地方自治体向け
『Office 365』対応セキュリティリファレンス

2016年6月15日
Version 1.0

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

更新日	版番号	改版内容
2016年6月15日	Version 1.0	初版

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.1.1	6 情報セキュリティのための組織	6.1 内部組織	6.1.1 情報セキュリティに対する経営陣の責任	経営陣は、情報セキュリティの責任に関する明りょうな方向づけ、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持することが望ましい。	経営陣は、クラウドサービスの利用における情報セキュリティについて組織を横断する役割及び責任を明確にし、組織全体としての責任者を割当て、承認することが望ましい。	—	クラウドサービスを利用した場合でも、情報セキュリティ管理全般に関するクラウド利用者の経営陣の責任は変化しない。しかしながら、クラウドサービスの内容（例えば、システム構成、契約内容など）を把握し、どのようなリスクが伴うのかについては、クラウド利用者の経営陣は十分に理解しておくことが期待される。クラウドサービスの利用における責任の所在が明確になるように、クラウド利用者の経営陣は情報システム環境の全体像を把握しておくことが期待される。	—	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services（GFS）内のOnline Services Security and Compliance（OSSC）チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
6.1.2	6 情報セキュリティのための組織	6.1 内部組織	6.1.2 情報セキュリティの調整	情報セキュリティ活動は、組織の中の、関連する役割及び職務機能をもつ様々な部署の代表が、調整することが望ましい。	クラウド利用者は、クラウドサービス利用における組織の責任者を明確にし、情報セキュリティ委員会などの調整活動に参加させることが望ましい。クラウド利用者は、クラウドサービス利用における責任者を定め、情報セキュリティ管理者一覧などに追記することが望ましい。クラウドサービス利用におけるクラウド利用者の責任者は経営陣（又は情報セキュリティ委員会など）によって承認されることが望ましい。	—	クラウドサービスの利用においては、情報システムの構築や利用に関する契約などが多者にわたる可能性があり、責任者を明確に決めて管理を行う必要がある。また、クラウドサービスに関する様々な情報を集約し様々な判断をする必要があるため、クラウドサービス利用における責任者は情報セキュリティ委員会などの組織の調整活動に参加することが期待される。	—	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services（GFS）内のOnline Services Security and Compliance（OSSC）チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
6.1.3	6 情報セキュリティのための組織	6.1 内部組織	6.1.3 情報セキュリティ責任の割当て	すべての情報セキュリティ責任を、明確に定めることが望ましい。	クラウド利用者は、クラウドサービス利用における情報セキュリティに関するクラウド利用者及びクラウド事業者の責任分界を確認することが望ましい。クラウド利用者は、情報セキュリティ責任について、クラウド利用者だけでは対応できない内容を明確にすることが望ましい。 クラウド利用者は、クラウド事業者の問合わせ窓口を確認し、窓口情報を最新に保つとともに、クラウドサービス利用におけるリスクを識別・管理することが望ましい。	クラウド事業者は、クラウド利用者、クラウド事業者及びインフラ事業者の間の責任分界を明確にし、 文書化することが望ましい。 クラウド事業者は、クラウドサービスの情報セキュリティに関する窓口を明確にし、開示することが望ましい。	クラウドサービスにおいては、情報セキュリティに関する一部の業務がクラウド事業者に委任される。 しかしながら、情報セキュリティに関する全体の責任はクラウド利用者に残ったままであるため、クラウド事業者が情報セキュリティに関する業務を正しく実行していることを、クラウド利用者が判断することが期待される。また、個人が情報セキュリティに責任をもつ領域がクラウドサービスによって変化をする場合（例えば、ID 管理が一元化できずにパスワードの変更を個人が配慮して行わなければならないなど）には、クラウド利用者はその責任範囲を明確にし、クラウドサービスの利用者に伝えなければならない。 多くの場合には情報セキュリティ責任者は組織のすべての情報セキュリティに責任をもつが、クラウドサービスは多様性を有しており、これらのすべてを把握することは困難であることが想定される。このような場合は、情報セキュリティ責任者の補助としてクラウドセキュリティ責任者又は担当者を置くことを検討する必要がある。 データの管理責任、アクセス制御及びインフラ管理などに関する役割及び責任の定義が曖昧な場合、ビジネス上の若しくは法的な問題が引き起こされる恐れがある。	—	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[65]では、セキュリティの一般規定において、マイクロソフトが講じているセキュリティ対策とOSTにおけるセキュリティに関する確約事項が、顧客データのセキュリティに関するマイクロソフトの唯一の責任であると明記されていることを確認した。 文献[08]では、マイクロソフト・クラウド・インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services（GFS）内のOnline Services Security and Compliance（OSSC）チームの存在を明示している。 文献[01]では、データガバナンスの一環として、Microsoft Online Services サービスの提供に使用される資産の所有者を割り当てるポリシー、データの安全な廃棄、非公開データの非運用環境への移動またはコピーの禁止、情報漏えいを防止する論理制御と物理制御について明示されている。加えて、資産に対するアクセス権を資産の所有者の承認を得たうえで付与されること、定期的なアクセスの確認や監査を行うこと、内部または外部の組織とのデータ交換手順の遵行、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスの制限も明示されている。 さらに、文献[19]では、Microsoft Operations Centersにおいて、データ管理も含めて全体の管理を実施していることが明示されている。 加えて、インタビューの結果、管理責任者を中心とした社内ミーティングが行われていることから、管理体制が整備されていると考えられる。	要NDA	文献[65](OST) 文献[08]「Online Services Security and Compliance チーム」 文献[01]「DG-01：データガバナンス－所有権／管理者責任」 文献[01]「DG-04：データガバナンス－保持ポリシー」 文献[01]「DG-05：データガバナンス－安全な廃棄」 文献[01]「DG-06：データガバナンス－非運用データ」 文献[01]「DG-07：データガバナンス－情報漏えい」 文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-09：情報セキュリティ－ユーザーアクセスの無効化」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「SA-03：セキュリティアーキテクチャ－データのセキュリティ／整合性」 文献[19]「Incident Management Model」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
6.1.4	6 情報セキュリティのための組織	6.1 内部組織	6.1.4 情報処理設備の認可プロセス	新しい情報処理設備に対する経営陣による認可プロセスを定め、実施することが望ましい。	クラウド利用者は、新たに利用する機器などを経営陣が認可するプロセスに、クラウドサービスを含めることが望ましい。クラウド利用者は、クラウドサービスの利用認可プロセスを策定することが望ましい。 クラウド利用者は、クラウドサービスの利用認可プロセスを文書化することが望ましい。 クラウドサービスの利用認可プロセスは、クラウド利用者の経営陣によって承認されることが望ましい。また、セキュリティ要求事項を満たしていることを確認するために情報セキュリティ委員会からも承認を得ることが望ましい。	クラウド事業者は、クラウド利用者がクラウドサービスの受入れを行うために必要な資料を作成し、提供することが望ましい。クラウド事業者は、SLA など、サービス開始前の合意事項を明確にすることが望ましい。	IaaS やPaaS の利用においては、既存の情報システム調達及び構築の標準や手順が適用可能な場合がある。SaaS では、アプリケーションのカスタマイズがクラウド利用者にとって容易ではないために、これまでの認可プロセスの標準に合致しない場合もある。その場合は、受入れについての標準や手順を再度検討し、標準の変更又は特例措置の検討を行う必要がある。	—	エンタープライズ向けクラウドサービスで使用するソフトウェアは、マイクロソフトが長年に渡り自社設置用として開発、販売してきたソフトウェア製品を基に、クラウドサービス用として改善、改良したもので、基となった自社設置用ソフトウェア、クラウドサービスの双方において、世界各国で様々な業界・業種のあらゆる規模のお客様に利用されています。 マイクロソフトは世界最大のソフトウェア企業であり、2014年版フォーチューン500でも34位にランクされる優良企業と自負しております。 Office 365は域内の複数のデータセンターを使用した冗長化構成を取っており、万一のデータセンター被災の際でも、別のデータセンターを使用してサービス提供が継続できる設計・運用としています。 暗号化有無を含むサービス仕様についてはOffice 365製品サイトで仕様を開示しています。 またトラストセンターと呼ばれる専用サイトで、可用性、透明性、セキュリティ、信頼性に関する情報を公開しています。 また、透明性レポートとして世界各国の政府機関からの情報開示請求に関するデータも開示しています。 管理者のユーザー識別情報は、米国、アイルランド ダブリン、オランダ アムステルダム、シンガポール、香港のマイクロソフト データセンターに保存されます。 お客様データについては、日本で契約するお客様のデータは日本で保管されます。 サービスの標準機能またはツールを使用して仮想マシンをクラウドとオンプレミスの間で移動することや、業界標準のデータ形式によるデータ移行が可能です。 上記すべてのサービスで、APIを使用したシステム間連携も可能となっています。 一般的なお客様への対応を想定した標準的なサポートメニューが付属しています。 万一セキュリティインシデントが発生した場合、マイクロソフト側に起因するものである場合、速やかにお客様に連絡することとしており、このことは契約書の記載事項となっています。お客様側に起因するものである場合、お客様コンテンツの保全やログ参照をはじめとする各種機能によってお客様側が調査を行うことが可能です。標準的なサポートメニューおよび有償のサポートプログラムのいずれも日本語での対応が可能です。 損害賠償は、お客様が直近12か月間にマイクロソフトに対して支払義務を負ったサービス利用料金を上限とする直接損害に限定しています お客様は、お客様コンテンツの所有者であり、いつでもコンテンツをダウンロードし、他のシステムで使用することができます。マイクロソフトまたはマイクロソフトのパートナーはそのためのツールを継続的に提供し続けます。 契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。 お客様コンテンツの内容を知りえないため、個人情報保護法における個人情報の委託先に該当しないものと考えておりますが、実務指針に書かれた内容には準拠可能と考えています。 費用およびお支払い条件はライセンスを購入先となる販売店にご確認ください。	適合可能	文献[65]および文献[66]では、利用業務固有のリスクを除き、提供事業者として安全確保に関する項目を盛り込んだ契約書が準備されていることを確認した。 インタビューの結果、標準の契約条件やSLAに含まれていない事項については、個別サポート契約の締結により補われる場合もあることを確認した。	要NDA	文献[65](OST) 文献[66](SLA)	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
6.1.5	6 情報セキュリティのための組織	6.1 内部組織	秘密保持契約	情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューすることが望ましい。	クラウド利用者は、情報保護に対する組織の必要を反映する秘密保持契約をクラウド事業者と締結することが望ましい。クラウド利用者は、クラウド事業者との契約に必要な秘密保持契約の内容が含まれていることを確認することが望ましい。もし必要な事項が含まれていない場合は、別途、秘密保持契約を締結することが望ましい。クラウド利用者は、クラウド事業者との秘密保持契約に「保護される情報の定義」が記載されていることを確認することが望ましい。	クラウド事業者は、クラウド利用者との契約時には秘密保持契約を締結することが望ましい。	クラウドサービスの利用においてはコンピュータ資源をネットワーク上（多くの場合はクラウド事業者のデータセンター）に配置しているが、データの所在などをクラウド利用者が特定することは技術的に難しい。クラウド利用者がすべての情報を適切に管理するためにも、重要な情報を双方が正しく認識し、協力しあうことが期待される。	—	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、“情報セキュリティの意識向上、教育、およびトレーニング” が規定されています。	適合可能	文献[01]では、マイクロソフトの法務部および人事部では、機密保持契約の締結および履行を定めたポリシーと手順を管理していることを確認した。 文献[65]では、標準のプライバシーとセキュリティの条件が定められていることを確認した。	公開文書	文献[01] 文献[65](OST)	—	—	—	—

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応								
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.1.6	6 情報セキュリティのための組織	6.1 内部組織	6.1.6 関係当局との連絡	関係当局との適切な連絡体制を維持することが望ましい。	クラウド利用者は、クラウド事業者の監督官庁、管轄裁判所、関連団体、相談窓口などを確認することが望ましい。クラウド利用者は、利用するクラウド事業者の監督官庁、関連団体を調査し、事故発生時の連絡リストに追加することが望ましい。	クラウド事業者は、提供するクラウドサービスの情報セキュリティに関して関連する監督官庁などを明確にし、開示することが望ましい。クラウド事業者は、個人情報の保護に関して監督官庁などを明確にし、開示することが望ましい。	クラウド利用者が複数のクラウド事業者と個別に契約し、複数のクラウドサービスを組み合わせて利用する場合には、それぞれのクラウド事業者の責任を明確にする必要がある。特に、様々なクラウドサービスを利用して一つのクラウドサービスとして提供する場合には、責任の切り分けが難しい場合もあるが、利用の前に責任分界点を明確にし、障害などに対応できるようにすることが期待される。	–	日本でご契約のお客様は日本法を準拠法とし、東京地方裁判所を管轄裁判所としています	適合可能	インタビュー及びNDA文書で確認したところ、日本でMicrosoft Online Servicesの契約をする場合、準拠法は日本法であることが確認できた。 また、インタビューで確認したところ、関係当局に対して監査は対応できないが、調査への協力は行われることが確認できた。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自らも関係当局との適切な連絡体制を維持する必要がある。
6.1.7	6 情報セキュリティのための組織	6.1 内部組織	6.1.7 専門組織との連絡	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持することが望ましい。	–	–	クラウド利用者及びクラウド事業者は、次のような組織などと調査し、クラウドサービスに関する情報収集の対象とすることが期待される。 a) クラウドサービスを専門とする、又はクラウドサービスに関連する団体や組織 b) クラウドサービスの事業者団体 c) クラウドサービスに関連する省庁や団体 d) クラウドサービス関連のニュースソース クラウドサービスでは、IaaS、PaaS、SaaSがサービスを共有して構成されている場合がある。例えば、複数のSaaS 事業者が同じPaaS やIaaS を利用していたり、一つのSaaS 事業者が複数のPaaS を利用したりしている場合などがそれにあたる。この場合、クラウド事業者は、どのクラウド事業者のどのサービスを利用しているのかをクラウド利用者に開示することが望ましい。 事前にこうした情報が開示されていれば、クラウド利用者は、あらかじめクラウドサービスやクラウド事業者の事故などが発生したときの影響と対策を検討することが可能になる。	–	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[05]では、マイクロソフトがセキュリティコミュニティと連携し、セキュリティガイダンスの提供等の対応が明示されている。	公開文書	文献[05] Microsoft Azureのトラストセキュリティセンター	–	–	–	利用者は、自らも情報セキュリティに関する組織との適切な連絡体制を維持することが望ましい。
6.1.8	6 情報セキュリティのための組織	6.1 内部組織	6.1.8 情報セキュリティの独立したレビュー	情報セキュリティ及びその実施のマネジメントに対する組織の取組み（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）について、あらかじめ計画した間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施することが望ましい。	クラウド利用者は、情報セキュリティに関するマネジメントレビューにおいて、組織が保有する情報システムと同様に、クラウドサービスに関する事項を追加することが望ましい。クラウド利用者は、情報セキュリティに関するマネジメントレビューの計画書にクラウドサービスを追加することが望ましい。クラウド利用者は、リスクアセスメントに基づき、クラウドサービスを情報セキュリティ監査の対象に追加することが望ましい。	–	クラウド利用者が、マネジメントレビューのための情報を提供する場合、クラウド事業者からクラウドサービスに関する情報を定期的に入手することが難しい場合がある。特にマルチテナントでクラウドサービスが展開されているクラウドサービスを利用している場合には、ログから得られる情報をクラウド事業者から提供してもらうために想定以上に時間を要する場合がある。そのため、事前にマネジメントレビューに必要な情報を精査し、それらの情報を得ることが可能であるかどうか、可能である場合は、必要な期間も併せてクラウド事業者に確認することが期待される。	–	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[01]では、Microsoft Online Services において情報セキュリティポリシーが定期的に確認及び更新されることが明示されている。 さらに文献[03]では、各ポリシー、標準、およびベースラインが年に 1 回のベースで見直されることが明示されている。	公開文書	文献[01]「IS-05：情報セキュリティ・ポリシーの確認」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、情報セキュリティに関するマネジメントレビューにおいて、組織が保有する情報システムと同様に、Office365に関する事項を追加することが望ましい。
6.2.1	6 情報セキュリティのための組織	6.2 外部組織	6.2.1 外部組織に関係したリスクの識別	外部組織がかかわる業務プロセスのの、組織の情報及び情報処理施設に対するリスクを識別し、また、外部組織にアクセスを許可する前に適切な管理策を実施することが望ましい。	クラウド利用者は、外部組織がかかわる業務プロセスの一つとしてクラウドサービスの利用を考慮することが望ましい。 クラウド利用者は、業務プロセスへのクラウドサービスの関与と影響を特定することが望ましい。 クラウド利用者は、クラウドサービスの利用により生じる情報セキュリティに対するリスクを識別・検討し、必要に応じてクラウドサービスの利用を開始する前に管理策を実施することが望ましい。	クラウド事業者は、クラウド利用者の情報セキュリティに重大な影響を与えると考えられるリスクを定義し、クラウド利用者にその情報を提供することが望ましい。 クラウド事業者がクラウド利用者と合意した場合、クラウド事業者は、クラウドサービスにおける情報セキュリティ対策や作業状況に関する情報（例えば、データの完全消去作業の実施報告書）を提供することが望ましい。	クラウド事業者が開示する情報セキュリティ対策の内容は、多くの場合は限定的、抽象的なものであることに留意する。リスクを特定することが困難な場合に、クラウド利用者が実施できる有効な管理策の一つに情報の暗号化がある。 クラウド利用者は、組織の一般的な情報セキュリティリスクに加え、クラウド固有のリスクを情報セキュリティ リスクアセスメントプロセスの入力として含め、オンプレミスの情報システムとクラウドサービスとの間でリスクの違いを評価することが望ましい。なお、クラウドサービスにおいて考慮すべきリスクには次のようなものがある。 a) クラウド利用者の情報は、クラウド事業者が所有するハードウェアに格納されるため、クラウド利用者は直接管理することができない。 b) クラウド事業者は、他のクラウド事業者が提供するクラウドサービスを利用してクラウドサービスを提供している場合があり、責任分界が曖昧である恐れがある。 c) 他のクラウド利用者と同一のコンピュータ環境を共有する場合があり、他のクラウド利用者の利用する環境との論理的な分割が適切に行われない恐れがある。 d) 一般的に、クラウドサービスの利用終了後、サービス利用中に使用されていたシステムリソースは再利用されるため、サービス利用終了後のデータ消去が適切に行われない場合、他のクラウド利用者によってデータがアクセスされる恐れがある。 情報セキュリティリスクは、クラウドサービスの利用によって高まる場合もあれば、低下する場合もある。クラウドサービスの利用においては、情報セキュリティ管理策の可視性及び情報セキュリティ管理レベルの達成度が限定されること、及び、リスクの識別が困難である傾向があることに留意する必要がある。	–	ビジネスの影響分析が適切な間隔で実行され、確認されます。次のような分析を行います。 ・ Microsoft Onine Services ビジネス環境およびプロセスに関連する脅威の特定 ・ 可能性のある影響と予想される損害を含んだ、特定した脅威の評価 ・ 特定された重大な脅威を軽減し、ビジネス プロセスを回復するための役員により承認された戦略 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（具体的には付属文書 A の項 14.1）で、“ビジネス継続性管理における情報セキュリティの側面” が規定されています。	適合可能	文献[01]では、Microsoft Online Services の継続性プログラムを主導するフレームワークに「文書化された手順による継続性の計画」があること、復元計画は定期的に検証されることが明示されている。 また、インタビュー等を通じて、委託先が契約通りに委託業務を遂行できないリスクはないことを確認した。 文献[74]を確認したところ、情報開示姿勢について、マイクロソフト社の情報開示方針及び開示内容が確認できた。また、リスク管理に直結する事項についても情報を開示していることが確認できた	要NDA	文献[01]「RS-03：復元 – ビジネス継続性の計画」RS-04：復元 – ビジネス継続性のテスト」 文献[74]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	利用者は、Office365を利用する業務の特性に応じてリスク分析・評価する必要がある。
6.2.2	6 情報セキュリティのための組織	6.2 外部組織	6.2.2 顧客対応におけるセキュリティ	顧客に組織の情報又は資産へのアクセスを許す前に、明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。	クラウド利用者が顧客に組織の情報又は資産へのアクセスを許可するために明確にしていたセキュリティ要求事項について、クラウドサービスを利用することによって変化するセキュリティ要求事項を明確にし、明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。 クラウド利用者がセキュリティ要求事項の明確化を行うにあたっては、クラウドサービスの利用に伴い生じる顧客の作業及びリスクを識別することが望ましい。	クラウド利用者が、クラウドサービスの利用に際してセキュリティ要求事項の順守状況を確認できるよう、クラウド事業者は、サービスの詳細に関する情報を提供することが望ましい。	自らの顧客に内部統制報告の責任を負うクラウド利用者は、顧客に対して内部統制の報告を行うにあたり、クラウド事業者の情報セキュリティ監査報告書の入手が必要か否か、及び入手が可能かについてクラウドサービスの利用を開始する前に検討しておく必要がある。 クラウド利用者は、次の点について顧客に明示しておくことが期待される。 a) 個人情報保護法などの法令に基づき、利用者の同意なくクラウドコンピューティング環境上の情報への顧客のアクセスが制限される場合がある。 b) クラウド事業者は、他のクラウド利用者に情報が漏えいするリスクを完全に排除できない場合であっても、クラウド利用者に対してアクセスを付与する場合がある。	–	トラストセンターと呼ばれる専用サイトで、可用性、透明性、セキュリティ、信頼性に関する情報を公開しています。 また、透明性レポートとして世界各国の政府機関からの情報開示請求に関するデータも開示しています。	適合可能	文献[66]を確認したところ、サービスの可用性・データの安全性・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について、マイクロソフト社のエンタープライズ向けクラウドサービスの状況が確認できた。 文献[74]を確認したところ、内部統制やリスク管理等に関する状況、外部監査の受検や各種公的認証の取得状況、組織体制について、再委託先管理を含む内部統制及びリスク管理の状況が確認できた。またISO 27001, SOC 1 and SOC 2を含む数多くの外部監査受検、公的認証の取得状況が確認できた。 文献[74]を確認したところ、情報開示姿勢について、マイクロソフト社の情報開示方針及び開示内容が確認できた。また、リスク管理に直結する事項についても情報を開示していることが確認できた	公開文書	文献[66] 文献[74]	–	–	–	利用者は、Office365へのセキュリティ要求事項を明確化し、自組織のセキュリティ要求事項をすべて満たしているか、契約に含有されているかを確認することが望ましい。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
6.2.3	6 情報セキュリティのための組織	6.2 外部組織	6.2.3 第三者との契約におけるセキュリティ	組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい。	クラウド利用者は，組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約に，クラウドサービスの利用契約が含まれるものとして考えることが望ましい。 クラウド利用者は，クラウドサービスへのセキュリティ要求事項を明確化し，自組織のセキュリティ要求事項をすべて満たしているか，契約に含有されているかを確認する事が望ましい。また，クラウド事業者との契約を比較した結果が経営陣（又は情報セキュリティ委員会）に承認されていることが望ましい。	—	—	—	—	エンタープライズ向けクラウドサービスで使用するソフトウェアは、マイクロソフトが長年に渡り自社設置用として開発、販売してきたソフトウェア製品を基に、クラウドサービス用として改善、改良したものです。基となった自社設置用ソフトウェア、クラウドサービスの双方において、世界各国で様々な業界・業種のあらゆる規模のお客様に利用されています。 マイクロソフトは世界最大のソフトウェア企業であり、2014年版フォーチューン500でも34位にランクされる優良企業と自負しております。 Office 365は域内の複数のデータセンターを使用した冗長化構成を取っており、万一のデータセンター被災の際でも、別のデータセンターを使用してサービス提供が継続できる設計・運用としています。 暗号化有無を含むサービス仕様についてはOffice 365製品サイトで仕様を開示しています。 またトラストセンターと呼ばれる専用サイトで、可用性、透明性、セキュリティ、信頼性に関する情報を公開しています。 また、透明性レポートとして世界各国の政府機関からの情報開示請求に関するデータも開示しています。 管理者のユーザー識別情報は、米国、アイルランド ダブリン、オランダ アムステルダム、シンガポール、香港のマイクロソフト データセンターに保存されます。 お客様データについては、米国（アイオワ州、バージニア州、イリノイ州、テキサス州、カリフォルニア州）、アイルランド（ダブリン）、オランダ（アムステルダム）、シンガポール、香港、日本（東京、埼玉、大阪）、ブラジル サンパウロ、オーストラリア（NSW、ビクトリア）のデータセンターを選択して利用いただけます。 （一部のデータセンターの利用は購入条件が設定されていることがあります） システムセンター（System Center）を使用して仮想マシンをクラウドとオンプレミスの間で移動することや、業界標準のデータ形式によるデータ移行が可能です。 上記すべてのサービスで、APIを使用したシステム間連携も可能となっています。 一般的なお客様への対応を想定した標準的なサポートメニューが付属しています。 万一セキュリティインシデントが発生した場合、マイクロソフト側に起因するものである場合、速やかにお客様に連絡することとしており、このことは契約書の記載事項となっています。お客様側に起因するものである場合、お客様コンテンツの保全やログ参照をはじめとする各種機能によってお客様側が調査を行うことが可能です。標準的なサポートメニューおよび有償のサポートプログラムのいずれも日本語での対応が可能です。 損害賠償は、お客様が直近12か月間にマイクロソフトに対して支払義務を負ったサービス利用料金を上限とする直接損害に限定しています お客様は、お客様コンテンツの所有者であり、いつでもコンテンツをダウンロードし、他のシステムで使用することができます。マイクロソフトまたはマイクロソフトのパートナーはそのためのツールを継続的に提供し続けます。 契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。 お客様コンテンツの内容を知りえないため、個人情報保護法における個人情報の委託先に該当しないものと考えておりますが、実務指針に書かれた内容には準拠可能と考えています。 費用およびお支払い条件はライセンスを購入先となる販売店にご確認ください。	適合可能	文献[65]および文献[66]では、利用業務固有のリスクを除き、提供事業者として安全確保に関する項目を盛り込んだ契約書が準備されていることを確認した。 インタビューの結果、標準の契約条件やSLAに含まれていない事項については、個別サポート契約の締結により補われる場合もあることを確認した。	要NDA	文献[65]（OST） 文献[66]（SLA）	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、Office365へのセキュリティ要求事項を明確化し、自組織のセキュリティ要求事項をすべて満たしているか、契約に含有されているかを確認することが望ましい。
7.1.1	7 資産の管理	7.1 資産に対する責任	7.1.1 資産目録	すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。	クラウド利用者は，クラウドコンピューティング環境にある組織の資産を資産管理の適用範囲に含めることが望ましい。 クラウド利用者は，資産目録にクラウドサービス名及びクラウド事業者名を追加することが望ましい。 クラウド利用者は，クラウド利用者による資産管理を支援する機能がクラウドサービスに付帯するかを確認することが望ましい。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産に関する資産目録の一覧を取得できる機能をクラウド利用者に提供することが望ましい。	クラウド事業者は大規模なIaaS の上でPaaS やSaaS を展開している場合があり，クラウド利用者がクラウドサービスに関連するシステムのすべてを資産目録に詳細に記載することは困難である。また，データ管理のために様々なメタデータ（データに関する情報）などが付与されており，これらのすべてをクラウド利用者が管理することも困難である。しかしながら，クラウド利用者は，自らがクラウドコンピューティング環境においたデータやプログラムなどを資産目録に記載することは可能であり，これらをもれなく記載することが期待される。 クラウドサービス環境にあるクラウド利用者の資産には，次のようなものがある。 a) 業務上の情報 b) 仮想化された装置 c) 仮想化されたストレージ d) ソフトウェア クラウド利用者の資産の種類はa，クラウドサービスに応じて多岐にわたる。例えば，SaaS 事業者が，提供するSaaS のインフラにIaaS を利用している場合，SaaS 事業者はクラウド利用者であり，SaaS において容量・能力及び資源などの監視・調整に使用するソフトウェアは，IaaS 事業者から見ると，自社の提供するIaaS サービス上にあるクラウド利用者の資産と解される場合がある。	—	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。 Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、“資産管理” が規定されています。	適合可能	文献[01]では、Microsoft Online Services サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services サービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 「DG-01：データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Office365上で作成される自身のデータを識別し、資産目録などで適切に管理する必要がある。
7.1.2	7 資産の管理	7.1 資産に対する責任	7.1.2 資産の管理責任者	情報及び情報処理施設と関連する資産のすべてについて，組織の中に，その管理責任者を指定することが望ましい。	クラウド利用者は，資産目録の管理責任者の項目にクラウドサービスに関連する項目を追加することが望ましい。 資産の管理責任者は，クラウドコンピューティング環境上の資産に関して次の責任をもつことが望ましい。 a) 情報及び情報処理に関連する資産が適切に分類されていることを確実にする。 b) 複数のクラウドサービスを連携し情報処理を行う場合には，適切な処理を管理するための方針，プロセス及び手順を定め，定期的に見直す。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の資産の責任者を明確にし，顧客対応のエスカレーションプロセスに追加することが望ましい。		—	Microsoft Online Services では、Window Azure サービスの提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。資産所有者は、その資産に関する情報を常に最新にしておく責任を担います。お客様は、自身のデータの管財人としての責任を担います。 ISO 27001 規格（具体的には付属文書 A の項 6.1.3 および 7.1.2）で、“情報セキュリティの責任と資産の所有権の割り当て” が規定されています。	適合可能	文献[01]では、Microsoft Online Services サービスの提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services サービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 「DG-01：データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Office365上で作成される自身のデータを識別し、資産目録などで適切に管理する必要がある。
7.1.3	7 資産の管理	7.1 資産に対する責任	7.1.3 資産利用の許容範囲	情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。	クラウド利用者は，利用するクラウドサービスごとに，どの資産が利用可能か，リスクアセスメントを行い，利用の許容範囲を明確にすることが望ましい。クラウド利用者は，クラウドサービスごとに，資産の利用可能性について検討することが望ましい。	—	—	—	（利用者側で対応する事項のため対象外）	対象外	—	—	—	—	—	—	利用者は、Office365上でどのデータ（資産）が利用可能か、リスクアセスメントを行い、利用の許容範囲を明確にする必要がある。
7.2.1	7 資産の管理	7.2 情報の分類	7.2.1 分類の指針	情報は，組織に対しての価値，法的要求事項，取扱いに慎重を要する度合い及び重要性の観点から分類することが望ましい。	クラウド利用者は，情報分類の指針にクラウドサービスを考慮した分類項目を追加することが望ましい。	クラウド事業者は，データの分類項目を明示することが望ましい。クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報がどのように分離されて管理されているかを明確にし，開示することが望ましい。	データの分類項目の例として，以下のようなものがある。 －データのタイプ －データ源の管轄裁判所 －コンテキスト（背景や位置づけなど） －法的制約 －契約上の制約 －価値，機微性 －組織における重要度 －第三者による不正な防止する義務 －許可されない開示や誤用に関する事項など	—	Microsoft Online Services の規格では、複数の該当するセキュリティ分類カテゴリーに資産を分類し、その後で一連の標準的なセキュリティおよびプライバシー属性を実装するためのガイダンスを用意しています。 ISO 27001 規格（具体的には付属文書 A の項 7.2）で、“情報の分類” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Online Services の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が実装されることが明示されている。	公開文書	文献[01]	—	—	—	利用者は、Office365上で作成される自身のデータを識別し、資産目録などで適切に分類する必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
7.2.2	7 資産の管理	7.1 資産に対する責任	7.2.2 情報のラベル付け及び取扱い	情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。	クラウド利用者は，クラウドサービスで利用する資産についてもラベル付けやマーキングができる仕組みを作ることが望ましい。クラウド利用者は，ラベル付けやマーキングをクラウドサービスの利用者が実施できるように手順書を作成することが望ましい。	クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を分類するためにフォルダ分類やラベル付け機能を提供することが望ましい。クラウド事業者は，クラウド利用者との合意に基づき，ラベル付け機能について次の情報を提供することが望ましい。 a) ラベル付けを行うための機能 b) ラベル付けのカスタマイズを行うための機能 クラウド事業者は，クラウドコンピューティング環境にあるクラウド利用者の情報を一時的に分類するためにマーキングなどの機能を提供することが望ましい。	SaaS やPaaS では標準的なオペレーティングシステムではなく，クラウド事業者独自のオペレーティングシステムを利用している場合がある。その場合，情報管理において使い慣れたインタフェースを利用することができず，情報のラベル付けの手段で対応できないことがある。利用するクラウドサービスのインタフェースを正しく理解して，利用者が自らラベル付けやマーキングができるように手順を見直す必要がある。	–	Microsoft Online Services の規格では，複数の該当するセキュリティ分類カテゴリーに資産を分類し，その後で一連の標準的なセキュリティおよびプライバシー属性を実装するためのガイダンスを用意しています。 ISO 27001 規格（具体的には付属文書 A の項 7.2）で、“情報の分類、ラベリング、および処理” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Online Services 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が実装されることが明示されている。	公開文書	文献[01]	–	–	–	利用者は、Office365上で作成された自身のデータを識別し、資産目録などで適切に分類する必要がある。
8.1.1	8 人的資源のセキュリティ	8.1 雇用前	8.1.1 役割及び責任	従業員，契約相手及び第三者の利用者のセキュリティの役割及び責任は，組織の情報セキュリティ基本方針に従って定め，文書化することが望ましい。	–	–	–	–	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、“情報セキュリティの意識向上、教育、およびトレーニング” が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Services が開催するセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること	要NDA	文献[01]「CO-03：コンプライアンス – サード パーティの監査」 文献[01]「DG-05：データ ガバナンス – 安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織の人的資源の情報セキュリティを行う必要がある。
8.1.2	8 人的資源のセキュリティ	8.1 雇用前	8.1.2 選考	従業員，契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は，関連のある法令，規則及び倫理に従って行うことが望ましい。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行われることが望ましい。	–	–	–	–	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、“情報セキュリティの意識向上、教育、およびトレーニング” が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Services が開催するセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること	要NDA	文献[01]「CO-03：コンプライアンス – サード パーティの監査」 文献[01]「DG-05：データ ガバナンス – 安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織の人的資源の情報セキュリティを行う必要がある。
8.1.3	8 人的資源のセキュリティ	8.1 雇用前	8.1.3 雇用条件	従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名することが望ましい。	–	–	–	–	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、“情報セキュリティの意識向上、教育、およびトレーニング” が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Servicesが開催するセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること	要NDA	文献[01]「CO-03：コンプライアンス – サード パーティの監査」 文献[01]「DG-05：データ ガバナンス – 安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織の人的資源の情報セキュリティを行う必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
8.2.1	8 人的資源のセキュリティ	8.2 雇用期間中	8.2.1 経営陣の責任	経営陣は，組織の確立された方針及び手順に従ったセキュリティの適用を，従業員，契約相手及び第三者の利用者に要求することが望ましい。	—	—	—	—	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Services が開催するセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること	要NDA	文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[01]「DG-05：データ ガバナンス - 安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織の人的資源の情報セキュリティを行う必要がある。
8.2.2	8 人的資源のセキュリティ	8.2 雇用期間中	8.2.2 情報セキュリティの意識向上，教育及び訓練	組織のすべての従業員，並びに，関係するならば，契約相手及び第三者の利用者は，職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け，また，定めに従ってそれを更新することが望ましい。	クラウド利用者は，組織のすべての従業員，契約相手及び第三者の利用者を対象にした教育・訓練の範囲に，組織が保有する情報システムと同様に，クラウドサービスの情報セキュリティに関する事項を加えることが望ましい。クラウド利用者は，クラウドサービスの利用において必要な職務に関連する組織に対して，クラウドサービス利用に関する情報セキュリティの方針及び手順について，適切な意識向上のための教育・訓練の内容を盛り込むことが望ましい。 クラウドサービスの情報セキュリティに関する教育・訓練は，利用者のリテラシーレベルや認知度に応じた内容とし，次のような内容を追加することが望ましい。 a) クラウドサービス利用のための方針，基準及び手順などの規程類 b) クラウドサービスごとの情報セキュリティリスク及びその対策 c) クラウドサービスを使用するにあたり考慮すべきシステム及びネットワーク環境におけるリス ク クラウド利用者は，組織におけるクラウドサービス利用に関する教育，訓練及び意識向上プログラムの実施にあたり，利用するクラウドサービスの操作マニュアル，予防措置及び連絡先に関する情報提供を，必要に応じてクラウド事業者に要求することが望ましい。	クラウド事業者は，クラウド利用者がクラウドサービスに関する情報セキュリティ教育，訓練及び意識向上プログラムを実施するにあたり，自社が提供するクラウドサービスの操作マニュアル及び連絡先情報を必要に応じて提供することが望ましい。	クラウド利用者とクラウド事業者の作業が重複する点は，お互いにおいて，教育を行い，訓練を協調して行うことが期待される。	—	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Online Services の管理者によって承認されていることが明示されている。 また、Microsoft Online Services サービスの一環として包括的なガイダンス、ヘルプ、トレーニング、及びトラブルシューティング用の資料を用意していることが明示されている。 文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Online Services または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Online Servicesのすべての契約業者のスタッフおよびGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。	公開文書	文献[01]「OP-02：運用管理・文書化」 文献[01]「HR-02：人的資源のセキュリティ - 雇用における合意事項」 「IS-11：情報セキュリティ - トレーニング／意識向上」	—	—	—	利用者は、ユーザに対する情報セキュリティ教育を実施する必要がある。
8.2.3	8 人的資源のセキュリティ	8.2 雇用期間中	8.2.3 懲戒手続	セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えることが望ましい。	—	—	クラウド事業者は，クラウドサービスに携わる者を懲戒した場合に，利用者に情報セキュリティとの影響がある場合は，懲戒の内容を連絡する必要があることに留意する。	—	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。 文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Servicesが開催するセキュリティトレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること	要NDA	文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[01]「DG-05：データ ガバナンス - 安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織の人的資源の情報セキュリティを行う必要がある。
8.3.1	8 人的資源のセキュリティ	8.3 雇用の終了又は変更	8.3.1 雇用の終了又は変更に関する責任	雇用の終了又は変更の実施に関する責任は，明確に定め，割り当てることが望ましい。	—	クラウド事業者は，クラウドサービスの提供終了や事業終了に伴う義務を明確に定義することが望ましい。	—	—	契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。	適合可能	文献[67]では、Office 365上の電子メールをオンプレミスのExchange Server環境にコピーして再構築可能なことが明示されている。 文献[68]では、Office 365のSharePoint Onlineのデータをオンプレミスの SharePoint環境にコピーして再構築可能なことが明示されている。	公開文書	文献[67] 文献[68]	—	—	—	利用者は、ユーザのサービス利用終了時に責任をもって当該ユーザのアクセス権やデータの削除を実施する必要がある。
8.3.2	8 人的資源のセキュリティ	8.3 雇用の終了又は変更	8.3.2 資産の返却	すべての従業員，契約相手及び第三者の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産すべてを返却することが望ましい。	クラウド利用者は，すべての従業員，契約相手及び第三者の利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。また，クラウドサービスを加えることが望ましい。クラウド利用者は，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産をクラウド利用者が管理できる機能を，自らの資産の返却プロセスに組み込むことが望ましい。	クラウド事業者は，クラウドサービスにおいて，クラウドサービスの利用者が，雇用，契約又は合意の終了時に返却する資産を，クラウド利用者が管理できる機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド利用者は，リモート環境から利用可能なクラウドサービスについては，資産の返却時期に特に留意する必要がある。	—	契約終了後、お客様管理者が全てのお客様コンテンツを移行し終わったことを最終的に再確認できるように、また、万一移行できなかったお客様コンテンツがあった場合のアクセス手段として、一定の期間、お客様管理者がサービスにアクセスする機能を提供します。一定期間後、マイクロソフトはお客様コンテンツの削除を開始いたします。この削除プロセスが開始した時点以降、お客様はお客様コンテンツへのアクセスを行うことはできなくなります。削除プロセスが完了した後、お客様コンテンツは回復不能な状態に削除されます。これらの削除については、契約書への記載事項となっています。	適合可能	文献[67]では、Office 365上の電子メールをオンプレミスのExchange Server環境にコピーして再構築可能なことが明示されている。 文献[68]では、Office 365のSharePoint Onlineのデータをオンプレミスの SharePoint環境にコピーして再構築可能なことが明示されている。	公開文書	文献[67] 文献[68]	—	—	—	利用者は、ユーザのサービス利用終了時に責任をもって当該ユーザのアクセス権やデータの削除を実施する必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							SI事業者・利用者で必要な対応
評価項目番号	章	節	項	管理策	クラウド利用者のための実施の手引	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.3.3	8 人的資源のセキュリティ	8.3 雇用の終了又は変更	8.3.3 アクセス権の削除	すべての従業員、契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正することが望ましい。	クラウド利用者は、クラウドサービスの利用者に対するアクセス権を、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する機能を提供することが望ましい。また、そのような機能について、クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は、クラウドサービスの利用者に対するアクセス権を、クラウド利用者が、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する機能を提供することが望ましい。また、そのような機能について、クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド利用者は、クラウド事業者との契約内容によっては、クラウドサービスの利用者との雇用、契約又は合意の終了後も、そのアクセス権を一定期間失効させることができない可能性があることに留意する必要がある。	–	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー－データのセキュリティ／整合性」 文献[07]「FAQ37」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、ユーザのサービス利用終了時に責任をもって当該ユーザのアクセス権やデータの削除を実施する必要がある。
9.1.1	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.1 物理的セキュリティ境界	情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いることが望ましい。	–	–	クラウド事業者は、複数のデータセンターを利用する場合にセキュリティの保護に差異が生じないように留意し、物理セキュリティ境界を用いることが期待される。 クラウド事業者は、クラウド利用者に対する情報提供に伴う情報セキュリティリスクを考慮し、取扱いに慎重を要する情報が露見しないよう、物理的セキュリティ境界及び関連する管理策に関する情報（例えば、データセンターの所在地、物理的アクセスの管理策など）の開示範囲を決定する必要がある。	ハードウェア機器を厳重な入退室管理、24 時間365 日の有人監視及び最新のセキュリティ技術を導入しているデータセンターに設置する。	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施錠可能な棚”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。	公開文書	文献[01]「FS-03：施設のセキュリティ － 管理されたアクセスポイント」	–	–	–	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.1.2	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.2 物理的入退管理策	セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護することが望ましい。	–	–	クラウド事業者は、データセンターなどの間でデータを交換する場合、共通の物理的入退管理策が講じられたセキュリティエリアでデータが交換される必要があることに注意を要する。	–	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。	公開文書	文献[01]「FS-03：施設のセキュリティ － 管理されたアクセスポイント」	–	–	–	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.1.3	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.3 オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用することが望ましい。	–	–	クラウド事業者は、オフィス、部屋及び施設に対する物理的なセキュリティに関する指針に差異が発生しないように留意することが期待される。	–	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。	適合可能	文献[01]では、データセンターの施設へのアクセスが制限されていること、電子カードによるアクセスコントロールされたドアなどで制限されていることが明示されている。	公開文書	文献[01]「FS-03：施設のセキュリティ － 管理されたアクセスポイント」	–	–	–	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.1.4	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.4 外部及び環境からの保護	火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害による被害からの物理的な保護を設計し、適用することが望ましい。	–	–	–	–	データ センターを保護するために、以下を含む環境の管理を実施しています。 · 温度管理 · 冷暖房、換気、および空調（HVAC） · 火災検知および抑制システム · 電力管理システム ISO 27001 規格（具体的には付属文書 A の項 9.1.4）で、“外部および環境による脅威に対する保護” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	NDA文書を確認したところ、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。 インタビューの結果、日本国内では地震帯に設置するなどの措置が講じられており、洪水などの影響を受けにくい位置に設置されていると考えられる。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.1.5	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.5 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する物理的な保護及び指針を設計し、適用することが望ましい。	クラウド利用者は、クラウドサービスを利用する場合に、セキュリティを保つべき領域が拡大しないか確認し、セキュリティを保つべき領域が拡大する場合は、作業に関する物理的な保護及び指針を設計し、適用することが望ましい。	クラウド事業者は、クラウドサービスによって、クラウド利用者の利用環境を拡大させるような機能が存在する場合は、その機能を開示することが望ましい（例えば、モバイルコンピューティングからの利用が可能になる、など）。	–	–	Office 365で提供するサービスの一覧は、TechNetライブラリ等で公開しています。 Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められています。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合） お客様には、大規模な変更については 12 か月前までに通知が行われ、計画済みのメンテナンスについては少なくとも 5 日前までに通知が行われます。ただし、このサービスはマルチテナントであるため、いつアップグレードを行うかに関して個々のお客様がそれを定義できるようにする条項はありません。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、“変更管理” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[114]では、Office 365 が提供するサービスの一覧が明示されている。 文献[01]では、Office 365に大規模な変更がある場合には、12ヶ月前に利用者に通知されることが明示されている。	公開文書	文献[114] 文献[01]「RM-01：リリース管理 － 新規開発／取得」	–	–	–	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.1.6	9 物理的及び環境的セキュリティ	9.1 セキュリティを保つべき領域	9.1.6 一般の人の立寄り場所及び受渡場所	一般の人が立ち寄る場所（例えば、荷物などの受渡場所）及び敷地内の認可されていない者が立ち入ることもある場所を管理し、また、可能な場合には、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離すことが望ましい。	–	–	クラウド事業者は、データセンターなどの間でデータを交換する場合、一般の人の立寄り場所及び受渡場所に関する指針に差異が発生しないように留意することが期待される。	–	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。	適合可能	インタビューの結果、日本国内では出入口付近およ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おり、侵入や破壊、機密情報漏洩等の防止措置がとられていると考えられる。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織が管理する施設の物理的および環境的セキュリティ対策を施す必要がある。
9.2.1	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.1 装置の設置及び保護	装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護することが望ましい。	–	–	クラウド事業者は、機器や、データセンターなどの間でデータを交換する場合、装置の設置及び保護の管理策に差異が発生しないよう留意することが期待される。	–	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。	適合可能	NDA文書を確認したところ、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。 インタビューの結果、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おり、浸水などの影響を受けにくい位置に設置されていると考えられる。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織が管理する装置の物理的および環境的セキュリティ対策を施す必要がある。
9.2.2	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.2 サポートユーティリティ	装置は、サポートユーティリティの不具合による、停電、その他の故障から保護することが望ましい。	–	–	クラウド事業者は、機器や、データセンターなどの間でデータを交換する場合、サポートユーティリティの保護に差異が発生しないよう留意することが期待される。	–	データ センターには、専用の 24 時間年中無休で稼働する無停電電源装置（UPS）および緊急電源サポート（発電機など）が装備されています。UPS と発電機の両方について定期的な保守が行われています。データ センターでは、緊急時の燃料供給のための調整が行われています。 データ センターには、以下の項目を監視するための専用の施設運用センターがあります。 · 電力システム、発電機、切替スイッチ、メインの分電装置、電力管理モジュール、無停電電源装置など、すべての重要な電気コンポーネントを含む。 · 冷暖房、換気、空調（HVAC）システム。データ センター内の空間温度と湿度、空間の与圧、外部の空気の取り入れを制御および監視します。 すべてのデータ センターに火災検知および抑制システムが存在します。 また、データ センター内のさまざまな場所に可搬式消火器が設置されています。施設および環境保護機器について、定期的な保守が行われています。 ISO 27001 規格（具体的には付属文書 A の項 9.1.4 および 9.2.2）で、“外部および環境による脅威に対する保護、およびサポート ユーティリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	インタビューの結果、日本国内では電源は複数回線で引き込まれており、受電設備の障害時の備えが講じられていると考えられる。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織が管理する装置の物理的および環境的セキュリティ対策を施す必要がある。
9.2.3	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.3 ケーブル配線のセキュリティ	データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受又は損傷から保護することが望ましい。	–	–	クラウド事業者は、データセンター間でデータを交換する場合、データセンターごとのケーブル配線のセキュリティに差異が生じないように留意することが期待される。	–	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施錠可能な棚”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	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。 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厳格された区画内（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。	要NDA	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	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。

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
9.2.4	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.4 装置の保守	装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守することが望ましい。	—	—	クラウド事業者は，データセンター間でデータを交換する場合，データセンターごとの保守の差異が生じないように留意することが期待される。	—	Microsoft Online Services の環境に向けた、サービス継続性の管理（SCM）の開発およびメンテナンス プロセスが用意されています。このプロセスには、Microsoft Online Services 資産を回復し、Microsoft Online Services の主要なビジネス プロセスを再開するための方法が含まれています。継続性ソリューションによって、サービスの運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.4）で、“機器のメンテナンス” が規定されています。	適合可能	文献[01]では、データ センターに、電力システム、冷暖房、換気、空調（HVAC）システムを監視するための専用の施設運用センターや、火災検知および抑制システムがあること、施設および環境保護機器について定期的な保守が行われていることが明示されている。	公開文書	文献[01]「RS-07：復元 – 機器の電源の故障」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、自組織が管理する装置の物理的および環境的セキュリティ対策を施す必要がある。
9.2.5	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.5 構外にある装置のセキュリティ	構外にある装置に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用することが望ましい。	—	—	—	—	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、“施設可能な柵”、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、“物理的なセキュリティ境界および環境上のセキュリティ” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	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。 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。	要NDA	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織が管理する装置の物理的および環境的セキュリティ対策を施す必要がある。
9.2.6	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.6 装置の安全な処分又は再利用	記憶媒体を内蔵した装置は，処分する前に，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又は問題が起きないように上書きしていることを確実にするために，すべてを点検することが望ましい。	クラウド利用者は，クラウド サービスの利用を終了した場合，使用されていた機器などが再利用されることに留意することが望ましい。	クラウド事業者は，バックアップを含め，取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを含む情報の取扱いに留意することが望ましい。クラウド事業者は，記憶媒体を内蔵した装置を処分する場合には，記録された情報を復元できないように安全に処分することが望ましい。また，記憶媒体を内蔵した装置を再利用する場合には，機密情報の漏えいに対する対策を実施することが望ましい。	—	—	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、焼却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 すべての Microsoft Online Services は、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、“機器の安全な処分または再使用とメディアの処分” が規定されています。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Online Servicesのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していることが明示されている。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。	要NDA	文献[01]「DG-05：データ ガバナンス – 安全な廃棄」	—	—	（マイクロソフト社とのNDAにより開示）	利用者は、Office365の利用終了にあたっては、自組織が管理する装置に保存された取扱いに慎重を要するデータを消去する必要がある。
9.2.7	9 物理的及び環境的セキュリティ	9.2 装置のセキュリティ	9.2.7 資産の移動	装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい。	クラウド利用者は，クラウド サービスでは，事前にクラウド利用者の許可なく，データの物理的な所在が移動される可能性があることに留意することが望ましい。	—	—	—	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一 可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織が管理する装置の物理的および環境的セキュリティ対策を施す必要がある。
10.1.1	10 通信及び運用管理	10.1 運用の手順及び責任	10.1.1 操作手順書	操作手順は，文書化し，維持していくことが望ましい。また，その手順は，必要とするすべての利用者に対して利用可能とすることが望ましい。	クラウド利用者は，利用するクラウド サービスの操作手順を作成することが望ましい。クラウド利用者は，手順書作成にあたり，クラウド事業者の情報提供方針を確認することが望ましい。	クラウド事業者は，クラウド利用者がクラウド サービスの操作手順を作成する際の情報提供に関する方針を定め，クラウド利用者に提示することが望ましい。クラウド事業者による情報提供の例として，次のようなものがある。 a) 利用者向け操作手順書の提示 b) 問合せ窓口	クラウド利用者は，クラウド サービスの環境においては，サービスの変更が一斉に行われ，操作手順の変更が発生する可能性があることに留意することが期待される。 クラウド利用者が他のクラウド サービスを利用して内部又は外部の利用者にサービスを提供する場合（例えば，IaaS を利用してSaaS を提供する場合など），クラウド利用者は，サービス仕様及びサービスレベルの提供を維持するためにクラウド事業者に対して，システム及びサービスに関する変更情報を要求することが想定される。	—	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Online Services の管理者によって承認されていることが明示されている。 また、Microsoft Online Services サービスの一環として包括的なガイダンス、ヘルプ、トレーニング、及びトラブルシューティング用の資料を用意していることが明示されている。	公開文書	文献[01]「OP-02：運用管理・文書化」	—	—	—	利用者は、Office365の利用環境における操作等について、実行、記録、結果確認などの操作手順を適切に管理することが望ましい。
10.1.2	10 通信及び運用管理	10.1 運用の手順及び責任	10.1.2 変更管理	情報処理設備及びシステムの変更は，管理することが望ましい。	クラウド利用者は，クラウド事業者からクラウド利用者に影響がある情報処理設備及びシステムの変更の通知を受けた場合は，その影響を確認し，記録することが望ましい。	クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更において，クラウド利用者に影響を及ぼすものをあらかじめ定義し，クラウド利用者に通知することが望ましい。クラウド事業者は，クラウドサービスの情報処理設備及びシステムの変更においてクラウド利用者に通知する項目並びに変更履歴を，クラウドサービスの利用を検討する者及びクラウド利用者に明示することが望ましい。	クラウド利用者は，クラウドサービスの環境においては，情報処理設備及びシステムの変更において，クラウド利用者に影響や及ぼすものを事前に周知することが望ましい。クラウド利用者，クラウド事業者ともに，IaaS などで利用される仮想化環境では，資産調達と連動せずに機器（例えば，仮想マシンなど）やソフトウェアのライセンスなどの追加が可能になることに留意することが期待される。 クラウド事業者がクラウド利用者に通知する項目の例として，次のようなものがある。 a) システム変更の実施予定日時 b) システム変更の内容 - 新規ソフトウェアのインストール又はパッチの適用 - ハードウェア変更 - ネットワーク変更 - ソフトウェア変更 - サービスの変更 - サブプロバイダの変更 - システムの物理的な移動 c) 変更に関するリスク評価 d) システム変更の開始及び完了の通知 e) 事前の取決めに基づく確認又は承認	—	変更の管理手順が定められています。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設において システム保守を実行するすべての関係者（Microsoft Online Services とサード パーティ）に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合）	適合可能	文献[01]では、マイクロソフトがMicrosoft Online Services サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Servicesの主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、および変更管理」が含まれていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Office365の利用環境の変更管理を適切に実施する必要がある。
10.1.3	10 通信及び運用管理	10.1 運用の手順及び責任	10.1.3 職務の分割	職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分割することが望ましい。	クラウド利用者は，クラウド サービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，分割すべき職務及び責任範囲（例えば，ID の使用者と登録者など）を明示することが望ましい。	クラウド事業者は，提供するクラウドサービスにおいて，組織の資産に対する，認可されていない又は意図しない変更又は不正使用の危険性を低減するために，クラウド利用者において分割することが望ましい職務及び責任範囲（例えば，ID の使用者と登録者など）を明示することが望ましい。	クラウドサービスにおいては，クラウド利用者にとって重要な処理であっても，職務の分割が技術的に実装されていない場合は，クラウド利用者は，職務の分割を運用で実装することが求められる場合がある。	—	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、“職務の分離” が規定されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 文献[75]では、管理者アカウントのみが提供され、職務の分割が必要であればクラウド利用者側で実施することを確認した。	公開文書	文献[01]「IS-07：情報セキュリティ – ユーザーアクセス ポリシー」 文献[75]	—	—	—	利用者は、自組織内で分割すべき職務及び責任範囲を特定し、分割することが望ましい。
10.1.4	10 通信及び運用管理	10.1 運用の手順及び責任	10.1.4 開発施設，試験施設及び運用施設の分離	開発施設，試験施設及び運用施設は，運用システムへの認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい。	クラウド利用者は，開発，試験及び運用環境を分離するため，必要に応じて仮想環境を利用することが望ましい。	—	クラウド利用者は，クラウドサービスの環境においては，開発施設，試験施設及び運用施設の分離が，物理的に困難である可能性に留意することが期待される。	—	Office 365 サービスでは、異なるホスティング サービスの開発スタッフや運用スタッフが、職務分離の原則に従うようにすることができます。ソース コード、ビルド サーバー、および運用環境に対するアクセスは、厳しく制御されています。 例: · Office 365 サービスの運用環境に対するアクセスは運用担当者に制限されます。開発チームとテスト チームには、運用環境内から提供された情報に対してアクセス権が与えられる場合があり、問題のトラブルシューティングに役立てることができます。 · Office 365 サービスのソース コード管理に対するアクセスはエンジニアリング担当者に制限され、運用担当者がソース コードを変更することはできません。 マイクロソフトの担当者は、マルチテナント環境の委託が行われる前にサーバーを構築します。サーバーの構築が完了すると、構築チームは自身のアクセス許可を削除します。サーバーを委託した時点から、マイクロソフトの担当者が委託されたサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、“職務の分離” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトがMicrosoft Online Services サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Servicesの主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、および変更管理」が含まれていることが明示されている。 文献[01]では、Microsoft Online Services 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ること、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ること、また、お客様の非公開データの運用環境から非運用環境への移動またはコピーは、お客様の同意が得られた場合やマイクロソフトの法務部門の指示による場合を除き禁止されていることが明示されている。 NDA文書を確認したところ、お客様データへのアクセスについて厳重に管理されていることが確認できた。	要NDA	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」 文献[01]「RM-04：リリース管理 – 品質テスト」「DG-06：データ ガバナンス – 非運用データ」	（マイクロソフト社とのNDAにより開示）	—	（マイクロソフト社とのNDAにより開示）	—

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応						
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
10.2.1	10 通信及び運用管理	10.2 第三者が提供するサービスの管理	10.2.1 第三者が提供するサービス	第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義及び提供サービスレベルが、第三者によって実施、運用及び維持されることを確実にすることが望ましい。	クラウド利用者は、クラウドサービスにおいて、クラウド事業者が、第三者（クラウドサービスを構成するためのネットワークを提供するプロバイダや関係るほかのクラウド事業者など。以下同じ。）が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義及び提供サービスレベルが、クラウド事業者によって実施、運用及び維持されることを、確実にしていることを確認することが望ましい。クラウド利用者は、クラウド事業者が、第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義及び提供サービスレベルによって、クラウド利用者が影響を受ける可能性についてあらかじめ考慮していることが望ましい。	クラウド事業者は、提供しているクラウドサービスにおいて利用している第三者が提供するサービスのうち、利用者の情報セキュリティ管理に影響のあるものを開示することが望ましい。クラウド事業者は、第三者が提供するサービスにおけるセキュリティ管理策、サービスの定義及びサービスレベルをクラウド利用者が定期的にレビューできるよう、必要に応じて次のような情報を提供することが望ましい。 a) 情報セキュリティに係るサービス運用報告書 b) 情報セキュリティに係る監査報告書 c) サービスレベル報告書 クラウド事業者は、提供するクラウドサービスがサプライチェーンを形成する場合には、リスク管理に関する目標を他の事業者に提示し、各事業者に対してリスク管理の実施及び目標の達成を求めることが望ましい。	クラウド利用者は、クラウドサービスの環境においては、様々な階層のサービスが複雑に作用するため、クラウド事業者の提供するクラウドサービスの特に依存する第三者サービスがないか（例えば、第三者のPaaS を利用したSaaS サービスであるか、など）留意することが期待される。 クラウド事業者は、クラウドサービスの環境においては、様々な階層のサービスが複雑に作用するため、お互いに実施したり、協同で実施したりすべきことに留意し、円滑な運用を図ることが期待される。	—	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格（具体的には付属文書 A の項 6.2 および 10.2）で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること、下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されることが明示されている。	公開文書	文献[01]「CO-03：コンプライアンス－サード パーティの監査」 文献[02]「顧客データが下請業者に開示される場合」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、自らが契約する第三者サービス（通信回線、電力等）について、適切に管理する必要がある。
10.2.2	10 通信及び運用管理	10.2 第三者が提供するサービスの管理	10.2.2 第三者が提供するサービスの監視及びレビュー	第三者が提供するサービス、報告及び記録は、常に監視し、レビューすることが望ましい。また、監査も定期的に実施することが望ましい。	クラウド利用者は、クラウドサービスにおいて、クラウド事業者によって、第三者が提供するサービス、報告及び記録が、常に監視され、レビューされていることを確認することが望ましい。クラウド利用者は、クラウドサービスにおいて、クラウド事業者によって、第三者が提供するサービスが、監査されていることを確認することが望ましい。	クラウド事業者は、提供しているクラウドサービスについて、クラウド利用者に対して次のような情報提供を必要に応じて行うことが望ましい。 d) 第三者が提供するサービス、報告及び記録を、常に監視し、レビューしていることの開示 e) 第三者が提供するサービス、報告及び記録を、常に監視し、レビューした記録の明示 f) 第三者が提供するサービスを監査していることの開示 g) 第三者が提供するサービスを監査した結果をまとめた報告書などの提示	クラウド利用者は、クラウドサービスの環境においては、様々な階層のサービスが複雑に作用するため、クラウドサービスが遵守していること（例えば、IaaS を利用したPaaS を利用したSaaS サービスである、など）に留意することが期待される。	—	施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地域のあらゆる事象の影響を受けにくいように設計されており、そこには第三者が提供するサービスの監視等も含まれます。マイクロソフトは国際的に通用する厳密なベストプラクティスに基づいて運用をしており、IOS/IEC27001:2005 認定や SSAE 16/ISAE 3403 SOC 1, AT101 SOC 2 認証を含む国際標準によって自身を評価しています。証明書や評価レポートは参照いただけます。	適合可能	文献[99]では、第三者が提供するサービスの監視や評価が行われていることが明示されている。	公開文書	文献[99]	—	—	—	利用者は、自らが契約する第三者サービス（通信回線、電力等）について、適切に管理する必要がある。
10.2.3	10 通信及び運用管理	10.2 第三者が提供するサービスの管理	10.2.3 第三者が提供するサービスの変更に対する管理	関連する業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、サービス提供の変更（現行の情報セキュリティ方針、手順及び管理策の保守・改善を含む。）を管理することが望ましい。	クラウド利用者は、クラウドサービスにおいて、クラウド事業者の利用する第三者のサービス提供の変更が影響を及ぼす可能性を確認することが望ましい。 クラウド利用者は、組織の情報セキュリティに影響を与える可能性のあるクラウド事業者の利用する第三者のサービス提供の変更について、クラウド利用者の変更管理プロセスに基づき、必要な対応を実施することが望ましい。	クラウド事業者は、クラウドサービスにおいて、第三者のサービス提供の変更に影響を及ぼす可能性がある場合、クラウド利用者へ通知することが望ましい。 クラウド事業者は、組織の情報セキュリティに影響を与える可能性のある、クラウド事業者の利用する第三者のサービス提供の変更について、クラウド利用者へ通知の方針を定め、クラウド利用者に通知することが望ましい。	クラウド事業者が、第三者のサービスの変更に関してクラウド利用者に通知する事項の例として、次のようなものがある。 a) システム変更の実施予定日時 b) システム変更の内容 c) 変更に関するリスク評価 d) システム変更の開始及び完了の通知 e) 事前の取決めに基づく確認又は承認 クラウド利用者は、クラウドサービスの環境においては、様々な階層のサービスが複雑に作用するため、クラウドサービスが遵守していること（例えば、IaaS を利用したPaaS を利用したSaaS サービスである、など）に留意することが期待される。	—	施設の所在地、施設やネットワークの回復能力やサービスのフェイルオーバー手順は、地域のあらゆる事象の影響を受けにくいように設計されており、そこには第三者が提供するサービスの監視等も含まれます。マイクロソフトは国際的に通用する厳密なベストプラクティスに基づいて運用をしており、IOS/IEC27001:2005 認定や SSAE 16/ISAE 3403 SOC 1, AT101 SOC 2 認証を含む国際標準によって自身を評価しています。証明書や評価レポートは参照いただけます。	適合可能	文献[99]では、第三者が提供するサービスの監視や評価が行われていることが明示されている。	公開文書	文献[99]	—	—	—	利用者は、自らが契約する第三者サービス（通信回線、電力等）について、適切に管理する必要がある。
10.3.1	10 通信及び運用管理	10.3 システムの計画作成及び受入れ	10.3.1 容量・能力の管理	要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測することが望ましい。	クラウド利用者は、要求されるシステム性能を満たすことを確実にするために、次の事項を実施することが望ましい。 a) クラウドサービスにおける容量・能力の限界値を把握する。 b) クラウドサービスにおける容量・能力の限界値が、要求されるシステム性能を満たすことを確認する。 c) クラウドサービスにおいて、資源の利用を監視・調整する仕組みがあることを確認し、現状の資源の利用を監視・調整する仕組みに組み込む。 クラウド利用者は、将来必要とする容量・能力を予測する仕組みに、クラウドサービスを組み込むことが望ましい。クラウド利用者は、クラウドサービスの環境においては、契約形態に応じた容量・能力の割当ての変更や、容量・能力の利用に応じた課金について留意することが望ましい。クラウド利用者は、クラウドサービスの容量・能力の追加が、容易にできるか確認することが望ましい。	クラウド事業者は、重大なインシデントを防ぐために、物理的な容量・能力の全体量を考慮して仮想化されたコンピューティング資源の全体量を監視し、適切に管理することが望ましい。 クラウド事業者は、クラウドサービスにおいて、システム全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握することが望ましい。	クラウドサービスによっては、CPU 利用率などの急激な上昇・降下が発生し、サービスの安定稼働に影響を及ぼす場合がある。このような事象は原因を特定できないことも多く、特定のしきい値を設けた監視による完全な予測や事前対応が難しい。そのため、クラウド利用者は、クラウドサービスにおけるCPU 利用率などの急激な上昇・降下に伴うリスクを評価した上でクラウドサービスを利用することが期待される。 一方、クラウド事業者は、そのようなリスクをクラウド利用者が識別・評価できるよう、あらかじめ示しておくことが期待される。	—	マイクロソフトでは、定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、CPU 使用率、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。	適合可能	文献[01]では、予防的な容量管理やサービスのパフォーマンス等を監視する運用プロセスを用意していることが明示されている。	公開文書	文献[01]「OP-02：運用管理 － 容量/リソース計画」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、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。
10.3.2	10 通信及び運用管理	10.3 システムの計画作成及び受入れ	10.3.2 システムの受入れ	新しい情報システム及びその改訂版・更新版の受入れ基準を確立し、また、開発中及びその受入れ前に適切なシステム試験を実施することが望ましい。	クラウド利用者は、新規のクラウドサービスや、利用中のクラウドサービスの改訂版・更新版に関して、受入れ基準を確立し、開発中及びその受入れ前にシステム試験を実施し、結果をクラウド事業者に通知することが望ましい。 クラウド利用者は、クラウドサービスの選定にあたり、クラウド事業者に対して次の情報を求めることが望ましい。 a) SLA（アクセスネットワークの容量・能力及び冗長化を含む） b) 試用に関する詳細（料金、試用期間及び免責事項を含む）	クラウド事業者は、クラウドサービスの改訂版・更新版の提供プロセスを、クラウド利用者に明示することが望ましい。クラウド事業者は、クラウドサービスにおいて、クラウド利用者へ改訂版・更新版の受入れ準備のための期間を提供することが望ましい（例えば、通知後一週間で運用環境に適用する、など）。クラウド事業者は、クラウド利用者が円滑にクラウドサービスの改訂版・更新版へ移行できるように、旧版との併用ができる期間を設けることが望ましい。	クラウド利用者は、クラウドサービスにおいて、新しい情報システム及びその改訂版・更新版の提供プロセスや、利用者の変更管理プロセスに関して、クラウド利用者に通知する事項の例として、次のようなものがある。 a) システム変更の実施予定日時 b) システム変更の内容 c) 変更に関するリスク評価 d) システム変更の開始及び完了の通知 e) 事前の取決めに基づく確認又は承認 クラウド利用者は、クラウドサービスの環境においては、様々な階層のサービスが複雑に作用するため、クラウドサービスが遵守していること（例えば、IaaS を利用したPaaS を利用したSaaS サービスである、など）に留意することが期待される。	—	変更の管理手順が定められています。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者（Microsoft Online Services とサード パーティ）に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 ・計画された変更の特定と文書化 ・変更によって生じる可能性のある影響の評価プロセス ・承認されている非運用環境における変更のテスト ・変更の通知計画 ・変更管理の承認プロセス ・変更の中止と復元計画（該当する場合）	適合可能	文献[01]では、マイクロソフトがMicrosoft Online Services サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Servicesの主要な変更の実装を制御するためのソフトウェア開発およびリリース管理プロセスに「計画された変更の特定と文書化」、「開始/終了条件に基づくテスト、認証、および変更管理」が含まれていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	—

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応								
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
10.4.1	10 通信及び運用管理	10.4 悪意のあるコード及びモバイルコードからの保護	10.4.1 悪意のあるコードに対する管理策	悪意のあるコードから保護するために、検出、予防及び回復のための管理策、並びに利用者に適切に意識させるための手順を実施することが望ましい。	クラウド利用者は、悪意のあるコードから情報やシステムを保護するために、検出、予防及び回復のための管理策だけでなく、クラウドサービスの利用者に対してクラウドサービス利用時の考慮事項を適切に意識させるための手順を策定して、実施することが望ましい。 クラウド利用者は、クラウドサービスにおいて、クラウド事業者が、悪意のあるコードからクラウド利用者を保護するために実施している次のような事項を確認することが望ましい。 a) 悪意のあるコードの検出、予防及び回復のための管理策 b) 悪意のあるコード及びその対策・対応について、クラウド利用者に適切に意識させるために実施している管理策とその実行結果 c) 悪意のあるコードに感染した場合のクラウド事業者における報告手順 クラウド利用者は、組織が実施している悪意のあるコード対策とクラウド事業者の悪意のあるコード対策を併せてリスク評価し、必要に応じて自ら追加の対策を実施することが望ましい。	クラウド事業者は、クラウドサービスの提供において、悪意のあるコードへのクラウド事業者の責任範囲と、クラウド利用者の責任範囲を明らかにすることが望ましい。クラウド事業者は、クラウドサービス内で、悪意のあるコードからクラウドサービスの利用者を保護するために、検出、予防及び回復のための管理策を実施し、また、クラウド利用者に適切に意識させるための手順を実施することが望ましい。	クラウドサービスを構成する環境において は、様々な階層のサービスが複雑に関連するため、それぞれの階層において、悪意のあるコードへの独自の対策が行われている可能性がある。そのため、クラウド利用者とクラウド事業者は、それぞれの階層における対策方式や検出精度の違いから検出結果の違いが発生する可能性に留意する必要がある。クラウド事業者は、ウイルス対策製品を導入した場合、パフォーマンスの問題や、可用性に影響を生じさせることに留意する必要がある。	—	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてウイルスがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。	適合可能	文献[01]では、システム上の悪意のある可能性のある動作を識別するために、多数の主要なセキュリティパラメータが監視されていることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockbox プロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、Office365の利用環境について悪意のあるコードに対する管理策を講ずる必要がある。
10.4.2	10 通信及び運用管理	10.4 悪意のあるコード及びモバイルコードからの保護	10.4.2 モバイルコードに対する管理策	モバイルコードの利用が認可された場合は、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする環境設定を行うことが望ましい。また、認可されていないモバイルコードを実行できないようにすることが望ましい。	—	クラウド事業者は、マルウェア感染の拡大を防ぐため、特定のクラウド利用者に対するサービスの停止を含むモバイルコード利用の方針を定めることが望ましい。また、クラウド事業者は、クラウドサービスにおけるモバイルコード利用の方針をクラウド利用者に提示し、方針に対する協力を求めることが望ましい。	クラウド事業者は、クラウドサービスにおいてモバイルコードを利用する場合、利用の可否をクラウド利用者が判断し、認可できるような仕組みを提示し、認可されたモバイルコードが、明確に定められたセキュリティ方針に従って動作することを確実にする方法をクラウド利用者に明示することが期待される。 また、同時に、クラウド事業者は、クラウドサービスの環境において、認可されていないモバイルコードを実行できないようにする方法を、クラウド利用者に明示することが期待される。 クラウド利用者は、悪意のあるコードに関する次のような事項について、クラウド事業者の情報提供方針を確認することが期待される。 a) セキュリティ関連の設定及び使用されているオプション b) セキュリティ管理策及び対象システムコンポーネント（例えば、ネットワーク、ゲストOS レイヤなど） c) ソフトウェア更新・パッチ適用に関するスケジュール及び情報（例えば、パッチの種類、パッチ適用の頻度及び対象システムなど） d) ぜい弱性の検出、報告及び改善のための基準及び手順（例えば、ベンダーの公開情報、侵入テストツールなど） e) 隣接するVM やVMM（Virtual Machine Monitor、仮想マシンモニタ／ハイパーバイザー）などの異なるクラウドコンポーネントの感染に備えたインシデント対応手順及び復旧手順 f) 利用者側で実装すべき悪意のあるコード対策 g) サービスレベル報告書に含まれる内容 － 未対応のぜい弱性に関するパッチ情報及び管理策 － 補完的統制に関する情報 － 特定のぜい弱性に関する情報及び傾向（例えば、仮想化レイヤなどに対するぜい弱性の分類及び重要度スコアなど）	—	マイクロソフトのセキュリティ開発ライフサイクル（SDL）は、Office 365 などのソフトウェアおよびサービスの設計、開発、および展開のあらゆる段階の情報を提供する、包括的なセキュリティ保証プロセスです。設計要件、攻撃対象の分析、および脅威のモデリングによって、SDL は、製品ライフサイクル全体を通じて、サービスの提供を開始する前から脆弱性と脅威の予測、特定、軽減に役立ちます。SDL は最新のデータとベスト プラクティスを用いて継続的に更新されます。これにより、Office 365 関連の新しいサービスとソフトウェアは最初の日から高度なセキュリティで保護されます。 マルウェア対策ソフトウェアの使用は、Office 365 の資産を悪意のあるソフトウェアから保護するための主要なメカニズムです。このソフトウェアは、コンピューター ウイルスやワームのサービス システムへの侵入を検出し、防止します。また、感染したシステムの検疫を行い、修復措置が取られるまでの間、それ以上の被害を防ぎます。マルウェア対策ソフトウェアは、悪意のあるソフトウェアを予防および検出する制御を提供します。 標準パッケージの使用の概要が示される場合、サーバー、ネットワーク デバイス、その他のマイクロソフト アプリケーションの標準の基本構成要件が記述されます。これらのパッケージは、事前にテストされ、セキュリティ制御で構成されています。 運用環境に対する更新プログラム、ホットフィックス、および修正プログラムなどの変更は、同じ標準の変更管理プロセスに従います。修正プログラムは、発行会社が指定する期間内に導入されます。変更は、導入前にレビュー チームと変更諮問委員会（CAB）により、適用性、リスク、およびリソースの割り当てについて見直しと評価が行われます。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。 文献[17]では、Office 365の環境においてもセキュリティ開発ライフサイクルに基づいて管理されていることが確認できた。	要NDA	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発／取得」 文献[17]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、Office365の利用環境についてモバイルコードに対する管理策を講ずる必要がある。
10.5.1	10 通信及び運用管理	10.5 バックアップ	10.5.1 情報のバックアップ	情報及びソフトウェアのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査することが望ましい。	クラウド利用者は、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの必要性を確認することが望ましい。 クラウド利用者は、自らが利用するクラウドサービスの特性を理解して、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定において、バックアップの可能性を確認することが望ましい。クラウド利用者は、自らが利用するクラウドサービスの特性を理解し、クラウドサービス上で扱う情報、ソフトウェア及びソフトウェアの設定のバックアップ手順を、次の事項を考慮して策定することが望ましい。 a) クラウドサービスに付帯するバックアップ機能及び復元機能 b) 利用者自身が追加開発するバックアップ機能及び復元機能 c) バックアップデータの暗号化（暗号化の必要性を含む） d) バックアップデータのローカルでの保管及び隔地保管 e) バックアップデータの保管期間	クラウド事業者は、クラウド利用者が行うべきバックアップ取得について明確にすることが望ましい。 また、利用者自身によるバックアップ取得が必要な場合、バックアップ取得を支援する情報若しくは機能を提供することが望ましい。クラウド事業者は、利用者にバックアップ機能及び復元機能を提供する場合には、利用者が実施する手順を明確にすることが望ましい。	クラウドサービスでは、クラウドサービスによってバックアップ不可能な情報がある点に留意する必要がある。クラウドサービス以外のシステム運用におけるバックアップ手順において、差分バックアップ、増分バックアップ、完全バックアップなど、バックアップ対象の特性に応じて使い分けている場合は、それぞれの手法による実施の可否を確認することが期待される。 IaaS サービスにおいては、作成された仮想イメージファイルを明示的にバックアップしておくことで、ある時点での環境を再現することができるが、バックアップを指定しない場合には再現することが難しい。 クラウド事業者は、クラウド利用者が必要に応じて仮想イメージファイルをバックアップできる手段を用意しておくことが期待される。 PaaS サービスにおいては、作成したアプリケーションなどのソースファイルなどをバックアップすることができないこともある。アプリケーションの開発中など、頻繁に機能の追加や削除を行う場合に備えて、開発途中の状態を維持できるかどうかを確認することが望ましい。また、実行環境や試験データなどが再現できるかどうかを確認することが期待される。 SaaS サービスでは、アプリケーションで利用するデータだけではなく、利用者アカウントの管理など、クラウドサービスの管理情報についてバックアップが可能かどうかを確認することが期待される。	—	バックアップの場合、内容がプライマリー データ センターからセカンダリー データ センターにレプリケートされます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。 Microsoft Online Services では、その提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。資産所有者は、その資産に関する情報を常に最新にしておく責任を担います。	適合可能	文献[01]では、Microsoft Online Services では障害復旧を目的として、インフラストラクチャデータのバックアップが定期的に作成され、データの復元が定期的に検証されること、レプリケーション機能が提供されていることが明示されている。また、利用者自らが自身のデータを抽出してバックアップできることが明示されている。	公開文書	文献[01]「DG-04：データガバナンス － 保持ポリシー」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、クラウドサービスにて実施されるバックアップに加えて、必要に応じて自身のデータを抽出し、取得したバックアップを保存することができる。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
10.6.1	10 通信及び運用管理	10.6 ネットワークセキュリティ管理	10.6.1 ネットワーク管理策	ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御することが望ましい。	クラウド利用者は、クラウドサービスの利用に関して、ネットワークサービスに関する情報をクラウド事業者に求めることが望ましい。クラウド利用者は、必要に応じて、私設網又は暗号化された通信経路を介してクラウドサービスを利用することが望ましい。	仮想化技術を用いて構築されたクラウドコンピューティング環境における仮想ネットワークは、物理ネットワーク上の仮想インフラ上に構成されており、物理・論理ネットワークのセキュリティポリシーが適切に誤和していない場合、ネットワークのぜい弱性が生じ、システム停止やアクセス制御違反が発生する恐れがあるため、クラウド事業者は、物理ネットワークのセキュリティポリシーを考慮した仮想ネットワークのセキュリティポリシーを定めることが望ましい。また、クラウド事業者は、仮想ネットワークのセキュリティ設定マニュアルを定め、運用担当者に配付することが望ましい。	クラウド事業者は、仮想化されたネットワークを通しての脅威が存在することを念頭におき、対策を行うことが望ましい。特に、IaaSにおいては、スイッチやファイアウォールもネットワークと同じホスト OS上で、仮想化サービスとして提供されることがあるため、ホストOS のぜい弱性が、スイッチングやフィルタリング、ブロッキングなどのネットワーク関連機能に影響を与える可能性に留意する必要がある。	–	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いています。	適合可能	文献[01]では、ネットワークが必要に応じて信頼境界によって論理的に分離されること、分離するためにネットワークACLとフィルタが組み込まれていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 文献[71]では、仮想マシンとして利用可能なファイアウォールやWAFのイメージがマーケットプレースに多数用意されており、これらを組み合わせて用いることで利用者が必要とするファイアウォール機能やWAF機能が容易に利用可能であることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー – 分離」 文献[27] 文献[71]	–	–	（マイクロソフト社とのNDAにより開示）	利用者は、自組織が管理するネットワークについて、適切に管理する必要がある。
10.6.2	10 通信及び運用管理	10.6 ネットワークセキュリティ管理	10.6.2 ネットワークサービスのセキュリティ	すべてのネットワークサービス（組織が自ら提供するか外部委託しているかを問わない。）について、セキュリティ特性、サービスレベル及び管理上の要求事項を特定し、また、いかなるネットワークサービス合意書にもこれらを盛り込むことが望ましい。	クラウド利用者は、クラウドサービスに含まれるすべてのネットワークサービス（組織が自ら提供するかが部委託しているかを問わない。）について、セキュリティ特性、サービスレベル及び管理上の要求事項に適合することを確認することが望ましい。クラウド利用者は、クラウドサービスに含まれるすべてのネットワークサービスについて、セキュリティ特性、サービスレベル及び管理上の要求事項を、クラウド事業者との合意書に盛り込むことが望ましい。クラウド利用者はクラウドサービスに含まれるネットワークサービスが、セキュリティを保つ能力を判定が、常に監視することが望ましい。	クラウド事業者は、クラウドサービスに含まれるすべてのネットワークサービスについて、セキュリティ特性、サービスレベル及び管理上の要求事項を、クラウド利用者と合意することが望ましい。クラウド事業者は、クラウド利用者が監視できる機能を提供することが望ましい。クラウド事業者は、クラウドサービスにおけるこれらの対策の実施を確実にすることが望ましい。クラウド事業者は、クラウドサービスについて、セキュリティ特性、サービスレベル及び管理上の要求事項が、適切に実行されていることを監査などで確認し、必要に応じてクラウド利用者に監査結果などを明示することが望ましい。	–	–	Office 365 データ センター内のネットワークは、複数の個別のネットワーク セグメントを作成するように設計されています。このセグメント化により、重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの強力で安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ－脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織が管理するネットワークについて、適切に管理する必要がある。
10.7.1	10 通信及び運用管理	10.7 媒体の取扱い	10.7.1 取外し可能な媒体の管理	取外し可能な媒体の管理のための手順は、備えることが望ましい。	–	–	クラウド事業者は、クラウドサービスのデータのバックアップを媒体などで実施する場合には、その管理に留意する必要がある。	–	可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	利用者は、Office365の利用環境において、取外し可能な媒体の管理のための手順を定める必要がある。
10.7.2	10 通信及び運用管理	10.7 媒体の取扱い	10.7.2 媒体の処分	媒体が不要になった場合は、正式な手順を用いて、セキュリティを保ち、かつ、安全に処分することが望ましい。	–	–	–	–	すべての Microsoft Online Services は、承認された記憶メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.6 および 10.7.2) で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、マイクロソフトがベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、Microsoft Online Servicesのすべてのサービスが承認された記憶域メディアと廃棄管理サービスを使用していることが明示されている。	公開文書	文献[01]「DG-05：データ ガバナンス – 安全な廃棄」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、Office365の利用環境において、媒体の処分手順を定める必要がある。
10.7.3	10 通信及び運用管理	10.7 媒体の取扱い	10.7.3 情報の取扱手順	情報の取扱い及び保管についての手順は、その情報を認可されていない開示又は不正使用から保護するために、確立することが望ましい。	クラウド利用者は、クラウドサービス上の組織の情報を認可されていない開示又は不正使用から保護するために、確立する	–	–	–	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約案者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8.2) で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフがMicrosoft Online Services または GFS が開催するセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ること、またMicrosoft Online Servicesのすべての契約案者のスタッフおよびGFSのスタッフが、提供を受けるサービスや担う役割に応じたトレーニングを受ける必要があることが明示されている。 文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策および態勢が整備されていることが明示されている。 文献[01]では、不正アクセス検知時および発見時の監視について明示されている。また権限のあるアクセス、権限の無いアクセス、システム例外、情報セキュリティイベントの監査ログについて明示されている。	公開文書	文献[01]「HR-02：人的資源のセキュリティ – 雇用における変更事項」 「IS-11：情報セキュリティ－トレーニング/意識向上」 文献[01]「IS-22：情報セキュリティインシデント管理」 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」	–	–	–	利用者は、Office365上の情報の取扱い手順を定める必要がある。
10.7.4	10 通信及び運用管理	10.7 媒体の取扱い	10.7.4 システム文書のセキュリティ	システム文書は、認可されていないアクセスから保護することが望ましい。	–	–	–	–	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。Microsoft Online Services では、Office 365 サービスの一環として、包括的なガイダンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 · ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 · Exchange 管理者向けのビデオ · ハイブリッド環境の構成に必要な記事および手順 · ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki · 停止や問題に関する情報が得られる、サービスの正常性ダッシュボード ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Online Services の管理者によって承認されていることが明示されている。また、利用者向けを含めた Microsoft Online Services のドキュメントがサイトに格納されていること、それらのドキュメントへのアクセスが担当業務に基づいて制限されていることが明示されている。	公開文書	文献[01]「OP-02：運用管理・文書化」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
10.8.1	10 通信及び運用管理	10.8 情報の交換	10.8.1情報交換の方針及び手順	あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えることが望ましい。	–	–	クラウド事業者は、情報交換の機能を含むクラウドサービスを提供する場合、この情報交換を保護するための機能を検討し、必要に応じて実装することが期待される。クラウド事業者は、クラウドサービスを利用した情報交換を保護するための機能及び利用手順を、クラウドサービスの利用を検討する者に明示することが期待される。クラウド事業者は、クラウドサービスを利用した情報交換を保護するための機能が適切に動作していることを監査などによって確認し、クラウド利用者にその実施の事実又は結果を明示することが期待される。クラウド利用者及びクラウド事業者は、クラウドサービスにおいて、通信経路が暗号化できず、データの改ざんチェック機能も備えていない機能がある可能性に留意する必要がある。	–	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 文献[01]では、Microsoft Online Services の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Online Services の管理者によって承認されていることが明示されている。また、Microsoft Online Services の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「SA-02：セキュリティアーキテクチャー – ユーザーID資格情報」	–	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
10.8.2	10 通信及び運用管理	10.8 情報の交換	10.8.2 情報交換に関する合意	組織と外部組織との間の情報及びソフトウェアの交換について，両者間での合意が成立することが望ましい。	—	—	—	—	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 文献[01]では、Microsoft Online Services の資産に対するアクセス権が、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されることが明示されている。 文献[01]では、標準的な運用手順が正式に文書化され Microsoft Online Services の管理者によって承認されていることが明示されている。また、Microsoft Online Services の資産にアクセスする権限が資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されていることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「SA-02：セキュリティアーキテクチャー - ユーザーID資格情報」	—	—	—	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
10.8.3	10 通信及び運用管理	10.8 情報の交換	10.8.3 配送中の物理的媒体	情報を格納した媒体は，組織の物理的境界を越えた配送の途中における，認可されていないアクセス，不正使用又は破損から保護することが望ましい。	—	—	—	—	可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一 可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
10.8.4	10 通信及び運用管理	10.8 情報の交換	10.8.4 電子的メッセージ通信	電子的メッセージ通信に含まれた情報は，適切に保護することが望ましい。	クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能があることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて，電子的メッセージ通信を利用する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを，クラウド事業者が監査していることを確認することが望ましい。	クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，電子的メッセージ通信を提供する場合は，電子的メッセージ通信に含まれた情報を適切に保護する機能が適切に動作していることを監査などによって確認し，必要に応じてクラウド利用者に監査結果を明示することが望ましい。	—	—	業界標準のトランスポート層セキュリティ（TLS)/SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.8）で、"情報の交換" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。	公開情報	文献[01]「IS-18：情報セキュリティ－暗号化」	—	—	—	利用者は、Office365の利用環境における電子的メッセージ通信の保護対策を適切に実施する必要がある。
10.8.5	10 通信及び運用管理	10.8 情報の交換	10.8.5 業務用情報システム	業務用情報システムの相互接続と関連がある情報を保護するために，個別方針及び手順を策定し，実施することが望ましい。	—	—	—	—	Office365はSaaSであり、業務用情報システムは対象外。	対象外	—	—	—	—	—	—	—
10.9.1	10 通信及び運用管理	10.9 電子取引サービス	10.9.1 電子商取引	公衆ネットワークを経由する電子商取引に含まれる情報は，不正行為，契約紛争，認可されていない開示及び改ざんから保護することが望ましい。	—	—	—	—	Office 365 は電子商取引ソリューションではありません。	対象外	—	—	—	—	—	—	—
10.9.2	10 通信及び運用管理	10.9 電子取引サービス	10.9.2 オンライン取引	オンライン取引に含まれる情報は，次の事項を未然に防止するために，保護することが望ましい。 －不完全な通信 －誤った通信経路設定 －認可されていないメッセージの変更 －認可されていない開示 －認可されていない複製又は再生	—	—	—	—	Office 365 は電子商取引ソリューションではありません。	対象外	—	—	—	—	—	—	—
10.9.3	10 通信及び運用管理	10.9 電子取引サービス	10.9.3 公開情報	認可されていない変更を防止するために，公開システム上で利用可能な情報の完全性を保護することが望ましい。	—	—	—	—	Office 365 は電子商取引ソリューションではありません。	対象外	—	—	—	—	—	—	—
10.10.1	10 通信及び運用管理	10.10 監視	10.10.1 監査ログ取得	利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを取得することが望ましく，また，将来の調査及びアクセス制御の監視を補うために，合意された期間，保持することが望ましい。	クラウド利用者は，クラウドサービス上で取得された監査ログは，将来の調査及びアクセス制御の監視を補うために，適切な期間，保持されることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得される監査ログが，クラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログは，将来の調査及びアクセス制御の監視を補うために，適切な期間，保持されることを確認することが望ましい。クラウド利用者は，クラウドサービス上で取得される監査ログが，クラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログの存在を確認することが望ましい。クラウド利用者は，クラウドサービス上で取得された監査ログが，将来の調査及びアクセス制御の監視を補うために適切かどうか確認することが望ましい。	クラウド事業者は，クラウドサービス上で取得するクラウドサービスの利用者の活動，例外処理及びセキュリティ事象を記録した監査ログを特定し，取得する機能をクラウド利用者に提供することが望ましい。 クラウド事業者は，クラウドサービス上で取得された監査ログは，クラウド利用者の将来の調査及びアクセス制御の監視を補うことを考慮し，保持する期間を定めることが望ましい。クラウド事業者は，クラウドサービス上で取得する利用者の活動，例外処理及びセキュリティ事象を記録した監査ログについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログの提供方法，提供のタイミングについて，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービス上で取得した監査ログを保持する期間を，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，ログの取扱いについて，個別のクラウド利用者の要請に応じることができることを考慮することが期待される。監査ログの内容及び提供方法に関しては，クラウド利用者とクラウド事業者が合意した形式で実施することが期待される。	アクセスログの取得・分析による不正アクセスの検知によって、セキュリティ確保が図られる。	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス テケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間 (24時間、48時間、過去7日、カスタム：30日まで) に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockbox プロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「SA-14：セキュリティアーキテクチャー - 監査ログ／侵入検出」 文献[17]のF.ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、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。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
10.10.2	10 通信及び運用管理	10.10 監視	10.10.2 システム使用状況の監視	情報処理設備の使用状況を監視する手順を確立すること．及び監視活動の結果を定めに従ってレビューすることが望ましい。	クラウド利用者は，クラウドサービスの使用状況を監視する手順を確立することが望ましい。また，監視活動の結果を定めに従ってレビューすることが望ましい。 クラウド利用者は，クラウドコンピューティングサービスの利用状況の監視手順を策定するために，クラウド事業者に次のような事項を確認することが望ましい。 a) 利用状況の記録の種類 b) 利用状況の記録の表示方法 c) 利用状況の記録の保持期間	クラウド事業者は，クラウドサービス上で使用状況をクラウド利用者が監視できる機能を提供することが望ましい。	—	アクセスログの取得・分析による不正アクセスの検知によって，セキュリティ確保が図られる。	マイクロソフトでは，定められたしきい値またはイベントに基づいた予防的な容量管理や、サービスのパフォーマンスおよび可用性、CPU 使用率、サービス使用率、ストレージ使用率、ネットワーク待ち時間が許容範囲であることを監視するハードウェアおよびソフトウェア サブシステムなどの運用プロセスを用意しています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ－脆弱性/更新プログラム管理」「IS-31：情報セキュリティ－ネットワーク/インフラストラクチャのサービス」	(マイクロソフト社とのNDAにより開示)	(マイクロソフト社とのNDAにより開示)	—	利用者は、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。
10.10.3	10 通信及び運用管理	10.10 監視	10.10.3 ログ情報の保護	ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護することが望ましい。	クラウド利用者は，クラウドサービス上のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確認するために，次のような情報をクラウド事業者に対して求めることが望ましい。 a) ログ情報の保護に関する方針 b) ログ情報の保護機能の概要 c) ログ情報の保護が適切に動作していることに関するクラウド事業者による監査の実施状況又は結果	クラウド事業者は，クラウドサービス上のクラウド利用者のログ機能及びログ情報が，改ざん及び認可されていないアクセスから保護されていることを確実にすることが望ましい。	クラウド事業者は，クラウドサービス上でログ情報を一括して取得し，一括した改ざん防止を行っている場合，必要なログとして提供されるログの完全性が担保できない可能性があることに留意することが期待される。	—	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス テナントの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 文献[01]では、情報システム監査ツールへのアクセスは、Microsoft Online Services で権限が与えられた担当者のみに制限されていることが明示されている。また、管理者は特定のタスクを実行するのに必要なアクセス権だけを持ち、エラーの可能性を抑えて、必要な場合に限りシステムや機能にアクセスできるようにしていることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ/整合性」 文献[01]「IS-29：情報セキュリティ－監査ツールへのアクセス」	(マイクロソフト社とのNDAにより開示)	—	—	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
10.10.4	10 通信及び運用管理	10.10 監視	10.10.4 実務管理者及び運用担当者の作業ログ	システムの実務管理者及び運用担当者の作業は，記録することが望ましい。	クラウド利用者は，クラウドサービス上に構築した利用者システムの実務管理者及び運用担当者の作業が，記録されていることを確認することが望ましい。クラウド利用者は，クラウドサービス上で記録された，システムの実務管理者及び運用担当者の作業の記録を，規定に従ってレビューすることが望ましい。	クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を，記録する機能を提供することが望ましい。クラウド事業者は，クラウドサービス上で，クラウド利用者のシステムの実務管理者及び運用担当者の作業を記録する機能を，クラウドサービスの利用を検討する者に明示することが望ましい。 クラウドコンピューティング環境に対する特権操作がクラウド利用者にゆだねられる場合，責任分界を明確にするために，クラウド事業者及びクラウド利用者双方の作業ログを取得・保管することが望ましい。	クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なときに必要なログが提供されない可能性に留意する必要がある。 クラウド利用者は，作業ログに関する仕様を確認したり，第三者タイムスタンプ及びWORM （Write－Once－Read－Many，書込み1回のみ可能かつ消去・変更不可）デバイスの盗聴防止機能の有無を確認することが期待される。 クラウド利用者は，クラウドサービスにおいて運用担当者のログが提供されない場合には，どのようなログをクラウド事業者が取得しているかについて情報提供を求めることが期待される。	—	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス テナントの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ/整合性」 文献[07]「FAQ37」	(マイクロソフト社とのNDAにより開示)	—	—	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
10.10.5	10 通信及び運用管理	10.10 監視	10.10.5 障害のログ取得	障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。	クラウド利用者は，クラウドサービス上の障害のログを取得し，分析し，また，障害に対する適切な処置をとることが望ましい。	クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を定めることが望ましい。クラウド事業者は，クラウド利用者に障害のログを提供する機能を提供することが望ましい。クラウド事業者は，クラウド利用者に提供する，障害のログの範囲を，クラウドサービスの利用を検討する者に明示することが望ましい。 クラウド事業者は，クラウド利用者に提供する，障害のログの提供方法を，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド利用者は，クラウド事業者がログ情報を一括して取得し，一括した管理を行っている場合，必要なログが提供されない可能性に留意する必要がある。	—	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス テナントの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[74]を確認したところ、「(5)情報開示姿勢」について、マイクロソフト社の情報開示方針及び開示内容が確認できた。また、リスク管理に直結する事項についても情報を開示していることが確認できた。また、インタビューの結果、Office365管理ポータル画面で操作できる事項について、利用者側でログ出力が可能であることが確認できた。	要NDA	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ/整合性」 文献[07]「FAQ37」 文献[74]	(マイクロソフト社とのNDAにより開示)	(マイクロソフト社とのNDAにより開示)	—	利用者は、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。
10.10.6	10 通信及び運用管理	10.10 監視	10.10.6 クロックの同期	組織又はセキュリティ領域内のすべての情報処理システム内のクロックは，合意された正確な時刻源と同期させることが望ましい。	クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差が発生するか確認することが望ましい。クラウド利用者は，クラウドサービスと組織内のシステムとの時刻差を定期的に監視・記録し，時刻差が発生することによって，影響がある事項を洗い出し，管理策を検討することが望ましい。クラウド利用者は，分析などにおいて，ログに記録された時刻など，クラウドサービスの時刻の差を考慮することが望ましい。	クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させることが望ましい。クラウド事業者は，クラウドサービスのすべての情報処理システム内のクロックを，合意された正確な時刻源と同期させる仕組みを，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，標準時の異なる複数の地域にまたがるシステムのクロックのずれに留意することが望ましい。クラウド事業者は，IaaS においては，仮想環境の時刻ずれのリスクに留意する必要がある。	—	Office365 のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準（PST、GMT、UTC など）を使用しています。可能な場合は、Office365 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Office365 サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格（具体的には付属文書 A の項 10.10.6）で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Online Services のすべてのサービスでは、一貫した時刻設定基準（PST、GMT、UTC など）を使用し、可能な場合は、Microsoft Online Services 環境全体で正確な時刻を維持するために、NTP を通じて同期されることが明示されている。	公開文書	文献[01]「SA-12：セキュリティアーキテクチャ － 時刻の同期」	(マイクロソフト社とのNDAにより開示)	—	—	利用者は、Office365の利用環境の時刻同期を実施する必要がある。

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目番号	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
11.1.1	11 アクセス制御	11.1 アクセス制御に対する業務上の要求事項目的	11.1.1 アクセス制御方針	アクセス制御方針は，アクセスについての業務上及びセキュリティの要求事項に基づいて確立し，文書化し，レビューすることが望ましい。	クラウド利用者は，既存のアクセス制御方針が，クラウドサービスが提供するアクセス制御機能で実現できるか確認することが望ましい。クラウド利用者は，クラウドサービスの利用者のアクセス権を既存のアクセス制御方針に組み込むことが望ましい。	クラウド事業者は，提供するクラウドサービスにおいて，利用者のアクセス制御機能を提供することが望ましい。クラウド事業者は，提供するクラウドサービスにおいてクラウド利用者が実施可能なアクセス制御機能について，クラウド利用者に明示することが望ましい。	クラウドサービスのアクセス権を既存のアクセス制御方針に組み込む際に，クラウド利用者が考慮するポイントとして次のような事項がある。 a) アクセス制御に係る職務の分離（例えば，ID の使用者と登録者など） b) アクセス権限付与に関する承認プロセス c) クラウド利用者に付与されるアクセス制御権限	–	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり，正式な確認および更新のプロセスが適用されます。Microsoft Online Services の資産に対するアクセス権は，ビジネス要件に基づいて，資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 · 資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいて付与されます。 · 適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 · 物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 ISO 27001 規格（具体的には付属文書 A の項 11）で、“アクセス制御” が規定されています。	適合可能	文献[01]では，業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること，資産に対するアクセス権は知る必要性のある人間に限定する原則，および最小権限の原則に基づいて付与されることが明示されている。 また，管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと，ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること，スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では，利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ／整合性」 文献[07]「FAQ37」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は，自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.2.1	11 アクセス制御	11.2 利用者アクセスの管理	11.2.1 利用者登録	すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者の登録・登録抹消についての正式な手順を備えることが望ましい。	クラウド利用者は，すべての情報システム及びサービスへのアクセスを許可及び無効とするために，利用者ID の登録・削除についての正式な手順に，クラウドサービスの利用を考慮することが望ましい。クラウド利用者は，必要に応じてクラウド事業者に利用者ID の登録・削除機能に関する情報を求め，クラウド事業者が提供する機能で組織の正式な手順が実現できることを確認することが望ましい。	クラウド事業者は，クラウド利用者のクラウドサービス利用者ID の登録・削除機能を提供することが望ましい。また，このような機能について，必要に応じて次の情報を提供することが望ましい。 a) 利用者 ID 登録・削除の手順 b) 利用者 ID 登録・削除に必要な情報 c) 利用者の同一性検証の仕様 d) サービスの一部として利用者ID 管理ツールを提供している場合は，利用者ID 管理ツールの仕様	クラウド利用者は，クラウドサービスの形態によっては，クラウドサービスの利用者ID を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド提供者が登録を代行する場合など，様々な形態が存在することを考慮する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザが存在する場合や，クラウド利用者の環境にクラウド事業者が利用する利用者ID を作成する必要がある場合は，クラウド利用者とクラウド提供者の間でその管理責任を明確に定義することが期待される。	–	当社がお客様のアカウントを作成することはありません。お客様自身が、Microsoft Online Services ポータルで直接アカウントを作成するか、またはローカルの Active Directory 内にアカウントを作成します。それらのアカウントは、Microsoft Online Services と同期することができます。そのため、作成するユーザー アカウントの正確性については、お客様がその責任を負います。	適合可能	文献[01]では、利用者アカウントの登録は利用者側の責任であることが明示されている。	公開文書	文献[01]「HR-03：人事 － 雇用の終了」	–	–	–	利用者は，自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.2.2	11 アクセス制御		11.2.2 特権管理	特権の割当て及び利用は，制限し，管理することが望ましい。	クラウド利用者は，特権の割当て及び利用を管理する既存の仕組みが，クラウドサービス上で実現できるか確認し，クラウドサービス利用における特権を管理することが望ましい。	クラウド事業者は，クラウド利用者に特権を付与する場合には，クラウド利用者がクラウドサービスにおける特権を管理する機能を提供することが望ましい。また，このような機能について，次のような情報をクラウド利用者に提供することが望ましい。 a) クラウド利用者の特権の種類及び役割 b) クラウド利用者の特権アカウント使用の監視・管理機能の仕様 c) クラウド利用者の特権アカウント使用に関するログ	クラウド利用者はクラウドサービスの形態によっては，特権を登録する際に，クラウド利用者が自ら設定できる場合や，クラウド事業者が登録を実施するなど，様々な形態が存在することに留意する必要がある。クラウドサービスの提供のために，クラウド利用者の環境にデフォルトユーザとして特権が存在する場合や，クラウド利用者の環境にクラウド事業者の特権を作成する必要がある場合は，クラウド利用者とクラウド事業者の間でその管理責任を明確に定義することが期待される。	–	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。（社内、社外） 管理者監査ログ 管理者が Exchange Online 環境で行った変更（RBAC の役割または Exchange の ポリシーや設定の変更など）を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。	適合可能	文献[01]では、情報セキュリティポリシーにおいて、業務の正当性に基づいてMicrosoft Online Servicesの資産にアクセスする権限の付与が必要になること、このアクセス権は、資産の所有者の承認によって付与され、知る必要性のある人間に限定する原則と最小特権の原則に基づいて制限されることを確認した。	公開文書	文献[01]	–	–	–	利用者は，自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.2.3	11 アクセス制御		11.2.3 利用者パスワードの管理	パスワードの割当ては，正式な管理プロセスによって管理することが望ましい。	クラウド利用者は，パスワードの割当てに関する既存の正式な管理プロセスが，クラウドサービスが提供する機能で実現できるか確認することが望ましい。クラウド利用者は，クラウド事業者があらかじめ設定したパスワード（初期パスワードなど）を，システム又はソフトウェアのインストール後に変更することが望ましい。	クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて利用するパスワードの割当ての管理プロセスの機能について，次のような情報を提供することが望ましい。 a) パスワードの発行，変更及び再発行の手順 b) パスワード割当てにおける認証及び認証の仕組み（例えば，多要素認証を用いた認証方法など）	クラウドサービスの利用者パスワードの管理機能は，利用するクラウドサービスの形態によっては，適切なインタフェースをクラウド利用者が設計する必要があることに留意する必要がある。	–	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365の認証については、強いパスワードのみが使用可能となっています。	適合可能	文献[01]では，パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開情報	文献[01]「SA-02：セキュリティアーキテクチャー － ユーザーID資格情報」 文献[17]	（マイクロソフト社とのNDAにより開示）	–	–	利用者は，承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負う。
11.2.4	11 アクセス制御		11.2.4 利用者アクセス権のレビュー	管理者は，正式なプロセスを使用して，利用者のアクセス権を定められた間隔でレビューすることが望ましい。	クラウド利用者は，アクセス権を一覧化する機能の仕様について，クラウド事業者に情報を求めることが望ましい。 クラウド利用者は，クラウドサービスの利用者のアクセス権をレビューする正式なプロセスが，クラウドサービスの機能で実現できることを確認することが望ましい。	クラウド事業者は，クラウドサービスにおいて，クラウド利用者がアクセス権をレビューする機能を提供することが望ましい。	–	–	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり、正式な確認および更新のプロセスが適用されます。Microsoft Online Services の資産に対するアクセス権は、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 · 資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されます。 · 適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 · 物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 ISO 27001 規格（具体的には付属文書 A の項 11）で、“アクセス制御” が規定されています。 管理者、およびアプリケーションやデータの所有者は、誰がアクセスしているかを定期的に確認する責任を負います。Microsoft Online では、提供しているサービスの中でお客様がエンド ユーザーによるアクセスの監査と委任を行うための強化された機能を用意しています。詳細については、対応するサービスの説明を参照してください。 ISO 27001 規格（具体的には付属文書 A の項 11.2）で、“ユーザー アクセスの管理と特権の管理” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、Microsoft Online Servicesの資産に対するアクセス権がビジネス要件に基づいて資産の所有者の承認を得たうえで付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 さらに、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられたスタッフまたは契約業者のスタッフに制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 加えて、Microsoft Online Servicesでは、利用者によるアクセスの監査と委任を行うための強化された機能を用意していることが明示されている。 文献[16][17]では、お客様がデータにアクセスできるユーザーとデータの使用方法を制御できることが明示されている。	公開情報	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限／承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー － データのセキュリティ／整合性」 文献[16]「ユーザー アカウント管理」 文献[17]「ユーザー アクセスへの対応」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は，自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.3.1	11 アクセス制御	11.3 利用者の責任	11.3.1 パスワードの利用	パスワードの選択及び利用時に，正しいセキュリティ慣行に従うことを，利用者に要求することが望ましい。	–	–	クラウド事業者は，クラウド利用者が，パスワードの選択及び利用をする際に，正しいセキュリティ慣行に従うことができる機能を提供することが期待される。クラウドサービスでは，複数のサービスを組み合わせて一つのパスワードを利用する場合があるので，クラウド事業者は，真の良いパスワードを用いることをクラウド利用者に助言することを考慮する必要がある。	–	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365の認証については、強いパスワードのみが使用可能となっています。	適合可能	文献[01]では，パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開文書	文献[01]「SA-02：セキュリティアーキテクチャー － ユーザーID資格情報」 文献[17]	（マイクロソフト社とのNDAにより開示）	–	–	利用者は，承認されていない第三者にパスワードが開示されないようにする責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任と、事実上推測できない十分なエントロピーを備えたパスワードを選択する責任を負う。
11.3.2	11 アクセス制御	11.3 利用者の責任	11.3.2 無人状態にある利用者装置	利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にすることが望ましい。	–	–	クラウド利用者は，共有環境でクラウドサービスを利用する場合には，認可されないアクセスについて留意する必要がある。	–	利用者環境については対象外。	対象外						利用者は，自組織が管理する無人状態の装置がある場合、その保護対策を策定する必要がある。
11.3.3	11 アクセス制御	11.3 利用者の責任	11.3.3 クリアデスク，クリアスクリーン方針	書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。	–	–	–	–	利用者環境については対象外。	対象外						利用者は、医療機関等の利用者側の施設における，適切な端末管理（スクリーンロック等）を行う必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応								SI事業者・利用者で必要な対応
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
11.4.1	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.1 ネットワークサービスの利用についての方針	利用することを特別に認可したサービスへのアクセスだけを，利用者に提供することが望ましい。	クラウド利用者は，ネットワークサービスの利用に関する方針に，クラウドサービスの利用に関する考慮事項を含めることが望ましい。クラウド利用者は，適切なクラウドサービスの利用者のみクラウドサービスが利用できるようネットワークを構成する方針を定めることが望ましい。 クラウド利用者は，クラウドサービスのネットワークの利用に関する方針に次の事項を含めることを確実にすることが望ましい。 a) ネットワークアクセス制御方針 b) アクセス管理サービス方針	クラウド事業者は，クラウドサービスの利用に関する方針をネットワークサービスの利用に関する方針を策定できるよう，クラウドサービス利用の管理に係る情報の種類及びその内容を提示することが望ましい。	クラウド事業者は，仮想化ソフトウェア固有の課題（例えば，仮想マシンから他仮想マシンへの攻撃など，仮想化ソフトウェア内での攻撃）を考慮し，各仮想マシンの隔離設計に留意する必要がある。クラウド事業者は，隔離設計は，物理ネットワーク側での対応や，ゾーン機能やプライベート VLAN 機能などの機能を活用する方法や，同機能を有するサードパーティ製品の活用などに留意する必要がある。	–	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。 Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモート ワーカーから Azure Virtual Network への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Azure データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[01]では、アクセス制御としてアクセスポリシー、アクセスの許可、最小限の権限、完全性及び秘密保持、認証、ネットワーク設計が含まれることを確認した。 文献[107]では、必要に応じて相互認証が可能なVPN接続を使用出来ることが明示されている。 また、インタビューにて、インターネットを経由したVPNで接続する場合には、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	文献[01] 文献[107]	–	（マイクロソフト社とのNDAにより開示）	–	–
11.4.2	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.2 外部から接続する利用者の認証	遠隔利用者のアクセスを管理するために，適切な認証方法を利用することが望ましい。	クラウド利用者は，自らが管理していないネットワーク（公衆無線LAN や携帯電話網による接続など）からクラウドサービスを利用する際に，適切な認証方法を利用することが望ましい。	クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を提供することが望ましい。クラウド事業者は，クラウドサービスへの接続方法に応じた認証方法を，クラウドサービスの利用を検討する者に明示することが望ましい。	–	–	改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 Office 365で、利用者・管理者のクライアント端末とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。	公開文書	文献[01]「SA-07: セキュリティアーキテクチャー – リモートユーザーの多要素認証」	–	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.4.3	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.3 ネットワークにおける装置の識別	特定の場所及び装置からの接続を認証するための手段として，自動的装置識別を考慮することが望ましい。	–	–	クラウド事業者は，クラウドサービスに接続する装置において，識別を可能にする機能（電子証明書やIO チップなどを利用した識別機能）を提供することが期待される。	–	Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモート ワーカーから Azure Virtual Network への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Azure データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[107]では、必要に応じて相互認証が可能なVPN接続を使用出来ることが明示されている。	公開文書	文献[107]	–	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.4.4	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.4 遠隔診断用及び環境設定用ポートの保護	診断用及び環境設定用ポートへの物理的及び論理的なアクセスは，制御することが望ましい。	クラウド利用者は，クラウド利用者がクラウドサービスの遠隔診断用及び環境設定ポートを管理する場合には，厳密に管理することが望ましい。	クラウド事業者は，クラウドサービスに遠隔診断用及び環境設定ポートが存在する場合は，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，クラウドサービスのホストOS 上で動作する仮想スイッチや仮想ファイアウォールなどの遠隔診断用及び環境設定ポートが存在する場合は，厳密に管理することが期待される。	–	Microsoft Online Services では、データ センターの物理的な コントロールを通じて診断ポートおよび構成ポートへの物理的なアクセスを制御します。診断ポートおよび構成ポートへのアクセスは、サービス/資産の所有者と、アクセスを必要としているハードウェア/ソフトウェアのサポート担当者の間の申し合わせによって初めて可能になります。ポート、サービス、およびコンピューターやネットワーク機器にインストールされている同様の機能の中で、ビジネス機能において特に必要とされないものは、無効にされるか削除されます。 ISO 27001 規格（具体的には付属文書 A の項 10.6.1、11.1.1、および 11.4.4）で、"ネットワーク制御とアクセス制御" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、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することが明示されている。	公開文書	文献[01]「IS-30: 情報セキュリティ - 診断/構成ポートへのアクセス」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
11.4.5	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.5 ネットワークの領域分割	情報サービス，利用者及び情報システムは，ネットワーク上，グループごとに分割することが望ましい。	クラウド利用者は，クラウド事業者のネットワークにおける分離を要求する必要性について考慮することが望ましい。 クラウド利用者は，クラウドサービスのネットワークを分離するため，ネットワークを異なるドメインに分離する機能の使用について，必要に応じてクラウド事業者に情報を求めることが望ましい。 クラウド利用者は，クラウドサービスの利用者のアクセス権限に基づいて，クラウドサービスのネットワークを論理的に分離することが望ましい。	クラウド事業者は，各クラウド利用者に割り当てたコンピューティング資源に，他のクラウド利用者や許可されていないユーザがアクセスできないように管理し，物理的な設定や移行にかかわらず，仮想環境の分離を確実にすることが望ましい。ネットワーク若しくはインタフェースの分離がなされていない場合，クラウド事業者は，アプリケーションレイヤの通信のエンドツーエンドでの暗号化を考慮することが望ましい。 クラウド事業者は，クラウド利用者の情報及びソフトウェアへのバックドアアクセスの可能性を識別するために，クラウド環境における情報セキュリティについて評価を実施することが望ましい。	クラウド事業者は，クラウドサービスのホストOS 上で動作する仮想スイッチや仮想ファイアウォールなどのネットワークを構成するように設計されています。このセグメント化により、重要なバックエンドサーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	–
11.4.6	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.6 ネットワークの接続制御	共有ネットワーク，特に，組織の境界を越えて広がっているネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続能力を制限することが望ましい（11.1 参照）。	クラウド利用者は，クラウドサービスのネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続を許可する範囲を制限することが望ましい。利用者のネットワークへのアクセス権は，アクセス制御方針の要求に従って，維持・更新することが望ましい。	クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを特定することが望ましい（例えば，電子メールなどのメッセージ通信，ファイル転送など）。クラウド事業者は，クラウドサービスで利用可能なネットワークサービスを，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，クラウドコンピューティングで利用できるサービスを増やすことで，他のゲストOSや，外部から受ける影響の増加に留意する必要がある。	–	Office 365 データ センター内のネットワークは、複数の個別のネットワーク セグメントを作成するように設計されています。このセグメント化により、重要なバックエンドサーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	–
11.4.7	11 アクセス制御	11.4 ネットワークのアクセス制御	11.4.7 ネットワークルーティング制御	コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，ルーティング制御の管理策をネットワークに対して実施することが望ましい。	クラウド利用者は，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするために，クラウドサービスを，ルーティング制御の管理策に加えることが望ましい。 クラウド事業者が，ホストOS 上のネットワークルーティングを行う場合は，クラウド利用者は，その設定が，コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反していないことを確認することが望ましい。	クラウド事業者は，ホストOS 上のネットワークルーティングについて，適切に設定することが望ましい。 クラウド事業者は，ホストOS 上のネットワークルーティングについて，適切に設定していることを利用者に明示することが望ましい。	ホストOS 上のネットワークルーティングについて，クラウド利用者が設定できる場合は，影響を考慮して設定する必要がある。	–	Office 365 データ センター内のネットワークは、複数の個別のネットワーク セグメントを作成するように設計されています。このセグメント化により、重要なバックエンドサーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	–
11.5.1	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.1 セキュリティに配慮したログオン手順	オペレーティングシステムへのアクセスは，セキュリティに配慮したログオン手順によって制御することが望ましい。	クラウド利用者は，クラウドサービスのオペレーティングシステムにログオンする場合，セキュリティに配慮したログオン手順で制御する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，クラウドサービスのオペレーティングシステムにクラウド利用者がログオンする場合，セキュリティに配慮したログオン手順で制御する機能を提供することが望ましい。また，そのような機能について，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウドサービスの形態においては，オペレーティングシステムが複数存在し，その利用者も異なる可能性があるため，クラウド事業者は，クラウド利用者の資産と権限に留意し，ログオン手順を定めることを求めることが期待される。	–	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365の認証については、強いパスワードのみが使用可能となっています。	適合可能	文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開情報	文献[01]「SA-02: セキュリティアーキテクチャー – ユーザーID資格情報」 文献[17]	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、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。
11.5.2	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.2 利用者の識別及び認証	すべての利用者は，各個人の利用ごとに一意な識別子（利用者ID）を保有することが望ましい。また，利用者が主張する同一性を検証するために，適切な認証技術を選択することが望ましい。	クラウド利用者は，クラウドサービスにおいて，すべてのクラウドサービスの利用者が，各個人の利用ごとに一意な識別子（利用者ID）を保有することができるか確認することが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術の選択が可能であるかを確認することが望ましい。	クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者ID）を保有することができるようにすることが望ましい。また，クラウドサービス利用者が主張する同一性を検証するために，クラウドサービスにおいて，適切な認証技術を選択することができる機能を提供することが望ましい。クラウド事業者は，クラウドサービスにおいて，すべてのクラウドサービス利用者に，各個人の利用ごとに一意な識別子（利用者ID）を保有することができるかどうか，クラウドサービスの利用を検討する者に明示することが望ましい。クラウド事業者は，クラウドサービスにおいて，選択できる認証技術を，クラウドサービスの利用を検討する者に明示することが望ましい。	クラウド事業者は，ID 管理をするサービスが，クラウドサービス利用者ID を個別に発行できるように設定することが期待される。クラウド事業者は，ID 管理をするサービスが，共有ID を発行する場合は，利用者が共有IDの利用者を個別に認識する必要があるか，検討が必要なことを明示することが期待される。	–	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365の認証については、強いパスワードのみが使用可能となっています。	適合可能	文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開情報	文献[01]「SA-02: セキュリティアーキテクチャー – ユーザーID資格情報」 文献[17]	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、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。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
11.5.3	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.3 パスワード管理システム	パスワードを管理するシステムは，対話式とすることが望ましく，また，良質なパスワードを確実とするものが望ましい。	クラウド利用者は，クラウドサービスのパスワードを管理するシステムが，対話式であり，また，良質なパスワードを確実とする機能があることを確認することが望ましい。	クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，対話式とすることが望ましい，クラウド事業者は，クラウドサービスのパスワードを管理するシステムを，良質なパスワードを確実とする機能とすることが望ましい，クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，対話式であることを，開示することが望ましい，クラウド事業者は，クラウドサービスのパスワードを管理するシステムは，良質なパスワードを確実とする機能があることを，利用を検討する者に明示することが望ましい。	クラウド事業者は，ID 管理をするサービスが，パスワード管理を適切に行われるように設定するとと同時に，その設定を機能させるインタフェースを提供することが期待される。クラウド事業者は，ID 管理をするサービスのみを提供する場合は，パスワードの管理が適切に行われるように設定する手順や，その設定を機能させるインタフェースを作成するための手順を利用者に明示することが期待される。	–	Office 365にログインする際のパスワード入力は非表示が可能であり、パスワードポリシーによりパスワードの複雑性を管理する事も可能です。 Office365の認証については、強いパスワードのみが使用可能となっています。	適合可能	文献[01]では、パスワードポリシーの適用状況が管理されており、強制的にユーザーに複雑なパスワードを使用させることが明示されている。 文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開情報	文献[01]「SA-02：セキュリティアーキテクチャー – ユーザーID資格情報」 文献[17]	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、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。
11.5.4	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.4 システムユーティリティの使用	システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理することが望ましい。	クラウド利用者は，クラウドサービスのシステム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムの使用を，制限し，厳しく管理することが望ましい。	クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラムを特定することが望ましい，クラウド事業者は，システム及び業務用ソフトウェアによる制御を無効にすることのできるユーティリティプログラム，クラウドサービスの利用を検討する者に明示することが望ましい。	システム管理者の利便性を重視するクラウドサービスの機能は，システム及びアプリケーションの管理策を無効化できるユーティリティプログラムである場合がある，クラウド利用者組織におけるクラウドサービス利用者に対しては，そのようなユーティリティプログラムの使用は制限し，厳密に管理することが期待される。	–	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり、正式な確認および更新のプロセスが適用されます。Microsoft Online Services の資産に対するアクセス権は、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 · 資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいて付与されます。 · 適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 · 物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 ISO 27001 規格（具体的には付属文書 A の項 11.2）で、"ユーザー アクセスの管理と特権の管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、アクセス制御ポリシーを用いることにより、利用者の資産に対するアクセス制御がビジネス要件に基づいて行われることが明示されている。また、資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいていること、適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てられることが明示されている。	公開情報	文献[01]「IS-08：情報セキュリティ – ユーザーアクセスの制限／承認」	–	–	–	利用者は、管理者アカウント等のシステムユーティリティを利用可能なアカウントを厳格に管理する必要がある。
11.5.5	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.5 セッションのタイムアウト	一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断することが望ましい。	クラウド利用者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションが遮断されることを確認することが望ましい。	クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能を提供することが望ましい，クラウド事業者は，クラウドサービスの利用中に，一定の使用中断時間が経過したときは，使用が中断しているセッションを遮断する機能について開示することが望ましい。	クラウド利用者は，利用するクラウドサービスによっては，タイムアウトによる遮断をしてはならないサービスもあることに留意する必要がある。クラウド事業者は，仮想 OS の管理アクセス対応機能ではホスト OS へのアクセス制御において，セッションタイムアウトに未対応のものがあることに留意する必要がある。クラウド利用者は，セッションタイムアウトについて端末のスクリーンセイバーの制限など他の管理策を実施できることに留意する必要がある。	–	いずれかの Office 365 Web アプリに認証すると、使用中のブラウザーと Office 365 Web アプリの間でセッションが確立されます。セッションの期間中は、Web アプリを再認証する必要はありません。ユーザーが非アクティブである場合、ユーザーがブラウザーまたはタブを閉じた場合、またはパスワード再設定などのその他の理由により認証トークンが期限切れになった場合に、セッションが期限切れになる可能性があります。Office 365 のさまざまな Web アプリには、それぞれ異なるセッション タイムアウトが設定されています。既定のタイムアウト値は、アプリの通常時の使用法と合致します。	適合可能	文献[95]では、Office365のサービス毎にセッションタイムアウトの時間が定められていることが明示されている。	公開文書	文献[95]	–	–	–	–
11.5.6	11 アクセス制御	11.5 オペレーティングシステムのアクセス制御	11.5.6 接続時間の制限	リスクの高い業務用ソフトウェアに対しては，更なるセキュリティを提供するために，接続時間の制限を利用することが望ましい。	クラウド利用者は，利用における リスクが高いと判断したクラウドサービスに対しては，接続時間の制限を利用できるか確認することが望ましい。	クラウド事業者は，利用におけるリスクが高いと判断されたクラウドサービスは，接続時間の制限を利用できる機能を提供することが望ましい，クラウド事業者は，リスクの高いクラウドサービスに対しては，接続時間の制限を利用できるかどうかを，開示することが望ましい。	クラウド事業者は，仮想OS の管理アクセス対応機能ではホストOS へのアクセス制御において，管理アクセス通信の接続時間の制限が未対応のものがあることに留意する必要がある。クラウド利用者は，接続時間について端末の利用時間の制限など他の管理策を実施できることに留意する必要がある。	–	いずれかの Office 365 Web アプリに認証すると、使用中のブラウザーと Office 365 Web アプリの間でセッションが確立されます。セッションの期間中は、Web アプリを再認証する必要はありません。ユーザーが非アクティブである場合、ユーザーがブラウザーまたはタブを閉じた場合、またはパスワード再設定などのその他の理由により認証トークンが期限切れになった場合に、セッションが期限切れになる可能性があります。Office 365 のさまざまな Web アプリには、それぞれ異なるセッション タイムアウトが設定されています。既定のタイムアウト値は、アプリの通常時の使用法と合致します。	適合可能	文献[95]では、Office365のサービス毎にセッションタイムアウトの時間が定められていることが明示されている。	公開文書	文献[95]	–	–	–	–
11.6.1	11 アクセス制御	11.6 業務用ソフトウェア及び情報のアクセス制御	11.6.1 情報へのアクセス制限	利用者及びサポート要員による情報及び業務用ソフトウェアシステム機能へのアクセスは，既定のアクセス制御方針に従って制限することが望ましい。	クラウド利用者は，クラウド利用者及びクラウド利用者のサポート要員によるクラウドサービスへのアクセスを，既定のアクセス制御方針に従って制限することが望ましい，クラウド利用者は，複数のシステムや情報を内包できるクラウドサービスでは，その重要性に応じて，アクセス権を強固にする必要があることに留意し，必要な管理策を設定できるような機能を準備することが望ましい。	クラウド事業者は，クラウド利用者におけるクラウドサービスへのアクセス制限のポート要員によるクラウドサービスへのアクセスを，既定のアクセス制御方針に従って制限することが望ましい，クラウド利用者が行える要件を定め，クラウドサービスの利用を検討する者に明示することが望ましい。	仮想マシンを操作するクライアントソフトウェアからは，ホストOS のサービスコンソール部分だけでなくゲストOS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施する必要があることに留意する必要がある。	–	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり、正式な確認および更新のプロセスが適用されます。Microsoft Online Services の資産に対するアクセス権は、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 · 資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいて付与されます。 · 適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 · 物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 ISO 27001 規格（具体的には付属文書 A の項 11.2）で、"ユーザー アクセスの管理と特権の管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、アクセス制御ポリシーを用いることにより、利用者の資産に対するアクセス制御がビジネス要件に基づいて行われることが明示されている。また、資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいていること、適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てられることが明示されている。	公開情報	文献[01]「IS-08：情報セキュリティ – ユーザーアクセスの制限／承認」	–	–	–	利用者は、ユーザーによる運用上もしくは業務上重要なファイルへのアクセス制限や記録・監査を適切に実施する必要がある。
11.6.2	11 アクセス制御	11.6 業務用ソフトウェア及び情報のアクセス制御	11.6.2 取扱いに慎重を要するシステムの隔離	取扱いに慎重を要するシステムは，専用の（隔離された）コンピュータ環境をもつことが望ましい。	クラウド利用者は，取扱いに慎重を要するシステムを，クラウドコンピューティングを利用して，構築する場合には，専用の（隔離された）コンピュータ環境上に構築できることを確認することが望ましい。	クラウド事業者は，取扱いに慎重を要するシステムを，クラウドコンピューティング内に構築する場合に備えて，専用の（隔離された）コンピュータ環境上に構築できる機能を提供することが望ましい。	クラウド利用者は，PaaS/IaaS 環境など，複数のシステムを内包できるクラウドサービス上では，そのシステムの重要性に応じて，アクセス権を強固にすることが期待される。クラウド事業者は，システム間の隔離をする管理策に留意する必要がある（仮想スイッチ上のarp スプーフィング防止機能など），仮想マシンを操作するクライアントソフトウェアからは，ホストOS のサービスコンソール部分だけでなくゲスト OS も操作することが可能な場合がある。その場合は，クラウド利用者は，権限管理をクラウドサービスの利用者ごとに細やかに設定して内部不正やシステム障害のリスクを減らすか，各仮想マシンへの管理アクセスは従来通りの方式で行うなど，仮想マシンを操作するクライアントソフトウェア経由でのアクセス時の権限管理を慎重に実施することが期待される。	–	Office365はSaaSであり、取扱いに慎重を要するシステムの構築は対象外。	対象外	–	–	–	–	–	–	–
11.7.1	11 アクセス制御	11.7 モバイルコンピューティング及びテレワーキング	11.7.1 モバイルのコンピューティング及び通信	モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するために，正式な方針を備え，また，適切なセキュリティ対策を採用することが望ましい。	クラウド利用者は，モバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，クラウドサービスを加え，適切な情報セキュリティ対策を採用することが望ましい，クラウドサービスにおいてモバイルコンピューティングを利用できる機能がある場合は，クラウド利用者は，その機能がモバイルコンピューティング設備・通信設備を用いた場合のリスクから保護するための正式な方針に，適合しているか確認することが望ましい。	クラウド事業者は，クラウドサービスにおいて，モバイルコンピューティングを利用できる機能を提供する場合は（一般的に，SaaS 又はアプリケーションレイヤにおけるサービスにおいて該当する），適切な情報セキュリティ対策を，クラウドサービスの利用を検討する者に明示することが望ましい。	モバイルコンピューティング設備・通信設備（例えば，ノート型コンピュータ，パームトップコンピュータ，ラップトップコンピュータ，IC カード，携帯電話）を用いる場合，業務情報が危険にさらされないことを確実にするために，特別な注意を払う必要がある，モバイルコンピューティング方針は，保護されていない環境におけるモバイルコンピューティング装置を用いた作業のリスクを考慮に入れる必要がある。 クラウドサービスでは，スマートフォンなどの携帯端末の利用を前提として提供されている場合があるため，それらの端末の利用についても留意する必要がある。	–	業界標準のトランスポート層セキュリティ（TLS)/SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化 (SSL)、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.8）で、"情報の交換" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	■盗聴・伝送データの暗号化 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。 文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 ■暗号鍵の管理主体 NDAに基づく文書を確認した結果、標準に従って暗号鍵が管理されていることが確認できた。	要NDA	文献[01]SA-11セキュリティアーキテクチャ・共有ネットワーク 文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利用した保存データの高度な暗号化」 文献[01]「IS-18：情報セキュリティ – 暗号化」	–	–	（マイクロソフト社とのNDAにより開示）	利用者は、モバイルコンピューティングで用いるOffice365の利用環境について、適切なセキュリティ対策を実施する必要がある。

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
11.7.2	11 アクセス制御	11.7 モバイルコンピューティング及びテレワーキング	11.7.2 テレワーキング	テレワーキングのための方針，運用計画及び手順を策定し，実施することが望ましい。	クラウド利用者は，クラウドサービスをテレワーキングで利用する場合，テレワーキングのための方針，運用計画及び手順に関する情報を提供する場合は，クラウドサービスにおいてテレワーキングを利用できる機能がある場合は，クラウド利用者は，その機能が，テレワーキングのための方針，運用計画及び手順に適合することを確認することが望ましい。	クラウドサービスにおいてテレワーキングを利用する機能を提供する場合は，テレワーキングの適切な保護を実施することが望ましい。クラウド事業者は，提供するクラウドサービスにおいて，テレワーキングを利用する機能を提供する場合は，講じているセキュリティのための管理策を，クラウドサービスの利用を検討する者に明示することが望ましい。	—	—	業界標準のトランスポート層セキュリティ（TLS）/SSL（Secure Sockets Layer）を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化（SSL）、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.8）で、“情報の交換” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	■盗聴・伝送データの暗号化 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。 文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 ■暗号鍵の管理主体 NDAに基づく文書を確認した結果、標準に従って暗号鍵が管理されていることが確認できた。	要NDA	文献[01]SA-11セキュリティアーキテクチャ・共有ネットワーク 文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利用した保存データの高度な暗号化」 文献[01]「IS-18：情報セキュリティ－暗号化」	—	—	（マイクロソフト社とのNDAにより開示）	利用者は、Office365を利用してテレワーキングを行う場合、運用計画および手順を策定する必要がある。
12.1.1	12 情報システムの取得，開発及び保守	12.1 情報システムのセキュリティ要求事項	12.1.1 セキュリティ要求事項の分析及び仕様化	新しいシステム又は既存の情報システムの改善に関する業務上の要求事項を記述した文書では，セキュリティの管理策についての要求事項を仕様化することが望ましい。	クラウド利用者は，システム構築の標準を記載した規程にクラウドサービス利用時の項目を追加することが望ましい。クラウド利用者は，システム利用標準に外部のクラウドサービスを利用する場合に必要な項目を追加することが望ましい。クラウド利用者は，システム利用標準には組織のセキュリティ基本方針とクラウド事業者のセキュリティ基本方針が組織のセキュリティ基本方針に反しないことを確認することが望ましい。 クラウド利用者は，クラウドサービスにおいて実施されている管理策が，組織のセキュリティ上の要求事項と整合しているかを分析・評価することが望ましい。この分析・評価の結果，情報セキュリティ要求事項を満たしていないと判断した場合，クラウドサービスの利用の制限や他の管理策の導入について検討することが望ましい。	クラウド事業者は，クラウドサービスで実装（提供）している情報セキュリティ対策及び機能を列記し，開示することが望ましい。	クラウド事業者によっては独自のオペレーティングシステムなどを利用している場合がある。この場合は標準的なオペレーティングシステムと違ってクラウド事業者からしかぜい弱性情報などを得ることができないことに留意すること。その場合，クラウド利用者は，クラウドサービスを単なるアウトソーシングと想定せずに，自らのシステムの一部としてクラウドサービスを把握し，クラウド事業者とのコミュニケーションをとりながら，情報セキュリティ対策を考慮することが期待される。	—	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、“情報セキュリティの意識向上、教育、およびトレーニング” が規定されています。	適合可能	文献[06]では、Microsoft Online Servicesの情報セキュリティとして、クラウドのセキュリティ設計、開発ライフサイクルのセキュリティ、サービスの運用及びコンプライアンスについて明示されている。	公開文書	文献[06]	—	—	—	—
12.2.1	12 情報システムの取得，開発及び保守	12.2 業務用ソフトウェアでの正確な処理	12.2.1 入力データの妥当性確認	業務用ソフトウェアに入力するデータは，正確で適切であることを確実にするために，その妥当性を確認することが望ましい。	—	—	—	—	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、“開発におけるセキュリティとサポート プロセス” が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Office365利用時の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。
12.2.2	12 情報システムの取得，開発及び保守	12.2 業務用ソフトウェアでの正確な処理	12.2.2 内部処理の管理	処理の誤り又は故意の行為によって発生する情報の破壊を検出するために、妥当性確認の機能を業務用ソフトウェアに組み込むことが望ましい。	—	—	—	—	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、“開発におけるセキュリティとサポート プロセス” が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	—
12.2.3	12 情報システムの取得，開発及び保守	12.2 業務用ソフトウェアでの正確な処理	12.2.3 メッセージの完全性	業務用ソフトウェアの真正性を確実にするための要求事項及びメッセージの完全性を保護するための要求事項を特定し，また，適切な管理策を特定し，実装することが望ましい。	—	—	—	—	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、“開発におけるセキュリティとサポート プロセス” が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	—
12.2.4	12 情報システムの取得，開発及び保守	12.2 業務用ソフトウェアでの正確な処理	12.2.4 出力データの妥当性確認	業務用ソフトウェアからの出力データは，保存する情報の処理が正しく，かつ，状況に対して適切であることを確実にするために，妥当性確認をすることが望ましい。	—	—	—	—	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、“開発におけるセキュリティとサポート プロセス” が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 － アウトソース開発」 「RM-01：リリース管理 － 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、Office365を利用して作成した出力情報の作成、誤受、保管、管理および廃棄について、不正防止対策および機密保護対策を講じる必要がある。
12.3.1	12 情報システムの取得，開発及び保守	12.3 暗号による管理策	12.3.1 暗号による管理策の利用方針	情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施することが望ましい。	クラウド利用者は，クラウドサービス上で利用する情報の暗号化機能が提供されていることを確認することが望ましい。クラウド利用者は，クラウドサービスにおいて提供されている情報の暗号化機能が，暗号による管理策の利用に関する方針に照らして適切であるか確認することが望ましい。 クラウド利用者は，クラウドサービスを利用するネットワーク経路が暗号化されていることを確認することが望ましい。 クラウド利用者は，クラウドサービスで利用する情報がシステム上で暗号化されていることを確認することが望ましい。	クラウド事業者は，暗号化に対応しているサービスを明確にし，クラウド利用者に明示することが望ましい。クラウド事業者は，暗号化されないサービスについて代替機能があれば明確にし，開示することが望ましい。	クラウドサービスの暗号化では特殊なデータ管理を行っている場合が多く，組織の手順書に定めた暗号化技術が適用できない場合がある。そのため，クラウド利用者は，資産分類に従った機密性確保のための暗号化が実施できるかどうかを確認し，サービスの選択，付加機能の選択を行うことが期待される。	—	業界標準のトランスポート層セキュリティ（TLS）/SSL（Secure Sockets Layer）を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 暗号化は、トランスポート層、クライアントと Exchange Online 間の暗号化（SSL）、インスタント メッセージングと IM フェデレーションなど、さまざまなレイヤーで提供されます。詳細については、ダウンロード センターから入手可能な Office 365 のセキュリティ サービスの説明を参照してください。また、マイクロソフトでは S/MIME、Active Directory Rights Management サービス、PGP をサポートしています。 Office 365 では静止状態のデータを暗号化することはありません。ただしお客様は、IRM または RMS を通じて暗号化を行うことができます。 ISO 27001 規格（具体的には付属文書 A の項 10.8）で、“情報の交換” が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	■盗聴・伝送データの暗号化 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。 文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 文献[01]では、通信時のデータがSSL等で暗号化されることが明示されている。また、保存時（静止状態）には標準では暗号化されないが、利用者の必要に応じて、Information Rights Management (IRM) 機能やRights Management Services (RMS)機能を用いて暗号化できることが明示されている。 ■暗号鍵の管理主体 NDAに基づく文書を確認した結果、標準に従って暗号鍵が管理されていることが確認できた。	要NDA	文献[01]SA-11セキュリティアーキテクチャ・共有ネットワーク 文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利用した保存データの高度な暗号化」 文献[01]「IS-18：情報セキュリティ－暗号化」	—	—	（マイクロソフト社とのNDAにより開示）	利用者は、暗号鍵の活用方法を利用開始前に検討する必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
12.3.2	12 情報システムの取得，開発及び保守	12.3 暗号による管理策	12.3.2 かぎ（鍵）管理	組織における暗号技術の利用を支持するために，かぎ管理を実施することが望ましい。	クラウド利用者は，クラウドサービスで管理すべき暗号かぎを識別し，かぎ管理手順を定めることが望ましい。 クラウド利用者は，クラウドサービスにおけるかぎ管理手順について，必要に応じて次のような情報を求めることが望ましい。 a) かぎの種類 b) かぎのライフサイクル（生成，変更，更新，保管，失効，回収，維持，破壊）の各プロセスにおける手順を含むかぎ管理システムの仕様 c) クラウド利用者側での実施が推奨される事項	クラウド事業者は，提供するクラウドサービスにおけるかぎ管理をクラウド利用者が実施できるよう，かぎ管理に関する情報提供の方針を定め，クラウド利用者に明示することが望ましい。	クラウドサービス（特にSaaS）においては独自の認証を行っている場合があり，既に運用している認証とかぎ管理の仕組みとの連携がとれない場合がある。クラウド利用者は，システムの要求事項に適応したかぎ管理ができるかどうかを確認し，必要に応じて要求を満たす認証方式と連携して管理することが期待される。	—		適合可能	文献[01]では、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 Online Services サービスの重要なコンポーネントのためのポリシー、手順、メカニズムがあることが明示されている。 また文献[41]では、鍵管理として、ユーザー独自のキー ライブラリをMicrosoft Online Services Storage サービスに格納する方法が例示されている。	公開文書	文献[01]「IS-19：情報セキュリティ－暗号化キーの管理」 文献[41]「キー記憶域と保存」	—	—	—	利用者は、暗号鍵の活用方法を利用開始前に検討する必要がある。
12.4.1	12 情報システムの取得，開発及び保守	12.4 システムファイルのセキュリティ	12.4.1 運用ソフトウェアの管理	運用システムにかかわるソフトウェアの導入を管理する手順を備えることが望ましい。	—	—	PaaS では実行環境のみが提供され，試験運用のプログラムと本番運用のプログラムを区別することが難しい場合がある。そのように，試験運用と本番運用のプログラムを実行環境上で区別することができない場合には，実行時に試験運用のプログラムを削除するか，試験運用と本番運用で別のアカウントを取得し，個別に管理することが期待される。	—	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。 マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、Microsoft Online Services サービスの提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Servicesサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、Microsoft Online Services の運用変更の管理手順に「承認されている非運用環境における変更のテスト」が含まれていること、お客様の非公開データの運用環境から非運用環境への移動またはコピーは、お客様の同意が得られた場合やマイクロソフトの法務部門の指示による場合を除き禁止されていることが明示されている。 NDA文書を確認したところ、お客様データへのアクセスについて厳重に管理されていることが確認できた。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 「DG-01：データ ガバナンス - 所有権/管理者責任」 文献[01]「RM-01：リリース管理 - 新規開発/取得」 「DG-06：データ ガバナンス - 非運用データ」	（マイクロソフト社とのNDAにより開示）	—	—	—
12.4.2	12 情報システムの取得，開発及び保守	12.4 システムファイルのセキュリティ	12.4.2 システム試験データの保護	試験データは，注意深く選択し，保護し，管理することが望ましい。	—	—	—	—	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。 マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、Microsoft Online Services サービスの提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Servicesサービス の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。 文献[01]では、Microsoft Online Services の運用変更の管理手順に「承認されている非運用環境における変更のテスト」が含まれていること、お客様の非公開データの運用環境から非運用環境への移動またはコピーは、お客様の同意が得られた場合やマイクロソフトの法務部門の指示による場合を除き禁止されていることが明示されている。 NDA文書を確認したところ、お客様データへのアクセスについて厳重に管理されていることが確認できた。	要NDA	文献[01]「FS-08：施設のセキュリティ - 資産管理」 「DG-01：データ ガバナンス - 所有権/管理者責任」 文献[01]「RM-01：リリース管理 - 新規開発/取得」 「DG-06：データ ガバナンス - 非運用データ」	（マイクロソフト社とのNDAにより開示）	—	（マイクロソフト社とのNDAにより開示）	—
12.4.3	12 情報システムの取得，開発及び保守	12.4 システムファイルのセキュリティ	12.4.3 プログラムソースコードへのアクセス制御	プログラムソースコードへのアクセスは，制限することが望ましい。	—	—	PaaS ではスクリプト言語を利用しているものが多く，ソースをそのまま実行環境に置かざるをえないことが多い。クラウド利用者は，プログラムソースコードの保護の観点で，どのようにコードを管理するかを明確にし，新たな手順を作成することが期待される。	—	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。 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。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及び/アプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身が各種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。	公開文書	文献[01]「IS-07：情報セキュリティ－ユーザーアクセスポリシー」 文献[01]「IS-08：情報セキュリティ－ユーザーアクセスの制限/承認」 文献[01]「IS-10：情報セキュリティ－ユーザーアクセスの確認」 文献[01]「IS-33：情報セキュリティ－ソースコードへのアクセスの制限」 文献[01]「SA-03：セキュリティアーキテクチャー－データのセキュリティ/整合性」 文献[07]「FAQ37」	（マイクロソフト社とのNDAにより開示）	—	—	—
12.5.1	12 情報システムの取得，開発及び保守	12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.1 変更管理手順	変更の実施は，正式な変更管理手順の使用によって，管理することが望ましい。	クラウド利用者は，変更管理手順にクラウドサービスに関する内容を追加することが望ましい。	クラウド事業者は，クラウドサービスの変更に関して，必要に応じて次の事項を実施することが望ましい。 a) システム変更の実施に関するクラウド利用者への通知 b) システム機能の追加・変更に関するクラウド利用者への通知 c) ソフトウェアの更新についての版数の管理 d) システム変更についての監査証跡・変更履歴の管理及び利用者への提示	クラウドサービスの利用においてはスケーラビリティの確保が十分になされているとはいえ，マルチテナントであることを考慮すれば，ある一定時期に十分なサービスが得られない場合があることに留意すること，また，IaaS やPaaS の契約形態においては自動的に帯域を確保する機能を有していないものもある。 スケーラビリティ以外の変更管理においても同様に、自動化されたシステムに依存せずに、クラウド利用者自らが管理できる手順を明確にすることが期待される。	—		Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められています。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者 (Microsoft Online Services とサード パーティ) に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合） お客様には、大規模な変更については 12 か月前までに通知が行われ、計画済みのメンテナンスについては少なくとも 5 日前までに通知が行われます。ただし、このサービスはマルチテナントであるため、いつアップグレードを行うかに関して個々のお客様がそれを定義できるようにする条項はありません。 ISO 27001 規格（具体的には付属文書 A の項 10.1.2）で、"変更管理" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。		文献[01]では、Office 365に大規模な変更がある場合には、12ヶ月前に利用者に通知されることが明示されている。	公開文書	文献[01]「RM-01：リリース管理 - 新規開発/取得」				—
12.5.2	12 情報システムの取得，開発及び保守	12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー	オペレーティングシステムを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要な業務用ソフトウェアをレビューし，試験することが望ましい。	クラウド利用者は，オペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況を確認することが望ましい。クラウド利用者は，業務用ソフトウェアのレビュー手順にオペレーティングシステムやウェブブラウザのクラウドサービスへの対応状況の確認を追加することが望ましい。 クラウド利用者は，利用しているクラウドサービスが対応するオペレーティングシステムやウェブブラウザやクライアント（端末含む）の対応状況を確認することが望ましい。 クラウド利用者は，クラウドサービスのオペレーティングシステムに変更があった場合，クラウド利用者が管理するアプリーションの技術的レビューを実施することが望ましい。 クラウド利用者が管理するアプリケーションに重大な影響を及ぼす可能性があるクラウドサービスのオペレーティングシステム変更については，クラウド事業者により情報が提供されることを確実にし，アプリケーションの技術的レビューを実施することが望ましい。	クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンを明示することが望ましい。クラウド事業者は，クラウドサービスを利用することができるオペレーティングシステムやウェブブラウザの種類とバージョンに変更が生じる場合は，あらかじめクラウド利用者に通知することが望ましい。	クラウドサービスのクラウド利用者側のインタフェースはウェブブラウザを利用することが多い，クラウドサービスではリッチインタフェースの実現のために様々な技術を提供している場合があるが，ブラウザの種類やバージョンによってはそれらの機能を活用できない場合がある。オペレーティングシステムのバージョンアップとともにクライアントのウェブブラウザがアップデートされることも考慮して，オペレーティングシステムアップデートの際には動作テストを行うことが期待される。	—		Office 365 は、最新のブラウザーと最新バージョンの Office で動作します。古いバージョンのブラウザーやメインストリーム サポートの対象でない Office バージョンを使用している場合は、以下の点に注意してください。 ユーザーがサービスに接続するのを Microsoft が意図的に阻止することはありませんが、Office 365 のパフォーマンスは徐々に低下します。 Microsoft は、セキュリティ以外の問題を解決する修正プログラムを提供しません。 Office 365 は、製造元にサポートされていないソフトウェアとは連携しません。	適合可能	文献[96]では、サポートするブラウザのバージョンを含めて、Office365製品のシステム動作要件が明示されている。	公開文書	文献[96]	—	—	—	利用者は、Office365の利用環境への影響についてレビューし、試験する必要がある。

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							SI事業者・利用者で必要な対応
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
12.5.3	12 情報システムの取得、開発及び保守	12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.3 パッケージソフトウェアの変更に対する制限	パッケージソフトウェアの変更は，抑止し，必要な変更だけに限ることが望ましい。また，すべての変更は，厳重に管理することが望ましい。	－	－	－	変更の管理手順が定められています。この手順には、Microsoft Online Services の管理レビューおよび承認のプロセスが含まれています。この変更管理手順は、Microsoft Online Services の施設においてシステム保守を実行するすべての関係者（Microsoft Online Services とサード パーティ）に対して通知されます。運用変更の管理手順は、以下のアクションについて考慮されています。 · 計画された変更の特定と文書化 · 変更によって生じる可能性のある影響の評価プロセス · 承認されている非運用環境における変更のテスト · 変更の通知計画 · 変更管理の承認プロセス · 変更の中止と復元計画（該当する場合）	適合可能	文献[17]では、運用のためにシステムにアクセスするエンジニアの役割に基づいたアクセス制御を行い，必要最小限の権限を与えるとともに，必要なセキュリティトレーニングに至るまで自動的に保証されるプロセスが確立していることを示している。また、異常検出時に人手を介さずに自動修正プログラムを展開する機能を備えていることを示している。	公開情報	文献[17]の「自動運用」および「遠反の防止、検出、および軽減」	－	－	－	－
12.5.4	12 情報システムの取得、開発及び保守	12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.4 情報の漏えい	情報の漏えいの可能性を抑止することが望ましい。	クラウド利用者は，情報漏えいが起きないように，クラウドサービスの利用手順を策定することが望ましい。クラウド利用者は，情報漏えいの可能性を考慮して，クラウドサービスの利用者にリスクと対策を周知することが望ましい。	クラウド事業者は，クラウドサービスにおける情報漏えいに関する対策を行い，円滑なシステムの運用に支障のない範囲でクラウド利用者にその対策内容を開示することが望ましい。	クラウドサービスではデータを一つのサーバ上に保存するのではなく，複数のサーバ上に分散して配置され，更に冗長性を高めるために，分割されたデータが複製されて複数のサーバ上に配置されることも多い。そのため，データの移動や削除などに伴ってすべてのデータが完全に消去をされず，残存オブジェクトとしてデータの一部が残ってしまう可能性がある。そのため，資産分類において完全消去を前提としているデータについては取扱いに慎重を要する。	－	組織間の資産の交換に関するリスクを最小限に抑えるために、内部または外部の組織との交換は、事前に定められた方法で行われており、スタッフまたは契約業者のスタッフによる Microsoft Online Services の運用環境へのアクセスは、厳しく管理されています。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"情報交換のポリシーと手順、および情報の漏えい" が規定されています。 Microsoft Online Services には、情報セキュリティ ポリシー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。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは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。 データ保存時の暗号化に関しては、利用者のアプリケーション側で対応する必要があります。弊社からは開発者向けに暗号化ライブラリを提供しており、こちらを利用することが可能です。また、暗号化キーの管理についてもMicrosoft Online Servicesの標準機能にては提供おりませんので、利用者にてご用意頂く必要がございます。 128 ビット以上の暗号化キーを使用する TLS により、Microsoft Online Services 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。	適合可能	文献[01]では、業務の正当性に基づいて Microsoft Online Services の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、ソースコードライブラリへのアクセスが権限を与えられた担当者に制限されていること、スタッフまたは契約業者のスタッフによるMicrosoft Online Servicesの運用環境へのアクセスが厳しく制御されていることが明示されている。 さらに文献[07]では、利用者の使用している仮想環境ごとに、利用者自身がを種ログやパフォーマンスカウンター値、クラッシュダンプ値などを取得できることが明示されている。 文献[07]では、データ保存時の暗号化に、暗号化ライブラリが提供されていることが明示されている。 文献[01]では、通信時のデータを暗号化するオプションが提供されることが明示されている。 文献[06]では、重要な内部の通信がSSLによって暗号化されることが明示されている。	公開文書	文献[01]「IS-07: 情報セキュリティ - ユーザーアクセス ポリシー」 文献[01]「IS-08: 情報セキュリティ - ユーザーアクセスの制限/承認」 文献[01]「IS-10: 情報セキュリティ - ユーザーアクセスの確認」 文献[01]「IS-33: 情報セキュリティ - ソースコードへのアクセスの制限」 文献[01]「SA-03 セキュリティアーキテクチャー - データのセキュリティ/整合性」 文献[07] 文献[01]「IS-18: 情報セキュリティ - 暗号化」 文献[06]	（マイクロソフト社とのNDAにより開示）	－	－	利用者は、Office365の利用環境において、情報漏えい対策を実施する必要がある。
12.5.5	12 情報システムの取得、開発及び保守	12.5 開発及びサポートプロセスにおけるセキュリティ	12.5.5 外部委託によるソフトウェア開発	組織は，外部委託したソフトウェア開発を監督し，監視することが望ましい。	－	－	－	Microsoft は、一部のサービス（カスタマー サポートなど）の提供を他社に委託することがあります。下請業者がサービスの提供を継続できるようにするためにのみ、下請業者に顧客データを開示します。下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されます。Microsoft によって管理されている施設や機器で業務を行う下請業者は当社のプライバシー基準に従う必要があります。その他のすべての下請業者は、Microsoft と同等のプライバシー基準に従う必要があります。Microsoft Online Services の顧客データを処理する権限を持つ下請事業者の一覧をダウンロードできます。	適合可能	文献[01]によると、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること、また、Microsoft によって管理されている施設や機器で業務を行う下請業者はMicrosoft のプライバシー基準に従うよう契約によって義務付けられていること、その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていることが明示されている。	公開文書	文献[01]「CO-03: コンプライアンス - サード パーティの監査」 文献[02]「Microsoft のプライバシー要件」	（マイクロソフト社とのNDAにより開示）	－	－	－
12.6.1	12 情報システムの取得、開発及び保守	12.6 技術的ぜい弱性管理	12.6.1 技術的ぜい弱性の管理	利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得することが望ましい。また，そのようなぜい弱性に組織がさらされている状況を評価し，それと関連するリスクに対処するために，適切な手段をとることが望ましい。	クラウド利用者は，技術的ぜい弱性についての情報収集について手順化し，利用しているクラウドサービスとの関連の有無を確認することが望ましい。クラウド利用者は，クラウド事業者から技術的ぜい弱性について情報を収集することが望ましい。クラウド利用者は，クラウド事業者以外の信頼できる情報源からぜい弱性について情報を収集することが望ましい。 クラウド利用者は，クラウドサービスにおける技術的ぜい弱性の管理について理解することが望ましい。 クラウドサービスにおける技術的ぜい弱性の管理がクラウド利用者のセキュリティ要求事項に適合しない場合，クラウド利用者による対策の実施を検討することが望ましい。	クラウド事業者は，提供するクラウドサービスに関連するリスクについて情報収集を行うことが望ましい。クラウド事業者は，必要に応じてぜい弱性や脅威に関する情報をクラウド利用者に通知することが望ましい。	クラウドサービスではクラウド事業者が独自技術を利用している事が多く，仕様が公開されていないためにクラウド利用者自らがぜい弱性に対応することが難しい。また，クラウド利用者同士の情報交換が難しいために、セキュリティ関連の情報についてクラウド事業者依存となる可能性が高い。クラウド利用者が，独自技術を利用してクラウドサービスを展開しているクラウド事業者と契約する際には，ぜい弱性に関する情報提供が行われるように要求することが期待される。また，クラウドサービスでは，クラウド事業者が用意したソフトウェアであっても，クラウド利用者にその管理権限と責任があり，クラウド事業者がそのソフトウェアの技術的ぜい弱性を管理しない場合がある。したがって，クラウド利用者は技術的ぜい弱性の管理責任にかかわるサービス内容及び契約内容を確認することが期待される。なお，技術的ぜい弱性の管理は，変更管理の従属機能とみなすことができるため，変更管理のプロセス10.1.2）及び手順（12.5.1）が利用できる。	－	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	公開文書	文献[06]	－	－	－	－
13.1.1	13 情報セキュリティインシデントの管理	13.1 情報セキュリティの事象及び弱点の報告	13.1.1 情報セキュリティ事象の報告	情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけすみやかに報告することが望ましい。	クラウド利用者は，クラウドサービスの利用者が利用中に気づいた事象について報告し，集約できる体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデントを定義することが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウドサービスの利用者が理解し，発生時に報告できるようにすることが望ましい。クラウド利用者は，情報セキュリティインシデントをクラウド事業者に報告できる手順を策定することが望ましい。	クラウド事業者は，情報セキュリティインシデントを受け付ける窓口を設置することが望ましい。クラウド事業者は，クラウドサービス自体のトラブル発生時でも情報セキュリティインシデントに対応できる窓口を運用することが望ましい。	－	組織事業の基礎を成す情報及びその情報を取り扱うプロセス、システム並びにネットワークの多くを、組織内に保持する場合と比べて、クラウドサービス利用においてはサーバの監視やログの取得が自由にできないことが多い。リアルタイム監視や膨大なログの解析といったことを前提としたインシデントレスポンスを行うことができない場合は、事前に取得できる情報を明確にし、それを前提に判断できる内容を情報セキュリティインシデントとして定義しなおすことが期待される。	－	Microsoft は、下請業者に対して、Microsoft のベンダー プライバシー アシュアランス プログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求します。また、Microsoft によって管理されている施設や機器で業務を行う下請業者は、当社のプライバシー基準に従うよう、契約によって義務付けられています。その他のすべての下請業者は、当社と同等のプライバシー基準に従うよう、契約によって義務付けられています。	適合可能	文献[07]では、利用者のインシデントをマイクロソフトのサポート担当が仮想マシンのログを取得し原因究明や解析を行うことが明示されている。 NDA文書を確認したところ、お客様が日本国内でクラウドサービス契約を締結し、日本国内でプレミアサポート契約を締結することで、24時間日本語対応が提供されることを確認した。	要NDA	文献[07]No.37-38	－	－	（マイクロソフト社とのNDAにより開示）	－
13.1.2	13 情報セキュリティインシデントの管理	13.1 情報セキュリティの事象及び弱点の報告	13.1.2 セキュリティ弱点の報告	すべての従業員，契約相手並びに第三者の情報システム及びサービスの利用者に，システム又はサービスの中で発見した又は疑いをもったセキュリティ弱点は，どのようなものでも記録し，また，報告するように要求することが望ましい。	クラウド利用者は，クラウドサービスのセキュリティ上の弱点に気づいた場合に記録し，報告する手順を策定することが望ましい。クラウド利用者は，当該サービスにおいてセキュリティ上の問題を発見した場合に，クラウド事業者に報告する手順を策定することが望ましい。	－	－	－	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]によると、ターミナルサービスサーバーが高度な暗号化設定を使用できること、Microsoft Online Services ではネットワークレベルのコンポーネントへのアクセスには 2 要素認証（RSA、SecurID）が必要であり、(Microsoft Online Services に接続するために) マイクロソフト企業ネットワークにリモートで接続するユーザーは2 要素認証によってセットアップされる直接アクセスを使用すること、Microsoft Online Services データ センター内のネットワークは複数の個別のネットワークセグメントを持つように設計されており、重要なバックエンドサーバーやストレージデバイスを公開用インターフェイスから分離できること、Microsoft Online Services はMSRCとGFSから通知された脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを主導すること、Microsoft Online Services ではセキュリティインシデント、脆弱性、および異常動作について報告し処理する手順があること、お客様のデータのセキュリティが侵害されまたは不正アクセスを受けたと Microsoft Online Services の担当者が判断した場合、お客様に通知することが明示されている。 文献[06]では、マイクロソフトの施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価および対応することが明示されている。 文献[07]では、利用者のインシデントについてマイクロソフト側で原因分析を行うことが明示されている。	公開文書	文献[01]「SA-07 セキュリティアーキテクチャー - リモート ユーザーの多要素認証」 「SA-09: セキュリティアーキテクチャー - 分離」 「IS-20: 情報セキュリティ - 脆弱性/更新プログラム管理」 「IS-23: 情報セキュリティ - インシデントの報告」 文献[06]「4.2 セキュリティ報告」 文献[07]「No.26 インシデントレスポンス」	－	－	－	－

経済産業省ガイドラインの評価項目							J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応						
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項			ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
13.2.1	13 情報セキュリティインシデントの管理	13.2 情報セキュリティインシデントの管理及びその改善	13.2.1 責任及び手順	情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするために，責任体制及び手順を確立することが望ましい。	クラウド利用者は，情報セキュリティインシデントに対する迅速な対応ができるように体制を構築することが望ましい。クラウド利用者は，クラウドサービスにおける情報セキュリティインシデント発生時の対応責任者を決めることが望ましい。クラウド利用者は，情報セキュリティインシデント対応の手順にクラウドサービスに関連する内容を追加することが望ましい。	クラウド事業者は，クラウドサービスにおける意⽋な情報セキュリティインシデントを定義することが望ましい。また，インシデント対応についての情報提供の⽅針を定め，クラウド利用者に提示することが望ましい。 クラウド事業者は，他の事業者との合意に基づき，サプライチェーン上で重⼤な情報セキュリティインシデントが⽣じたときに共有すべき情報を⽂書化することが望ましい。	クラウドサービスではサーバのリアルタイム監視や，ログの柔軟な管理が困難なため，情報セキュリティインシデントにクラウドサービスの利用者が最初に気づく可能性がある。このため，情報セキュリティインシデントのエスカレーション⼿順を⾒直し，クラウドサービスの利用者からの情報提供が⾏われやすい環境を考慮する必要がある。	—	マイクロソフト データセンターあるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連するお客様に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。そのためお客様がデータセンターに立ち⼊ったとしても、お客様コンテンツにアクセスすることはできないため、経営不安等の理由によるお客様コンテンツ保全のためのデータセンター⽴⼊を受け⼊れる⽤意はありません。	適合可能	文献[01]では、インシデント発生時の体制について、インシデントマネージャーやインシデントエンジニアについて、インシデントの処理方法や管理の役割、責任について、および法務、経営管理者へのエスカレーションとコミュニケーション計画について明示されている。 また、文献[04]では侵入テスト、文献[08]では多層防御アプローチについて明示されている。	公開文書	文献[01]「IS-22. 情報セキュリティインシデント管理」 文献[04] 文献[08]	—	—	—	利用者は、インシデント発生時のトレーサビリティをマイクロソフトが提供するログのみで確保できないと判断した場合は、ユーザ⾃⾝でログを取得し、トレーサビリティを確保できるようにしておくことが望ましい。
13.2.2	13 情報セキュリティインシデントの管理	13.2 情報セキュリティインシデントの管理及びその改善	13.2.2 情報セキュリティインシデントからの学習	情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えることが望ましい。	クラウド利用者は，クラウドサービスの情報セキュリティインシデントについて記録し定量化することが望ましい。クラウド利用者は，クラウドサービスに関するセキュリティインシデントを記録し，定量化することが望ましい。クラウド利用者は，事故の発生や影響を軽減するために定量化した情報をクラウド事業者と共有することが望ましい。	クラウド利用者が情報セキュリティインシデントを評価できるよう，クラウド事業者は，クラウド利用者との合意に基づき次の情報を提供することが望ましい。 a) 情報セキュリティインシデントの統計情報 b) 情報セキュリティインシデントによる影響 c) 情報セキュリティインシデントへの対応 d) 情報セキュリティインシデントへの予防策	クラウドサービスではサーバの監視やログ管理が困難なために，クラウド利用者は、サーバ上の情報セキュリティインシデントに関する情報を⾃ら取得することが難しい。そのため、クラウド利用者は、クラウド事業者の情報を基に情報セキュリティインシデントの定量化を⾏い、情報セキュリティインシデントの予測などを⾏うことができる体制づくりを考慮する必要がある。	—	マイクロソフト データセンターあるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連するお客様に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。そのためお客様がデータセンターに立ち⼊ったとしても、お客様コンテンツにアクセスすることはできないため、経営不安等の理由によるお客様コンテンツ保全のためのデータセンター⽴⼊を受け⼊れる⽤意はありません。	適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03. 復元 – ビジネス継続性の計画」「RS-04. 復元 – ビジネス継続性のテスト」 文献[65]	—	—	—	利用者は、インシデント発生時のトレーサビリティをマイクロソフトが提供するログのみで確保できないと判断した場合は、ユーザ⾃⾝でログを取得し、トレーサビリティを確保できるようにしておくことが望ましい。
13.2.3	13 情報セキュリティインシデントの管理	13.2 情報セキュリティインシデントの管理及びその改善	13.2.3 証拠の収集	情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定められている証拠に関する規則に従うために，証拠を収集，保全及び提出することが望ましい。	クラウド利用者は，情報セキュリティ事故が法的処置に及ぶ場合を想定して，必要な証拠の収集，保全を実施することが望ましい。また，クラウド事業者がそれらの情報を保管しているか確認することが望ましい。 クラウド事業者がクラウド利用者の法的証拠となり得る情報を管理する場合，クラウド利用者は，次の手順を実施することが望ましい。 1. クラウド利用者にとって法的証拠となり得る情報を明確にする 2. クラウド事業者によって管理されている情報が記録され，適切に保管されているかを確認する 3. クラウド事業者によって管理されている情報を収集・保持する 4. 収集した情報の中で，クラウド利用者にとって証拠として活用できる情報を識別し，保全する クラウド利用者は，クラウド事業者がクラウド利用者にとって法的証拠となり得る情報を管理する場合，クラウド事業者に情報を求めることが望ましい。 クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を取得することが望ましい。クラウド利用者は，クラウドサービスに関して法的な要求に基づいてログなどの証拠を必要期間保存することが望ましい。	クラウド事業者は，法的な証拠となる可能性がある情報については記録し，適切に保管しておくことが望ましい。クラウド事業者は，どのような記録がどの程度の期間保管されているかをクラウド利用者に明示することが望ましい。	クラウドサービスの利用においてはコスト削減のために保存データの容量を必要最低限にすることがある。そのため，外部の継続的証拠保全のためのサービス（e-discovery サービスやリモートジャーナリングサービスなど）を別途契約するなどの方法もある。	—	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。 外部からの不正アクセス等の対応として、ファイアウォール、パケットフィルタリングにより、偽装トラフィックや不適切なブロードキャスティングなどはできないようになっています。 外部からの不正アクセス対策として、複数の⼿段による多層的な予防措置を⾏っているほか、検出、抑制、回復⼿段を合わせて使⽤しています。 また、クラウドサービスチームに専⾨のCSIRTを置き、全社CSIRTと連携してインシデント対応を⾏うこととしています。	適合可能	文献[01]では、インシデントの対応に関する法的な準備において、マイクロソフトのセキュリティ インシデント対応プロセス中の抑制⼿順の⼀環として、エスカレーション チームの最も高い優先度の対処事項は、インシデントを抑制してデータの安全性を確保することであること、エスカレーション チームは、対応の形式を作り、適切なテストを実⾏し、変更を実装することを確認した。	公開文書	文献[01]	—	—	—	利用者は、インシデント発生時のトレーサビリティをマイクロソフトが提供するログのみで確保できないと判断した場合は、ユーザ⾃⾝でログを取得し、トレーサビリティを確保できるようにしておくことが望ましい。
14.1.1	14 事業継続管理	14.1 事業継続管理における情報セキュリティの側面	14.1.1 事業継続管理手続への情報セキュリティの組込み	組織全体を通じた事業継続のために，組織の事業継続に必要な情報セキュリティの要求事項を取り扱う，管理された手続を，策定し，維持することが望ましい。	—	—	—	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 主要なリソースの責任の割り当て · 通知、エスカレーション、宣言のプロセス · 回復時間に関する目標、および回復ポイントに関する目標 · 文書化された手順による継続性の計画 · 該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム · テスト、メンテナンス、および改訂のプロセス ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[08]では、ビジネス継続性管理計画の開発ライフサイクルを使用して、6 つのフェーズすべてにおいて、障害復旧計画を作成し、保守することが明示されている。 文献[19]では、Microsoft Operations Center(MOC)にて、防犯管理も含めて全体の管理を実施していることが明示されている。 NDA文書を確認したところ、情報セキュリティに関する管理者が割り当てられ役割と責任が明確化されていることが確認できた。	要NDA	文献[08]「ビジネス継続性の管理」 文献[19]「Incident Management Model」	（マイクロソフト社とのNDAにより開示）	—	（マイクロソフト社とのNDAにより開示）	利用者は、Office365の利用を前提に、事業継続計画を策定する必要がある。
14.1.2	14 事業継続管理	14.1 事業継続管理における情報セキュリティの側面	14.1.2 事業継続及びリスクアセスメント	業務プロセスの中断を引き起こし得る事象は，そのような中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。	クラウド利用者は，クラウドサービス利用が事業継続にどのような影響を及ぼすかを判断し，要求事項としてまとめることが望ましい。クラウド利用者は，クラウドサービスが関与する業務を特定することが望ましい。クラウド利用者は，クラウドサービスが関与する資産を特定し，クラウドサービス利用に関連する情報セキュリティインシデントが業務に及ぼす影響を特定し，クラウドサービスの利用に係る事業継続についてリスク識別し，評価することが望ましい。 クラウド利用者は，リスクアセスメントにおいてはクラウド事業者と調整し，技術的・運営的な背景なども検討することが望ましい。	クラウド事業者は，クラウドサービスのサービスレベルについて中断の発生確率及び影響，並びに中断が情報セキュリティに及ぼす結果とともに，特定することが望ましい。	クラウドサービスにおけるサービスレベルはSaaS，PaaS，IaaS がそれぞれ依存関係にある場合もあり，特にSaaS では高稼働率を実現することが難しい場合がある。そのため，業務において本来必要な稼働率を検討し（例えば，システムの最大許容停止時間及び⽬標復旧時間の設定），SLA などによって確認することが期待される。	—	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 主要なリソースの責任の割り当て · 通知、エスカレーション、宣言のプロセス · 回復時間に関する目標、および回復ポイントに関する目標 · 文書化された手順による継続性の計画 · 該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム · テスト、メンテナンス、および改訂のプロセス ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、Microsoft Online Services の継続性プログラムを主導するフレームワークに「文書化された手順による継続性の計画」があること、復元計画は定期的に検証されることが明示されている。 また、インタビュー等を通じて、委託先が契約通りに委託業務を遂行できないリスクはないことを確認した。	要NDA	文献[01]「RS-03. 復元 – ビジネス継続性の計画」「RS-04. 復元 – ビジネス継続性のテスト」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、Office365の利用を前提に、事業継続計画を策定する必要がある。

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応							
評価項目項番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	SI事業者・利用者で必要な対応
14.1.3	14 事業継続管理	14.1 事業継続管理における情報セキュリティの側面	14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施	重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施することが望ましい。	クラウド利用者は、リスクアセスメントの結果に応じて、クラウドサービスにおける冗長化の状況を確認することが望ましい。	クラウド事業者は、クラウドサービスを提供するシステムの冗長化を図ることが望ましい。 クラウド事業者は、クラウドサービスの冗長化の状況を、クラウドサービスの利用を検討する者に明示することが望ましい。	事業継続管理における クラウドサービスの関係は情報システムの稼働率だけではなく、クラウドサービス上で作成されたデータを他のシステムに持ち出すことができるか、また現在利用しているシステムからデータを容易に持ち込むことができるかなども検討することが期待される。さらに、システムの最大許容停止時間を考慮してこれらの課題に対して検討する必要がある。クラウドサービスを提供するシステムの冗長化を図る観点として、次のようなものがある。 a) データのバックアップ b) データセンター c) サポートユーティリティ（例えば、電源、ケーブル配線施設やそれらのコントローラなど） d) ハードウェア e) クラウドプラットフォーム f) クラウド制御システム	—	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 主要なリソースの責任の割り当て · 通知、エスカレーション、宣言のプロセス · 回復時間に関する目標、および回復ポイントに関する目標 · 文書化された手順による継続性の計画 · 該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム · テスト、メンテナンス、および改訂のプロセス ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。	公開文書	文献[01]の「OP-04：運用管理 - 装置のメンテナンス」	—	—	—	利用者は、Office365の利用を前提に、事業継続計画を策定する必要がある。
14.1.4	14 事業継続管理	14.1 事業継続管理における情報セキュリティの側面	14.1.4 事業継続計画策定の枠組み	すべての計画が整合したものになることを確実にするため、情報セキュリティとの要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持することが望ましい。	—	—	—	—	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 · 主要なリソースの責任の割り当て · 通知、エスカレーション、宣言のプロセス · 回復時間に関する目標、および回復ポイントに関する目標 · 文書化された手順による継続性の計画 · 該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム · テスト、メンテナンス、および改訂のプロセス ISO 27001 規格（具体的には付属文書 A の項 14.1）で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Online Services の管理者によって承認されていることが明示されている。 NDA文書を確認したところ、事業継続を目的として、復旧に必要な情報が確保できていることが確認できた。	要NDA	文献[01]「OP-02：運用管理・文書化」	（マイクロソフト社とのNDAにより開示）	—	（マイクロソフト社とのNDAにより開示）	利用者は、Office365の利用を前提に、事業継続計画を策定する必要がある。
14.1.5	14 事業継続管理	14.1 事業継続管理における情報セキュリティの側面	14.1.5 事業継続計画の試験、維持及び再評価	事業継続計画が最新で効果的なものであることを確実にするために、定めに従って試験・更新することが望ましい。	クラウド利用者は、事業継続計画の試験及び更新において、クラウド事業者が関与可能かを確認することが望ましい。	クラウド事業者は、クラウド利用者の事業継続計画の試験・更新に関する協力可否について、クラウド利用者との合意に基づき情報を提供することが望ましい。	クラウド利用者は、サービス可用性について適切な条項を契約に規定し、クラウド利用者の事業継続計画の試験・更新において組み込むことが推奨される。 クラウド事業者は、リソースやインフラなどの高集約によるインシデントの影響の拡大がクラウドの特徴であることを踏まえ、クラウドサービス提供にかかわるクラウド事業者組織における教育訓練の内容を適時に見直し、障害対応要員の定期的及び必要に応じた教育・訓練を実施することが期待される。 クラウド利用者が事業継続に係るリスクアセスメントを実施する際に考慮すべき事項には、次のようなものがある。 a) クラウドサービスの障害などによる停止 b) 法執行機関の要請によるサービスの一時停止 c) クラウドサービスの終了 d) 財務状況の変化に伴うクラウド事業者の変更 クラウド事業者は、クラウド利用者の事業継続計画策定・実施に関連して、クラウド利用者との合意に基づき、次のような情報を提供することが望ましい。 a) クラウド事業者の災害復旧計画 b) システムの多重化など、可用性を確実にするための対策 c) クラウドサービスの目標復旧時間	—	Microsoft Office 365 のサービスは、高水準のサービスを維持できる回復力の高いシステムで提供されています。サービス継続性のための対策は、Office 365 のシステム設計の一部です。これらの対策により、Office 365 は、ハードウェアやアプリケーションの障害、データ破損、ユーザーに影響を与えるその他のインシデントといった予期せぬイベントから迅速に復旧できます。サービス継続性ソリューションは、重大なサービス停止（たとえば、自然災害やインシデントによって、ある Microsoft のデータ センター全体が使用不能になった場合など）の際にも適用されます。 致命的な障害から復旧した後、データ センターの完全な冗長性がサービスに復元されるまで一定の時間がかかります。たとえば、データ センター 1 に障害が発生すると、サービスがデータ センター 2 のリソースによって復元されます。ただし、データ センター 1 の復元されたリソースまたはデータ センター 3 の新規リソースによって、データ センター 2 のサービスの継続性がサポートされるまで時間がかかります。Office 365サービス レベル契約 (SLA) は、この期間に適用されます。 Office 365 の開発および運用チームは、お客様にビジネス継続性を提供するうえで重要な役割を担う専門の Office 365 サポート組織にサポートされています。サポート スタッフはサービスおよびサービスに関連するアプリケーションに精通しており、Microsoft 社内のアーキテクチャ、開発、テストの専門家と直接やり取りします。サポート組織は運用および製品開発チームと密接に協力することで、迅速な問題解決を実現し、お客様の声を反映するための窓口になります。お客様からのフィードバックは、計画、開発、運用プロセスに役立てられます。	適合可能	文献[11]では、Microsoft Office365におけるサービス継続性のための対策が取られており、また利用者との窓口として専門のサポート組織が情報提供を行うことが明示されている。	公開情報	文献[11]	—	—	—	利用者は、Office365の利用を前提に、事業継続計画を策定する必要がある。
15.1.1	15 順守	15.1 法的要求事項の順守	15.1.1 適用法令の識別	各情報システム及び組織について、すべての関連する法令、規則及び契約上の要求事項並びにこれらの要求事項を満たすための組織の取組み方を、明確に定め、文書化し、また、最新に保つことが望ましい。	クラウド利用者は、クラウドコンピューティングサービスに関する法執行機関が、複数の国／地域に関連し得ることを踏み、クラウド事業者に対して情報提供を求めることが望ましい。クラウド利用者は、クラウドコンピューティングサービスに関する管轄裁判所について、クラウド事業者に対して情報提供を求めることが望ましい。 クラウド利用者は、クラウドサービスの利用目的に応じて、クラウド利用者自らが適用を受ける法令、規制及び契約上の要求事項などを洗い出すことが望ましい。クラウド利用者は、クラウドサービスの利用に関する契約に定められた準拠法と裁判管轄を確認し、文書化することが望ましい。クラウド利用者は、クラウド事業者が適用を受ける法令を調査し、文書化することが望ましい。	クラウド事業者は、複数の国／地域の法執行機関がかかわるクラウドサービスを提供している場合、それらの国／地域についてクラウド利用者に知らせることが望ましい。クラウド事業者は、国家連合、国、州、地方自治体により法規制が異なるかを確認し、それぞれの国家連合、国、州、地方自治体の名称をクラウド利用者に明示することが望ましい。クラウド事業者は、関連する法規制について、それぞれの管轄裁判所の場所を明示することが望ましい。 クラウド事業者は、クラウド事業を営む地域（国、州など）、データセンターの所在する地域（国、州など）及びクラウド事業者自らが適用を受ける法令、規制及び契約上の要求事項を明示することが望ましい。 クラウド事業者は、他のクラウド事業者が提供するクラウドサービスを利用している場合、利用しているクラウドサービスの裁判管轄及び適用を受ける法令・規制を確認・文書化し、最新に保つことが望ましい。 クラウド事業者は、クラウド事業者は、クラウド利用者との合意に基づき、法令、規制及び契約上の要求事項が適用される地理的場所にクラウド利用者のデータが保持されていることを確実にするため、法的順守を監視することが望ましい。	SaaS として契約しているクラウド事業者が国内企業であったとしても、そのバックボーンとなるPaaSやIaaS のクラウド事業者が海外の企業である場合もあるため、クラウド事業者が事業を行う国の法律や業界団体の慣習などについても洗い出し、検討することが期待される。 適用法令は、私法と公法を分けて識別することが望ましい。例えば、私人間に適用される法は「当事者が当該法律行為の当時に選択した地の法による」法の適用に関する通則法第7 条）である。つまり、契約時に準拠法を定めるのが一般的であるため、契約当事者間の適用法令が問題になることはかない。一方、国家がかかわる公法の適用は、原則として属地的に定まる。外国法人でも日本国内において事業を行う限り、原則として国内法の適用を受け、逆に日本法人でも外国において事業を行う限り、外国法の適用を受けることがある。例えば、データセンターが外国にあっても我が国で事業を営む企業は、我が国の捜査機関の捜査を受け、外国のサーバ内の情報が差押えられることがあり、逆にデータセンターが国内にあっても外国で事業を営む企業は、その国の捜査機関の捜査を受け、我が国のサーバ内の情報が差押えられることがある。	—	マイクロソフトはデータセンター所在地を開示しています。当該国にデータを保存することによる法令適用や業務の継続性の影響の有無はお客様による判断が必要です。 マイクロソフト データセンターあるいはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連するお客様に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 万一アカウント不正使用などが疑われる場合、そのアカウント使用に関わる情報は、クラウドサービスの標準的な機能を使用してお客様側で調査することが可能です。 マイクロソフトは、お客様がお客様データの所有者でありアクセス権を保持することを契約書に記載しており、このことはマイクロソフトの経営不安が発生した場合でも継続して保障される事項です。 お客様コンテンツはマイクロソフトデータセンター内で厳密なアクセス権管理及び運用権限分割によって保護されており、また、マイクロソフトが使用する運用アカウントはお客様コンテンツへのアクセス権限を有していません。そのためお客様がデータセンターに立ち入ったとしても、お客様コンテンツにアクセスすることはできないため、経営不安等の理由によるお客様コンテンツ保全のためのデータセンター立入を受け入れる用意はありません。	適合可能	NDA文書で確認したところ、日本でMicrosoft Online Servicesの契約をする場合、準拠法は日本法であることが確認できた。 またインタビュー及びNDA文書で確認したところ、データセンターの所在地の開示についてのマイクロソフト社の情報提供方針が確認できた。	要NDA	—	—	—	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織に適用される法令等に照らして、Office365の利用がその要求事項を満たすことを確認する必要がある。
15.1.2	15 順守	15.1 法的要求事項の順守	15.1.2 知的財産権（IPR）	知的財産権が存在する可能性があるものを利用するとき、及び権利関係のあるソフトウェア製品を利用するときは、法令、規則及び契約上の要求事項の順守を確実にするための適切な手順を導入することが望ましい。	クラウド利用者は、クラウド利用の目的に合せ、知的財産権の要求事項を確認することが望ましい。	クラウド事業者は、自らの知的財産権についてクラウド利用者に利用を許諾する範囲及び制約を、クラウド利用者に通知することが望ましい。	—	—	お客様がクラウドサービス上で開発、作成するソフトウェアの知的財産権はお客様が所有するものとし、契約書に記載しています。	適合可能	文献[65]およびNDA文書では、知的財産権や使用権の帰属が規定・明記されていることを確認した。	要NDA	文献[65](OST)	—	—	（マイクロソフト社とのNDAにより開示）	—

経済産業省ガイドラインの評価項目								J-LIS文書の要求事項	ガイドラインに対するMicrosoftの見解	Office 365における対応								SI事業者・利用者で必要な対応
評価項目番	章	節	項	管理策	クラウド利用者のための実施の手引き	クラウド事業者の実施が望まれる事項				ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料		
15.1.3	15 順守	15.1 法的要求事項の順守	15.1.3 組織の記録の保護	重要な記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊及び改ざんから保護することが望ましい。	クラウド利用者は、クラウドサービス上で利用する重要な記録は法令や規制に従って保護することが望ましい。クラウド利用者は、クラウドサービス上で利用する重要な記録は必要に応じて取り出せるように保管することが望ましい。	クラウド事業者は、法令や規制に従って、クラウドサービス上の記録を保護することが望ましい。	クラウドサービスでは、国内外問わず、様々なクラウド事業者を利用する事ができる。しかし、クラウド事業者の中には、特定国内における法律に対応できないクラウド事業者がある可能性もある。そのため、遵守すべき法律を考慮して記録の保管を適切に行うことができるクラウド事業者を選択するか、自ら記録を保管する体制を構築することが期待される。	–	マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されています。 マイクロソフト データセンター あるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連するお客様に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、“アクセス制御” が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[08]では、マイクロソフトのクラウド インフラストラクチャ内の重要サーバーの監査ログは（ほぼ）リアルタイムに収集され、重要な関連性のあるイベント を抽出、OSSC が詳細な分析を実行して疑わしいアクティビティを検索することが明示されている。 文献[06]では、「機密データに対する最終なアクセス制御」、「悪意のある行為の検出」、「複数のレベルにおける、監視、ログ、レポート」のメカニズム等により、サービス運用時に承認されていない開発者や管理者からの操作を保護していることが明示されている。 文献[07]では、最適化への継続的な取り組みの一環としてPDCAサイクルを採用していることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[62]では、ID管理に Azure Active Directory Premiumを契約して使用することで、高度なセキュリティレポートが利用可能であることが明示されている。 文献[01]では、業務の正当性に基づいて Microsoft Azure の資産にアクセスする権限が付与されること、資産に対するアクセス権は知る必要性のある人間に限定する原則、および最小権限の原則に基づいて付与されることが明示されている。 また、管理者及びアプリケーションやデータの所有者は誰がアクセスしているかを定期的に確認する責任を負うこと、適切なアクセスの準備が行われていることを検証するために、定期的にアクセスの確認監査を行うことが明示されている。 文献[65]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。 文献[80]及び文献[81]によると、管理ポータルにて操作ログ（オペレーション ログ）が提供されている。この操作ログを確認することで、特定のサブスクリプションに対して管理者・共同管理者がどのような作業を行ったか確認することが可能であることが明示されている。 また、インタビュー等を通じて、Azure Active Directory Premium では、特権IDの利用履歴を含む監査ログが取得されていることが確認できた。 また、インタビュー等を通じて、ログ保持期間は30日間とされていることが確認できた。	要NDA	文献[08]「ホストのセキュリティ監査およびレポート」 文献[06]の「サービス運用」 文献[07] 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ／侵入検出」 文献[62] 文献[01]「SA-12：セキュリティアーキテクチャー - 時刻の同期」 文献[65](OST) 文献[80] 文献[81]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織に適用される法令等に照らして、Office365の利用がその要求事項を満たすことを確認する必要がある。
15.1.4	15 順守	15.1 法的要求事項の順守	15.1.4 個人データ及び個人情報の保護	個人データ及び個人情報の保護は、関連する法令、規制、及び適用がある場合には、契約条項の中の要求に従って確実にすることが望ましい。	クラウド利用者は、クラウドサービスで個人情報を利用する際には、法令及び組織の個人情報保護方針に従って利用できるように適切な手順を策定することが望ましい。 クラウド利用者は、クラウドサービスの利用目的に応じて、データ保護及び個人情報保護に係る、国内外の法令、規則及び契約上の要求事項を識別することが望ましい。	クラウド事業者は、クラウド利用者がデータの保護及び個人情報保護に関する法規制を識別できるよう、自らのクラウドサービスに影響を及ぼす法的管轄に関する国／地域の情報を提供することが望ましい。	個人情報保護法の要求事項及び当該要求事項の実現のために企業等が定める規程に対応できないクラウド事業者が存在するかもしれない。そのため、個人情報保護に関する基準や手順がクラウド事業者の提供するクラウドサービスに合致するかどうかを検討することが期待される。	–	日本でご契約のお客様は日本法を準拠法とし、東京地方裁判所を管轄裁判所としています	適合可能	インタビュー及びNDA文書で確認したところ、日本でMicrosoft Online Servicesの契約をする場合、準拠法は日本法であることが確認できた。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織に適用される法令等に照らして、Office365の利用がその要求事項を満たすことを確認する必要がある。
15.1.5	15 順守	15.1 法的要求事項の順守	15.1.5 情報処理施設の誤用防止	認可されていない目的のための情報処理施設の利用は、阻止することが望ましい。	–	–	–	–	アクセスは職務によって制限されるため、必要な担当者だけに Microsoft Online Servicesを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証を実施しています。	適合可能	文献[01]では、データセンターの施設へのアクセスを制限することが明示されている。	公開文書	文献[01]「FS-03：施設のセキュリティ－管理されたアクセスポイント」	–	–	–	–
15.1.6	15 順守	15.1 法的要求事項の順守	15.1.6 暗号化機能に対する規制	暗号化機能は、関連するすべての協定、法令及び規制を順守して用いることが望ましい。	クラウド利用者は、暗号技術をクラウドサービス上で利用する際には、輸出規制などに抵触しないか確認することが望ましい。	クラウド事業者は、クラウド利用者が輸出規制などに抵触しないよう、暗号化機能にかかわる法令などの情報をクラウド利用者に提供することが望ましい。	暗号化技術については輸出規制などの問題もあり、海外のクラウド事業者のデータセンターに配置できない場合もある。クラウドサービス上で暗号化機能を利用する場合には、輸出規制などに抵触する可能性について十分に検討する必要がある。	–	業界標準のトランスポート層セキュリティ（TLS)/SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。	適合可能	文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。	公開文書	文献[05]	–	–	–	利用者は、自組織に適用される法令等に照らして、Office365の利用がその要求事項を満たすことを確認する必要がある。
15.2.1	15 順守	15.2 セキュリティ方針及び標準の順守、並びに技術的順守	15.2.1 セキュリティ方針及び標準の順守	管理者は、セキュリティ方針及び標準類への順守を達成するために、自分の責任範囲におけるすべてのセキュリティ手順が正しく実行されることを確実にすることが望ましい。	クラウド利用者は、クラウドサービスに関連する新しい規程や管理策が既存の規程や管理策同様に順守されるようにすることが望ましい。クラウド利用者は、クラウドサービスに関連する標準や手順が、既存の情報セキュリティ基本方針に合致しているかをレビューすることが望ましい。クラウド利用者は、クラウドサービスが情報セキュリティ基本方針に合致しない場合、原因を調査し、必要に応じて双方を是正することが望ましい。	クラウド事業者は、独立したレビュー及び評価（例えば、内部／外部監査、認証、ぜい弱性、ペネトレーションテストなど）を定期的に実施し、情報セキュリティ基本方針及び適用される法的要件を組織が遵守していることを確実にすることが望ましい。また、クラウド事業者は、クラウド利用者の個別の監査要求に応えられるように、クラウド利用者との合意に基づき、独立したレビュー及び評価の結果を提供することが望ましい。	クラウドサービスの利用においては現在運用している管理策やセキュリティ要件に合致する機能を有していない場合が考えられる。特にSaaS においては、個別に機能の付加が容易ではないため、必要に応じてその他のサービスを利用したり、代替する機能を検討したりすることが望ましい。PaaS においても場合によってはこれまでに利用してきたAPI などが利用できないこともある。そのため、実行環境の制限などを十分に精査して、セキュリティを損なわないように標準などを見直すことが期待される。	–	マイクロソフトはお客様に代わり、専門の第三者を選定し外部監査を受け、その結果をお客様に利用可能にすることによって、お客様による監査を代行して実施しています。この第三者監査はISO27001 および SSAE16 またはこれらの後継の規格に準じて行われます。 お客様はマイクロソフトに指示を出すことにより、お客様の監査権を行使しています。お客様はマイクロソフトに与える指示を変更することができます。 上記の2点は契約書に記載の事項となっています。 マイクロソフトが提供する上記の第三者監査レポートに重大な不備がありお客様のクラウドサービス利用の継続に支障が出る場合、あるいはセキュリティ対策の不備によってお客様コンテンツの安全性に重大な懸念が生じるような場合、お客様はマイクロソフト専門担当者を通じてお客様がコンプライアンス、法的要件あるいは規制対応に必要となる情報を請求し監査することができます（追加の契約が必要になる場合があります）。	適合可能	NDA文書を確認したところ、マイクロソフトが提供する第三者監査レポートに重大な不備があり、クラウドサービス利用の継続に支障が出る場合、あるいはセキュリティ対策の不備によってお客様コンテンツの安全性に重大な懸念が生じるような場合、お客様はマイクロソフト専門担当者を通じてお客様がコンプライアンス、法的要件あるいは規制対応に必要となる情報を請求し監査することができる。この監査の実施にはコンプライアンスプログラムへの参加が必要である。	要NDA	–	–	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、Microsoft Office365 及びGFSのISO27001認定については BSIグループのWebサイトを参照することができる。新規の利用者の場合、NDAに基づいて請求することでその他の監査情報を請求することにより入手できる。 利用者は、事前に承認を得ることにより、利用者自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。
15.2.2	15 順守	15.2 セキュリティ方針及び標準の順守、並びに技術的順守	15.2.2 技術的順守点検	情報システムを、セキュリティ実施標準の順守に関して、定めに従って点検することが望ましい。	クラウド利用者は、クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検することが望ましい。クラウドサービスでは様々な機能がクラウド事業者主導で追加されることがあるため、クラウド利用者は、これらの機能が組織の技術的なセキュリティ要求事項に合致しているかを確認し、必要に応じて様々な機能の利用の可否を決定することが望ましい。	クラウド事業者は、クラウドサービスが組織の技術的なセキュリティ要求事項に適合しているかを定期的に点検し、その結果を情報提供の方針に基づいてクラウド利用者に開示することが望ましい。	SaaS では機能の追加がされた場合に、一般利用者権限で機能の利用が可能になる場合がある。クラウド利用者は、セキュリティ要求事項に合致しない機能は管理者権限で停止できるかどうかを確認し、必要に応じて機能の制限ができることを確認することが期待される。	–	災害、犯罪防止、運用における責任と権限、入館等の対応が適切に行われているかの確認をするために、マイクロソフトのオンラインサービスの管理組織であるGlobal Foundation Service（GFS)に属するOnline Services Security and Compliance（OSSC)の情報セキュリティ管理システム（ISMS)によりレビュープロセスが確立されています。使用する統制策（ISO27001/27005、SAS70 TypeIおよび II、SOX,PCI DSS, FISMA等）の有効性を保証する厳格なコンプライアンス テストを実施し、責任の明確化および体制を確立しています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス－監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、Microsoft Office365 及びGFSのISO27001認定については BSIグループのWebサイトを参照することができる。新規の利用者の場合、NDAに基づいて請求することでその他の監査情報を請求することにより入手できる。 利用者は、事前に承認を得ることにより、利用者自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。
15.3.1	15 順守	15.3 情報システムの監査に対する考慮事項	15.3.1 情報システムの監査に対する管理策	運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意されることが望ましい。	クラウド利用者は、クラウドサービスの監査について方針を定めることが望ましい。クラウド利用者は、クラウドサービスを監査する場合において、全体的な業務プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。	クラウド事業者は、クラウドサービスの監査について方針を定め、監査を定期的に実施することが望ましい。クラウド事業者は、クラウドサービスを監査する場合において、全体的な支障プロセスの中断リスクを最小限にするための予防措置を行うことが望ましい。 また、クラウド事業者は、クラウド利用者との合意に基づき、利用者の情報システム監査実施に有用な情報を提供することが望ましい。	クラウド事業者を監査対象に入れた場合、複数のデータセンターにデータが分散されていたり、実際のデータの所在がどのサーバに あるのかを特定することができないなど、物理的に幾つかの管理策に対して監査が実施できないという問題に直面する可能性がある。そのため、クラウド事業者の監査についてはどのような監査を実施するか、あらかじめ監査項目や監査手順を明確にし、監査を実施することが期待される。 クラウド利用者は、利用するクラウドサービスについて自ら監査を実施する代わりに、クラウド事業者が提供する監査報告書を確認することができる。	定期的な情報セキュリティ監査の実施によって、セキュリティ確保が図られる。	当社の独立した監査と認定は、個々のお客様の監査に代わって、お客様と共有されます。これらの認定と認証は、当社のセキュリティおよび準拠の目標を設定および達成する方法を正確に表しており、すべてのお客様に対する約束を検証するための実用的なメカニズムとして機能します。数千にものぼるお客様に当社のサービスの監査を許可することは現実的ではなく、それによってセキュリティとプライバシーが侵害される可能性があります。当社の独立した第三者の検証プログラムには 1 年ごとに実施される監査が含まれており、それによって、Microsoft Online Services のセキュリティ制御を検証しています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス－監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、Microsoft Office365 及びGFSのISO27001認定については BSIグループのWebサイトを参照することができる。新規の利用者の場合、NDAに基づいて請求することでその他の監査情報を請求することにより入手できる。 利用者は、事前に承認を得ることにより、利用者自身のアプリケーションに対する非侵略的な侵入テストを実施することができる。
15.3.2	15 順守	15.3 情報システムの監査に対する考慮事項	15.3.2 情報システムの監査ツールの保護	情報システムを監査するツールの不正使用又は悪用を防止するために、それらのツールへのアクセスは、抑制することが望ましい。	–	–	–	–	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、“職務の分離” が規定されています。	適合可能	文献[01]では、情報システム監査ツールへのアクセスは、Microsoft Online Services で権限が与えられた担当者のみに制限されていることが明示されている。また、管理者は特定のタスクを実行するのに必要なアクセス権だけを持ち、エラーの可能性を抑えて、必要な場合に限りシステムや機能にアクセスできるようにしていることが明示されている。	公開文書	文献[01]「IS-29：情報セキュリティ－監査ツールへのアクセス」	–	–	–	–

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.1.1(1)	第2部 情報セキュリティ対策の基本的枠組み	2.1 導入・計画	2.1.1 組織・体制の整備	(1) 最高情報セキュリティ責任者の設置	(a) 府省庁は、府省庁における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者１人を置くこと。	2.1.1(1)-1 最高情報セキュリティ責任者は、次に掲げる事務を統括すること。 a) 情報セキュリティ対策推進のための組織・体制の整備 b) 府省庁対策基準の決定、見直し c) 対策推進計画の決定、見直し d) 情報セキュリティインシデントに対処するために必要な指示その他の措置 e) 前各号に掲げるもののほか、情報セキュリティに関する重要事項	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(2)				(2) 情報セキュリティ委員会の設置	(a) 最高情報セキュリティ責任者は、府省庁対策基準等の審議を行う機能を持つ組織として、府省庁の情報セキュリティを推進する部局及びその他行政事務を実施する部局の代表者を構成員とする情報セキュリティ委員会を置くこと。	2.1.1(2)-1 情報セキュリティ委員会の委員長及び委員は、最高情報セキュリティ責任者が情報セキュリティを推進する部局及びその他の行政事務を実施する部局の代表者から指名すること。 2.1.1(2)-2 情報セキュリティ委員会は、次に掲げる事項を審議すること。 a) 府省庁対策基準 b) 対策推進計画 c) 前各号に掲げるもののほか、情報セキュリティに関し必要な事項	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(3)				(3) 情報セキュリティ監査責任者の設置	(a) 最高情報セキュリティ責任者は、その指示に基づき実施する監査に関する事務を統括する者として、情報セキュリティ監査責任者１人を置くこと。	2.1.1(3)-1 情報セキュリティ監査責任者は、命により次の事務を統括すること。 a) 監査実施計画の策定 b) 監査実施体制の整備 c) 監査の実施指示及び監査結果の最高情報セキュリティ責任者への報告 d) 前各号に掲げるもののほか、情報セキュリティの監査に関する事項	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(4)				(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置	(a) 最高情報セキュリティ責任者は、業務の特性等から同質の情報セキュリティ対策の運用が可能な組織のまとまりごとに、情報セキュリティ対策に関する事務を統括する者として、情報セキュリティ責任者１人を置くこと。そのうち、情報セキュリティ責任者を統括し、最高情報セキュリティ責任者を補佐する者として、統括情報セキュリティ責任者１人を選任すること。	2.1.1(4)-1 統括情報セキュリティ責任者は、命を受け、次の事務を統括すること。 a) 要管理対策区域の決定並びに当該区域における施設及び環境に係る対策の決定 b) 情報セキュリティ対策に関する実施手順の整備及び見直し並びに実施手順に関する事務のとりまとめ c) 情報セキュリティ対策に係る教育実施計画の策定及び当該実施体制の整備 d) 例外措置の適用審査記録の台帳整備等 e) 情報セキュリティインシデントに対処するための緊急連絡窓口の整備等 f) 前各号に掲げるもののほか、情報セキュリティ対策に係る事務 2.1.1(4)-2 情報セキュリティ責任者は、命を受け、管理を行う組織のまとまりにおける情報セキュリティ対策を推進するため、次の事務を統括すること。 a) 定められた区域ごとの区域情報セキュリティ責任者の設置 b) 課室の課室情報セキュリティ責任者の設置 c) 情報システムごとの情報システムセキュリティ責任者の設置 d) 情報セキュリティインシデントの原因調査、再発防止策等の実施 e) 情報セキュリティに係る自己点検計画の策定及び実施手順の整備 f) 前各号に掲げるもののほか、管理を行う組織のまとまりの情報セキュリティ対策に関する事務	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
					(b) 情報セキュリティ責任者は、遵守事項3.2.1(2)(a)で定める区域ごとに、当該区域における情報セキュリティ対策の事務を統括する区域情報セキュリティ責任者1人を置くこと。	2.1.1(4)-3 区域情報セキュリティ責任者は、命を受け、定められた区域における施設及び環境に係る情報セキュリティ対策に関する事務を統括すること。		適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
					(c) 情報セキュリティ責任者は、課室ごとに情報セキュリティ対策に関する事務を統括する課室情報セキュリティ責任者1人を置くこと。	2.1.1(4)-4 課室情報セキュリティ責任者は、命を受け、課室における情報の取扱いその他の情報セキュリティ対策に関する事務を統括すること。		適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
					(d) 情報セキュリティ責任者は、所管する情報システムに対する情報セキュリティ対策に関する事務の責任者として、情報システムセキュリティ責任者を、当該情報システムの企画に着手するまでに選任すること。	2.1.1(4)-5 情報システムセキュリティ責任者は、命を受け、情報システムにおける情報セキュリティ対策に関する事務を担うこと。 2.1.1(4)-6 情報システムセキュリティ責任者は、所管する情報システムの管理業務において必要な単位ごとに情報システムセキュリティ管理者を置くこと。		適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(5)				(5) 最高情報セキュリティアドバイザーの設置	(a) 最高情報セキュリティ責任者は、情報セキュリティについて専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、自らへの助言を含む最高情報セキュリティアドバイザーの業務内容を定めること。	2.1.1(5)-1 最高情報セキュリティ責任者は、以下を例とする最高情報セキュリティアドバイザーの業務内容を定めること。 a) 府省庁全体の情報セキュリティ対策の推進に係る最高情報セキュリティ責任者への助言 b) 情報セキュリティ関係規程の整備に係る助言 c) 対策推進計画の策定に係る助言 d) 教育実施計画の立案に係る助言並びに教材開発及び教育実施の支援 e) 情報システムに係る技術的事項に係る助言 f) 情報システムの設計・開発を外部委託により行う場合に調達仕様に含めて提示する情報セキュリティに係る要求仕様の策定に係る助言 g) 行政事務従事者に対する日常的な相談対応 h) 情報セキュリティインシデントへの対処の支援 i) 前各号に掲げるもののほか、情報セキュリティ対策への助言又は支援	セキュリティとプライバシーに関する業界のベスト プラクティスに対応するため、Microsoft Online Services では全体的な ISMS が設計および実装されています。	適合可能	文献[08]では、マイクロソフト クラウド インフラストラクチャの情報セキュリティ プログラム（オンラインのセキュリティ リスクに対処するために使用されるポリシーやプログラムを含む）を担当するGlobal Foundation Services (GFS)内のOnline Services Security and Compliance(OSSC)チームの存在を明示している。	公開文書	文献[08]「Online Services Security and Compliance チーム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(6)				(6) 情報セキュリティインシデントに備えた体制の整備	(a) 最高情報セキュリティ責任者は、CSIRTを整備し、その役割を明確化すること。	2.1.1(6)-1 最高情報セキュリティ責任者は、以下を含むCSIRTの役割を規定すること。 a) 報告窓口からの情報セキュリティインシデントの報告の受付 b) 情報セキュリティインシデントの最高情報セキュリティ責任者等への報告 c) 内閣官房情報セキュリティセンターへの連絡 d) 被害の拡大防止を図るための応急措置の指示又は勧告 2.1.1(6)-2 最高情報セキュリティ責任者は、CSIRTの代表者（PoC（Point of Contact））を置くこと。	Microsoft Online では、インシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発しています。セキュリティ インシデントには以下のものが含まれます（ただしこれらに限りません）。電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動。 マイクロソフトのプロセスは、特定、封じ込め、根絶、復元、および教訓の学習の手順から構成されています。 ISO 27001 規格（具体的には付属文書 A の項 13.2）で、"セキュリティ インシデントの対応計画" が規定されています。	適合可能	文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策および態勢が整備されていることが明示されている。	公開文書	文献[01]「IS-22：情報セキュリティインシデント管理」	―	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(b) 最高情報セキュリティ責任者は、行政事務従事者のうちからCSIRTに属する職員として専門的な知識又は適性を有すると認められる者を選任すること。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者としてCSIRT責任者を置くこと。	-	外部からの不正アクセス対策として、複数の手段による多層的な予防措置を行っているほか、検出、抑制、回復手段を合わせて使用しています。 また、クラウドサービスチームに専門のCSIRTを置き、全社CSIRTと連携してインシデント対応を行うこととしています。	適合可能	文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策および態勢が整備されていることが明示されている。	公開文書	文献[01]「IS-22：情報セキュリティインシデント管理」	―	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
					(c) 最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。	-		適合可能	文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策および態勢が整備されていることが明示されている。	公開文書	文献[01]「IS-22：情報セキュリティインシデント管理」	―	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
					(d) 最高情報セキュリティ責任者は、CYMATに属する職員を指名すること。	-	（CYMATについては対象外）	対象外	―	―	―	―	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.1(7)				(7) 兼務を禁止する役割	(a) 行政事務従事者は、情報セキュリティ対策の運用において、以下の役割を兼務しないこと。 (ア) 承認又は許可（以下、本項において「承認等」という。）の申請者と当該承認等を行う者（以下、本項において「承認権限者等」という。） (イ) 監査を受ける者とその監査を実施する者 (b) 行政事務従事者は、承認等を申請する場合において、自らが承認権限者等であるときその他承認権限者等が承認等の可否の判断をすることが不適切と認められるときは、当該承認権限者等の上司又は適切な者に承認等を申請し、承認等を得ること。	【 基本対策事項 】規定なし	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[17]では、マイクロソフト データ センターにおいてお客様のデータが保存されている IT システムにアクセスするスタッフは役割ベースのアクセス制御（RBAC：職務分離の原則と最小限の権限の付与という原則に従う自動化プロセス）によって制御されること、当該スタッフは、身元審査、指紋、必要なセキュリティ トレーニング、アクセスの承認などの資格要件を満たしていることが保証されることが明示されている。 また、文献[01]では、マイクロソフトのサポート スタッフはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があることが明示されている。	公開文書	文献[17]「組込みのセキュリティ/自動運用」 文献[01]「IS-15：情報セキュリティ－職務分離」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティに関する体制を検討する必要がある。
2.1.2(1)			2.1.2 府省庁対策基準・対策推進計画の策定	(1) 府省庁対策基準の策定	(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、統一基準に準拠した府省庁対策基準を定めること。	【 基本対策事項 】規定なし	（府省庁対策基準については対象外）	対象外	―	―	―	―	―	―	利用者は、自組織の対策基準を検討する必要がある。
2.1.2(2)				(2) 対策推進計画の策定	(a) 最高情報セキュリティ責任者は、情報セキュリティ委員会における審議を経て、情報セキュリティ対策を総合的に推進するための計画（以下「対策推進計画」という。）を定めること。また、対策推進計画には、府省庁の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた全体方針並びに以下に掲げる取組の方針・重点及びその実施時期を含めること。 (ア) 情報セキュリティに関する教育 (イ) 情報セキュリティ対策の自己点検 (ウ) 情報セキュリティ監査 (エ) 情報システムに関する技術的な対策を推進するための取組 (オ) 前各号に掲げるもののほか、情報セキュリティ対策に関する重要な取組	【 基本対策事項 】規定なし	（府省庁対策基準については対象外）	対象外	―	―	―	―	―	利用者は、自組織の対策推進計画を検討する必要がある。
2.2.1(1)		2.2 運用	2.2.1 情報セキュリティ関係規程の運用	(1) 情報セキュリティ対策に関する実施手順の整備・運用	(a) 統括情報セキュリティ責任者は、府省庁における情報セキュリティ対策に関する実施手順を整備（本統一基準で整備すべき者を別に定める場合を除く。）し、実施手順に関する事務を統括し、整備状況について最高情報セキュリティ責任者に報告すること。 (b) 統括情報セキュリティ責任者は、情報セキュリティ対策における雇用の開始、終了及び人事異動時等に関する管理の規定を整備すること。 (c) 情報セキュリティ責任者又は課室情報セキュリティ責任者は、行政事務従事者より情報セキュリティ関係規程に係る課題及び問題点の報告を受けた場合は、統括情報セキュリティ責任者に報告すること。	【 基本対策事項 】規定なし	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Services のスタッフや契約業者のスタッフに対して情報資産やセキュリティに関連する役割と責任を含む情報セキュリティ ポリシーが提示されていることが明示されている。 さらに、インタビュー等を通じて、防災、防犯、業務の観点から、責任や権限が明確化されていることを確認した。	要NDA	文献[01]「IS-13：情報セキュリティ－役割/責任」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織の情報セキュリティ関係規程を適切に運用する必要がある。
2.2.1(2)				(2) 違反への対処	(a) 行政事務従事者は、情報セキュリティ関係規程への重大な違反を知った場合は、情報セキュリティ責任者にその旨を報告すること。 (b) 情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反の報告を受けた場合及び自らが重大な違反を知った場合には、違反者及び必要な者に情報セキュリティの維持に必要な措置を講じさせるとともに、統括情報セキュリティ責任者を通じて、最高情報セキュリティ責任者に報告すること。	【 基本対策事項 】規定なし	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格（具体的には付属文書 A の項 8.2）で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]にて、従業員との雇用にあたる合意事項として、下記の記載を確認した。 ・すべての従業員は Microsoft Online Servicesが開催するセキュリティ トレーニング プログラムに参加し、定期的なセキュリティ意識向上に関する最新情報を受け取ること ・セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われること ・従業員との契約に機密保持条項を含めていること また文献[01]では、Microsoft Online Services では契約により、下請業者に対し重要なプライバシーおよびセキュリティ要件を満たすよう求めることが明示されている。 文献[02]では、下請業者に対する情報セキュリティ対策として下記が明示されている。 ・Microsoft は下請業者がサービスの提供を継続できるようにする場合に限り下請業者に顧客データを開示すること ・下請業者はそれ以外の目的のために顧客データを使用することは禁じられ、情報の機密保持を要求されること ・Microsoft が下請業者に対してMicrosoft のベンダープライバシーアシュアランスプログラムへの参加、契約による当社のプライバシー要件への準拠、および定期的なプライバシー トレーニングの受講を要求すること ・Microsoft によって管理されている施設や機器で業務を行う下請業者は Microsoft のプライバシー基準に従うよう契約によって義務付けられていること ・その他のすべての下請業者は当社と同等のプライバシー基準に従うよう契約によって義務付けられていること インタビュー等を通じて、外部委託先の選定についての手順が定まっていること、最終的に委託業者は文献[42]についての合意が求められることを確認した。	要NDA	文献[01]「CO-03：コンプライアンス－サード パーティの監査」 文献[01]「DG-05：データ ガバナンス－安全な廃棄」 文献[02]「顧客データが下請業者に開示される場合」 文献[02]「Microsoft のプライバシー要件」 文献[42]	―	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における情報セキュリティ規程違反の対処を適切に行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.2.2(1)			2.2.2 例外措置	(1) 例外措置手続の整備	(a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者（以下「許可権限者」という。）及び、審査手続を定めること。	2.2.2(1)-1 最高情報セキュリティ責任者は、例外措置について以下を含む手順を定めること。 a) 例外措置の許可権限者 b) 事前申請の原則その他の申請方法 c) 審査項目その他の審査方法 ・申請者の情報（氏名、所属、連絡先） ・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等） ・例外措置の適用を申請する期間 ・例外措置の適用を申請する措置内容（講ずる代替手段等） ・例外措置により生じる情報セキュリティ上の影響と対処方法 ・例外措置の適用を終了した旨の報告方法 ・例外措置の適用を申請する理由	各サービス・情報資産の特性に合わせて、そのサービス・資産のセキュリティ部門がセキュリティ例外処置に対する対応手順を定めることとしています。実際の例外措置の承認は情報資産の管理責任者の承認を必要とすると定めています。また、オンラインサービス運用管理規定（OSA）に対する例外は開発終了条件の未達とみなされ特別な承認処理を行うこととしています。	適合可能	インタビュー等を通じて、セキュリティに関連する例外措置の対応手順を定めていること、また例外措置の承認は情報資産の管理責任者による承認が必要であることを定めていることが確認できた。	要NDA	―	―	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織の情報セキュリティに係る例外措置手続を定め、運用する必要がある。
					(b) 統括情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、許可権限者に対して、定期的に申請状況の報告を求めること。	2.2.2(1)-2 許可権限者は、例外措置の適用審査記録に以下の内容を記載し、適用審査記録の台帳として保管するとともに、統括情報セキュリティ責任者へ定期的に報告すること。 a) 審査した者の情報（氏名、役割名、所属、連絡先） b) 申請内容 ・申請者の情報（氏名、所属、連絡先） ・例外措置の適用を申請する情報セキュリティ関係規程の該当箇所（規程名と条項等） ・例外措置の適用を申請する期間 ・例外措置の適用を申請する措置内容（講ずる代替手段等） ・例外措置の適用を終了した旨の報告方法 ・例外措置の適用を申請する理由 c) 審査結果の内容 ・許可又は不許可の別 ・許可又は不許可の理由 ・例外措置の適用を許可した情報セキュリティ関係規程の該当箇所（規程名と条項等） ・例外措置の適用を許可した期間 ・許可した措置内容（講ずるべき代替手段等） ・例外措置を終了した旨の報告方法		適合可能	インタビュー等を通じて、セキュリティに関連する例外措置の対応手順を定めていること、また例外措置の承認は情報資産の管理責任者による承認が必要であることを定めていることが確認できた。	要NDA	―	―	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織の情報セキュリティに係る例外措置手続を定め、運用する必要がある。
2.2.2(2)				(2) 例外措置の運用	(a) 行政事務従事者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。ただし、行政事務の遂行に緊急を要し、当該規定の趣旨を充分尊重した扱いを取ることができる場合であって、情報セキュリティ関係規程の規定とは異なる代替の方法を直ちに採用すること又は規定されている方法を実施しないことが不可避のときは、事後速やかに届け出ること。 (b) 許可権限者は、行政事務従事者による例外措置の適用の申請を、定められた審査手続に従って審査し、許可の可否を決定すること。 (c) 許可権限者は、例外措置の申請状況を台帳に記録し、統括情報セキュリティ責任者に報告すること。 (d) 統括情報セキュリティ責任者は、例外措置の申請状況を踏まえた情報セキュリティ関係規程の追加又は見直しの検討を行い、最高情報セキュリティ責任者に報告すること。	【 基本対策事項 】規定なし		適合可能	インタビュー等を通じて、セキュリティに関連する例外措置の対応手順を定めていること、また例外措置の承認は情報資産の管理責任者による承認が必要であることを定めていることが確認できた。	要NDA	―	―	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織の情報セキュリティに係る例外措置手続を定め、運用する必要がある。
2.2.3(1)			2.2.3 教育	(1) 教育体制等の整備	(a) 統括情報セキュリティ責任者は、情報セキュリティ対策に係る教育について、対策推進計画に基づき教育実施計画を策定し、その実施体制を整備すること。	2.2.3(1)-1 統括情報セキュリティ責任者は、行政事務従事者の役割に応じて教育すべき内容を検討し、教育のための資料を整備すること。 2.2.3(1)-2 統括情報セキュリティ責任者は、行政事務従事者が毎年度最低1回は教育を受講できるように、教育実施計画を立案するとともに、その実施体制を整備すること。 2.2.3(1)-3 統括情報セキュリティ責任者は、行政事務従事者の着任又は異動後に、3か月以内に受講できるように、その実施体制を整備すること。	マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティ トレーニング プログラムに参加し、該当する場合は定期的なセキュリティ意識向上に関する最新情報を受け取ります。セキュリティ教育は継続的なプロセスであり、リスクを最小限に抑えるために定期的に行われます。社内トレーニングの例としては、BlueHat が挙げられます。 Microsoft Online Services のすべての契約業者のスタッフは、その提供するサービスや実行する役割に応じたトレーニングを受ける必要があります。 ISO 27001 規格 (具体的には付属文書 A の項 8.2) で、"情報セキュリティの意識向上、教育、およびトレーニング" が規定されています。	適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加することが明示されている。	公開文書	文献[01]「HR-02：人的資源のセキュリティ－雇用における合意事項」「IS-11：情報セキュリティ－トレーニング/意識向上」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティ教育を実施する必要がある。
2.2.3(2)				(2) 教育の実施	(a) 課室情報セキュリティ責任者は、行政事務従事者に対して、情報セキュリティ関係規程に係る教育を適切に受講させること。 (b) 行政事務従事者は、教育実施計画に従って、適切な時期に教育を受講すること。 (c) 課室情報セキュリティ責任者は、CYMAT及びCSIRTに属する職員に教育を適切に受講させること。 (d) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者に情報セキュリティ対策に関する教育の実施状況について報告すること。	【 基本対策事項 】規定なし		適合可能	文献[01]では、マイクロソフト内の該当するすべてのスタッフは、Microsoft Online Services がスポンサーとなっているセキュリティトレーニング プログラムに参加することが明示されている。	公開文書	文献[01]「HR-02：人的資源のセキュリティ－雇用における合意事項」「IS-11：情報セキュリティ－トレーニング/意識向上」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織の情報セキュリティ教育を実施する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.2.4(1)			2.2.4 情報セキュリティインシデントへの対処	(1) 情報セキュリティインシデントに備えた事前準備	(a) 統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した際の報告窓口を含む府省庁関係者への報告手順を整備し、行政事務従事者に周知すること。 (b) 統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した際の府省庁外との情報共有を含む対処手順を整備すること。 (c) 統括情報セキュリティ責任者は、情報セキュリティインシデントに備え、行政事務の遂行のため特に重要と認めた情報システムについて、緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備すること。 (d) 統括情報セキュリティ責任者は、情報セキュリティインシデントへの対処の訓練の必要性を検討し、行政事務の遂行のため特に重要と認めた情報システムについて、その訓練の内容及び体制を整備すること。 (e) 統括情報セキュリティ責任者は、情報セキュリティインシデントについて府省庁外の者から報告を受けるための窓口を整備し、その窓口への連絡手段を府省庁外の者に周知すること。	【 基本対策事項 】規定なし	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]では、専門チームが組織され、サイバー攻撃に対する防止策・事前対策、検知・対応策および態勢が整備されていることが明示されている。	公開文書	文献[01]「IS-22: 情報セキュリティインシデント管理」	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
2.2.4(2)				(2) 情報セキュリティインシデントの認知時における報告・対処	(a) 行政事務従事者は、情報セキュリティインシデントを認知した場合には、府省庁の報告窓口に報告し、指示に従うこと。	【 基本対策事項 】規定なし		適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03: 復元 – ビジネス継続性の計画」「RS-04: 復元 – ビジネス継続性のテスト」 文献[65]	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
					(b) CSIRT責任者は、情報セキュリティインシデントを認知した場合にはその状況を確認し、情報セキュリティインシデントについて最高情報セキュリティ責任者に速やかに報告すること。	【 基本対策事項 】規定なし		適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03: 復元 – ビジネス継続性の計画」「RS-04: 復元 – ビジネス継続性のテスト」 文献[65]	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
					(c) CSIRTは、認知した情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び情報セキュリティインシデントからの復旧に係る指示又は勧告を行うこと。	【 基本対策事項 】規定なし		適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03: 復元 – ビジネス継続性の計画」「RS-04: 復元 – ビジネス継続性のテスト」 文献[65]	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
					(d) 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、府省庁で定められた対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処すること。	【 基本対策事項 】規定なし		適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03: 復元 – ビジネス継続性の計画」「RS-04: 復元 – ビジネス継続性のテスト」 文献[65]	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
					(e) 情報システムセキュリティ責任者は、認知した情報セキュリティインシデントが複数の府省庁で共通的に使用する情報システム（一府省庁でハードウェアからアプリケーションまで管理・運用している情報システムを除く。以下「基盤となる情報システム」という。）に関するものであり、当該基盤となる情報システムの情報セキュリティ対策に係る運用管理規程等が定められている場合には、当該運用管理規程等に従い、適切に対処すること。	【 基本対策事項 】規定なし	（基盤となる情報システムについては対象外）	対象外	–	–	–	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
					(f) CSIRTは、府省庁の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房情報セキュリティセンターに連絡すること。また、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態等においては、「大規模サイバー攻撃等への初動対処について（平成22年3月19日内閣危機管理監決裁）」に基づく報告も行うこと。	【 基本対策事項 】規定なし	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[05]では、マイクロソフトがセキュリティコミュニティと連携し、セキュリティガイダンスの提供等の対応が明示されている。	公開文書	文献[05] Microsoft Azureのトラストセキュリティセンター	–	–	–	利用者は必要に応じて、情報共有機関やセキュリティベンダー等と連携する必要がある。
					(g) CSIRTは、情報セキュリティインシデントに関して、府省庁を含む関係機関と情報共有を行うこと。	【 基本対策事項 】規定なし		適合可能	文献[05]では、マイクロソフトがセキュリティコミュニティと連携し、セキュリティガイダンスの提供等の対応が明示されている。	公開文書	文献[05] Microsoft Azureのトラストセキュリティセンター	–	–	–	利用者は必要に応じて、情報共有機関やセキュリティベンダー等と連携する必要がある。
					(h) CSIRTは、CYMATの支援を受ける場合には、支援を受けるに当たって必要な情報提供を行うこと。	【 基本対策事項 】規定なし	（CYMATは対象外）	対象外	–	–	–	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。
2.2.4(3)				(3) 情報セキュリティインシデントの原因調査・再発防止	(a) 情報セキュリティ責任者は、CSIRTの指示を受けた場合は、当該指示又は勧告を踏まえ、情報セキュリティインシデントの原因を調査するとともに再発防止策を検討し、それを報告書として最高情報セキュリティ責任者に報告すること。 (b) 最高情報セキュリティ責任者は、情報セキュリティ責任者から情報セキュリティインシデントについての報告を受けた場合には、その内容を確認し、再発防止策を実施するために必要な措置を指示すること。	【 基本対策事項 】規定なし	マイクロソフトのエンタープライズ向けクラウドサービスは、外部の第三者および内部の専門チームにより定期的にセキュリティ診断を受けています。 エンタープライズ向けクラウドサービスはそれぞれに、セキュリティインシデント対応チーム（CSIRT）を組織し、上位組織となる全社CSIRTと相互連携する態勢を整えています。また、マイクロソフトはサイバー犯罪に対応するデジタルクライムユニット（DSU）により最新の状況の監視と対応を進め、サイバー攻撃情報を、サイバークライムセンター（CCC）を通して関係者との共有を進めています。	適合可能	文献[01]で、セキュリティインシデントの対応報告の際のインシデントの特定（システムおよびセキュリティに関する警告や関連付け）が実施され、影響範囲の特定や根絶、再発防止策について明示されている。 文献[65]では、セキュリティインシデントの通知、情報セキュリティインシデントの記録および追跡について明示されている。	公開文書	文献[01]「RS-03: 復元 – ビジネス継続性の計画」「RS-04: 復元 – ビジネス継続性のテスト」 文献[65]	–	–	–	利用者は、自組織における情報セキュリティインシデントへの対処を適切に行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.3.1(1)		2.3 点検	2.3.1 情報セキュリティ対策の自己点検	(1) 自己点検計画の策定・手順の準備	(a) 統括情報セキュリティ責任者は、対策推進計画に基づき年度自己点検計画を策定すること。 (b) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検票及び自己点検の実施手順を整備すること。	【 基本対策事項 】規定なし	Microsoft Online Services の環境に向けた、サービス継続性の管理 (SCM) の開発およびメンテナンス プロセスが用意されています。このプロセスには、Microsoft Online Services 資産を回復し、Microsoft Online Services の主要なビジネス プロセスを再開するための方法が含まれています。継続性ソリューションによって、サービスの運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.4) で、"機器のメンテナンス" が規定されています。 Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。	適合可能	文献[01]では、Microsoft Online Servicesの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 また、インタビュー等を通じて、機器の障害防止の観点から、適切な対応がなされていることを確認した。 文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「OP-04：運用管理 – 機器のメンテナンス」「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織における情報セキュリティ対策の自己点検を適切に行う必要がある。
2.3.1(2)				(2) 自己点検の実施	(a) 情報セキュリティ責任者は、年度自己点検計画に基づき、行政事務従事者に自己点検の実施を指示すること。 (b) 行政事務従事者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。	【 基本対策事項 】規定なし	権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、Microsoft Online Servicesの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 また、インタビュー等を通じて、機器の障害防止の観点から、適切な対応がなされていることを確認した。 文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「OP-04：運用管理 – 機器のメンテナンス」「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織における情報セキュリティ対策の自己点検を適切に行う必要がある。
2.3.1(3)				(3) 自己点検結果の評価・改善	(a) 統括情報セキュリティ責任者及び情報セキュリティ責任者は、行政事務従事者による自己点検結果を分析し、評価すること。統括情報セキュリティ責任者は評価結果を最高情報セキュリティ責任者に報告すること。 (b) 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、自己点検の結果により明らかになった問題点について、統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示すること。	【 基本対策事項 】規定なし		適合可能	文献[01]では、Microsoft Online Servicesの環境に向けたメンテナンスプロセスが用意されていることが明示されている。 また、インタビュー等を通じて、機器の障害防止の観点から、適切な対応がなされていることを確認した。 文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「OP-04：運用管理 – 機器のメンテナンス」「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	利用者は、自組織における情報セキュリティ対策の自己点検を適切に行う必要がある。
2.3.2(1)			2.3.2 情報セキュリティ監査	(1) 監査実施計画の策定	(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。	2.3.2(1)-1 情報セキュリティ監査責任者は、対策推進計画に基づき、以下を例とする監査実施計画を策定すること。 a) 監査の目的（例：自己点検の適切性を監査すること等） b) 監査の対象（例：監査の対象となる組織、情報システム、業務等） c) 監査の方法（例：自己点検結果を検証するため、査閲、点検、観察、ヒアリング等を行う。監査の基準は、府省庁対策基準及び実施手順とする） d) 監査の実施体制（例：監査責任者、監査実施者の所属、氏名） e) 監査の実施時期（例：対象ごとの実施時期）	マイクロソフトでは、不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊から、お客様のデータを保護できるように、合理的かつ適切で、技術的および組織的な対策、内部統制、情報セキュリティ ルーチンを実装しており、今後もこれを維持していきます。年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されています。 ISO 27001 規格 (具体的には第 4.2.3 節) で、"Information Security Management System (ISMS) の監視およびレビュー" が規定されています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。
					(b) 情報セキュリティ監査責任者は、情報セキュリティの状況の変化に応じ、対策推進計画で計画された以外の監査の実施の指示を、最高情報セキュリティ責任者から受けた場合には、追加の監査実施計画を定めること。	–		適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。
2.3.2(2)				(2) 監査の実施	(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項を含む監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告すること。 (ア) 府省庁対策基準に統一基準を満たすための適切な事項が定められていること	2.3.2(2)-1 情報セキュリティ監査責任者は、監査業務の実施において必要となる者を、被監査部門から独立した者から選定し、情報セキュリティ監査実施者に指名すること。 2.3.2(2)-2 情報セキュリティ監査責任者は、組織内における監査遂行能力が不足等している場合には、府省庁外の者に監査の一部を請け負わせること。	マイクロソフトでは、不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊から、お客様のデータを保護できるように、合理的かつ適切で、技術的および組織的な対策、内部統制、情報セキュリティ ルーチンを実装しており、今後もこれを維持していきます。年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されています。 ISO 27001 規格 (具体的には第 4.2.3 節) で、"Information Security Management System (ISMS) の監視およびレビュー" が規定されています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。
					(イ) 実施手順が府省庁対策基準に準拠していること (ウ) 自己点検の適正性の確認を行うなどにより、被監査部門における実際の運用が情報セキュリティ関係規程に準拠していること	–		適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。
2.3.2(3)				(3) 監査結果に応じた対処	(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する対処計画の策定等を情報セキュリティ責任者に指示すること。	2.3.2(3)-1 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ監査を受けた部門以外の部門においても同種の課題又は問題点がある可能性が高く、並びに緊急に同種の課題又は問題点があることを確認する必要があると判断した場合には、他の部門の情報セキュリティ責任者に対しても、同種の課題又は問題点の有無を確認するように指示すること。	マイクロソフトでは、不慮の損失、破壊、または変更、承認されていない開示やアクセス、または不法行為による破壊から、お客様のデータを保護できるように、合理的かつ適切で、技術的および組織的な対策、内部統制、情報セキュリティ ルーチンを実装しており、今後もこれを維持していきます。年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されています。 ISO 27001 規格 (具体的には第 4.2.3 節) で、"Information Security Management System (ISMS) の監視およびレビュー" が規定されています。	適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。
					(b) 情報セキュリティ責任者は、監査報告書等に基づいて最高情報セキュリティ責任者から改善を指示されたことについて、対処計画を策定し、報告すること。	–		適合可能	文献[01]では、年に 1 度、国際的に認められた第三者機関による監査を受けており、セキュリティ、プライバシー、継続性、およびコンプライアンスに関するポリシーと手順を遵守していることが独立機関によって検証されていることが明示されている。	公開文書	文献[01]「CO-01：コンプライアンス – 監査計画」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織における情報セキュリティ監査を適切に行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
2.4.1(1)		2.4 見直し	2.4.1 情報セキュリティ対策の見直し	(1) 情報セキュリティ関係規程の見直し	(a) 最高情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、府省庁対策基準について必要な見直しを行うこと。 (b) 統括情報セキュリティ責任者は、情報セキュリティの運用及び自己点検・監査等の結果等を踏まえて情報セキュリティ対策に関する実施手順を見直し、又は整備した者に対して規定の見直しを指示し、見直し結果について最高情報セキュリティ責任者に報告すること。	【 基本対策事項 】規定なし	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。Microsoft Online Services では、Office 365 サービスの一環として、包括的なガバナンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 ・ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 ・Exchange 管理者向けのビデオ ・ハイブリッド環境の構成に必要な記事および手順 ・ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki ・停止や問題に関する情報が得られる、サービスの正常性ダッシュボード ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて情報セキュリティポリシーが定期的に確認及び更新されることが明示されている。 さらに文献[03]では、各ポリシー、標準、およびベースラインが年に 1 回のベースで見直されることが明示されている。	公開文書	文献[01]「IS-05：情報セキュリティ・ポリシーの確認」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織のおける情報セキュリティ対策の見直しを適切に行う必要がある。
2.4.1(2)				(2) 対策推進計画の見直し	(a) 最高情報セキュリティ責任者は、情報セキュリティ対策の運用及び点検・監査等を総合的に評価するとともに、情報セキュリティに係る重大な変化等を踏まえ、情報セキュリティ委員会の審議を経て、対策推進計画について定期的な見直しを行うこと。	【 基本対策事項 】規定なし	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。Microsoft Online Services では、Office 365 サービスの一環として、包括的なガバナンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 ・ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 ・Exchange 管理者向けのビデオ ・ハイブリッド環境の構成に必要な記事および手順 ・ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki ・停止や問題に関する情報が得られる、サービスの正常性ダッシュボード ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて情報セキュリティポリシーが定期的に確認及び更新されることが明示されている。 さらに文献[03]では、各ポリシー、標準、およびベースラインが年に 1 回のベースで見直されることが明示されている。	公開文書	文献[01]「IS-05：情報セキュリティ・ポリシーの確認」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織のおける情報セキュリティ対策の見直しを適切に行う必要がある。
3.1.1(1)	第3部 情報の取扱い	3.1 情報の取扱い	3.1.1 情報の取扱い	(1) 情報の取扱いに係る規定の整備	(a) 統括情報セキュリティ責任者は、以下を含む情報の取扱いに関する規定を整備し、行政事務従事者へ周知すること。	3.1.1(1)-1 統括情報セキュリティ責任者は、情報の取扱いに関する規定として、以下を例とする手順を整備すること。 a) 情報のライフサイクル全般にわたり必要な手順（行政事務の遂行以外の目的での情報の利用等の禁止等） b) 情報の入手・作成時の手順 c) 情報の利用・保存時の手順 d) 情報の提供・公表時の手順 e) 情報の運搬・送信時の手順 f) 情報の消去時の手順 g) 情報のバックアップ時の手順	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。Microsoft Online Services では、Office 365 サービスの一環として、包括的なガバナンス、ヘルプ、トレーニング、およびトラブルシューティング用の資料を用意しています。管理ポータルには、次のような使用可能な数多くのリソースへのリンクが用意されています。 ・ユーザー、および Office 365 を管理する必要のある管理者向けのヘルプ記事 ・Exchange 管理者向けのビデオ ・ハイブリッド環境の構成に必要な記事および手順 ・ヘルプ記事やホワイトペーパーが公開されているコミュニティ フォーラムや Wiki ・停止や問題に関する情報が得られる、サービスの正常性ダッシュボード ISO 27001 規格 (具体的には付属文書 A の項 10.8.1 および 12.5.4) で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて全体的なISMSが設計および実装されていること、情報セキュリティポリシーの文書が規定されていることが明示されている。 さらに文献[03]では、情報セキュリティ ポリシー プログラムを通じて、各ポリシー、標準、およびベースラインが整備される取組みが明示されている。	公開文書	文献[01]「IS-01：情報セキュリティ・管理プログラム」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、情報の取扱いに関する規定を整備する必要がある。
					(ア) 情報の格付及び取扱制限についての定義	-	（Office365上の情報の格付及び取扱いについてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の格付け及び取扱制限について定める必要がある。
					(イ) 情報の格付及び取扱制限の明示等についての手続	3.1.1(1)-2 統括情報セキュリティ責任者は、情報の格付及び取扱制限の明示の方法について、以下を例に、規定を整備すること。 a) 電磁的記録として取り扱われる情報に明示する場合 ・電磁的記録の本体である文書ごとにヘッダ部分又は情報の内容へ直接記載 ・電磁的ファイル等の取扱単位ごとにファイル名自体へ記載 ・フォルダ単位等で取り扱う情報は、フォルダ名に記載 ・電子メールで取り扱う情報は、メール本文又はメール件名に記載 b) 外部電磁的記録媒体に保存して取り扱う情報に明示する場合 ・保存する電磁的ファイル又は文書等の単位ごとに記載 ・外部電磁的記録媒体本体に記載 c) 書面に印刷されることが想定される場合 ・書面のヘッダ部分等に記載 ・冊子等の単位で取り扱う場合は、冊子の表紙、裏表紙等に記載 d) 既に書面として存在している情報に対して格付や取扱制限を明示する場合 ・手書きによる記入 ・スタンプ等による押印 3.1.1(1)-3 統括情報セキュリティ責任者は、情報の格付及び取扱制限の明示を省略する必要がある場合には、これらに係る認識が共通となるその他の措置の実施条件や実施方法について、規定を整備すること。	（Office365上の情報の格付及び取扱いについてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の格付け及び取扱制限について定める必要がある。
					(ウ) 情報の格付及び取扱制限の継承、見直しに関する手続	3.1.1(1)-4 統括情報セキュリティ責任者は、情報の加工時、複製時等における格付及び取扱制限の継承、見直しについて、以下を例に、規定を整備すること。 a) 情報を作成する際に、参照した情報又は入手した情報の機密性に係る格付及び取扱制限を継承する。 b) 既存の情報に、より機密性の高い情報を追加するときは、格付及び取扱制限を見直す。 c) 機密性の高い情報から機密に該当する部分を削除したときは、残りの情報の機密性に応じて格付及び取扱制限を見直す。 d) 情報を複製する場合には、元となる情報の機密性に係る格付及び取扱制限を継承する。 e) 完全性及び可用性については、作成時又は複製時に適切な格付を決定する。 f) 他者が決定した情報の格付及び取扱制限を見直す必要がある場合には、その決定者（決定について引き継いだ者を含む。）又はその上司（以下本項において「決定者等」という。）に確認を求める。	（Office365上の情報の格付及び取扱いについてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の格付け及び取扱制限について定める必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.1.1(2)				(2) 情報の目的外での利用等の禁止	(a) 行政事務従事者は、自らが担当している行政事務の遂行のために必要な範囲に限って、情報を利用等すること。	【 基本対策事項 】規定なし	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格（具体的には付属文書 A の項 10.1.3）で、"職務の分離" が規定されています。	適合可能	文献[01]「IS-13：情報セキュリティ－役割/責任」 文献[01]「IS-15：情報セキュリティ－職務分離」	公開文書	文献[01]「IS-13：情報セキュリティ－役割/責任」 文献[01]「IS-15：情報セキュリティ－職務分離」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織のユーザが情報の目的外での利用を禁止する対策を講じる必要がある。
3.1.1(3)				(3) 情報の格付及び取扱制限の決定・明示等	(a) 行政事務従事者は、情報の作成時及び府省庁外の者が作成した情報を入手したことに伴う管理の開始時に、格付及び取扱制限の定義に基づき格付及び取扱制限を決定し、明示等すること。 (b) 行政事務従事者は、情報を機密性3情報と決定した場合には、機密性3情報として取り扱う期間を明示等すること。 (c) 行政事務従事者は、情報を作成又は複製する際に、参照した情報又は入手した情報に既に格付及び取扱制限の決定がなされている場合には、元となる情報の機密性に係る格付及び取扱制限を継承すること。 (d) 行政事務従事者は、修正、追加、削除その他の理由により、情報の格付及び取扱制限を見直す必要があると考える場合には、情報の格付及び取扱制限の決定者（決定を引き継いだ者を含む。）又は決定者の上司（以下この項において決定者等という。）に確認し、その結果に基づき見直すこと。	【 基本対策事項 】規定なし	（Office365上の情報の格付及び取扱いについてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の格付け及び取扱制限について定める必要がある。
3.1.1(4)				(4) 情報の利用・保存	(a) 行政事務従事者は、利用する情報に明示等された格付及び取扱制限に従い、当該情報を適切に取り扱うこと。	3.1.1(4)-1 行政事務従事者は、情報の格付及び取扱制限に応じて、情報を以下のとおり取り扱うこと。 a) 要保護情報を放置しないこと。 b) 機密性3情報を必要以上に複製しないこと。 c) 要機密情報を必要以上に配布しないこと。 d) 閲覧可能範囲の制限が指定されている情報については、制限範囲外の者に情報の参照等をさせないために、施錠のできる書庫・保管庫に保存する。 e) 書面に機密性3情報を出力する場合は、書面ごとに一連番号を付与し、その所在を明らかにしておく。 f) 電磁的記録媒体に保存された要保護情報について、適切なアクセス制御を行う。 g) 電磁的記録媒体に要機密情報を保存する場合には、主体認証情報を用いて保護するか又は情報を暗号化する。 h) 電磁的記録媒体に要保全情報を保存する場合には、電子署名の付与を行うなど、改ざん防止のための措置を講ずる。 i) 情報の保存方法を変更する場合には、格付、取扱制限及び記録媒体の特性に応じて必要な措置を講ずる。 j) 情報の格付又は取扱制限が明示等されていない場合には、情報の作成元への確認を行う。	（Office365上の情報の利用・保存についてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報について、自組織のユーザに対して、格付け及び取扱制限に従い適切に利用させる必要がある。
					(b) 行政事務従事者は、機密性3情報について要管理対策区域外で情報処理を行う場合は、情報システムセキュリティ責任者及び課室情報セキュリティ責任者の許可を得ること。 (c) 行政事務従事者は、要保護情報について要管理対策区域外で情報処理を行う場合は、必要な安全管理措置を講ずること。 (d) 行政事務従事者は、保存する情報にアクセス制限を設定するなど、情報の格付及び取扱制限に従って情報を適切に管理すること。 (e) 行政事務従事者は、USBメモリ等の外部電磁的記録媒体を用いて情報を取り扱う際、定められた利用手順に従うこと。	-	（Office365上の情報の利用・保存についてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報について、自組織のユーザに対して、格付け及び取扱制限に従い適切に利用させる必要がある。
3.1.1(5)				(5) 情報の提供・公表	(a) 行政事務従事者は、情報を公表する場合には、当該情報が機密性1情報に格付されるものであることを確認すること。 (b) 行政事務従事者は、閲覧制限の範囲外の者に情報を提供する必要が生じた場合は、当該格付及び取扱制限の決定者等に相談し、その決定に従うこと。また、提供先において、当該情報に付された格付及び取扱制限に応じて適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ずること。 (c) 行政事務従事者は、機密性3情報を閲覧制限の範囲外の者に提供する場合には、課室情報セキュリティ責任者の許可を得ること。	-	（Office365上の情報の提供・公表についてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の提供・公表について適切に運用する必要がある。
					(d) 行政事務従事者は、電磁的記録を提供又は公表する場合には、当該電磁的記録の付加記録（更新の履歴、文書のプロパティ等をいう。）等からの不用意な情報漏えいを防止するための措置を講ずること。	3.1.1(5)-1 行政事務従事者は、電磁的記録媒体を他の者へ提供する場合は、当該電磁的記録媒体に保存された不要な要機密情報を抹消すること。	（Office365上の情報の提供・公表についてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、取扱う情報の提供・公表について適切に運用する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.1.1(6)				(6) 情報の運搬・送信	(a) 行政事務従事者は、機密性3情報、要保全情報又は要安定情報を、要管理対策区域外に持ち出し他の場所に運搬する場合又は府省庁外通信回線を使用して送信する場合には、課室情報セキュリティ責任者の許可を得ること。	-	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー（静脈認証）、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 · マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 · アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 · マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格 (具体的には付属文書 A の項 9) で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータ センター SSAE16 の監査対象となっております。 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。 Office 365で、利用者・管理者のクライアント機器とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」 「SA-11: セキュリティアーキテクチャー - 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	ー	利用者は、自組織のユーザに対して、機密性の高い情報の運搬・送信を適切に実施させる必要がある。
					(b) 行政事務従事者は、要保護情報が記録又は記録された記録媒体を要管理対策区域外に持ち出す場合には、安全確保に留意して運搬方法を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。ただし、他府省庁の要管理対策区域であって、統括情報セキュリティ責任者があらかじめ定めた区域のみに持ち出す場合は、当該区域を要管理対策区域と見なすことができる。 (c) 行政事務従事者は、要保護情報である電磁的記録を電子メール等で送信する場合には、安全確保に留意して送信の手段を決定し、情報の格付及び取扱制限に応じて、安全確保のための適切な措置を講ずること。	3.1.1(6)-1 行政事務従事者は、要保護情報が記録又は記載された記録媒体の要管理対策区域外への運搬を第三者へ依頼する場合は、セキュアな運送サービスを提供する運送事業者により運搬すること。 3.1.1(6)-2 行政事務従事者は、要機密情報である電磁的記録を要管理対策区域外に運搬又は府省庁外通信回線を使用して送信する場合には、情報漏えいを防止するため、以下を例とする対策を講ずること。 a) 運搬又は送信する情報を暗号化する。 b) 運搬又は送信を複数の情報に分割してそれぞれ異なる経路及び手段を用いる。 c) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。 3.1.1(6)-3 行政事務従事者は、要保全情報である電磁的記録を要管理対策区域外に運搬又は府省庁外通信回線を使用して送信する場合には、情報の改ざんを防止するため、以下を例とする措置を講ずること。 a) 電子署名を付与する。 b) あらかじめバックアップを取得しておく。 3.1.1(6)-4 行政事務従事者は、要保護情報である電磁的記録を送信する場合は、安全確保に留意して、以下を例に当該情報の送信の手段を決定すること。 a) 府省庁管理の通信回線を用いて送信する。 b) 信頼できる通信回線を使用して送信する。 c) VPNを用いて送信する。 d) S/MIME等の暗号化された電子メールを使用して送信する。 e) 府省庁独自で運用するなどセキュリティが十分確保されたウェブメールサービス又はオンラインストレージ環境を利用する。	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー（静脈認証）、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 · マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 · アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 · マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格 (具体的には付属文書 A の項 9) で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータ センター SSAE16 の監査対象となっております。 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。 Office 365で、利用者・管理者のクライアント機器とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」 「SA-11: セキュリティアーキテクチャー - 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	ー	利用者は、自組織のユーザに対して、機密性の高い情報の運搬・送信を適切に実施させる必要がある。
3.1.1(7)				(7) 情報の消去	(a) 行政事務従事者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること。 (b) 行政事務従事者は、電磁的記録媒体を廃棄する場合には、当該記録媒体内に情報が残留した状態とならないよう、全ての情報を復元できないように抹消すること。 (c) 行政事務従事者は、要機密情報である書面を廃棄する場合には、復元が困難な状態にすること。	【 基本対策事項 】規定なし	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、償却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 すべての Microsoft Online Services は、承認された記憶域メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.6 および 10.7.2) で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、承認された記憶域メディアと廃棄管理サービスを使用すること、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ることが明示されている。 NDA文書を確認したところ、重要な記録は契約等に基づいて紛失などに備えていることが確認できた。	要NDA	文献[01]「DG-05: データガバナンス - 安全な廃棄」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、重要な印字済帳票の授受および廃棄の方法を定める必要がある。
3.1.1(8)				(8) 情報のバックアップ	(a) 行政事務従事者は、情報の格付に応じて、適切な方法で情報のバックアップを実施すること。	3.1.1(8)-1 行政事務従事者は、要保全情報又は要安定情報である電磁的記録又は重要な設計書について、バックアップを取得すること。	バックアップの場合、内容がプライマリー データ センターからセカンダリー データ センターにレプリケートされます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。	適合可能	文献[01]では、定期的にプライマリーデータセンターからセカンダリーデータセンターにレプリケートされること、お客様は必要に応じて自社でのデータの抽出およびバックアップの実行を選択できることが明示されている。	公開文書	文献[01]「DG-04: データガバナンス - 保持ポリシー」	（マイクロソフト社とのNDAにより開示）	ー	ー	利用者は、必要に応じて自組織でのデータの抽出およびバックアップの実行を選択する必要がある。
					(b) 行政事務従事者は、取得した情報のバックアップについて、格付及び取扱制限に従って保存場所、保存方法、保存期間等を定め、適切に管理すること。 (c) 行政事務従事者は、保存期間を過ぎた情報のバックアップについては、本項(7)の規定に従い、適切な方法で消去、抹消又は廃棄すること。	3.1.1(8)-2 行政事務従事者は、要保全情報、要安定情報である電磁的記録のバックアップ又は重要な設計書のバックアップの保管について、災害等により生ずる業務上の支障を考慮し、適切なバックアップの手段又は保管場所を選定すること。	バックアップの場合、内容がプライマリー データ センターからセカンダリー データ センターにレプリケートされます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。	適合可能	文献[01]では、定期的にプライマリーデータセンターからセカンダリーデータセンターにレプリケートされること、お客様は必要に応じて自社でのデータの抽出およびバックアップの実行を選択できることが明示されている。	公開文書	文献[01]「DG-04: データガバナンス - 保持ポリシー」	（マイクロソフト社とのNDAにより開示）	ー	ー	利用者は、必要に応じて自組織でのデータの抽出およびバックアップの実行を選択する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
3.2.1(1)		3.2 情報を取り扱う区域の管理	3.2.1 情報を取り扱う区域の管理	(1) 要管理対策区域における対策の基準の決定	(a) 統括情報セキュリティ責任者は、要管理対策区域の範囲を定めること。	-	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
					(b) 統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。 (ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。 (イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。	3.2.1(1)-1 統括情報セキュリティ責任者は、以下を例とする、要管理対策区域の安全性を確保するための段階的な対策の水準（以下"クラス"という。）を定めること。 a) 下表のとおり、3段階のクラスを定める。 クラス3 一部の限られた者以外の者の立入りを制限する必要があるなど、クラス2より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域 クラス2 行政事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域 クラス1 クラス3、クラス2以外の要管理対策区域 ※便宜上、要管理対策区域外の区域はクラス0と呼び、クラス0＜クラス1＜クラス2＜クラス3の順位を設ける。すなわち、クラス0が最も下位のクラス、クラス3が最も上位のクラスとなる。	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
						3.2.1(1)-2 統括情報セキュリティ責任者は、クラス1の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。 a) 不特定の者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。 b) 不特定の者が容易に立ち入らないように、立ち入る者の身元、訪問目的等の確認を行うための措置を講ずること。また、出入口が無人になるなどにより立入りの確認ができない時間帯がある場合には、確認ができない時間帯に施錠するための措置を講ずること。 c) クラス2以上の区域に不正に立ち入った者を容易に判別することができるように、以下を含む措置を講ずること。 · 行政事務従事者は、身分証明書等を着用、明示する。クラス2及びクラス3の区域においても同様とする。 · 一時的に立ち入った者に入館カード等を貸与し、着用、明示させる。クラス2及びクラス3の区域においても同様とする。この際、一時的に立ち入った者と継続的に立入りを許された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行う。また、悪用防止のために一時的に立ち入った者に貸与したものは、退出時に回収する。	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
						3.2.1(1)-3 統括情報セキュリティ責任者は、クラス2の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。 a) クラス2の区域への立入りを許可されていない者が容易に立ち入らないように、壁、施錠可能な扉、パーティション等で囲むことで、下位のクラスの区域と明確に区分すること。ただし、窓口のある執務室等の明確に区分できない区域については、不特定の者が出入りできる時間帯は行政事務従事者が窓口を常に目視できるような措置を講ずること。 b) クラス2の区域への立入りを許可されていない者が容易に立ち入らないように、施錠可能な扉を設置し全員不在時に施錠すること。 c) クラス2の区域へ許可されていない者が容易に立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
						3.2.1(1)-4 統括情報セキュリティ責任者は、クラス3の区域について、以下を含む施設の整備、設備の設置等の物理的な対策及び入退管理対策の基準を定めること。 a) クラス3の区域への立入りを許可されていない者の立入り等を防止するために、壁、常時施錠された扉、固定式のパーティション等強固な境界で下位のクラスの区域と明確に区分すること。 b) クラス3の区域へ許可されていない者が立ち入らないように、立ち入る者が許可された者であることの確認を行うための措置を講ずること。 c) クラス3の区域への立入りを許可されていない者に、不必要に情報を与えないために、区域の外側から内部の重要な情報や情報システムが見えないようにすること。 d) 一時的に立ち入った者が不正な行為を行うことを防止するために、一時的に立ち入った者を放置しないなどの措置を講ずること。業者が作業を行う場合は立会いや監視カメラ等により監視するための措置を講ずること。	データ センターの建物は目立たないようにし、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
						3.2.1(1)-5 統括情報セキュリティ責任者は、以下を例とする、区域へのクラスの割当ての基準を定めること。 a) クラスの割当ての基準を以下のように定める。 ・サーバ室や日常的に機密性が高い情報を取り扱う執務室には、一部の限られた者以外の者が立ち入り盗難又は破壊をすること、情報システムを直接操作して情報窃取すること等を防止するために、クラス3を割り当てる。 ・一般的な執務室や執務室内の会議室には、行政事務従事者以外の者が立ち入り、情報システムを盗難又は破壊すること、情報システムを直接操作して情報窃取すること等を防止するために、クラス2を割り当てる。	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
3.2.1(2)				(2) 区域ごとの対策の決定	(a) 情報セキュリティ責任者は、統括情報セキュリティ責任者が定めた対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。	-		適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
					(b) 区域情報セキュリティ責任者は、管理する区域について、統括情報セキュリティ責任者が定めた対策の基準と、周辺環境や当該区域で行う行政事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。	3.2.1(2)-1 区域情報セキュリティ責任者は、管理する区域において、クラスの割当ての基準を参考にして当該区域に割り当てるクラスを決定するとともに、決定したクラスに対して定められた対策の基準と、周辺環境や当該区域で行う行政事務の内容、取り扱う情報等を勘案し、当該区域において実施する対策を決定すること。この際、決定したクラスで求められる対策のみでは安全性が確保できない場合は、当該区域で実施する個別の対策を含め決定すること。		適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
3.2.1(3)				(3) 要管理対策区域における対策の実施	(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。行政事務従事者が実施すべき対策については、行政事務従事者が認識できる措置を講ずること。	3.2.1(3)-1 区域情報セキュリティ責任者は、管理する区域について、以下を例とする利用手順等を整備し、当該区域を利用する行政事務従事者に周知すること。 a) 扉の施錠及び開閉に関する利用手順 b) 一時的に立ち入る者が許可された者であることを確認するための手順 c) 一時的に立ち入る者を監視するための手順	データ センターの建物は目立たないように、その場所でマイクロソフトのデータ センター ホスティング サービスが提供されていることを公表しないようにします。データ センターの施設へのアクセスは制限されます。主要な内部エリアまたは受付エリアには、その周囲のドアに電子カードによるアクセス コントロール機器が取り付けられており、これによって内部施設へのアクセスが制限されます。マイクロソフトのデータ センター内の重要なシステム（サーバー、発電機、電子パネル、ネットワーク機器など）が設置されている部屋は、電子カードによるアクセス コントロール、キーによるロック、共連れ防止機能、生体認証デバイスなどのさまざまなセキュリティ メカニズムによって入室が制限されます。 特定の資産に関しては、ポリシーやビジネス要件に応じて、"施錠可能な棚"、または施設境界内に設置される施錠可能なケージなど、他の物理的な障壁を敷設する場合があります。 ISO 27001 規格（具体的には付属文書 A の項 9）で、"物理的なセキュリティ境界および環境上のセキュリティ" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
					(b) 区域情報セキュリティ責任者は、災害から要安定情報を取り扱う情報システムを保護するために物理的な対策を講ずること。 (c) 行政事務従事者は、利用する区域について区域情報セキュリティ責任者が定めた対策に従って利用すること。また、行政事務従事者が府省庁外の者を立ち入らせる際には、当該府省庁外の者にも当該区域で定められた対策に従って利用させること。	-		適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織における要管理対策区域における対策の基準を定める必要がある。加えて、使用するクラウドサービスを当該区画に加えた場合、そのクラウドサービスが基準を満たしていることを確認する必要がある。
4.1.1(1)	第4部 外部委託	4.1 外部委託	4.1.1 外部委託	(1) 外部委託に係る規定の整備	(a) 統括情報セキュリティ責任者は、外部委託に係る以下の内容を含む規定を整備すること。 (ア) 外部委託を認める情報システムの範囲並びに委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準 (イ) 委託先の選定基準	【 基本対策事項 】規定なし	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格（具体的には付属文書 A の項 6.2 および 10.2）で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求することが明示されている。	公開文書	文献[01]「CO-03: コンプライアンス - サード パーティの監査」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、外部委託に係る規定の整備を適切に行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
4.1.1(2)				(2) 外部委託に係る契約	(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。 (ア) 委託先に提供する情報の委託先における目的外利用の禁止 (イ) 委託先における情報セキュリティ対策の実施内容及び管理体制 (ウ) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制 (エ) 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供 (オ) 情報セキュリティインシデントへの対処方法 (カ) 情報セキュリティ対策その他の契約の履行状況の確認方法 (キ) 情報セキュリティ対策の履行が不十分な場合の対処方法	4.1.1(2)-1 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、以下の内容を含む委託先における情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書等を提出させること。また、変更があった場合は、速やかに再提出させること。 a) 当該委託業務に携わる者の特定 b) 当該委託業務に携わる者が実施する具体的な情報セキュリティ対策の内容 4.1.1(2)-2 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先との情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順について委託先と合意し、定められた手順により情報を取り扱うこと。	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.2 および 10.2) で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。 サービス仕様のうち、サービスの根本となる機能に関して「主な機能」として契約書に記載し、その機能を将来的に提供し続けることをお約束しています。サービス仕様の詳細については、継続的にサービス仕様を拡張、追加していくという考えのもと契約事項とはしていませんが、弊社ホームページ上で公開しています。 データ保護管理策については、契約書に記載しています。 マイクロソフトはエンタープライズ向けクラウドサービスの提供にあたって、一部の作業を外部に委託していますが、この委託先が行う作業も含め、クラウドサービス提供に関わる責任は最終的にマイクロソフトにあるものとして、契約書に記載しています。マイクロソフトの責任とみなさない境界線についてはSLA適用除外事項としてSLAに記載しています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求していることが明示されている。 文献[65]、文献[66]およびNDA文書では、主なサービス仕様、データ保護管理策などが規定・明記され、実現に向けた対策が講じられていることを確認した。 また、NDA文書では、外部委託先に対してマイクロソフトの義務を継承させ、マイクロソフトが責任を負うことが明記されていることを確認した。 文献[72]では、サービス仕様の拡張・追加の取り組みが継続的にされていることが明示されている。	要NDA	文献[01]「CO-03: コンプライアンス – サード パーティの監査」 文献[65](OST) 文献[66](SLA) 文献[72]	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、自組織で定めた選定基準等に従って、クラウドサービスを選定する必要がある。
					(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること。 (ア) 情報セキュリティ監査の受入れ (イ) サービスレベルの保証 (c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させること。	-		適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求することが明示されている。 文献[65]、文献[66]およびNDA文書では、主なサービス仕様、データ保護管理策などが規定・明記され、実現に向けた対策が講じられていることを確認した。 また、NDA文書では、外部委託先に対してマイクロソフトの義務を継承させ、マイクロソフトが責任を負うことが明記されていることを確認した。 文献[72]では、サービス仕様の拡張・追加の取り組みが継続的にされていることが明示されている。	要NDA	文献[01]「CO-03: コンプライアンス – サード パーティの監査」 文献[65](OST) 文献[66](SLA) 文献[72]	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、自組織で定めた選定基準等に従って、クラウドサービスを選定する必要がある。
4.1.1(3)				(3) 外部委託における対策の実施	(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。 (b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を行政事務従事者より受けた場合は、当該サービスの利用を中止するなど、必要な措置を講じ、委託先に契約に基づく必要な措置を講じさせること。 (c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託した業務の終了時に、委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。	【 基本対策事項 】規定なし	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.2 および 10.2) で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。 サービス仕様のうち、サービスの根本となる機能に関して「主な機能」として契約書に記載し、その機能を将来的に提供し続けることをお約束しています。サービス仕様の詳細については、継続的にサービス仕様を拡張、追加していくという考えのもと契約事項とはしていませんが、弊社ホームページ上で公開しています。 データ保護管理策については、契約書に記載しています。 マイクロソフトはエンタープライズ向けクラウドサービスの提供にあたって、一部の作業を外部に委託していますが、この委託先が行う作業も含め、クラウドサービス提供に関わる責任は最終的にマイクロソフトにあるものとして、契約書に記載しています。マイクロソフトの責任とみなさない境界線についてはSLA適用除外事項としてSLAに記載しています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求することが明示されている。 文献[65]、文献[66]およびNDA文書では、主なサービス仕様、データ保護管理策などが規定・明記され、実現に向けた対策が講じられていることを確認した。 また、NDA文書では、外部委託先に対してマイクロソフトの義務を継承させ、マイクロソフトが責任を負うことが明記されていることを確認した。 文献[72]では、サービス仕様の拡張・追加の取り組みが継続的にされていることが明示されている。	要NDA	文献[01]「CO-03: コンプライアンス – サード パーティの監査」 文献[65](OST) 文献[66](SLA) 文献[72]	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、使用するクラウドサービスにおける情報セキュリティ対策の実施状況を定期的に確認する必要がある。
4.1.1(4)				(4) 外部委託における情報の取扱い	(a) 行政事務従事者は、委託先への情報の提供等において、以下の事項を遵守すること。 (ア) 委託先に要保護情報を提供する場合、提供する情報を必要最小限とし、あらかじめ定められた安全な受渡し方法により提供すること。 (イ) 提供した要保護情報が委託先において不要になった場合は、これを確実に返却又は抹消させること。 (ウ) 委託業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに情報システムセキュリティ責任者又は課室情報セキュリティ責任者に報告すること。	【 基本対策事項 】規定なし	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.2 および 10.2) で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。 お客様コンテンツは、データの所有者であるお客様利用者と、お客様使用者またはお客様管理者によってアクセス権を付与されたお客様利用者のみがアクセスできるよう、厳密に管理、制御されています。お客様の明示的な指示によってマイクロソフト担当者がお客様コンテンツにアクセスする等ごく稀な場合も含め、お客様コンテンツへのアクセスは記録され、お客様管理者はログを参照することでアクセス履歴を調査することが可能です。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求することが明示されている。 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求することが明示されている。 文献[65]では、マイクロソフトはインシデント発生時にフォレンジックについては対応せず、トレーサビリティ調査に対応できるようログの提供を行っていることを確認した。	公開文書	文献[01]「CO-03: コンプライアンス – サード パーティの監査」 文献[65](OST)	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、使用するクラウドサービス上で要保護情報を取扱う場合は、自組織のユーザに対して、要保護情報の取扱いを適切に実施させる必要がある。 利用者は、インシデント発生時のトレーサビリティをマイクロソフトが提供するログのみで確保できないと判断した場合は、ユーザ自身でログを取得し、トレーサビリティを確保できるようにしておくことが望ましい。
4.1.2(1)			4.1.2 約款による外部サービスの利用	(1) 約款による外部サービスの利用に係る規定の整備	(a) 統括情報セキュリティ責任者は、以下を含む約款による外部サービスの利用に関する規定を整備すること。また、当該サービスの利用において要機密情報が取り扱われないよう規定すること。 (ア) 約款による外部サービスを利用してよい業務の範囲 (イ) 業務に利用する約款による外部サービス	-	（外部サービスの利用の可否は利用者側の判断のため対象外）	対象外	―	―	―	―	―	―	利用者は、約款による外部サービスの利用に係る規定を整備する必要がある。
					(ウ) 利用手続及び運用手順 (b) 情報セキュリティ責任者は、約款による外部サービスを利用する場合は、利用するサービスごとの責任者を定めること。	4.1.2(1)-1 統括情報セキュリティ責任者は、府省庁において約款による外部サービスを業務に利用する場合は、以下を例に利用手続及び運用手順を定めること。 a) 利用申請の許可権限者 b) 利用申請時の申請内容 ・利用する組織名 ・利用するサービス ・利用目的（業務内容） ・利用期間 ・利用責任者（利用アカウントの責任者） c) サービス利用中の安全管理に係る運用手順 ・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認 ・情報の滅失、破壊等に備えたバックアップの取得 ・利用者への定期的な注意喚起（禁止されている要機密情報の取扱いの有無の確認等） d) 情報セキュリティインシデント発生時の連絡体制		対象外	―	―	―	―	―	―	利用者は、約款による外部サービスの利用に係る規定を整備する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
4.1.2(2)				(2) 約款による外部サービスの利用における対策の実施	(a) 行政事務従事者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用すること。	【 基本対策事項 】規定なし	（外部サービスの利用の可否は利用者側の判断のため対象外）	対象外	–	–	–	–	–	–	利用者は、約款による外部サービスの利用に係る規定を整備する必要がある。
4.1.3(1)			4.1.3 ソーシャルメディアサービスによる情報発信	(1) ソーシャルメディアサービスによる情報発信時の対策	(a) 統括情報セキュリティ責任者は、府省庁が管理するアカウントでソーシャルメディアサービスを利用することを前提として、以下を含む情報セキュリティ対策に関する運用手順等を定めること。 (ア) 府省庁のアカウントによる情報発信が実際の府省庁のものであると明らかとするために、アカウントの運用組織を明示するなどの方法でなりすましへの対策を講ずること。 (イ) パスワード等の主体認証情報を適切に管理するなどの方法で不正アクセスへの対策を講ずること。	4.1.3(1)-1 統括情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。 a) アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている府省庁ウェブサイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、その旨をアカウント運用ポリシーに明示する。 b) URL短縮サービスは、利用するソーシャルメディアサービスが自動的にURLを短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。	（ソーシャルメディアサービスの利用は対象外）	対象外	–	–	–	–	–	–	–
						4.1.3(1)-2 統括情報セキュリティ責任者は、府省庁のアカウントによる情報発信が実際の府省庁のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。 a) 府省庁からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、府省庁が運用していることを利用者に明示すること。 b) 府省庁からの情報発信であることを明らかにするために、府省庁が政府ドメイン名を用いて管理しているウェブサイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。 c) 運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている府省庁ウェブサイト上のページのURLを記載すること。 d) ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。	（ソーシャルメディアサービスの利用は対象外）	対象外	–	–	–	–	–	–	–
						4.1.3(1)-3 統括情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。 a) パスワードを適切に管理すること。具体的には、ログインパスワードは十分な長さと複雑さを持たせ、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。 b) 二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。 c) ソーシャルメディアへのログインに利用する端末を紛失したり盗難に遭ったりした場合は、その端末を悪用されてアカウントを乗っ取られる可能性があるため、当該端末の管理を厳重に行うこと。 d) ソーシャルメディアへのログインに利用する端末が不正アクセスされると、その端末が不正に遠隔操作されたり、端末に保存されたパスワードが窃取されたりする可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、適切なセキュリティ対策を実施すること。	（ソーシャルメディアサービスの利用は対象外）	対象外	–	–	–	–	–	–	–
						4.1.3(1)-4 統括情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。 a) 自己管理ウェブサイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。 b) アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織のCSIRTや内閣官房情報セキュリティセンターに報告するなど、適切な対処を行うこと。	（ソーシャルメディアサービスの利用は対象外）	対象外	–	–	–	–	–	–	–
					(b) 情報セキュリティ責任者は、府省庁において情報発信のためにソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めること。 (c) 行政事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、府省庁の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。	-	（ソーシャルメディアサービスの利用は対象外）	対象外	–	–	–	–	–	–	–

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
5.1.1(1)	第5部 情報システムのライフサイクル	5.1 情報システムに係る文書等の整備	5.1.1 情報システムに係る台帳等の整備	(1) 情報システム台帳の整備	(a) 統括情報セキュリティ責任者は、全ての情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳に整備すること。	5.1.1(1)-1 統括情報セキュリティ責任者は、以下の内容を含む台帳を整備すること。 a) 情報システム名 b) 管理課室 c) 当該情報システムセキュリティ責任者の氏名及び連絡先 d) システム構成 e) 接続する府省庁外通信回線の種別 f) 取り扱う情報の格付及び取扱制限に関する事項 g) 当該情報システムの設計・開発、運用・保守に関する事項 また、民間事業者等が提供する情報処理サービスにより情報システムを構築する場合は、以下を含む内容についても台帳として整備すること。 a) 情報処理サービス名 b) 契約事業者 c) 契約期間 d) 情報処理サービスの概要 e) ドメイン名（インターネット上で提供される情報処理サービスを利用する場合） f) 取り扱う情報の格付及び取扱制限に関する事項	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る台帳等を整備する必要がある。
					(b) 情報システムセキュリティ責任者は、情報システムを新規に構築し、又は更改する際には、当該情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告すること。	5.1.1(1)-2 情報システムセキュリティ責任者は、政府情報システム管理データベースの登録対象となるシステムについては、当該データベースに必要な情報を記録すること。		適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る台帳等を整備する必要がある。
5.1.1(2)				(2) 情報システム関連文書の整備	(a) 情報システムセキュリティ責任者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を網羅した情報システム関連文書を整備すること。 (ア) 情報システムを構成するサーバ装置及び端末関連情報	5.1.1(2)-1 情報システムセキュリティ責任者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備すること。 a) サーバ装置及び端末を管理する行政事務従事者及び利用者を特定する情報 b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン c) サーバ装置及び端末の仕様書又は設計書	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る関連文書等を整備する必要がある。
					(イ) 情報システムを構成する通信回線及び通信回線装置関連情報	5.1.1(2)-2 情報システムセキュリティ責任者は、所管する情報システムを構成する通信回線及び通信回線装置関連情報として、以下を含む文書を整備すること。 a) 通信回線及び通信回線装置を管理する行政事務従事者を特定する情報 b) 通信回線装置の機種並びに利用しているソフトウェアの種類及びバージョン c) 通信回線及び通信回線装置の仕様書又は設計書 d) 通信回線の構成 e) 通信回線装置におけるアクセス制御の設定 f) 通信回線を利用する機器等の識別コード、サーバ装置及び端末の利用者と当該利用者の識別コードとの対応 g) 通信回線の利用部門		適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る関連文書等を整備する必要がある。
					(ウ) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順 (エ) 情報セキュリティインシデントを認知した際の対処手順	5.1.1(2)-3 情報システムセキュリティ責任者は、所管する情報システムについて、情報システム構成要素ごとのセキュリティ維持に関する以下を含む手順を定めること。 a) サーバ装置及び端末のセキュリティの維持に関する手順 b) 通信回線を介して提供するサービスのセキュリティの維持に関する手順 c) 通信回線及び通信回線装置のセキュリティの維持に関する手順		適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る関連文書等を整備する必要がある。
5.1.2(1)			5.1.2 機器等の調達に係る規定の整備	(1) 機器等の調達に係る規定の整備	(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を府省庁が確認できることを加えること。	5.1.2(1)-1 統括情報セキュリティ責任者は、機器等の選定基準に、サプライチェーン・リスクを低減するための要件として、以下を例に規定すること。 a) 調達した機器等に不正な変更が見付かったときに、追跡調査や立入検査等、府省庁と調達先が連携して原因を調査・排除できる体制を整備していること。 5.1.2(1)-2 統括情報セキュリティ責任者は、調達する機器等において、設計書の検査によるセキュリティ機能の適切な実装の確認、開発環境の管理体制の検査、脆弱性テスト等、第三者による情報セキュリティ機能の客観的な評価を必要とする場合には、ISO/IEC 15408に基づく認証を取得しているか否かを、調達時の評価項目とすることを機器等の選定基準として定めること。	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る機器等の調達に係る規定等を整備する必要がある。加えて、使用するクラウドサービスが当該規定等を満たしていることを確認する必要がある。
					(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。	5.1.2(1)-3 統括情報セキュリティ責任者は、機器等の納入時の確認・検査手続には以下を含む事項を確認できる手続を定めること。 a) 調達時に指定したセキュリティ要件の実装状況 b) 機器等に不正プログラムが混入していないこと		適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08: 施設のセキュリティ - 資産管理」「DG-01: データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに係る機器等の調達に係る規定等を整備する必要がある。加えて、使用するクラウドサービスが当該規定等を満たしていることを確認する必要がある。
5.2.1(1)	5.2 情報システムのライフサイクルの各段階における対策	5.2.1 情報システムの企画・要件定義	(1) 実施体制の確保	(a) 情報システムセキュリティ責任者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、情報システムを統括する責任者に求めること。 (b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システムを整備し、運用管理する府省庁が定める運用管理規程等に応じた体制の整備を、情報システムを統括する責任者に求めること。	【 基本対策事項 】規定なし	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格（具体的には付属文書 A の項 12.5）で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04: リリース管理 - アウトソース開発」「RM-01: リリース管理 - 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムのライフサイクル全般にわたって、情報セキュリティを維持する体制を確保する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
5.2.1(2)				(2) 情報システムのセキュリティ要件の策定	(a) 情報システムセキュリティ責任者は、情報システムを構築する目的、対象とする業務等の業務要件及び当該情報システムで取り扱われる情報の格付等に基づき、以下の事項を含む情報システムのセキュリティ要件を策定すること。	5.2.1(2)-1 情報システムセキュリティ責任者は、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用し、情報システムが提供する業務及び取り扱う情報、利用環境等を考慮した上で、脅威に対抗するために必要となるセキュリティ要件を適切に決定すること。 5.2.1(2)-2 情報システムセキュリティ責任者は、開発する情報システムが運用される際に想定される脅威の分析結果並びに当該情報システムにおいて取り扱う情報の格付及び取扱制限に応じて、セキュリティ要件を適切に策定し、仕様書等に明記すること。	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を (基盤のレベルにおいても) 十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(ア) 情報システムに組み込む主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等のセキュリティ機能要件	5.2.1(2)-3 情報システムセキュリティ責任者は、開発する情報システムが対抗すべき脅威について、適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、セキュリティ設計仕様書（ST：Security Target）を作成し、ST確認を受けること。		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(イ) 情報システム運用時の監視等の運用管理機能要件	5.2.1(2)-4 情報システムセキュリティ責任者は、情報システム運用時のセキュリティ監視等の運用管理機能要件を明確化し、仕様書等へ適切に反映するために、以下を含む措置を実施すること。116 a) 情報システム運用時に情報セキュリティ確保のために必要となる管理機能を仕様書等に明記すること。 b) 情報セキュリティインシデントの発生を監視する必要があると認めた場合には、監視のために必要な機能について、以下を例とする機能を仕様書等に明記すること。 ・府省庁外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能 ・不正プログラム感染や踏み台に利用されること等による府省庁外への不正な通信を監視する機能 ・府省庁内通信回線への端末の接続を監視する機能 ・端末への外部電磁的記録媒体の挿入を監視する機能 ・サーバ装置等の機器の動作を監視する機能		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(ウ) 情報システムに関連する脆弱性についての対策要件	5.2.1(2)-5 情報システムセキュリティ責任者は、開発する情報システムに関連する脆弱性への対策が実施されるよう、以下を含む対策を仕様書等に明記すること。 a) 既知の脆弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。 b) 開発時に情報システムに脆弱性が混入されることを防ぐためのセキュリティ実装方針。 c) セキュリティ侵害につながる脆弱性が情報システムに存在することが発覚した場合に修正が施されること。		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(b) 情報システムセキュリティ責任者は、国民・企業と政府との間で申請及び届出等のオンライン手続を提供するシステムについて、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」に基づきセキュリティ要件を策定すること。	-		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(c) 情報システムセキュリティ責任者は、機器等を調達する場合には、「IT製品の調達におけるセキュリティ要件リスト」を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定すること。	5.2.1(2)-6 情報システムセキュリティ責任者は、構築する情報システムの構成要素のうち製品として調達する機器等について、当該機器等に存在するセキュリティ上の脅威へ対抗するためのセキュリティ要件を策定するために、以下を含む事項を実施すること。 a) 「IT製品の調達におけるセキュリティ要件リスト」を参照し、リストに掲載されている製品分野の「セキュリティ上の脅威」が自身の運用環境において該当する場合には、「国際標準に基づくセキュリティ要件」と同等以上のセキュリティ要件を調達時のセキュリティ要件とすること。ただし、「IT製品の調達におけるセキュリティ要件リスト」の「セキュリティ上の脅威」に挙げられていない脅威にも対抗する必要がある場合には、必要なセキュリティ要件を策定すること。 b) 「IT製品の調達におけるセキュリティ要件リスト」に掲載されていない製品分野においては、調達する機器等の利用環境において対抗すべき脅威を分析し、必要なセキュリティ要件を策定すること。		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
					(d) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して情報システムを構築する場合は、基盤となる情報システム全体の情報セキュリティ水準を低下させることのないように、基盤となる情報システムの情報セキュリティ対策に関する運用管理規程等に基づいたセキュリティ要件を適切に策定すること。	-		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った設計・開発を行う必要がある。
5.2.1(3)				(3) 情報システムの構築を外部委託する場合の対策	(a) 情報システムセキュリティ責任者は、情報システムの構築を外部委託する場合は、以下の事項を含む委託先に実施させる事項を、調達仕様書に記載するなどして、適切に実施させること。 (ア) 情報システムのセキュリティ要件の適切な実装	-	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.2 および 10.2) で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。 マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を (基盤のレベルにおいても) 十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受け	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求すること、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求することが明示されている。 文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「CO-03：コンプライアンス – サード パーティの監査」 文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	(マイクロソフト社とのNDAにより開示)	―	―	利用者は、使用するクラウドサービスが、自ら定めたセキュリティ要件を満たしていることを確認する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(イ) 情報セキュリティの観点に基づく試験の実施	5.2.1(3)-1 情報システムセキュリティ責任者は、情報セキュリティの観点に基づく試験の実施について、以下を含む事項を実施させること。 a) ソフトウェアの作成及び試験を行う情報システムについては、情報セキュリティの観点から運用中の情報システムに悪影響が及ばないように、運用中の情報システムと分離すること。 b) 情報セキュリティの観点から必要な試験がある場合には、試験項目及び試験方法を定め、これに基づいて試験を実施すること。 c) 情報セキュリティの観点から実施した試験の実施記録を保存すること。	やすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。 システム開発のライフ サイクルの中には、重要なセキュリティの確認および承認のチェックポイントが含まれています。ビジネス上、運用上、および技術上のリスクが特定されます。また、コンプライアンス、セキュリティ、プライバシー、サービスの継続性の各領域がカバーされます。セキュリティ開発ライフサイクルは統合型セキュリティ開発の先駆者として、Microsoft Online Services の中核を構成しています。 詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求すること、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求することが明示されている。 文献[01]では、Microsoft Online Services の運用変更の管理手順に「承認されている非運用環境における変更のテスト」が含まれていること、お客様の非公開データの運用環境から非運用環境への移動またはコピーは、お客様の同意が得られた場合やマイクロソフトの法務部門の指示による場合を除き禁止されていることが明示されている。 文献[10]では、マイクロソフトで採用されている「セキュリティ開発ライフサイクル（SDL）」にて、テスト段階にてコードインスペクションの実施やファジングテストの実施が明示されている。	公開文書	文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[01]「RM-01：リリース管理 - 新規開発/取得」 「DG-06：データ ガバナンス - 非運用データ」 文献[10]	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、使用するクラウドサービスが、自ら定めたセキュリティ要件を満たしていることを確認する必要がある。
					(ウ) 情報システムの開発環境及び開発工程における情報セキュリティ対策	5.2.1(3)-2 情報システムセキュリティ責任者は、開発工程における情報セキュリティ対策として、以下を含む事項を実施させること。 a) ソースコードが不正に変更されることを防ぐために、以下の事項を含むソースコードの管理を適切に行うこと。 ・ソースコードの変更管理 ・ソースコードの閲覧制限のためのアクセス制御 ・ソースコードの滅失、き損等に備えたバックアップの取得 b) 情報システムに関連する脆弱性についての対策要件として定めたセキュリティ実装方針に従うこと。 c) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビュー及びソースコードレビューの範囲及び方法を定め、これに基づいてレビューを実施すること。		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。 文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求すること、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求することが明示されている。	公開文書	文献[01]「RM-04：リリース管理 - アウトソース開発」 「RM-01：リリース管理 - 新規開発/取得」 文献[01]「CO-03：コンプライアンス - サード パーティの監査」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、使用するクラウドサービスが、自ら定めたセキュリティ要件を満たしていることを確認する必要がある。
5.2.1(4)				(4) 情報システムの運用・保守を外部委託する場合の対策	(a) 情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、調達仕様書に記載するなどして、適切に実施させること。	5.2.1(4)-1 情報システムセキュリティ責任者は、情報システムの運用・保守を外部委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるために、以下を含む要件を調達仕様書に記載するなどして、適切に実施させること。 a) 情報システムの運用環境に課せられるべき条件の整備 b) 情報システムのセキュリティ監視を行う場合の監視手順や連絡方法 c) 情報システムの保守における情報セキュリティ対策 d) 運用中の情報システムに脆弱性が存在することが判明した場合の情報セキュリティ対策	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格 (具体的には付属文書 A の項 6.2 および 10.2) で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。 マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求すること、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求することが明示されている。 文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「CO-03：コンプライアンス - サード パーティの監査」 文献[01]「RM-04：リリース管理 - アウトソース開発」 「RM-01：リリース管理 - 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、使用するクラウドサービスが、自ら定めたセキュリティ要件を満たしていることを確認する必要がある。
5.2.2(1)			5.2.2 情報システムの調達・構築	(1) 機器等の選定時の対策	(a) 情報システムセキュリティ責任者は、機器等の選定時において、選定基準に対する機器等の適合性を確認し、その結果を機器等の選定における判断の一要素として活用すること。	【 基本対策事項 】規定なし	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ - 資産管理」 「DG-01：データ ガバナンス - 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムに使用する機器等について、適切に選定する必要がある。
5.2.2(2)				(2) 情報システムの構築時の対策	(a) 情報システムセキュリティ責任者は、情報システムの構築において、情報セキュリティの観点から必要な措置を講ずること。	5.2.2(2)-1 情報システムセキュリティ責任者は、情報システムの構築において以下を含む情報セキュリティ対策を行うこと。 a) 情報システム構築の工程で扱う要保護情報への不正アクセス、滅失、き損等に対処するために開発環境を整備すること。 b) セキュリティ要件が適切に実装されるようにセキュリティ機能を設計すること。 c) 情報システムへの脆弱性の混入を防ぐために定めたセキュリティ実装方針に従うこと。 d) セキュリティ機能が適切に実装されていること及びセキュリティ実装方針に従った実装が行われていることを確認するために、設計レビューやソースコードレビュー等を実施すること。 e) 脆弱性検査を含む情報セキュリティの観点での試験を実施すること。 5.2.2(2)-2 情報システムセキュリティ責任者は、情報システムの運用保守段階へ移行するに当たり、以下を含む情報セキュリティ対策を行うこと。 a) 情報セキュリティに関わる運用保守体制の整備 b) 運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施 c) 情報セキュリティインシデントを認知した際の対処方法の確立	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 - アウトソース開発」 「RM-01：リリース管理 - 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った構築を行う必要がある。
					(b) 情報システムセキュリティ責任者は、構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること。	-		適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 - アウトソース開発」 「RM-01：リリース管理 - 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った構築を行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
5.2.2(3)				(3) 納品検査時の対策	(a) 情報システムセキュリティ責任者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。	【 基本対策事項 】規定なし	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」 「RM-01：リリース管理 – 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、自組織で管理する情報システムのセキュリティ要件を策定し、当該セキュリティ要件に従った構築を行う必要がある。
5.2.3(1)			5.2.3 情報システムの運用・保守	(1) 情報システムの運用・保守時の対策	(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能を適切に運用すること。	5.2.3(1)-1 情報システムセキュリティ責任者は、情報システムのセキュリティ監視を行う場合は、以下の内容を含む監視手順を定め、適切に監視運用すること。 (a) 監視するイベントの種類 (b) 監視体制 (c) 監視状況及び情報セキュリティインシデントを認知した場合の報告手順 (d) 監視運用における情報の取扱い（機密性の確保） 5.2.3(1)-2 情報システムセキュリティ責任者は、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。 5.2.3(1)-3 情報システムセキュリティ責任者は、情報システムにおいて取り扱う情報について、当該情報の格付及び取扱制限が適切に守られていることを確認すること。 5.2.3(1)-4 情報システムセキュリティ責任者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したりや測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、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。
					(b) 情報システムセキュリティ責任者は、基盤となる情報システムを利用して構築された情報システムを運用する場合は、基盤となる情報システムを整備し、運用管理する府省庁との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。 (c) 情報システムセキュリティ責任者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。	-	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 利用者側では、以下のログを取得可能。 Exchange Online 送受信ログ（メッセージの追跡ログ） 指定した期間（24時間、48時間、過去7日、カスタム：30日まで）に 送受信したメールのログを確認可能。(社内、社外) 管理者監査ログ 管理者が Exchange Online 環境で行った変更 (RBAC の役割または Exchange の ポリシーや設定の変更など) を追跡可能。 保持期間は 90 日間。 メールボックス監査ログ メールボックス所有者以外のユーザーからのメールボックスへのアクセス（代理人による アクセス、共有メールボックスへのアクセスなど）を追跡可能。 ログが有効になっているときの保持期間は 90 日間。 SharePoint Online いつ・誰が・どのサイトの・どのアイテムを・どうしたのレベルでのログを出力可能 アイテムの編集 アイテムのチェックインと チェックアウト アイテムの移動またはコピー アイテムの削除または復元 ログ情報の保持期限は 既定で30日間 マイクロソフト運用者によるアクセスには、ワンタイムパスワードあるいは電子証明書による二要素認証を実施しています。 また、特権の利用は記録され、監査されています。	適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、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。
5.2.4(1)			5.2.4 情報システムの更改・廃棄	(1) 情報システムの更改・廃棄時の対策	(a) 情報システムセキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。 (ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策 (イ) 情報システム廃棄時の不要な情報の抹消	【 基本対策事項 】規定なし	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする (分解、切断、粉砕、償却など) 破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 すべての Microsoft Online Services は、承認された記憶域メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格 (具体的には付属文書 A の項 9.2.6 および 10.7.2) で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、すべての Microsoft Online Services が承認された記憶域メディアと廃棄管理サービスを使用していることが明示されている。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。	要NDA	文献[01]「DG-05：データ ガバナンス – 安全な廃棄」	―	―	（マイクロソフト社とのNDAにより開示）	利用者は、クラウドサービス契約終了時のデータ削除処理（一定期間経過後にデータ削除される、等）について理解する必要がある。
5.2.5(1)			5.2.5 情報システムについての対策の見直し	(1) 情報システムについての対策の見直し	(1) 情報システムについての対策の見直し (a) 情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。	【 基本対策事項 】規定なし	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	公開文書	文献[06]	―	―	―	利用者は、自組織が管理する情報システムについての対策の見直しを適切に行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
5.3.1(1)		5.3 情報システムの運用継続	5.3.1 情報システムの運用継続計画の整備・整合的運用の確保	(1) 情報システムの運用継続計画の整備・整合的運用の確保	(a) 統括情報セキュリティ責任者は、府省庁において非常時優先業務を支える情報システムの運用継続計画を整備するに当たり、非常時における情報セキュリティに係る対策事項を検討すること。 (b) 統括情報セキュリティ責任者は、情報システムの運用継続計画の教育訓練や維持改善を行う際等に、非常時における情報セキュリティに係る対策事項が運用可能であるかを確認すること。	【 基本対策事項 】規定なし	Microsoft Online Services では、業界およびマイクロソフトのベスト プラクティスに合致し、すべてのレベルにおいて継続性プログラムを主導するフレームワークを保持しています。 Microsoft Online Services のフレームワークには以下のものが含まれています。 ・主要なリソースの責任の割り当て ・通知、エスカレーション、宣言のプロセス ・回復時間に関する目標、および回復ポイントに関する目標 ・文書化された手順による継続性の計画 ・該当するすべての関係者が継続性の計画を実行できるように準備するためのトレーニング プログラム ・テスト、メンテナンス、および改訂のプロセス ISO 27001 規格 (具体的には付属文書 A の項 14.1) で、"ビジネス継続性管理における情報セキュリティの側面" が規定されています。	適合可能	文献[01]では、Microsoft Online Services の継続性プログラムを主導するフレームワークを保持していることが明示されている。	公開文書	文献[01]「RS-03:復元 - ビジネス継続性の計画」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、障害時・災害時に関係者への連絡先と連絡手順を定めておく必要がある。
6.1.1(1)	第6部 情報システムのセキュリティ要件	6.1 情報システムのセキュリティ機能	6.1.1 主体認証機能	(1) 主体認証機能の導入	(a) 情報システムセキュリティ責任者は、情報システムや情報へのアクセスを管理するため、主体を特定し、それが正当な主体であることを検証する必要がある場合、識別及び主体認証を行う機能を設けること。	6.1.1(1)-1 情報システムセキュリティ責任者は、主体認証は、以下を例とする主体認証方式を決定すること。 a) 知識（パスワード等、利用者本人のみが知り得る情報）による認証 b) 所有（電子証明書を格納するICカード又はワンタイムパスワード生成器等、利用者本人のみが所有する機器等）による認証 c) 生体（指紋や静脈等、本人の生体的な特徴）による認証 6.1.1(1)-2 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、知識による主体認証方式を用いる場合には、以下の機能を設けること。 a) 利用者が自ら主体認証情報を設定する機能や、利用者以外の者が主体認証情報を設定する場合に、利用者へ安全な方法で主体認証情報を割り当てる機能 b) 利用者が主体認証情報としてパスワードを設定する際に、以下の要素を考慮して、セキュリティ上の強度が指定以上となるよう、情報システムに要求する機能 ・パスワードに用いる文字の種類とその組み合わせ ・パスワードの桁数 ・パスワードの有効期間 ・大規模な辞書を用いたパスワード解析への耐性	顧客は所有するIDの不正使用を制限する権利と責任を保持します。Active Directory Federation Serviceを構築する事で、IPアドレスによる、アクセス制御を実装することは可能。またサードパーティ製のアクセスコントロールソリューションとと組み合わせることで、PC端末制御を行うことも可能。 またWindows Azure 多要素認証を組み合わせて利用する事で、多要素認証を実施することも可能。	適合可能	文献[17]では、多要素認証として電話による第2要素が使用できることが明示されている。	公開情報	文献[17]	―	―	―	利用者は、パスワード等の漏えいを防止するため、エンドユーザーに対し注意喚起する必要がある。
					(b) 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置を講ずること。	6.1.1(1)-3 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、利用者に主体認証情報の定期的な変更を求める場合には、利用者に対して定期的な変更を促す機能のほか、以下の機能を設けること。 a) 利用者が定期的に変更しているか否かを確認する機能 b) 利用者が定期的に変更しなければ、情報システムの利用を継続させない機能 6.1.1(1)-4 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報が第三者に対して明らかにならないよう、以下を例とする方法を用いて適切に管理すること。 a) 主体認証情報を送信又は保存する場合には、その内容を暗号化する。 b) 知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう注意を促す。 c) 主体認証情報に対するアクセス制限を設ける。 6.1.1(1)-5 情報システムセキュリティ責任者は、主体認証を行う情報システムにおいて、主体認証情報を他の主体に利用され、又は利用されるおそれを認識した場合に当該主体認証情報を用いた不正アクセスが行われないよう、当該主体認証による情報システムの利用を停止する機能を設けること。		適合可能	文献[01]では、Microsoft Online Services において、Active Directory を使用してパスワード ポリシーの適用状況を管理していること、システムが強制的にユーザーに複雑なパスワードを使用させるように構成されていることが明示されている。	公開文書	文献[01]「SA-02:セキュリティアーキテクチャー - ユーザーID資格情報」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、パスワード等の漏えいを防止するため、エンドユーザーに対し注意喚起する必要がある。
6.1.2(1)			6.1.2 アクセス制御機能	(1) アクセス制御機能の導入	(a) 情報システムセキュリティ責任者は、情報システムが取り扱う情報へのアクセスを、主体によって制御する必要がある場合、当該情報システムにアクセス制御を行う機能を設けること。	-	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11:セキュリティアーキテクチャー - 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。
					(b) 情報システムセキュリティ責任者は、アクセス制御機能の導入に当たり、情報セキュリティの強度や利便性を考慮の上、利用者及び所属するグループの属性に基づくアクセス制御だけでなく、利用時間帯や利用端末ごとの制御等、アクセス制御機能に求める情報セキュリティ上の要件を定めること。	6.1.2(1)-1 情報システムセキュリティ責任者は、以下を例とするアクセス制御機能の要件を定めること。 a) 情報システム利用者やそのグループ属性に基づくアクセス制御 b) 利用時間や利用時間帯によるアクセス制御 c) 同時利用者数によるアクセス制御 d) 同一IDによる複数アクセスの禁止 e) IPアドレスによる端末の制限		適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11:セキュリティアーキテクチャー - 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。
6.1.2(2)				(2) 適正なアクセス制御の実施	(a) 情報システムセキュリティ責任者は、行政事務従事者自らがアクセス制御を行うことができない情報システムについて、当該情報システムに保存されることとなる情報の格付及び取扱制限に従い、適正にアクセス制御を行うこと。	【 基本対策事項 】規定なし	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11:セキュリティアーキテクチャー - 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
6.1.3(1)			6.1.3 権限管理機能	(1) 権限管理機能の導入	(a) 情報システムセキュリティ責任者は、情報システムを利用する主体に対して、主体認証を行う必要がある場合、情報システムの管理を実現するための権限に係る管理の機能を設けること。	6.1.3(1)-1 情報システムセキュリティ責任者は、権限管理を行う情報システムにおいて、以下を含めた機能を導入すること。 a) 最小限の特権機能 b) 内部からの不正操作や誤操作の防止機能	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。
					(b) 情報システムセキュリティ責任者は、情報システムに権限管理機能を導入するに当たり、管理者権限の特権を悪意ある第三者等によって、不正に窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。	-		適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、エンドユーザーに対する各種資源、システムへのアクセス権限の付与、見直し手続きを明確化する必要がある。
6.1.3(2)				(2) 識別コード・主体認証情報の付与管理	(a) 情報システムセキュリティ責任者は、情報システムを利用する主体に対して、全ての識別コード及び主体認証情報を適切に付与し、適切に管理するための措置を講ずること。	6.1.3(2)-1 情報システムセキュリティ責任者は、情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与（発行、更新及び変更を含む。以下この項において同じ。）すること。	Microsoft Online Services では、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしています。ID とアクセスの管理に関連した Microsoft Online Services の主要な制御は、Office 365 および GFS に対する SSAE 16/ISAE 3402監査を通じて、毎年正式に監査されています。さらに、これらの制御は、Microsoft Online Services のポリシーおよび規格に準拠しているかが社内で評価されます。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
						6.1.3(2)-2 情報システムセキュリティ責任者は、識別コード及び知識による主体認証情報を付与された主体に対し、初期設定の主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。		適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
						6.1.3(2)-3 情報システムセキュリティ責任者は、識別コードは、情報システムを利用する主体ごとに個別に付与すること。ただし、情報システムセキュリティ責任者の判断の下、やむを得ず、複数の主体で共用する識別コード（以下「共用識別コード」という。）を付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、共用識別コードの取扱いに関する規定を整備し、その規定に従って利用者に付与すること。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
						6.1.3(2)-4 情報システムセキュリティ責任者は、管理者権限を持つ識別コードを付与する場合は、以下の措置を講ずること。 a) 業務上必要な場合に限定する。 b) 初期設定の識別コードを変更できる場合には、識別コードを初期設定以外のものに変更する。 c) 初期設定の主体認証情報を変更できる場合には、主体認証情報を初期設定以外のものに変更する。 d) ネットワーク経由のログインを制限する。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
						6.1.3(2)-5 情報システムセキュリティ責任者は、主体が情報システムを利用する必要がなくなった場合には、以下の措置を講ずること。 a) 当該主体の識別コードを無効にする。 b) 識別コードを追加又は削除する時に、不要な識別コードの有無を点検する。 c) 主体認証情報の不正な利用を防止するために、当該主体に交付した主体認証情報格納装置を返還させる。	適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	ー	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
						6.1.3(2)-6 情報システムセキュリティ責任者は、業務上の責務と必要性を勘案し、必要最小限の範囲に限ってアクセス権を与えるようにアクセス制御を設定すること。また、人事異動等により、識別コードを追加又は削除する時に、不適切なアクセス制御設定の有無を点検すること。		適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
						6.1.3(2)-7 情報システムセキュリティ責任者は、その他、識別コードの付与に当たっては、以下を例とする措置を講ずること。 a) 単一の情報システムにおいては、行政事務従事者１人に対する単一の識別コードのみの付与 b) 行政事務従事者への識別コードの付与に関する記録及び当該記録を消去する場合の情報セキュリティ責任者からの事前の許可 c) ある主体に付与した識別コードを別の主体に対して付与することの禁止		適合可能	文献[01]では、Microsoft Online Services において、アクセス制御および資格情報管理システムが、Microsoft Online Services のポリシーおよび規格に準拠するように設計され、運用されるようにしていることが明示されている。 NDA文書を確認したところ、アクセス権の設定手続きが適切であることが確認できた。	要NDA	文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、自組織のエンドユーザーに対して、クラウドサービスを利用するためのIDを付与し、そのIDを含めた認証情報を適切に管理させる必要がある。
6.1.4(1)			6.1.4 ログの取得・管理	(1) ログの取得・管理	(a) 情報システムセキュリティ責任者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行う必要がある場合、ログを取得すること。	6.1.4(1)-1 情報システムセキュリティ責任者は、情報システムに含まれる構成要素（サーバ装置・端末等）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。	Office365 のセキュリティを高め、イベント ログ、およびプロセスやレコードの監視において正確で詳しいレポートを作成するために、すべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用しています。可能な場合は、Office365 環境全体で正確な時刻を維持するために、標準化と参照のための中央時間ソースをホスティングする Office365 サーバーの時計がネットワーク タイム プロトコルを通じて同期されます。 ISO 27001 規格（具体的には付属文書 A の項 10.10.6）で、"時刻の同期" が規定されています。詳細については、マイクロソフトが認定を取得し、公開されている ISO 規格を確認することをお勧めします。 マイクロソフトのすべての建物へのアクセスは管理されており、アクセスはカード リーダーによって制限されます（正規の ID バッジをカード リーダーに通します）。また、データ センターへの入室は生体認証によって制限されます。 また、特権の利用は記録され、監査されています。 マイクロソフト データセンターあるはクラウドサービス内でセキュリティインシデントの発生が疑われる場合、マイクロソフトは迅速に真偽を調査し、影響範囲や被害を特定し、関連するお客様に速やかに通知します。このセキュリティインシデント発生時の通知は契約書に記載の事項です。 Microsoft Azure には、情報セキュリティ ポリシーが導入されています。 アクセスの準備、認証、アクセスの承認、アクセス権の削除、および定期的なアクセスの確認を含む、アクセス管理のライフサイクル要件も扱います。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは特定のプロセスを経由したもののみが可能であり、特定のプロセスによって承認を受けた場合、作業の実行に必要となる最少の特権、最少の時間のみ特権が有効化されることになっています。カスタマーデータにアクセスする際に最少権限を使用することは契約書（OST）記載済み。	適合可能	文献[01]では、Microsoft Online Services のすべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用し、可能な場合は、Microsoft Online Services 環境全体で正確な時刻を維持するために、NTP を通じて同期されることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「SA-12：セキュリティアーキテクチャー – 時刻の同期」 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、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。
					(b) 情報システムセキュリティ責任者は、情報システムにおいて、ログとして取得する情報項目、ログの保存期間、要保護情報の観点でのログ情報の取扱方法、及びログが取得できなくなった場合の対処方法等について定め、適切にログを管理すること。	6.1.4(1)-2 情報システムセキュリティ責任者は、以下を例とする、ログとして取得する情報項目を定め、管理すること。 a) 事象の主体（人物又は機器等）を示す識別コード b) 識別コードの発行等の管理記録 c) 利用者による情報システムの操作記録 d) 事象の種類 e) 事象の対象 f) 正確な日付及び時刻 g) 試みられたアクセスに関わる情報 h) 電子メールのヘッダ情報及び送信内容 i) 通信パケットの内容 j) 操作する者、監視する者、保守する者等への通知の内容 6.1.4(1)-3 情報システムセキュリティ責任者は、ログの保存期間を定めること。 6.1.4(1)-4 情報システムセキュリティ責任者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。 6.1.4(1)-5 情報システムセキュリティ責任者は、ログが取得できなくなった場合の対処方法を定めること。		適合可能	文献[01]では、Microsoft Online Services のすべてのサービスでは、一貫した時刻設定基準 (PST、GMT、UTC など) を使用し、可能な場合は、Microsoft Online Services 環境全体で正確な時刻を維持するために、NTP を通じて同期されることが明示されている。 文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「SA-12：セキュリティアーキテクチャー – 時刻の同期」 文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、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。
					(c) 情報システムセキュリティ責任者は、情報システムにおいて、取得したログを定期的に点検又は分析する機能を設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。	6.1.4(1)-6 情報システムセキュリティ責任者は、取得したログを効率的かつ確実に点検及び分析し、その結果を報告するために、以下を例とする、当該作業を支援する機能を導入すること。 a) ログ情報をソフトウェア等により集計し、時系列で表示し、報告書を生成するなどの作業の自動化		適合可能	文献[01]では、ログに対するアクセスがポリシーによって制限されること、定期的に確認されることが明示されている。 文献[17]では、利用者が定めた監査ポリシーによりログが記録でき、またそれらの監査データを表示したり集約してレポートを確認できることが明示されている。 文献[26]では、Office365で利用可能な主な監査レポートが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「SA-14：セキュリティアーキテクチャー – 監査ログ/侵入検出」 文献[17]の「ポリシーの監査と保持」 文献[26]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、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。
6.1.5(1)			6.1.5 暗号・電子署名	(1) 暗号化機能・電子署名機能の導入	(a) 情報システムセキュリティ責任者は、情報システムで取り扱う情報の漏えいや改ざん等を防ぐため、以下の措置を講ずること。 (ア) 要機密情報を取り扱う情報システムについては、暗号化を行う機能の必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。 (イ) 要保全情報を取り扱う情報システムについては、電子署名の付与及び検証を行う機能を設ける必要性の有無を検討し、必要があると認めたときは、当該機能を設けること。	6.1.5(1)-1 情報システムセキュリティ責任者は、暗号化又は電子署名を行う情報システムにおいて、以下を例とする措置を講ずること。 a) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とする。 b) 複数のアルゴリズムを選択することが可能な構成とする。 c) 選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装された製品であって、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれにひも付く主体認証情報等が安全に保護される製品を利用することを前提とするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択する。 d) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納する。 e) 機微な情報のやり取りを行う情報システムを新規に構築する場合は、安全性に実績のある暗号プロトコルを選択し、長期的な秘匿性を保証する観点を考慮する。	Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルは暗号化されて保存されています。 業界標準のトランスポート層セキュリティ（TLS）/SSL（Secure Sockets Layer）を使用して暗号化されます。TLS/SSL の使用により、クライアントとサーバー間に極めて安全な接続が確立され、デスクトップとデータ センター間でデータの機密性と整合性が確保されます。 Office 365ではOutlook、Outlook on the Web（OWA）、EASクライアントにおいてS/MIME によるお客様暗号鍵を使った暗号化、電子署名を行うことが可能です。	適合可能	文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。 文献[17]では、電子メールの利用時にS/MIMEによる利用者の暗号鍵を使った暗号化、電子署名が利用可能であることが明示されている。	公開情報	文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利用した保存データの高度な暗号化」 文献[05] 文献[17]	―	―	―	利用者は、Exchange Online上の電子メールメッセージや、SharePoint Online上のファイルについて、個別に暗号化や電子署名を施す必要があれば、利用者側の責任の下、適切に実施する必要がある。 利用者は、自組織のエンドユーザが端末にダウンロードしたファイル等については、端末側の暗号化機能などを用いて対策を講じる必要がある。 利用者は、自組織のエンドユーザが使用する端末や周辺機器に格納される一時データなどを適切に管理する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(b) 情報システムセキュリティ責任者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システムで使用する暗号及び電子署名のアルゴリズム及び運用方法について、以下の事項を含めて定めること。 (ア) 行政事務従事者が暗号化及び電子署名に対して使用するアルゴリズムについて、「電子政府推奨暗号リスト」に記載された暗号化及び電子署名のアルゴリズムが使用可能な場合には、それを使用させること。 (イ) 情報システムの新規構築又は更新に伴い、暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、「電子政府推奨暗号リスト」に記載されたアルゴリズムを採用すること。 (ウ) 暗号化及び電子署名に使用するアルゴリズムが危殆化した場合を想定した緊急対応手順を定めること。 (エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。 (c) 情報システムセキュリティ責任者は、府省庁における暗号化及び電子署名のアルゴリズム及び運用方法に、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な電子証明書を政府認証基盤（GPKI）が発行している場合は、それを使用するように定めること。	-		適合可能	文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 文献[05]では、保存されているデータの暗号化において、AES-256 を含めた暗号化機能が選択できることが明示されている。 文献[17]では、電子メールの利用時にS/MIMEによる利用者の暗号鍵を使った暗号化、電子署名が利用可能であることが明示されている。	公開情報	文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利した保存データの高度な暗号化」 文献[05] 文献[17]	—	—	—	利用者は、Exchange Online上の電子メールメッセージや、SharePoint Online上のファイルについて、個別に暗号化や電子署名を施す必要があれば、利用者側の責任の下、適切に実施する必要がある。 利用者は、自組織のエンドユーザが端末にダウンロードしたファイル等については、端末側の暗号化機能などを用いて対策を講じる必要がある。 利用者は、自組織のエンドユーザが使用する端末や周辺機器に格納される一時データなどを適切に管理する必要がある。
6.1.5(2)				(2) 暗号化・電子署名に係る管理	(a) 情報システムセキュリティ責任者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること。 (ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全な方法で提供すること。	6.1.5(2)-1 情報システムセキュリティ責任者は、署名検証者が、電子署名の正当性を容易に検証するための情報を入手できるよう、以下を例とする方法により、当該情報の提供を可能とすること。 a) 信頼できる機関による電子証明書の提供 b) 府省庁の窓口での電子証明書の提供	Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルは暗号化されて保存されています。 Office 365ではOutlook、Outlook on the Web（OWA）、EASクライアントにおいてS/MIME によるお客様暗号鍵を使った暗号化、電子署名を行うことが可能です。 暗号方式についてはマイクロソフト全体のセキュリティ等活を行う部門が使用を中止すべき方式を決定し、その決定を受けてOffice 365側での設定を変更します。 暗号化技術に特化した情報提供サイトを公開しております。 [参考情報] Microsoft Trust Center https://www.microsoft.com/en-us/TrustCenter/Security/Encryption ゼロデイ脆弱性が、攻撃によって脆弱性が判明するような場合、セキュリティインシデントレスポンスの一環として必要な防止策を検討・実施することとしています。また、攻撃が生じる前の未公開の脆弱性については、深刻度や対策がオンラインサービスに与える影響などを判断の上、対策を実施することとしています。SSL3.0 の Hearblead 脆弱性に対応してSSL3.0 の利用を停止したのが実際の例です。 https://community.office365.com/ja-jp/b/office_365_buzz/archive/2014/10/30/protecting-you-against-the-ssl-3-0-vulnerability	適合可能	文献[17]では、電子メールの利用時にS/MIMEによる利用者の暗号鍵を使った暗号化、電子署名が利用可能であることが明示されている。	公開情報	文献[17]	—	—	—	利用者は、Exchange Online上の電子メールメッセージや、SharePoint Online上のファイルについて、個別に暗号化や電子署名を施す必要があれば、利用者側の責任の下、適切に実施する必要がある。
					(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズムの危殆化に関する情報を定期的に入手し、必要に応じて、行政事務従事者と共有を図ること。	-		適合可能	文献[109]では、Office365で使用される暗号化方式とともに、脆弱性を持つために使用を中止した暗号化方式が明示されている。	公開情報	文献[109]	—	—	—	利用者は、Exchange Online上の電子メールメッセージや、SharePoint Online上のファイルについて、個別に暗号化や電子署名を施す必要があれば、利用者側の責任の下、適切に実施する必要がある。
6.2.1(1)		6.2 情報セキュリティの脅威への対策	6.2.1 ソフトウェアに関する脆弱性対策	(1) ソフトウェアに関する脆弱性対策の実施	(a) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。 (d) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。	6.2.1(1)-1 情報システムセキュリティ責任者は、対象となるソフトウェアの脆弱性に関して、以下を含む情報を適宜入手すること。 a) 脆弱性の原因 158 b) 影響範囲 c) 対策方法 d) 脆弱性を悪用する不正プログラムの流通状況 6.2.1(1)-2 情報システムセキュリティ責任者は、利用するソフトウェアはサポート期間を考慮して選定し、サポート期間を過ぎたソフトウェアは原則として利用しないこと。 6.2.1(1)-3 情報システムセキュリティ責任者は、構成要素ごとにソフトウェアのバージョン等を把握し、脆弱性対策の状況を確認すること。	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター（MSRC）は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 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。 ゼロデイ脆弱性が、攻撃によって脆弱性が判明するような場合、セキュリティインシデントレスポンスの一環として必要な防止策を検討・実施することとしています。また、攻撃が生じる前の未公開の脆弱性については、深刻度や対策がオンラインサービスに与える影響などを判断の上、対策を実施することとしています。SSL3.0 の Hearblead 脆弱性に対応してSSL3.0 の利用を停止したのが実際の例です。 https://community.office365.com/ja-jp/b/office_365_buzz/archive/2014/10/30/protecting-you-against-the-ssl-3-0-vulnerability	適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。 文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	要NDA	文献[01]「IS-20：情報セキュリティ－脆弱性／更新プログラム管理」「IS-31：情報セキュリティ－ネットワーク／インフラストラクチャのサービス」 文献[06]	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、クラウド事業者から提供された脆弱性情報に基づき、適切な対応を行う必要がある。
					(b) 情報システムセキュリティ責任者は、公開された脆弱性の情報がない段階において、サーバ装置、端末及び通信回線装置上で採り得る対策がある場合は、当該対策を実施すること。	-		適合可能	文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。 また、インタビュー等を通じて、ゼロデイ脆弱性に対する対策が行われていることが確認できた。	要NDA	文献[06]	—	（マイクロソフト社とのNDAにより開示）	—	利用者は、クラウド事業者から提供された脆弱性情報に基づき、適切な対応を行う必要がある。
					(c) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。	6.2.1(1)-4 情報システムセキュリティ責任者は、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項について判断すること。 a) 対策の必要性 b) 対策方法 c) 対策方法が存在しない場合の一時的な回避方法 d) 対策方法又は回避方法が情報システムに与える影響 e) 対策の実施予定 f) 対策試験の必要性 g) 対策試験の方法 h) 対策試験の実施予定		適合可能	文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	公開文書	文献[06]	—	—	—	利用者は、クラウド事業者から提供された脆弱性情報に基づき、適切な対応を行う必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
						6.2.1(1)-5 情報システムセキュリティ責任者は、脆弱性対策を実施する場合には、少なくとも以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。 a) 実施日 b) 実施内容 c) 実施者 6.2.1(1)-6 情報システムセキュリティ責任者は、セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイル（以下「対策用ファイル」という。）は、信頼できる方法で入手すること。		適合可能	文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	公開文書	文献[06]	–	–	–	利用者は、クラウド事業者から提供された脆弱性情報に基づき、適切な対応を行う必要がある。
					(d) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用するソフトウェア及び独自に開発するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が講じられていない状態が確認された場合は対処すること。	＜6.2.1(1)(d)関連＞ 6.2.1(1)-7 情報システムセキュリティ責任者は、脆弱性対策の状況を確認する間隔は、可能な範囲で短くすること。		適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。 文献[06]では、マイクロソフトのセキュリティに関する脆弱性は、Microsoft Security Response Centerまたは電子メールを通じて報告できること、マイクロソフトは、標準的な施設から報告された脆弱性やインシデントに対して、一定の手順に従って評価及び対応することが示されている。	公開文書	文献[01]「IS-20：情報セキュリティ－脆弱性／更新プログラム管理」「IS-31：情報セキュリティ－ネットワーク／インフラストラクチャのサービス」 文献[06]	–	–	–	利用者は、クラウド事業者から提供された脆弱性情報に基づき、適切な対応を行う必要がある。
6.2.2(1)			6.2.2 不正プログラム対策	(1) 不正プログラム対策の実施	(a) 情報システムセキュリティ責任者は、サーバ装置及び端末に不正プログラム対策ソフトウェア等を導入すること。ただし、当該サーバ装置及び端末で動作可能な不正プログラム対策ソフトウェア等が存在しない場合を除く。	6.2.2(1)-1 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等及びその定義ファイルは、常に最新のものが利用可能となるよう構成すること。 6.2.2(1)-2 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。 6.2.2(1)-3 情報システムセキュリティ責任者は、不正プログラム対策ソフトウェア等は、定期的に全てのファイルを対象としたスキャンを実施するよう構成すること。	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてウイルスがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、Lockboxプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]では、ウイルス対策ソフトウェアを複数層で実行していることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織のエンドユーザーが使用する端末に対して、不正プログラム対策を適切に実施する必要がある。
					(b) 情報システムセキュリティ責任者は、想定される不正プログラムの感染経路の全てにおいて、不正プログラム対策ソフトウェア等により対策を講ずること。	6.2.2(1)-4 情報システムセキュリティ責任者は、想定される全ての感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。		適合可能	文献[01]では、ウイルス対策ソフトウェアを複数層で実行していることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織のエンドユーザーが使用する端末に対して、不正プログラム対策を適切に実施する必要がある。
					(c) 情報システムセキュリティ責任者は、不正プログラム対策の状況を適宜把握し、必要な対処を行うこと。	6.2.2(1)-5 情報システムセキュリティ責任者は、不正プログラム対策の実施を徹底するため、以下を例とする不正プログラム対策に関する状況を把握し、必要な対処を行うこと。 a) 不正プログラム対策ソフトウェア等の導入状況 b) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況		適合可能	文献[01]では、ウイルス対策ソフトウェアを複数層で実行していることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織のエンドユーザーが使用する端末に対して、不正プログラム対策を適切に実施する必要がある。
6.2.3(1)			6.2.3 サービス不能攻撃対策	(1) サービス不能攻撃対策の実施	(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システム（インターネットからアクセスを受ける情報システムに限る。以下この項において同じ。）については、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。	6.2.3(1)-1 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置について、以下を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。 a) パケットフィルタリング機能 b) 3-way handshake時のタイムアウトの短縮 c) 各種Flood攻撃への防御 d) アプリケーションゲートウェイ機能	Microsoft Online では、インシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発しています。セキュリティ インシデントには以下のものが含まれます（ただしこれらに限りません）。電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動。	適合可能	文献[01]では、ルータによるフィルタリングが行われていることが明示されている。 文献[17]では、利用者による過剰な通信や、DoS攻撃などを監視し、トラフィック調整が行われることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[17]の「サービス拒否攻撃を防ぐためのトラフィック調整」 文献[27]	–	–	（マイクロソフト社とのNDAにより開示）	–
					(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。	6.2.3(1)-2 情報システムセキュリティ責任者は、サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断する、又は通信回線の通信量を制限するなどの手段を有する情報システムを構築すること。 6.2.3(1)-3 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置に設けられている機能を有効にするだけではサービス不能攻撃の影響を排除又は低減できない場合には、以下を例とする対策を検討すること。 a) インターネットに接続している通信回線の提供元となる事業者が別途提供する、サービス不能攻撃に係る通信の遮断等の対策 b) サービス不能攻撃の影響を排除又は低減するための専用の対策装置の導入 c) サーバ装置、端末及び通信回線装置及び通信回線の冗長化 6.2.3(1)-4 情報システムセキュリティ責任者は、サービス不能攻撃を受け、サーバ装置、通信回線装置又は通信回線が過負荷状態に陥り利用できない場合を想定し、攻撃への対処を効率的に実施できる手段の確保について検討すること。		適合可能	文献[01]では、ルータによるフィルタリングが行われていることが明示されている。 文献[17]では、利用者による過剰な通信や、DoS攻撃などを監視し、トラフィック調整が行われることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[17]の「サービス拒否攻撃を防ぐためのトラフィック調整」 文献[27]	–	–	（マイクロソフト社とのNDAにより開示）	–

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応							SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(c) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについては、サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。	6.2.3(1)-5 情報システムセキュリティ責任者は、特定した監視対象について、監視方法及び監視記録の保存期間を定めること。 6.2.3(1)-6 情報システムセキュリティ責任者は、監視対象の監視記録を保存すること。		適合可能	文献[01]では、ルータによるフィルタリングが行われていることが明示されている。 文献[17]では、利用者による過剰な通信や、DoS攻撃などを監視し、トラフィック調整が行われることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[17]の「サービス拒否攻撃を防ぐためのトラフィック調整」 文献[27]	－	－	（マイクロソフト社とのNDAにより開示）	－
6.2.4(1)			6.2.4 標的型攻撃対策	(1) 標的型攻撃対策の実施	(a) 情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。	6.2.4(1)-1 情報システムセキュリティ責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下を例とする対策を行うこと。 a) 不要なサービスについて機能を削除又は停止する。 b) 不審なプログラムが実行されないよう設定する。 c) パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。 6.2.4(1)-2 情報システムセキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を利用した、組織内部への侵入を低減するため、以下を例とする対策を行うこと。 a) 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定しておく。 b) 外部電磁的記録媒体をサーバ装置及び端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。 c) サーバ装置及び端末について、自動再生（オートラン）機能を無効化する。 d) サーバ装置及び端末について、外部電磁的記録媒体内にあるプログラムを一律に実行拒否する設定とする。 e) サーバ装置及び端末について、使用を想定しないUSBポートを無効化する。 f) 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。	Microsoft Online では、インシデントが発生した場合、そのインシデントに対して組織的に対応するための強力なプロセスを開発しています。セキュリティ インシデントには以下のものが含まれます (ただしこれらに限りません)。電子メール ウイルス、マルウェア、ワーム、サービス拒否攻撃、不正アクセス、および Microsoft Online コンピューター ネットワークまたはデータ処理機器に対する他の種類の権限のない活動または不正な活動。	適合可能	文献[01]では、ルータによるフィルタリングが行われていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[27]	－	－	（マイクロソフト社とのNDAにより開示）	利用者は、自組織に対する標的型攻撃への対策を講ずる必要がある。
					(b) 情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。	6.2.4(1)-3 情報システムセキュリティ責任者は、情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについて、以下を例とする対策を行うこと。 a) 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。 b) 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。 6.2.4(1)-4 情報システムセキュリティ責任者は、端末の管理者権限アカウントについて、以下を例とする対策を行うこと。 a) 不要な管理者権限アカウントを削除する。 b) 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。 6.2.4(1)-5 情報システムセキュリティ責任者は、重点的に守るべき業務・情報を取り扱う情報システムについては、高度サイバー攻撃対処のためのリスク評価等のガイドラインに従って、対策を講ずること。		適合可能	文献[01]では、ルータによるフィルタリングが行われていることが明示されている。 文献[27]では、セキュリティインシデント対応の一環として、多層防御を行っている各階層にて監視を行い、不正アクセスを検知する仕組みがあることが明示されている。 NDA文書を確認したところ、CSIRTに相当するインシデントレスポンスチームが組織され、年に一度訓練が実施されていることが確認できた。	要NDA	文献[01]「SA-09：セキュリティアーキテクチャー－分離」 文献[27]	－	－	（マイクロソフト社とのNDAにより開示）	利用者は、自組織に対する標的型攻撃への対策を講ずる必要がある。
6.3.1(1)		6.3 アプリケーション・コンテンツの作成・提供	6.3.1 アプリケーション・コンテンツの作成時の対策	(1) アプリケーション・コンテンツの作成に係る規定の整備	(a) 統括情報セキュリティ責任者は、アプリケーション・コンテンツの提供時に府省庁外の情報セキュリティ水準の低下を招く行為を防止するための規定を整備すること。	【 基本対策事項 】規定なし	（行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外）	対象外	－	－	－	－	－	－	－
6.3.1(2)				(2) アプリケーション・コンテンツのセキュリティ要件の策定	(2) アプリケーション・コンテンツのセキュリティ要件の策定 (a) 情報システムセキュリティ責任者は、府省庁外の情報システム利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション・コンテンツについて以下の内容を仕様に含めること。 (ア) 提供するアプリケーション・コンテンツが不正プログラムを含まないこと。	6.3.1(2)-1 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツが不正プログラムを含まないことを確認するために、以下を含む対策を行うこと。 a) アプリケーション・コンテンツを提供する前に、不正プログラム対策ソフトウェアを用いてスキャンを行い、不正プログラムが含まれていないことを確認すること。 b) 外部委託により作成したアプリケーションプログラムを提供する場合には、委託先事業者に、当該アプリケーションの仕様に反するプログラムコードが含まれていないことを確認させること。	（行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外）	対象外	－	－	－	－	－	－	－
					(イ) 提供するアプリケーションが脆弱性を含まないこと。 (ウ) 実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。	－	（行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外）	対象外	－	－	－	－	－	－	－
					(エ) 電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。	6.3.1(2)-4 情報システムセキュリティ責任者は、文書ファイル等のコンテンツの提供において、当該コンテンツが改ざん等なく真正なものであることを確認できる手段がない場合は、「https://」で始まるURLのウェブページから当該コンテンツをダウンロードできるように提供すること。 6.3.1(2)-5 情報システムセキュリティ責任者は、改ざん等がなく真正なものであることを確認できる手段の提供として電子証明書を用いた署名を用いるとき、政府認証基盤（GPKI）の利用が可能である場合は、政府認証基盤により発行された電子証明書を用いて署名を施すこと。	（行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外）	対象外	－	－	－	－	－	－	－
					(オ) 提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのOSやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、OSやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。	－	（行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外）	対象外	－	－	－	－	－	－	－

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(力) サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。	6.3.1(2)-2 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツにおいて、府省庁外のウェブサイト等のサーバへ自動的にアクセスが発生する機能が仕様に反して組み込まれていないことを、HTMLソースを表示させるなどして確認すること。必要があって当該機能を含める場合は、当該府省庁外へのアクセスが情報セキュリティ上安全なものであることを確認すること。 6.3.1(2)-3 情報システムセキュリティ責任者は、提供するアプリケーション・コンテンツに、本来のサービス提供に必要のない府省庁外へのアクセスを自動的に発生させる機能を含めないこと。	(行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外)	対象外	–	–	–	–	–	–	–
					(b) 行政事務従事者は、アプリケーション・コンテンツの開発・作成を外部委託する場合において、前号に掲げる内容を調達仕様に含めること。	–	(行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外)	対象外	–	–	–	–	–	–	–
6.3.2(1)			6.3.2 アプリケーション・コンテンツ提供時の対策	(1) 政府ドメイン名の使用	(a) 情報システムセキュリティ責任者は、府省庁外向けに提供するウェブサイト等が実際の府省庁提供のものであることを利用者が確認できるように、go.jpで終わるドメイン名（以下「政府ドメイン名」という。）を情報システムにおいて使用するよう仕様に含めること。ただし、4.1.3項に掲げる場合を除く。 (b) 行政事務従事者は、府省庁外向けに提供するウェブサイト等の作成を外部委託する場合においては、前号と同様、政府ドメイン名を使用するよう調達仕様に含めること。	【 基本対策事項 】規定なし	(行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外)	対象外	–	–	–	–	–	–	–
6.3.2(2)				(2) 不正なウェブサイトへの誘導防止	(a) 情報システムセキュリティ責任者は、利用者が検索サイト等を経由して府省庁のウェブサイトになりすました不正なウェブサイトへ誘導されないよう対策を講ずること。	6.3.2(2)-1 情報システムセキュリティ責任者は、府省庁外向けに提供するウェブサイトに対して、以下を例とする検索エンジン最適化措置（SEO対策）を講ずること。 a) クローラからのアクセスを排除しない。 b) cookie機能を無効に設定したブラウザでも正常に閲覧可能とする。 c) 適切なタイトルを設定する。 d) 不適切な誘導を行わない。 6.3.2(2)-2 情報システムセキュリティ責任者は、府省庁外向けに提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、検索結果に不審なサイトが存在した場合は、速やかにその検索サイト事業者へ報告するとともに、不審なサイトへのアクセスを防止するための対策を講ずること。	(行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外)	対象外	–	–	–	–	–	–	–
6.3.2(3)				(3) 府省庁外のアプリケーション・コンテンツの告知	(a) 行政事務従事者は、府省庁外の者が提供するアプリケーション・コンテンツを告知する場合は、以下の対策を講ずること。 (ア) 告知するアプリケーション・コンテンツを管理する組織名を明記する。 (イ) 告知するアプリケーション・コンテンツの所在場所の有効性（リンク先のURLのドメイン名の有効期限等）を確認した時期又は有効性を保証する期間について明記する。 (ウ) 電子メールの送信により告知する場合には、告知内容についての問合わせ先として政府ドメイン名による電子メールアドレスを明記するか又は告知する電子メールに政府ドメイン名による電子署名を付与する。	【 基本対策事項 】規定なし	(行政サービスのためのアプリケーション・コンテンツの作成・提供は対象外)	対象外	–	–	–	–	–	–	–
7.1.1(1)	第7部 情報システムの構成要素	7.1 端末・サーバ装置等	7.1.1 端末	(1) 端末の導入時の対策	(a) 情報システムセキュリティ責任者は、要保護情報を取り扱う端末について、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	7.1.1(1)-1 情報システムセキュリティ責任者は、モバイル端末を除く端末について、原則としてクラス2以上の要管理対策区域に設置すること。 7.1.1(1)-2 情報システムセキュリティ責任者は、端末の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 a) モバイル端末を除く端末を、容易に切断できないセキュリティワイヤを用いて固定物又は搬出が困難な物体に固定する。 b) モバイル端末を保管するための設備（利用者が施錠できる袖机やキャビネット等）を用意する。 7.1.1(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。 a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。 b) 要管理対策区域外で使用するモバイル端末に対して、盗み見されるおそれがある場合にのぞき見防止フィルタを取り付ける。	(端末についてはお客様実施事項)	対象外	–	–	–	–	–	–	利用者は、端末導入時にセキュリティ対策を講ずる必要がある。
					(b) 情報システムセキュリティ責任者は、要管理対策区域外で要機密情報を取り扱うモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。	7.1.1(1)-4 情報システムセキュリティ責任者は、第三者により情報窃取されることを防止するために、以下を例とする、端末に保存される情報を暗号化するための機能又は利用者が端末に情報を保存できないようにするための機能を設けること。 a) 端末に、ハードディスク等の電磁的記録媒体全体を暗号化する機能を設ける。 b) 端末に、ファイルを暗号化する機能を設ける。 c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。 d) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。 e) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。 f) ハードディスク等電磁的記録媒体に保存されている情報を遠隔から消去する機能（遠隔データ消去機能）を設ける。	(端末についてはお客様実施事項)	対象外	–	–	–	–	–	–	利用者は、端末導入時にセキュリティ対策を講ずる必要がある。
					(c) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	7.1.1(1)-5 情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 a) ソフトウェアベンダのサポート状況 b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容 c) インストール時に同時にインストールされる他のソフトウェア d) その他、ソフトウェアの利用に伴う情報セキュリティリスク	(端末についてはお客様実施事項)	対象外	–	–	–	–	–	–	利用者は、端末導入時にセキュリティ対策を講ずる必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1.1(2)				(2) 端末の運用時の対策	(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。 (b) 情報システムセキュリティ責任者は、所管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。	【 基本対策事項 】規定なし	（端末についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、端末運用時にセキュリティ対策を講ずる必要がある。
7.1.1(3)				(3) 端末の運用終了時の対策	(a) 情報システムセキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。	【 基本対策事項 】規定なし	（端末についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、端末運用終了時に端末上に情報があれば抹消する必要がある。
7.1.2(1)			7.1.2 サーバ装置	(1) サーバ装置の導入時の対策	(a) 情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置について、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。	7.1.2(1)-1 情報システムセキュリティ責任者は、要保護情報を取り扱うサーバ装置については、クラス2以上の要管理対策区域に設置すること。	お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。	適合可能	インタビューの結果、日本国内では入退室者を識別・記録する出入管理設備が設置されており、入館には事前申請と顔写真入りの身分証明書が必要であることから、不法侵入を防止する措置が講じられていると考えられる。	要NDA	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織が管理する情報システムについて、サーバ装置の導入時には適切な対策を実施する必要がある。
					(b) 情報システムセキュリティ責任者は、障害や過度のアクセス等により サービスが提供できない事態となることを防ぐため、要安定情報を取り扱う情報システムについて、将来の見通しも考慮し、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。	7.1.2(1)-2 情報システムセキュリティ責任者は、サーバ装置の盗難及び不正な持ち出しを防止するために、以下を例とする対策を講ずること。 a) 施錠可能なサーバラックに設置して施錠する。 b) 容易に切断できないセキュリティワイヤを用いて、固定物又は搬出が困難な物体に固定する。 7.1.2(1)-3 情報システムセキュリティ責任者は、第三者による不正操作及び表示用デバイスの盗み見を防止するために、以下を例とする対策を講ずること。 a) 一定時間操作が無いと自動的にスクリーンロックするよう設定する。		適合可能	文献[01]では、運用の継続性と可用性を確保するために、サービス運用環境のセキュリティ、コンプライアンス、およびプライバシーの要件が代替サイトに反映されることが書かれており、本体装置の予備のみならず、代替サイトに切り替わることが示されている。	公開情報	文献[01]の「OP-04：運用管理 – 装置のメンテナンス」	–	–	–	利用者は、自組織が管理する情報システムについて、サーバ装置の導入時には適切な対策を実施する必要がある。
					(c) 情報システムセキュリティ責任者は、多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。	7.1.2(1)-5 情報システムセキュリティ責任者は、以下を考慮した上で、利用を認めるソフトウェア及び利用を禁止するソフトウェアをバージョンも含め定めること。 a) ソフトウェアベンダのサポート状況 b) ソフトウェアが行う外部との通信の有無及び通信する場合はその通信内容 c) インストール時に同時にインストールされる他のソフトウェア d) その他、ソフトウェアの利用に伴う情報セキュリティリスク	（利用者によるソフトウェアの追加による利用は対象外）	対象外	–	–	–	–	–	–	利用者は、自組織が管理する情報システムについて、サーバ装置の導入時には適切な対策を実施する必要がある。
					(d) 情報システムセキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う際に送受信される情報が漏えいすることを防止するための対策を講ずること。	–	改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 Office 365で、利用者・管理者のクライアント機器とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	公開文書	文献[01]「SA-07：セキュリティアーキテクチャー – リモートユーザーの多要素認証」 文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	–	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する責任を負う。
7.1.2(2)				(2) サーバ装置の運用時の対策	(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。	–	（利用者によるソフトウェアの追加による利用は対象外）	対象外							利用者は、自組織が管理する情報システムについて、サーバ装置の運用時には適切な対策を実施する必要がある。
					(b) 情報システムセキュリティ責任者は、所管する範囲のサーバ装置の構成やソフトウェアの状態を定期的に確認し、不適切な状態にあるサーバ装置を検出等した場合には改善を図ること。	7.1.2(2)-1 情報システムセキュリティ責任者は、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。	Microsoft Online Services では、その提供に使用される資産に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装しています。Microsoft Online Services 環境の主要な資産の一覧は保持されています。資産の所有者は、資産一覧の中でその資産の情報（所有者または関連する代理人、場所、セキュリティ分類など）が最新であるように保守する責任を担います。資産の所有者は、資産保護を規格に応じて分類し、保守する役割も担います。資産の一覧を検証するために、定期的な監査が実施されます。 ISO 27001 規格（具体的には付属文書 A の項 7）で、"資産管理" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、その提供に使用される資産（ハードウェア）に関して記録を残し、その資産の所有者を割り当てるよう求める正式なポリシーを実装していること、また、Microsoft Online Services の提供に使用される資産（資産の定義にはデータとハードウェアを含む）に関して記録を残していることが明示されている。	公開文書	文献[01]「FS-08：施設のセキュリティ – 資産管理」 「DG-01：データ ガバナンス – 所有権/管理者責任」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、自組織が管理する情報システムについて、サーバ装置の運用時には適切な対策を実施する必要がある。
					(c) 情報システムセキュリティ責任者は、サーバ装置上での不正な行為、無許可のアクセス等の意図しない事象の発生を監視する措置を講ずること。ただし、サーバ装置の利用環境等から不要と判断できる場合はこの限りではない。	7.1.2(2)-2 情報システムセキュリティ責任者は、サーバ装置上での不正な行為及び無許可のアクセス等の意図しない事象の発生を監視するために、以下を例とする対策を講ずること。 a) アクセスログ等を定期的に確認する。 b) IDS/IPSを設置する。 c) 不正プログラム対策ソフトウェアを利用する。 d) ファイル完全性チェックツールを利用する。 e) CPU、メモリ、ディスクI/O等のシステム状態を確認する。	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性/侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ – 脆弱性/更新プログラム管理」「IS-31：情報セキュリティ – ネットワーク/インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	–	利用者は、自組織が管理する情報システムについて、サーバ装置の運用時には適切な対策を実施する必要がある。
					(d) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置について、情報のバックアップを取得するなど、サーバ装置を正常な運用状態に復元することが可能になるよう、必要な措置を講ずること。	7.1.2(2)-3 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置については、運用状態を復元するために以下を例とする対策を講ずること。 a) サーバ装置の運用に必要なソフトウェアの原本を別に用意しておく。 b) 定期的なバックアップを実施する。 c) サーバ装置を冗長構成にしている場合には、サービスを提供するサーバ装置を代替サーバ装置に切り替える訓練を実施する。 d) バックアップとして取得した情報からサーバ装置の運用状態を復元するための訓練を実施する。	バックアップの場合、内容がプライマリー データ センターからセカンダリー データ センターにレプリケートされます。このように、レプリケーションは定期的に行われるため、特に決められたバックアップ スケジュールはありません。お客様は、必要に応じて、自社でのデータの抽出およびバックアップの実行を選択できます。お客様のデータは、堅牢なバックアップ、復元、フェールオーバーの各機能を備えた冗長な環境に格納され、可用性、ビジネスの継続性、および迅速な回復を実現します。ローカル ディスクの障害から守るための冗長なディスクから、地理的に分散したデータ センターへの継続的で完全なデータ レプリケーションに至るまで、複数レベルのデータの冗長性が実装されています。Microsoft Online では、年に 1 度、バックアップおよび回復の作業を検証しています。	適合可能	文献[01]では、定期的にプライマリーデータセンターからセカンダリーデータセンターにレプリケートされること、お客様は必要に応じて自社でのデータの抽出およびバックアップの実行を選択できることが明示されている。	公開文書	文献[01]「DG-04：データガバナンス – 保持ポリシー」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、必要に応じて自社でのデータの抽出およびバックアップの実行を選択する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.1.2(3)				(3) サーバ装置の運用終了時の対策	(a) 情報システムセキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。	【 基本対策事項 】規定なし	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハード ドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、償却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。	適合可能	文献[01]では、マイクロソフトはベスト プラクティスの手順とNIST 800-88 準拠の消去ソリューションを使用していること、すべての Microsoft Online Services が承認された記憶域メディアと廃棄管理サービスを使用していることが明示されている。 NDA文書を確認したところ、NIST800-88に準拠した方式でデータ廃棄が行われていることが確認できた。	要NDA	文献[01]「DG-05：データ ガバナンス - 安全な廃棄」	—	—	（マイクロソフト社とのNDAにより開示）	利用者は、自組織が管理する情報システムについて、サーバ装置の運用時には適切な対策を実施する必要がある。
7.1.3(1)			7.1.3 複合機・特定用途機器	(1) 複合機	(a) 情報システムセキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。	7.1.3(1)-1 情報システムセキュリティ責任者は、「IT製品の調達におけるセキュリティ要件リスト」を参照するなどし、複合機が備える機能、設置環境及び取り扱う情報の格付及び取扱制限に応じ、当該複合機に対して想定される脅威を分析した上で、脅威へ対抗するためのセキュリティ要件を調達仕様書に明記すること。	（複合機については対象外）	対象外	—	—	—	—	—	—	—
					(b) 情報システムセキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講ずること。	7.1.3(1)-2 情報システムセキュリティ責任者は、以下を例とする運用中の複合機に対する、情報セキュリティインシデントへの対策を講ずること。 a) 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。 b) 複合機が備える機能のうち利用しない機能を停止する。 c) 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで利用者認証が成功した者のみ印刷が許可される機能等を活用する。 d) 府省庁内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。 e) 複合機をインターネットに直接接続しない。 f) リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。 g) 利用者ごとに許可される操作を適切に設定する。	（複合機については対象外）	対象外	—	—	—	—	—	—	—
					(c) 情報システムセキュリティ責任者は、複合機の運用を終了する際に、複合機の電磁的記録媒体の全ての情報を抹消すること。	7.1.3(1)-3 情報システムセキュリティ責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機については、当該機能を活用することにより複合機内部の情報を抹消すること。当該機能を備えていない複合機については、外部委託先との契約時に外部委託先に複合機内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。	（複合機については対象外）	対象外	—	—	—	—	—	—	—
7.1.3(2)				(2) 特定用途機器	(a) 情報システムセキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じた対策を講ずること。	7.1.3(2)-1 情報システムセキュリティ責任者は、特定用途機器の特性に応じて、以下を例とする対策を講ずること。 a) 特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。 b) 特定用途機器が備える機能のうち利用しない機能を停止する。 c) 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。 d) インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。 e) 特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。	（特定用途機器については対象外）	対象外	—	—	—	—	—	—	—
7.2.1(1)		7.2 電子メール・ウェブ等	7.2.1 電子メール	(1) 電子メールの導入時の対策	(a) 情報システムセキュリティ責任者は、電子メールサーバが電子メールの不正な中継を行わないように設定すること。	-	電子メールの運用ポリシーについては、利用者自身で管理することが出来ます。 Exchange Onlineに関しては、4拠点クラスター構成、自動フェイルオーバを行う機能を提供しております。 また計画メンテナンス時においても、Exchange Online、Exchange Online Archiving (EOA)、および Exchange Online Protection (EOP)ついては、 予定されていたダウンタイムはありません。	適合可能	文献[01]では、以下のようなテクノロジをサポートすることにより、基本機能を拡張できることが明示されている。 ・メッセージのトランスポートルールの構成 ・電子メールデータ漏えい保護製品との統合 また、Microsoft Exchange メールサーバーでは、電子メールのメッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行できることが明示されている。	公開情報	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。
					(b) 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする行政事務従事者の主体認証を行う機能を備えること。 a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するためにSMTP認証等の主体認証機能を導入する。	7.2.1(1)-1 情報システムセキュリティ責任者は、電子メールクライアントから電子メールサーバへの電子メールの受信時及び送信時に、以下を例とする行政事務従事者の主体認証を行う機能を備えること。 a) 電子メールの受信時に限らず、送信時においても不正な利用を排除するためにSMTP認証等の主体認証機能を導入する。		適合可能	文献[01]では、以下のようなテクノロジをサポートすることにより、基本機能を拡張できることが明示されている。 ・メッセージのトランスポートルールの構成 ・電子メールデータ漏えい保護製品との統合 また、Microsoft Exchange メールサーバーでは、電子メールのメッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行できることが明示されている。	公開情報	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。
					(c) 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。	7.2.1(1)-2 情報システムセキュリティ責任者は、以下を例とする電子メールのなりすましの防止策を講ずること。 a) SPF（Sender Policy Framework）、DKIM（DomainKeys Identified Mail）等の送信ドメイン認証技術による送信側の対策を行う。 b) SPF、DKIM等の送信ドメイン認証技術による受信側の対策を行う。 c) S/MIME（Secure/Multipurpose Internet Mail Extensions）等の電子メールにおける電子署名の技術を利用する。		適合可能	文献[01]では、以下のようなテクノロジをサポートすることにより、基本機能を拡張できることが明示されている。 ・メッセージのトランスポートルールの構成 ・電子メールデータ漏えい保護製品との統合 また、Microsoft Exchange メールサーバーでは、電子メールのメッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行できることが明示されている。	公開情報	文献[01]「IS-21：情報セキュリティ－ウイルス／悪意のあるソフトウェアへの対策」	（マイクロソフト社とのNDAにより開示）	—	—	利用者は、電子メールの危険性を考慮し、電子メールの運用方針を明確にする必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.2.2(1)			7.2.2 ウェブ	(1) ウェブサーバの導入・運用時の対策	(a) 情報システムセキュリティ責任者は、ウェブサーバの管理や設定において、以下の事項を含む情報セキュリティ確保のための対策を講ずること。 (ア) ウェブサーバが備える機能のうち、不要な機能を停止又は制限すること。	7.2.2(1)-1 情報システムセキュリティ責任者は、不要な機能の停止又は制限として、以下を例とするウェブサーバの管理や設定を行うこと。 a) CGI機能を用いるスクリプト等は必要最低限のものに限定し、CGI機能を必要としない場合は設定でCGI機能を使用不可とする。 b) ディレクトリインデックスの表示を禁止する。 c) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。 d) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
					(イ) ウェブコンテンツの編集作業を担当する主体を限定すること。	7.2.2(1)-2 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業を担当する主体の限定として、以下を例とするウェブサーバの管理や設定を行うこと。 a) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。 b) OSやアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
					(ウ) 公開してはならない又は無意味なウェブコンテンツが公開されないように管理すること。	7.2.2(1)-3 情報システムセキュリティ責任者は、公開してはならない又は無意味なウェブコンテンツが公開されないよう管理することとして、以下を例とするウェブサーバの管理や設定を行うこと。 a) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。 b) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
					(エ) ウェブコンテンツの編集作業に用いる端末を限定し、識別コード及び主体認証情報を適切に管理すること。	7.2.2(1)-4 情報システムセキュリティ責任者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証情報の適切な管理として、以下を例とするウェブサーバの管理や設定を行うこと。 a) ウェブコンテンツの更新の際は、専用の端末を使用して行う。 b) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元のIPアドレスを必要最小限に制限する。 c) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
					(オ) サービスの利用者の個人に関する情報を通信する場合等、通信時の盗聴等による情報の漏えいを防止する必要がある場合は、暗号化の機能及び電子証明書による認証の機能を設けること。	7.2.2(1)-5 情報システムセキュリティ責任者は、通信時の盗聴による第三者への情報の漏えいの防止及び正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下を例とするウェブサーバの実装を行うこと。 a) SSL（TLS）機能を適切に用いる。 b) SSL（TLS）機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
					(b) 情報システムセキュリティ責任者は、ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認すること。	–	（ウェブサーバについては対象外）	対象外	–	–	–	–	–	–	–
7.2.2(2)				(2) ウェブアプリケーションの開発時・運用時の対策	(a) 情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。また、運用時においても、これらの対策に漏れが無いか定期的に確認し、対策に漏れがある状態が確認された場合は対処を行うこと。	7.2.2(2)-1 情報システムセキュリティ責任者は、以下を含むウェブアプリケーションの脆弱性を排除すること。 a) SQLインジェクション脆弱性 b) OSコマンドインジェクション脆弱性 c) ディレクトリトラバーサル脆弱性 d) セッション管理の脆弱性 e) アクセス制御欠如と認可処理欠如の脆弱性 f) クロスサイトスクリプティング脆弱性 g) クロスサイトリクエストフォージェリ脆弱性 h) クリックジャッキング脆弱性 i) メールヘッダインジェクション脆弱性 j) HTTPヘッダインジェクション脆弱性 k) evalインジェクション脆弱性 l) レースコンディション脆弱性 m) バッファオーバーフロー及び整数オーバーフロー脆弱性	マイクロソフトでは、Office 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用します。セキュリティ開発ライフサイクルは、コミュニケーション サービスやコラボレーション サービスの安全を（基盤のレベルにおいても）十分に確保するうえで役立ちます。セキュリティ開発ライフサイクルは、設計要件の確立 (Establish Design Requirements)、攻撃の分析 (Analyze Attack Surface)、および脅威モデル (Threat Modeling) によって、マイクロソフトがサービス実行中の潜在的な脅威、攻撃を受けやすいサービスの無防備な側面の要素を特定するうえで役立ちます。 設計、開発、または実装の段階で潜在的な脅威が特定された場合、マイクロソフトはサービスを制限したり不要な機能を削除することにより、攻撃の可能性を最小限に抑えることができます。不要な機能を削除した後、設計フェーズで制御機能を十分にテストすることにより、検証フェーズでのこれらの潜在的な脅威を減らします。詳細については、次の URL にアクセスしてください。 http://www.microsoft.com/security/sdl/ ISO 27001 規格 (具体的には付属文書 A の項 12.5) で、"開発におけるセキュリティとサポート プロセス" が規定されています。	適合可能	文献[01]では、マイクロソフトがOffice 365 サービスの設計、開発、および実装にあたって、ソフトウェアのセキュリティ保証プロセスである「セキュリティ開発ライフサイクル」を適用していること、Microsoft Online Services およびシステム変更に関して、運用変更の管理手順が定められていることが明示されている。	公開文書	文献[01]「RM-04：リリース管理 – アウトソース開発」「RM-01：リリース管理 – 新規開発/取得」	（マイクロソフト社とのNDAにより開示）	–	–	–
7.2.3(1)			7.2.3 ドメインネームシステム（DNS）	(1) DNSの導入時の対策	(a) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、名前解決を停止させないための措置を講ずること。	7.2.3(1)-1 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムの名前解決を提供するDNSのコンテンツサーバにおいて、以下を例とする名前解決を停止させないための措置を講ずること。 a) DNSのコンテンツサーバを冗長化する。 b) 通信回線装置等で、DNSのコンテンツサーバへのサービス不能攻撃に備えたアクセス制御を行う。	（DNSについては対象外）	対象外	–	–	–	–	–	–	利用者は、Office365で使用する自組織のドメイン名を管理するDNSを適切に運用する必要がある。
					(b) 情報システムセキュリティ責任者は、DNSのキャッシュサーバにおいて、名前解決の要求への適切な応答をするための措置を講ずること。	7.2.3(1)-2 情報システムセキュリティ責任者は、DNSのキャッシュサーバにおいて、以下を例とする名前解決の要求への適切な応答をするための措置を講ずること。 a) 府省庁外からの名前解決の要求には応じず、府省庁内からの名前解決の要求の 216 みに回答を行うように措置を講ずる。 b) キャッシュサーバの設定、ファイアウォール等でアクセス制御を行う。 c) ルートヒントファイル（DNSルートサーバの情報が登録されたファイル）の更新の有無を定期的（3か月に一度程度）に確認し、最新のDNSルートサーバの情報を維持する。	（DNSについては対象外）	対象外	–	–	–	–	–	–	利用者は、Office365で使用する自組織のドメイン名を管理するDNSを適切に運用する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(c) 情報システムセキュリティ責任者は、DNSのコンテンツサーバにおいて、府省庁のみで使用する名前の解決を提供する場合、当該情報が外部に漏えいしないための措置を講ずること。	7.2.3(1)-3 情報システムセキュリティ責任者は、府省庁内のみで使用する名前の解決を提供するDNSのコンテンツサーバにおいて、以下を例とする当該情報が外部に漏えいしないための措置を講ずること。 a) 内部向けの名前解決を提供するコンテンツサーバを外部向けのコンテンツサーバとは別々に設置し、コンテンツサーバの設定、ファイアウォール等でアクセス制御を行う。	(DNSについては対象外)	対象外	–	–	–	–	–	利用者は、Office365で使用する自組織のドメイン名を管理するDNSを適切に運用する必要がある。
7.2.3(2)				(2) DNSの運用時の対策	(a) 情報システムセキュリティ責任者は、DNSのコンテンツサーバを複数台設置する場合は、管理するドメインに関する情報についてサーバ間で整合性を維持すること。 (b) 情報システムセキュリティ責任者は、DNSのコンテンツサーバにおいて管理するドメインに関する情報が正確であることを定期的に確認すること。	【 基本対策事項 】規定なし	(DNSについては対象外)	対象外	–	–	–	–	–	利用者は、Office365で使用する自組織のドメイン名を管理するDNSを適切に運用する必要がある。
7.3.1(1)		7.3 通信回線	7.3.1 通信回線	(1) 通信回線の導入時の対策	1) 通信回線の導入時の対策 (a) 情報システムセキュリティ責任者は、通信回線構築時に、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じた適切な回線種別を選択し、情報セキュリティインシデントによる影響を回避するために、通信回線に対して必要な対策を講ずること。 (b) 情報システムセキュリティ責任者は、通信回線において、サーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。	7.3.1(1)-1 情報システムセキュリティ責任者は、通信回線を経由した情報セキュリティインシデントの影響範囲を限定的にするため、通信回線の構成、当該通信回線に接続する情報システムにて取り扱う情報の格付及び取扱制限に応じて、以下を例とする通信経路の分離を行うこと。 a) 外部との通信を行うサーバ装置及び通信回線装置のセグメントをDMZとして構築し、内部のセグメントと通信経路を分離する。 b) 業務目的や取り扱う情報の格付及び取扱制限に応じて情報システムごとにVLANにより通信経路を分離し、それぞれの通信制御を適切に行う。 c) 他の情報システムから独立した専用の通信回線を構築する。	Office 365 データ センター内のネットワークは、複数の個別のネットワーク セグメントを作成するように設計されています。このセグメント化により、重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。 修正プログラムは弊社で作成したもので、お客様に提供するパッチと同様、電子署名がつけられたものを使用します。また、社外から入手する際には、信頼できる提供元から入手し、ハッシュ値などの確認を行うこととしています。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	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。
					(c) 情報システムセキュリティ責任者は、要機密情報を取り扱う情報システムを通信回線に接続する際に、通信内容の秘匿性の確保が必要と考える場合は、通信内容の秘匿性を確保するための措置を講ずること。	7.3.1(1)-2 情報システムセキュリティ責任者は、通信経路における盗聴及び情報の改ざん等の脅威への対策として、通信内容の秘匿性を確保するための機能を設けること。通信回線の秘匿性確保の方法として、SSL(TLS)、IPsec等による暗号化を行うこと。また、その際に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。	改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 Office 365で、利用者・管理者のクライアント機器とOffice 365システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、リモート接続するユーザーに対して2要素認証が必要である ことが明示されている。 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	公開文書	文献[01]「SA-07：セキュリティアーキテクチャー – リモートユーザーの多要素認証」 文献[01]「SA-11：セキュリティアーキテクチャー – 共有ネットワーク」	–	–	–	利用者は、自組織のユーザーによるアクセス状況を適切に確認する必要がある。
					(d) 情報システムセキュリティ責任者は、行政事務従事者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること。	7.3.1(1)-3 情報システムセキュリティ責任者は、府省庁内通信回線への接続を許可された情報システムであることを確認し、無許可の情報システムの接続を拒否するための機能として、以下を例とする対策を講ずること。 a) 情報システムの機器番号等により接続機器を識別する。 b) クライアント証明書により接続機器の認証を行う。	Site-to-Site VPN または Point-to-Site VPN を使用して、お客様のサイトとリモート ワーカーから Azure Virtual Network への接続が可能です。パフォーマンスをさらに向上させる場合は、オプションの ExpressRoute プライベート ファイバー リンクを使用して Azure データセンターに接続することで、トラフィックがインターネットに流出するのを防ぐことができます。	適合可能	文献[01]では、アクセス制御としてアクセスポリシー、アクセスの許可、最小限の権限、完全性及び秘密保持、認証、ネットワーク設計が含まれることを確認した。 文献[107]では、必要に応じて相互認証が可能なVPN接続を使用出来ることが明示されている。 また、インタビューにて、インターネットを経由したVPNで接続する場合には、AES-256などの標準的な方式によって暗号化され、証明書によって相互に認証されることが確認できた。	要NDA	文献[01] 文献[107]	–	（マイクロソフト社とのNDAにより開示）	–	利用者は、端末機器の接続について管理する必要がある。
					(e) 情報システムセキュリティ責任者は、通信回線装置を要管理対策区域に設置すること。ただし、要管理対策区域への設置が困難な場合は、物理的な保護措置を講ずるなどして、第三者による破壊や不正な操作等が行われないようにすること。	7.3.1(1)-4 情報システムセキュリティ責任者は、第三者による通信回線及び通信回線装置の破壊、不正操作等への対策として、以下を例とする措置を講ずること。 a) 通信回線装置を施錠可能なラック等に設置する。 b) 庁舎内に敷設した通信ケーブルを物理的に保護する。 c) 通信回線装置の操作ログを取得する。	Office 365 データ センター内のネットワークは、複数の個別のネットワーク セグメントを作成するように設計されています。このセグメント化により、重要なバックエンド サーバーやストレージ デバイスを公開用インターフェイスから物理的に分離できます。インターネットを介して提供されるサービスに対するお客様のアクセスは、ユーザーのインターネット対応ロケーションから開始され、マイクロソフト データ センターで終了します。お客様とマイクロソフト データ センターの間で確立されるこれらの接続は、業界標準の TLS (Transport Layer Security) / SSL (Secure Sockets Layer) を使用して暗号化されます。TLS/SSL の効果的な使用により、ブラウザーとサーバーの極めて安全な接続が確立され、デスクトップとデータ センターの間でデータの機密性や整合性が確保されます。Office 365 サービス ネットワークの終端でルーターをフィルタリングすることにより、Office 365 サービスに対する不正な接続を防ぐためのパケット レベルでのセキュリティが実現されます。 ISO 27001 規格 (具体的には付属文書 A の項 10.6.2) で、"ネットワーク サービスのセキュリティ" が規定されています。 修正プログラムは弊社で作成したもので、お客様に提供するパッチと同様、電子署名がつけられたものを使用します。また、社外から入手する際には、信頼できる提供元から入手し、ハッシュ値などの確認を行うこととしています。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	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。
					(f) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線について、当該通信回線の継続的な運用を可能とするための措置を講ずること。	7.3.1(1)-5 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムが接続される通信回線を構築する場合は、以下を例とする対策を講ずること。 a) 通信回線の性能低下や異常の有無を確認するため、通信回線の利用率、接続率等の運用状態を定常的に確認、分析する機能を設ける。 b) 通信回線及び通信回線装置を冗長構成にする。	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	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。
					(g) 情報システムセキュリティ責任者は、府省庁内通信回線にインターネット回線、公衆通信回線等の府省庁外通信回線を接続する場合には、府省庁内通信回線及び当該府省庁内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること。	7.3.1(1)-6 情報システムセキュリティ責任者は、府省庁内通信回線に、インターネット回線や公衆通信回線等の府省庁外通信回線を接続する場合には、外部からの不正アクセスによる被害を防止するため、以下を例とする対策を講ずること。 a) ファイアウォール、WAF（Web Application Firewall）、リバースプロキシ等により通信制御を行う。 b) 通信回線装置による特定の通信プロトコルの利用を制限する。 c) IDS/IPSにより不正アクセスを検知及び遮断する。	(府省庁内の通信回線は対象外)	適合可能	文献[19]では、Microsoftがオンラインサービスおよびデータへの高速で信頼性の高い接続性を確保するために、2,000以上のネットワークを組み合わせていること、インターネットの障害時に瞬時の再ルーティングを可能にするため多くのプロバイダへの複数のパスを提供することなどが明示されている。	公開文書	文献[19]「Global Network Reliability」	（マイクロソフト社とのNDAにより開示）	–	–	利用者は、回線接続にあたり外部からの不正アクセスを防ぐ対策を講ずる必要がある。
					(h) 情報システムセキュリティ責任者は、府省庁内通信回線と府省庁外通信回線との間で送受信される通信内容を監視するための措置を講ずること。	–	(府省庁内外の通信内容監視は対象外)	対象外	–	–	–	–	–	利用者は、回線接続にあたり自組織内外の通信の監視について検討する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(i) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること。ただし、ソフトウェアを変更することが困難な通信回線装置の場合は、この限りでない。	-	（通信回線装置が動作するためのソフトウェアは対象外）	対象外	—	—	—	—	—	—	—
					(j)情報システムセキュリティ責任者は、保守又は診断のために、遠隔地から通信回線装置に対して行われるリモートアクセスに係る情報セキュリティを確保すること。	7.3.1(1)-7 情報システムセキュリティ責任者は、遠隔地から保守又は診断のためのリモートメンテナンスのセキュリティ確保のために、以下を例とする対策を講ずること。 a) リモートメンテナンス端末の機器番号等の識別コードによりアクセス制御を行う。 b) 主体認証によりアクセス制御する。 c) 通信内容の暗号化により秘匿性を確保する。 d) ファイアウォール等の通信制御のための機器に例外的な設定を行う場合は、その設定により脆弱性が生じないようにする。	Microsoft Online Services では、記述された物理データ センター コントロール、およびポートへの物理的なアクセスを制御するためのサポート手順を通じて、診断ポートおよび構成ポートへの物理的なアクセスを制御します。診断ポートおよび構成ポートへのアクセスは、サービス／資産の所有者と、アクセスを必要としているハードウェア／ソフトウェアのサポート担当者の間の申し合わせによって初めて可能になります。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。 改ざん等の不正行為が起こらぬようマイクロソフトの管理業務は監査されています。監査証跡を参照して、変更の履歴を確認することができます。 Office 365で、利用者・管理者のクライアント機器とOffice 365 システム間の通信は全てTLSまたはSSLによって暗号化されます。 データセンター間での通信についてはTLSにより保護され、改ざんを未然に防止しています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて、物理データ センターコントロール、およびポートへの物理的なアクセスを制御するためのサポート手順を通じて、診断ポートおよび構成ポートへの物理的なアクセスを制御することが明示されている。 文献[01]では、リモート接続するユーザーに対して2要素認証が必要であることが明示されている。 文献[01]によると、利用者端末とOffice 365サービス間の通信はTLSにより暗号化されることが明示されている。	公開文書	文献[01]「IS-30：情報セキュリティ－診断/構成ポートへのアクセス」 文献[01]「SA-07：セキュリティアーキテクチャー－リモートユーザーの多要素認証」 文献[01]「SA-11：セキュリティアーキテクチャー－共有ネットワーク」	（マイクロソフト社とのNDAにより開示）	—	—	—
					(k) 情報システムセキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、当該通信回線サービスの情報セキュリティ水準及びサービスレベルを確保するための措置について、情報システムの構築を委託する事業者と契約時に取り決めておくこと。	-	Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求しています。さらに、Microsoft Online Services は、これらのサード パーティ プロバイダーに対し、年に 1 度第三者機関による監査を受けるか、Microsoft Online Services の年次の第三者機関による監査に参加するように要求しています。 ISO 27001 規格（具体的には付属文書 A の項 6.2 および 10.2）で、"サード パーティとの契約およびサード パーティによるサービス提供の管理におけるセキュリティの対処" が規定されています。	適合可能	文献[01]では、Microsoft Online Services は契約に基づいて、マイクロソフトに対するサード パーティのサービス プロバイダーに、Microsoft Online Services の情報セキュリティ ポリシーで規定された要件を実現し維持するように要求することが明示されている。	公開文書	文献[01]「CO-03：コンプライアンス－サード パーティの監査」	（マイクロソフト社とのNDAにより開示）	—	—	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。
7.3.1(2)				(2) 通信回線の運用時の対策	(a) 情報システムセキュリティ責任者は、情報セキュリティインシデントによる影響を防止するために、通信回線装置の運用時に必要な措置を講ずること。	7.3.1(2)-1 情報システムセキュリティ責任者は、通信回線及び通信回線装置の運用・保守に関わる作業を実施する場合は、情報セキュリティインシデント発生時の調査対応のための作業記録を取得し保管すること。 7.3.1(2)-2 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。	Microsoft Online Services では、環境をスキャンして脆弱性が生じていないかをチェックするためのテクノロジを実装しています。また、脆弱性を特定し、主要な論理制御が適切に行われているかを確認するため、定期的な脆弱性／侵入に関する調査が実施されます。 マイクロソフトのセキュリティ レスポンス センター (MSRC) は、外部のセキュリティ脆弱性の通知サイトを定期的に監視しています。Microsoft Online Services では、定例的な脆弱性管理プロセスの一環として、それらの脆弱性の危険度を評価し、必要に応じてリスクを軽減するためのアクションを Microsoft Online Services 全体で主導します。 権限のないリソースにアクセスを行うプロセスがあった場合、そのプロセス名は監視結果に記録され、アラートが通知されます。	適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ－脆弱性／更新プログラム管理」「IS-31：情報セキュリティ－ネットワーク／インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、使用する通信回線や通信回線装置について、運用時のセキュリティ対策を適切に実施する必要がある。
					(b) 情報システムセキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。 (c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。 (d) 情報システムセキュリティ責任者は、情報システムの情報セキュリティの確保が困難な事由が発生した場合には、当該情報システムが他の情報システムと共有している通信回線について、共有先の他の情報システムを保護するため、当該通信回線とは別に独立した閉鎖的な通信回線に構成を変更すること。	-		適合可能	文献[01]では、Microsoft Online Serviceにおいて、環境をスキャンして脆弱性が生じていないかをチェックしていること、システムのパフォーマンスがしきい値に達したり不測のイベントが発生した場合、監視システムは警告を生成して、運用スタッフがそのしきい値やイベントに対処できるようにしていることが明示されている。 また、インタビュー等を通じて、不正アクセス検知時に必要なアラートやプロセス名などの情報が運用管理者に提供されることが確認できた。	要NDA	文献[01]「IS-20：情報セキュリティ－脆弱性／更新プログラム管理」「IS-31：情報セキュリティ－ネットワーク／インフラストラクチャのサービス」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	—	利用者は、使用する通信回線や通信回線装置について、運用時のセキュリティ対策を適切に実施する必要がある。
7.3.1(3)				(3) 通信回線の運用終了時の対策	(a) 情報システムセキュリティ責任者は、通信回線装置の運用を終了する場合には、当該通信回線を構成する通信回線装置が運用終了後に再利用された時又は廃棄された後に、運用中に保存していた情報が漏えいすることを防止するため、当該通信回線装置の電磁的記録媒体に記録されている全ての情報を抹消するなど適切な措置を講ずること。	【 基本対策事項 】規定なし	マイクロソフトはベスト プラクティスの手順と、NIST 800-88 準拠の消去ソリューションを使用しています。データを消去できないハードドライブの場合は、壊し（つまり切断する）、情報の回復を不可能にする（分解、切断、粉砕、備却など）破壊処理を使用します。廃棄する資産の種類によって適切な処分方法が決まります。破壊の記録は保持されます。 すべての Microsoft Online Services は、承認された記憶域メディアと廃棄管理サービスを使用します。用紙に印刷された文書は、あらかじめ決められた保存期間後に承認された方法で破棄されます。 ISO 27001 規格（具体的には付属文書 A の項 9.2.6 および 10.7.2）で、"機器の安全な処分または再使用とメディアの処分" が規定されています。	適合可能	文献[01]では、Microsoft Online Services において、承認された記憶域メディアと廃棄管理サービスを使用すること、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ることが明示されている。 NDA文書を確認したところ、重要な記録は契約等に基づいて紛失などに備えていることが確認できた。	要NDA	文献[01]「DG-05：データガバナンス－安全な廃棄」	（マイクロソフト社とのNDAにより開示）	—	（マイクロソフト社とのNDAにより開示）	利用者は、使用する通信回線や通信回線装置について、運用時のセキュリティ対策を適切に実施する必要がある。
7.3.1(4)				(4) リモートアクセス環境導入時の対策	(a) 情報システムセキュリティ責任者は、VPN回線を整備する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。	7.3.1(4)-1 情報システムセキュリティ責任者は、VPN回線を整備してリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。 a) 利用開始及び利用停止時の申請手続の整備 b) 通信を行う端末の識別又は認証 c) 利用者の認証 d) 通信内容の暗号化 e) 主体認証ログの取得及び管理 f) リモートアクセスにおいて利用可能な公衆通信網の制限 g) アクセス可能な情報システムの制限 h) リモートアクセス中の他の通信回線との接続禁止	（リモートアクセス環境の導入は対象外）	対象外	—	—	—	—	—	利用者は、リモートアクセスを利用してOffice365を使用する場合は、リモートアクセス環境におけるセキュリティ対策を講ずる必要がある。
					(b) 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること。	7.3.1(4)-2 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、以下を例とする対策を講ずること。 a) 利用開始及び利用停止時の申請手続の整備 b) 利用者の認証又は発信者番号による識別及び認証 c) 主体認証ログの取得及び管理 d) アクセス可能な情報システムの制限 e) リモートアクセス中の他の通信回線との接続禁止	（リモートアクセス環境の導入は対象外）	対象外	—	—	—	—	—	利用者は、リモートアクセスを利用してOffice365を使用する場合は、リモートアクセス環境におけるセキュリティ対策を講ずる必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
7.3.1(5)				(5) 無線LAN環境導入時の対策	(a) 情報システムセキュリティ責任者は、無線LAN技術を利用して府省庁内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずること。	7.3.1(5)-1 情報システムセキュリティ責任者は、無線LAN技術を利用して府省庁内通信回線を構築する場合は、通信回線の構築時共通の対策に加えて、以下を含む措置を講ずること。 a) 無線LAN回線利用申請手続の整備 b) 無線LAN通信の暗号化 c) 通信を行う端末の識別又は認証 d) 利用者の認証 e) 主体認証ログの取得及び管理 f) 無線LAN経由でアクセス可能な情報システムの明確化 g) 無線LANに接続する端末及び通信回線装置の管理 h) 不正プログラム感染を認知した場合の対処手順	（無線LAN環境の導入は対象外）	対象外	―	―	―	―	―	―	利用者は、無線LANを利用してOffice365を使用する場合は、無線LAN環境におけるセキュリティ対策を講ずる必要がある。
7.3.2(1)			7.3.2 IPv6通信回線	(1) IPv6通信を行う情報システムに係る対策	(a) 情報システムセキュリティ責任者は、IPv6技術を利用する通信を行う情報システムを構築する場合は、製品として調達する機器等について、IPv6 Ready Logo Programに基づくPhase-2準拠製品を、可能な場合には選択すること。 (b) 情報システムセキュリティ責任者は、IPv6通信の特性等を踏まえ、IPv6通信を想定して構築する情報システムにおいて、以下の事項を含む脅威又は脆弱性に対する検討を行い、必要な措置を講ずること。 (ア) グローバルIPアドレスによる直接の到達性における脅威 (イ) IPv6通信環境の設定不備等に起因する不正アクセスの脅威 (ウ) IPv4通信とIPv6通信を情報システムにおいて共存させる際の処理考慮漏れに起因する脆弱性の発生 (エ) アプリケーションにおけるIPv6アドレスの取扱い考慮漏れに起因する脆弱性の発生	【 基本対策事項 】規定なし	Office 365 は IPv6 に対応しています。 https://support.office.com/ja-jp/article/Office-365-%25E3%2582%25B5%25E3%2583%25BC%25E3%2583%2593%25E3%2582%25B9%25E3%2581%25A7%25E3%2581%25AE-IPv6-%25E3%2582%25B5%25E3%2583%259D%25E3%2583%25BC%25E3%2583%2588-c08786fb-298e-437c-8222-dab7625fc815?ui=ja-JP&rs=ja-JP&ad=JP	適合可能	文献[110]では、Office365のExchange OnlineおよびSharePoint OnlineがIPv6に対応していることが明示されている。	公開文書	文献[110]	―	―	―	利用者は、自組織が管理する情報システムにおけるIPv6通信について、適切に管理する必要がある。
7.3.2(2)				(2) 意図しないIPv6通信の抑止・監視	(a) 情報システムセキュリティ責任者は、サーバ装置、端末及び通信回線装置を、IPv6通信を想定していない通信回線に接続する場合には、自動トンネリング機能で想定外のIPv6通信パケットが到達する脅威等、当該通信回線から受ける不正なIPv6通信による情報セキュリティ上の脅威を防止するため、IPv6通信を抑止するなどの措置を講ずること。	【 基本対策事項 】規定なし		適合可能	文献[110]では、Office365のExchange OnlineおよびSharePoint OnlineがIPv6に対応していることが明示されている。	公開文書	文献[110]	―	―	―	利用者は、自組織が管理する情報システムにおけるIPv6通信について、適切に管理する必要がある。
8.1.1(1)	第8部 情報システムの利用	8.1 情報システムの利用	8.1.1 情報システムの利用	(1) 情報システムの利用に係る規定の整備	(a) 統括情報セキュリティ責任者は、府省庁の情報システムの利用のうち、情報セキュリティに関する規定を整備すること。	8.1.1(1)-1 統括情報セキュリティ責任者は、府省庁の情報システムの利用のうち、情報セキュリティに関する規定として、以下を例とする実施手順を定めること。 a) 情報システムの基本的な利用のうち、情報セキュリティに関する手順 b) 電子メール及びウェブの利用のうち、情報セキュリティに関する手順 c) 識別コードと主体認証情報の取扱手順 d) 暗号と電子署名の利用に関する手順 e) 不正プログラム感染防止の手順 f) アプリケーション・コンテンツの提供時に府省庁外の情報セキュリティ水準の低下を招く行為の防止に関する手順 g) ドメイン名の使用に関する手順	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて全体的なISMSが設計および実装されていること、情報セキュリティポリシーの文書が規定されていることが明示されている。 さらに文献[03]では、情報セキュリティ ポリシー プログラムを通じて、各ポリシー、標準、およびベースラインが整備される取組みが明示されている。	公開文書	文献[01]「IS-01：情報セキュリティ・管理プログラム」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、情報システムの利用に係る規定を整備する必要がある。
					(b) 統括情報セキュリティ責任者は、要保護情報について要管理対策区域外で情報処理を行う場合を想定し、要管理対策区域外に持ち出した端末や利用した通信回線から情報が漏えいするなどのリスクを踏まえた安全管理措置に関する規定及び許可手続を定めること。	8.1.1(1)-2 統括情報セキュリティ責任者は、要管理対策区域外にて情報処理を行う際の安全管理措置として、以下を例とする措置を規定し、行政事務従事者に遵守させること。 a) モバイル端末で利用する電磁的記録媒体に保存されている要機密情報の暗号化 b) 盗み見に対する対策（のぞき見防止フィルタの利用等） c) 盗難・紛失に対する対策（不要な情報をモバイル端末に保存しない、端末の放置の禁止、利用時以外のシャットダウン及びネットワークの切断、モバイル端末を常時携帯する、常に身近に置き目を離さないなど） d) 利用する場所や時間の限定 e) 端末及び外部電磁的記録媒体等についての盗難・紛失が発生した際の緊急対応手順 8.1.1(1)-3 統括情報セキュリティ責任者は、要管理対策区域外にて行政事務従事者が情報処理を行う際の許可等の手続として、以下を例とする手続を規定し、行政事務従事者に遵守させること。 a) 許可権限者の決定（情報システムセキュリティ責任者又は課室情報セキュリティ責任者が想定される。） b) 利用時の許可申請手続 c) 手続内容（利用者、利用期間、主たる利用場所、目的、利用する情報、端末、通信回線の接続形態等） d) 利用期間満了時の手続 e) 許可権限者による手続内容の記録	標準的な運用手順が、正式に文書化され、Microsoft Online Services の管理者によって承認されています。標準的な運用手順は少なくとも年に 1 度見直されます。 ISO 27001 規格（具体的には付属文書 A の項 10.8.1 および 12.5.4）で、"文書化された運用手順とシステムの文書化のセキュリティ" が規定されています。	適合可能	文献[01]では、Microsoft Online Servicesにおいて全体的なISMSが設計および実装されていること、情報セキュリティポリシーの文書が規定されていることが明示されている。 さらに文献[03]では、情報セキュリティ ポリシー プログラムを通じて、各ポリシー、標準、およびベースラインが整備される取組みが明示されている。	公開文書	文献[01]「IS-01：情報セキュリティ・管理プログラム」 文献[03]「情報セキュリティ ポリシー プログラム」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、情報システムの利用に係る規定を整備する必要がある。
					(c) 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めること。	8.1.1(1)-4 統括情報セキュリティ責任者は、USBメモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順として以下の事項を含めて定めること。 a) 府省庁支給の外部電磁的記録媒体を使用する（私物や出所不明の媒体を使用しない）。 b) 主体認証機能や暗号化機能を備えるセキュアな外部電磁的記録媒体が存在する場合、これに備わる機能を利用する。 c) 要機密情報は保存される必要がなくなった時点で速やかに削除する。 d) 外部電磁的記録媒体を使用する際には、事前に不正プログラム対策ソフトウェアによる検疫・駆除を行う。	可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書（OST）に記載しています。	適合可能	インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	―	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、端末側での取外し可能な媒体の管理のための手順を定める必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.1.1(2)				(2) 情報システム利用者の規定の遵守を支援するための対策	(a) 情報システムセキュリティ責任者は、行政事務従事者による規定の遵守を支援する機能について情報セキュリティリスクと業務効率化の観点から支援する範囲を検討し、当該機能を持つ情報システムを構築すること。	8.1.1(2)-1 情報システムセキュリティ責任者は、府省庁外のウェブサイトについて、行政事務従事者が閲覧できる範囲を制限する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。 a) ウェブサイトフィルタリング機能 b) 事業者が提供するウェブサイトフィルタリングサービスの利用 8.1.1(2)-2 情報システムセキュリティ責任者は、行政事務従事者が不審なメールを受信することによる被害をシステム的に抑止する機能を情報システムに導入すること。具体的には、以下を例とする機能を導入すること。また、当該機能に係る設定や条件について定期的に見直すこと。 a) 受信メールに対するフィルタリング機能 b) 受信メールをテキスト形式で表示する機能 c) スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがないメールクライアントの導入	（ウェブサイトの利用については対象外）	対象外	―	―	―	―	―	―	利用者は、自組織のユーザーによるウェブサイト閲覧やメール利用におけるセキュリティ対策を適切に講ずる必要がある。
8.1.1(3)				(3) 情報システムの利用時の基本的対策	(a) 行政事務従事者は、行政事務の遂行以外の目的で情報システムを利用しないこと。 (b) 行政事務従事者は、情報システムセキュリティ責任者が接続許可を与えた通信回線以外に府省庁の情報システムを接続しないこと。 (c) 行政事務従事者は、府省庁内通信回線に、情報システムセキュリティ責任者の接続許可を受けていない情報システムを接続しないこと。 (d) 行政事務従事者は、情報システムで利用を禁止するソフトウェアを利用しないこと。また、情報システムで利用を認めるソフトウェア以外のソフトウェアを職務上の必要により利用する場合は、情報システムセキュリティ責任者の承認を得ること。	-	マイクロソフトの担当者がサーバー上で実行されるシステムへのアクセス許可を得ることができる方法は限られています。サポート スタッフは、アクセスを求めるサービス チケットの直接の結果として、またはソフトウェアのインストールや問題解決のためのシステム更新の直接の結果として、アクセス権を入手する場合があります。このような場合、監査ログによって、誰がいつログインしたかが示されます。Office 365 が採用しているプロセスは、マイクロソフトが保持している認定に準拠しています。 不正行為、誤使用、またはエラーの可能性を最小限に抑えるため、Microsoft Online Services の環境内の機密度の高い機能や重要な機能に対して、職務の分離が実装されています。 ISO 27001 規格 (具体的には付属文書 A の項 10.1.3) で、"職務の分離" が規定されています。	適合可能	文献[01]では、標準的な運用手順が正式に文書化され、Microsoft Online Service の管理者によって承認されていることが明示されている。 文献[17]では、エンジニアの申請を受けてロックボックスプロセスがアクセス時間とレベル、監視の要否を判断することが明示されている。 NDA文書を確認したところ、規定に則ったオペレーションの手続きが適切であることが確認できた。	要NDA	文献[01]「OP-02: 運用管理・文書化」 文献[17]「組込みのセキュリティ/自動運用」	（マイクロソフト社とのNDAにより開示）	―	（マイクロソフト社とのNDAにより開示）	利用者は、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。
					(e) 行政事務従事者は、情報システムの設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するための措置を講ずること。	8.1.1(3)-1 行政事務従事者は、第三者による不正操作のおそれがある場合は、情報システムを不正操作から保護するために、以下を例とする措置を講ずること。 a) スクリーンロックの設定 b) 利用後のログアウト徹底 c) 利用後に情報システムを鍵付き保管庫等に格納し施錠		適合可能	文献[17]では、Office365ではID基盤に Windows Azure Active Directoryを使用し、様々な認証オプションを用意することで、様々なIDの不正使用防止機能を有することが明示されている。	公開情報	文献[17]の「ユーザーアクセスへの対応」	―	―	―	利用者は、自組織のユーザーが使用する端末に対する不正操作防止対策を適切に講ずる必要がある。
					(f) 行政事務従事者は、要保護情報を取り扱うモバイル端末にて情報処理を行う場合は、定められた安全管理措置を講ずること。 (g) 行政事務従事者は、機密性3情報、要保全情報又は要安定情報を取り扱う情報システムを要管理対策区域外に持ち出す場合には、情報システムセキュリティ責任者又は課室情報セキュリティ責任者の許可を得ること。	-	アクセスは職務によって制限されるため、必要な担当者だけにお客様のアプリケーションやサービスを管理する権限が与えられます。物理的なアクセス権限では、次のような複数の認証とセキュリティのプロセスを利用します。バッジとスマートカード、生体スキャナー（静脈認証）、社内のセキュリティ責任者、継続的なビデオ監視、およびデータ センター環境への物理アクセスの際の 2 要素認証。 データ センター内のさまざまなドアに取り付けられた物理的な入室管理装置に加え、マイクロソフトのデータ センター管理組織では、物理的なアクセスを許可された従業員、契約業者、訪問者のみに限定するための、運用上の手順を導入しています。 ・マイクロソフトのデータ センターへの一時的または永続的なアクセスを付与する権限は、その資格を持つスタッフに限定されます。要求とそれに対応する権限付与の決定は、チケット/アクセス システムによって追跡されます。 ・アクセスを要求する従業員には、身元確認が完了した後にバッジが発行されます。 ・マイクロソフトのデータ センター管理組織は、定期的にアクセス リストの確認を行います。この監査の結果として、確認後に適切な処置が実行されます。 ISO 27001 規格 (具体的には付属文書 A の項 9) で、"物理的なセキュリティおよび環境上のセキュリティ" が規定されています。 データセンタの入館記録は四半期に一回レビューしており、このプロセスはデータセンター SSAE16 の監査対象となっております。 可搬型記憶装置等については通常の運用プロセスでは使用しません。例外的に可搬型記憶装置を使用する場合には、追加の承認プロセスをとることを契約書(OST)に記載しています。	適合可能	文献[01]では、マイクロソフトのデータセンター内の重要なシステムが設置されている部屋は様々なセキュリティメカニズムによって入室を制限することが明示されている。 また、インタビュー等を通じて、危険物や可搬型記録媒体等の持込み物、及び持出し物については、適切に管理されていることが確認できた。 加えて、万が一可搬型記録媒体が機器に差し込まれた時にも、アラートがあがったりデータが暗号化されていることで、情報の持ち出しが困難であることが確認できた。	要NDA	文献[01]「FS-03: 施設のセキュリティ - 管理されたアクセスポイント」	（マイクロソフト社とのNDAにより開示）	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織のユーザーが端末にダウンロードした情報に対するセキュリティ対策を適切に講ずる必要がある。
8.1.1(4)				(4) 電子メール・ウェブの利用時の対策	(a) 行政事務従事者は、要機密情報を含む電子メールを送受信する場合には、それぞれの府省庁が運営し、又は外部委託した電子メールサーバにより提供される電子メールサービスを利用すること。 (b) 行政事務従事者は、府省庁外の者へ電子メールにより情報を送信する場合は、当該電子メールのドメイン名に政府ドメイン名を使用すること。ただし、当該府省庁外の者にとって、当該行政事務従事者が既知の者である場合は除く。 (c) 行政事務従事者は、不審な電子メールを受信した場合には、あらかじめ定められた手順に従い、対処すること。 (d) 行政事務従事者は、ウェブクライアントの設定を見直す必要がある場合は、情報セキュリティに影響を及ぼすおそれのある設定変更を行わないこと。 (e) 行政事務従事者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。 (f) 行政事務従事者は、閲覧しているウェブサイトに表示されるフォームに要機密情報を入力して送信する場合には、以下の事項を確認すること。 (ア) 送信内容が暗号化されること (イ) 当該ウェブサイトが送信先として想定している組織のものであること	【 基本対策事項 】規定なし	（電子メール・ウェブの利用についてはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、電子メール利用時の対策を講ずる必要がある。
8.1.1(5)				(5) 識別コード・主体認証情報の取扱い	(a) 行政事務従事者は、主体認証の際に自己に付与された識別コード以外の識別コードを用いて情報システムを利用しないこと。	-	（主体認証情報の取扱いはお客様実施事項）	対象外	―	―	―	―	―	―	―	利用者は、パスワード等を適切に管理する必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
					(b) 行政事務従事者は、自己に付与された識別コードを適切に管理すること。	8.1.1(5)-1 行政事務従事者は、自己に付与された識別コードを適切に管理するため、以下を含む措置を講ずること。 a) 知る必要のない者に知られるような状態で放置しない。 b) 他者が主体認証に用いるために付与及び貸与しない。 c) 識別コードを利用する必要がなくなった場合は、定められた手続に従い、識別コードの利用を停止する。	（主体認証情報の取扱いはお客様実施事項）	対象外	―	―	―	―	―	利用者は、パスワード等を適切に管理する必要がある。
					(c) 行政事務従事者は、管理者権限を持つ識別コードを付与された場合には、管理者としての業務遂行時に限定して、当該識別コードを利用すること。	-	（主体認証情報の取扱いはお客様実施事項）	対象外	―	―	―	―	―	―	利用者は、パスワード等を適切に管理する必要がある。
					(d) 行政事務従事者は、自己の主体認証情報の管理を徹底すること。	8.1.1(5)-2 行政事務従事者は、知識による主体認証情報を用いる場合には、以下の管理を徹底すること。 a) 自己の主体認証情報を他者に知られないように管理する。 b) 自己の主体認証情報を他者に教えない。 c) 主体認証情報を忘却しないように努める。 d) 主体認証情報を設定するに際しては、容易に推測されないものにする。 e) 異なる識別コードに対して、共通の主体認証情報を用いない。 f) 異なる情報システムにおいて、識別コード及び主体認証情報についての共通の組合せを用いない。(シングルサインオンの場合を除く。) g) 情報システムセキュリティ責任者から主体認証情報を定期的に変更するように指示されている場合は、その指示に従って定期的に変更する。 8.1.1(5)-3 行政事務従事者は、所有による主体認証情報を用いる場合には、以下の管理を徹底すること。 a) 主体認証情報格納装置を本人が意図せずに使われることのないように安全措置を講じて管理する。 b) 主体認証情報格納装置を他者に付与及び貸与しない。 c) 主体認証情報格納装置を紛失しないように管理する。紛失した場合には、定められた報告手続に従い、直ちにその旨を報告する。 d) 主体認証情報格納装置を利用する必要がなくなった場合には、これを情報システムセキュリティ責任者に返還する。	アクセス制御ポリシーはポリシー全体を構成するコンポーネントの 1 つであり、正式な確認および更新のプロセスが適用されます。Microsoft Online Services の資産に対するアクセス権は、ビジネス要件に基づいて、資産の所有者の承認を得たうえで付与されます。加えて、以下の項目が適用されます。 ・資産に対するアクセス権は、知る必要性のある人間に限定する原則、および最小特権の原則に基づいて付与されます。 ・適用可能であれば、役割ベースのアクセス制御を使用して、個人ではなく、特定の職務または責任領域に対して論理的なアクセス権を割り当てます。 ・物理的および論理的なアクセス制御ポリシーは、規格に準拠します。 ISO 27001 規格（具体的には付属文書 A の項 11）で、"アクセス制御" が規定されています。 マイクロソフト管理者のアクセスは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。	適合可能	文献[01]では、Microsoft Online Services において、Active Directory を使用してパスワード ポリシーの適用状況を管理していること、システムが強制的にユーザーに複雑なパスワードを使用させるように構成されていることが明示されている。	公開文書	文献[01]「SA-02：セキュリティアーキテクチャー – ユーザーID資格情報」	（マイクロソフト社とのNDAにより開示）	―	―	利用者は、パスワード等の漏えいを防止するため、エンドユーザーに対し注意喚起する必要がある。
8.1.1(6)				(6) 暗号・電子署名の利用時の対策	(a) 行政事務従事者は、情報を暗号化する場合及び情報に電子署名を付与する場合には、定められたアルゴリズム及び方法に従うこと。 (b) 行政事務従事者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、定められた鍵の管理手順等に従い、これを適切に管理すること。 (c) 行政事務従事者は、暗号化された情報の復号に用いる鍵について、鍵のバックアップ手順に従い、そのバックアップを行うこと。	【 基本対策事項 】規定なし	Office 365上でお客様が使用する電子メールデータやSharePoint Online上のファイルは暗号化されて保存されています。	適合可能	文献[43]では、電子メール保存データが BitLocker ドライブ暗号化を使用して暗号化されていることが明示されている。 文献[44]では、SharePoint OnlineおよびOneDrive for Business が、ファイル単位の暗号化機能を備えていることが明示されている。 また、NDA文書を確認したところ、暗号化キー管理が適切に行われていることが確認できた。	要NDA	文献[43]「保存データの暗号化」 文献[44]「ファイル単位の暗号化を利用した保存データの高度な暗号化」	―	―	（マイクロソフト社とのNDAにより開示）	利用者は、利用者側で暗号化を行う場合は、暗号鍵の取扱手続きなどを適切に定める必要がある。
8.1.1(7)				(7) 不正プログラム感染防止	(a) 行政事務従事者は、不正プログラム感染防止に関する措置に努めること。	8.1.1(7)-1 行政事務従事者は、不正プログラム対策ソフトウェアを活用し、不正プログラム感染を回避するための以下措置に努めること。 a) 不正プログラム対策ソフトウェア等により不正プログラムとして検知された実行ファイルを実行しない。また、データファイルをアプリケーション等で読み込まない。 b) 不正プログラム対策ソフトウェア等に係るアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持する。 c) 不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にする。 d) 不正プログラム対策ソフトウェア等により定期的に全てのファイルに対して、不正プログラムの検査を実施する。 8.1.1(7)-2 行政事務従事者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること。 8.1.1(7)-3 行政事務従事者は、不正プログラムに感染するリスクを低減する情報システムの利用方法として、以下のうち実施可能な措置を講ずること。 a) 不審なウェブサイトを閲覧しない。 b) アプリケーションの利用において、マクロ等の自動実行機能を無効にする。 c) プログラム及びスクリプトの実行機能を無効にする。 d) 安全性が確実でないプログラムをダウンロードしたり実行したりしない。	Microsoft Online Services は、一般的な悪意のあるソフトウェアから確実に保護されるように、ウイルス対策ソフトウェアを複数の層で実行します。たとえば、Microsoft Online の環境内のサーバーでは、アップロードされたファイルやサービスからダウンロードしたファイルをスキャンしてウイルスがないか確認するウイルス対策ソフトウェアを実行しています。さらに、Microsoft Exchange メール サーバーでは、電子メール メッセージをスキャンしてマルウェアがないか確認するための追加のウイルス対策ソフトウェアを実行しています。 保守回線等は外部への連絡用であり、外部から他の機器に対するアクセスを許容するように設定されていません。何らかの手段によって外部から他の機器へのアクセスが可能になってしまった場合でも、システム特権アカウントは無効化されており、Lockboxプロセスを経由した特権アカウントの作成が行われないため、本番環境へのアクセスが可能になることはありません。	適合可能	文献[01]では、ウイルス対策ソフトウェアを複数層で実行していることが明示されている。 また、インタビュー等を通じて、保守作業に必要な特権アカウントはLockboxプロセスにより管理され、一時的に特権が与えられて行われる保守作業が監視されていることが確認できた。	要NDA	文献[01]「IS-21：情報セキュリティ – ウイルス／悪意のあるソフトウェアへの対策」	―	（マイクロソフト社とのNDAにより開示）	―	利用者は、自組織のユーザーが使用する端末に対する不正プログラム感染防止対策を適切に講ずる必要がある。
					(b) 行政事務従事者は、情報システムが不正プログラムに感染したおそれがあることを認識した場合は、感染した情報システムの通信回線への接続を速やかに切断するなど、必要な措置を講ずること。	-	万が一、ウィルスに感染した場合、直ちに駆除ツールを利用して、ウィルスの駆除、隔離を実施	適合可能	文献[01]では、ウイルスなどのインシデント発生時に、組織的なプロセス（特定、封じ込め、根絶、復元、および教訓の学習）により対応することが明示されている。	公開情報	文献[01]「IS-22：情報セキュリティ – インシデント管理」	―	―	―	利用者は、自組織のユーザーが使用する端末に対する不正プログラム感染防止対策を適切に講ずる必要がある。

NISCガイドライン等の評価項目							ガイドラインに対するMicrosoftの見解	Microsoft Azure における対応						SI事業者・利用者で必要な対応
評価項目項番	部	節	項	統一基準の遵守事項	統一基準の遵守事項の内容	ガイドラインの基本対策事項		ガイドラインへの適合性	本調査で確認した内容	確認文書等の開示レベル	確認した公開文書	第三者認証等から類推した内容	MS社へのインタビューで確認した内容	NDAに基づき確認した資料	
8.2.1(1)		8.2 府省庁支給以外の端末の利用	8.2.1 府省庁支給以外の端末の利用	(1) 府省庁支給以外の端末の利用規定の整備・管理	(a) 統括情報セキュリティ責任者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。 (c) 情報セキュリティ責任者は、府省庁支給以外の端末による行政事務に係る情報処理に関する安全管理措置の実施状況を管理する責任者を定めること。	8.2.1(1)-1 統括情報セキュリティ責任者は、以下を例に府省庁支給以外の端末を利用する際の許可等の手続に関する手順を整備し、行政事務従事者に周知すること。 a) 以下を含む府省庁支給以外の端末利用時の申請内容 ・申請者の氏名、所属、連絡先 ・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合） ・利用する端末の機種名 ・利用目的、取り扱う情報の概要、機密性3情報の利用の有無等 ・主要な利用場所 ・利用する主要な通信回線サービス ・利用する期間 b) 利用許諾条件 c) 申請手順 d) 利用期間中の不具合、盗難・紛失、修理、機種変更等の際の届出の手順 e) 利用期間満了時の利用終了又は利用期間更新の手続方法 f) 許可権限者（遵守事項8.2.1(1)(c)において定める、府省庁支給以外の端末の安全管理措置の実施状況を管理する責任者（以下、この項において「端末管理責任者」という。））	（端末の利用についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、自組織のユーザーが使用する端末に対して、適切なセキュリティ対策を講ずる必要がある。
					(b) 統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。	8.2.1(1)-2 統括情報セキュリティ責任者は、府省庁支給以外の端末により要機密情報を取り扱う場合は、行政事務従事者が講ずるべき安全管理措置の実施手順について、以下を例に整備すること。 a) パスワード等による端末ロックの常時設定 b) OSやアプリケーションの最新化 c) 不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（府省庁として不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める） d) 遠隔データ消去機能の設定 e) 要機密情報の暗号化等による秘匿性の確保 f) 端末内の要機密情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある） g) 府省庁提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ） h) 以下を例とする禁止事項の遵守 ・端末、OS、アプリケーション等の改造行為 ・安全性が確認できないアプリケーションのインストール及び利用 ・利用が禁止されているソフトウェアのインストール及び利用 ・許可されない通信回線サービスの利用（利用する回線を限定する場合） ・第三者への端末の貸与	（端末の利用についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、自組織のユーザーが使用する端末に対して、適切なセキュリティ対策を講ずる必要がある。
					(d) 前号で定める責任者は、要機密情報を取り扱う府省庁支給以外の端末について、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずるとともに、行政事務従事者に適切に安全管理措置を講じさせること。	8.2.1(1)-3 情報システムセキュリティ責任者は、府省庁支給以外の端末により要機密情報を取り扱う府省庁の情報システムにリモートアクセスする環境を構築する場合、基盤となる情報システムにより各府省庁に提供されるリモートアクセス環境が利用可能であれば活用し、端末の盗難・紛失や不正プログラム感染等により情報窃取されることを防止するために、以下を例とする対策を講ずること。 a) シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。 b) セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。 c) ファイル暗号化等のセキュリティ機能を持つアプリケーションを活用したリモートアクセス環境を構築する。利用者は専用のアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。	（端末の利用についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、自組織のユーザーが使用する端末に対して、適切なセキュリティ対策を講ずる必要がある。
8.1.1(2)				(2) 府省庁支給以外の端末の利用時の対策	(a) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、遵守事項8.2.1(1)(c)で定める責任者の許可を得ること。 (b) 行政事務従事者は、要機密情報を府省庁支給以外の端末で取り扱う場合は、課室情報セキュリティ責任者の許可を得ること。 (c) 行政事務従事者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合には、府省庁にて定められた手続及び安全管理措置に関する規定に従うこと。 (d) 行政事務従事者は、情報処理の目的を完了した場合は、要機密情報を府省庁支給以外の端末から消去すること。	【 基本対策事項 】規定なし	（端末の利用についてはお客様実施事項）	対象外	–	–	–	–	–	–	利用者は、自組織のユーザーが使用する端末に対して、適切なセキュリティ対策を講ずる必要がある。