金融機関向け『Microsoft Azure』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）
株式会社電通国際情報サービス（ISID）
SCSK株式会社（SCSK）
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）及び「Microsoft Azure における対応」欄の軽微な修正
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	FISC安全対策基準（第9版）に対するMicrosoftの見解	Microsoft Azure における対応					SI事業者・利用者で必要な対応
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	
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。

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	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。
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。

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	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	ー	ー	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、使用権等の権利の帰属 (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	ー	ー	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。
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	ー	ー	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	ー	ー	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」こと、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	ー	ー	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。

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	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	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。不正な開発行為や管理行為を阻止するために、スマートカードベースの2要素認証によるアクセス制御や、不正行為の自律的な検出によるコントロールの組み合わせ、運用担当者は職務が分離されており、アプリケーション、システム、ネットワークインフラストラクチャへのアクセスを制限しております。 利用者のMicrosoft Azure サブスクリプションへの認証として、ActiveDirectoryでの認証、クレームベースの認証、Microsoft IDでの認証等あるが、いずれの場合においてもパスワード非印字により、パスワードを知られない対策を講じています。利用者のMicrosoft Azureサブスクリプションへの認証については、強いパスワードのみが使用可能となっています。 利用者は、Microsoft Azure上で実装するアプリケーションの認証に関する対応を実施する必要があります。 ＜参考情報：マイクロソフトが実施している事＞ ・ホワイトペーパー「信頼できるクラウド:Microsoft Azure のセキュリティ、プライバシー、コンプライアンス」 http://download.microsoft.com/download/D/6/F/D6F3C9DB-A263-4B28-9855-B40243694E43/Microsoft%20Azure%20-%20SecurityPrivacyCompliance.pdf	適合可能	文献[02]に、Microsoft AzureへのアクセスにおけるID管理策として、多要素認証の利用、強力なパスワードポリシーの適用等の保護策について記載されている。 文献[07]に、Azure Active DirectoryによるID管理を行う場合に、「使用可能文字」「文字制限」の設定や「有効期限（無期限含む）」「アカウントロックアウト」等の変更を行うことが出来ることが明示されている。 文献[17]に、Microsoft Azureにおける多要素認証（MFA）の検証方法として、「パスワード」「ユーザーの所持品（電話など、容易には複製できない、信頼済みのデバイス）」「生体認証」が明示されている。 SOC2レポートにおいて、利用者がMicrosot Azureへアクセスする際のパスワードポリシー適用について記載されていることを確認した。	文献[02] ID 管理とアクセス管理 文献[07] Azure Active Directory のパスワード ポリシーと制限 文献[17] Multi-Factor Authentication とそのしくみについて	SOC2レポート LA-2	―	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。 利用者がAzure上で構築するアプリケーションやサービスで独自に用いるIDやパスワード等については、利用者が適切な対策を講じる必要がある。
実2	利用者は、ご要件合わせて、Microsoft Azure 上に実装するアプリケーションについての相手端末確認に関する対応を実施頂く必要があります。	対象外	―	―	―	―	利用者は公衆通信網を通じて自動着信端末に出力するアプリケーションを作成する場合は、相手先端末確認機能を設ける必要がある。
実3	利用者は、 Microsoft Azure 上に実装するアプリケーションのデータ保存時の暗号化に関して、対応を実施する必要があります。 なお、マイクロソフトは、利用者に暗号化について柔軟な選択肢を提供しております。 また、開発者向けに暗号化ライブラリを提供しており、こちらを利用することが可能です。	適合可能	文献[03]に、サーバー側暗号化方式として、「サービスが管理するキー」「ユーザーが管理するキー」「ユーザーが制御するハードウェア上でサービスが管理するキー」が選択可能であることが明示されている。 文献[08]には、利用者がMicrosoft Azure上でデータの暗号化を行うためのベストプラクティスが公開され、ファイルレベルのデータ暗号化に関する手法も記載されている。 文献[11]には、Microsoftのスタッフによる顧客データへのアクセスの禁止原則及び、利用者支援のために例外的にアクセスを行う場合の認可・認証手続及びアクセス履歴の記録の保持について明記されている。	文献[03] Azure の暗号化モデル 文献[08] ファイルレベルのデータ暗号化を適用する 文献[11] P13 マイクロソフトのスタッフによるアクセスの禁止	―	―	蓄積データの暗号化が必要な場合は、利用者のアプリケーションやサービスで実施する必要がある。 端末や周辺機器、アプリケーションが生成する一時データなどの管理は利用者の責任である。
実4	マイクロソフトは128 ビット以上の暗号化キーを使用する TLS により、Microsoft Azure データセンター間および対象のデータセンターのクラスター間で送信される制御メッセージを保護します。エンドユーザーとユーザーの仮想マシン間のトラフィックを暗号化する事も可能です。 Azure Portalなどの公開されている Azureサービス管理機能に接続するときには、HTTPSによる接続を行います。 利用者は、Microsoft Azure 上で実装するアプリケーションの通信に対して、データの保護に関する対応を実施する必要があります。	適合可能	文献[01]に、Azure Portalへのアクセスは TLS1.2により暗号化されていること、データセンター内通信及びデータセンター間通信がTLSにより暗号化されている旨が明示されている。 SOC2レポートにおいて、Microsoft Azureの内部通信、管理ポータルの通信の暗号化が記載されていることを確認した。	文献[01] P25 DSI-03: Data Security & Information Lifecycle Management – e-Commerce Transactions	SOC2レポート DS-2, DS-3	―	利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。

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	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5	利用者は、Microsoft Azure 上に実装するアプリケーションに関する対応を実施頂く必要があります。 利用者は、OSレベルの Firewall 設定や 3rd Party 製品の利用の他に、Microsoft Azure で提供している機能を利用することが可能です。 なお、マイクロソフトは Microsoft Azure へのアクセスコントロール、および認証で不正アクセスを制御しています。また外部からの不正アクセス等の対応として、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないように対策を実施しております。	適合可能	文献[04]に、利用者がネットワークセキュリティグループを使用してアクセス制御リスト（ACL)を作成可能であることが記載されている。また、Azure Platformに固有のセキュリティ層による保護についても明記されている。	文献[04] Azure 仮想ネットワークの概要	ー	ー	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	利用者は、Microsoft Azure 上に実装するアプリケーションについて、ご要件合わせて不良データの混入防止に関する対応を実施頂きます。 なお、マイクロソフトは Microsoft Azure への外部からの不正アクセス等の対応として、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないように対策を実施しております。 処理エラーのリスクを抑えるため、Microsoft Azure 環境内に内部処理制御が実装されています。内部処理制御は、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ます。内部処理制御の例としては、ハッシュトータルやチェックサムの使用などがあります（ただしこれらに限定されません）。	適合可能	文献[01]に、「Microsoft Azure では、許容可能な基準を定め、アプリケーションシステムに対するデータ入力が正確で想定範囲内に収まるようにしている」旨が明示されている。	文献[01] P7 AIS-03: Application & Interface Security - Data Integrity	ー	ー	利用者がAzure上で構築するアプリケーションやサービスにおける不良データ検出機能は、それらのアプリケーションやサービス上で利用者が対策を行う必要がある。
実7	マイクロソフトの管理業務は改ざん等の不正行為が起こらぬよう監査されています。監査証跡を参照して、変更の履歴を確認することができます。 またMicrosoft Azure内部コンポーネント間の全ての通信はTLSで保護され、改ざんを未然に防止しています。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。 利用者は、実装するアプリケーションの通信に必要な改ざん検知策に関する対応を実施する必要があります。	適合可能	文献[01]に、Azure Portalへのアクセスは TLS1.2により暗号化されていること、データセンター内通信及びデータセンター間通信がTLSにより暗号化されている旨が明示されている。 同じく文献[01]に、仮想マシンへ読み込みと書き込みはストレージ分析を介してログを取得しており、利用者のアカウントにおいて参照可能である旨が明示されている。 SOC2レポートにおいて、Microsoft Azureの内部通信の暗号化が記載されていることを確認した。	文献[01] P25 DSI-03: Data Security & Information Lifecycle Management - e-Commerce Transactions P57 IVS-02: Infrastructure & Virtualization Security - Change Detection	SOC2レポート DS-3	ー	利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者がSSL暗号化を用いるなどの対策を行う必要がある。
実8	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。不正な開発行為や管理行為を阻止するために、スマートカードベースの2要素認証によるアクセス制御や、不正行為の自律的な検出によるコントロールの組み合わせ、特定の運用担当者に関する経歴の確認基準に応じて、アプリケーション、システム、ネットワークインフラストラクチャへのアクセスを制限しております。 利用者は、Microsoft Azure 上に実装するアプリケーションについて、ご要件合わせてIDの不正使用防止機能に関する対応を実施します。	適合可能	文献[01]に、Microsoft Azureへのアクセスはアクセス管理ポリシーによって統制されていること、ポリシーは定期的に見直しと更新が行われることが明示されている。また、ポリシーは知る必要と最小権限の原則に基づき、業務上の役割に応じて決定されること、アクセス権の自動失効機能を有すること、Active Directryによるパスワードポリシーの実装などが示されている。 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、従業員等のアクセス認証に関して記載されていることを確認した。	文献[01] P46 IAM-02: Identity & Access Management - Credential Lifecycle / Provision Management P30 DCS-09: Datacenter Security - User Access	SOC2レポート OA-2	ー	利用者がAzure上で構築するアプリケーションやサービスで独自に用いる認証については、利用者が適切な本人確認機能を設ける必要がある。 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	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。不正な開発行為や管理行為を阻止するために、スマートカードベースの2要素認証によるアクセス制御や、不正行為の自律的な検出によるコントロールの組み合わせ、特定の運用担当者に関する経歴の確認基準に応じて、アプリケーション、システム、ネットワークインフラストラクチャへのアクセスを制限しております。 利用者は、Microsoft Azure 上に実装するアプリケーションについては、ご要件合わせてIDの不正使用防止機能に関する対応を実施頂きます。	適合可能	文献[01]に、Microsoft Azureへのアクセスはアクセス管理ポリシーによって統制されていること、ポリシーは定期的に見直しと更新が行われることが明示されている。また、ポリシーは知る必要と最小権限の原則に基づき、業務上の役割に応じて決定されること、アクセス権の自動失効機能を有すること、Active Directryによるパスワードポリシーの実装などが示されている。 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、管理者権限アクセスの統制と接続手段の管理について記載されていることを確認した。	文献[01] P46 IAM-02: Identity & Access Management - Credential Lifecycle / Provision Management P30 DCS-09: Datacenter Security - User Access	SOC2レポート OA-1, OA-9	ー	利用者がAzure上で構築するアプリケーションやサービスで独自に用いる認証については、利用者が適切な認証機構を用いる必要がある。

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	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10	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。不正な開発行為や管理行為を阻止するために、スマートカードベースの2要素認証によるアクセス制御や、不正行為の自律的な検出によるコントロールの組み合わせ、特定の運用担当者に関する経歴の確認基準に応じて、アプリケーション、システム、ネットワークインフラストラクチャへのアクセスを制限しております。 利用者は、Microsoft Azure 上に実装するアプリケーションについては、ご要件合わせてIDの不正使用防止機能に関する対応を実施する必要があります。 参考情報：MS 実施事項 ・ホワイトペーパー「信頼できるクラウド:Microsoft Azure のセキュリティ、プライバシー、コンプライアンス」 http://download.microsoft.com/download/D/6/F/D6F3C9DB-A263-4B28-9855-B40243694E43/Microsoft%20Azure%20-%20SecurityPrivacyCompliance.pdf	適合可能	文献[05]に、Azure Active Directoryレポートを利用することにより、Windows Azureへのアクセスについて、「発生の日付と時刻」「アクティビティの開始者またはアクター」「アクティビティ」「ターゲット」等のログを入手可能である旨が明示されている。 SOC2レポートにおいて、管理者権限アクセスのログ取得について記載されていることを確認した。	文献[05] 監査ログ	SOC2レポート VM-2	―	利用者は、自らが定めた監査ポリシーに従って記録されたログなどを、定期的に確認する必要がある。 利用者がAzure上で構築したアプリケーションやサービスのアクセス履歴については、利用者が適切にログの蓄積及び確認を行う必要がある。
実11	利用者は、ご要件に合わせて、Microsoft Azure上で実装するアプリケーションの取引内容の制限機能に関する対応を実施頂く必要があります。	対象外	―	―	―	―	取引制限機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実12	利用者は、ご要件に合わせて、Microsoft Azure上で実装するアプリケーションの事故時の取引禁止機能に関する対応を実施頂く必要があります。	対象外	―	―	―	―	取引禁止機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実13	マイクロソフトには、格納域内のデータおよび伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあります。 利用者は、暗号等で利用する鍵の不正使用防止に関する対応を実施する必要があります。	適合可能	文献[03]に、サーバー側暗号化方式として、「サービスが管理するキー」「ユーザーが管理するキー」「ユーザーが制御するハードウェア上でサービスが管理するキー」が選択可能であることが明示されている。 同じく文献[03]には、Key Vaultを用いた鍵の管理とアクセス制御が利用可能である旨が記載されている。 SOC2レポートにおいて、暗号鍵の安全な保管について記載されていることを確認した。	文献[03] Azure の暗号化モデル	SOC2レポート DS-1	―	端末側で使用する暗号鍵は、第三者に解読されたり漏洩することを、利用者が対策を講じる必要がある。 利用者がAzure上で構築したアプリケーションやサービスで独自に使用する暗号鍵の保護については、利用者が対策する必要がある。
実14	マイクロソフトは、外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようにしています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。 利用者は、実装するアプリケーションの通信に対してデータの保護対策に関する対応を実施する必要があります。 利用者側で、OSレベルでの Firewall 設定の他にアプリケーションのご要件に応じて対応を実施する必要があります。	適合可能	文献[01]に、ネットワーク境界の防護のため、ファイアウォール、ロードバランサー、IPフィルター等を用いた対策を採用している旨が明示されている。 文献[04]に、利用者がネットワークセキュリティグループを使用してアクセス制御リスト（ACL)を作成可能であることが記載されている。また、Azure Platformに固有のセキュリティ層による保護についても明記されている。 文献[06]に、クラウド基盤等への不正侵入を含む攻撃に対抗してインシデントレスポンスチームが設置されている旨、明示されている。 SOC2レポートにおいて、ネットワークフィルタリングによる不正侵入防止について記載されていることを確認した。	文献[01] P60 IVS-09: Infrastructure & Virtualization Security - Segmentation 文献[04] Azure 仮想ネットワークの概要 文献[06] P6 Azure Security Incident Response Process	SOC2レポート OA-16	―	ネットワークACLを用いて不正侵入を防止するためには、利用者が適切にネットワークACLを設定する必要がある。 ファイアウォールによる通信の送受信の確認や、WAFによるWebアプリケーションの保護などは、利用者が必要性を判断して構成する必要がある。
実15	マイクロソフトは、外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようにしています。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。 利用者が実装するアプリケーション環境について保護対策が必要な場合には、利用者側で対策を実施する必要があります。OSレベルでの Firewall 設定の他にアプリケーションのご要件に応じて対応を実施して頂きます。	適合可能	文献[01]に、ネットワーク境界の防護のため、ファイアウォール、ロードバランサー、IPフィルター等を用いた対策を採用している旨が明示されている。 文献[04]に、利用者がネットワークセキュリティグループを使用してアクセス制御リスト（ACL)を作成可能であることが記載されている。また、Azure Platformに固有のセキュリティ層による保護についても明記されている。 文献[06]に、クラウド基盤等への不正侵入を含む攻撃に対抗してインシデントレスポンスチームが設置されている旨、明示されている。 SOC2レポートにおいて、管理者権限アクセスの統制と接続手段の管理について記載されていることを確認した。	文献[01] P60 IVS-09: Infrastructure & Virtualization Security - Segmentation 文献[04] Azure 仮想ネットワークの概要 文献[06] P6 Azure Security Incident Response Process	SOC2レポート OA-1	―	ネットワークACLを用いてアクセス可能な機器を必要最小限にするためには、利用者が適切にネットワークACLを設定する必要がある。

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	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16	マイクロソフトは Microsoft Azure へ外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないように対策を実施しております。 外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。 利用者は、 Microsoft Azure 上に実装するアプリケーションについては、IDの不正使用防止機能に関する対応を実施する必要があります。	適合可能	文献[05]に、Azure Active Directoryレポートを利用することにより、Windows Azureへのアクセスについて、「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人によって行われた可能性があるサインイン試行の指標）」「リスクのフラグ付きユーザー（侵害された可能性があるユーザー アカウントの指標）」に関するレポートを入手可能である旨が明示されている。 文献[06]に、クラウド基盤等への不正侵入を含む攻撃に対抗してインシデントレスポンスチームが設置されている旨、明示されている。 SOC2レポートにおいて、不正行為の予兆や境界侵害を監視するシステムについて記載されていることを確認した。	文献[05] セキュリティ 文献[06] P6 Azure Security Incident Response Process	SOC2レポート VM-3	―	利用者がAzure上で構築したアプリケーションやサービスに対する不正アクセスの監視については、利用者が対策する必要がある。
実17	利用者は、要件に合わせて、Microsoft Azure上で実装するアプリケーションの不正取引に関する対策を実施します。	対象外	―	―	―	―	異常な取引状況を把握する機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実18	利用者は、要件に合わせて、Microsoft Azure上で実装するアプリケーションの異例取引を監視するための対応を実施頂きます。	対象外	―	―	―	―	異例取引の監視機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実19	マイクロソフトにおいては、Microsoft Azure プラットフォーム インフラストラクチャの各層は、障害発生時にも運用を継続できるように設計されています。 利用者は、 Azure 上で実装するアプリケーション環境について保護対策に関する対応を実施する必要があります。 利用者がビジネス目標に応じて、継続的な監視、テスト、監査を行い、 インシデント発生時には、検出、可視化された情報あら利用者の標準的なセキュリティレスポンスとフォレンジックプロセスを使用して復旧を行います。	適合可能	文献[06]に、特定、封じ込め、一掃、復旧、教訓を得るの各フェーズに従うセキュリティインシデント対応サイクルについて明示されている。 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、インシデント事象等の定義、チームによる対処規程の文書化、報告とレビューのプロセスが記載されていることを確認した。	文献[06] P6 Azure Security Incident Response Process	SOC2レポート SOC2-20, IM-1, IM-2, IM-3, IM-4, IM-5	―	利用者がAzure上で構築したアプリケーションやサービスに対する不正アクセスについては、利用者が対応策及び復旧策を講じる必要がある。
実20	マイクロソフトはコード開発からインシデント対応まで、セキュリティをあらゆる段階で優先させています。Microsoft Security Development Lifecycle（SDL）は、ソフトウェア製品の脆弱性の数と重大度を最小限に抑えるように設計された一連のプロセスとツールです。これは、より一貫して安全なソフトウェアを構築するために、開発担当者の教育、開発プロセスの安全性、個人および製品チームのアカウンタビリティを包括しています。 AzureはSDLを使用して、開発プロセス全体を通じてセキュリティ脅威に対処します。コーディング中に開発ベストプラクティスとコードセキュリティ標準に従って、デプロイメント前にテストと検証にさまざまなツールを使用する必要があります。開発中のこれらの積極的なチェックは、リリース後に潜在的な脅威に対するソフトウェアの脆弱性を軽減し、SDLはそれらを適用するための構造化された一貫した方法論で Azure の保護を行っております。 利用者は、 Azure 上で実装するアプリケーション環境について保護対策に関する対応を実施する必要があります。 利用者がビジネス目標に応じて、継続的な監視、テスト、監査を行い、 インシデント発生時には、検出、可視化された情報あら利用者の標準的なセキュリティレスポンスとフォレンジックプロセスを使用して復旧を行います。	適合可能	文献[11]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠してい」る旨が明示されている。 文献[09]に、SDLにおけるセキュア開発ツールやテスト手法について記載されている。 SOC2レポートにおいて、ソースコードのマルウェア検査及び、パッチ適用時の評価方法と手順の確立について記載されていることを確認した。	文献[11] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-6, VM-5	―	利用者がAzure上で構築したアプリケーションやサービスに対する不正プログラムへの防御対策については、利用者が対応を講じる必要がある。
実21	実 20に同じ	適合可能	文献[06]に、クラウド基盤等への不正侵入を含む攻撃に対抗してインシデントレスポンスチームが設置されている旨が明示されている。 文献[11]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠してい」る旨が明示されている。 文献[09]に、SDLにおけるセキュア開発ツールやテスト手法について記載されている。 SOC2レポートにおいて、ソースコードのマルウェア検査及び、パッチ適用時の評価方法と手順の確立について記載されていることを確認した。	文献[06] P6 Azure Security Incident Response Process 文献[11] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-6, VM-5	―	利用者がAzure上で構築したアプリケーションやサービスに対する不正プログラムの検知対策については、利用者が対応を講じる必要がある。

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	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22	実 20に同じ	適合可能	文献[06]に、特定、封じ込め、一掃、復旧、教訓を得るの各フェーズに従うセキュリティインシデント対応サイクルについて明示されている。 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、インシデント事象等の定義、チームによる対処規程の文書化、報告とレビューのプロセス、年次のインシデント対応手順テストが記載されていることを確認した。	文献[06] P6 Azure Security Incident Response Process	SOC2レポート IM-1, IM-2, IM-3, IM-4, IM-5, IM-6	ー	利用者がAzure上で構築したアプリケーションやサービスに対する不正プログラムの被害時対策については、利用者が対応を講じる必要がある。
実23	マイクロソフトにおいては、Microsoft Azureのプラットフォームの基盤の管理として標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 利用者は、Azure上に構築された利用者システムにおける正確かつ安全に運用するマニュアルの整備を実施する必要があります。	適合可能	文献[01]に、ISMSによる文書管理と年次の見直しが行われている旨が明示されている。 同じく文献[01]に、標準運用手順にもとづく管理について例示されている。 SOC2レポートにおいて、ISMSによる統制と監査の実施が記載されていることを確認した。	文献[01] P37 GRM-06: Governance and Risk Management – Policy P33 EKM-03: Encryption & Key Management – Sensitive Data Protection	SOC2レポート SOC2-20	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実24	マイクロソフトにおいては、エンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 利用者は、Microsoft Azure 上に実装するアプリケーションの障害対策・災害対策に関する対応を実施する必要があります。 利用者は、Microsoft Azure が提供する複数のリージョンを利用し、可用性を重視したアーキテクチャー設計/構築することにより、ビジネス継続性を実現することが可能です。	適合可能	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。 文献[10]に、Azure Security Centerを利用することで、「優先順位が付けられたアラートとインシデント」の参照、「電子メール通知」等の機能を利用可能であることが明記されている。 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及び、BCPの文書化が記載されていることを確認した。	文献[01] P12 BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing P13 BCR-04: Business Continuity Management & Operational Resilience – Documentation 文献[10] 優先順位が付けられたアラートとインシデント	SOC2レポート IM-1, BC-1	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実25	組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure には、情報セキュリティ ポリシーをが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 マイクロソフト管理者のアクセスはLockboxを経由したもののみが可能であり、Lockboxによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）に記載。 利用者は、Microsoft Azure 上に実装するアプリケーションについて、システムへのアクセス制御に関する対応を実施する必要があります。	適合可能	文献[01]に、Microsoft Azureへのアクセスはアクセス管理ポリシーによって統制されていること、ポリシーは定期的に見直しと更新が行われることが明示されている。また、ポリシーは知る必要と最小権限の原則に基づき、業務上の役割に応じて決定されること、アクセス権の自動失効機能を有すること、Active Directryによるパスワードポリシーの実装などが示されている。 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、管理者権限アクセスの統制と接続手段の管理について記載されていることを確認した。	文献[01] P46 IAM-02: Identity & Access Management – Credential Lifecycle / Provision Management P30 DCS-09: Datacenter Security – User Access	SOC2レポート OA-1	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。 利用者は、利用者自身のユーザーによるアクセスを制御し、そのようなアクセスを適切に確認する責任を負う。

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	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26	組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure には、情報セキュリティ ポリシーをが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 マイクロソフト管理者のアクセスはLockboxを経由したもののみが可能であり、Lockboxによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）に記載。 なお、Azureサブスクリプションへのアクセスに利用するIDのパスワード、利用者アプリケーションで利用するパスワードの管理は利用者にて対応頂きます。	適合可能	文献[02]に、Microsoft Azureへのアクセスにおけるid管理策として、多要素認証の利用、強力なパスワードポリシーの適用等の保護策について記載されている。 文献[07]に、Azure Active DirectoryによるID管理を行う場合に、「使用可能文字」「文字制限」の設定や「有効期限（無期限含む）」「アカウントロックアウト」等の変更を行うことが出来ることが明示されている。 SOC2レポートにおいて、利用者認証において要求されるパスワード強度規程について記載されていることを確認した。	文献[02] ID 管理とアクセス管理 文献[07] Azure Active Directory のパスワード ポリシーと制限	SOC2レポート OA-4	ー	利用者は、承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分な強度を備えたパスワードを選択する責任を負う。
実27	マイクロソフトにおいては、組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Azure の運用環境へのアクセスは、厳しく管理されています。 Microsoft Azure には、情報セキュリティ ポリシーをが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 マイクロソフト管理者のアクセスはLockboxを経由したもののみが可能であり、Lockboxによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。 利用者は、Microsoft Azure 上に実装するアプリケーションについて、システムへのアクセス制御に関する対応を実施する必要があります。	適合可能	文献[01]に、Microsoft Azureへのアクセスはアクセス管理ポリシーによって統制されていること、ポリシーは定期的に見直しと更新が行われることが明示されている。また、ポリシーは知る必要と最小権限の原則に基づき、業務上の役割に応じて決定されること、アクセス権の自動失効機能を有すること、Active Directryによるパスワードポリシーの実装などが示されている。 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、管理者権限アクセスの統制と接続手段の管理及び、従業員等のアクセス認証について記載されていることを確認した。	文献[01] P46 IAM-02: Identity & Access Management – Credential Lifecycle / Provision Management P30 DCS-09: Datacenter Security – User Access	SOC2レポート OA-1, OA-2	ー	利用者がAzure上で構築する環境でのアクセス権限の付与、見直し手続きについては、利用者が明確にする必要がある。
実28	利用者は、Microsoft Azure 上に実装するアプリケーションについて、利用者データの授受・管理に関する対応を実施する必要があります。	対象外	ー	ー	ー	ー	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。
実29	利用者は、Microsoft Azure 上に実装するアプリケーションについて、利用者データの授受・管理に関する対応を実施する必要があります。 なお、Microsoft Azure では、Microsoft Azure のデータ分類体系に従ってデータを分類し、その後で一連の標準的なセキュリティおよびプライバシー属性を実装します。 ISO/IEC 27001:2013 規格A.13 "COMMUNICATIONS SECURITY" およびA.14 "SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE" においてデータをネットワーク経由にて不正に取得しない為のネットワーク関連のセキュリティや、情報の管理についての対応を規定しています。	対象外	ー	ー	ー	ー	利用者は、データファイルの修正及び管理方法を定める必要がある。
実30	マイクロソフトには、格納域内のデータおよび伝送中のデータの暗号化をサポートする効率的なキー管理のために確立された、Microsoft Azure サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあります。 利用者は、Microsoft Azure 上に実装するアプリケーションについて、利用する暗号鍵管理の対応を実施する必要があります。	適合可能	文献[03]に、サーバー側暗号化方式として、「サービスが管理するキー」「ユーザーが管理するキー」「ユーザーが制御するハードウェア上でサービスが管理するキー」が選択可能であることが明示されている。 文献[08]には、利用者がMicrosoft Azure上でデータの暗号化を行うためのベストプラクティスが公開され、ファイルレベルのデータ暗号化に関する手法も記載されている。 SOC2レポートにおいて、暗号鍵の安全な保管及び、暗号化ポリシーと鍵管理手続きについて記載されていることを確認した。	文献[03] Azure の暗号化モデル 文献[08] ファイルレベルのデータ暗号化を適用する	SOC2レポート DS-1, DS-4	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実31	利用者は、Microsoft Azure 上に実装するアプリケーション関する教育・訓練に関する対応を実施する必要があります。 なお、マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。コンピュータシステムのオペレーションにあたっては、自動化されオペレータは存在せず、不正行為についても自律的な検出によるコントロールも組み合わせて運用されております。	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。	ー	ー	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

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	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32	マイクロソフトにおいて、Microsoft Azure のセキュリティ グループは、専門のサポート グループへのエスカレーションや依頼を含め、悪意のあるイベントへの対応を行います。システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティ パラメーターが監視されます。 利用者は、Microsoft Azure 上に実装するアプリケーションに関する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[06]に、特定、封じ込め、一掃、復旧、教訓を得るの各フェーズに従うセキュリティインシデント対応サイクルについて明示されている。 同じく文献[06]に、クラウド基盤等への不正侵入を含む攻撃に対抗してインシデントレスポンスチームが設置されている旨、明示されている。 SOC2レポートにおいて、ソースコードのマルウェア検査及び、パッチ適用時の評価方法と手順の確立について記載されていることを確認した。	文献[06] P6 Azure Security Incident Response Process	SOC2レポート SDL-6, VM-5	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実33	利用者は、Azureにアクセスするまでのネットワーク経路に関する契約については、回線事業者との間で協議する必要があります。	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に同じ	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	利用者は、 Microsoft Azure 上に実装するアプリケーションに関するオペレータの対策を実施する必要があります。 なお、マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。コンピュータシステムのオペレーションにあたっては、自動化されオペレータは存在せず、不正行為についても自律的な検出によるコントロールも組み合わせて運用されております。	適合可能	インタビュー等を通じて、通常時運用の自動化と不正行為のシステムによる検出と監視について確認した。	―	―	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	利用者は、運用管理者がオペレーター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。 例）制服の着用 　腕章の着用 　名札の着用
実36	利用者は、Microsoft Azure 上に実装するアプリケーションに関するオペレータの対策を実施する必要があります。 なお、マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。コンピュータシステムのオペレーションにあたっては、自動化されオペレータは存在せず、不正行為についても自律的な検出によるコントロールも組み合わせて運用されております。	適合可能	インタビュー等を通じて、通常時運用の自動化と不正行為のシステムによる検出と監視について確認した。	―	―	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	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	利用者は、Microsoft Azure 上に実装するアプリケーションに関するオペレータの対策を実施する必要があります。 なお、マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。コンピュータシステムのオペレーションにあたっては、自動化されオペレータは存在せず、不正行為についても自律的な検出によるコントロールも組み合わせて運用されております。	適合可能	インタビュー等を通じて、通常時運用の自動化と不正行為のシステムによる検出と監視について確認した。	―	―	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	利用者は、オペレーターチームの編成及びオペレーション手順を定める必要がある。
実38	利用者は、Microsoft Azure 上に実装するアプリケーションに関するオペレータの対策を実施する必要があります。 なお、マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。コンピュータシステムのオペレーションにあたっては、自動化されオペレータは存在せず、不正行為についても自律的な検出によるコントロールも組み合わせて運用されております。	適合可能	インタビュー等を通じて、通常時運用の自動化とログの記録・不正監視について確認した。	―	―	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	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。
実39	マイクロソフトにおいて、データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 Microsoft Azure のストレージはレプリケーション機能があり、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができる仕組みになっています。 利用者は、Microsoft Azure 上に実装するアプリケーションについて、データバックアップの対応を実施する必要があります。	適合可能	文献[01]に、仮想マシンのデータは地域内のストレージに複製されており、Azure Backupサービスを利用することで復旧可能である旨が明示されている。 同じく文献[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が明示されている。 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] P13 BCR-07: Business Continuity Management & Operational Resilience - Equipment Maintenance P17 BCR-11: Business Continuity Management & Operational Resilience - Retention Policy	SOC2レポート DS-5, DS-8	―	利用者は、必要に応じて自社でのデータの抽出及びバックアップの実行を選択する必要がある。

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	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40	マイクロソフトはコード開発からインシデント対応まで、セキュリティをあらゆる段階で優先させています。Microsoft Security Development Lifecycle（SDL）は、ソフトウェア製品の脆弱性の数と重大度を最小限に抑えるように設計された一連のプロセスとツールです。これは、より一貫して安全なソフトウェアを構築するために、開発担当者の教育、開発プロセスの安全性、個人および製品チームのアカウンタビリティを包括しています。 AzureはSDLを使用して、開発プロセス全体を通じてセキュリティ脅威に対処します。コーディング中に開発ベストプラクティスとコードセキュリティ標準に従って、デプロイメント前にテストと検証にさまざまなツールを使用する必要があります。開発中のこれらの積極的なチェックは、リリース後に潜在的な脅威に対するソフトウェアの脆弱性を軽減し、SDLはそれらを適用するための構造化された一貫した方法論で Azure の保護を行っております。 利用者は、 Azure 上で実装するアプリケーションのプログラムファイル管理を実施する必要があります。利用者アプリケーションに対する継続的な監視、テスト、監査の実施、インシデント発生時の対応は、利用者にて責任を負います。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるソフトウェア管理策について記載されている。 SOC2レポートにおいて、ソースコード管理用リポジトリについて記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-5	ー	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	実40と同じ	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるソフトウェア管理策について記載されている。 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[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート DS-5, DS-8	ー	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	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。ネットワーク装置の運用もSDNを取り入れてプログラムにより自動化され、構成情報も定期的にバックアップが取得されております。 Microsoft Azure では、データ センターの物理的な コントロールを通じて診断ポートおよび構成ポートへの物理的なアクセスを制御します。診断ポートおよび構成ポートへのアクセスは、サービス/資産の所有者と、アクセスを必要としているハードウェア/ソフトウェアのサポート担当者の間の申し合わせによって初めて可能になります。ポート、サービス、およびコンピューターやネットワーク機器にインストールされている同様の機能の中で、ビジネス機能において特に必要とされないものは、無効にされるか削除されます。 利用者は、Microsoft Azure 上に実装するアプリケーションの実行環境について、ネットワーク構成情報の管理を実施する必要があります。	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、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	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実43	マイクロソフトは Microsoft Azure の運用とサポートに関する厳格なセキュリティ対策基準を尊守しております。ネットワーク装置の運用もSDNを取り入れてプログラムにより自動化され、構成情報も定期的にバックアップが取得されております。 データ保持のポリシーと手順は、規制、法律、契約、またはビジネス上の要件に従って定義および維持されています。Microsoft Azure のバックアップおよび冗長性プログラムは、年に 1 度レビューと検証が行われます。 Microsoft Azure では障害復旧を目的として、インフラストラクチャ データのバックアップが定期的に作成され、データの復元が定期的に検証されます。 利用者は、Microsoft Azure 上に実装するアプリケーションの実行環境について、ネットワーク構成情報の管理を実施する必要があります。	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が明示されている。 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	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実44	マイクロソフトにおいては、標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azure では、Microsoft Azure サービスの一環として、包括的なガイダンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。Microsoft Azure のドキュメントは、サイトの中心に格納されています。 システム ドキュメントへのアクセスは、担当業務に基づいて Microsoft Azure の各チームに制限されます。 利用者は、Microsoft Azure 上に実装するアプリケーションについてのドキュメントの保管管理に関する対応を実施頂く必要があります。	適合可能	文献[01]に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が明示されている。 SOC2レポートにおいて、ISMSによる統制と監査の実施が記載されていることを確認した。 FedRAMP System Security Planにおいて、ドキュメントへのアクセスと職務の分離について記載されていることを確認した。	文献[01] P13 BCR-04: Business Continuity Management & Operational Resilience – Documentation	SOC2レポート SOC2-20 FedRAMP System Security Plan AC-01	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

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	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45	標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azure では、Microsoft Azure サービスの一環として、包括的なガイダンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。Microsoft Azure のドキュメントは、サイトの中心に格納されています。 システム ドキュメントへのアクセスは、担当業務に基づいて Microsoft Azure の各チームに制限されます。 利用者アプリケーションに関するドキュメントは、利用者にて管理頂きます。	適合可能	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、ISMSによる統制と監査の実施、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。 FedRAMP System Security Planにおいて、ドキュメントへのアクセスと職務の分離について記載されていることを確認した。	文献[01] 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 SOC2-20, DS-5, DS-8 FedRAMP System Security Plan AC-01	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実46	マイクロソフトにおいて、Microsoft Azure では、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。 利用者は、 Microsoft Azure 上に実装するアプリケーション実行環境について、システム運用状況の監視に関する対応を実施する必要があります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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、不正行為の予兆や境界侵害を監視するシステム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 VM-3	ー	利用者がAzure上で構築する環境での監視対象、監視内容及び監視方法については、利用者が整備する必要がある。
実47	マイクロソフトにおいて、予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを確立しております。 利用者は、Microsoft Azure 上に実装するアプリケーション実行環境について、監視に関する対応を実施する必要があります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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、ネットワーク可用性の監視及び、予測に基づく容量管理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 BC-10, CCM-5	ー	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	マイクロソフトでは、MCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。ハードウェア機器の保守についてもこれに基づき実施しています。 利用者は、実装するアプリケーションで利用するソフトウェアの管理を実施する必要があります。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。その管理は利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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、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。 SOC2レポートにおいて、主要情報資産台帳の維持管理及び、グローバルデータセンター運用チームのチケット管理システムによる構成管理/廃棄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	SOC2レポート SOC2-2, SOC2-3	ー	資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を負い、資産保護を規格に応じて分類し、保守する役割を担う。 利用者は、自身のデータの管財人としての責任を負う。
実49	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。ハードウェア機器の保守についてもこれに基づき実施しています。 利用者は、実装するアプリケーションに関する構成管理を実施する必要があります。利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。その管理は利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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	ー	利用者がAzureへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。

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	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50	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。ハードウェア機器の保守についてもこれに基づき実施しています。 利用者は、実装するアプリケーションのネットワーク構成を管理する必要があります。利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。その管理は利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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	ー	利用者がAzureへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。
実51	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。ハードウェア機器の保守についてもこれに基づき実施しています。 利用者は、実装するアプリケーションの構成を管理する必要があります。利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロールができます。 また、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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。 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	ー	利用者がAzureへ接続するために機器・ネットワーク等を設置する場合は、当該環境における対策は利用者にて実施する必要がある。
実52	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。データセンターのハードウェア機器の保守についてもこれに基づき実施しています。定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。 利用者は、実装するアプリケーションの構成を管理する必要があります。仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロール、仮想アプライアンスの導入を行うことができます。これに対する対障害構成や管理については利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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	ー	ー
実53	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロールを行うことができます。障害・災害に対する構成や管理は利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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、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	ー	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う。

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	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54	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoftのクラウドの管理を行ってます。MCIOにの組織において各サービスの監視、メンテナンス等の運用を行っております。 MCIOでは運用手順が文書化されており、確立しております。定期的な見直しを実施しています 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲスト OS、ソフトウェア及びアプリケーションのコントロールを行うことができます。これに対する保守・管理は利用者の責任となります。 なお、Microsoft Azure の利用者側に設置される設備（管理端末、オンプレミスサーバー等）の管理は利用者の責任となります。	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	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOでは、24時間、365日での運用管理を行っており、異常状態を早期に発見する為に各種設備のキャパシティー管理を実施しております。 事前予防的な監視により、Microsoft Azure 基盤の主要サブシステムのパフォーマンスを、許容されるサービスのパフォーマンスと可用性に対して確立された境界を基準にして継続的に測定しています。しきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしています。システム パフォーマンスおよび容量の使用率については、環境を最適化するために事前に計画を立てています。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲスト OS、ソフトウェア及びアプリケーションのコントロールを行うことができます。これに対する監視・対策については利用者の責任となります。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実56	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置・権限、および運用管理手順が文書化され確立しています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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、バッチ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	―	―

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	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57	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置・権限、および運用管理手順が文書化され確立しています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。 ご参考資料： ・ホワイトペーパー「信頼できるクラウド:Microsoft Azure のセキュリティ、プライバシー、コンプライアンス」 http://download.microsoft.com/download/D/6/F/D6F3C9DB-A263-4B28-9855-B40243694E43/Microsoft%20Azure%20-%20SecurityPrivacyCompliance.pdf なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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。 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	ー	ー
実58	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置・権限、および運用管理手順が文書化され確立しています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。 なお、利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。	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。 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	ー	ー
実59	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置・権限、および運用管理手順が文書化され確立しています。 アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Azure サービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO/IEC 27001:2013 規格A.11 PHYSICAL AND ENVIRONMENTAL SECURITYにおいて物理的にデータを安全に管理する事、入退室管理について対応を規定しています。 利用者側に設置される設備（オンプレミス側の管理端末・サーバー等）の管理は利用者の責任となります。また、管理業務を実施できる環境の限定などの対応は、利用者にて実施頂く必要があります。	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	ー	利用者は、Azureが発行する秘密キーを利用して認証を行う場合、秘密キーの管理は利用者自身が行う必要がある。 また、利用者がAzure上に構築する環境に対する管理業務を実施できる環境の限定やアクセス権限の管理などの対応は、利用者自身が行う必要がある。

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	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60	マイクロソフトでは、災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、オンラインサービスの管理組織であるGlobal Foundation Service（GFS)に属するOnline Services Security and Compliance (OSSC)の情報セキュリティ管理システム (ISMS)によりレビュープロセスが確立されています。使用する統制策（ISO27001/27005、SAS70 TypeIおよびII, SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。	適合可能	文献[11]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、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[11] P8 インシデント管理と対応	SOC2レポート PE-5, PE-6	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実61	ー	対象外	ー	ー	ー	ー	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	ー	対象外	ー	ー	ー	ー	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	ー	対象外	ー	ー	ー	ー	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	ー	対象外	ー	ー	ー	ー	利用者は、エンドユーザーからの届出の受付体制の整備、事故口座の管理を行う必要がある。
実65	ー	対象外	ー	ー	ー	ー	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	ー	対象外	ー	ー	ー	ー	利用者は、出力情報の作成、授受、保管、管理及び廃棄について、不正防止対策及び機密保護対策を講じる必要がある。
実67	ー	対象外	ー	ー	ー	ー	利用者は、未使用重要帳票の在庫管理及び廃棄の方法を定める必要がある。
実68	ー	対象外	ー	ー	ー	ー	利用者は、重要な印字済帳票の授受及び廃棄の方法を定める必要がある。
実69	利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲスト OS、ソフトウェア及びアプリケーションのコントロールを行うことができます。利用者は、顧客データを保護するための多要素認証、アクセス制御、暗号化などを実装することができます。これらの管理は利用者の責任となります。	適合可能	文献[03]に、サーバー側暗号化方式として、「サービスが管理するキー」「ユーザーが管理するキー」「ユーザーが制御するハードウェア上でサービスが管理するキー」が選択可能であることが明示されており、利用者が自身の暗号鍵により顧客データを保護することが出来ると考えられる。 文献[11]には、Microsoftのスタッフによる顧客データへのアクセスの禁止原則及び、利用者支援のために例外的にアクセスを行う場合の認可・認証手続及びアクセス履歴の記録の保持について明記されている。 SOC2レポートにおいて、暗号鍵の安全な保管について記載されていることを確認した。	文献[03] Azure の暗号化モデル 文献[11] P13 マイクロソフトのスタッフによるアクセスの禁止	SOC2レポート DS-1	ー	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	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOの組織において各管理責任者の配置、および運用管理手順、障害時、災害における対象方法が文書化され確立しています。 利用者は、実装するアプリケーションに関する障害時・災害時の連絡手段を定める必要があります。	適合可能	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。 同じく文献[01]に、セキュリティインシデント発生時はAzure Online Services上で情報開示が行われる旨が明示されている。 SOC2レポートにおいて、インシデント対応フレームワークの策定について記載されていることを確認した。	文献[01] P12 BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing P73 SEF-02: Security Incident Management, E-Discovery & Cloud Forensics – Incident Management	SOC2レポート IM-1	ー	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う。

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	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71	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。MCIOでは影響分析が適切な間隔で実行され、確認されます。次のような分析を行います。 ・ Microsoft Azure ビジネス環境およびプロセスに関連する脅威の特定 ・ 可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・ 特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 ビジネスの影響評価、依存関係の分析、およびリスク評価は、少なくとも年に一度、実施または更新されます。お客様は、アプリケーションおよび設計に対する影響を分析し、目標復旧時間 (RTO) と目標復旧時点 (RPO) の要件を満たしていることを確認する責任を負います。 ISO 27001 規格 A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENTにおいて、障害、災害じにおけるビジネス継続の為の管理についての対応が規定されております。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除、ゲストOSやソフトウェア及びアプリケーションのコントロールを行うことができます。利用者アプリケーションに関する障害・災害への対策は、利用者にて実施となります。	適合可能	文献[01]に、「文書化された手順による継続性の計画」や復元計画の定期的な検証に」ついて明示されている。 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、チームによる対処規程、BCPの文書化、BCP/DR標準手順の策定・テスト・改善について記載されていることを確認した。	文献[01] P42 RS-03 復元 – ビジネス継続性の計画	SOC2レポート IM-1, IM-3, BC-1, BC-3, BC-4, BC-5	ー	利用者がAzure上で構築した環境については、障害時・災害時に利用者自身が実施すべきコンピュータシステムの復旧手順を明確にする必要がある。
実72	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。標準的な運用手順が、正式に文書化され、Microsoft Azure の管理者によって承認されています。標準的な運用手順は少なくとも年に一度見直されます。 Microsoft Azure では、Microsoft Azure サービスの一環として、包括的なガイダンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。Microsoft Azure のドキュメントは、サイトの中心に格納されています。 システム ドキュメントへのアクセスは、担当業務に基づいて MCIOの各チームに制限されます。 ISO 27001 規格 A.12 OPERATIONS SECURITY A.16 INFORMATION SECURITY INCIDENT MANAGEMENT A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENTにおいて、運用手順の文書化、障害、災害じにおけるビジネス継続の為の管理についての対応が規定されております。 利用者は、実装するアプリケーションに関する障害調査・分析・再発防止策検討を実施する必要があります。	適合可能	文献[10]に、Azure Security Centerを利用することで、「優先順位が付けられたアラートとインシデント」の参照、「電子メール通知」等の機能を利用可能であることが明記されている。 SOC2レポートにおいて、Azureに重大な影響を及ぼすインシデント発生時の対応について記載されていることを確認した。	文献[10] 優先順位が付けられたアラートとインシデント	SOC2レポート IM-4	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実73	マイクロソフトでは、エンタープライズ ビジネス継続性の管理 (EBCM) フレームワークが確立されており、Server and Tools Business (STB) など、Microsoft Azure を担当する個々のビジネス ユニットに適用されます。指定された STB ビジネス継続性プログラム オフィス (BCPO) は、Microsoft Azure の管理者と協力して、重要なプロセスを特定し、リスクを評価します。STB BCPO は EBCM フレームワークと BCM ロードマップに関するガイダンスを Microsoft Azure チームに提供します。このガイダンスには以下のコンポーネントが含まれます。 ・ガバナンス ・影響の許容範囲 ・ビジネスの影響分析 ・依存関係の分析 (非技術面および技術面) ・戦略 ・計画 ・テスト ・トレーニングおよび意識向上 ISO 27001 規格 A.12 OPERATIONS SECURITY A.16 INFORMATION SECURITY INCIDENT MANAGEMENT A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENTにおいて、運用手順の文書化、障害、災害じにおけるビジネス継続の為の管理についての対応が規定されております。 利用者は、実装するアプリケーションに関するコンティンジェンシープランを定める必要があります。	適合可能	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、運用手順書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、BCPの文書化、DR計画の作成と試験、BCP/DR標準手順の策定・テスト・改善ついて記載されていることを確認した。	文献[01] P12 BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing	SOC2レポート BC-1, BC-2, BC-3	ー	利用者は、システムの管理者、管理方法を定め、障害時・災害時の対応指針を明確にしたうえで、地理的な冗長性のためにアプリケーションやデータを複数のリージョンに展開する等の対策を実施する責任を負う。
実74	マイクロソフトでは、Microsoft Azure を複数の地域でサービス提供しています。（日本の場合には、東日本もしくは西日本から選択可能です。） 利用者アプリケーションの構成として、複数地域を利用した冗長化構成を取る事で、災害・障害が起きた場合において継続利用をする事が可能です。 また、Microsoft Azure のストレージはレプリケーション機能があり、Microsoft データ センター内で障害が発生した場合にお客様のデータが損失するのを防ぐことができる仕組みになっています。 利用者は、Microsoft Azure 上に実装する仮想マシンやアプリケーションについて、データバックアップサイト対応などのフォールトス対策を実施する必要があります。	適合可能	文献[12]に、「地域はフォールトトレランスを備えている」旨が明示されている。 文献[18]に、「Azure リージョン間でアプリケーションをレプリケート」するための「Azure Site Recovery」について明示されている。 SOC2レポートにおいて、BCPの文書化、BCPOによるリスクアセスメント、Microsoftとしての事業継続マネジメント、データセンターの事業継続計画の作成と試験について記載されていることを確認した。	文献[12] 地域 文献[18] 簡単なデプロイと管理	SOC2レポート BC-1, BC-5, BC-7, BC-8	ー	仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 本番サイトと異なる地域にバックアップサイト向けの仮想マシンを設ける場合は、利用者が適切な地理的な場所に仮想マシンを作成する必要がある。 仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。 ホット・フェールオーバー機能を用いるためには、利用者が第2のストレージアカウントを作成して構成する必要がある。 Site Recovery機能を用いるためには、利用者が当該機能を構成する必要がある。

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	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75	マイクロソフトでは、Microsoft Azure についての変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、実装するアプリケーションの開発・変更手順を定める必要があります。	適合可能	文献[01]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。 同じく文献[01]に、リリース前に、コード検証、レビュー、セキュリティテストが実施される旨が明示されている。 文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるソフトウェア管理策について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、リリース時の関係者承認手続について記載されていることを確認した。	文献[01] P19 CCC-01.1: Change Control & Configuration Management – New Development / Acquisition P21 CCC-03: Change Control & Configuration Management – Quality Testing 文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, CM-2	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実76	マイクロソフトでは、Microsoft Azure についての変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、実装するアプリケーションのテスト環境を構築する必要があります。（Azure上に本番環境と論理的に分離した環境を構築することが可能です。）	適合可能	文献[01]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。 ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、及び変更管理 同じく文献[01]に、リリース前に、コード検証、レビュー、セキュリティテストが実施される旨が明示されている。 SOC2レポートにおいて、テスト環境とテストデータの分離について記載されていることを確認した。	文献[01] P19 CCC-01.1: Change Control & Configuration Management – New Development / Acquisition P21 CCC-04: Change Control & Configuration Management – Unauthorized Software Installations	SOC2レポート SDL-4	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実77	マイクロソフトでは、Microsoft Azure についての変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、実装するアプリケーションの本番移行手順を定める必要があります。	適合可能	文献[01]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。 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー 同じく文献[01]に、共通の変更管理プロセスが示され、ソースコードライブラリへのアクセス制御や多要素認証、変更ログの記録など実施される旨が明示されている。 文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるソフトウェア管理策について記載されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[01] P19 CCC-01.1: Change Control & Configuration Management – New Development / Acquisition P21 CCC-04: Change Control & Configuration Management – Unauthorized Software Installations 文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート CM-1, CM-2	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実78	マイクロソフトでは、Microsoft Azure についての変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・計画された変更の特定と文書化 ・ビジネスの目標、優先度、およびシナリオの特定（製品の計画時） ・機能/コンポーネント設計の仕様決定 ・全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・DEV（開発）、INT（統合テスト）、STAGE（運用前）、PROD（運用）環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、実装するアプリケーションの開発・変更時のドキュメント作成手順を定める必要があります。	適合可能	文献[01]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 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象について記載されていることを確認した。	文献[01] P19 CCC-01.1: Change Control & Configuration Management – New Development / Acquisition	SOC2レポート SDL-1, SDL-2	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

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	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79	マイクロソフトでは、Microsoft Azure についての変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスが確立されています。このプロセスには以下のものが含まれます。 ・ 計画された変更の特定と文書化 ・ ビジネスの目標、優先度、およびシナリオの特定 (製品の計画時) ・ 機能/コンポーネント設計の仕様決定 ・ 全体的なリスク/影響を評価するための、事前に定義された条件/チェックリストに基づく運用準備のレビュー ・ DEV (開発)、INT (統合テスト)、STAGE (運用前)、PROD (運用) 環境それぞれに応じた開始/終了条件に基づくテスト、認証、および変更管理 利用者は、実装するアプリケーションの開発・変更時のドキュメント保管管理方法を定める必要があります	適合可能	文献[01]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[01]に、「システムドキュメントへのアクセスは、担当業務に基づいて各チームに制限される」旨が明示されている。 SOC2レポートにおいて、ソースコード管理用リポジトリについて記載されていることを確認した。	文献[01] P19 CCC-01.1: Change Control & Configuration Management – New Development / Acquisition 文献[01] P16 BCR-10: Business Continuity Management & Operational Resilience – Policy	SOC2レポート SDL-5	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実80	利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲスト OS、ソフトウェア及びアプリケーションのコントロールを行うことができます。Microsoft Azure上に導入するパッケージソフトについては利用者にて評価する体制の整備が必要になります。 なお、マイクロソフトでは Microsoft Azure プラットフォーム内の基盤となるオペレーティング システム (OS) に対する変更は、運用環境に移る前に、品質、パフォーマンス、他のシステムへの影響、復旧目標、およびセキュリティ機能に関して、少なくともレビューとテストが行われます。変更は、運用環境に展開される前に、さまざまなテスト環境でテストされ、承認されます。 ISO 27001 規格A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCEにおいてシステム開発、変更における対応が規定されています。	適合可能	文献[01]に、外部のビジネスパートナーと共同開発を行う場合も、SDLを含む開発・リリース管理プロセスが適用されること、NIST SP 800-53に基づいた統制が行われることが明示されている。 同じく文献[01]に、Azureに対するシステム更新は情報セキュリティ管理ポリシーに従い、セキュリティ開発ライフサイクル (SDL) による変更管理、リリース管理、整合性の検証が行われる旨が明示されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[01] P20 CCC-02.1: Change Control & Configuration Management – Outsourced Development P7 AIS-04: Application & Interface Security – Data Security / Integrity	SOC2レポート CM-1, CM-2	ー	利用者は、Azure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る。
実81	利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲスト OS、ソフトウェア及びアプリケーションのコントロールを行うことができます。Microsoft Azure上に導入するパッケージソフトについては利用者により運用、管理体制を明確にする必要があります。 なお、マイクロソフトでは、Microsoft Azure サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を (基盤のレベルにおいても) 十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威のモデリング (Threat Modeling) によって、サービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面などの要素をマイクロソフトが特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格A.6 ORGANIZATION OF INFORMATION SECURITY A.12 OPERATIONS SECURITY A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCEにおいて情報セキュリティの管理体制、オペレーション手順の確立およびセキュアな開発環境における対応が規定されています。	適合可能	文献[01]に、サードパーティーベンダーによるサービスは監視され、標準的名監査手続きにより検証されている旨、明示されている。 同じく文献[01]に、外部のビジネスパートナーと共同開発を行う場合も、SDLを含む開発・リリース管理プロセスが適用されること、NIST SP 800-53に基づいた統制が行われることが明示されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[01] P5 AIS-01: Application & Interface Security – Application Security 文献[01] P20 CCC-02.1: Change Control & Configuration Management – Outsourced Development	SOC2レポート CM-1, CM-2	ー	利用者は、Azure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	マイクロソフトにおいて、Microsoft Azure のクラウド基盤の運用は、ベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し (つまり切断する)、情報の回復を不可能にする (分解、切断、粉砕、焼却など) 破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 利用者は、実装するアプリケーションに関する廃棄について、関連部署との調整・連絡や運用終結の確認などの手順を明確にする必要があります。 なお、「オンライン サービス条件」に従い、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、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。	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「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。 FedRAMP System Security Planにおいて、情報媒体を施設外で修理する場合において全ての情報を削除する旨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 FedRAMP System Security Plan MA-02	ー	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

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	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83	マイクロソフトにおいて、Microsoft Azure のクラウド基盤の運用は、ベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 利用者は、実装するアプリケーションに関する廃棄について、関連部署との調整・連絡や運用終結の確認などの手順を明確にする必要があります。 なお、「オンライン サービス条件」に従い、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、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。 ご参考資料: ・マイクロソフトによるデータの管理方法 https://www.microsoft.com/ja-jp/trustcenter/privacy/you-own-your-data ・Microsoft Azure の法的情報 https://azure.microsoft.com/ja-jp/support/legal/	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	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実84	マイクロソフトでは、Microsoft Azure プラットフォーム基盤を構成する各装置は全て冗長化しています。また、監視・障害対応として以下を実施しています。 ・H/W死活 Azure 側で監視し障害時は別 H/W へ自動切替 ・ネットワーク死活 経路冗長化により自動切替 ・OS死活 Azure 側で監視し障害時は再起動、又は別 H/W へ自動切替 ・プロセス IIS 等 Windows 提供プロセスは Azure 側で監視し障害時は 再起動 なお、利用者は、仮想マシンなどの Azure リソースの構成、ゲストOSやソフトウェアのコントロール、仮想アプライアンスの導入を行うことができます。利用者アプリケーションの冗長化、監視は利用者にて実施します。	適合可能	文献[11]に、国内・国外それぞれの場合において選択した地域内でのデータの冗長化について明示されている。 文献[01]に、十分に離れた同地域内のデータセンターにデータが自動コピーされる旨について明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化について記載されていることを確認した。	文献[11] P11 データの冗長化 文献[01] P12 BCR-01: Business Continuity Management & Operational Resilience - Business Continuity Planning	SOC2レポート DS-6	―	―
実85	マイクロソフトでは、Microsoft Azure プラットフォーム基盤を構成する各装置は全て冗長化しています。また、監視・障害対応として以下を実施しています。ストレージに関しては、同一データセンター内での3重化、オプションとして異なるデータセンター間での6重化までのデータ冗長化を行っています。 なお、利用者は、仮想マシンなどの Azure リソースの構成、ゲストOSやソフトウェアのコントロールを行うことができます。利用者が使用する仮想ディスク等の追加・設定が可能です。	適合可能	文献[11]に、国内・国外それぞれの場合において選択した地域内でのデータの冗長化について明示されている。 文献[01]に、十分に離れた同地域内のデータセンターにデータが自動コピーされる旨について明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化について記載されていることを確認した。	文献[11] P11 データの冗長化 文献[01] P12 BCR-01: Business Continuity Management & Operational Resilience - Business Continuity Planning	SOC2レポート DS-6	―	仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。
実86	マイクロソフトでは、Microsoft Azure プラットフォーム基盤の各層でネットワーク デバイスの冗長化を行い、各データセンターで 2 社のインターネット サービス プロバイダーを利用しています。フェールオーバーはほとんどの場合、自動で実行され（人の介入は不要）、ネットワークは、異常やネットワークの潜在的な問題を検出するために、ネットワーク運用センターで 24 時間 365 日常時監視しています。 利用者は、仮想ネットワークなどの Azure リソースの構成、仮想アプライアンスの導入ができます。また、利用者のオンプレミス環境と Microsoft Azure 間を閉域ネットワークで接続することも可能です。利用者のネットワーク環境の冗長化構成と監視については利用者にて実施します。	適合可能	文献[13]に大規模プライベートWANによるネットワーク容量の確保と障害時の自動ルーティングについて明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化について記載されていることを確認した。	文献[13] キャパシティと耐久性を常に制御できる状態に	SOC2レポート DS-6	―	―

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	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87	マイクロソフトでは、Microsoft Azure プラットフォーム基盤の各層でネットワーク デバイスの冗長化を行い、各データセンターで 2 社のインターネット サービス プロバイダーを利用しています。フェールオーバーはほとんどの場合、自動で実行され（人の介入は不要）、ネットワークは、異常やネットワークの潜在的な問題を検出するために、ネットワーク運用センターで 24 時間 365 日常時監視しています。 利用者は、仮想ネットワークなどの Azure リソースの構成、仮想アプライアンスの導入ができます。また、利用者のオンプレミス環境と Microsoft Azure 間を閉域ネットワークで接続することも可能です。利用者のネットワーク環境の冗長化構成と監視については利用者にて実施します。 ご参考情報 ・マイクロソフトは高速で信頼性の高いグローバル ネットワークをどのように構築しているのか https://blogs.technet.microsoft.com/mssvrpmj/2017/05/01/how-microsoft-builds-its-fast-and-reliable-global-network/	適合可能	文献[13]に大規模プライベートWANによるネットワーク容量の確保と障害時の自動ルーティングについて明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化について記載されていることを確認した。	文献[13] キャパシティと耐久性を常に制御できる状態に	SOC2レポート DS-6	―	―
実88	マイクロソフトでは、Microsoft Azureの管理・運用に利用する端末については、監視センターにおける集中監視を実施し複数端末により管理しております。 利用者は、Azureサブスクリプションへアクセスする端末や、利用者アプリケーションを管理する端末の予備・代替に関する対応を行う必要があります。	適合可能	文献[11]に「複数レベルの監視」について明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化について記載されていることを確認した。	文献[11] P8 運用上のセキュリティの強化	SOC2レポート DS-6	―	―
実89	マイクロソフトでは、Microsoft Azure プラットフォームと提供サービスのセキュリティおよび品質の確保に取り組んでいます。Microsoft Azure の基盤およびサービスは「セキュリティ開発ライフサイクル（SDL)ガイドライン」に基づき開発してます。 https://www.microsoft.com/en-us/sdl https://www.microsoft.com/ja-jp/trustcenter/security 利用者は、実装するアプリケーションおよび、他社パッケージソフトウェアの利用に関するセキュリティ対策を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるセキュリティ要求について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象、ソースコードのマルウェア検査について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, SDL-2, SDL-6	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実90	マイクロソフトでは、Microsoft Azure プラットフォームと提供サービスのセキュリティおよび品質の確保に取り組んでいます。Microsoft Azure の基盤およびサービスは「セキュリティ開発ライフサイクル（SDL)ガイドライン」に基づき開発してます。 https://www.microsoft.com/en-us/sdl https://www.microsoft.com/ja-jp/trustcenter/security 利用者は、実装するアプリケーションおよび、他社パッケージソフトウェアの利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおける設計工程について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象、ソースコードのマルウェア検査について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, SDL-2, SDL-6	―	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実91	マイクロソフトでは、Microsoft Azure プラットフォームと提供サービスのセキュリティおよび品質の確保に取り組んでいます。Microsoft Azure の基盤およびサービスは「セキュリティ開発ライフサイクル（SDL)ガイドライン」に基づき開発してます。 https://www.microsoft.com/en-us/sdl https://www.microsoft.com/ja-jp/trustcenter/security 利用者は、実装するアプリケーションおよび、他社パッケージソフトウェアの利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおける実装工程について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象、ソースコードのマルウェア検査について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, SDL-2, SDL-6	―	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実92	マイクロソフトでは、Microsoft Azure プラットフォームと提供サービスのセキュリティおよび品質の確保に取り組んでいます。Microsoft Azure の基盤およびサービスは「セキュリティ開発ライフサイクル（SDL)ガイドライン」に基づき開発してます。 https://www.microsoft.com/en-us/sdl https://www.microsoft.com/ja-jp/trustcenter/security 利用者は、実装するアプリケーションおよび、他社パッケージソフトウェアの利用にあたり、ソフトウェア品質確保に関する対応を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおける検証工程について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象、ソースコードのマルウェア検査について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, SDL-2, SDL-6	―	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。

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	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93	マイクロソフトでは、Microsoft Azure プラットフォームと提供サービスのセキュリティおよび品質の確保に取り組んでいます。Microsoft Azure の基盤およびサービスは「セキュリティ開発ライフサイクル（SDL)ガイドライン」に基づき開発してます。 https://www.microsoft.com/en-us/sdl https://www.microsoft.com/ja-jp/trustcenter/security 利用者は、実装するアプリケーションおよび、他社パッケージソフトウェアの利用にあたり、プログラム配布を考慮した信頼性確保に関する対応を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるリリース管理について記載されている。 SOC2レポートにおいて、Azure Platformの開発・変更がSDLに従うこと、実装前に文書化すべき対象、ソースコードのマルウェア検査について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート SDL-1, SDL-2, SDL-6	ー	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実94	利用者は、パッケージベンダーとパッケージの品質確保に関する確認・協議を実施する必要があります。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおけるプロジェクト全体を通してのセキュリティ要求水準の適用、APIレベルまでの安全性分析について記載されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート CM-1, CM-2	ー	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実95	マイクロソフトでは、Microsoft Azure プラットフォームの機器増設等の変更作業についてリリース管理プロセスが確立されております。構成変更作業は自動化されており、人的ミスを防ぎ、正確かつ迅速に行える仕組みとなっています。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロールを行うことができます。これらの展開・構成管理は利用者にて実施します。これを自動化するための各種仕組みを Microsoft Azure の機能として提供しています。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおける設計時のセキュリティ要求の確立、ツールの活用、リリース管理について記載されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート CM-1, CM-2	ー	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実96	マイクロソフトでは、Microsoft Azure プラットフォームの機器増設等の変更作業についてリリース管理プロセスが確立されております。構成変更作業は自動化されており、人的ミスを防ぎ、正確かつ迅速に行える仕組みとなっています。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェア及びアプリケーションのコントロールを行うことができます。これらの展開・構成管理は利用者にて実施します。なお、これを自動化するための各種仕組みを Microsoft Azure の機能として提供しています。	適合可能	文献[08]に、「Azureの開発は、マイクロソフトのセキュリティ開発ライフサイクル（SDL）に準拠している」旨が明示されている。 文献[09]に、SDLにおける事前セキュリティリスクアセスメント、セキュリティ検証試験の実施、リリース前のセキュリティ検証について記載されている。 SOC2レポートにおいて、統合変更管理の文書化と周知、リリース時の関係者承認手続について記載されていることを確認した。	文献[08] P7 セキュリティの設計と運用 文献[09] What is the Security Development Lifecycle ?	SOC2レポート CM-1, CM-2	ー	利用者がAzure上で構築するミドルウェアやアプリケーションソフトウェアの信頼性については、利用者が対策する必要がある。
実97	利用者アプリケーションが使用するデータ・ファイルのアクセス方法・制御に関しては、利用者にて実装します。 なお、Microsoft Azure内部では、ファイルシステムとして、データ不整合等が起こらないよう排他制御を行っております。	適合可能	文献[45]に、「BLOB ストレージ」「Table サービス」「キュー サービス」「ファイル サービス」それぞれにおける同時実行制御について明示されている。	文献[45] Microsoft Azure Storage での同時実行制御の管理	ー	ー	利用者がAzure上で構築するアプリケーションやサービスで矛盾発生を防止するためには、利用者が必要な対策を行う必要がある。
実98	利用者アプリケーションが使用するファイル・データの突合機能は、利用者にて実装します。 なお、Microsoft Azure内部では、処理エラーのリスクを抑えるため、Microsoft Azure 環境内に内部処理制御が実装されています。内部処理制御は、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ます。内部処理制御の例としては、ハッシュトータルやチェックサムの使用などがあります。	適合可能	文献[01]に、内部処理エラーリスク抑制のための管理策としてハッシュトータルや、チェックサムの検証等を行っていることが明示されている。	文献[01] P7 AIS-03.1: Application & Interface Security - Data Integrity	ー	ー	利用者がAzure上で構築するアプリケーションやサービスで扱うファイル間の不整合を発見するためには、それらのアプリケーションやサービスで突合機能を設ける必要がある。
実99	マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。標準的な運用手順が、正式に文書化されています。標準的な運用手順は少なくとも年に一度見直されます。 機器増設等の変更作業についてリリース管理プロセスが確立されており、自動化されていますので、人的ミスを防ぎ、正確かつ迅速に行える仕組みとなっています。 利用者は、実装するアプリケーションが稼働する仮想マシン等のオペレーションの自動化・簡略化について対応する必要があります。	適合可能	文献[01]に、ISMSによる文書管理と年次の見直しが行われている旨が明示されている。 同じく文献[01]に、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。 SOC2レポートにおいて、離籍者のアカウント停止の自動化、システム障害・ハードウェア障害時のリストア自動化について記載されていることを確認した。 インタビュー等を通じて、通常時運用の自動化と効率化について確認した。	文献[01] P37 GRM-06: Governance and Risk Management - Policy P25 DCS-03: Datacenter Security - Equipment Identification	SOC2レポート OA-3, DS-14	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	利用者がAzure上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。

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	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100	利用者は、実装するアプリケーションが稼働する仮想マシン等のオペレーションの自動化・簡略化について対応する必要があります。 マイクロソフトではMCIO(Microsoft Infrastructure and Oprerations)といわれる組織により、Microsoft Azure のクラウド基盤の管理を行ってます。機器増設等の変更作業についてリリース管理プロセスが確立されており、自動化されていますので、人的ミスを防ぎ、正確かつ迅速に行える仕組みとなっています。 また、Azure管理ポータル上で、利用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	適合可能	文献[01]に、ISMSによる文書管理と年次の見直しが行われている旨が明示されている。 同じく文献[01]に、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。 インタビュー等を通じて、通常時運用の自動化とログの記録と監視について確認した。	文献[01] P37 GRM-06: Governance and Risk Management – Policy P25 DCS-03: Datacenter Security – Equipment Identification	―	通常時運用は自動化されおり、オペレータによる運用は行っていない。また、不正監視も自動で行われる。	利用者がAzure上で構築するアプリケーションやサービスの運用における信頼性については、利用者が対策する必要がある。
実101	マイクロソフトでは、Microsoft Azure プラットフォームを構成する機器・ソフトウェアに対し、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視し、必要時に対応するための運用プロセスを用意しています。 利用者は、実装するアプリケーションの監視と対応策に関する対応を実施する必要があります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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、ネットワーク可用性の監視及び、予測に基づく容量管理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 BC-10, CCM-5	―	利用者がAzure上で構築するアプリケーションやサービスの監視制御については、利用者が行うがある。
実102	マイクロソフトでは、Microsoft Azure プラットフォームを構成する機器・ソフトウェアに対し、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視し、必要時に対応するための運用プロセスを用意しています。マイクロソフトは利用者のデータおよびシステムの重要性には関与しません。 利用者は、実装するアプリケーションに関して、システムの重要性に応じた監視に関する対応を実施する必要があります。	適合可能	文献[01]に、しきい値とイベントが定義され、予防的容量管理を行われていること、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。 文献[11]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、インシデント対応フレームワークの策定、インシデント事象等の定義、チームによる対処規程の文書化及び、不正行為の予兆や境界侵害を監視するシステム、不正イベント検知時の適時対応、内部と第三者による可用性監視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 文献[11] P8　インシデント管理と対応	SOC2レポート IM-1, IM-2, IM-3, IM-4, VM-3, VM-4, VM-12	―	利用者がAzure上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。
実103	マイクロソフトでは、Microsoft Azure プラットフォームを構成する機器・ソフトウェアに対し、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視し、必要時に対応するための運用プロセスを用意しています。 利用者は、実装するアプリケーションに関して、監視と監視状況に応じた対応を実施する必要があります。	適合可能	文献[11]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、インシデント対応フレームワークの策定、インシデント事象等の定義、チームによる対処規程の文書化及び、不正行為の予兆や境界侵害を監視するシステム、不正イベント検知時の適時対応、内部と第三者による可用性監視について記載されていることを確認した。	文献[11] P8　インシデント管理と対応	SOC2レポート IM-1, IM-2, IM-3, IM-4, VM-3, VM-4, VM-12	―	利用者がAzure上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。
実104	マイクロソフトでは、Microsoft Azure プラットフォーム基盤を構成する各装置・ソフトウェア構成は全てを冗長化しています。また、障害時における対応プロセスも文書化しています。パターン化できるケースについては自動にて対応できるように構成・運用しています。 利用者は、実装するアプリケーションの障害時の縮退・再構成に関する対応を実施する必要があります。利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロールを行うことができます。これらを冗長化構成とする事で、障害が起きた場合において継続利用をする事が可能です。	適合可能	文献[11]に、国内・国外それぞれの場合において選択した地域内でのデータの冗長化による喪失回避について明示されている。 文献[13]に大規模プライベートWANによるネットワーク容量の確保と障害時の自動ルーティングについて明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化、データの自動複製による影響の最小化について記載されていることを確認した。	文献[11] P11 データの冗長化 文献[13] キャパシティと耐久性を常に制御できる状態に	SOC2レポート DS-6, DS-7	―	利用者がAzure上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。 ホット・フェールオーバー機能を用いるためには、利用者が第2のストレージアカウントを作成して構成する必要がある。
実105	電子商取引ソリューションの要件に応じたアプリケーションの実装は利用者にて対応します。	対象外	―	―	―	―	取引制限機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。

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	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106	マイクロソフトでは、Microsoft Azure プラットフォーム基盤を構成する各装置・ソフトウェア構成は全てを冗長化しています。また、障害時における対応プロセスも文書化しています。パターン化できるケースについては自動にて対応できるように構成・運用しています。 利用者アプリケーションの障害時対応については、利用者の責任にて実施します。 利用者は、仮想マシンなどの Azure リソースの追加・構成・削除ができ、ゲストOS、ソフトウェアのコントロールを行うことができます。これらを冗長化構成とする事で、障害が起きた場合において継続利用をする事が可能です。	適合可能	文献[11]に、国内・国外それぞれの場合において選択した地域内でのデータの冗長化による喪失回避について明示されている。 文献[13]に大規模プライベートWANによるネットワーク容量の確保と障害時の自動ルーティングについて明示されている。 SOC2レポートにおいて、主要コンポーネントの冗長化による顧客影響の最小化、データの自動複製による影響の最小化、ハードウェアとシステム障害検知時のデータ自動リストアについて記載されていることを確認した。	文献[11] P11 データの冗長化 文献[13] キャパシティと耐久性を常に制御できる状態に	SOC2レポート DS-6, DS-7, DS-14	―	利用者がAzure上で構築するアプリケーションやサービスの障害の早期発見及び早期回復については、利用者が対策する必要がある。 仮想マシンを冗長化する場合は、Azureの冗長構成機能を用いて利用者が実施する必要がある。 仮想マシンの状態やデータのバックアップの作成は、Azureのレプリケーション機能を用いて利用者が実施する必要がある。 ホット・フェールオーバー機能を用いるためには、利用者が第2のストレージアカウントを作成して構成する必要がある。
実107	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実108	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実109	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実110	利用者は、要件に応じて、カード取引監視方法を明確にする必要があります。	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実111	対象外	対象外	―	―	―	―	カードの偽造防止対策が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実112	利用者は、要件に応じて、インターネット・モバイルサービスの不正使用防止機能を設ける必要があります。	対象外	―	―	―	―	利用者は、オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設ける必要がある。 仮想マシン(VM)ロールの場合、お客様は仮想マシンを評価して更新する責任を負う。 加えて、下記のいずれについても、SI事業者あるいは利用者が対応する必要がある。 ・通常とは異なる取引が行われた時等、取引のリスクに応じた更なる本人確認 ・利用者機器（パソコンなど）のシステム環境チェック機能 ・取引内容をモニタリングし、疑わしい取引や異常を検知した場合は取引を一時的に中断する仕組み ・ハードウェアトークン等を利用したトランザクション認証
実113	利用者は、要件に応じて、利用者自身が使用状態を確認する機能を実装する必要があります。	対象外	―	―	―	―	利用者は、利用者自身が使用状態を確認する機能を設ける必要がある。
実114	利用者は、要件に応じて、インターネット・モバイルサービスの安全対策に関する情報開示を実施する必要があります。	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実115	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。

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	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116	利用者は、要件に応じて、インターネット・モバイルサービスの運用管理方法を明確にする必要があります。	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実117	利用者は、要件に応じて、本人確認機能を実装します。	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実118	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実119	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実120	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実121	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実122	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実123	対象外	対象外	―	―	―	―	利用者がAzure上で構築する環境については、利用者が対策する必要がある。
実124	利用者は、要件に応じて、遠隔制御機能を実装します。	対象外	―	―	―	―	―
実125	対象外	対象外	―	―	―	―	―
実126	対象外	対象外	―	―	―	―	―
実127	対象外	対象外	―	―	―	―	―
実128	対象外	対象外	―	―	―	―	―
実129	対象外	対象外	―	―	―	―	―
実130	対象外	対象外	―	―	―	―	―
実131	対象外	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	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132	対象外	対象外	―	―	―	―	―
実133	対象外	対象外	―	―	―	―	―
実134	対象外	対象外	―	―	―	―	―
実135	対象外	対象外	―	―	―	―	―
実136	対象外	対象外	―	―	―	―	利用者は、エンドユーザに対して、媒体等の紛失/盗難/破損等によりエンドユーザが被る可能性のある損害及びこれらに対するエンドユーザの責任について、明示する必要がある。
実137	対象外	対象外	―	―	―	―	電子的価値の保護機能が必要なアプリケーションやサービスについては、利用者が対策する必要がある。
実138	利用者は、要件に応じて、Microsoft Azure上に利用者が構築するメールサービスについての運用方針を明確にする必要があります。 なお、Microsoft Azureサービスとしてはメール機能を提供していません。	対象外	―	―	―	―	Azure上に利用者により構築するメールサービスについての運用方針については、利用者により明確にする必要がある。
実139	利用者は、要件に応じて、電子メール送受信、ホームページ閲覧等の不正使用防止機能に関する対応を実施する必要があります。	対象外	―	―	―	―	業務目的以外の電子メールの送受信やホームページの閲覧等については、利用者が対策する必要がある。
実140	利用者は、実装するアプリケーションにおいて生体認証が必要な場合、生体認証情報の管理を実施する必要があります。	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	利用者は、実装するアプリケーションにおいて生体認証が必要な場合、生体認証情報の管理を実施する必要があります。	対象外	―	―	―	―	利用者がAzure上で構築するアプリケーションやサービスで独自に生体認証を用いる場合は、利用者が適切な対策を行う必要がある。
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、電気的干渉、停電、電気的な乱れ（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。	―

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	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、バッチ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	―	―	―
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離隔された区画内（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離隔された区画内（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、消化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、消化設備を有している。	―
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。	―

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	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。	―
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、内装等の防炎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。 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。	―

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	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。	―
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。	―

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	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は不燃材及び防炎性能を有するものを使用しており、防炎対策が施されていると考えられる。	―	―	内装等は不燃材及び防炎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。	―
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。	―

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	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を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	FISC安全対策基準（第9版）に対するMicrosoftの見解	Microsoft Azure における対応					SI事業者・利用者で必要な対応
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	
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。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。	―

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	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。	―
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。	―

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	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。	―
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（SA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。	―

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	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	―	―	―
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	―	―	―	―	―

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	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	―	―	―	―	―
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	―	―	―	―	―

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	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	―	―	―	―	―
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	―	―	―	―	―

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	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	―	―	―	―	―
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	―	―	―	―	―

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	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137	データセンタ以外に対する要件のため	対象外	―	―	―	―	―
監1	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。 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。 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。	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	FISC安全対策基準（第９版改訂）に対するMicrosoftの見解	Microsoft Azure における対応					SI事業者・利用者で必要な対応
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	
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、使用権等の権利の帰属 (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4	マイクロソフトは128 ビット以上の暗号化キーを使用する TLS により、Microsoft Azure データセンター間および対象のデータセンターのクラスター間で送信される制御メッセージを保護します。エンドユーザーとユーザーの仮想マシン間のトラフィックを暗号化する事も可能です。 Azure Portalなどの公開されている Azureサービス管理機能に接続するときには、HTTPSによる接続を行います。 利用者は、Microsoft Azure 上で実装するアプリケーションの通信に対して、データの保護に関する対応を実施する必要があります。	適合可能	文献[01]に、Azure Portalへのアクセスは TLS1.2により暗号化されていること、データセンター内通信及びデータセンター間通信がTLSにより暗号化されている旨が明示されている。 SOC2レポートにおいて、Microsoft Azureの内部通信、管理ポータルの通信の暗号化が記載されていることを確認した。	文献[01] P25 DSI-03: Data Security & Information Lifecycle Management – e-Commerce Transactions	SOC2レポート DS-2, DS-3	―	利用者がAzure上で構築するアプリケーションやサービスで重要なデータを伝送する場合は、利用者が適切な暗号技術を用いるなどの対策を行う必要がある。
実142	利用者は、Microsoft Azure 上でQR コード決済機能を含むアプリケーションを実装する際の安全対策を実施する必要があります。	対象外	–	–	–	–	利用者は、Azure上でQRコード決済機能を含むアプリケーションを実装する場合、安全対策の措置を講ずる必要がある。
実143	利用者は、Microsoft Azure 上でQR コード決済機能を含むアプリケーションを実装する際の顧客保護の措置を実施する必要があります。	対象外	–	–	–	–	利用者は、Azure上でQRコード決済機能を含むアプリケーションを実装する場合、顧客保護の措置を講ずる必要がある。
実144	利用者は、Microsoft Azure 上でQR コード決済機能を含むアプリケーションを実装する際、利用上の留意事項を顧客に明示する必要があります。	対象外	–	–	–	–	利用者は、Azure上でQRコード決済機能を含むアプリケーションを実装する場合、利用上の留意事項を顧客に明示する措置を講ずる必要がある。