

金融機関向け『Office365』対応 セキュリティリファレンス（FISC第9版改訂）

2020年 1月 31日
Version 1.1

作成者：

株式会社三菱総合研究所（MRI）
日本ビジネスシステムズ株式会社（JBS）
トレンドマイクロ株式会社（TrendMicro）
株式会社FIXER（FIXER）
日本電気株式会社（NEC）

※「金融機関等コンピュータシステムの安全対策基準」は金融情報システムセンター（FISC）の刊行物です。
FISC安全対策基準の項番の記載についてはFISCからの承諾を得ております。

更新日	版番号	改版内容
2018年7月17日	Version 1.0.0	初版
2019年6月21日	Version 1.0.1	「FISC安全対策基準の項目」欄の記載様式修正(項番を記載)
2020年1月31日	Version 1.1	安全対策基準第9版改訂に伴う追記(シート追加)

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
統1	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における規定は、利用者が整備を行う必要がある。クラウド事業者に関連する規定に関しては、「2 外部の統制」の内容を踏まえ決定を行うことが望ましい。
統2	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における計画は、利用者が策定を行う必要がある。クラウド事業者の新機能提供予定を考慮する場合は、公開資料の参照を行うか、必要に応じてヒアリング等を行うことが考えられる。
統3	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における計画は、利用者が策定を行う必要がある。クラウド事業者の新機能提供予定を考慮する場合は、公開資料の参照を行うか、必要に応じてヒアリング等を行うことが考えられる。
統4	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統5	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における態勢は、利用者が整備する必要がある。クラウド事業者への態勢確認、対応手順の確認は「2 外部の統制」の内容を踏まえて実施することが望ましい。
統6	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統7	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統8	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における体制は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統9	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統10	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統11	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統12	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。
統13	お客様の内部の統制のため対象外	対象外	－	－	－	－	利用者における組織は、利用者が整備する必要がある。クラウド事業者への外部委託を含めた管理は、責任分界点を合意し、「2 外部の統制」の内容を踏まえて実施することが望ましい。

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	SI事業者・利用者が必要な対応
統14	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における教育は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統15	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における教育は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統16	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における教育は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統17	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における訓練は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統18	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における管理は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統19	お客様の内部の統制のため対象外	対象外	—	—	—	—	利用者における管理は、利用者が実施 する必要がある。クラウド事業者への外 部委託を含めた管理は、責任分界点を 合意し、「2 外部の統制」の内容を踏まえ て実施することが望ましい。
統20	マイクロソフトは世界最高レベルの実績と技術、事業継続性に加え、クラウドに関 する高い透明性を持ち、データプライバシーや監査対応など金融機関が必要とする 要件を網羅した契約を用意しています。 詳細は「FISC安全対策基準 第9版 適合説明書（Compliance Companion for FISC guidelines v9）」をご参照ください。	適合可能	文献[14]に、外部委託先を客観的に評価するための項目として、FISC安全 対策基準（第9版）に例示された以下13項目に対するマイクロソフトの回答 が記載されている。 (1)業務に係る実績、技術力 (2)事業継続性（経営方針、経営体力・収益力、人的基盤、被災時のBCM・ データのバックアップ） (3)サービスの可用性・データの安全性（機密性保護）・完全性の確保のた めの態勢、セキュリティ対策の実施状況（機密保護状況を含む） (4)内部統制やリスク管理等に関する状況（再委託先管理も含む）、外部監 査の受検や各種公的認証の取得状況、組織体制（コンプライアンス体制を 含む） (5)情報開示における条件 (6)監査の受入に関する方針、訪問調査の受入スタンス、コミュニケーション ルート (7)既存システムとの連携・新システムへのデータ移行の容易性 (8)保守体制・サポート体制 (9)インシデントが発生した場合の想定損害額（直接損害、間接損害）と外 部委託先側が提示する損害賠償・保証上限額とのバランス (10)契約終了時の対応 (11)個人データの取扱い (12)委託費と支払い条件 (13)係争等に関する国外における裁判に関する事項	文献[14] P3 統20	—	—	利用者は選定手続きを明確にし、客観的 評価をもとに委託可否を決定し、責任者 の承認を得る必要がある。
統21	マイクロソフトのクラウド契約は金融機関のお客様が必要とする要件を盛り込んだ 内容になっています。 詳細は「FISC安全対策基準 第9版 適合説明書（Compliance Companion for FISC guidelines v9）」をご参照ください。	適合可能	文献[14]に、外部委託先との契約時に考慮すべき事項として、FISC安全対策 基準（第9版）に例示された以下16項目に対するマイクロソフト回答が記 載されている。 (1)基本的な事項 (2)個別契約条件、サービス仕様、データ保護の管理策 (3)サービスレベル未達の場合の対応 (4)情報開示範囲、監督当局等による検査等への協力義務、金融機関による 監査受入、事業者と利用者間の報告・連絡等の運営ルール、インシデント レスポンスの取扱い (5)反社会的勢力・テロ組織と関わりがないことの表明・確約 (6)契約の解除条件、契約終了時のデータの返却・消去等及び、契約終了 時の原状回復・新システム移行時における協力義務 (7)損害が発生した場合の協議及び賠償に関する取決め (8)委託業務の成果の知的財産権、使用权等の権利の帰属 (9)外部委託先からの情報開示 (10)複数の外部委託先への委託 (11)再委託管理 (12)監査・モニタリング (13)インシデント発生時の立入調査 (14)記憶装置等の障害・交換 (15)国外におけるデータ保管時の留意点 (16)トレーサビリティの確保	文献[14] P6 統21	—	—	利用者は選契約時に考慮すべき事項を 盛り込み、契約締結手続きを行う必要が ある。

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
統22	マイクロソフトはオンラインサービス条件(OST)の中で、お客様のデータをサービス提供以外の目的では利用しないことを記載しています。マイクロソフトはユーザー認証、権限とアクセスの管理、特権最小化の原則などの対策を通じてこのルールの順守を確実なものとしています。 またお客様は、マイクロソフトがオンラインサービスの提供に当たってお約束する様々なセキュリティ対策をマイクロソフトが適切に実施しているかどうかを、第三者が実施する標準監査レポートによって確認することが可能です。	適合可能	文献[15]に、「顧客データは、Online Service の提供に適合する目的を含め、このサービスをお客様に提供する目的にのみ使用または処理される」旨を明記し、Online Service 固有の条件としてサービスの範囲の定義を記載している。 また、監査コンプライアンスとして「標準またはフレームワークにおいて監査の実施が規定されている場合、かかる制御標準またはフレームワークに関する監査は、少なくとも年 1 回実施される」とする旨が記載されており、Service Trust Portalから監査レポートが実際に入手できることを確認した。 ※要ユーザー登録	文献[15] P9 データ保護条件 P11 監査コンプライアンス P18 Online Service 固有の条件	－	－	利用者は遵守状況を定期的に確認する必要がある。
統23	お客様は委託業務の遂行状況として、オンラインサービスの稼働状況についてのレポートをオンラインサービスの管理ポータルにより確認することが可能です。また、プレミアサポート契約を締結のお客様は、プレミアサポート担当者から稼働状況についての定期的な報告を受けたり、新機能の提供予定に関するロードマップについての情報を受けたりすることも可能です。	適合可能	文献[15]に、セキュリティ対策として、セキュリティに関する確約事項が記載されている。 また、管理ポータルよりオンラインサービスの稼働状況レポートが入手できることを確認した。	文献[15] P15 付録B セキュリティ対策	－	－	利用者は遵守状況を定期的に確認する必要がある。
統24	マイクロソフト オンラインサービスでは、統制対象クラウド拠点として、お客様のデータが保管される場所をウェブサイト上で公開しています。	適合可能	文献[16]に、「お客様はどこにご自身のデータが格納されているかを把握できる」と、データの複製を原則地域内に限ることが明記されている。 また、Service Trust PortalからISO 27017及び27018の認証レポートを入手することが可能であることから、クラウドサービス固有のリスクに対する対策について考慮していると考えられる。	文献[16] データの保管場所	－	－	利用者は自身のセキュリティ対策状況とクラウドサービスの対策状況を踏まえたうえで安全対策を講ずる必要がある。
統25	Azure サービスを利用して共同センターを構築するお客様は、共同センターを構築運営するお客様が、共同センターを利用する金融機関との間でどのように緊急事態対応を行うかなどを対策する必要があります。	適合可能	文献[15]に、情報セキュリティインシデント管理及びビジネス継続性管理について確約事項が明記されている。	文献[15] P15 付録B セキュリティ対策	－	－	利用者は、確約事項及び契約内容を踏まえたうえで、共同センターを利用する金融機関間で適切な安全対策を講ずる必要がある。
統26	金融機関相互のシステム・ネットワークではないため対象外	対象外	－	－	－	－	－
実1	お客様利用者が入力する Office 365 のパスワード入力画面はすべて規定で非表示となっています。弱いパスワードの使用は許可されません。またADFSなどによりお客様のADの認証によりOffice 365へのアクセスを行う構成とすることができま す。 マイクロソフト担当者は本番環境アクセスの際にスマートカード認証を使用しています。	適合可能	文献[21]に、企業ドメインアカウントのパスワードは Active Directory 上のポリシーによって管理されており、パスワードの長さ、複雑さ、有効期限の最小要件が指定される旨、明示されている。 また文献[23]にも、Azure Active Directory B2C上において「パスワードの複雑さのルール」を指定可能である旨が明示されている。	文献[21] P23 IAM-02 Identity & Access Management – Credential Lifecycle / Provision Management 文献[23]	－	－	利用者は、自ら設定したパスワードを第三者に漏洩したり、第三者が類推しやすいパスワードを設定することを防ぐ必要がある。
実2	Office 365は自動着信端末へ金融情報を通知するシステムではありません	対象外	－	－	－	－	IPv4アドレスでアクセス制限を行うためには、AD FS と組み合わせてOffice 365 を使用し、制限するためのルールを適切に設定する必要がある。 また、その他の端末確認(制限)機能を用いる場合には、サードパーティのサービスなどとOffice 365を組み合わせて使用する必要がある。
実3	Office 365上の電子メールデータ、ファイルデータは暗号化して保存しています。	適合可能	文献[22]に、Exchange Online、Skype for Business、SharePoint Online、及びOneDrive for Businessにおいては、ボリュームレベルの暗号化に加え、サービス暗号化を使用して顧客データを暗号化する旨が明示されている。 また文献[21]にも、Office 365においてはBitLockerを使用し、ボリュームレベルで顧客データを暗号化している旨が明示されている。 SOC2レポートにおいて、保存データがポリシーに従って暗号化されていることについて記載されていることを確認した。	文献[22] P8 Encryption in Microsoft Office 365 文献[21] P17 EKM-03 Encryption & Key Management – Sensitive Data Protection	SOC2レポート CA-54	－	エンドユーザーに対するアクセス制御は、利用者側で設定・管理を行う必要がある。 利用者が端末にダウンロードしたファイル等については、端末側の暗号化機能などを用いて対策を講じる必要がある。 端末や周辺機器に格納される一時データなどの管理は利用者の責任である。
実4	Office 365とお客様機器間、およびOffice 365データセンター間でのお客様データにかかわる通信はTLSにより暗号化されます。	適合可能	文献[22]に、Office 365サーバ間の接続はTLSあるいはIPsec、クライアントとの通信はTLSによって暗号化される旨が明示されている。 また文献[21]にも、Office 365においては通信データがTLSによって暗号化される旨が明示されている。 SOC2レポートにおいて、利用者データセンター間の通信、データセンター同士の通信がそれぞれ暗号化されていることについて、記載されていることを確認した。	文献[22] P12 Encryption of Office 365 customer data in transit 文献[21] P16 EKM-03 Encryption & Key Management Sensitive Data Protection	SOC2レポート CA-44	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	SI事業者・利用者で必要な対応
実5	Office 365 SharePoint Onlineではファイル単位にアクセス制御を実施しています。	適合可能	文献[21]に、Office 365においては、SharePointドキュメントや電子メールメッセージなどの顧客が作成したデータは、Office365におけるデータ分類スキームにおいて最もセキュリティ制御が厳格な「顧客データ」として取り扱われる旨が明示されている。 同じく文献[21]に、Office 365 の資産に対するアクセス権については、「知る必要性のある人間に限定する原則」及び「最小特権の原則」に基づき、ビジネス要件や資産所有者の承認のもとに付与される旨、明示されている。	文献[21] P14 DSI-01 Data Security & Information Lifecycle Management Classification 文献[21] P24 IAM-03 Identity & Access Management Diagnostic / Configuration Ports Access	－	－	利用者に対するアクセス権限の設定は、SI事業者や利用者の管理者により適切に行われる必要がある。
実6	Office 365において、メールアドレス、ファイル名など利用者が入力するデータにフォーマットが定めてあるものについて、そのエラーチェックを実施しています。	適合可能	文献[21]に、Microsoft Office 365においては入力データに関して許容可能な基準を定めているほか、処理エラーのリスクを抑えるため、Office 365 環境内に「内部処理制御 (Internal processing controls)」が実装されている旨、及び内部処理制御が「処理環境内だけでなくアプリケーション内にも存在している (exist in applications, as well as in the processing environment.)」旨が明示されている。	文献[21] P6 AIS-03 Application & Interface Security – Data Integrity	－	－	－
実7	Office 365とお客様機器間、およびOffice 365データセンター間でのお客様データにかかわる通信はTLSにより暗号化されます。	適合可能	文献[22]に、Office 365サーバー間の接続はTLSあるいはIPsec、クライアントとの通信はTLSによって暗号化される旨が明示されている。 また文献[21]にも、Office 365においては通信データがTLSによって暗号化される旨が明示されている。 同じく文献[21]に、ネットワーク環境の通信制御、信頼ゾーンとの境界を監視している旨が記載されている。 SOC2レポートにおいて、利用者とデータセンター間の通信、データセンター同士の通信がそれぞれ暗号化されていることについて、記載されていることを確認した。	文献[22] P12 Encryption of Office 365 customer data in transit 文献[21] P16 EKM-03 Encryption & Key Management Sensitive Data Protection P28 IVS-06 Infrastructure & Virtualization Security Network Security IVS-06	SOC2レポート CA-44	－	－
実8	Office 365はAzure ADとの連携によりお客様管理者、利用者の認証を行います。なりすまし対策として、SSO、多要素認証の利用、端末特定などを行うことが可能です。	適合可能	文献[17]に、Office365においては、ID基盤として強力な認証オプションを有するAzure Active Directoryを使用しており、ユーザ携帯電話へのコール、テキストコード送信、アプリへのコード通知、オフィス電話への通話といった多要素認証が使用可能である旨が明示されている。 また文献[24]に、電話の通話、テキストメッセージ、または専用アプリでの通知のほか、サードパーティの多要素認証ソリューションもサポートしている旨が明示されている。	文献[17] P15 安全なエンド ユーザー アクセス 文献[24] Office 365	－	－	特に、インターネットバンキングで用いる電子証明書の管理や認証方式の選択は、利用者の責任である。
実9	お客様はAD FS連携などによりお客様ADによる不正使用防止を行うことが可能です。	適合可能	文献[17]に、ID基盤として、強力な認証オプションを有するAzure Active Directoryを使用する旨が明示されている。 また文献[24]に、電話の通話、テキストメッセージ、または専用アプリでの通知のほか、サードパーティの多要素認証ソリューションもサポートしている旨が明示されている。	文献[17] P15 安全なエンド ユーザー アクセス 文献[24] Office 365	－	－	－
実10	お客様はお客様管理者や利用者のサインインやOffice 365に利用状況について、管理ポータルまたはOffice 365 Management Activity APIによってログを取得し、調査することが可能です。また、取得したログデータについての適切な保護対策を行う必要があります。	適合可能	文献[17]に、マイクロソフトにおいては、データへのアクセス履歴やアクセス状況を顧客に伝えるという原則のもとにオンラインサービスを運用している旨が明示されている。 同じく文献[17]に、Office 365 の監査ポリシーを利用してイベントをログに記録可能である旨が明示されている。 また文献[31]に、管理者が参照可能なユーザアクティビティ関連レポートについて明示されている。	文献[17] P17 プライバシーの設計 文献[17] P21 お客様によるコンプライアンス制御 文献[31] Office 365 管理センターで利用可能なアクティビティ レポート	－	－	利用者は、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。
実11	Office 365は電子取引ソリューションではありません	対象外	－	－	－	－	－
実12	Office 365は電子取引ソリューションではありません	対象外	－	－	－	－	－
実13	お客様データの暗号化に使用した暗号鍵は別の暗号鍵によって保護され、異なる機器に保管されます。詳細は、Microsoft Cloud – Encryptionを参照してください。	適合可能	文献[22]に、「Azure Key Vault」を使用することで、暗号鍵や、Hardware Security Modules (HSMs) 内に格納された鍵を使用するパスワードなどを暗号化することが可能になる旨が明示されている。 SOC2レポートにおいて、保存データがポリシーに従って暗号化されていることについて記載されていることを確認した。	文献[22] P4 Azure Key Vault	SOC2 CA-54	－	端末側で使用する暗号鍵は、第三者に解読されたり漏洩することを防ぐために、利用者が対策を講じる必要がある。

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者に必要な対応
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
実14	Office 365はお客様データとOffice 365システムの保護のため、インターネットからOnline Servicesネットワークを切り離して維持し、統制のために物理的な分離、論理的な分離、ファイアウォールを使用しています。不正侵入やDDoS攻撃を検出する仕組みも取り入れています。 お客様はお客様ネットワーク環境について不正侵入対策を行う必要があります。	適合可能	文献[21]に、システムはネットワーク層においてセグメント化され、役割ベースのアクセス制御によって厳しくアクセス制限されている旨が明示されている。 同じく文献[21]に、マイクロソフトのデータセンターにおいては、自動化された仕組みを通じてデバイス構成の不一致を検出するほか、未使用ポートをデフォルトで無効にすることにより不正アクセスを防止している旨が明示されている。 また文献[32]に、クラウド基盤等への不正侵入を含む攻撃に対抗して設置されるインシデントレスポンスチームについて明示されている。 ISO 27001の管理策「ネットワークの管理策」並びに「ネットワークの分離」で求められている要件を考慮すると、外部ネットワークからの不正アクセス防止策に関しては十分考慮されていると考えられる。	文献[21] P23 IAM-01 Identity & Access Management – Audit Tools Access 文献[21] P12 DCS-03 Datacenter Security Equipment Identificatio 文献[32] P3 Cloud security challenges	ISO 27001:2013 A.13.1.1, A.13.1.3	—	—
実15	Office 365は不正アクセスの防止のためにネットワークを分離し、必要最小限の接続のみを許可する設定を行っています。 お客様はお客様の外部ネットワークからのアクセス経路についての対応が必要です。	適合可能	文献[21]に、システムはネットワーク層においてセグメント化され、役割ベースのアクセス制御によって厳しくアクセス制限されている旨が明示されている。 同じく文献[21]に、マイクロソフトのデータセンターにおいては、自動化された仕組みを通じてデバイス構成の不一致を検出するほか、未使用ポートをデフォルトでオフにすることにより不正アクセスを防止している旨が明示されている。 また文献[32]に、クラウド基盤等への不正侵入を含む攻撃に対抗して設置されるインシデントレスポンスチームについて明示されている。 ISO 27001の管理策「ネットワークの管理策」並びに「ネットワークの分離」で求められている要件を考慮すると、外部ネットワークからの不正アクセス防止策に関しては十分考慮されていると考えられる。	文献[21] P23 IAM-01 Identity & Access Management – Audit Tools Access 文献[21] P12 DCS-03 Datacenter Security Equipment Identificatio 文献[32] P3 Cloud security challenges	ISO 27001:2013 A.13.1.1, A.13.1.3	—	—
実16	Office 365はアクセスを監視し、ログを記録しています。システムに対する不正アクセスや内部アカウントへの攻撃はセキュリティインシデントとしてマイクロソフトが対応します。 お客様管理者や利用者アカウントに対するサインイン失敗はOffice 365管理センターあるいはその他の手段でお客様に提供されます。お客様はこれらのアカウントについてのログを監視する必要があります。	適合可能	文献[21]に、潜在的なセキュリティ上の問題は、Office 365の内部インシデント対応計画に則って調査及びエスカレーションされる旨が明示されている。 SOC2レポートにおいて、セキュリティチームへのセキュリティインシデントの通知プロセス、セキュリティチームでの対応手順の確立、ネットワーク機器のセキュリティイベント監視について記載されていることを確認した。 ISO 27001の管理策「イベントログ取得」で求められている要件を考慮すると、情報セキュリティに関するイベントログの記録と保持に関しては十分考慮されていると考えられる。	文献[21] P33 SEF-02 Security Incident Management, EDiscovery & Cloud Forensics – Incident Management	SOC2レポート CA-26, CA-47, CA-48 ISO 27001:2014 A.12.4.1	—	ログインの失敗などのイベントを利用者側の管理者に通知するためには、AD FSと組み合わせてOffice 365 を使用し、適用する監査ポリシーを適切に設定する必要がある。
実17	Office 365は金融取引のためのサービスではありません	対象外	—		—	—	—
実18	Office 365は金融取引のためのサービスではありません	対象外	—		—	—	—
実19	マイクロソフトはインシデント対応に関するポリシーを作成し、目的や対象範囲、役割、責任、管理者の取り組み、組織間の調整、コンプライアンスを規定して文書化したうえで、関連するすべてのスタッフまたは役割に配布しています。 また、お客様はお客様管理者や利用者のアカウントやお客様関連設備で生じた不正アクセスに対する対策を実施する必要があります。	適合可能	文献[21]に、潜在的なセキュリティ上の問題は、Office 365の内部インシデント対応計画に則って調査及びエスカレーションされる旨が明示されている。 ISO 27001の「情報セキュリティインシデントの管理及びその改善」に関する一連の管理策で求められている要件を考慮すると、情報セキュリティインシデント発生時の対応・復旧・再発防止策に関しては十分考慮されていると考えられる。	文献[21] P33 SEF-02 Security Incident Management, EDiscovery & Cloud Forensics – Incident Management	ISO 27001:2013 A.16.1.1~A.16.1.7	—	—
実20	Office 365はアンチウイルスソフトウェアを使用して、Office 365およびお客様データを悪意あるソフトウェアから保護しています。	適合可能	文献[21]に、Office 365上の資産保護のため、不正プログラム対策ソフトウェアが初期構成の段階で実装されている旨が明示されている。 SOC2レポートにおいて、マルウェアの検出と既知の脆弱性対策、感染システムの隔離等の対策について記載されていることを確認した。 ISO 27001の管理策「マルウェアに対する管理策」で求められている要件を考慮すると、不正プログラムからの保護や検出・復旧のための管理策に関しては十分考慮されていると考えられる。	文献[21] P28 IVS-07 Infrastructure & Virtualization Security OS Hardening and Base Controls	SOC2レポート CA-45 ISO 27001:2013 A.12.2.1	—	—
実21	実20に同じ	適合可能	文献[21]に、Office 365上の資産保護のため、不正プログラム対策ソフトウェアが初期構成の段階で実装されている旨が明示されている。 SOC2レポートにおいて、マルウェアの検出と既知の脆弱性対策、感染システムの隔離等の対策について記載されていることを確認した。 ISO 27001の管理策「マルウェアに対する管理策」で求められている要件を考慮すると、不正プログラムからの保護や検出・復旧のための管理策に関しては十分考慮されていると考えられる。	文献[21] P28 IVS-07 Infrastructure & Virtualization Security OS Hardening and Base Controls	SOC2レポート CA-45 ISO 27001:2013 A.12.2.1	—	—

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	SI事業者・利用者で必要な対応
実22	マイクロソフトはインシデント対応に関するポリシーを作成し、目的や対象範囲、役割、責任、管理者の取り組み、組織間の調整、コンプライアンスを規定して文書化したうえで、関連するすべてのスタッフまたは役割に配布しています。 お客様はお客様側で発生するインシデント対応を計画する必要があります。	適合可能	文献[21]に、Office 365上の資産保護のため、不正プログラム対策ソフトウェアが初期構成の段階で実装されている旨が明示されている。 同じく文献[21]に、潜在的なセキュリティ上の問題は、Office 365の内部インシデント対応計画に則って調査及びエスカレーションされる旨が明示されている。 ISO 27001の「情報セキュリティインシデントの管理及びその改善」に関する一連の管理策で求められている要件を考慮すると、情報セキュリティインシデント発生時の対応・復旧・再発防止策に関しては十分考慮されていると考えられる。	文献[21] P28 IVS-07 Infrastructure & Virtualization Security OS Hardening and Base Controls P33 SEF-02 Security Incident Management, EDiscovery & Cloud Forensics – Incident Management	ISO 27001:2013 A.16.1.1–A.16.1.7	—	—
実23	マイクロソフトは構成管理に関するポリシーを作成し、目的や対象範囲、役割、責任、管理者の取り組み、組織間の調整、コンプライアンスを規定して文書化し、すべてのユーザーに配布しています。 お客様はOffice 365の利用に関するマニュアルの整備を行う必要があります。	適合可能	文献[21]に、操作手順書やサーバーのベースラインやセキュリティ強化に関する手引き、システム構築ドキュメントを含む豊富な(Extensive)ドキュメントが、内部サイト上に保存され、権限のある担当者に提供されている旨が明示されている。 ISO 27001の「運用の手順及び責任」に関する「操作手順書」の管理策で求められている要件を考慮すると、操作手順の文書化に関しては十分考慮されていると考えられる。	文献[21] P7 BCR-04 Business Continuity Management & Operational Resilience Documentation	ISO 27001:2013 A.12.1.1	—	利用者は、操作等のマニュアルを用意する必要がある。
実24	マイクロソフトはインシデント対応に関するポリシーを作成し、目的や対象範囲、役割、責任、管理者の取り組み、組織間の調整、コンプライアンスを規定して文書化したうえで、関連するすべてのスタッフまたは役割に配布しています。 お客様管理者向けにはRSS、サービス正常性ダッシュボード(SHD)、管理アプリなどにより通知します。お客様は利用者向けの通知や自社環境での障害・災害に対する対応を行う必要があります。	適合可能	文献[21]に、「Enterprise Business Continuity Management (EBCM)」フレームワークが確立されている旨が、またEBCMフレームワークに関するガイドランスには、ガバナンス／影響の許容範囲／ビジネスの影響分析／依存関係の分析（非技術面及び技術面）／戦略／計画／テスト／トレーニング及び意識向上といったコンポーネントが含まれる旨が明示されている。 SOC2レポートにおいて、インシデントレスポンスガイドの共有と利用、Service Health Centerを通じた利用者への重要インシデントに関する情報開示について記載されていることを確認した。 ISO 27001の「運用の手順及び責任」に関する「操作手順書」の管理策、「運用の手順及び責任」に関する一連の管理策で求められている要件を考慮すると、操作手順の文書化と障害・災害時の事業継続マネジメントに関しては十分考慮されていると考えられる。	文献[21] P12 BCR-01 Business Continuity Management & Operational Resilience – Business Continuity Planning	SOC2レポート CA-13, CA-15 ISO 27001:2013 A.12.1.1, A.17.1.1–17.1.3	—	利用者は、エンドユーザーへの通知を行う必要がある。
実25	マイクロソフトはアクセス制御ポリシーを作成し、目的や対象範囲、役割、責任、管理者の取り組み、組織間の調整、コンプライアンスを規定して文書化し、配布しています。また、マイクロソフトは、明確に規定したスタッフまたは役割にのみ、システム上の特権を持つアカウントを割り当てます。 お客様はOffice 365上のデータについて所有者およびアクセス権限所有者を適切に管理する必要があります。	適合可能	文献[21]に、Office 365の情報セキュリティポリシーにおいて、資産所有者による資産へのアクセス許可及び制限が「必要性」と「最小特権」の原則に基づくほか、同ポリシーが、アクセスプロビジョニング、認証、アクセス許可、アクセス権の削除、定期的なアクセスレビューといった、アクセス管理ライフサイクルの要件にも取り組んでいる旨が明示されている。 SOC2レポートにおいて、パスワードポリシーの適用による利用者認証について記載されていることを確認した。 ISO 27001の管理策「アクセス制御方針」並びに「特権アクセスの管理」で求められている要件を考慮すると、アクセス権限所有者の特定に関しては十分考慮されていると考えられる。	文献[21] P23 IAM-02 Identity & Access Management Credential Lifecycle / Provision Management	SOC2レポート CA-34 ISO 27001:2013 A.9.1.1, A.9.2.3	—	利用者は、エンドユーザーによる運用上もしくは業務上重要なファイルへのアクセスの記録や監査について、委託の要否を判断する必要がある。
実26	マイクロソフトは、パスワードの最低限の複雑さとパスワード文字数の下限、有効期間の上限を設定して制限を加え、保管時と転送時にパスワードを暗号化して、パスワードの再利用を禁止します。詳細は監査対象統制策 ISO 27001-2013 A.9.3.1 を参照してください。 お客様はお客様管理者や利用者のパスワード管理についての統制を実施する必要があります。	適合可能	文献[21]に、企業ドメインアカウントのパスワードは Active Directory 上のポリシーによって管理されており、パスワードの長さ、複雑さ、有効期限の最小要件が指定される旨が明示されている。 また文献[23]にも、Azure Active Directory B2C上において「パスワードの複雑さのルール」を指定可能である旨が明示されている。 SOC2レポートにおいて、パスワードポリシーの適用による利用者認証について記載されていることを確認した。 ISO 27001の管理策「秘密認証情報の利用」で求められている要件を考慮すると、セキュリティポリシーに則ったパスワードの取り扱い周知に関しては十分考慮されていると考えられる。	文献[21] P23 IAM-02 Identity & Access Management – Credential Lifecycle / Provision Management 文献[23]	SOC2レポート CA-34 ISO 27001:2013 A.9.3.1	—	利用者は、パスワード等の漏えいを防止するため、エンドユーザーに対し注意喚起する必要がある。
実27	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および MCIOTeamに対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。 お客様はお客様管理者や利用者のID管理及びアクセス権管理を実施する必要があります。	適合可能	文献[21]に、Office 365の情報セキュリティポリシーにおいて、資産所有者による資産へのアクセス許可及び制限が「必要性」と「最小特権」の原則に基づくほか、同ポリシーが、アクセスプロビジョニング、認証、アクセス許可、アクセス権の削除、定期的なアクセスレビューといった、アクセス管理ライフサイクルの要件にも取り組んでいる旨が明示されている。 SOC2レポートにおいて、システムアクセス時の事前申請手続きと承認権限者による認可について記載されていることを確認した。 ISO 27001の管理策「利用者アクセスの提供」並びに「利用者アクセス権のレビュー」で求められている要件を考慮すると、アクセス権管理手続きに関しては十分考慮されていると考えられる。	文献[21] P23 IAM-02 Identity & Access Management Credential Lifecycle / Provision Management	SOC2レポート CA-33 ISO 27001:2013 A.9.2.2, A.9.2.5	—	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。
実28	Office 365の利用に際して、マイクロソフト関係者がお客様データの授受・保管を行うことはありません。 お客様はOffice 365上のお客様データについての授受・保管についての統制を実施する必要があります。	対象外	—	—	—	—	利用者は、データファイルの授受、保管方法を定める必要がある。

FISC安全対策基準（第9版）の項目		Office 365 における対応						SI事業者・利用者が必要な対応
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容		
実29	実28と同様	対象外	—	—	—	—	利用者は、データファイルの修正および 管理方法を定める必要がある。	
実30	マイクロソフトは、Office 365 上でお客様データの暗号化に使用する鍵を保護し、 社内規定に従って厳密な管理を行っています。 お客様は、Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルについて、お客様管理の暗号鍵による暗号化を行うことが可 能です。この場合、暗号鍵の管理、生成、保管などについてはお客様の責任範囲 となります。	適合可能	文献[21]に、暗号鍵管理のためのポリシー、手順、及びメカニズムが確立し ている旨が明示されている。 ISO 27001の管理策「鍵管理」で求められている要件を考慮すると、暗号鍵 の利用や保護等に関する規定の作成に関しては十分考慮されていると考 えられる。	文献[21] P16 EKM-01 Encryption & Key Management Entitlement	ISO 27001:2013 A.10.1.2	—	利用者は、利用者側で暗号化を行う場 合は、暗号鍵の取扱手続きなどを適切 に定める必要がある。	
実31	お客様はお客様管理者や利用者のOffice 365利用の習熟についてく教育、訓練 を行う必要があります。 マイクロソフトは Office 365 の運用に際してオペレータによる運用を行っていま せん	適合可能	インタビュー等を通じて、通常時運用は自動化されていることを確認し、円 滑に運用されていると考えられる。	—	—	通常時運用は自動化されて いる	—	
実32	マイクロソフトは、マルウェアの検出、阻止、復旧を行う統制を実施します。 アンチウイルス ソフトウェアの使用は、Microsoft Online Services 資産を悪意ある ソフトウェアから保護する主要なメカニズムです。この種のソフトウェアは、サービ ス システムに対するコンピューター ウイルスやワームの侵入を検出して阻止しま す。 お客様はOffice 365に接続する機器についてコンピュータウイルス対策を実施す る必要があります。	適合可能	文献[21]に、Office 365上の資産保護のため、不正プログラム対策ソフト ウェアが初期構成の段階で実装されている旨が明示されている。 同じく文献[21]に、潜在的なセキュリティ上の問題は、Office 365の内部イン シデント対応計画に則って調査及びエスカレーションされる旨が明示され ている。 SOC2レポートにおいて、マルウェアの検出と既知の脆弱性対策、感染シス テムの隔離等の対策について記載されていることを確認した。 ISO 27001の管理策「マルウェアに対する管理策」並びに「情報セキュリティ インシデントの管理及びその改善」に関する一連の管理策で求められてい る要件を考慮すると、不正プログラムからの保護や検出・復旧のための管 理策、マルウェア感染時のインシデント管理策に関しては十分考慮されて いると考えられる。	文献[21] P28 IVS-07 Infrastructure & Virtualization Security OS Hardening and Base Controls P33 SEF-02 Security Incident Management, EDiscovery & Cloud Forensics – Incident Management	SOC2レポート CA-45 ISO 27001:2013 A.12.2.1, A.16.1.1- 16.1.7	—	—	
実33	Office 365への接続はインターネットあるいは仮想プライベート接続回線 ExpressRoute for Office 365によって行います。お客様は接続形式について検討 し、契約の明確化を行う必要があります。	対象外	—	—	—	—	利用者は、回線接続契約に際して、接続 条件を明確にする必要がある。	
実34	実33と同様	対象外	—	—	—	—	利用者は、契約や規定により接続相手 先の本人確認や端末確認の方法を明確 にし、適切な管理を行う必要がある。	
実35	マイクロソフトは高度に自動化された仕組みによって Office 365 を運用しており、 オペレータによる運用は行っておりません。 お客様はお客様管理者について資格確認を行う必要があります。	適合可能	文献[21]に、商用環境における設定変更について、役割ベースのアクセス 制御が行われ、多要素認証を必要とし、すべてのアクセス要求が記録、監 査される旨が明示されている。	文献[21] P11 CCC-04 Change Control & Configuration Management Unauthorized Software Installations	—	—	利用者は、運用管理者がオペレータ の資格確認を行う必要がある。また、例 外的に開発担当者等にオペレーション資 格を付与するときは運用管理者が承認 する必要がある。 資格確認の例) 制服の着用 腕章の着用 名札の着用	
実36	マイクロソフトは高度に自動化された仕組みによって Office 365 を運用しており、 オペレータによる運用は行っておりません。 お客様はお客様管理者の操作についての依頼・承認手続きを明確にする必要が あります。	適合可能	文献[21]に、Office 365の本番環境へのアクセス権は、特定のセキュリティ グループの承認済みメンバーにのみ与えられており、作業員については、 事前に承認された場合のみ、ジャストインタイムでアクセスが許可される旨 が明示されている。	文献[21] P11 CCC-04 Change Control & Configuration Management Unauthorized Software Installations	—	—	利用者は、オペレーションの依頼・承認 移管する手続きを定める必要がある。	
実37	マイクロソフトは高度に自動化された仕組みより Office 365 を運用しており、オペ レータによる運用を行っておりません。 お客様はお客様管理者の操作に関してオペレーション実行体制を明確にする必要 があります。	適合可能	文献[21]に、商用環境における設定変更について、役割ベースのアクセス 制御が行われ、多要素認証を必要とし、すべてのアクセス要求が記録、監 査される旨が明示されている。	文献[21] P11 CCC-04 Change Control & Configuration Management Unauthorized Software Installations	—	—	利用者は、オペレーターチームの編成お よびオペレーション手順を定める必要が ある。	
実38	マイクロソフトは高度に自動化された仕組みより Office 365 を運用しており、オペ レータによる運用を行っておりません。 お客様はお客様管理者による操作記録を取得し、確認することが必要です。	適合可能	文献[21]に、商用環境における設定変更について、役割ベースのアクセス 制御が行われ、多要素認証を必要とし、すべてのアクセス要求が記録、監 査される旨が明示されている。	文献[21] P11 CCC-04 Change Control & Configuration Management Unauthorized Software Installations	—	—	利用者は、オペレーション実行時の運行 状況を確認し、オペレーションを記録する 必要がある。	

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者が必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
実39	Microsoft Online Services システムは、いかなるメディア バックアップも使用しません。また、Microsoft Online Services はデータセンター レプリケーション ソリューションを利用します。 お客様は保持期限や法的保留、バージョンングの設定を行い、Office 365 内のデータが適切に保護されることを確認する必要があります。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、アプリケーションと利用者コンテンツのバックアップ取得、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報のバックアップ」で求められている要件を考慮すると、バックアップ方針に従ったバックアップの実行と検査に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-49, CA-50, CA-51 ISO 27001:2013 A.12.3.1	－	利用者は、必要に応じて自社でのデータの抽出およびバックアップの実行を選択する必要がある。
実40	Microsoft Online Service のソース コード ライブラリへのアクセスは、承認された Microsoft Online Services スタッフと Microsoft Online Services 契約スタッフに限定されます。可能であれば、ソース コード ライブラリに独立したプロジェクト用の作業領域を個別に確保します。Microsoft Online Services スタッフと Microsoft Online Services 契約スタッフは、自らの職務で利用する作業領域に対するアクセス許可のみを受けます。ソース コード ライブラリに対する変更を監査ログに詳述し、そのログを保持します。	適合可能	文献[21]に、ソースコードライブラリへのアクセスは許可された担当者に限定されているほか、指定されたレビューによるレビューによって変更内容は制御されており、変更の詳細は監査ログに記録・保持される旨が明示されている。 ISO 27001の管理策「プログラムソースコードへのアクセス制御」で求められている要件を考慮すると、プログラムソースコードへのアクセス制限に関しては十分考慮されていると考えられる。	文献[21] P24 IAM-06 Identity & Access Management Source Code Access Restriction	ISO 27001:2013 A.9.4.5	－	利用者は、プログラムファイルの管理方法を定める必要がある。
実41	マイクロソフトは、情報システムの破壊や侵害、障害が発生しても欠かすことのできない重要な活動とビジネス機能について取り扱う、情報システム用の緊急時対応策を策定します。 マイクロソフトは、ハードウェア、ネットワーク、データセンターの各レベルで起きる障害を予測し、対策を立てて取り組むべく、Microsoft Online Services のソフトウェア、サービス、コントロールを刷新しました。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考慮すると、業務継続のための可用性確保に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	ISO 27001:2013 A.17.2.1	－	利用者は、重要なプログラムのバックアップを取得し、保管管理方法を明確にする必要がある。
実42	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、ネットワーク装置を含む機器へのアクセスは多要素認証により制限されていること、ポリシーに違反する設不正な設定変更を自動検知する仕組みを採用していることが明示されている。 同じく文献[01]に、診断ポート、構成ポートへのアクセスは利用者の認可の上ではじめて可能になるように制御されていること、不使用ポート等などは無効化されていることが明示されている。 SOC2レポートにおいて、ネットワーク機器の管理手続、ネットワーク機器へのアクセス管理、アクセス方法の制限について記載されていることを確認した。	文献[01] P25 DCS-03: Datacenter Security – Equipment Identification P47 IAM-03: Identity & Access Management – Diagnostic / Configuration Ports Access	SOC2レポート VM-7, OA-9, OA-13	－	－
実43	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、障害・災害からの復旧を目的とするインフラストラクチャデータのバックアップが定期的に作成され、データの復元が定期的に検証される旨、明示されている。 SOC2レポートにおいて、主要コンポーネントの遠隔地バックアップの実施、及びデータ保全サービスについて記載されていることを確認した。	文献[01] P17 BCR-11: Business Continuity Management & Operational Resilience – Retention Policy	SOC2レポート DS-5, DS-8	－	－
実44	Office 365 の運用関連ドキュメントについては社内の SharePoint サイトおよび Office 365 Trust Metadata Record ツールに格納し、紛失、不正利用、破損などから適切に保護されています	適合可能	文献[21]に、操作手順書やサーバーのベースラインやセキュリティ強化に関する手引き、システム構築ドキュメントを含む豊富な(Extensive)ドキュメントが、内部サイト上に保存され、権限のある担当者に提供されている旨が明示されている。 ISO 27001の管理策「文書の適切な管理」並びに「文書の十分な保護」で求められている要件を考慮すると、運用ドキュメントの管理と保護に関しては十分考慮されていると考えられる。	文献[21] P7 BCR-04 Business Continuity Management & Operational Resilience Documentation	ISO 27001:2013 C.7.5.3.Part1-a, C.7.5.3.Part1-b	－	－
実45	実44と同様	適合可能	文献[21]に、操作手順書やサーバーのベースラインやセキュリティ強化に関する手引き、システム構築ドキュメントを含む豊富な(Extensive)ドキュメントが、内部サイト上に保存され、権限のある担当者に提供されている旨が明示されている。 同じく文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 ISO 27001の管理策「文書の十分な保護」で求められている要件を考慮すると、運用ドキュメントの保護に関しては十分考慮されていると考えられる。	文献[21] P7 BCR-04 Business Continuity Management & Operational Resilience Documentation P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	ISO 27001:2013 C.7.5.3.Part1.b	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
実46	マイクロソフトは、許容されるサービスのパフォーマンスと可用性の基準に照らし、Microsoft Online Services プラットフォームの主要サブシステムのパフォーマンスを予防的に監視し、常時測定します。しきい値に達した場合や異常イベントが検知された場合は、運用担当者が問題に対処できるよう、監視システムから警告が発行されます。 お客様は Office 365 接続用回線・設備や、Office 365 からの監視アラートの受信などについて監視体制を整備する必要があります。	適合可能	文献[21]に、Office 365においては、サービスプラットフォームの主要なサブシステムの稼働状況を継続監視しており、しきい値に達するか異常を検知した場合には警告することで運用スタッフが対処可能である旨が明示されている。 SOC2レポートにおいて、処理容量と可用性が運用チームによって監視されていること、ネットワーク機器のセキュリティイベントの監視について記載されていることを確認した。 ISO 27001の管理策「容量・能力の管理」で求められている要件を考慮すると、リソースの監視と調整、将来的な予測に関しては十分考慮されていると考えられる。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	文献[21] P34 STA-03 Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	SOC2レポート CA-30、CA-48 ISO 27001:2013 A.12.1.3	不正アクセス検知時に必要なアラートやプロセス名などの情報を運用管理者に提供している	—
実47	マイクロソフトでは、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、CPU 使用率、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。 お客様は Office 365 接続用回線・設備や、Office 365 内の記憶領域使用量などについて使用状況の確認を行う必要があります。	適合可能	文献[21]に、Office 365においては、サービスプラットフォームの主要なサブシステムの稼働状況を継続監視しており、しきい値に達するか異常を検知した場合には警告することで運用スタッフが対処可能である旨が明示されている。 SOC2レポートにおいて、処理容量と可用性が運用チームによって監視されていること、マネジメント層によってレビューされていることについて記載されていることを確認した。 ISO 27001の管理策「容量・能力の管理」で求められている要件を考慮すると、リソースの監視と調整、将来的な予測に関しては十分考慮されていると考えられる。	文献[21] P34 STA-03 Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	SOC2レポート CA-30、CA-31 ISO 27001:2013 A.12.1.3	—	利用者は、各種資源の能力及び使用状況の確認を行い、システムの性能強化や機能強化、組み合わせの再検討等を行う必要がある。
実48	Microsoft Online Services 環境内の主要なハードウェア資産のインベントリは、資産管理ツールで管理します。資産所有者は、資産インベントリに記載された資産所有者や、関係する担当者、場所、セキュリティ分類などの最新情報を管理する責任を負います。また、資産所有者は、標準に従って資産の保護を分類し、維持する必要があります。	適合可能	文献[21]に、Office 365においてはデータベース上で資産目録を集中管理しており、分類及び所有権の検証を毎月実施している旨が明示されている。 SOC2レポートにおいて、ソフトウェアの変更とリリースの管理規程が文書化・維持管理されたうえで実際に適用させていることについて記載されていることを確認した。 ISO 27001の管理策「資産目録」並びに「装置の保守」で求められている要件を考慮すると、構成・バージョンの管理と維持に関しては十分考慮されていると考えられる。	文献[21] P12 Datacenter Security Asset Management DCS-01	SOC2レポート CA-18 ISO 27001:2013 A.8.1.1、A.11.2.4	—	—
実49	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、ネットワーク装置を含む機器へのアクセスは多要素認証により制限されていること、ポリシーに違反する設不正な設定変更を自動検知する仕組みを採用していることが明示されている。 同じく文献[01]に、資産管理ポリシーに従った維持管理・保護が行われており、全ての機器にはラベルが貼り付けられていることが明示されている。 SOC2レポートにおいて、ネットワーク機器へのアクセス管理、アクセス方法の制限及び、データセンターへの入館手続と物理アクセス管理について記載されていることを確認した。	文献[01] P25 DCS-03: Datacenter Security – Equipment Identification P26 DSI-04: Data Security & Information Lifecycle Management –Handling / Labeling / Security Policy	SOC2レポート OA-9、OA-13、OA-14、PE-1、PE-4	—	—
実50	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、ネットワーク装置を含む機器へのアクセスは多要素認証により制限されていること、ポリシーに違反する不正な設定変更を自動検知する仕組みを採用していることが明示されている。 同じく文献[01]に、資産管理ポリシーに従った維持管理・保護が行われており、全ての機器にはラベルが貼り付けられていることが明示されている。 SOC2レポートにおいて、ネットワーク機器へのアクセス管理、アクセス方法の制限及び、データセンターへの入館手続と物理セキュリティ対策について記載されていることを確認した。	文献[01] P25 DCS-03: Datacenter Security – Equipment Identification P26 DSI-04: Data Security & Information Lifecycle Management –Handling / Labeling / Security Policy	SOC2レポート OA-9、OA-13、OA-14、PE-1、PE-4	—	—
実51	＜本項は Azure用評価シートを参照ください＞	適合可能	同じく文献[01]に、資産管理ポリシーに従った維持管理・保護が行われており、全ての機器にはラベルが貼り付けられていることが明示されている。 SOC2レポートにおいて、文書化された規則に基づいたデータセンター設備保守の手続と実施について記載されていることを確認した。	文献[01] P26 DSI-04: Data Security & Information Lifecycle Management –Handling / Labeling / Security Policy	SOC2レポート PE-6	—	—
実52	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理が行われていること、サービスのパフォーマンスと可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容可能水準内にあることをシステムにより監視していること、異常を検知した場合は運用要員に警告が発せられることが明示されている。 SOC2レポートにおいて、データセンター設備の24時間365日監視及び、文書化された規則に基づいたデータセンター設備保守の手続と実施について記載されていることを確認した。	文献[01] P57 IVS-04: Infrastructure & Virtualization Security – Information System Documentation	SOC2レポート PE-5、PE-6	—	—

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者に必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
実53	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、「サービスの提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装している」旨が、及び「資産所有者は、その資産に関する情報を常に最新にしておく責任を担う」旨が明示されている。 同じく文献[01]に、Azureの主要サービスに関する事業継続計画が文書化され、障害・災害対応時の役割・責任・復旧手順などが示されていること、運用手順諸等の文書がセキュリティの確保された内部サイトに保管されていること、BCPチームによる復旧手順のテストが最低年1回は実施されていることが明示されている。 SOC2レポートにおいて、インシデント対応フレームワークの策定、BCPの文書化、データセンター設備の24時間365日監視、文書化された規則に基づいたデータセンター設備保守の手続と実施、温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理について記載されていることを確認した。	文献[01] P26 DSI-04: Data Security & Information Lifecycle Management –Handling / Labeling / Security Policy P12 BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing P13 BCR-04: Business Continuity Management & Operational Resilience – Documentation	SOC2 レポート IM-1, BC-1, PE-5, PE-6, PE-7	－	－
実54	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、資産管理ポリシーに従った維持管理・保護が行われており、全ての機器にはラベルが貼り付けられていることが明示されている。 同じく文献[01]に、データセンター施設の管理がセキュリティポリシーに則って行われていることが明示されている。 SOC2レポートにおいて、BCPの文書化、データセンター設備の24時間365日監視、文書化された規則に基づいたデータセンター設備保守の手続と実施について記載されていることを確認した。	文献[01] P26 DSI-04: Data Security & Information Lifecycle Management –Handling / Labeling / Security Policy P29 DCS-06: Datacenter Security – Policy	SOC2レポート BC-1, IM-1, PE-5, PE-6	－	－
実55	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理が行われていること、サービスのパフォーマンスと可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容可能水準内にあることをシステムにより監視していること、異常を検知した場合は運用要員に警告が発せられることが明示されている。 同じく文献[01]に、データセンター施設の管理がセキュリティポリシーに則って行われていることが明示されている。 SOC2レポートにおいて、予測に基づく容量管理、データセンター設備の24時間365日監視、文書化された規則に基づいたデータセンター設備保守の手続と実施について記載されていることを確認した。	文献[01] P57 IVS-04: Infrastructure & Virtualization Security – Information System Documentation P29 DCS-06: Datacenter Security – Policy	SOC2レポート CCM-5, BC-1, IM-1, PE-5, PE-6	－	－
実56	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、データセンター施設の入館は業務上の必要がある場合に限られ、事前の認可申請を行い、バッジの発行を受ける必要があることが明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。 SOC2レポートにおいて、データセンターへの入館手続、資格確認、物理アクセス管理、データセンター設備の24時間365日監視について記載されていることを確認した。	文献[01] P30 DCS-08: Datacenter Security – Unauthorized Persons Entry P30 DCS-09: Datacenter Security – User Access	SOC2レポート PE-1, PE-2, PE-4, PE-5	－	－
実57	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、データセンター施設のエントランスは24時間365日の監視が行われ、施錠管理、バッジによる個人別入館許可が行われていることが明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。 SOC2レポートにおいて、データセンターへの入館手続、資格確認、物理アクセス管理、データセンター設備の24時間365日監視について記載されていることを確認した。	文献[01] P30 DCS-07: Datacenter Security – Secure Area Authorization P30 DCS-09: Datacenter Security – User Access	SOC2レポート PE-1, PE-2, PE-4, PE-5	－	－
実58	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。 SOC2レポートにおいて、データセンターへの入館手続、資格確認、物理アクセス管理、データセンター設備の24時間365日監視について記載されていることを確認した。	文献[01] P30 DCS-08: Datacenter Security – Unauthorized Persons Entry P30 DCS-09: Datacenter Security – User Access	SOC2レポート PE-2, PE-4	－	－
実59	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、データセンター施設の管理がセキュリティポリシーに則って行われていることが明示されている。 同じく文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 SOC2レポートにおいて、物理アクセス管理及び、データセンター設備の24時間365日監視について記載されていることを確認した。	文献[01] P29 DCS-06: Datacenter Security – Policy P30 DCS-08: Datacenter Security – Unauthorized Persons Entry	SOC2レポート PE-4, PE-5	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	SI事業者・利用者が必要な対応
実60	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[P10]に、「24 時間 365 日体制のグローバルなインシデント対応サービスを提供」し、攻撃や悪意のある活動の影響抑制を行っている旨が明記されている。 SOC2レポートにおいて、BCPの文書化、BCP/DR標準手順の策定・テスト・改善、データセンターへの入館手続、データセンター設備の24時間365日監視について記載されていることを確認した。	文献[P10] P8 インシデント管理と対応	SOC2レポート BC-1, BC-3, BC-4, BC-5, PE-1, PE-5	－	－
実61	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、エンドユーザが操作できる権限を明確にする必要がある。
実62	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、操作権限を付与するオペレータカード（オペレータキー、IDを含む）の管理者を定めて管理する必要がある。
実63	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、エンドユーザの操作内容を記録し、検証できる体制を整備する必要がある。
実64	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	－
実65	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、データの入力手続き、承認等の手順を策定する必要がある。
実66	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、出力情報の作成、授受、保管、管理および廃棄について、不正防止対策および機密保護対策を講じる必要がある。
実67	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	－
実68	Office 365は金融取引を実行するシステムではありません	対象外	－	－	－	－	利用者は、重要な印字済帳票の授受および廃棄の方法を定める必要がある。
実69	お客様のデータはお客様に帰属する為、顧客や生体認証に関するデータやデータの制御を行なう事、それらの管理は利用者の責任となります。	対象外	－	－	－	－	利用者は、顧客データの管理・取扱い方法を定める必要がある。特に機微情報を取り扱う場合は、必要な措置を行う必要がある。
実70	Microsoft Online Services では、業界およびマイクロソフトのベストプラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、および回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、および改訂のプロセス	適合可能	文献[25]に、ポータルサイトに管理者アカウントでログインすることで、サービスの稼働状況をリアルタイムで取得できる旨が明示されている。 SOC2レポートにおいて、インシデントレスポンスガイドの共有と利用、Service Health Centerを通じた利用者への重要インシデントに関する情報開示、サービスチームのオンコール体制について記載されていることを確認した。 ISO 27001の管理策「情報セキュリティに関する組織内外の情報伝達」に関連する一連の管理策で求められている要件を考慮すると、障害時・災害時の連絡手段を定めることに関しては十分考慮されていると考えられる。	文献[25] How to check Office 365 service health	SOC2レポート CA-13, CA-15, CA-29 ISO 27001:2013 C.7.4	－	利用者は、障害時・災害時に関係者への連絡先と連絡手順を定めておく必要がある。
実71	実70と同様	適合可能	文献[21]に、「Enterprise Business Continuity Management (EBCM)」フレームワークが確立されている旨、及びまたEBCMフレームワークに関するガイドダンスには、ガバナンス／影響の許容範囲／ビジネスの影響分析／依存関係の分析（非技術面及び技術面）／戦略／計画／テスト／トレーニング及び意識向上といったコンポーネントが含まれる旨が明示されている。 SOC2レポートにおいて、インシデントレスポンスガイドの共有と利用、Service Health Centerを通じた利用者への重要インシデントに関する情報開示、サービスチームのオンコール体制、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。	文献[21] P12 BCR-01 Business Continuity Management & Operational Resilience – Business Continuity Planning	SOC2レポート CA-13, CA-15, CA-29, CA-30	－	利用者は、障害時・災害時におけるコンピュータシステムの復旧手順を明確にする必要がある。

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	SI事業者・利用者で必要な対応
実72	実70と同様	適合可能	文献[21]に、「Enterprise Business Continuity Management (EBCM)」フレームワークが確立されている旨、及びまたEBCMフレームワークに関するガイドランスには、ガバナンス／影響の許容範囲／ビジネスの影響分析／依存関係の分析（非技術面及び技術面）／戦略／計画／テスト／トレーニング及び意識向上といったコンポーネントが含まれる旨が明示されている。 SOC2レポートにおいて、インシデントレスポンスガイドの共有と利用、Service Health Centerを通じた利用者への重要インシデントに関する情報開示、サービスチームのオンコール体制、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。	文献[21] P12 BCR-01 Business Continuity Management & Operational Resilience – Business Continuity Planning	SOC2レポート CA-13, CA-15, CA-29, CA-30	－	－
実73	お客様は、Office 365の利用に関するコンティンジェンシープランを策定する必要があります。 マイクロソフトの対応については実70を参照ください	適合可能	文献[21]に、「Enterprise Business Continuity Management (EBCM)」フレームワークが確立されている旨が、及びEBCMフレームワークに関するガイドランスには、ガバナンス／影響の許容範囲／ビジネスの影響分析／依存関係の分析（非技術面及び技術面）／戦略／計画／テスト／トレーニング及び意識向上といったコンポーネントが含まれる旨が明示されている。 SOC2レポートにおいて、インシデントレスポンスガイドの共有と利用、Service Health Centerを通じた利用者への重要インシデントに関する情報開示、サービスチームのオンコール体制、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。	文献[21] P12 BCR-01 Business Continuity Management & Operational Resilience – Business Continuity Planning	SOC2レポート CA-13, CA-15, CA-29, CA-30	－	－
実74	Microsoft Online Services システムは、いかなるメディア バックアップも使用しません。また、Microsoft Online Services はデータセンター レプリケーション ソリューションを利用します。各 Microsoft Online Services サービスのビジネス継続計画は、Microsoft Online Services データのレプリケーションを実行する手順を示します。 マイクロソフトは、情報システムの破壊や侵害、障害が発生しても欠かすことのできない重要な活動とビジネス機能について取り扱う、情報システム用の緊急時対応策を策定します。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報のバックアップ」並びに「情報処理施設の可用性」で求められている要件を考慮すると、災害時にバックアップサイトとしての機能を果たすための構成に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50, CA-51 ISO 27001:2013 A.12.3.1, A.17.2.1	－	－
実75	マイクロソフトは、情報セキュリティの留意点を反映したシステム開発ライフサイクルを使用して、情報システムを管理します。マイクロソフトによるライフサイクル サポートの実装は、すべてのエンジニアリングと開発プロジェクトが準拠する SDL プロセスの中で概要が示されています。これは、セキュリティに関する特定の考慮事項を組み込んだソフトウェア開発モデルです。セキュリティ要件分析は、すべてのシステム開発プロジェクトに対して実行する必要があります。この分析ドキュメントはフレームワークとして機能し、完成した開発プロジェクトに対して想定されるリスクを明らかにするほか、開発段階で採用しテストできる軽減策を特定します。 お客様は Office 365 の環境変更等について手順を明確にする必要があります。	適合可能	文献[21]に、Office 365においては、ソフトウェア開発、ハードウェアの変更、リリース管理のすべてに適用される、ISO 27001、SOC 1 / SOC 2、NIST 800-53といった規制ガイドラインと一致する、変更管理プロセス管理のための標準操作手順が開発済みである旨が明示されている。 SOC2レポートにおいて、ソフトウェアの変更とリリースの管理規程が文書化・維持管理されたうえで実際に適用されていること、リリース前にコードレビューを含むセキュリティレビューが行われていることについて記載されていることを確認した。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」「システムの変更管理手順」「セキュリティに配慮したシステム構築の原則」「セキュリティに配慮した開発環境」で求められている要件を考慮すると、システム開発・変更における正当性の検証に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing	SOC2レポート CA-18, CA-46 ISO 27001:2013 A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6	－	－
実76	マイクロソフトは、製品、システム コンポーネント、運用サービスの開発者に対して、開発中にテストや評価を実行するよう要求します。サービス チームは、マイクロソフト SDL プロセスに従って、すべてのシステム開発とメンテナンス作業を実施する責任を負います。 変更は分離されたテスト環境を使用してテストされ、その後、本番環境に1顧客として構成されたマイクロソフト社内IT環境でテストされ、先行リリースを希望するお客様環境での実利用テストを経て全顧客の環境へ展開されます。 お客様は Office 365 本番テナントの一部、あるいはテスト用別テナントを使用してテスト環境を整備する必要があります。	適合可能	文献[21]に、Office 365のインフラにおいては、運用環境と非運用環境が物理的かつ論理的に分離されている旨が明示されている。 SOC2レポートにおいて、変更管理が定められたプロセスに従って実施されレビューされること、リリース前にコードレビューを含むセキュリティレビューが行われていることについて記載されていることを確認した。 ISO 27001の管理策「セキュリティに配慮した開発環境」「システムセキュリティの試験」「システムの受入れ試験」で求められている要件を考慮すると、テスト環境の整備に関しては十分考慮されていると考えられる。	文献[21] P29 IVS-08 Infrastructure & Virtualization Security Production / NonProduction Environments	SOC2レポート CA-21, CA-46 ISO 27001:2013 A.14.2.6, A.14.2.8, A.14.2.9	－	－
実77	マイクロソフトは、情報セキュリティの留意点を反映したシステム開発ライフサイクルを使用して、情報システムを管理します。マイクロソフトによるライフサイクル サポートの実装は、すべてのエンジニアリングと開発プロジェクトが準拠する SDL プロセスの中で概要が示されています。これは、セキュリティに関する特定の考慮事項を組み込んだソフトウェア開発モデルです。 また、公式のセキュリティ品質保証プロセスを導入して、セキュリティに対する既知の脅威と悪用に関する脆弱性をテストします。このプロセスでは、自動セキュリティテスト ツールを使用し、システムを運用リリースする前にあらゆる重度の脆弱性を改善することが求められます。 お客様はユーザーやデータの本番移行、変更の本番適用について移行手順を明確にする必要があります。	適合可能	文献[21]に、Office 365においては、ソフトウェア開発、ハードウェアの変更、リリース管理のすべてに適用される、ISO 27001、SOC 1 / SOC 2、NIST 800-53といった規制ガイドラインと一致する、変更管理プロセス管理のための標準操作手順が開発済みである旨が明示されている。 SOC2レポートにおいて、ソフトウェアの変更とリリースの管理規程が文書化・維持管理されたうえで実際に適用されていること、変更管理が定められたプロセスに従って実施されレビューされること、リリース前にコードレビューを含むセキュリティレビューが行われていることについて記載されていることを確認した。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」「システムの変更管理手順」「システムセキュリティの試験」「システムの受入れ試験」で求められている要件を考慮すると、リリース時の安全性確保に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing	SOC2レポート CA-18, CA-21, CA-46 ISO 27001:2013 A.14.2.1, A.14.2.5, A.14.2.8, A.14.2.9	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	SI事業者・利用者で必要な対応
実78	Office 365のISMSは作成が必要となるドキュメントを規定しています。マイクロソフトおよびOffice 365のセキュリティポリシーはOffice 365の各チームに対する情報セキュリティの目標とベースラインを規定します。これは担当マネージャの戦略的な優先順位として変換され実施されます。	適合可能	文献[21]に、ソフトウェア開発及びリリースの標準管理プロセスによる管理が明示されている。管理プロセスに含まれる管理策として以下が示されている。 ・計画された変更の特定と文書化 同じく文献[21]に、操作手順書やサーバーのベースラインやセキュリティ強化に関する手引き、システム構築ドキュメントを含む豊富な(Extensive)ドキュメントが、安全な内部サイト上に保存され、権限のある担当者に提供されている旨が明示されている。 ISO 27001の管理策「ISMSの定める文書の整備」「作成対象文書の規定」「ドキュメントの管理」「ドキュメントの保護」で求められている要件を考慮すると、ドキュメント作成手順に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-01 Change Control & Configuration Management – New Development / Acquisition P7 BCR-04 Business Continuity Management & Operational Resilience Documentation	ISO 27001:2013 C.7.5.1.a、C.7.5.2.a、C.7.5.3.Part1.a、C.7.5.3.Part1.b	—	—
実79	実78と同様	適合可能	文献[21]に、ソフトウェア開発及びリリースの標準管理プロセスによる管理が明示されている。管理プロセスに含まれる管理策として以下が示されている。 ・計画された変更の特定と文書化 同じく文献[21]に、操作手順書やサーバーのベースラインやセキュリティ強化に関する手引き、システム構築ドキュメントを含む豊富な(Extensive)ドキュメントが、安全な内部サイト上に保存され、権限のある担当者に提供されている旨が明示されている。 ISO 27001の管理策「ISMSの定める文書の整備」「作成対象文書の規定」「ドキュメントの管理」「ドキュメントの保護」で求められている要件を考慮すると、ドキュメント作成手順に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-01 Change Control & Configuration Management – New Development / Acquisition P7 BCR-04 Business Continuity Management & Operational Resilience Documentation	ISO 27001:2013 A.12.1.1、A.14.2.2、C.7.5.3.Part1.a、C.7.5.3.Part1.b	—	—
実80	お客様は、マイクロソフト以外のサードパーティが Office 365 上で提供するアドオンやアプリ、追加ツール等を導入する場合、それに対する評価、運用、管理の体制を明確にする必要があります。	対象外	—	—	—	—	利用者は、Office365サービスの導入にあたり、その有効性、信頼性、生産性などを評価する体制を整備する必要があります。
実81	お客様は、マイクロソフト以外のサードパーティが Office 365 上で提供するアドオンやアプリ、追加ツール等を導入する場合、それに対する評価、運用、管理の体制を明確にする必要があります。	対象外	—	—	—	—	利用者は、Office365サービス導入後の運用にあたり、運用・管理体制を明確にする必要がある。
実82	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉碎、償却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 すべての Microsoft Online Services は、承認された記憶域メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 詳細については監査対象統制策の中の、右欄に記載の項目を参照してください。	適合可能	文献[21]に、マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用している旨、及び消去不能なハードドライブについては、シュレッダー等によって破壊している旨、及び破壊の記録が保持されている旨が明示されている。 ISO 27001の管理策「取外し可能な媒体の管理」「媒体の処分」で求められている要件を考慮すると、廃棄計画と廃棄手順に関しては十分考慮されていると考えられる。	文献[21] P15 Data Security & Information Lifecycle Management Secure Disposal	ISO 27001:2013 A.8.3.1、A.8.3.2	—	—
実83	＜本項は Azure用評価シートを参照ください＞	適合可能	文献[01]に、「ベストプラクティスの手順と、NIST 800-88 準拠の消去ソリューション」に関する記載、及び「Windows Azure のすべてのサービスは、承認された記憶メディアと廃棄管理サービスを使用」する旨が明示されている。 SOC2レポートにおいて、ハードディスク廃棄時の破壊規定、顧客データの削除規定について記載されていることを確認した。	文献[01] P27 DSI-07: Data Security & Information Lifecycle Management – Secure Disposal	SOC2レポート DS-10、DS-15	—	—
実84	マイクロソフトは、情報システムの破壊や侵害、障害が発生しても欠かすことのできない重要な活動とビジネス機能について取り扱う、情報システム用の緊急時対応策を策定します。 マイクロソフトは、ハードウェア、ネットワーク、データセンターの各レベルで起きる障害を予測し、対策を立てて取り組むべく、Microsoft Online Services のソフトウェア、サービス、コントロールを刷新しました。 障害の対処をデータセンター層（サードパーティ製ハードウェアに依存する）の代わりに、アプリケーション層（自社ソフトウェア内）で実施するように工夫することで、Microsoft Online Services は高い可用性と信頼性を達成しています。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考慮すると、装置障害時の可用性維持に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50、CA-51 ISO 27001:2013 A.17.2.1	—	—
実85	マイクロソフトは、情報システムの破壊や侵害、障害が発生しても欠かすことのできない重要な活動とビジネス機能について取り扱う、情報システム用の緊急時対応策を策定します。 マイクロソフトは、ハードウェア、ネットワーク、データセンターの各レベルで起きる障害を予測し、対策を立てて取り組むべく、Microsoft Online Services のソフトウェア、サービス、コントロールを刷新しました。 障害の対処をデータセンター層（サードパーティ製ハードウェアに依存する）の代わりに、アプリケーション層（自社ソフトウェア内）で実施するように工夫することで、Microsoft Online Services は高い可用性と信頼性を達成しています。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考慮すると、装置障害時の可用性維持に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50、CA-51 ISO 27001:2013 A.17.2.1	—	—

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者が必要な対応
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
実86	実84に同じ お客様はOffice 365に接続するための通信系機器について対応が必要になることが あります。	適合可能	文献[19]に、データセンター及び各ノードが世界規模で分散されている旨、 及び障害発生時には再ルーティングが可能である旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地 での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考 慮すると、装置障害時の可用性維持に関しては十分考慮されていると考え られる。	文献[19] P4 Global Network Reliability	SOC2レポート CA-50、CA-51 ISO 27001:2013 A.17.2.1	—	—
実87	実84に同じ お客様はOffice 365に接続する回線部分について対応が必要になることがありま す。	適合可能	文献[19]に、データセンター及び各ノードが世界規模で分散されている旨、 2,000以上のネットワークを収容可能な世界最大規模のバックボーン回線に 接続されている旨、及び障害発生時には再ルーティングが可能である旨が 明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地 での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考 慮すると、装置障害時の可用性維持に関しては十分考慮されていると考え られる。	文献[19] P4 Global Network Reliability	SOC2レポート CA-50、CA-51 ISO 27001:2013 A.17.2.1	—	—
実88	実84に同じ（Office 365では端末系装置に該当するものはありませんが、監視装 置の端末、DevOpsエンジニアが使用する端末は地域冗長性を持たせたり、予備 機による代替が簡単に可能としています） お客様はお客様環境で使用する特定端末についての対応が必要になることがあ ります。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のため の代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地 での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報処理施設の可用性」で求められている要件を考 慮すると、装置障害時の可用性維持に関しては十分考慮されていると考え られる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50、CA-51 ISO 27001:2013 A.17.2.1	—	—
実89	マイクロソフトは、情報セキュリティの留意点を反映したシステム開発ライフサイ クルを使用して、情報システムを管理します。マイクロソフトによるライフサイクル サ ポートの実装は、すべてのエンジニアリングと開発プロジェクトが準拠する SDL プ ロセスの中で概要が示されています。これは、セキュリティに関する特定の考慮事 項を組み込んだソフトウェア開発モデルです。セキュリティ要件分析は、すべての システム開発プロジェクトに対して実行する必要があります。 詳細は管理対象統制策の中の、右欄の記載の項目を参照してください。	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されてい る。 同じく文献[21]に、進行中の脅威モデル、コードレビュー、セキュリティテスト によってセキュリティ違反を防止するSDLの概要について明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」で求めら れている要件を考慮すると、ソフトウェア開発の一連の工程におけるセキュ リティ対策に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing P6 AIS-01 Application & Interface Security Application Security 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.1	—	—
実90	実89に同じ	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されてい る。 同じく文献[21]に、進行中の脅威モデル、コードレビュー、セキュリティテスト によってセキュリティ違反を防止するSDLの概要について明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」で求めら れている要件を考慮すると、ソフトウェア開発の一連の工程におけるセキュ リティ対策に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing P6 AIS-01 Application & Interface Security Application Security 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.1	—	—
実91	実89に同じ	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されてい る。 同じく文献[21]に、進行中の脅威モデル、コードレビュー、セキュリティテスト によってセキュリティ違反を防止するSDLの概要について明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」で求めら れている要件を考慮すると、ソフトウェア開発の一連の工程におけるセキュ リティ対策に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing P6 AIS-01 Application & Interface Security Application Security 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.1	—	—

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	SI事業者・利用者で必要な対応
実92	実89に同じ	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されている。 同じく文献[21]に、進行中の脅威モデル、コードレビュー、セキュリティテストによってセキュリティ違反を防止するSDLの概要について明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮した開発のための方針」で求められている要件を考慮すると、ソフトウェア開発の一連の工程におけるセキュリティ対策に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing P6 AIS-01 Application & Interface Security Application Security 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.1	－	－
実93	マイクロソフトは、情報システムの仕様、設計、開発、実装、変更において、情報システム セキュリティ エンジニアリングの原則を適用します。あらゆるエンジニアリングと開発のプロジェクトで、マイクロソフト SDL プロセスに従います。マイクロソフト SDL プロセスは、すべての Microsoft Online Services システムに標準セキュリティ エンジニアリングの原則を実装する、以下のフェーズを規定しています。 詳細は、監査対象統制策の中、右欄記載の項目を参照してください。	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されている。 同じく文献[21]に、進行中の脅威モデル、コードレビュー、セキュリティテストによってセキュリティ違反を防止するSDLの概要について明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮したシステム構築の原則」並びに「システムセキュリティの試験」で求められている要件を考慮すると、リリース時の整合性検査及びマルウェア検査に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing P6 AIS-01 Application & Interface Security Application Security 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.5、A.14.2.8	－	－
実94	お客様は、マイクロソフト以外のサードパーティが Office 365 上で提供するアドオンやアプリ、追加ツール等を導入する場合、それに対する評価、運用、管理の体制を明確にする必要があります。	適合可能	文献[21]に、マイクロソフトの定める開発規定である「Security Development Lifecycle(SDL)」に従った品質管理策を実施していることが明示されている。 また文献[09]に、「セキュリティ開発ライフサイクル＝Security Development Lifecycle (SDL)」によるセキュリティ対策の詳細について明示されている。 ISO 27001の管理策「セキュリティに配慮したシステム構築の原則」で求められている要件を考慮すると、リリース時の整合性検査に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing 文献[09] SDL PRACTICE #5: ESTABLISH DESIGN REQUIREMENTS	ISO 27001:2013 A.14.2.5	－	－
実95	マイクロソフトでは大規模なクラウド環境の維持管理のために、定型的な作業のほとんどの部分を自動化し、合理化しています。自動化されたプロセスの一部は、SOC2レポートの、Office Service Plus、ユーザーアクセス権管理(New user or modification of user access, Termination access removal, Just-in-time access)、Customer Lockboxプロセス、サーバー構築プロセス(Server build-out process)などに記載があります。また、自動化されたテストについては監査対象統制策の中、右欄に記載の項目で監査されています。	適合可能	文献[21]に、Office 365においては、ソフトウェア開発、ハードウェアの変更、リリース管理のすべてに適用される、ISO 27001、SOC 1 / SOC 2、NIST 800-53といった規制ガイドラインと一致する、変更管理プロセス管理のための標準操作手順が開発済みである旨が明示されている。 SOC2レポートにおいて、新規アクセスの承認やアクセス可能時間の制御を自動化して実施されていることについて記載されていることを確認した。 ISO 27001の「開発及びサポートプロセスにおけるセキュリティ」に関する一連の管理策で求められている要件を考慮すると、変更管理における正確性を確保した上での合理化に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing	SOC2レポート Description of control activities ISO 27001:2013 A.14.2.1-A.14.2.9	－	－
実96	実運用されている Microsoft Online Services システムに対する変更は、公式の変更統制手順に従います。この手順には、レビューと承認のプロセスが含まれます。 詳細は、監査対象統制策の中、右欄の項目を参照してください。	適合可能	文献[21]に、Office 365においては、ソフトウェア開発、ハードウェアの変更、リリース管理のすべてに適用される、ISO 27001、SOC 1 / SOC 2、NIST 800-53といった規制ガイドラインと一致する、変更管理プロセス管理のための標準操作手順が開発済みである旨、明示されている。 SOC2レポートにおいて、ソフトウェアの変更とリリースの管理規程が文書化・維持管理されたうえで実際に適用されていること、リリース前にコードレビューを含むセキュリティレビューが行われていることについて記載されていることを確認した。 ISO 27001の「システムの変更管理手順」「オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー」に関する一連の管理策で求められている要件を考慮すると、変更管理における品質向上対策に関しては十分考慮されていると考えられる。	文献[21] P10 CCC-03 Change Control & Configuration Management Quality Testing	SOC2レポート CA-18、CA-46 ISO 27001-201 A.14.2.2、A.14.2.3	－	－
実97	SharePoint Online、OneDrive for Business上では文書管理機能の一部として、バージョン管理、排他制御機能を提供しています。競合する変更が行われた場合、利用者は別ファイルとして保存した文書の内容を確認し、競合を解決することが必要になる場合があります。	適合可能	文献[29]に、SharePoint Onlineにおけるファイルのチェックアウト機能について明示されている。 文献[30]に、Word Onlineにおける共同編集について明示されている。	文献[29] ファイルのチェックアウトを必須にするようにライブラリを設定する 文献[30] Word Online で文書の共同作業を行う	－	－	－
実98	実97に同じ	適合可能	文献[21]に、Microsoft Office 365においては処理エラーのリスクを抑えるため、Office 365 環境内に「内部処理制御 (Internal processing controls)」が実装されている旨、及び内部処理制御が「処理環境内だけでなくアプリケーション内にも存在している (exist in applications, as well as in the processing environment.)」旨が明示されている。	文献[21] P6 AIS-03 Application & Interface Security – Data Integrity	－	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	SI事業者・利用者で必要な対応
実99	Office 365は運用作業の効率化とセキュリティ確保のため、オペレーションのほとんどもを自動化しています。 お客様はOffice 365の管理作業について、自動化、簡略化を図ることが望ましいとされます。	適合可能	文献[21]に、Office 365環境においては、デバイス構成の不一致を検出するプロセスが自動化されている旨が明示されている。 同じく文献[21]に、Office 365環境においては、不要ユーザーアカウントの削除処理が自動化されている旨が明示されている。 同じく文献[21]に、Office 365環境においては、内部から開始されたDoS攻撃を自動的に検知する旨が明示されている。	文献[21] P12 DCS-03 Datacenter Security Equipment Identification P23 IAM-02 Identity & Access Management Credential Lifecycle / Provision Management	—	—	—
実100	マイクロソフトは高度に自動化された仕組みによって Office 365 を運用しており、オペレータによる運用は行っておりません。 お客様管理者が入力する項目について、数値、メールアドレスなどフォーマットが決まっているものについて入力チェックを行っています お客様はOffice 365管理作業についてオペレーションミスの防止策を充実させる必要があります。	適合可能	文献[21]に、Microsoft Office 365においては入力データに関して許容可能な基準を定めているほか、処理エラーのリスクを抑えるため、Office 365 環境内に「内部処理制御 (Internal processing controls)」が実装されている旨、及び内部処理制御が「処理環境内だけでなくアプリケーション内にも存在している (exist in applications, as well as in the processing environment.)」旨が明示されている。	文献[21] P6 AIS-03 Application & Interface Security – Data Integrity	—	—	—
実101	マイクロソフトは、許容されるサービスのパフォーマンスと可用性の基準に照らして、Microsoft Online Services プラットフォームの主要サブシステムのパフォーマンスを予防的に監視し、常時測定します。 お客様は、Office 365接続に使用するネットワークについて、負荷状況の監視、制御する必要があります。また、メールボックス使用量やSPO使用量などを監視、制御する必要があります。	適合可能	文献[21]に、Office 365においては、サービスプラットフォームの主要なサブシステムの稼働状況を継続監視しており、しきい値に達するか異常を検知した場合には警告することで運用スタッフが対処可能である旨、明示されている。 SOC2レポートにおいて、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。 ISO 27001の管理策「容量・能力の管理」で求められている要件を考慮すると、リソースの監視と調整、将来的な予測に関しては十分考慮されていると考えられる。	文献[21] P34 STA-03 Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	SOC2レポート CA-30 ISO 27001:2013 A.12.1.3	—	—
実102	マイクロソフトは、許容されるサービスのパフォーマンスと可用性の基準に照らして、Microsoft Online Services プラットフォームの主要サブシステムのパフォーマンスを予防的に監視し、常時測定します。 お客様は、Office 365接続に使用するネットワークや関連するオンプレシシステムについて、運用状況を監視する機能を設ける必要があります。	適合可能	文献[21]に、Office 365においては、サービスプラットフォームの主要なサブシステムの稼働状況を継続監視しており、しきい値に達するか異常を検知した場合には警告することで運用スタッフが対処可能である旨が明示されている。 SOC2レポートにおいて、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。 ISO 27001の管理策「容量・能力の管理」で求められている要件を考慮すると、リソースの監視と調整、将来的な予測に関しては十分考慮されていると考えられる。	文献[21] P34 STA-03 Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	SOC2レポート CA-30 ISO 27001:2013 A.12.1.3	—	—
実103	マイクロソフトは、許容されるサービスのパフォーマンスと可用性の基準に照らして、Microsoft Online Services プラットフォームの主要サブシステムのパフォーマンスを予防的に監視し、常時測定します。 お客様は、Office 365接続に使用するネットワークや関連するオンプレシシステムについて、障害を切り分ける機能を設ける必要があります。	適合可能	文献[21]に、Office 365においては、サービスプラットフォームの主要なサブシステムの稼働状況を継続監視しており、しきい値に達するか異常を検知した場合には警告することで運用スタッフが対処可能である旨が明示されている。 SOC2レポートにおいて、処理容量と可用性が運用チームによって監視されていることについて記載されていることを確認した。 ISO 27001の管理策「容量・能力の管理」で求められている要件を考慮すると、リソースの監視と調整、将来的な予測に関しては十分考慮されていると考えられる。	文献[21] P34 STA-03 Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	SOC2レポート CA-30 ISO 27001:2013 A.12.1.3	—	—
実104	マイクロソフトは、ハードウェア、ネットワーク、データセンターの各レベルで起きる障害を予測し、対策を立てて取り組むべく、Microsoft Online Services のソフトウェア、サービス、コントロールを刷新しました。 障害の対処をデータセンター層（サードパーティ製ハードウェアに依存する）の代わりに、アプリケーション層（自社ソフトウェア内）で実施するように工夫することで、Microsoft Online Services は高い可用性と信頼性を達成しています。 お客様はOffice 365接続に使用するネットワークおよび関連するシステムについての、縮退・再構成機能を設ける必要があります。	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報のバックアップ」並びに「情報処理施設の可用性」で求められている要件を考慮すると、障害時の運用継続機能に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50, CA-51 ISO 27001:2013 A.12.3.1, A.17.2.1	—	—
実105	Office 365は金融取引のためのサービスではありません。	対象外	—	—	—	—	—
実106	実104に同じ	適合可能	文献[21]に、Office 365においては、バックアップ情報の保存と復元のための代替ストレージサイトが設置されている旨が明示されている。 SOC2レポートにおいて、システムのフェイルオーバー試験の実施、遠隔地での顧客コンテンツのコピー保全について記載されていることを確認した。 ISO 27001の管理策「情報のバックアップ」並びに「情報処理施設の可用性」で求められている要件を考慮すると、障害時のリカバリ機能に関しては十分考慮されていると考えられる。	文献[21] P8 BCR-07 Business Continuity Management & Operational Resilience Equipment Maintenance	SOC2レポート CA-50, CA-51 ISO 27001:2013 A.12.3.1, A.17.2.1	—	—

FISC安全対策基準（第9版）の項目	FISC安全対策基準（第9版） に対するMicrosoftの見解	Office 365 における対応					SI事業者・利用者に必要な対応
項番		FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
実107	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実108	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実109	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実110	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実111	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実112	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実113	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実114	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実115	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実116	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実117	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実118	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実119	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実120	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実121	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実122	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実123	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－

FISC安全対策基準（第9版）の項目	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	Office 365 における対応				SI事業者・利用者で必要な対応
項番			本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
実124	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実125	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実126	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実127	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実128	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実129	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実130	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実131	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実132	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実133	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実134	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実135	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実136	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	利用者は、電子的価値を蓄積する媒体等の紛失、盗難、破壊について、エンドユーザに対して明示する必要がある。 例) 契約時の取引規定 電子的価値を蓄積する媒体の裏面
実137	Office 365は金融サービス提供のためのシステムではありません	対象外	－	－	－	－	－
実138	電子メールの運用ポリシーについては、利用者自身で管理することが出来ます。 Exchange Onlineに関しては、4拠点クラスター構成、自動フェイルオーバーを行う機能を提供しております。 また計画メンテナンス時においても、Exchange Online、Exchange Online Archiving (EOA)、および Exchange Online Protection (EOP)については、予定されていたダウンタイムはありません。	適合可能	文献[26]に、Exchange Onlineのメールボックスは、地理的に分散したMicrosoftデータセンター内の複数のデータベースコピーに継続的にレプリケートされており、ローカル障害の発生時にデータを復元する機能を提供可能である旨が明示されている。	文献[26] Mailbox replication at data centers	－	－	利用者は、電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	SI事業者・利用者で必要な対応
実139	お客様は、業務目的以外の電子メールの送受信に対処するため、不正使用防止機能を講ずる必要があります。	対象外	—	—	—	—	利用者は、業務目的以外の電子メール送受信やホームページの閲覧等に対処するために、適切なアクセス制限や運用ルールなどにより対策を講じることが望ましい。
実140	Office 365は金融サービス提供のためのシステムではありません	対象外	—	—	—	—	利用者は、生体認証情報を用いる場合、安全に管理するための必要な手順を定める必要がある。
実141	Office 365は金融サービス提供のためのシステムではありません	対象外	—	—	—	—	利用者は、生体認証情報を用いる場合、その特性を考慮した安全対策を定める必要がある。
設1	マイクロソフト オンラインサービスの機器は、窃盗、火気、爆発、煙、水、ほこり、振動、地震、有害物質、電氣的干渉、停電、電氣的な乱れ（電圧の急上昇）、放射線などの環境的なリスクから保護される場所に配置します。	適合可能	ISO 27001の管理策「外部からの脅威と環境面での脅威に対するセキュリティ」並びに「機器の設置と保護」で求められている要件を考慮すると、コンピュータセンターの立地に関しては十分考慮されていると考えられる。 また、インタビューの結果、立地に起因する各種災害（窃盗、火災、爆発、煙、水、ちり、振動、地震、有害な化学物質、電気干渉、停電、電気障害、放射線など）に対する考慮がなされていることが確認できた。	—	ISO 27001:2013 A.11.1.4, A.11.2.1	立地に起因する各種災害（窃盗、火災、爆発、煙、水、ちり、振動、地震、有害な化学物質、電気干渉、停電、電気障害、放射線など）を考慮している	—
設2	物理的な保護に関連するポリシーと手順は年1回見直しが行われます。	適合可能	文献[01]に、Azureは地理的に分散されたる配置の施設で稼動しており、各施設は24時間365日の稼動を行うために電源傷害や物理的進入、ネットワーク故障への対策が行われている旨が明示されている。 ISO 27001の管理策「事業継続性とリスクの評価」、「リスクの評価」並びに「リスクへの対応」で求められている要件を考慮すると、コンピュータセンターの立地に関するリスク評価のPDCAサイクルが確立していると考えられる。	文献[01] P13 BCR-05: Business Continuity Management & Operational Resilience – Environmental Risks	ISO 27001:2013 A.11.1.5	—	—
設3	データセンターの建物と区画は、環境的な脅威からの保護が十分に行えるように、十分な強度の確保、防火・耐火、防水、緊急避難路など、建築や消防などの関連する法規制に適合するよう設計・建築されています。	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、火災時の消化活動、避難を容易にするための十分な幅員の通路を確保していると考えられる。	—	—	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	—
設4	設3に同じ	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、隣接する建物との間隔は十分確保できていると考えられる。	—	—	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	—
設5	設3に同じ	適合可能	文献[01]に、データセンター施設のエントランスは24時間365日の監視が行われ、施錠管理、バッジによる個人別入館許可が行われていることが明示されている。 インタビュー等により、建物への不法侵入や破壊行為を防止する為の措置（アクセス管理、警報、監視カメラ、24時間の警備員常駐）が行われていることが確認できた。	文献[01] P30 DCS-07: Datacenter Security – Secure Area Authorization	—	建物への不法侵入や破壊行為を防止する為の措置（アクセス管理、警報、監視カメラ、24時間の警備員常駐）を行っている。	—
設6	看板等は外部には掲示していません	適合可能	文献[01]に、データセンター施設の入館は業務上の必要がある場合に限られ、事前の認可申請を行い、バッジの発行を受ける必要があることが明示されている。 FedRAMP System Security Planにおいて、建物への接近を認める前に個人別の認証を行っていることについての記載を確認した。	文献[01] P30 DCS-08: Datacenter Security – Unauthorized Persons Entry	FedRAMP System Security Plan PE-03(a)	—	—
設7	避雷針を設けています	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、避雷設備も設置されていると考えられる。	—	—	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	—
設8	独立区画としています	適合可能	文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。	文献[01] P30 DCS-08: Datacenter Security – Unauthorized Persons Entry P30 DCS-09: Datacenter Security – User Access	—	—	—

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設9	回線・電力線の地下埋設、独立した区画への配線など、防止措置を施しています	適合可能	ISO 27001の管理策「配線のセキュリティ」で求められている要件を考慮すると、敷地内の通信回線及び電力線の配線に関しては十分考慮されていると考えられる。 FedRAMP System Security Planにおいて、電気配線は環境リスクを排除できる場所に敷設することについて記載されていることを確認した。 インタビューの結果、日本国内では外部ケーブル配管は基本的に地中埋設とし、建物構内は第三者がアクセスできないよう施錠により隔離された区画内（MDF室、IDF室等）に配線されるよう設計されており、配線に関しては十分考慮されていると考えられる。	－	ISO 27001:2013 A.11.2.3 FedRAMP System Security Plan PE-09	外部ケーブル配管は基本的に地中埋設とし、建物構内は、第三者がアクセスできないよう施錠により隔離された区画内（MDF室、IDF室等）に配線されるよう設計されている。	－
設10	設3に同じ	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認しており、耐火建築物であると考えられる。	－	－	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	－
設11	設3に同じ	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認しており、免震構造、空調、消火設備を備えているため、構造の安全性を有していると考えられる。	－	－	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。 日本国内のデータセンタにおいては、免震構造、空調、消火設備を有している。	－
設12	設3に同じ	適合可能	FedRAMP System Security Planにおいて、漏水対策及び浸水の検知について記載されていることを確認した。 インタビューの結果、日本国内では壁面、屋根部には漏水の防止措置が講じられていると考えられる。	－	FedRAMP System Security Plan PE-15	壁面にはフッ素樹脂等での塗装を施し、屋根部はアスファルト等の防水層の上に高性能断熱材を施し防水措置をしている。	－
設13	設3に同じ	適合可能	インタビューの結果、日本国内では外壁には強度のあるPCコンクリート等で施工されていることを確認しており、破壊行為等への対策が講じられていると考えられる。	－	－	外壁には強度のあるPCコンクリート等で施工されている。	－
設14	設3に同じ	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認しており、延焼を防止するための措置が講じられていると考えられる。	－	－	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	－
設15	設3に同じ	適合可能	ISO 27001の管理策「物理セキュリティの境界」で求められている要件を考慮すると、情報処理施設のある領域を物理セキュリティ境界により保護することに関しては十分考慮されていると考えられる。 インタビューの結果、日本国内では外部に面したガラス部分には容易な破壊を防止する強度のものを採用し、あわせて侵入センサー、もしくは監視カメラ等を設置していることを確認した。また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階窓部分への接近を防止、もしくは検知する仕組みを採用していることを確認した。これらの対策により、必要な防犯措置が講じられていると考えられる。	－	ISO 27001:2013 A.11.1.1	外部に面したガラス部分には、容易な破壊を防止する強度ものの採用し、あわせて侵入センサー、もしくは監視カメラ等を設置している。 また、敷地部分にも侵入センサー、もしくは監視カメラを設置し、低層階窓部分への接近を防止、もしくは検知する仕組みを採用している。	－
設16	出入口で施設への入出を管理し、物理的アクセスの承認を実施します。データセンターへの主なアクセスは、セキュリティスタッフが 24 時間 365 日常駐している単一の入口を必ず通るようにします。	適合可能	文献[01]に、データセンター施設のエントランスは24時間365日の監視が行われ、施錠管理、バッジによる個人別入館許可が行われていることが明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。 ISO 27001の管理策「受渡場所」「物理的入退管理」で求められている要件を考慮すると、物品の搬出入を含めた入退管理に関しては十分考慮されていると考えられる。	文献[01] P30 DCS-07: Datacenter Security – Secure Area Authorization P30 DCS-09: Datacenter Security – User Access	ISO 27001:2013 A.11.1.6, A.11.1.2	－	－
設17	非常口には警報装置を設置し、ビデオ監視を実施します。	適合可能	ISO 27001の管理策「受渡場所」で求められている要件を考慮すると、認可されていない者が立ち入る可能性のある場所の隔離に関しては十分考慮されていると考えられる。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、適切な位置に非常口が設けられていると考えられる。	－	ISO 27001:2013 A.11.1.6	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	－
設18	設3に同じ	適合可能	FedRAMP System Security Planにおいて、漏水対策及び浸水の検知について記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、適切な防水措置が講じられていると考えられる。	－	FedRAMP System Security Plan PE-15	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。	－
設19	設3に同じ	適合可能	インタビューの結果、日本国内では出入口扉は十分な強度を有した建具とし、施錠付きとしていることから、防犯・防災対策が施されていると考えられる。	－	－	出入口扉は十分な強度を有した建具とし、施錠付きとしている。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
設20	設3に同じ	適合可能	インタビューの結果、日本国内では建築基準法に規定する不燃材料及び消防法に規定する防災性能を有するものを使用しており、内装等の防災対策が講じられていると考えられる。	－	－	建築基準法に規定する不燃材料及び消防法に規定する防災性能を有するものを使用している。	－
設21	設3に同じ	適合可能	インタビューの結果、日本国内では間仕切壁、天井、照明器具等の地震による落下・損壊防止措置を実施しており、必要な防止措置が講じられていると考えられる。	－	－	間仕切壁、天井、照明器具等の地震による落下・損壊防止措置を実施している。	－
設22	設3に同じ	適合可能	インタビューの結果、立地起因する各種災害（窃盗、火災、爆発、煙、水、ちり、振動、地震、有害な化学物質、電気干渉、停電、電気障害、放射線など）に対する考慮がなされていることが確認できた。 特に、日本国内では上位階に設置するなどの措置が講じられていることを確認したため、浸水などの影響を受けにくいと考えられる。	－	－	日本国内では、浸水などの影響の受けにくい上位階に設置するなどの措置を講じている。	－
設23	マイクロソフト オンラインサービスの設備は、外部やエレベータなどから直接入れるような区画には設置されていません。	適合可能	インタビューの結果、日本国内では出入口付近及びエレベーターまたは階段より直接入れないように設置されていることを確認したため、侵入や破壊、機密情報漏洩等の防止措置がとられていると考えられる。	－	－	日本国内では、出入口付近及びエレベーターまたは階段より直接入れないよう設置されている。	－
設24	マイクロソフトのデータセンタでは、場所や部屋の目的を外部の第三者に表示していません	適合可能	インタビューの結果、マイクロソフトのデータセンターでは、場所や部屋の目的を外部の第三者に表示していないことが確認された。	－	－	マイクロソフトのデータセンターでは、場所や部屋の目的を外部の第三者に表示していない。	－
設25	適切な区間を確保して配置しています	適合可能	インタビューの結果、必要な空間が確保されていることを確認した。	－	－	保守、避難のために必要な空間の確保を行っている。	－
設26	コンピュータ室は専用の区画としています	適合可能	文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。	文献[01] P30 DCS-08: Datacenter Security – Unauthorized Persons Entry P30 DCS-09: Datacenter Security – User Access	－	－	－
設27	受付エリアと施設内部を隔てるドアに電子的なアクセス制御装置を設置し、承認された担当者だけが通行できるよう制限します。データセンター内の随所のドアで物理的な立ち入り管理により承認された担当者と訪問者だけが物理的にアクセスできるよう制限します。	適合可能	ISO 27001の管理策「受渡場所」で求められている要件を考慮すると、認可されていない者が立ち入る可能性のある場所の隔離に関しては十分考慮されていると考えられる。 FedRAMP System Security Planにおいて、施設入退管理、入退室の監視と検証について記載されていることを確認した。 インタビューの結果、日本国内では常時利用する出入口は1箇所であり、前室も設けていることを確認しており、入退室管理が適切に行われていると考えられる。	－	ISO 27001:2013 A.11.1.6, FedRAMP System Security Plan PE-03, PE-06	日本国内では、常時利用する出入口は1箇所であり、前室も設けている。	－
設28	設3に同じ	適合可能	インタビューの結果、日本国内ではコンピュータ室やデータ保管室等への出入は万全のセキュリティを確保しているため、不法侵入や危険物の投込みの可能性が十分に低減されており、扉の物理的な強化を超えた防犯・防災対策が行われてる。また扉も鍵施錠の上、非常時に備えて内側より緊急解錠が可能となっている。これらより、十分な防犯・防災対策が取られていると考えられる。	－	－	当該ルームへの出入は万全のセキュリティを確保しているため不法侵入、危険物の投込みの危険性はない。扉は鍵施錠だが、非常時に備え、内側より緊急解錠が可能となっている。	－
設29	設3に同じ	適合可能	インタビューの結果、日本国内ではコンピュータ室には窓を設けていないことから、窓に起因するリスクは存在しないと考えられる。	－	－	コンピュータ室には窓を設けていない。	－
設30	設3に同じ	適合可能	FedRAMP System Security Planにおいて、非常灯の設置について記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、適切な位置に非常口及び避難器具が設置されていると考えられる。 具体的には、2方向避難を基本とし2ヶ所以上の非常口を設置している。また、消防法をクリアした避難器具の設置、マシン室、廊下、非常口等への誘導標識の設置を行っている。	－	FedRAMP System Security Plan PE-12	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。ルームの大きさによるが、基本的には2方向避難のため、2ヶ所以上非常口を設置している。 消防法をクリアした避難器具を配備している。 誘導標識をマシン室、廊下、非常口等に設けている。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者が必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設31	設3に同じ	適合可能	文献[01]に、データセンターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 SOC2レポートにおいて、温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理について記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認した。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	SOC2 レポート PE-7	日本国内では建築基準法に準じたデータセンターを利用している。	－
設32	設3に同じ	適合可能	FedRAMP System Security Planにおいて、漏水対策及び浸水の検知について記載されていることを確認した。 インタビューの結果、日本国内では室内に水使用設備がなく、空調室には床防水塗装、防水堤、排水口、漏水センサー等が必要に応じて設置されていることから、漏水防止対策が講じられていると考えられる。	－	FedRAMP System Security Plan PE-15	室内に水使用設備はない。空調方式による違いはあるが、空調室には床防水塗装、防水堤、排水口、漏水センサー等を設置している。	－
設33	設3に同じ	適合可能	FedRAMP System Security Planにおいて、温度及び湿度の計測と維持について記載されていることを確認した。 インタビューの結果、日本国内では空調による湿度管理を実施しており、あわせて収容ラック個々でのアース敷設を基本としていることから、静電気防止措置が講じられていると考えられる。	－	FedRAMP System Security Plan PE-14	空調による湿度管理を実施している。 あわせて、収容ラック個々でのアース敷設を基本としている。	－
設34	設3に同じ	適合可能	インタビューの結果、日本国内では内装等是不燃材及び防災性能を有するものを使用しており、防災対策が施されていると考えられる。	－	－	内装等是不燃材及び防災性能を有するものを使用している。	－
設35	設3に同じ	適合可能	インタビューの結果、日本国内では間仕切壁、天井、照明器具等の地震による落下・損壊防止措置を実施しており、必要な防止措置が講じられていると考えられる。	－	－	間仕切壁、天井、照明器具等の地震による落下・損壊防止措置を実施している。	－
設36	設3に同じ	適合可能	インタビューの結果、日本国内ではフリーアクセス床に地震時に損壊することのない耐震措置を実施しており、必要な措置が行われていると考えられる。	－	－	地震時に損壊することのない耐震措置を実施している。	－
設37	早期火災報知設備(高感度煙検知器)を設置しています	適合可能	文献[01]に、データセンターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 SOC2レポートにおいて、温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理について記載されていることを確認した。 FedRAMP System Security Planにおいて、火災の検知と消化のための装置の敷設について記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、適切な自動火災報知装置が設置されていると考えられる。具体的には、早期火災報知設備（高感度煙感知器）が設置されている。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	SOC2 レポート PE-7 FedRAMP System Security Plan PE-13	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。早期火災報知設備を具備している。（高感度煙感知器）	－
設38	非常時の連絡装置を設置しています	適合可能	インタビューの結果、非常時の連絡装置が設置されていることを確認した。	－	－	非常時の連絡装置を設置している。	－
設39	ガス式の消火装置を設置しています	適合可能	文献[01]に、データセンターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 SOC2レポートにおいて、温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理について記載されていることを確認した。 FedRAMP System Security Planにおいて、火災の検知と消化のための装置の敷設について記載されていることを確認した。 またインタビューの結果、日本国内では消防法に準じたデータセンターを利用しており、また窒素ガス消火装置、スプリンクラー、煙探知装置が設置されていることから、適切な消火設備が設置されていると考えられる。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	SOC2 レポート PE-7 FedRAMP System Security Plan PE-13	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。 日本国内では、窒素ガス消火設備、スプリンクラー、煙探知装置が設置されている。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設40	設3に同じ	適合可能	FedRAMP System Security Planにおいて、ケーブルは環境リスクを排除できる場所に保護されることについて記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、ケーブル貫通部分の延焼防止措置が講じられていると考えられる。 具体的には、難燃ケーブルを使用し、貫通部には防火パテ等の不燃材料による延焼防止措置をしている。また、ケーブルが防火区画を貫通する場合は、認定を受けている防火措置工法により防火性能を確保している。	－	FedRAMP System Security Plan PE-09	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。 難燃ケーブルを使用し、貫通部には防火パテ等の不燃材料による延焼防止措置をしている。ケーブルが防火区画を貫通する場合は、認定を受けている防火措置工法により防火性能を確保している。	－
設41	設3に同じ	適合可能	FedRAMP System Security Planにおいて、火災の検知と消化のための対策において、煙を考慮した記載がなされていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用しており、必要な排煙設備が設置されていると考えられる。	－	FedRAMP System Security Plan PE-13	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。 消防法等、法規に準拠した排煙設備が設置されている。	－
設42	設3に同じ	適合可能	FedRAMP System Security Planにおいて、非常灯の非常電源対応について記載されていることを確認した。 インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認しており、コンピュータ室には非常用照明設備及び携帯用照明器具が設置されていると考えられる。	－	FedRAMP System Security Plan PE-12	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。 非常用照明設備を具備している。	－
設43	水使用設備は設置していません	適合可能	FedRAMP System Security Planにおいて、漏水対策及び浸水の検知について記載されていることを確認した。 インタビューの結果、日本国内では水使用設備はコンピュータ室、データ保管室に設置されていないことを確認した。	－	FedRAMP System Security Plan PE-15	日本国内では、水使用設備はコンピュータ室、データ保管室に設置されていない。	－
設44	マイクロソフトのデータセンターは必要とされる地震対策が施された建物となっていることや、オンラインサービスの特性から震度による運転の停止などを行うことが適切ではないことから、地震感知器は設置していませんが、オンラインサービスは遠隔地からの操作による停止や別地域への稼働切り替えが可能なことから、本件によるシステムリスクはありません。 お客様は、地震の被害によるシステム停止だけでなく、電源や空調、ハードウェア、ソフトウェア、ネットワークなどの障害によるシステム停止に対応するために、必要な冗長化構成、高可用性設計を行う必要があります。	適合可能	インタビューの結果、サービス特性から震度に応じた運転停止判断は行わないこととしていることを確認した。 本項目で想定しているデータの破損、電気火災等の二次災害のリスクに関しては以下の代替管理策を鑑みてリスクを受容可能な水準で対策しているものと考えられる。 ・データの破損は、文献[13]並びにSOC2レポートに障害時の縮退・再構成機能に関する記載がある ・電気火災等の二次災害は、インタビューにおいて耐震措置を講じていることを確認し、更にFedRAMP System Security Planにおいては火災の検知と消化のための対策が記載されている	文献[13]キャパシティと耐久性に常に制御できる状態に	SOC2レポートDS-6, DS-7 FedRAMP System Security Plan PE-13	マイクロソフトのデータセンターは必要とされる地震対策が施された建物となっていることや、オンラインサービスの特性から震度による運転の停止などを行うことが適切ではないことから、地震感知器は設置していないが、オンラインサービスは遠隔地からの操作による停止や別地域への稼働切り替えが可能である。	代替管理策の受入可否を判断する
設45	コンピュータ室の出入口には入退室者を識別する装置を設置し、また、施設へのアクセスにはセキュリティスタッフが24時間常駐する単一の入口を通過するようにしています	適合可能	文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。 FedRAMP System Security Planにおいて、施設入退管理、入退室の監視と検証について記載されていることを確認した。 またインタビューの結果、日本国内では入退室者を識別・記録する出入管理設備が設置されており、入館には事前申請と顔写真入りの身分証明書が必要であることを確認しており、不法侵入を防止する措置が講じられていると考えられる。	文献[01]P30 DCS-07: Datacenter Security – Secure Area Authorization P30 DCS-09: Datacenter Security – User Access	FedRAMP System Security Plan PE-03, PE-06	日本国内では、入退室者を識別・記録する出入管理設備が設置されており、入館には事前申請と顔写真入りの身分証明書が必要である。	－
設46	設1に同じ	適合可能	文献[01]に、データセンターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 FedRAMP System Security Planにおいて、温度及び湿度の計測と維持について記載されていることを確認した。 またインタビューの結果、日本国内では中央監視設備にて温湿度監視を実施し、異常時には警報を転送していることを確認しており、必要な対策が施されていると考えられる。	文献[01]P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	FedRAMP System Security Plan PE-14	中央監視設備にて温湿度監視を実施し、異常時には警報を転送する。	－
設47	ケーブルを吊り下げ式で配線し、必要に応じて金属管による保護などにより対策しています。また、建物の構造によって小動物が移動できる通路等を制限しています	適合可能	インタビューの結果、日本国内では建物の構造でネズミ等が通れる通路等を制限しており、また餌となる食料品等を放置していないことから、ネズミ対策が施されていると考えられる。	－	－	建物の構造で、ネズミ等が通れる通路等を制限している。また、餌となる食料品等は放置していない。	－
設48	コンピュータ室に什器は配置していません	適合可能	インタビューの結果、コンピュータ室に什器は配置されていないことを確認した。	－	－	コンピュータ室に什器は配置していない。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者に必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設49	コンピュータ室のコンピュータ機器はアースするなど静電気防止措置を講じています	適合可能	インタビューの結果、日本国内ではコンピュータ室にアースを設置するとともに、静電気防止のためのタイル床などを使用していることから、静電気防止措置が講じられていると考えられる。	－	－	日本国内では、コンピュータ室ではアースを設置するとともに、静電気防止のためのタイル床などを使用している。コンピュータ室内に什器・備品を常設していない。	－
設50	設3に同じ	適合可能	インタビューの結果、日本国内では建物自体が免震構造であり、ラックへの耐震措置も講じられていることから、コンピュータ機器や什器に対する耐震措置が講じられていると考えられる。また、可搬型の機器等については、盗難や振動による故障に備えて固定されていることを確認した。	－	－	日本国内では、建物自体が免震構造であり、ラックへの耐震措置も講じられている。	－
設51	運搬車等の使用はありません	適合可能	インタビューの結果、運搬車等の使用がないことを確認した。	－	－	運搬車等は使用していない。	－
設52	電源・空調室は、地震や火災、水害等による被害から保護されるよう設計され、十分な強度を持つ独立した区画としています。	適合可能	インタビューの結果、立地起因する各種災害（窃盗、火災、爆発、煙、水、ちり、振動、地震、有害な化学物質、電気干渉、停電、電気障害、放射線など）に対する考慮がなされていることが確認できた。また、日本国内の電源室・空調室は、外部から2重又は3重の壁に囲まれた建物内部に設置されていることも確認した。これらの結果から外部の影響を受けにくい位置にあり、災害の影響を受ける恐れは十分低減されていると考えられる。	－	－	電源室・空調室は、外部から2重又は3重の壁に囲まれた建物内部に設置されており、外部の影響を受けにくい位置にある。	－
設53	設52に同じ	適合可能	インタビューの結果、日本国内では建築基準法に準じたデータセンターを利用していることを確認しており、電源室・空調室は保守点検に十分な広さと高さを有していると考えられる。	－	－	日本国内では、建築基準法及び消防法に準じたデータセンターを利用している。消防法を満たしている十分な広さと高さを有している。	－
設54	設52に同じ	適合可能	インタビューの結果、日本国内では電源室・空調機械室は独立・専用化していることを確認しており、保守管理及び障害の拡大防止の措置が講じられていると考えられる。	－	－	電源室、空調室は、独立・専用化している。	－
設55	設52に同じ	適合可能	インタビューの結果、日本国内では電源室・空調機械室に窓はなく扉錠を設置していることを確認しており、外部からの侵入防止、防火、防水対策が講じられていると考えられる。	－	－	電源室内に窓はなく、扉錠を設置している。	－
設56	設52に同じ	適合可能	インタビューの結果、日本国内では電源室・空調機械室は耐火構造で延焼防止措置を実施していることを確認しており、火災による延焼防止対策が講じられていると考えられる。	－	－	耐火構造であり、延焼防止措置を実施している。	－
設57	設52に同じ	適合可能	文献[01]に、データセンターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 FedRAMP System Security Planにおいて、火災の検知と消化のための装置の敷設について記載されていることを確認した。 またインタビューの結果、日本国内では早期火災報知設備（煙感知器）が設置されていることを確認しており、早期の火災を発見するための対策が施されていると考えられる。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	FedRAMP System Security Plan PE-13	早期火災報知設備を具備している。（煙感知器）	－
設58	設52に同じ	適合可能	FedRAMP System Security Planにおいて、火災の検知と消化のための装置の敷設について記載されていることを確認した。 インタビューの結果、日本国内ではガス消火方式を採用してことを確認しており、火災時の対策が施されていると考えられる。	－	FedRAMP System Security Plan PE-13	ガス消火方式を採用している。	－
設59	設52に同じ	適合可能	インタビューの結果、日本国内では空調機械室には床防水塗装、防水堤、排水口、漏水センサー等が必要に応じて設置されていることを確認しており、漏水防止対策が講じられていると考えられる。	－	－	空調方式による違いはあるが、床防水塗装、防水堤、排水口、漏水センサー等を設置している。	－
設60	設52に同じ	適合可能	インタビューの結果、日本国内では電源室・空調機械室について、防火区画を形成する壁面のケーブル・ダクト貫通部及びこれと近接する部分には防火措置が施されていることを確認しており、延焼防止措置が講じられていると考えられる。	－	－	防火区画を形成する壁面のケーブル、ダクト貫通部及びこれと近接する部分には延焼防止措置を構じている。	－
設61	設52に同じ	適合可能	インタビューの結果、電源・空調室は、地震や火災、水害等による被害から保護されるよう設計され、十分な強度を持つ独立した区画とされていることを確認した。	－	－	電源・空調室は、地震や火災、水害等による被害から保護されるよう設計され、十分な強度を持つ独立した区画としている。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設62	複数の異経路での電源引き込み、自家発電機とUPS装置の利用などにより電源供給の確保を行っています。発電機とUPS装置は提供ベンダーの推奨の時期、方法で定期的な保守が行われています。また、自家発電機の燃料供給について優先契約を締結しています。電源の安定化と保護のため、避雷針など落雷対策、分電設備の専用化、アース設置、過電流対策を実施しています	適合可能	インタビューの結果、複数の異経路での電源引き込み、自家発電機とUPS装置の利用などにより電源供給の確保を行っており、発電機とUPS装置は提供ベンダーの推奨の時期、方法で定期的な保守が行われているほか、自家発電機の燃料供給について優先契約を締結していることや、電源の安定化と保護のため、避雷針など落雷対策、分電設備の専用化、アース設置、過電流対策を実施していることを確認した。	－	－	複数の異経路での電源引き込み、自家発電機とUPS装置の利用などにより電源供給の確保を行ってる。発電機とUPS装置は提供ベンダーの推奨の時期、方法で定期的な保守が行われている。また、自家発電機の燃料供給について優先契約を締結し、電源の安定化と保護のため、避雷針など落雷対策、分電設備の専用化、アース設置、過電流対策を実施している。	－
設63	設62に同じ	適合可能	文献[01]に、「データセンターには、専用の 24 時間365日無休で稼働する無停電電源装置（UPS）及び緊急電源サポート（発電機など）が装備されている」旨が明示されている。	文献[01] P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	－	－
設64	設62に同じ	適合可能	文献[01]に、「データセンターには、専用の 24 時間365日無休で稼働する無停電電源装置（UPS）及び緊急電源サポート（発電機など）が装備されている」旨が明示されている。	文献[01] P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	－	－
設65	設62に同じ	適合可能	インタビューの結果、日本国内では建物に応じた方式の避雷設備を設置していることを確認しており、落雷対策が施されていると考えられる。	－	－	建物により方式に違いはあるが、避雷設備を設置している。	－
設66	設52に同じ	適合可能	インタビューの結果、日本国内では電源装備、蓄電池装備ともに耐震措置が講じられていることを確認しており、地震による移動、損傷等を防止する対策が施されていると考えられる。	－	－	電源設備、蓄電池設備とも、耐震措置を講じている。	－
設67	設62に同じ	適合可能	インタビューの結果、日本国内ではコンピュータ室に設置する分電盤及び配線は専用回路としていることを確認しており、コンピュータシステムへの影響は最小限とする対策が施されていると考えられる。	－	－	コンピュータ室に設置する分電盤及び配線は専用回路としている。	－
設68	設62に同じ	適合可能	インタビューの結果、日本国内ではエレベーターと空調設備は別系統の電源を用いていることを確認しており、それらの負荷変動がコンピュータシステムに影響しない対策が施されていると考えられる。	－	－	エレベーター、空調設備とは別系統であり、負荷変動の影響を及ぼすことはない。	－
設69	設62に同じ	適合可能	インタビューの結果、日本国内ではコンピュータシステムの接地は統合接地方式で行われていることを確認しており、適切に施工されていると考えられる。	－	－	新接地方式（統合接地方式）で接地を基本としている。	－
設70	設62に同じ	適合可能	インタビューの結果、日本国内では各機器個別でブレーカ設置を基本とし、特にコンピュータシステム向けの電源配線はすべて個別ブレーカからの配線を基本としてアース線を設置しており、過電流や漏電への措置が施されていると考えられる。	－	－	各機器個別でのブレーカ設置を基本としている。特にコンピュータシステム向けの電源配線は、すべて個別ブレーカからの配線を基本とし、アース線を設置している。	－
設71	設62に同じ	適合可能	文献[01]に、「データセンターには、専用の 24 時間365日無休で稼働する無停電電源装置（UPS）及び緊急電源サポート（発電機など）が装備」されており、「データセンターでは、緊急時の燃料供給のための調整が行われている」旨が明示されている。 またインタビューの結果、日本国内では建築基準法及び消防法に準拠した防災、防犯設備用予備電源を設置し、セキュリティ機器については無停電電源装置に接続された電源による給電を基本としていることを確認しており、停電時の対策が施されていると考えられる。	文献[01] P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	「建築基準法施工令第126条の3、5、7等」、「消防法」に準拠した防災、防犯設備用予備電源を設置している。 セキュリティ機器については、A電源での給電を基本としている。	－
設72	コンピュータシステムと低エネルギー消費の両立のため、専用の空調設備(HVAC)をN+1構成とし、温度・湿度を継続的に監視し、適切な範囲となるよう制御しています。	適合可能	インタビューの結果、日本国内では空調設備を、全利用時の発熱見合いに対してn+1台以上の構成で設計されており、空調設備の能力に余裕があると考えられる。	－	－	全利用時の発熱見合いに対して、n+1台構成以上での設置を基本としている。	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					
項番	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	SI事業者・利用者に必要な対応
設73	設73に同じ	適合可能	文献[01]に、データ センターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location	－	－	－
設74	設73に同じ	適合可能	インタビューの結果、日本国内ではコンピュータ室専用の空調設備を設置しており、的確な温湿度制御が可能であると考えられる。	－	－	コンピュータ室専用の空調を設置している。	－
設75	設73に同じ	適合可能	インタビューの結果、日本国内では空調設備を、全利用時の発熱見合いに対してn+1台以上の構成で設計されており、空調設備の予備が設置されていると考えられる。	－	－	全利用時の発熱見合いに対して、n+1台構成以上での設置を基本としている。	－
設76	設73に同じ	適合可能	文献[01]に、データ センターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 同じく文献[01]に、データセンター内の電源管理システムや設備等を監視するための施設運用センターが存在する旨が明示されている。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	－	－
設77	設52に同じ	適合可能	インタビューの結果、日本国内では空調設備は専用室に設置され、第三者の専用室への入室が困難であることから、侵入、破壊に対する防止対策が講じられていると考えられる。	－	－	空調設備は専用室に設置されており、第三者の専用室への入室は不可能である。	－
設78	設52に同じ	適合可能	インタビューの結果、日本国内では空調設備の耐震措置を講じており、地震による移動、損傷等の防止対策は施されていると考えられる。	－	－	空調設備の耐震措置を講じている。 建築基準法施行令第39条の2に準拠（SALレベルでの対応）を基本としている。	－
設79	設52に同じ	適合可能	インタビューの結果、日本国内では空調設備の断熱材料及び吸排気口はすべて不燃材料を使用しており、火災時の損傷防止対策は講じられていると考えられる。	－	－	空調設備の断熱材料及び吸排気口は全て不燃材料を使用している。	－
設80	データセンターの設備監視室では、電源設備、空調設備、防災設備、防犯設備を24時間体制で集中して監視しています	適合可能	文献[01]に、データ センターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 同じく文献[01]に、データセンター内の電源管理システムや設備等を監視するための施設運用センターが存在する旨が明示されている。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	－	－
設81	設81に同じ	適合可能	文献[01]に、データ センターを保護するために温度管理／冷暖房、換気、及び空調（HVAC）／火災検知及び抑制システム／電力管理システムを含む環境の管理を実施している旨が明記されている。 同じく文献[01]に、データセンター内の電源管理システムや設備等を監視するための施設運用センターが存在する旨が明示されている。	文献[01] P14 BCR-06: Business Continuity Management & Operational Resilience – Equipment Location P15 BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures	－	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設82	回線関連設備はコンピュータ室に設置し、入退室を厳しく制限・管理しています	適合可能	文献[01]に、データセンター内はセキュリティエリアの異なる区画はドアによって隔てられており、バッジによる入退室許可、入退室ログの取得、カメラによる監視が行われている旨が明示されている。 同じく文献[01]に、データセンター内設備・機器への物理アクセスにはIDカードもしくは生体データによる認証が必要である旨が明示されている。	文献[01] P30 DCS-07: Datacenter Security – Secure Area Authorization P30 DCS-09: Datacenter Security – User Access	－	－	－
設83	設24に同じ	適合可能	インタビューの結果、Microsoftのデータセンターでは、場所や部屋の目的を外部の第三者に表示していないことを確認した。	－	－	データセンターの場所や部屋の目的を外部の第三者に表示していない。	－
設83-1	回線と電源の分離を行い、金属ケース等による保護を実施しています	適合可能	インタビューの結果、回線と電源の分離を行い、金属ケース等による保護を実施していることを確認した。	－	－	回線と電源の分離を行い、金属ケース等による保護を実施している。	－
設84	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設85	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設86	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設87	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設88	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設89	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設90	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設91	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設92	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設93	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設94	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設95	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設96	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設97	データセンタ以外に対する要件のため	対象外	－	－	－	－	－

FISC安全対策基準（第9版）の項目	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	Office 365 における対応				SI事業者・利用者で必要な対応
項番			本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
設98	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設99	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設100	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設101	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設102	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設103	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設104	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設105	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設106	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設107	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設108	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設109	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設110	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設111	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設112	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設113	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設114	データセンタ以外に対する要件のため	対象外	－	－	－	－	－

FISC安全対策基準（第9版）の項目	FISC安全対策基準（第9版） に対するMicrosoftの見解	FISC安全対策基準への 適合性	Office 365 における対応				SI事業者・利用者に必要な対応
項番			本調査で確認した内容	確認した公開文書	第三者認証等から 確認した内容	Microsoftへのインタ ビューで確認した内容	
設115	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設116	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設117	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設118	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設119	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設120	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設121	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設122	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設123	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設124	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設125	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設126	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設127	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設128	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設129	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設130	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設131	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設132	データセンタ以外に対する要件のため	対象外	－	－	－	－	－
設133	データセンタ以外に対する要件のため	対象外	－	－	－	－	－

FISC安全対策基準（第9版）の項目		Office 365 における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
設134	データセンタ以外に対する要件のため	対象外	—	—	—	—	—
設135	データセンタ以外に対する要件のため	対象外	—	—	—	—	—
設136	データセンタ以外に対する要件のため	対象外	—	—	—	—	—
設137	データセンタ以外に対する要件のため	対象外	—	—	—	—	—
監1	<p>マイクロソフトはお客様に代わり、外部の第三者機関を選定して SOC1、SOC2、ISO 27001 監査を実施し、その結果を開示しています。</p> <p>お客様はこれらの監査結果レポートを確認したり、Audit WebCast に参加して弊社監査担当者から直接説明を受けたり質疑応答するなどにより、オンラインサービスのシステム監査の全部または一部を代替することが可能です。</p> <p>マイクロソフトは金融機関のお客様による監査・監督の権利を保障し、より詳細な質問や情報請求に対して、その分野を担当する専門家から回答を受けたり情報を入手したりする機会を用意することをお約束しています。この機会を活用することで事実確認を行ったり意見交換を行うことが可能です。マイクロソフトは多くの業界・地域のお客様に広くオンラインサービスを提供するために FISC 安全対策基準を含む多くの基準、規格に適合するように作られたマイクロソフト社内の基準と標準手順に従ってオンラインサービスを設計・運用しています。お客様による事実確認は、マイクロソフトが行うと約束している内容に照らして、マイクロソフトが正しく実施しているかどうかという観点で実施していただく必要があります。</p>	適合可能	文献[15]に、監査コンプライアンスとして「標準またはフレームワークにおいて監査の実施が規定されている場合、かかる制御標準またはフレームワークに関する監査は、少なくとも年 1 回実施されるものとします。」旨が記載されており、Service Trust Portalから監査レポートが実際に入手できることを確認した。 ※要ユーザー登録	文献[15] P11 監査コンプライアンス	—	—	利用者は、システム監査体制を整備する必要があり、必要に応じて監査レポートの確認、監査担当者への質疑応答等を行う。

FISC安全対策基準（第9版改訂）の項目		Microsoft Azure における対応					SI事業者・利用者で必要な対応
項番	FISC安全対策基準（第9版改訂）に対するMicrosoftの見解	FISC安全対策基準への適合性	本調査で確認した内容	確認した公開文書	第三者認証等から確認した内容	Microsoftへのインタビューで確認した内容	
統21	マイクロソフトのクラウド契約は金融機関のお客様が必要とする要件を盛り込んだ内容になっています。 詳細は「FISC安全対策基準 第9版 適合説明書（Compliance Companion for FISC guidelines v9）」をご参照ください。	適合可能	文献[14]に、外部委託先との契約時に考慮すべき事項として、FISC安全対策基準（第9版）に例示された以下16項目に対するマイクロソフト回答が記載されている。 (1)基本的な事項 (2)個別契約条件、サービス仕様、データ保護の管理策 (3)サービスレベル未達の場合の対応 (4)情報開示範囲、監督当局等による検査等への協力義務、金融機関による監査受入、事業者と利用者間の報告・連絡等の運営ルール、インシデントレスポンスの取扱い (5)反社会的勢力・テロ組織と関わりがないことの表明・確約 (6)契約の解除条件、契約終了時のデータの返却・消去等及び、契約終了時の原状回復・新システム移行時における協力義務 (7)損害が発生した場合の協議及び賠償に関する取決め (8)委託業務の成果の知的財産権、使用权等の権利の帰属 (9)外部委託先からの情報開示 (10)複数の外部委託先への委託 (11)再委託管理 (12)監査・モニタリング (13)インシデント発生時の立入調査 (14)記憶装置等の障害・交換 (15)国外におけるデータ保管時の留意点 (16)トレーサビリティの確保	文献[14] P6 統21	—	—	利用者は契約時に考慮すべき事項を盛り込み、契約締結手続きを行う必要がある。 また、サービス条件等について定期的に確認を行う必要がある。
実142	Office365はQR コード決済のサービスではありません。	対象外	—	—	—	—	—
実143	Office365はQR コード決済のサービスではありません。	対象外	—	—	—	—	—
実144	Office365はQR コード決済のサービスではありません。	対象外	—	—	—	—	—