれるセキュリティ機能を把握し、それに含まれない範囲については自ら対策を講じる必要がある。
6.11-02					C. 最低限のガイドライン	2. 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。	同上 (6.10-04)	適合可能	文献[07]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[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 NDA文献[N03]にて、Azure AD Premium1ライセンスを利用することで、条件付きアクセス（IPアドレス制御）が実施できることが確認できた。 文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル (SRTP)、およびその他の業界標準暗号化技術 (256 ビットの Advanced Encryption Standard (AES) 暗号化など) を使用することにより、すべてのTeamsデータがネットワーク上で保護されることが明示されている。	要NDA	文献[07] 文献[18] 文献[33]	—	—	NDA文献[N03]	利用者及びSI事業者は、使用するシステムの重要度に応じて適切な認証方式を採用し実装する必要がある。 Microsoft Online Serviceでは標準で提供されている認証方式から適切な認証方式を選択し使用することができる。それで不足する場合は追加の認証技術の採用を検討する必要がある。
6.11-03					C. 最低限のガイドライン	3. 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。	オンラインサービスデータ保護追加契約(DPA) 付属文書A – セキュリティ対策にて物理セキュリティおよび論理セキュリティやアクセス制御などが明記されています。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products	適合可能	文献[01]にて、Microsoft Online Serviceは地理的に分散されたマイクロソフトの施設で運用され、各施設は24時間365 日体制で運用できるように設計されており、物理的な侵入対策を講じていることが明示されている。 文献[37]にて、データセンターには、“最小特権”の入館制御モデルが適用されており、すべての施設は防犯式の内部および外部施設ドア、適切に配置された単身入館ゲート、隔離された荷受けドック、2 要素認証式の生体認証スキャナ、カードキーリーダーを備え、機密性の高いエリアへの入場を制限していることが明示されている。また、物理的な入館制御には、身分証明書の検証、訪問者や第三者に対する入館制限と適切な監督が含まれることが明示されている。 さらに、警報システムやビデオ監視と録画などのセキュリティシステムが導入されていることが明示されている。 文献[07]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] 文献[07] 文献[37]	—	—	—	—
6.11-04					C. 最低限のガイドライン	4. 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若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。	さまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure ネットワークアーキテクチャ、監視において「Azure では、構成設定、およびハードウェア、ソフトウェアおよびネットワーク デバイスのベースライン構成が年 1 回審査および更新されます。変更がテスト環境から運用環境に導入される前に、開発、検証、および承認されていること。 Azure ベースのサービスに必要なベースライン構成は、サービス チームと Azure のセキュリティおよびコンプライアンス チームによって審査されます。サービス チームの審査は、運用サービスを展開する前の検証作業の一環として行われます。」	適合可能	インタビューにて、ネットワーク機器の調達にあたっては、セキュリティ要求に対する充足を含めた、信頼性の高い機器が調達されることが確認できた。	要NDA	—	—	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。	—	利用者は、VPN装置を含む利用者側のネットワーク機器について、安全性が確認出来る機器を利用する必要がある。
6.11-05					C. 最低限のガイドライン	5. 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。例えば、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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における通信および運用管理の対策において 「境界を越えるデータ -マイクロソフトは、パブリック ネットワークを介して伝送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。 -当社は、当社の施設外へ持ち出されるメディア内の顧客データへのアクセスを制限します。」 を明記しています。 また利用者は、メール/ファイルの内容をIRM または AIP / RMS を通じて暗号化を行うことができます。 https://azure.microsoft.com/ja-jp/services/information-protection/	適合可能	文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル (SRTP)、およびその他の業界標準暗号化技術 (256 ビットの Advanced Encryption Standard (AES) 暗号化など) を使用することにより、すべてのTeamsデータがネットワーク上で保護されてい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[18]	—	インターネットを経由したVPNで接続する場合は、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。	—	—

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.11-06					C. 最低限のガイドライン	6. 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の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又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又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）	準拠法は日本となります。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における情報セキュリティインシデントおよび事業継続性の管理の対策を明記しています。 また、SLAにおいてもMicrosoft Online Services サービス レベル契約 (SLA)を規定しています。	適合可能	文献[08]にて、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ていることが明示されている。 文献[08]および文献[09]にて、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。 文献[25]にて、情報に関する責任の範囲について以下が明示されている。 ・お客様とマイクロソフトは、お客様が個人データの管理者であり、マイクロソフトが当該データの処理者であることに合意するものとします。 ・オンライン サービスの技術的および組織的な対策がお客様の要件 (適用されるデータ保護要件に基づくお客様のセキュリティ義務を含む) を満たしているかどうかに関し、お客様は、自身の責任において独自に判断する必要があります。	公開文書	文献[08] 文献[09] 文献[25]	–	–	–	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 Serviceの契約書および使用条件を確認し、Microsoft Online Service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					C. 最低限のガイドライン	7. 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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策への明記およびさまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure ネットワークアーキテクチャ、監視において「Azure では、構成設定、およびハードウェア、ソフトウェアおよびネットワーク デバイスのベースライン構成が年 1 回審査および更新されます。変更がテスト環境から運用環境に導入される前に、開発、検証、および承認されていること。 Azure ベースのサービスに必要なベースライン構成は、サービス チームと Azure のセキュリティおよびコンプライアンス チームによって審査されます。サービス チームの審査は、運用サービスを展開する前の検証作業の一環として行われます。」	適合可能	文献[08]にて、アクセス制御のポリシーを定めていることが明示されている。 また、情報システムへのアクセス制限のルールについて以下が明示されている。 ・マイクロソフトは、データおよびリソースへの承認済みアクセスを許可、変更、または取り消すことができる担当者を指名します。 ・顧客データを含むシステムに複数の個人がアクセスすることができる場合には、マイクロソフトは、それらの個人に個別の ID/ログインを割り当てます。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用できることが明示されている 文献[05]にて、Azure Active Directory (Azure AD) を使用して、Microsoft Teams を管理するために必要な、異なるレベルのアクセス権限を持つ管理者を指定可能であることが明示されている。 なお、Teamsの管理者ロールには4種類あり、Teamsサービス管理者、Teams通信管理者、Teams通信サポート スペシャリスト、およびTeams通信サポートエンジニアが含まれ、それぞれのロールに許可されている操作内容が明示されている。 文献[17]にて、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明示されている。	公開文書	文献[05] 文献[08] 文献[17] 文献[25] 文献[26]	–	–	–	利用者及びSI事業者は、リモートメンテナンスをする際のアクセス権限管理を講じる必要がある。
6.11-08					C. 最低限のガイドライン	8. 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、骨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。	同上 (6.11-06)	適合可能	文献[08]にて、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ていることが明示されている。 文献[08]および文献[09]にて、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。 文献[25]にて、情報に関する責任の範囲について以下が明示されている。 ・お客様とマイクロソフトは、お客様が個人データの管理者であり、マイクロソフトが当該データの処理者であることに合意するものとします。 ・オンライン サービスの技術的および組織的な対策がお客様の要件 (適用されるデータ保護要件に基づくお客様のセキュリティ義務を含む) を満たしているかどうかに関し、お客様は、自身の責任において独自に判断する必要があります。	公開文書	文献[08] 文献[09] 文献[25]	–	–	–	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、利用の可否を決定する必要がある。
6.11-09					C. 最低限のガイドライン	9. 患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI 個人認証等の技術を用いた対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	同上 (6.11-05)	適合可能	文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル（SRTP）、およびその他の業界標準暗号化技術 (256 ビットの Advanced Encryption Standard (AES) 暗号化など) を使用することにより、すべてのTeamsデータがネットワーク上で保護されていることが明示されている。 文献[28]にて、利用者のアクティビティとして以下のレポートが取得可能であることが明示されている。 ・サインイン: マネージド アプリケーションの使用状況とユーザー サインイン アクティビティに関する情報 ・監査ログ: ユーザーとグループの管理や、マネージド アプリケーションとディレクトリのアクティビティに関するシステムアクティビティ情報 ・リスクの高いサインイン : ユーザーアカウントの正当な所有者ではないユーザーによるサインイン試行	公開文書	文献[18] 文献[28]	–	–	–	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					C. 最低限のガイドライン	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。	同上 (6.11-05)およびAzure ExpressRoute などのプライベート接続サービスを利用することが可能です https://azure.microsoft.com/ja-jp/services/expressroute/ またMicrosoft Teamsのセキュリティガイドでもネットワーク通信の暗号化について公開しています。 https://docs.microsoft.com/ja-jp/microsoftteams/teams-security-guide Teams におけるネットワーク通信は、既定で暗号化されています。すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュア リアルタイム転送プロトコル (SRTP)、およびその他の業界標準暗号化技術 (256 ビットの Advanced Encryption Standard (AES) 暗号化など) を使用することにより、すべての Teams データがネットワーク上で保護されます。	適合可能	文献[11]にて、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が確認できた。 文献[18]にて、O365 トラフィックは TLS/HTTPS 暗号化チャネル経由で行われ、すべてのトラフィックの暗号化に証明書が使用されることが明示されている。	要NDA	文献[11] 文献[18]	–	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。	–	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					D. 推奨されるガイドライン	1. 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。	Windows Virtual Desktopなどの仮想デスクトップ環境の利用も可能です https://azure.microsoft.com/ja-jp/services/virtual-desktop/ https://docs.microsoft.com/ja-jp/azure/virtual-desktop/teams-on-wvd	適合可能	文献[11]にて、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。 文献[08]にて、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すると明示されている。 文献[18]にて、O365 トラフィックは TLS/HTTPS 暗号化チャネル経由で行われ、すべてのトラフィックの暗号化に証明書が使用されることが明示されている。	要NDA	文献[08] 文献[11] 文献[18]	–	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。	–	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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 法令で定められた記名・押印を電子署名で行うことについて	「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）	電子署名とは、電磁的記録に記録された情報について、保存すべき期間中における当該情報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）故意又は過失による虚偽入力、書換え、消去及び混同を防止すること。 （イ）作成の責任の所在を明確にすること。 （施行通知第2 2(3)②） 「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1 (1)）	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、法令で署名又は記名・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ケ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。	C. 最低限のガイドライン	法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。 （1）厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-02					C. 最低限のガイドライン	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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-03					C. 最低限のガイドライン	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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-04					C. 最低限のガイドライン	（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ー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ー」（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、一般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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-05					C. 最低限のガイドライン	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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-06					C. 最低限のガイドライン	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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
6.12-07					C. 最低限のガイドライン	（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、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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療データに対する電子署名について適切に対応する必要がある。
7.1-01	7 電子保存の要求事項について	7.1 真正性の確保について	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）故意又は過失による虚偽入力、書換え、消去及び混同を防止すること。 （イ）作成の責任の所在を明確にすること。 （施行通知第2 2(3)②） 「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」 （外部保存改正通知第2 1 (1)）	真正性とは、正当な権限において作成された記録に対し、虚偽入力、書き換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。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誤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、委託先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。	C. 最低限のガイドライン	【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。	標準で多要素認証などをサポートしています。 https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-mfa-howitworks Azure Active Directory Premium P1以上で条件付きアクセスを利用することができより細かいアクセス制御（デバイス制御など）を設定することができます。 https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/overview	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	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の仕組みについて、適切に構築する必要がある。
7.1-02					C. 最低限のガイドライン	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。	ユーザー/グループ単位で必要なアクセス権を設定する必要があります。 https://docs.microsoft.com/ja-jp/microsoftteams/assign-roles-permissions 利用者の操作は監査することが可能です。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療情報システム上のユーザの権限管理を適切に実施する必要がある。
7.1-03					C. 最低限のガイドライン	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。	Azure Active Directory PremiumやMicrosoft Intuneによる MDM機能、また これらを併用した条件付きアクセスにより、場所や人、アプリケーションの利用条件によりニ要素認証や、アクセス制限を行う機能を実現することができます。 https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/overview	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	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					C. 最低限のガイドライン	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。	Microsoft 365 コンプライアンスの機能を活用することで、メールやTeamsチャットに保存されたメッセージの長期保管や管理者による監査、運用の操作を記録することが可能となり、また権限に応じたアクセスコントロールが可能です。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/?view=o365-worldwide	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者側で管理責任者、操作者以外による機器の操作を運用上防止するルールは利用者側で実施する必要がある。
7.1-05					C. 最低限のガイドライン	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。	利用者の操作は監査することが可能です。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide Microsoft 365 E5に含まれるeDiscovery and Audit を利用するとログの保有期間を1年間に延長することができます。 E5がない場合、90日以上前はPowerShell で取り出し必要があります	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者及びSI事業者は、医療情報システムによる電磁的記録が、いつ・誰が行ったかを明確にする仕組みを構築する必要がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から裏付した内容	マイクロソフト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	
7.1-06					C. 最低限のガイドライン	(2) 記録の確定手順の確立と、作成責任者の識別情報の記録 a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合 1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データ保護条件 – データ処理の性質 (権利の帰属)にて「マイクロソフトは、本条でお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。」が明記されています。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	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					C. 最低限のガイドライン	2. 「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者及びSI事業者は、医療情報システムにおける電磁的記録の確定において、作成責任者による確認が可能な機能を構築する必要がある。
7.1-08					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、記録の確定を、適切な権限を持った確定者が実施するよう業務の設計を行う必要がある。
7.1-09					C. 最低限のガイドライン	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。	同上 (7.1-05)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データの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がある。
7.1-10					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用する必要がある。
7.1-11					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、確定者が何らかの理由で確定操作ができない場合、代替策の例やルールを運用管理規程で定め、記録の確定の責任の所在を明確にする必要がある。
7.1-12					C. 最低限のガイドライン	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。	同上 (7.1-05, 06)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	運用管理規程等に当該装置により作成された記録の確定ルールを利用者側で定義する必要がある。
7.1-13					C. 最低限のガイドライン	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。	同上 (7.1-05). また医療機関等に保存する場合、医療情報システムの管理は利用者が適切に行う必要があります。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データの履歴バックアップを作成すること、データのバックアップを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がある。
7.1-14					C. 最低限のガイドライン	(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。	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。 https://docs.microsoft.com/ja-jp/sharepoint/troubleshoot/lists-and-libraries/library-versioning-setting-changes TeamsのドキュメントはSharePoint Onlineの機能を利用	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	データの履歴バックアップを作成すること、その他のフォールト トレランスを提供するための追加の手順を実施する責任は利用者側にある。 更新履歴を保存し、更新前と更新後の内容を照らし合わせる機能を備える必要がある。
7.1-15					C. 最低限のガイドライン	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。		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データの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がある。 また、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					C. 最低限のガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、代行操作に関するルールを運用管理規程で定める必要がある。
7.1-17					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、代行操作に関する機能の整備を行う必要がある。
7.1-18					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、代行操作に関する機能の整備を行う必要がある。
7.1-19					C. 最低限のガイドライン	(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。	さまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure ネットワーク アーキテクチャ、監視および操作において「Azure では、構成設定、およびハードウェア、ソフトウェアおよびネットワーク デバイスのベースライン構成が年 1 回審査および更新されます。変更がテスト環境から運用環境に導入される前に、開発、検証、および承認されていること。 Azure ベースのサービスに必要なベースライン構成は、サービス チームと Azure のセキュリティおよびコンプライアンス チームによって審査されます。サービス チームの審査は、運用サービスを展開する前の検証作業の一環として行われます。」 「Azure 環境にインストールされているソフトウェア スタック内のすべてのコンポーネントは、Microsoft セキュリティ開発ライフサイクル (Security Development Lifecycle: SDL) プロセスに従ってカスタムビルドされています。すべてのソフトウェア コンポーネント (オペレーティング システム (OS) イメージや SQL Database を含む) が、変更管理およびリリース管理プロセスの一部としてデプロイされます。すべてのノード上で実行される OS は、Windows Server 2008 または Windows Server 2012 のカスタマイズされたバージョンです。正確なバージョンは、OS に期待される役割に従ってファブリック コントローラー (FC) によって選択されます。さらに、ホスト OS では、承認されていないソフトウェア コンポーネントのインストールは許可されません。 一部の Azure コンポーネントは、ゲスト OS で実行されているゲスト VM に Azure のお客様としてデプロイされます。」	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、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					C. 最低限のガイドライン	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。	同上 (7.1-19)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システム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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	マイクロソフト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	
7.1-21					C. 最低限のガイドライン	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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策にてセキュリティトレーニングを明記しています。 マイクロソフトはマイクロソフト担当者に、関連するセキュリティ手順およびそれぞれの役割について通知します。また、マイクロソフトは、マイクロソフト担当者に、セキュリティ規則および手順に対する違反により生じ得る結果についても通知します。マイクロソフトは、トレーニングにおいては匿名データのみを使用します。 またデータ保護条件 – 下請け処理者の使用に関する通知および規制において明確化しています	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、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行う必要がある。
7.1-22					C. 最低限のガイドライン	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。	同上 (7.1-19)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、医療情報システム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					C. 最低限のガイドライン	【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C. 最低限のガイドライン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委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。	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。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における通信および運用管理の対策において 「境界を越えるデータ -マイクロソフトは、パブリック ネットワークを介して伝送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。 – 当社は、当社の施設外へ持ち出されるメディア内の顧客データへのアクセスを制限します。」 を明記しています。 上記以外にもAzure ExpressRoute などのプライベート接続サービスを利用することが可能です https://azure.microsoft.com/ja-jp/services/expressroute/ また利用者は、メール/ファイルの内容をIRM または AIP / RMS を通じて暗号化を行うことができます。 https://azure.microsoft.com/ja-jp/services/information-protection/	適合可能	文献[11]にて、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および、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。 文献[18]にて、Teamsのオーディオ、ビデオ、アプリケーション共有に参加している2つのエンドポイント間のメディアトラフィックに対する中間者攻撃は、SRTP を使用してメディアストリームを暗号化することで防ぐことができる。また、暗号化鍵は、独自のシグナリングプロトコル（Teams Call Signalingプロトコル）を介して2つのエンドポイント間でネゴシエートされます。それは、TLS 1.2とAES-256（GCMモード）で暗号化されたUDP / TCP チャネルを利用することが明示されている。	要NDA	文献[11] 文献[18]	–	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および、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。	–	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					C. 最低限のガイドライン	(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。	同上 (7.1-23)	適合可能	文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル（SRTP）、およびその他の業界標準暗号化技術（256 ビットの Advanced Encryption Standard（AES）暗号化など）を使用することにより、すべてのTeamsデータがネットワーク上で保護されていることが明示されている。	公開文書	文献[18]	–	–	–	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。
7.1-25					C. 最低限のガイドライン	(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。	同上 (7.1-01)	適合可能	文献[33]にて、Teamsを含むMicrosoft 365 (Office 365 含む)プランは、ユーザーログインのセキュリティを強化する多要素認証 (MFA) をサポートしており、MFAを使用して、ユーザーは、パスワードを正しく入力した後に、スマートフォンでの電話、テキストメッセージ、またはアプリの通知による認証が行えることが明示されている。 加えて、NDA文献[N03]にて、Azure AD Premium 2ライセンスを利用することで、AzureADを通して不審なサインインや資格情報の漏洩などに対する多要素認証の強制やパスワードリセット等が行えることが確認できた。	要NDA	文献[33]	–	–	NDA文献[N03]	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 見読性の確保について	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2 2(3)①）	見読性とは、電子媒体に保存された内容を、「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、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-文書法の精神にされば、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、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。 ・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。 ・複数媒体に分かれて記録された情報の相互関係が、そのままでは一管して分かりにくい。これらに適切に対応することにより、紙の記録と同等とい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ない最低限の見読性を確保する対策も考慮に含める必要がある。特に、災害等の非常時には、システムが完全に停止してしまうおそれもあるため、定期的なバックアップを実施して、診療録等に記載された患者情報を確認できるようにしておくことが望ましい。 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 委託と第三者提供における責任分界」を参考にしつつ、あらかじめ責任を明確化しておき、速やかな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。	C. 最低限のガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、患者情報の所在を確実に把握できるよう、適切な管理を行う必要がある。
7.2-02					C. 最低限のガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、電子媒体に関する見読化手段の管理を行う必要がある。
7.2-03					C. 最低限のガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、検索表示に関するアプリケーションの機能を確保する必要がある。
7.2-04					C. 最低限のガイドライン	(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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における事業継続性の対策 「– 当社は、顧客データを処理する当社情報システムが設置されている施設について緊急時対応計画を保持しています。 -マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データを再構築することを試みるように設計されています。」を明記しています。 また可用性についても情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure-availability	適合可能	文献[08]にて、ビジネス継続性管理として以下が明示されている。 ・マイクロソフトは、顧客データを処理するマイクロソフト情報システムが設置されている施設について緊急時対応計画を保持しています。 ・マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データを再構築することを試みるように設計されています。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	–	–	–	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					D. 推奨されるガイドライン	【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C. 最低限のガイドラインの診療録等を見読することができること。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、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がある。
7.2-06					D. 推奨されるガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、データの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がある。
7.2-07					D. 推奨されるガイドライン	(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C. 最低限のガイドラインの診療録等を見読することができること。	同上 (7.2-04)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	利用者は、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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	マイクロソフト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	
7.2-08					D. 推奨されるガイドライン	【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D. 推奨されるガイドライン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。	同上（7.2-04）	適合可能	文献[08]にて、ビジネス継続性管理として以下が明示されている。 ・マイクロソフトは、顧客データを処理するマイクロソフト情報システムが設置されている施設について緊急時対応計画を保持しています。 ・マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データを再構築することを試みるように設計されています。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	—	—	—	利用者は、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がある。
7.2-09					D. 推奨されるガイドライン	（2）緊急に必要になると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。	同上（7.2-04）	適合可能	文献[08]にて、ビジネス継続性管理として以下が明示されている。 ・マイクロソフトは、顧客データを処理するマイクロソフト情報システムが設置されている施設について緊急時対応計画を保持しています。 ・マイクロソフトの冗長ストレージおよびそのデータ回復手順は、損失または破壊される前の元の状態または最後に複製されたときの状態で顧客データを再構築することを試みるように設計されています。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	—	—	—	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 保存性の確保について	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2 2(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2 1(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又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。	C. 最低限のガイドライン	【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。	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。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策への明記およびさまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure Microsoft 365 E5 セキュリティ機能により利用者からサイバー攻撃を保護します https://www.microsoft.com/ja-jp/microsoft-365/business/threat-protection	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、医療機関など利用者側の機器等について、セキュリティ対策を適切に行う必要がある。
7.3-02					C. 最低限のガイドライン	（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。	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。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策においてアセット管理 「アセット一覧。マイクロソフトは、顧客データが保管されているすべてのメディアの一覧を保持します。かかるメディアの一覧へのアクセスは、かかるアクセスを書面で許可されている当社担当者に制限されます。」 アセットの取り扱い -マイクロソフトは顧客データを分類して、識別しやすくするとともに、かかるデータへのアクセスを適切に制限できるようにします。 -マイクロソフトは、顧客データの印刷に制限を課し、顧客データを含む印刷物の廃棄手順を定めています。 -マイクロソフトの担当者は、顧客データを携帯用デバイスに格納し、顧客データにリモート アクセスし、または顧客データをマイクロソフトの施設以外で処理するために、マイクロソフトの許可を得る必要があります。」と明記しています。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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					C. 最低限のガイドライン	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容量（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。	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。 データ保護については以下のサイトで情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/protection-customer-data	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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					C. 最低限のガイドライン	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。	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。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策におけるアセット管理および物理セキュリティおよび論理セキュリティ を明記しています。 また物理セキュリティについては以下のサイトで情報を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/physical-security	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、医療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					C. 最低限のガイドライン	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。	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。 利用者の操作は監査することが可能です。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide Microsoft 365 E5に含まれるeDiscovery and Auditを利用するとログの保有期間を1年間に延長することができます。 E5がない場合、90日以上前はPowerShell で取り出す必要があります	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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					C. 最低限のガイドライン	5. 各保存場所における情報が き損した時に、バックアップされたデータを用いて き損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	同上（7.3-03）	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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がある。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
7.3-07					C. 最低限のガイドライン	(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。	同上 (7.3-03)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、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がある。
7.3-08					C. 最低限のガイドライン	(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、データ形式の選択・設定を行う必要がある。
7.3-09					C. 最低限のガイドライン	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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
7.3-10					C. 最低限のガイドライン	【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C. 最低限のガイドライン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。	同上 (7.1-23)	適合可能	文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、およびOAuth、TLS、セキュアリアルタイム転送プロトコル（SRTP）、およびその他の業界標準暗号化技術（256 ビットの Advanced Encryption Standard（AES）暗号化など）を使用することにより、すべてのTeamsデータがネットワーク上で保護されていることが明示されている。 インタビューにて、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。	要NDA	文献[18]	—	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。	—	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					C. 最低限のガイドライン	(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。	同上 (7.2-04)	適合可能	文献[09]にて、各種サービスレベルを定めており、SLAに基づくサービスのパフォーマンス上の問題、または可用性の問題に対してはサービスクレジットをての対応を行っていることが明示されている。	公開文書	文献[09]	—	—	—	—
7.3-12					D. 推奨されるガイドライン	【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。	同上 (7.3-04)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
7.3-13					D. 推奨されるガイドライン	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。		対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
7.3-14					D. 推奨されるガイドライン	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。	同上 (7.3-05)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、データの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					D. 推奨されるガイドライン	(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。	同上 (7.3-03)	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	利用者は、医療機関など利用者側の施設等で管理する記憶媒体の劣化対策を行う必要がある。
7.3-16					D. 推奨されるガイドライン	【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。	同上 (7.1-23)	適合可能	インタビューにて、ネットワーク機器等の各種内部機器は、Microsoft独自のものを開発、採用しており、互換性についても考慮されていることが確認できた。 文献[08]にて、セキュリティ、法令またはシステム パフォーマンスに関する要因によって迅速な削除が必要となる場合を除き、マイクロソフトはお客様に対し、重要な機能の削除またはサービスの停止について 12 か月前までに通知することが明示されている。 文献[37]にて、データセンター管理担当者の承認のもと、定期的なメンテナンスが行われていることが明示されている。	要NDA	文献[08] 文献[37]	—	ネットワーク機器等の各種内部機器は、Microsoft独自のものを開発、採用しており、互換性についても考慮されている。	—	—
8.1.2-01	8 診療録及び診療諸記録を外部に保存する際の基準	8.1 電子媒体による外部保存をネットワークを通じて行う場合 8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	(安全管理措置) 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は き損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 (個人情報保護法第20条) 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。その一方で金融機関、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. C. 最低限のガイドラインのガイドライン」で定める、「①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. C. 最低限のガイドラインのガイドライン」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。	C. 最低限のガイドライン	① 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (ア) 病院や診療所の内部で診療録等を保存すること。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
8.1.2-02					C. 最低限のガイドライン	(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
8.1.2-03					C. 最低限のガイドライン	(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
8.1.2-04					C. 最低限のガイドライン	(エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取り扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
8.1.2-05					C. 最低限のガイドライン	(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—
8.1.2-06					C. 最低限のガイドライン	(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。	—	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	—	—	—	—	—	—

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	マイクロソフト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	
8.1.2-07					C. 最低限のガイドライン	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。	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―	―	―	―
8.1.2-08					C. 最低限のガイドライン	(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。	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―	―	―	―
8.1.2-09					C. 最低限のガイドライン	(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。	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―	―	―	―
8.1.2-10					C. 最低限のガイドライン	(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。	―	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	―	―	―	―	―	―
8.1.2-11					C. 最低限のガイドライン	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。	準拠法は日本となります。 オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策を明記しています。 また、SLAにおいてもMicrosoft Online Services サービス レベル契約 (SLA)を規定しています。	適合可能	文献[09]にて、各種サービスレベルを定めており、SLAに基づくサービスのパフォーマンス上の問題、または可用性の問題に対してはサービスクレジットをての対応を行っていることが明示されている。 文献[08]および文献[09]にて、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・明示されている。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出力などの基本的な機能は、標準サービスで提供されていることを確認した。また、データ管理の保証（利用者データの保証、など）、統制環境の保証（再委託先管理、機密保護の維持、統制環境の維持）を行うことが明示されている。	公開文書	文献[08] 文献[09]	―	―	―	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。
8.1.2-12					C. 最低限のガイドライン	(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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策における通信および運用管理の対策において 「境界を越えるデータ -マイクロソフトは、パブリック ネットワークを介して伝送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。 -当社は、当社の施設外へ持ち出されるメディア内の顧客データへのアクセスを制限します。」 を明記しています。 また利用者は、メール/ファイルの内容をIRM または AIP / RMS を通じて暗号化を行うことができます。 https://azure.microsoft.com/ja-jp/services/information-protection/	適合可能	6.11の確認事項のとおり。	―	―	―	―	―	―
8.1.2-13					C. 最低限のガイドライン	(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。	マイクロソフトではサービスにおけるセキュリティ対策の契約書への明記やマイクロソフト トラストセンターなどにて幅広く情報を公開しています。 また、ISO 27001など90以上のコンプライアンス認証に対応しており、SOCなど第三者機関による監査も定期的に実施しています。 定期的に情報はアップデートされますので、最新情報はWebサイトをご確認ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products https://www.microsoft.com/ja-jp/trust-center/ https://docs.microsoft.com/ja-jp/microsoftteams/teams-security-guide	適合可能	文献[23]にて、ISO27001等の第三者認証を取得、維持していることと、新しい監査レポートとアーカイブ済みの監査レポートが明示されていることから、有効なリスク管理態勢を有していると考えられる。	公開文書	文献[23]	―	―	―	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。
8.1.2-14					C. 最低限のガイドライン	(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。	オンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products データ保護条件 – データ処理の性質（権利の帰属）にて「マイクロソフトは、本条でお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。」が明記されています。 また、Microsoft 365 E5に含まれるCustomer Lockboxの仕組みを利用すると Microsoft側がデータを参照する際に利用者の事前承認が可能となります。	適合可能	文献[08]にて、顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Servicesの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 インタビューにて、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[08] 文献[25]	―	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。	―	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等について、保守作業に必要な範囲を超えた閲覧の禁止に関して確認する必要がある。
8.1.2-15					C. 最低限のガイドライン	(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。	同上 (8.1.2-14)	適合可能	文献[08]にて、顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Servicesの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 インタビューにて、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[08] 文献[25]	―	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。	―	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。
8.1.2-16					C. 最低限のガイドライン	(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。		適合可能	文献[08]にて、顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Servicesの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 なお、上記事項については文献[25]でも同様の事柄が明示されている。 インタビューにて、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[08] 文献[25]	―	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。	―	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。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	第三者認証等から確認した内容	マイクロソフト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	
8.1.2-17					C. 最低限のガイドライン	(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	同上 (8.1.2-13)	適合可能	文献[19]、及び文献[32]にて、Microsoft Teamsではプライバシー、コンプライアンス、セキュリティに対する様々な対策がなされ、ISO27001等の各種認証を取得済みであることが明示されている。	公開文書	文献[19] 文献[32]	–	–	–	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。
8.1.2-18					D. 推奨されるガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–	–
8.1.2-19					D. 推奨されるガイドライン	(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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1.2-20					D. 推奨されるガイドライン	(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。	同上 (8.1.2-14)およびオンライン サービス データ保護追加契約 (DPA)をご参照ください。 https://www.microsoft.com/ja-jp/licensing/product-licensing/products 付属文書 A – セキュリティ対策への明記およびさまざまなセキュリティ対策内容を公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/infrastructure	適合可能	文献[08]にて、施設への物理アクセスとして、マイクロソフトは顧客データを処理する情報システムが配置されている施設へのアクセスを、許可された特定の個人に制限していることが明示されている。コンポーネントへの物理アクセスとして、マイクロソフトはメディアの種類、許可された送付者/受領者、日付および時刻、メディアの数ならびに含まれる顧客データの種類を含め、顧客データを収録したメディアの出入りを記録していることが明示されている。 また、同文献では顧客データの取り扱いについては以下が明示されている。 ・Microsoft Online Serviceの提供に適合する目的を含め、Microsoft Online Serviceをお客様に提供する目的にのみ使用されます。 ・マイクロソフトが、広告または同様の商用目的で顧客データを使用し、また当該データから情報を取得することはありません。 ・両当事者の間において、お客様が顧客データのすべての権利、権限、および権益を留保します。 ・マイクロソフトは、Microsoft Online Serviceをお客様に提供するためにお客様がマイクロソフトに付与する権利を除き、顧客データに関するいかなる権利も取得しません。 なお、上記事項については文献[25]でも同様の事柄が明示されている。	公開文書	文献[08] 文献[25]	–	–	–	利用者は、医療情報システム提供事業者が提供するサービス内容及び約款等を確認する必要がある。
8.1.2-21					D. 推奨されるガイドライン	(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。	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。 利用者の操作は監査することが可能です。 https://docs.microsoft.com/ja-jp/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide Microsoft 365 E5に含まれるeDiscovery and Auditを利用するとログの保有期間を1年間に延長することができます。 E5がない場合、90日以上前はPowerShell で取り出す必要があります	適合可能	文献[03]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[06]では、Office 365で利用可能な主な監査レポートが明示されている。 文献[26]にて、Microsoft側がお客様データにアクセスする際には、カスタマーロックボックス（有償）を用いた承認フローを利用可能であることが明示されている。 文献[18]にて、Teamsにおけるネットワーク通信は、既定で暗号化されており、すべてのサーバーについて証明書の使用を必須にしていること、および OAuth、TLS、セキュアリアルタイム転送プロトコル（SRTP）、およびその他の業界標準暗号化技術（256 ビットの Advanced Encryption Standard（AES）暗号化など）を使用することにより、すべてのTeamsデータがネットワーク上で保護されていることが明示されている。	公開文書	文献[03] 文献[06] 文献[18] 文献[26]	–	–	–	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。
8.1.3-01		8.1 電子媒体による外部保存をネットワークを通じて行う場合 8.1.3 個人情報の保護	（安全管理措置） 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は き損の防止そ の他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。 （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22 条） 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。	C. 最低限のガイドライン	(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。	同上 (8.1.2-13)	適合可能	文献[08]および文献[09]にて、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文献[N01]、NDA文献[N02]、及びインタビューにて、Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれていることが確認できた。 「組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について」は、本ガイドライン6.11項にて記述している。	要NDA	文献[08] 文献[09]	–	Microsoft従業員、委託者に対し、守秘義務契約に関する事柄については、就業契約に盛り込まれている。	NDA文献[N01] NDA文献[N02]	–
8.1.3-02					C. 最低限のガイドライン	(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、病歴、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。	同上 (8.1.2-14) マイクロソフトクラウドの利用は個人データの第三者提供や取扱いの委託に当たらないため、マイクロソフトクラウド利用のために個人情報保護法上の事業者の監督(法22条)のための覚書締結・本人の同意は不要です。	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–	利用者は、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。
8.1.3-03					C. 最低限のガイドライン	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行い、理解を得る必要がある。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–	利用者は、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。
8.1.3-04					C. 最低限のガイドライン	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。	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–	利用者は、乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

Copyright (C) MRI All Rights Reserved.

厚生労働省ガイドラインの評価項目							ガイドラインに対するマイクロソフト社の見解	Microsoft Teams 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	A. 制度上の要求事項	B. 考え方（抜粋）	分類	ガイドライン		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	マイクロソフト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	
8.1.4-01		8.1 電子媒体による外部保存をネットワークを通じて行う場合 8.1.4 責任の明確化	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	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.1.5-01		8.1 電子媒体による外部保存をネットワークを通じて行う場合 8.1.5 留意事項	ネットワークを通じて外部保存を受託する事業者において可搬 媒体に保存する場合にあっては、「付則1 電子媒体による外部保存を可搬媒体を用いて行う場合」に掲げる事項についても十分留意すること。	–	–	–	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.2-01		8.2 電子媒体による外部保存を可搬媒体を用いて行う場合	付則1 へ移動したのでそちらを参照されたい。	–	–	–	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.3-01		8.3 紙媒体のままで外部保存を行う場合	付則2 へ移動したのでそちらを参照されたい。	–	–	–	–	対象外	利用者にて対応いただく事項のため、本項目は対象外とする。	–	–	–	–	–	–
8.4.1-01		8.4 外部保存全般の留意事項について 8.4.1 運用管理規程	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3 1）	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。	–	–	物理的なセキュリティ対策を以下のサイトで公開しています。 https://docs.microsoft.com/ja-jp/azure/security/fundamentals/physical-security データ関連のデバイス Microsoft では、NIST 800-88 コンプライアンスのベスト プラクティスの手順とワイプ ソリューションを採用しています。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。 機器の廃棄 システムの寿命がくると、Microsoft 運用担当者は、データを格納しているハードウェアが侵襲できない第三者の手に渡らないよう、厳格なデータ処理およびハードウェア廃棄の手続きを実行します。セキュリティで保護された消去アプローチは、それをサポートしているハード ドライブに使用されます。ワイプできないハード ドライブの場合、このドライブを破壊して情報の復旧を不可能にする破棄プロセスが使用されます。この破棄のプロセスでは、分解、損壊、粉砕、または焼却処理が可能です。資産の種類に従って破棄の手段が決定されます。破棄の記録が保存されます。すべての Azure サービスは、承認済みのメディア ストレージと破棄管理サービスを利用します。	適合可能	文献[08]にて、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。 文献[37]にて、資産が使用停止されると、データセンターではメディアのサニタイズに関する NIST SP 800-88ガイドラインに従ってメディアをサニタイズし、適切な廃棄方法は資産の種類によって決定されることが明示されている。また、安全な過程管理に従った手順が踏まれ、破壊証明書の発行と適切な保管がなされることが明示されている。	公開文書	文献[08] 文献[37]	–	–	–	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 Service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策略化 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策略化することが可能である。
8.4.2-02		8.4 外部保存全般の留意事項について 8.4.2 外部保存契約終了時の処理について	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。	–	–	同上 (8.4.1-01)	適合可能	文献[08]にて、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。 文献[37]にて、資産が使用停止されると、データセンターではメディアのサニタイズに関する NIST SP 800-88ガイドラインに従ってメディアをサニタイズし、適切な廃棄方法は資産の種類によって決定されることが明示されている。また、安全な過程管理に従った手順が踏まれ、破壊証明書の発行と適切な保管がなされることが明示されている。	公開文書	文献[08] 文献[37]	–	–	–	

Copyright (C) MRI All Rights Reserved.