CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.

日本語版の提供について

「CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1J」(以下CAIQと記述)は、Cloud Security Allianceより提供されている「CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1」の日本語訳で、原文をそのまま翻訳しています。
従いまして、日本独自の法令や基準に関する記述は含まれておりません。
原文と日本語版の内容に相違があった場合には、原文が優先されます。
また、この翻訳版は予告なく変更される場合があります。
以下の変更履歴(日付、バージョン、変更内容)をご確認ください。

変更履歴

日付	バージョン	変更内容
2015年1月31日	日本語バージョン1.0	
2015年2月19日	日本語バージョン1.1	コメントのミス修正

日本クラウドセキュリティアライアンスに関する情報は、以下のURLより参照可能ですのでご覧ください。
http://cloudsecurityalliance.jp

日本語バージョン1.1
2015年2月19日

CAIQ v3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Group	CGID	CID	Control Specification	Control Specification 日本語訳	Consensus Assessment Questions	Consensus Assessment Questions 日本語訳
Application & Interface Security *Application Security* *アプリケーションとインターフェースセキュリティ* *アプリケーションセキュリティ*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	アプリケーションプログラミングインタフェース（API）は、業界の認める標準（たとえばWebアプリケーションの場合、OWASPなど）に従って、設計、開発及び導入しなければならない。また、APIは該当する法的及び規制上の遵守義務に従わなければならない。	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	業界標準（Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NISTなど）を、システム／ソフトウエア開発ライフサイクル（SDLC）にセキュリティを組み込むために利用していますか？
		AIS-01.2			Do you use an automated source code analysis tool to detect security defects in code prior to production?	製品出荷前にセキュリティの不具合のあるコードを見つけるために、自動化されたソースコード解析ツールを利用していますか？
		AIS-01.3			Do you use manual source-code analysis to detect security defects in code prior to production?	製品出荷前にセキュリティの不具合のあるコードを見つけるために、手動でソースコード解析を行っていますか？
		AIS-01.4			Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	あなたにソフトウエアを提供するすべての事業者が、システム／ソフトウエア開発ライフサイクル（SDLC）セキュリティの業界標準に従っていることを確認していますか？
		AIS-01.5			(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	(SaaSのみ) アプリケーションにセキュリティの脆弱性が無いかどうかの検証を行い、問題がある場合は実稼働環境に展開する前に対応していますか？
Application & Interface Security *Customer Access Requirements* *アプリケーションとインターフェースセキュリティ* *顧客アクセス要求*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, (removed all) identified security, contractual, and regulatory requirements for customer access shall be addressed.	データ、資産、情報システムへの顧客のアクセスを許可する前に、顧客のアクセスに関して特定されたセキュリティ上、契約上、及び規制上の要求事項を把握していなければならない。	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	顧客にデータ、資産、情報システムへのアクセスを許可する前に、顧客のアクセスに関して特定されたすべてのセキュリティ上、契約上、及び規制上の要求事項が（顧客に）知らされていて、満たされていますか？
		AIS- 02.2			Are all requirements and trust levels for customers' access defined and documented?	顧客のアクセスに対するすべての要件と信頼レベルが、定義され文書化されていますか？
Application & Interface Security *Data Integrity* *アプリケーションとインターフェースセキュリティ* *データの完全性*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	手動またはシステムによる処理エラー、データ破損、または誤用が発生しないようにするために、アプリケーションインタフェース及びデータベースには、データの入出力の完全性チェックルーチン（マッチングやエディットチェックなど）を実装しなければならない。	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	アプリケーションのインタフェース及びデータベースで手動又はシステムによる処理エラー、データ破壊が発生しないようにするために、データの入出力のチェックルーチン（マッチングやエディットチェックなど）を実装していますか？
Application & Interface Security *Data Security / Integrity* *アプリケーションとインターフェースセキュリティ* *データセキュリティ / 完全性*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alternation, or destruction.	不正な開示、改ざんまたは破壊を防ぐために、複数のシステムインタフェース、司法管轄、商取引を構成する機能をまたがって（機密性、完全性、可用性）を含むデータのセキュリティを確保するようことができポリシー及び手順を確立し維持しなければならない。	Is your Data Security Architecture designed using an industry standard (e.g, CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	データセキュリティアーキテクチャは、業界標準を使用して設計されていますか？(たとえば、CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)
Audit Assurance & Compliance *Audit Planning* *監査保証とコンプライアンス* *監査計画*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	監査計画は、業務プロセスの中断に対応できるように開発され維持されなければならない。監査計画は、セキュリティ運用の効果的な実装にフォーカスレビューしなければならない。監査活動は、監査を実施する前に同意を得なければならない。	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	監査上の言明を、業界で受け入れられた構造化フォーマット（たとえば、CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program,など）で作成していますか？
Audit Assurance & Compliance *Independent Audits* *監査保証とコンプライアンス* *独立した監査*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures and compliance obligations.	独立したレビュー及び評価を、少なくとも年に1回実施し、設定されたポリシー、基準、手順、ならびに遵守義務への不適合について、組織が確実に把握できるようにしなければならない。	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	テナントに対して、あなたが作成したSOC2/ ISO 27001あるいは同様の第三者機関による監査または承認レポートの参照を認めていますか？
		AAC-02.2			Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?	クラウドサービス基盤に対するネットワークペネトレーションテストを、業界のベストプラクティスやガイダンスに規定されたように定期的に行うように指示していますか？
		AAC-02.3			Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	クラウド基盤のアプリケーションペネトレーションテストを業界のベストプラクティスやガイダンスに規定されたように定期的に行うように指示していますか？
		AAC-02.4			Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	内部監査を、業界のベストプラクティスやガイダンスに規定されたように定期的に行うように指示していますか？
		AAC-02.5			Do you conduct external audits regularly as prescribed by industry best practices and guidance?	外部監査を、業界のベストプラクティスやガイダンスに規定されたように定期的に行うように指示していますか？
		AAC-02.6			Are the results of the penetration tests available to tenants at their request?	ペネトレーションテストの結果を、要求に応じてテナントに公開していますか？
		AAC-02.7			Are the results of internal and external audits available to tenants at their request?	内部監査及び外部監査の結果を、要求に応じてテナントに公開していますか？
		AAC-02.8			Do you have an internal audit program that allows for cross-functional audit of assessments?	部門にまたがった評価の監査を許可するような内部監査プログラムがありますか？
Audit Assurance & Compliance *Information System Regulatory Mapping* *監査保証とコンプライアンス* *情報システムに関する規制の把握*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	組織は、業務の必要性に関連した基準、規制、法律、法定要件を網羅するコントロールフレームワークを作成し維持しなければならない。コントロールフレームワークは、ビジネスプロセスに影響を及ぼす変更が反映されていることを確実にするために、少なくとも年1回レビューされなければならない。	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	データが1つのテナントのために生成される場合、不用意に他のテナントのデータにアクセスすることが無いように、顧客のデータを論理的に分割するか暗号化することができますか？
		AAC-03.2			Do you have capability to recover data for a specific customer in the case of a failure or data loss?	障害あるいはデータ損失の場合、特定の顧客のデータをリカバリすることができますか？
		AAC-03.3			Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	顧客データの保存を、特定の国あるいは地理的位置に限定することはできますか？

		AAC-03.4			Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	関連する司法権における規制上の要件をモニターし、変更がある場合はセキュリティ施策を法的要求事項の変更に適合させ、関連する規制上の要件を遵守することを保証できる変更管理プログラムを持っていますか？
Business Continuity Management & Operational Resilience *Business Continuity Planning* *事業継続管理と運用* *レジリエンス* *事業継続計画*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	すべての事業継続計画が、検査、保守及び情報セキュリティの要求事項に関する優先順位の特定について一貫性を持つように、事業継続計画立案及び計画作成のための一貫性のある統一された枠組みを確立し、文書化し、採用しなければならない。事業継続計画の要求事項には、以下が含まれる。 ・関連する依存関係に従った目的及び範囲の定義 ・計画の利用者が理解し利用できるようにすること ・(一人または複数の)指名された責任者(オーナー)が計画のレビュー、更新及び承認に責任を負うこと ・伝達経路、役割及び責任の定義 ・詳細な復旧の手順、手動による回避策及び参考情報 ・計画発動の手順	Do you provide tenants with geographically resilient hosting options?	テナントに対して、地理的な観点から回復可能なホスティングのオプションを提供していますか？
		BCR-01.2			Do you provide tenants with infrastructure service failover capability to other providers?	テナントに対して、基盤サービスを他のプロバイダーにフェールオーバする機能を提供していますか？
Business Continuity Management & Operational Resilience *Business Continuity Testing* *事業継続管理と運用* *レジリエンス* *事業継続テスト*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	事業継続計画及びセキュリティインシデント対応計画は、事前に定められた間隔で、または組織及び環境の重大な変化に合わせて検証されなければならない。インシデント対応計画には、影響を受ける顧客(テナント)、及び重要なサプライチェーン内の事業プロセスの依存関係をになうその他の取引関係先を関与させなければならない。	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	継続的に有効な状態を保つため、事業継続性プランは、計画された間隔あるいは大きな組織変更や環境変更が行われた時にテストされていますか？
Business Continuity Management & Operational Resilience *Power / Telecommunications* *事業継続管理と運用* *レジリエンス* *データセンターのユーティリティ / 環境状態*	BCR-03	BCR-03.1	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	不正な妨害または損害から保護することを目的として、あらかじめ定められた間隔でデータセンター設備サービス及び環境状況(水、電力、温度及び湿度管理、通信、インターネット接続など)の安全を確保し、監視し、維持し、有効性が継続していることを確認しなければならない。また、予想されるまたは予想外の事態に備えて、自動フェールオーバーまたはその他の冗長性を持った設計を行わなければならない。	Do you provide tenants with documentation showing the transport route of their data between your systems?	テナントに対して、システム間のデータの移送経路を示した文書を提供していますか？
		BCR-03.2			Can tenants define how their data is transported and through which legal jurisdictions?	テナントは、データがどのように移送され、どのような法域を通っていくかを指定できますか？
Business Continuity Management & Operational Resilience Documentation 事業継続管理と運用 レジリエンス 文書	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	情報システムに関する文書(管理者ガイド、ユーザガイド、アーキテクチャー図など)は、権限を持った人が次の事項を確実に実施するために、利用できなければならない: ・情報システムの設定、インストール及び運用 ・システムのセキュリティ機能の有効利用	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	情報システムの文書(たとえば、管理者及びユーザガイド、アーキテクチャダイアグラムなど)は、情報システムの構成、インストレーション、運用の権限を与えられた人が利用できますか？
Business Continuity Management & Operational Resilience *Environmental Risks* *事業継続管理と運用* *レジリエンス* *環境リスク*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	自然災害や故意による攻撃(火災、洪水、静電気あるいは雷、太陽によって誘発される磁気嵐、風、地震、津波、爆発、原子力事故、火山活動、バイオハザード、市民暴動、土砂災害、地殻運動、その他の自然または人的災害)による被害に対する物理的保護を想定し、設計し、対応策を適用しなければならない。	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	自然災害や故意による攻撃からの損害を予測し、それらに対する物理的保護対策を設計し、適用していますか？
Business Continuity Management & Operational Resilience *Equipment Location* *事業継続管理と運用* *レジリエンス* *機器の位置*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	環境上の脅威、危険、及び権限を持たないアクセスの機会によるリスクを軽減するために、設備を環境上のリスクの高い場所から隔離し、妥当な距離をとった位置に予備の設備を備えることでこれを補強しなければならない。	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	データセンタは、大きな影響のある環境リスク(洪水、竜巻、地震、台風など)が高い確率/頻度で起こる場所にありますか？
Business Continuity Management & Operational Resilience *Equipment Maintenance* *事業継続管理と運用* *レジリエンス* *機器のメンテナンス*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	システムの運用の継続性と保守要員の確保を確実にするため、機器の保守に関する方針及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	仮想基盤を利用する場合、クラウドソリューションは仮想化と独立したハードウェアのリストア及びリカバリ能力を持っていますか？
		BCR-07.2			If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	仮想基盤を利用する場合、テナントに対して仮想マシンの前の時点の状態をリストアできるようにしていますか？
		BCR-07.3			If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	仮想基盤を利用する場合、仮想マシンのイメージをダウンロードし新しいクラウドプロバイダに移行することができますか？
		BCR-07.4			If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	仮想基盤を利用する場合、顧客が仮想イメージを外部の保存場所にコピーすることを許可されていますか？
		BCR-07.5			Does your cloud solution include software/provider independent restore and recovery capabilities?	クラウドソリューションは、ソフトウエアやプロバイダに依存しないリストア及びリカバリの機能を持っていますか？

Business Continuity Management & Operational Resilience *Equipment Power Failures* *事業継続管理と運用* *レジリエンス* *機器の停電*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	防御手段は、地理的に固有のビジネスインパクト評価（BIA）に基づいて、自然及び人的な脅威に対処できるように実地に適用しなければならない。	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	セキュリティ機構と冗長性は、ユーティリティサービスが停止した場合（たとえば、停電、ネットワークの中断など）機器を保護するように実装されていますか？
Business Continuity Management & Operational Resilience *Impact Analysis* *事業継続管理と運用* *レジリエンス* *影響解析*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	事業中断が組織（クラウドプロバイダ、クラウド利用者）に与える影響を判断するための手段を定義し文書化しておかなければならない。これには、以下の事項が含まれる。 ・重要な製品及びサービスの特定 ・プロセス、アプリケーション、事業パートナー、サードパーティサービスプロバイダなど、すべての依存関係の特定 ・重要な製品及びサービスへの脅威の把握 ・予想されたまたは予想外の事業中断による影響の確認及び時間経過に伴うこれらの影響の変化の確認 ・最大許容停止時間の設定 ・復旧の優先順位の設定 ・最大許容停止時間内に重要な製品及びサービスを再開するための目標復旧時間の設定 ・再開に必要な資源の見積もり	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	テナントに対して、稼働中のSLAの履行状況について、可視化とレポーティングの機能を提供していますか？
		BCR-09.2			Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	テナントは、標準に基づく情報セキュリティの指標（CSA, CAMMなど）を利用できますか？
		BCR-09.3			Do you provide customers with ongoing visibility and reporting of your SLA performance?	顧客に対して、稼働中のSLAの履行状況について、可視化とレポーティングの機能を提供していますか
Business Continuity Management & Operational Resilience *Policy* *事業継続管理と運用* *レジリエンス* *管理プログラム*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	業界によって受け入れられるような標準（ITIL v4、COBIT 5など）に基づいて事業部門、従業員、顧客を支援する組織のIT機能を適切に計画し、提供し、支援することを目的として、適切なITガバナンス及びサービス管理のためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。さらに、ポリシーと手順では、（必要な）役割と責任を定義し、定期的な従業員訓練によって周知徹底しなければならない。	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	ポリシー及び手続きを確立し、サービス運用を支援する権限のあるすべての人々に利用可能にしていますか？
Business Continuity Management & Operational Resilience *Retention Policy* *事業継続管理と運用* *レジリエンス* *保持ポリシー*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	重要な資産の保持期間を、それぞれのポリシー及び手順、ならびに該当する法的または規制上の遵守義務に従って定義し、これに準拠するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。バックアップ及び復旧のための手段は、事業継続計画の一部として導入し、有効性の確認のために適宜テストしなければならない。	Do you have technical control capabilities to enforce tenant data retention policies?	テナントデータの保存ポリシーを実施するための技術的な能力を持っていますか？
		BCR-11.2			Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	政府や第三者機関からテナントデータの提供を要求された場合に対する文書化された手続きがありますか？
		BCR-11.4			Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	規制、法令、契約、ビジネスの要求に対するコンプライアンスを保証するために、バックアップ及び冗長化機能を実装していますか？
		BCR-11.5			Do you test your backup or redundancy mechanisms at least annually?	最低限1年に1回、バックアップあるいは冗長化機能のテストを行っていますか？
Change Control & Configuration Management New Development / Acquisition 変更管理と構成管理 新規開発及び調達	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装し、データ、実/仮想アプリケーション、インフラストラクチャーネットワーク及びシステムコンポーネント、ならびに事業用・業務用・データセンター用各施設の新規の開発及び調達が、組織の事業責任者もしくはその責にある職務または機能によって、確実に事前承認されているようにしなければならない。	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	開発、新しいアプリケーション/システム/データベース/基盤/サービス/運用の開発、調達に対する管理権限付与のためのポリシー及び手続きは確立されていますか？
		CCC-01.2			Is documentation available that describes the installation, configuration and use of products/services/features?	製品/サービス/機能のインストレーション、構成、利用を記述した文書は利用可能ですか？
Change Control & Configuration Management	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the	外部のビジネスパートナーは、組織内の開発者向けの変更管理、リリース、テストのためのポリシーと手順（たとえば、ITILサービス管理プロセス）と同じものに従わなければならない	Do you have controls in place to ensure that standards of quality are being met for all software development?	すべてのソフトウエア開発において品質標準が満たされていることを保証するための管理はできていますか？

Outsourced Development *変更管理と構成管理* *開発の外部委託*		CCC-02.2	organization (e.g. ITIL service management processes).	なし。	Do you have controls in place to detect source code security defects for any outsourced software development activities?	外部委託されたソフトウエア開発に対して、ソースコード上のセキュリティ不具合を見つけるための管理はできていますか？
Change Control & Configuration Management *Quality Testing* *変更管理と構成管理* *品質検査*	CCC-03	CCC-03.1	Organization shall follow a defined qualty change control and testing process (e.g. ITIL Service Management) with established baselines, testing and release standards which focus on system availability, confidentiality and integrity of systems and services	組織は、システムとサービスの可用性、機密性、完全性を目的とするベースライン、テスト及びリリースの基準を備えた、明確に定義された品質及び変更管理とテストプロセス（たとえば、ITILサービスマネジメント）に従わなければならない。	Do you provide your tenants with documentation that describes your quality assurance process?	品質保証プロセスについて記述された文書をテナントに提供していますか？
		CCC-03.2			Is documentation describing known issues with certain products/services available?	製品/サービスの既知の問題を記述した文書は利用できますか？
		CCC-03.3			Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	提供されている製品及びサービスについて、通知されたバグとセキュリティの脆弱性を分類（トリアージ）し、改善するためのポリシーと手続きは確立されていますか？
		CCC-03.4			Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	全てのデバッグコードとテストコードは、リリースされたソフトウエアのバージョンから削除されていることを保証するための方法はありますか？
Change Control & Configuration Management *Unauthorized Software Installations* *変更管理と構成管理* *未承認のソフトウェアのインストール*	CCC-04	CCC-04.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	組織が所有または管理するユーザのエンドポイントデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）、ITインフラストラクチャーネットワーク及びシステムコンポーネントに承認されていないソフトウェアがインストールされることを防ぐために、方針及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	承認されていないソフトウエアがシステム上にインストールされることを制限しモニターすることができますか？
Change Control & Configuration Management *Production Changes* *変更管理と構成管理* *業務の変更*	CCC-05	CCC-05.1	Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, as well as infrastructure network and systems components. Technical measures shall be implemented to provide assurance that, prior to deployment, all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA).	以下の変更を適用する際のリスクを管理するため、インフラストラクチャーネットワーク及びシステムコンポーネントと同様に、業務上重要な、又は顧客（テナント）に影響する実/仮想アプリケーション及びシステム間インタフェース（API）の設計及び設定するためのポリシー及び手順を確立しなければならない。導入前に、技術的対策を施すことによって、すべての変更が、登録された変更要求、業務上重要な又は顧客（テナント）に影響するリスクの分析、契約（SLA）に従った顧客（テナント）への通知及びその承認、のすべてを満たすことを保証しなければならない。	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?	稼働環境の変更管理手続き、及び変更管理におけるテナントの役割/権利/責任を記述した文書をテナントに提供していますか？
Data Security & Information Lifecycle Management *Classification* *データセキュリティと情報ライフサイクル管理* *分類*	DSI-01	DSI-01.1	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	データ及びデータを含むオブジェクトは、データタイプ、価値、機微性、組織にとっての重要性に基づいて、データの所有者によって機密区分されなければならない。	Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?	ポリシータグ/メタデータを通して、仮想マシンを特定することができますか？（たとえば、タグは、ゲストOSによるブート/インスタンス化/不適切な国でのデータ移送を制限することができる）
		DSI-01.2			Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?	ポリシータグ/メタデータ/ハードウエアタグ（たとえば、TXT/TPM, VN-Tagなど）を通して、ハードウエアを特定することができますか？
		DSI-01.3			Do you have a capability to use system geographic location as an authentication factor?	認証の要素のひとつとして、システムの地理上の位置を使用することができますか？
		DSI-01.4			Can you provide the physical location/geography of storage of a tenant's data upon request?	要求に応じて、テナントの物理的位置/地理的なデータの保管場所を提供できますか？
		DSI-01.5			Can you provide the physical location/geography of storage of a tenant's data in advance?	事前に、テナントの物理的位置/地理的なデータの保管場所を提供できますか？
		DSI-01.6			Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	構造的データラベル付け標準（たとえば、ISO 15489, Oasis XML Catalog Specification, CSAデータタイプガイダンス）に準拠していますか？
		DSI-01.7			Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?	データの移送経路あるいはリソースのインスタンス化のために許容できる地理的な位置を定義することをテナントに許可しますか？

Data Security & Information Lifecycle Management *Data Inventory / Flows* *データセキュリティと情報ライフサイクル管理* *データ保存 / フロー*	DSI-02	DSI-02.1	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	サービスのアプリケーション、インフラストラクチャーネットワーク、及びシステム内に（常時または一次的に）存在するデータのデータフローを作成し、文書化し、維持するためのポリシー及び手順を確立しなければならない。特に、プロバイダは、地理的な所在場所の要件の支配下にあるデータが、定義された境界を越えて移動しないことを保証しなければならない。	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	サービスアプリケーション、基盤ネットワーク、システムに（永続的あるいは一時的に）存在するデータのためのデータフローを棚卸し、文書化し、維持していますか？
		DSI-02.2			Can you ensure that data does not migrate beyond a defined geographical residency?	データが、定義されている地理的存在範囲を超えて移行されていないことを保証できますか？
Data Security & Information Lifecycle Management *eCommerce Transactions* *データセキュリティと情報ライフサイクル管理* *e コマーストランザクション*	DSI-03	DSI-03.1	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	一般に開放されたネットワークを使って送受信されるe-コマースに関わるデータは、契約違反やデータ破壊を防ぐことができる方法により、適切に分類し、不正行為や許可されていない開示または変更から保護しなければならない。	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	テナントがパブリックネットワーク（たとえば、インターネット）に送信するデータを保護するために、公開されている暗号化手法（3.4ES, AESなど）を提供していますか？ （訳注：3.4ESは3DESのことと思われますが原文に忠実に訳しています）
		DSI-03.2			Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	基盤コンポーネントがパブリックネットワークを通してお互いに通信を行う必要がある場合（たとえば、インターネット越しにある環境から別の環境にデータをレプリケートする）、公開されている暗号化手法を使用していますか？
Data Security & Information Lifecycle Management *Handling / Labeling / Security Policy* *データセキュリティと情報ライフサイクル管理* *処理 / ラベル付 / セキュリティポリシー*	DSI-04	DSI-04.1	Policies and procedures shall be established for labeling, handling, and the security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	データ及びデータを含むオブジェクトのラベリング、処理取扱い、セキュリティのためのポリシー及び手順を確立しなければならない。データをまとめて格納するオブジェクトには、ラベルを継承して保持する仕組みを実装しなければならない。	Are policies and procedures established for labeling, handling and the security of data and objects that contain data?	データ及びデータを含むオブジェクトのラベリング、処理取扱い、セキュリティのためのポリシー及び手順を確立していますか？
		DSI-04.2			Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?	データをまとめて格納するオブジェクトには、ラベルを継承して保持する仕組みを実装していますか？
Data Security & Information Lifecycle Management *Nonproduction Data* *データセキュリティと情報ライフサイクル管理* *非実稼働データ*	DSI-05	DSI-05.1	Production data shall not be replicated or used in non-production environments.	本番環境のデータは、テスト環境にコピーしたり使用したりしてはならない。	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	本番環境のデータが非本番環境にコピーされたり使用されたりしないことを保証する手続きを取っていますか？
Data Security & Information Lifecycle Management *Ownership / Stewardship* *データセキュリティと情報ライフサイクル管理* *管理責任 / 受託責任*	DSI-06	DSI-06.1	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	すべての情報に対して管理責任者が指名されなければならない。管理責任者の責任は、定義され、文書化され、通知されなければならない。	Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?	データ管理責任者の責任は、定義され、文書化され、通知されていますか？
Data Security & Information Lifecycle Management *Secure Disposal* *データセンタセキュリティ* *安全な廃棄*	DSI-07	DSI-07.1	Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	テスト環境での顧客データの利用は、影響を受けるデータのすべての顧客から明確で文書化された許可を必要とする。また、機微なデータ要素を取扱うことに関するすべての法律及び規制要件に従わなければならない。	Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?	アーカイブ及びバックアップされたデータは、テナントによって決められた方法で安全に削除（たとえば、消磁/暗号書き込みによる消去）するようにしていますか？
		DSI-07.2			Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	顧客がクラウド環境の使用を終了するかリソースの使用を終了した場合、関係するすべてのコンピューティング資源でテナントデータを削除することを含む、サービス終了のための文書化された手続きを提供していますか？
Datacenter Security *Asset Management* *データセンタセキュリティ* *資産管理*	DCS-01	DCS-01.1	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership y defined roles and responsibilities.	資産は事業上の重要性、サービスレベルの期待値、運用の継続性の要件の視点から分類しなければならない。すべてのサイトや地理的場所に位置する業務上不可欠な資産の完全な目録とその使用履歴を維持し、定期的に更新し、定義された役割及び責任を持つ管理責任者を割当てなければならない。	Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?	すべての重要な資産資産について、所有権を含む完全な目録を維持していますか？
		DCS-01.2			Do you maintain a complete inventory of all of your critical supplier relationships?	重要な納入業者との関係の完全な目録を維持していますか？

Datacenter Security *Controlled Access Points* *データセンタセキュリティ コントロールされたアクセスポイント*	DCS-02	DCS-02.1	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	機微なデータ及び情報システムを保護するために、物理的なセキュリティ境界（フェンス、壁、柵、警備員、ゲート、電子的監視、物理的認証メカニズム、受付デスク、安全パトロールなど）を実装しなければならない。	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	物理的なセキュリティ境界（フェンス、壁、柵、警備員、ゲート、電子的監視、物理的認証メカニズム、受付デスク、安全パトロールなど）を実装していますか？
Datacenter Security *Equipment Identification* *データセンタセキュリティ アイデンティフィ*	DCS-03	DCS-03.1	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	接続認証の手段として自動的に機器を識別する仕組みを使用しなければならない。接続認証の完全性を確認するために、既知の機器の所在場所に基づいて所在場所を特定する技術を使用することができるかもしれない。	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	既知の機器の所在場所に基づいて接続認証の完全性を確認するために、自動的に機器を識別する仕組みを使用していますか？
Datacenter Security *Offsite Authorization* *データセンタセキュリティ オフサイト認証*	DCS-04	DCS-04.1	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	ハードウェア、ソフトウェアまたはデータをサイト外の場所に移動させるには、事前の承認を取得しなければならない。	Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)	データを1つの物理的な場所から別の場所に移動する（たとえば、オフサイトバックアップ、事業継続性のためのフェールオーバ、レプリケーション）場合のシナリオを記述した文書を、テナントに提供していますか？
Datacenter Security *Offsite equipment* *データセンタセキュリティ オフサイト機器*	DCS-05	DCS-05.1	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premise. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full write of the drive to ensure that the erased drive is released to inventory for reuse and deployment or securely stored until it can be destroyed.	組織の構外で使用される装置の安全な処分（資産のタイプによる）のためのポリシー及び手順を確立しなければならない。これは、情報の復元を不可能な状態にする完全削除ソリューションか破壊プロセスを含むべきである。消去されたドライブが再利用や配備のために在庫に回されるか破壊されるまで安全に保管されていることを保証するために、消去はドライブ全体を上書きすべきである。	Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?	資産管理と機器の再利用を統制するポリシーと手続きを文書化し、証拠としてテナントに提供できますか？
Datacenter Security *Policy* *データセンタセキュリティ ポリシー*	DCS-06	DCS-06.1	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas.	オフィス、部屋、施設、機微な情報を保存する安全なエリア内での安全とセキュリティが確保された労働環境を維持するためのポリシー及び手順を確立し、これらを補強するための業務プロセスを実装しなければならない。	Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	オフィス、部屋、施設、セキュリティエリア内で安全でセキュアな作業を維持するために確立された文書化したポリシーと手続きを、証拠としてテナントに提供できますか？
		DCS-06.2			Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?	文書化されたポリシー、標準、手続きに関するトレーニングを担当者及び関係する第三者に行っていることを、証拠として提供できますか？
Datacenter Security *Secure Area Authorization* *データセンタセキュリティ セキュアエリア認証*	DCS-07	DCS-07.1	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	許可された者だけが立入りできるようにするために、物理的なアクセスコントロールの仕組みによってセキュリティエリアへの入退出を制限し監視しなければならない。	Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	（データがどこに保管されアクセスされるか、に基づいて司法権管轄が決まることを受けて）データの行き来を許可する地理的な位置をテナントが指定することを許可しますか？
Datacenter Security *Unauthorized Persons Entry* *データセンタセキュリティ 許可されていない個人エントリ*	DCS-08	DCS-08.1	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	サービスエリアなどの出入口、及び許可されていない者が施設内に立ち入る可能性のある場所は、データの破壊、改ざん、紛失を避けるために、監視及び管理し、可能であれば、データの保管及び処理施設から離さなければならない。	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	サービスエリアなどの出入口、及び許可されていない者が施設内に立ち入る可能性のある場所は、データの保管及び処理施設から離して監視及び管理していますか？
Datacenter Security *User Access* *データセンタセキュリティ ユーザアクセス*	DCS-09	DCS-09.1	Physical access to information assets and functions by users and support personnel shall be restricted.	利用者及びサポートスタッフによる情報資産及び情報処理機能への物理的アクセスを制限しなければならない。	Do you restrict physical access to information assets and functions by users and support personnel?	利用者及び支援スタッフによる情報資産及び情報処理機能への物理的アクセスを制限していますか？
Encryption & Key Management *Entitlement* *暗号化と鍵管理 権限付与*	EKM-01	EKM-01.1	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	鍵には識別可能な所有者が存在し（つまり鍵とアイデンティティが紐付いていること）、また（組織には）鍵管理ポリシーがなくてはならない。	Do you have key management policies binding keys to identifiable owners?	鍵を識別可能な所有者に紐付ける鍵管理ポリシーがありますか？

Encryption & Key Management *Key Generation* *暗号化と鍵管理* *鍵作成*	EKM-02	EKM-02.1	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	サービスの暗号システムの暗号鍵を管理するためのポリシー及び手順を確立しなければならない（鍵の生成から廃棄、更新に至るライフサイクルの管理、PKI、使用される暗号プロトコルの設計及びアルゴリズム、安全な鍵生成に適したアクセス制御、暗号化データまたはセッションに使用される鍵の隔離を含む交換及び保管など）。プロバイダは、要求に応じて、特に顧客（テナント）データがサービスの一部として利用されたり、顧客（テナント）が管理の実施に対する責任の一部を共有したりしている場合は、顧客（テナント）に暗号システム内の変更を通知しなければならない。	Do you have a capability to allow creation of unique encryption keys per tenant?	テナントごとに独自の暗号鍵を作成することができますか？
		EKM-02.2			Do you have a capability to manage encryption keys on behalf of tenants?	テナントに代わって暗号鍵を管理できますか？
		EKM-02.3			Do you maintain key management procedures?	鍵管理手続きを行っていますが？
		EKM-02.4			Do you have documented ownership for each stage of the lifecycle of encryption keys?	暗号鍵のライフサイクルの各ステージにおける所有権を文書化していますか？
		EKM-02.5			Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?	暗号鍵の管理に、第三者/オープンソース/自社のフレームワークを使用していますか？
Encryption & Key Management **Sensitive Data Protection** **暗号化と鍵管理** **機微データの保護**	EKM-03	EKM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	該当する法的及び規制上の遵守義務に従って、ストレージ（ファイルサーバ、データベース、エンドユーザのワークステーションなど）内、データの使用時（メモリ）、及びデータの送信時（システムインタフェース、公的ネットワーク経由、電子メッセージ通信など）の機微なデータの保護を目的として暗号プロトコルを使用するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	Do you encrypt tenant data at rest (on disk/storage) within your environment?	自身の環境のディスクやストレージ上で、テナントのデータを暗号化していますか？
		EKM-03.2			Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	ネットワーク間及びハイパバイザーインスタンス間の移送において、データ及び仮想マシンイメージの保護のため暗号化を行いますか？
		EKM-03.3			Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)?	テナントが作成した暗号鍵をサポートしますか？あるいは、テナントが公開鍵証明書にアクセスすることなしにデータを暗号化すること（たとえば、IDベースの暗号化）を許可しますか？
		EKM-03.4			Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?	暗号化管理ポリシー、手続き、ガイドラインを構築し定義した文書を持っていますか？
Encryption & Key Management *Storage and Access* *暗号化と鍵管理* *保管とアクセス*	EKM-04	EKM-04.1	Platform and data appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	オープンな検証済みの形式かつ標準アルゴリズムであるプラットフォームやデータに適した暗号化方式（AES-256など）を使用しなければならない。鍵は（当該クラウドプロバイダの）クラウド内に保管するのではなく、クラウドの利用者または信頼できる鍵管理プロバイダが保管しなければならない。鍵の管理と鍵の使用は、異なる責務として分離されなければならない。	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	オープンな検証済みの形式かつ標準アルゴリズムであるプラットフォームやデータに適した暗号化方式を採用していますか？
		EKM-04.2			Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	暗号鍵は、クラウドの利用者又は信頼できる鍵管理プロバイダが保管していますか？
		EKM-04.3			Do you store encryption keys in the cloud?	暗号鍵は、クラウド内に保存されていますか？
		EKM-04.4			Do you have separate key management and key usage duties?	鍵管理と鍵使用は、異なった責務として分離されていますか？
Governance and Risk Management *Baseline Requirements* *ガバナンスとリスク管理* *ベースライン要求*	GRM-01	GRM-01.1	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.	開発済みまたは購入済みで、組織が所有または管理する実/仮想アプリケーション、インフラストラクチャーシステム及びネットワークコンポーネントのための基準となるセキュリティの要求事項を確立しなければならない。またそれらの要求事項は該当する法的及び規制上の遵守義務に準拠していなければならない。標準的な設定から逸脱する場合は、導入、提供、使用の前に、変更管理ポリシー及び手順に従って承認を受けなければならない。セキュリティベースラインの要求事項への準拠は、その頻度がビジネス要求に基づいて設定され承認されない場合、少なくとも年1回は再評価されなければならない。	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	（たとえば、ハイパーバイザ、オペレーティングシステム、ルータ、DNSサーバなど）のすべての基盤コンポーネントに対して、情報セキュリティ基準を文書化していますか？
		GRM-01.2			Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	情報セキュリティ基準に対する基盤の遵守状況を、継続的にモニターしレポートすることはできますか？
		GRM-01.3			Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?	クライアントに対して、クライアント自身の内部標準に準拠したトラステッド仮想マシンのイメージを提供することができますか？
Governance and Risk Management **Data Focus Risk Assessments** **ガバナンスとリスク管理** **データフォーカスリスクアセスメント**	GRM-02	GRM-02.1	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	データガバナンスの要求事項に関連するリスクアセスメントを事前に定められた間隔で実施し、その際に以下の事項を考慮しなければならない。 ・機微のデータがどこで保管され、アプリケーション、データベース、サーバ、ネットワークインフラストラクチャー間で送受信されるかの認識 ・定められた保存期間及び使用終了時の廃棄に関する要求事項への準拠 ・データの分類ならびに許可されていない使用、アクセス、紛失、破壊及び改ざんからの保護	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?	テナントが業界標準の継続監視（物理的・論理的なクラウド管理状態の検証をテナントが継続して行うことができる）を実装可能にするために、セキュリティ管理健全性データを提供していますか？
		GRM-02.2			Do you conduct risk assessments associated with data governance requirements at least once a year?	少なくとも1年に一度、データガバナンスの要求に基づくリスク評価を行っていますか？
Governance and Risk Management *Management Oversight* *ガバナンスとリスク管理* *管理の監視*	GRM-03	GRM-03.1	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures and standards that are relevant to their area of responsibility.	管理者は、自らの責任範囲に関わるセキュリティポリシー、手順及び標準を認識し、遵守し続ける責任がある。	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	技術マネージャ、ビジネスマネージャ、上級マネージャは、管理者や従業員の責任範囲の一部として、セキュリティポリシー、手続き、及び標準についての認識とコンプライアンスを維持する責任を持っていますか？

Governance and Risk Management *Management Program* *ガバナンスとリスク管理* *管理プログラム*	GRM-04	GRM-04.1	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	資産及びデータを紛失、誤用、許可されていないアクセス、開示、改変、破壊から保護するために、管理的、技術的、物理的保護措置を含む情報セキュリティマネジメントプログラム(ISMP)を開発し、文書化し、承認し、実装しなければならない。セキュリティプログラムは、事業の特性に関わる範囲では、少なくても以下の分野を含めなければならない。 ・リスク管理 ・セキュリティポリシー ・情報セキュリティの組織 ・資産管理 ・人的セキュリティ ・物理的及び環境的セキュリティ ・通信及び運用管理 ・アクセス制御 ・情報システムの取得、開発及び保守	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	情報セキュリティ管理プログラム(ISMP)を記述した文書を、テナントに提供していますか？
		GRM-04.2			Do you review your Information Security Management Program (ISMP) least once a year?	情報セキュリティ管理プログラム(ISMP)を、少なくとも1年に一度レビューしていますか？
Governance and Risk Management *Management Support / Involvement* *ガバナンスとリスク管理* *補強 / 関与*	GRM-05	GRM-05.1	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	経営陣及び管理職は、文書による明確な指示及びコミットメントを通じて情報セキュリティを担保するための業務指示を発し、指示が実施に移されたことを確認しなければならない。	Do you ensure your providers adhere to your information security and privacy policies?	プロバイダが、情報セキュリティとプライバシーポリシーを遵守していることを確実に確認できていますか？ （クラウドユーザの監督責任として述べていることに注意）
Governance and Risk Management *Policy* *ガバナンスとリスク管理* *ポリシー*	GRM-06	GRM-06.1	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	情報セキュリティのポリシー及び手順を確立し、影響を受けるすべての人員及び外部の取引関係者がいつでもレビューできるよう準備しておかなければならない。情報セキュリティのポリシーは、組織の事業責任者(またはその責任を負うその他の役割もしくは機能)によって承認され、事業責任者のための情報セキュリティにおける役割及び責任を明示した戦略的事業計画及び情報セキュリティマネジメントプログラムによって担保されなければならない。	Do your information security and privacy policies align with industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	情報セキュリティとプライバシーポリシーは、業界標準 (ISO-27001, ISO-22307, CoBITなど)と合っていますか？
		GRM-06.2			Do you have agreements to ensure your providers adhere to your information security and privacy policies?	テナント自身の情報セキュリティとプライバシーポリシーを遵守することを、プロバイダが合意していますか？ （クラウドユーザの責任として述べていることに注意）
		GRM-06.3			Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?	規則と標準に対する管理、アーキテクチャ、プロセスをマップしたデューデリジェンスの結果を提供できますか？
		GRM-06.4			Do you disclose which controls, standards, certifications and/or regulations you comply with?	遵守している管理、標準、認証、規則を公開できますか？
Governance and Risk Management *Policy Enforcement* *ガバナンスとリスク管理* *ポリシー強化*	GRM-07	GRM-07.1	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	セキュリティポリシー及び手順に違反した従業員に対する正式な懲罰あるいは制裁のポリシーを確立しなければならない。違反した場合に講じられる措置を従業員に認識させなければならない。また、ポリシー及び手順で懲戒手続きを規定しなければならない。	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	セキュリティポリシー及び手順に違反した従業員に対する正式な懲罰あるいは制裁のポリシーを確立していますか？
		GRM-07.2			Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	ポリシー及び手順に違反した場合の処置を、従業員に周知していますか？
Governance and Risk Management **Policy Impact on Risk Assessments** **ガバナンスとリスク管理** **リスクアセスメントにおけるポリシーインパクト**	GRM-08	GRM-08.1	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	リスクアセスメントの結果には、その妥当性と有効性を維持するために、セキュリティポリシー、手順、標準及び管理策の更新を含めなければならない。	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	リスクアセスメントの結果には、セキュリティポリシー、手順、標準及び管理策の妥当性と有効性を維持するための更新を含めていますか？
Governance and Risk Management *Policy Reviews* *ガバナンスとリスク管理* *ポリシーレビュー*	GRM-09	GRM-09.1	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	情報セキュリティポリシーとセキュリティ戦略との継続的な合致、情報セキュリティポリシーの有効性、正確性、妥当性、及び法的または規制上の遵守義務への適用性を確認するために、組織の事業責任者(またはその責任を負うその他の役割もしくは機能)は、事前に定められた間隔または組織変更に対応して情報セキュリティポリシーをレビューしなければならない。	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	情報セキュリティあるいはプライバシーポリシーを変更した場合、テナントに知らせていますか？
		GRM-09.2			Do you perform, at minimum, annual reviews to your privacy and security policies?	プライバシーとセキュリティのポリシーについて、最低1年ごとにレビューしていますか？
Governance and Risk Management **Risk Assessments** **ガバナンスとリスク管理** **リスクアセスメント**	GRM-10	GRM-10.1	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using	定性的手法または定量的手法を使用して、特定されたすべてのリスクの発生可能性及び影響度を判断するために、企業の組織構造に適合した正式なリスクアセスメントを、少なくとも年1回または事前に定められた間隔で、(及び情報システムを変更した時に)、実施しなければならない。固有リスク及び残存リスクに関連する発生可能性及び影響度は、すべ	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	企業全体の枠組みとして、正式なリスクアセスメントを少なくとも年1回、または所定の間隔で実施し、定性的手法又は定量的手法を使用して、特定されたすべてのリスクの発生可能性及び影響度を判断していますか？

		GRM-10.2	qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	てのリスクカテゴリ（たとえば、監査結果、脅威分析及び脆弱性診断、規制の遵守など）を考慮し、独立して判断されなければならない。	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?	固有リスク及び残存リスクに関連する発生可能性及び影響度は、すべてのリスクカテゴリ（たとえば、監査結果、脅威分析及び脆弱性診断、規制の遵守など）を考慮し、独立して判断していますか？
Governance and Risk Management Risk Management Framework **ガバナンスとリスク管理 リスク管理フレームワーク**	GRM-11	GRM-11.1	Organizations shall develop and maintain an enterprise risk management framework to mitigate risk to an acceptable level.	リスクを受容可能なレベルにまで軽減しなければならない。リスク基準に基づく受容可能なレベルは、妥当な対策所要時間及び経営陣の承認に基づいて設定され文書化されなければならない。	Do you have a documented, organization-wide program in place to manage risk?	リスクを管理するにあたって、文書化された組織全体に渡るプログラムを持っていますか？
		GRM-11.2			Do you make available documentation of your organization-wide risk management program?	組織全体のリスク管理プログラムの文書を、利用可能にしていますか？
Human Resources *Asset Returns* *人事* *資産返却*	HRS-01	HRS-01.1	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.	従業員の退職時あるいは外部との取引関係の終了時には、組織に帰属するすべての資産を定められた期間内に返却しなければならない。	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	プライバシー侵害をモニターし、プライバシーに関わるイベントがテナントデータに影響を与える可能性がある場合、テナントに迅速に知らせることができますか？
		HRS-01.2			Is your Privacy Policy aligned with industry standards?	プライバシーポリシーは、業界標準に整合していますか？
Human Resources *Background Screening* *人事* *経歴スクリーニング*	HRS-02	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	現地の法律、規制、倫理及び契約上の制約に従って、すべての採用予定者、契約者及び第三者の経歴を確認しなければならない。この確認は、アクセスされるデータの分類、業務の要求事項及び受容可能なリスクに応じて行わなければならない。	Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?	現地の法律、規制、倫理及び契約上の制約に基づき、すべての採用予定者、契約者及び第三者にたいする経歴の確認を行っていますか？
Human Resources *Employment Agreements* *人事* *雇用契約*	HRS-03	HRS-03.1	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	雇用契約書には、確立された情報ガバナンス及びセキュリティポリシーの遵守に関する規定及び条件を取り入れなければならない。また、新規採用された従業員（フルタイムまたはパートタイム従業員、臨時従業員など）に企業の施設、資源、資産へのアクセスを許可する前に、雇用契約書に署名させなければならない。	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	満たさなければならない従業員個々の役割と情報セキュリティの管理責任に基づき、従業員のトレーニングを行っていますか？
		HRS-03.2			Do you document employee acknowledgment of training they have completed?	トレーニングを終了したことを従業員が確認する文書はありますか？
		HRS-03.3			Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?	顧客/テナントの情報を守るため、すべての従業員は雇用の条件としてNDAあるいは機密保持契約にサインしていますか？
		HRS-03.4			Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?	トレーニングプログラムの期限内の完了を、重要システムへのアクセスの許可、及びアクセス維持のための前提条件としていますか？
		HRS-03.5			Are personnel trained and provided with awareness programs at least once a year?	最低1年に一回、従業員にトレーニング及び認識を高めるためのプログラムを提供していますか？
Human Resources *Employment Termination* *人事* *雇用の終了*	HRS-04	HRS-04.1	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	雇用の終了もしくは雇用手続きの変更に関する役割及び責任は、明確に割り当てられ、文書化され、通知されなければならない。	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	雇用の変更及び終了を管理するためのポリシー、手続き、ガイドラインは文書化されていますか？
		HRS-04.2			Do the above procedures and guidelines account for timely revocation of access and return of assets?	上記の手続き及びガイドラインは、タイムリーなアクセス権の失効や資産の返却を含んでいますか？
Human Resources *Portable / Mobile Devices* *人事* *モバイルデバイス管理*	HRS-05	HRS-05.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	企業の資源へのモバイルデバイスからのアクセスを許可することに関連するビジネスリスクを管理するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。また、より高い保証となる補完的コントロール、実行可能なポリシー及び手順（セキュリティ訓練の義務付け、身元確認の強化、権限付与とアクセス制御、デバイス監視など）の実施が必要な場合もある。	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g. laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	ポータブルあるいはモバイル機器（たとえば、ラップトップ、携帯電話、PDA）から、機微なデータやテナントのデータへのアクセスを厳格に制限するために、ポリシーと手順が構築され、その対策が実装されていますか？これらのデバイスは、一般的に非ポータブルなデバイス（たとえば、プロバイダの組織の施設内にあるデスクトップコンピュータ）よりもリスクが高いです。
Human Resources *Nondisclosure Agreements* *人事* *守秘義務契約*	HRS-06	HRS-06.1	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	データ及び運用の詳細事項を保護するための組織のニーズに合わせて、守秘義務契約もしくは秘密保持契約に関する要求事項を特定し、文書化し、事前に定めた間隔でレビューしなければならない。	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	データ及び運用の詳細事項を保護するための組織のニーズに合わせて、守秘義務契約もしくは秘密保持契約に関する要求事項を特定し、文書化し、事前に定めた間隔でレビューしていますか？

Human Resources *Roles / Responsibilities* *人事* *ロール / 責任*	HRS-07	HRS-07.1	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	契約社員、従業員及び外部の利用者が情報資産及びセキュリティに関連している場合、その役割及び責任を文書化しなければならない。	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	プロバイダ自身の管理者責任とテナントの管理者責任を明確にしたロール定義の文書を、テナントに提供していますか？
Human Resources *Acceptable Use* *人事* *技術的に受け入れられる使用*	HRS-08	HRS-08.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	組織が所有または管理するユーザのエンドポイントデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）、IT基盤のネットワーク及びシステムコンポーネントの使用を許可する範囲及び条件を定義するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。さらに、必要に応じて、個人のモバイルデバイス及び関連するアプリケーションを使用して企業の資源にアクセスすること（すなわち、BYOD）を許可する範囲及び条件を定義することも考慮し、適宜取り入れなければならない。	Do you provide documentation regarding how you may or access tenant data and metadata?	テナントのデータやメタデータを、どのように利用しアクセスするかについて記述した文書を提供していますか？
		HRS-08.2			Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?	インスペクション技術（検索エンジンなど）を用いて、テナントのデータ使用についてのメタデータを収集あるいは作成していますか？
		HRS-08.3			Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?	インスペクション技術を通してテナントのデータ/メタデータにアクセスすることを、テナントが拒否（opt out）できますか？
Human Resources *Training / Awareness* *人事* *トレーニング / 認識向上*	HRS-09	HRS-09.1	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	組織のすべての契約社員、外部の利用者、従業員に対してセキュリティ意識向上の訓練プログラムを策定し、必要に応じて義務付けなければならない。組織のデータにアクセスするすべての個人は、組織に関係する専門的機能に関連する組織の手順、プロセス、ポリシーについての意識の向上及び定期的更新のために有用な訓練を受けなければならない。	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?	テナントのデータにアクセスするすべての人に対して、クラウドに関連したアクセスの問題やデータ管理の問題（たとえば、マルチテナント、国籍、クラウド展開モデル、職務の分離、利害の含意と対立）についての正式でロールベースのセキュリティ意識向上のトレーニングプログラムを用意していますか？
		HRS-09.2			Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	管理者やデータスチュワード（データ責任者）は、セキュリティとデータの完全性に関する法的な責任の教育を受けていますか？
Human Resources *User Responsibility* *人事* *ユーザ責任*	HRS-10	HRS-10.1	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	すべての人員に、以下の事項に対する自身の役割及び責任を認識させなければならない。 -設定されたポリシー、手順、適用される法律上または規則上の遵守義務に対する認識及びコンプライアンスを維持すること -安全でセキュアな作業環境を維持すること	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	ユーザに対して、公開されているセキュリティポリシー、手続き、標準、適切な規則上の要求を継続的に認識し、遵守する責任をもっていることを周知していますか？
		HRS-10.2			Are users made aware of their responsibilities for maintaining a safe and secure working environment?	ユーザに対して、安全でセキュアな作業環境を維持するための責任をもっていることを周知していますか？
		HRS-10.3			Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?	ユーザに対して、操作員のいない状態の機器が安全な方法で運用されていることに対する責任を持っていることを周知していますか？
Human Resources *Workspace* *人事* *ワークスペース*	HRS-11	HRS-11.1	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions had been disabled after an established period of inactivity.	無人の作業場所で、機微な文書が（デスクトップ上などで）閲覧可能な状態に置かれないようにするため、また、一定時間使用されない場合にユーザのセッションが無効になるようにするために、ポリシー及び手順を確立しなければならない。	Do your data management policies and procedures address tenant and service level conflicts of interests?	データ管理ポリシーと手続きは、テナントとサービスレベルの利害関係の不整合に対応していますか？
		HRS-11.2			Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?	データ管理ポリシーと手続きは、テナントデータに対する権限のないアクセスに対応するための監査ログ改ざん検知、あるいはソフトウエア完全性チェック機能を含めていますか？
		HRS-11.3			Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?	仮想マシン管理基盤は、仮想マシンの作成/構成の不正な変更を検出するための監査ログ改ざん検知、あるいはソフトウエア完全性チェック機能を含めていますか？
Identity & Access Management *Audit Tools Access* *アイデンティティとアクセス管理* *監査ツールアクセス*	IAM-01	IAM-01.1	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	ログデータが改ざんされたり悪用されたりすることのないように、組織の情報システムとやり取りをする監査ツールへのアクセス及び使用については適切な隔離や取扱い制限を行わなければならない。	Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	情報セキュリティ管理システムへのアクセスを制限し、ログを取り、モニターしていますか？(たとえば、ハイパバイザ、ファイアウォール、脆弱性スキャナー、ネットワークスニファー、APIなど)
		IAM-01.2			Do you monitor and log privileged access (administrator level) to information security management systems?	情報セキュリティ管理システムへの特権アクセス（管理者レベル）をモニターしログを取っていますか？

Identity & Access Management **Credential Lifecycle / Provision Management** **アイデンティティとアクセス管理** **資格証明のライフサイクル / プロビジョニング管理**	IAM-02	IAM-02.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	データや組織が所有または管理する実/仮想アプリケーションインタフェース、IT基盤のネットワーク及びシステムコンポーネントにアクセスするすべての社内及び顧客（テナント）ユーザの適切な身元確認、権限付与、アクセス管理を確実に行うために、ユーザアクセスのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。これらのポリシー、手順、プロセス及び手段には、以下の事項を含めなければならない。 ・職務機能（社内従業員及び臨時従業員の変更、顧客管理によるアクセス、仕入れ先との取引関係、その他の第三者との取引関係など）に基づき最少権限付与原則に沿って定められた、ユーザアカウントの権限付与及び解除を行うための手順ならびにその基準となる役割ならびに職責 ・ビジネスケースを考慮した、より高度の保証及び多要素認証用秘密情報の配備（たとえば、管理インタフェース、鍵生成の機能、リモートアクセスなどを利用する場合、職務権限分離の確実な実施、緊急アクセスを行う場合、大規模なリソースを必要とするプロビジニングや地理的に分散した配備を行うような場合、重要なシステムへの人員の冗長配置の場合など） ・マルチテナントアーキテクチャにおける、それぞれのサードパーティー（プロバイダや他のテナントなど）ごとの、データ及びセッションに対するアクセスの隔離に関する事項 ・IDの信用性確認、サービス間連携アプリケーション（API）と情報処理の相互運用性（たとえばSSOと認証フェデレーションなどについてのもの）に関する事項 •インスタンス化から破棄に至るまでのアカウント認証用情報のライフサイクル管理に関する事項 ・アカウントの認証用情報及びID記憶の最小化または再利用（可能な場合）に関する事項 ・データ及びセッションへのアクセスのための認証、許可、アカウンティング（AAA）ルールに関する事項（たとえば暗号化、強力かつマルチファクターの期限付き非共有の認証シークレットを使用するといった規則） ・データ及びセッションへのアクセスのための認証、許可、アカウンティング（AAA）ルールを、顧客（テナント）自身が管理するための許可範囲及び提供する補助機能に関する事項 ・該当する法律または規制遵守の要求事項への準拠に関する事項れのサードパーティー（プロバイダや他のテナントなど）ごとの、データ及びセッションに対するアクセスの隔離に関する事項 ・IDの信用性確認、サービス間連携アプリケーション（API）と情報処理の相互運用性（たとえばSSOと認証フェデレーションなどについてのもの）に関する事項 •インスタンス化から破棄に至るまでのアカウント資格情報のライフサイクル管理に関する事項 ・アカウントの資格情報及びID記憶の最小化又は再利用（可能な場合）に関する事項 ・データ及びセッションへのアクセスのための認証、許可、アカウンティング（AAA）ルールに関する事項（たとえば暗号化、強力かつマルチファクターの期限付き非共有の認証シークレットを使用するといった規	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	ビジネスの目的のためにすでに必要のないシステムへのアクセスをタイムリーに削除していますか？
		IAM-02.2			Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?	ビジネスの目的のためにすでに必要のないシステムへのアクセスを削除するのにかかる時間を追跡できる計測手段を提供していますか？
Identity & Access Management *Diagnostic / Configuration Ports Access* *アイデンティティとアクセス管理* *診断 / 設定ポートアクセス*	IAM-03	IAM-03.1	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	診断ポート及び設定ポートへのユーザアクセスはその権限を付与された担当者及びアプリケーションに限定しなければならない。	Do you use dedicated secure networks to provide management access to your cloud service infrastructure?	クラウドサービス基盤への管理用のアクセスを提供するため、独立した安全なネットワークを利用していますか？
Identity & Access Management *Policies and Procedures* *アイデンティティとアクセス管理* *ポリシーと手順*	IAM-04	IAM-04.1	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	ITインフラストラクチャーにアクセスするすべての人に関するID情報を保管し管理し、個人のアクセスレベルを決定するためのポリシー及び手順を確立しなければならない。ユーザのIDに基づいてネットワーク資源へのアクセスを制御するためのポリシーも確立しなければならない。	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	ITインフラストラクチャーにアクセスするすべての人に関する個人のアクセスレベルを含むID情報を保管し管理していますか？
		IAM-04.2			Do you manage and store the user identity of all personnel who have network access, including their level of access?	ネットワーク資源へアクセスするユーザの個人のアクセスレベルを含むID情報を管理していますか？
Identity & Access Management *Segregation of Duties* *アイデンティティとアクセス管理* *職務の分離*	IAM-05	IAM-05.1	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	ユーザロールの競合に関連する事業リスクに対処することを目的として規定された職務の分離方針に応じてユーザアクセスを制限するために、ユーザアクセスポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	クラウドサービスの提供において、職務の分離がどのように維持されているかについて、テナントに文書で提供していますか？

Identity & Access Management *Source Code Access Restriction* *アイデンティティとアクセス管理* *ソースコードアクセス制限*	IAM-06	IAM-06.1	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	定められたユーザアクセスのポリシー及び手順に基づいて、職務に応じた最小権限付与原則に従い、組織自身が開発したアプリケーション、プログラム、オブジェクトソースコード、その他の知的財産（IP）へのアクセス及び自社開発のソフトウェアの使用を適切に制限しなければならない。	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	プロバイダのアプリケーション、プログラム、オブジェクトソースコードへの承認されてないアクセスを防止するコントロールができていますか？また、承認された人のみに制限されていることを保証していますか？
		IAM-06.2			Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	テナントのアプリケーション、プログラム、オブジェクトソースコードへの承認されてないアクセスを防止するコントロールができていますか？また、承認された人のみに制限されていることを保証していますか？
Identity & Access Management *Third Party Access* *アイデンティティとアクセス管理* *第三者アクセス*	IAM-07	IAM-07.1	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	組織の情報システム及びデータへの第三者のアクセスを必要とする業務プロセスで発生するリスクを特定、評価、優先順位付けした後、権限のないまたは不適切なアクセスの発生可能性及び影響度を最小限に抑え、監視し、測定するために、それに対応できるリソースを投入しなければならない。 リスク分析から導き出されるリスクに対応した管理策は（第三者に）アクセスを提供する前に実装されなければならない。	Do you provide multi-failure disaster recovery capability?	複数の障害に対する災害復旧機能（体制？）を提供していますか？
		IAM-07.2			Do you monitor service continuity with upstream providers in the event of provider failure?	上流のプロバイダのサービス障害に際してのサービス継続性能力を継続的にモニターしていますか？
		IAM-07.3			Do you have more than one provider for each service you depend on?	外部依存している各々のサービスにおいて、サービスを提供することができる複数のプロバイダを持っていますか？
		IAM-07.4			Do you provide access to operational redundancy and continuity summaries, including the services you depend on?	外部依存しているサービスを含め、運用の冗長性と継続性についての概要情報に（顧客が）アクセスできるようにしていますか？
		IAM-07.5			Do you provide the tenant the ability to declare a disaster?	テナントが災害を通知する方法を提供していますか？
		IAM-07.6			Do you provided a tenant-triggered failover option?	テナントがフェールオーバオプションを開始できる方法を提供していますか？
		IAM-07.7			Do you share your business continuity and redundancy plans with your tenants?	事業継続性と冗長性の計画をテナントに提供していますか？
Identity & Access Management **Trusted Sources** **アイデンティティとアクセス管理** **信頼された発行元**	IAM-08	IAM-08.1	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	認証に用いられるID（本人識別情報）の保存及びアクセスの許容範囲に関するポリシーと手順を定め、ID（本人識別情報）へのアクセスは、業務上必要と明確に認められたユーザのみを対象とした最小権限の原則と複製制限に基づき管理されなければならない。	Do you document how you grant and approve access to tenant data?	どのようにテナントのデータへのアクセス権の付与と許可を行っているかについて文書化していますか？
		IAM-08.2			Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?	アクセス制御のため、データ分類方法についてプロバイダとテナントの間で調整する方法を用意していますか？
Identity & Access Management *User Access Authorization* *アイデンティティとアクセス管理* *ユーザアクセス権限*	IAM-09	IAM-09.1	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part of the service and/or customer (tenant) has some shared responsibility over implementation of control.	データや組織が所有または管理する実/仮想アプリケーション、基幹システム、ネットワークコンポーネントへのユーザアクセス（従業員、契約社員、顧客（テナント）、事業パートナー、供給者関係など）の提供は、アクセスが許可される前に組織の管理者によって承認され、定められたポリシーや手順に従って適切に制限されていなければならない。 プロバイダは、要求に応じて、特に顧客（テナント）のデータがサービスの一部として利用されたり、顧客（テナント）が管理策の実装に対する責任の一部を共有したりしている場合は、このユーザアクセス提供を顧客（テナント）に通知しなければならない。	Does your management provision the authorization and restrictions for user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	組織の管理者は、データや組織が所有又は管理する（実/仮想）アプリケーション、基幹システム、ネットワークコンポーネントへアクセスする前に、ユーザアクセス（従業員、委託先、顧客（テナント）、事業パートナー、供給者関係）を、許可し、また適切に制限していますか？
		IAM-09.2			Do your provide upon request user access (e.g. employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	貴社は、データや組織が所有又は管理する（実/仮想）アプリケーション、基幹システム、ネットワークコンポーネントへのユーザアクセス（従業員、委託先、顧客（テナント）、事業パートナー、供給者関係）を、要求に応じて提供していますか？
Identity & Access Management *User Access Reviews* *アイデンティティとアクセス管理* *ユーザアクセスレ*	IAM-10	IAM-10.1	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow	ユーザアクセスは、その権限付与の妥当性について、組織の事業責任者もしくは責任ある立場の役割または機能をもつ者により、組織が職務機能に基づく最小権限の原則に従っていることを表す証拠に基づいて、定期的に再評価し、承認を受けなければならない。アクセス違反が特定された場合、定められたユーザアクセスのポリシー及び手順に従って改善措置を実施しなければならない。	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	少なくとも1年に一度、すべてのシステムユーザ及び管理者に対して権限の確認を行っていますか？（テナントが管理しているユーザを除く）
		IAM-10.2			If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?	ユーザが不適切な権限を持っていることが判明した場合には、すべての改善措置と証明の作業は記録されますか？

ビュー		IAM-10.3	established user access policies and procedures.		Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?	不適切なアクセス権がテナントのデータに対して許可されている場合、テナントとの間でユーザ権限の改善措置し証明の報告を共有していますか？
Identity & Access Management *User Access Revocation* *アイデンティティとアクセス管理* *ユーザアクセス取り消し*	IAM-11	IAM-11.1	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	定められたポリシー及び手順に従い、ユーザのステータスの変更（雇用またはその他の取引関係の終了、職務の変更または転任など）に対応して、データや組織が所有または管理する実/仮想アプリケーション、インフラストラクチャーシステム、ネットワークコンポーネントへのユーザアクセス権限の取り消し（解除または変更）を適時に行わなければならない。プロバイダは、要求に応じて、特に顧客（テナント）データがサービスの一部として利用されたり、顧客（テナント）が管理の実施に対する責任の一部を共有したりしている場合は、これらの変更を顧客（テナント）に通知しなければならない。	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?	従業員、委託先、顧客、ビジネスパートナー、サードパーティーにおけるステータスの変更が発生した場合、組織のシステム、情報資産、データに対するユーザのアクセス権の適時な権限の終了、取消し、修正が行える仕組みを整えていますか？
		IAM-11.2			Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	ステータスの変更は、雇用関係の終了、契約、合意、雇用の変更、組織内の移動を含んでいますか？
Identity & Access Management *User ID Credentials* *アイデンティティとアクセス管理* *ユーザID 認証*	IAM-12	IAM-12.1	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	適切な本人確認、権限付与、アクセス管理を確実に実施するため、定められたポリシー及び手順に従って、内部で管理する自社または顧客（テナント）のユーザアカウントの資格情報を、以下に示すような視点から、適切に制限しなければならない。 ·IDの信用性確認、サービス間連携アプリケーション（API）と情報処理の相互運用性（SSOと認証フェデレーションの場合など） · 作成から破棄に至るまでのアカウント資格情報のライフサイクル管理 ·アカウントの資格情報及びIDストアの最小化または再利用（実現可能な場合） ·業界に広く受け入れられる標準方式や法規制を遵守した認証、許可、アカウンティング（AAA）ルール（たとえば、強力かつマルチファクター、期限設定、非共有の認証秘密情報使用など）	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	サービスに対して、既存の顧客ベースのシングルサインオン(SSO)の利用あるいは統合をサポートしていますか？
		IAM-12.2			Do you use open standards to delegate authentication capabilities to your tenants?	テナントへの承認権限の委譲に対して、オープン標準を使用していますか？
		IAM-12.3			Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	ユーザの認証、許可の手段として、アイデンティティ連携標準（SAML, SPML, WS-Federeation など）をサポートしていますか？
		IAM-12.4			Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	ユーザアクセスに対して地域の法律や行政上の制限を行うために、ポリシーの実行点Policy Enforcement Point(たとえば、XACML)機能を用意していますか？
		IAM-12.5			Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	データに対して、ロールベース及びコンテキストベースの権利を可能にするID管理システム（テナントのデータのクラス分けを可能にする）を持っていますか？
		IAM-12.6			Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?	テナントに対して、ユーザアクセスのための強固な（マルチファクター）認証オプション（デジタル証明書、トークン、生体認証など）を提供していますか？
		IAM-12.7			Do you allow tenants to use third-party identity assurance services?	テナントに対して、サードパーティのID保証サービスの利用を許可していますか？
		IAM-12.8			Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?	パスワード（最短の長さ、寿命、履歴、複雑さ）とアカウントロックアウト（ロックアウト閾値、ロックアウト期間）のポリシーの強制適用をサポートしていますか？
		IAM-12.9			Do you allow tenants/customers to define password and account lockout policies for their accounts?	テナント/顧客が、アカウントのパスワード及びアカウントロックアウトポリシーを定義することを許可しますか？
		IAM-12.10			Do you support the ability to force password changes upon first logon?	最初のログオン時にパスワードの変更を強制する機能を提供していますか？
		IAM-12.11			Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	ロックアウトされたアカウントを解除するための機能を持っていますか？（たとえば、emailによるセルフサービス、定義されたチャレンジ質問、手動による解除）
Identity & Access Management *Utility Programs Access* *アイデンティティとアクセス管理* *ユーティリティプログラムアクセス*	IAM-13	IAM-13.1	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	システム、オブジェクト、ネットワーク、仮想マシン、アプリケーション制御を無効にする可能性のあるユーティリティプログラムは、使用を制限しなければならない。	Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?	仮想化されたパーティションをきちんと管理することができるユーティリティ（たとえば、シャットダウン、クローンなど）は、的確に制限されモニターされていますか？
		IAM-13.2			Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?	仮想基盤を直接目標とする攻撃（たとえば、shimming, Blue Pill, Hyper jumpingなど）を検知することはできますか？
		IAM-13.3			Are attacks that target the virtual infrastructure prevented with technical controls?	仮想基盤を直接目標とする攻撃は、技術的な管理を用いて防ぐことができますか？
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection* *インフラと仮想化のセキュリティ* *監査ログ / 侵入検知*	IVS-01	IVS-01.1	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	適用される法令もしくは規則に対する遵守義務を果たし、疑わしいネットワークの動作やファイルの不整合について、特定のユーザアクセスに起因することを説明できるようにし、セキュリティ違反の事態が生じた際のフォレンジック調査をサポートするために、監査ログに関する保護、保持、ライフサイクル管理を高いレベルで実現しなければならない。	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	インシデントに対するタイムリーな検出、ルート個—図分析による調査、対応のために、ファイル完全性保持（ホスト）ツールとネットワーク侵入防御(IDS)ツールは、実装されていますか？
		IVS-01.2			Is physical and logical user access to audit logs restricted to authorized personnel?	監査ログへの物理的及び論理的ユーザアクセスは、承認された人のみに制限されていますか？
		IVS-01.3			Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?	（貴システムの）コントロール（管理体系）、アーキテクチャ、プロセスに対する規制や標準のマッピングがデューデリジェンスに基づいて行われているという証拠を提供できますか？
		IVS-01.4			Are audit logs centrally stored and retained?	監査ログは、集中して保存され維持されていますか？
		IVS-01.5			Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	監査ログは、セキュリティ関連事象に関して定期的にレビューされていますか（たとえば、自動ツールを使用して）？
Infrastructure & Virtualization Security *Change Detection* *インフラと仮想化のセキュリティ* *変更検知*	IVS-02	IVS-02.1	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	プロバイダは、すべての仮想マシンイメージの完全性を常に確認しなければならない。仮想マシンイメージに対して行われた変更は、その実行状態（待機時、停止時、実行中など）に関係なく、すべて記録し、注意喚起をしなければならない。イメージの変更または移動とその後のイメージの完全性の確認の結果は、電子的手段（ポータル、アラートなど）によって顧客がすぐ得られるようにしなければならない。	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g. dormant, off or running)?	仮想マシンイメージに対して行われた変更は、その実行状態（待機時、停止時、実行中など）に関係なく、すべて記録し注意喚起をうながしていますか？

		IVS-02.2			Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g. portals or alerts)?	仮想マシンの変更又はイメージの移動とその後のイメージの完全性の確認の結果は、電子的手段（ポータル、アラートなど）によって顧客が直ちに得られるようになっていますか？
Infrastructure & Virtualization Security *Clock Synchronization インフラと仮想化のセキュリティ 時間同期*	IVS-03	IVS-03.1	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	活動を時系列に追跡及び再現できるよう、すべての関連する情報処理システムのシステム時刻を同期するために、互いに合意された信頼できる外部の時刻発生源を使用しなければならない。	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	全てのシステムが同じ時間を参照するように、同期した時間サービスプロトコル（たとえば、NTP）を使用していますか？
Infrastructure & Virtualization Security Information System Documentation インフラと仮想化のセキュリティ 情報システム文書	IVS-04	IVS-04.1	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	法的及び規制上の遵守義務に従って、必要なシステム性能を実現するために、可用性、品質、適切な容量及び資源を計画し、準備し、測定しなければならない。システムの過負荷のリスクを軽減するために、将来必要な容量を予測しなければならない。	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	システム（ネットワーク、ストレージ、メモリ、I/Oなど）のオーバーサブスクリプションのレベル、発生した状況／シナリオについて記述したドキュメントを提供していますか？
		IVS-04.2			Do you restrict use of the memory oversubscription capabilities present in the hypervisor?	ハイパーバイザ上で、メモリのオーバーサブスクリプション機能の利用を制限していますか？
		IVS-04.3			Do your system capacity requirements take into account current, projected and anticipated capacity needs for all systems used to provide services to the tenants?	テナントにサービスを提供するすべてのシステムに対して、現在の容量、計画されている容量、予想容量を考慮したシステム容量要件になっていますか？
		IVS-04.4			Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?	システムのパフォーマンスは、テナントに提供しているサービスに使用されるすべてのシステムに対して、規制、契約、ビジネス要求に継続的に見あうようにモニターされ調整されていますか？
Infrastructure & Virtualization Security *Management - Vulnerability Management インフラと仮想化のセキュリティ 管理 - 脆弱性管理*	IVS-05	IVS-05.1	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	実装者は、セキュリティ脆弱性の評価ツールまたはサービスが、使用される仮想化技術に対応していることを確実にしなければならない。（すなわち仮想化対応）	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g. virtualization aware)?	脆弱性の評価ツール又はサービスが、使用される仮想化技術に対応していますか？（仮想化対応能力の有無）
Infrastructure & Virtualization Security *Network Security インフラと仮想化のセキュリティ ネットワークセキュリティ*	IVS-06	IVS-06.1	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, these configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and compensating controls.	ネットワーク環境及び仮想マシンは、信頼できるネットワークと信頼できないネットワーク接続間のトラフィックを制限し監視するよう設計し構成されなければならず、また定期的な見直しを必要とする。これらの構成は、少なくとも年一回レビューされなければならない。そして、これらは、すべての許可されているサービス、プロトコル、ポートについて、それらの使用を正当化する文書と、補完的コントロールによってサポートされなければならない。	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	IaaS提供において、貴社の仮想化ソリューションを用いて、階層化されたセキュリティアーキテクチャと同等の環境をどのように構築するかのガイダンスを、顧客に提供していますか？
		IVS-06.2			Do you regularly update network architecture diagrams that include data flows between security domains/zones?	セキュリティドメイン/ゾーンの間のデータの流れを含んだネットワークダイアグラムを定期的にアップデートしていますか？
		IVS-06.3			Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?	ネットワークにおいて、セキュリティドメイン/ゾーン間のアクセス/接続性（たとえば、ファイアウォールのルール）の許容値の妥当性を定期的にレビューしていますか？
		IVS-06.4			Are all firewall access control lists documented with business justification?	全てのファイアーウオールのアクセスコントロールリストは、業務上の必要性について記述してありますか？
Infrastructure & Virtualization Security *OS Hardening and Base Conrols インフラと仮想化のセキュリティ OS 堅牢性と基本管理*	IVS-07	IVS-07.1	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	各オペレーティングシステムは、業務に必要十分なポート、プロトコル、サービスのみを提供するように強化されねばならず、また、あらかじめ用意された技術的管理策、たとえばウイルス対策やファイル整合性モニタ（ファイルハッシュチェック）やログ収集ツールなどを、基本となる運用上の確立された標準またはテンプレートの一部として持っていなくてはならない。	Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?	オペレーティングシステムは、OSの基本ビルド標準またはテンプレートの一環として、技術的管理策（つまり、ウイルス対策、ファイル整合性モニター、ロギング）を用いて、ビジネスニーズに合致したポート、プロトコル、サービスのみを提供するように強化されていますか？
Infrastructure & Virtualization Security *Production / Nonproduction Environments インフラと仮想化のセキュリティ 本番 / テスト環境*	IVS-08	IVS-08.1	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	情報資産への権限のないアクセスまたは変更を防ぐために、本番環境とテスト環境を分離しなければならない。環境の分離は、次の内容を含む： ステートフルインスペクション機能を持ったファイアウォール、ドメイン/レルム認証ソース、及び職務として環境に個人的にアクセスするための明確な職務の分離。	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	SaaSあるいはPaaS提供において、本番環境とテストプロセス環境とを別の環境としてテナントに提供していますか？
		IVS-08.2			For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?	IaaS提供において、望ましい本番環境とテスト環境をどのように作成するかのガイダンスを提供していますか？
		IVS-08.3			Do you logically and physically segregate production and non-production environments?	本番環境と非本番環境を論理的にかつ物理的に分離していますか？
Infrastructure & Virtualization Security *Segmentation インフラと仮想化のセキュリティ 区分*	IVS-09	IVS-09.1	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	複数組織（マルチテナント）が所有または管理する実/仮想アプリケーション、基盤システム、ネットワークコンポーネントは、プロバイダや特定（テナント）ユーザによるアクセスが他の（テナント）ユーザと適切に分離されるよう、以下の事項に基づいて設計し、開発し、導入し、設定しなければならない： ・定められたポリシー及び手順 ・より強固な内部統制と高レベルの保証を確実にさせることによる、事業上の重要資産、ユーザの機微データ、セッションの隔離 ・法的及び規制上の遵守義務への準拠	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	ビジネスと顧客のセキュリティ要求を保証するため、システム及びネットワーク環境をファイアウォールか仮想ファイアウォールで保護していますか？
		IVS-09.2			Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?	法律上、規則上、契約上の要求を保証するため、システム及びネットワーク環境をファイアウォールか仮想ファイアウォールで保護していますか？
		IVS-09.3			Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?	本番環境と非本番環境の分離を保証するため、システム及びネットワーク環境をファイアウォールか仮想ファイアウォールで保護していますか？
		IVS-09.4			Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	機微のデータの保護及び隔離を保証するため、システム及びネットワーク環境をファイアウォールか仮想ファイアウォールで保護していますか？
Infrastructure & Virtualization Security *VM Security - vMotion Data Protection インフラと仮想化のセキュリティ VM セキュリティ - Vmotion データ保護*	IVS-10	IVS-10.1	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	物理サーバ、アプリケーションまたはデータを仮想サーバに移行させる場合には、安全で暗号化された通信回線を使用しなければならない。また、このような移行には、可能な場合、本番用のネットワークから分離された作業用のネットワークを使用しなければならない。	Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?	物理サーバ、アプリケーション又はデータを仮想サーバに移行させる場合に、安全で暗号化された通信回線を使用していますか？
		IVS-10.2			Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?	物理サーバ、アプリケーション又はデータを仮想サーバに移動させる場合に、本番用のネットワークから分離されたネットワークを使用していますか？

Infrastructure & Virtualization Security *VMM Security - Hypervisor Hardening* *インフラと仮想化のセキュリティ* *VMM セキュリティ - ハイパバイザ堅牢性*	IVS-11	IVS-11.1	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	ハイパーバイザー管理機能または仮想システムをホストするシステムの管理コンソールへのアクセスは、最小権限の原則に基づいて担当者が制限され、技術的管理策（二要素認証、監査証跡の取得、IPアドレスのフィルタリング、ファイアウォール、管理コンソールに対するTLSで保護された通信など）によって担保されなければならない。	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g. two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	仮想システムをホストするシステムに対するすべてのハイパーバイザー管理機能又は管理コンソールへの人によるアクセスは、最小権限の原則に基づいて制限され、技術的管理策（二要素認証、監査証跡の取得、IPアドレスのフィルタリング、ファイアウォール、管理コンソールに対するTLSで保護された通信など）によってサポートされていますか？
Infrastructure & Virtualization Security *Wireless Security* *インフラと仮想化のセキュリティ* *ワイヤレスセキュリティ*	IVS-12	IVS-12.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	ワイヤレスネットワーク環境を保護するためのポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。これには以下の事項を含む。 ・権限のないトラフィックを制限するために、境界にファイアウォールを導入し設定する ・認証及び送信用の強力な暗号化を装備したセキュリティ設定で、ベンダのデフォルト設定を置き換える（暗号鍵、パスワード、SNMP通信など） ・ワイヤレスネットワークデバイスへのユーザアクセスを権限のある人に制限する ・権限のない（不正な）ワイヤレスネットワークデバイスの存在を検出し、適宜ネットワークから切断する	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	ワイヤレスネットワーク環境の境界を保護し承認されていないワイヤレストラフィックを制限するためのポリシーと手順が構築され、そのためのメカニズムが構成され実装されていますか？
		IVS-12.2			Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)	ワイヤレスセキュリティ設定においてベンダーによるデフォルトの設定を置き換えて、認証と伝送のための強固な暗号化を確実に有効にするために、ポリシーと手順が構築され、そのためのメカニズムが実装されていますか？（たとえば、暗号鍵、パスワード、SNMP通信ストリングなど）
		IVS-12.3			Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	ワイヤレスネットワーク環境を保護し、承認されていない(不正な)ネットワークデバイスを検出しタイムリーにネットワークから隔離するためのポリシーと手順が構築され、そのためのメカニズムが実装されていますか？
Infrastructure & Virtualization Security *Network Architecture* *インフラと仮想化のセキュリティ* *ネットワークアーキテクチャ*	IVS-13	IVS-13.1	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	ネットワーク構成図は、法規制上のコンプライアンスに影響する可能性のある高リスクの環境やデータの流れを識別し明示しなければならない。技術的対策を実装し、多層防御技術（たとえば、パケットの詳細分析、トラフィック制限、ハニーネットなど）を適用して、異常な内向きまたは外向きの通信パターン（たとえばMACアドレス詐称やARPポイズニング攻撃）や分散サービス妨害（DDoS）攻撃などのネットワークベースの攻撃を検知し速やかに対処しなければならない。	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	ネットワーク構成図は、法規制上のコンプライアンスに影響する可能性のある高リスクの環境やデータの流れを明示していますか？
		IVS-13.2			Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	技術的対策を実装し、多層防御技術（たとえば、パケットの詳細分析、トラフィック制御、ブラックホール）を適用し、異常な内向き及び外向きの通信パターン（たとえばMACアドレス詐称やARPポイズニング攻撃）や分散サービス妨害（DDoS）攻撃などのネットワークベースの攻撃を検知し速やかに対処していますか？
Interoperability & Portability *APIs* *相互運用性と移植容易性* *API*	IPY-01	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	コンポーネント間の相互運用性を最大限にサポートし、アプリケーションの移行を実現するために、プロバイダは、オープンで一般に公開されているAPIを使用しなければならない。	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	サービスにおいて利用可能なすべてのAPIのリストを開示し、どれが標準でどれが個別のものかを明示していますか？
Interoperability & Portability *Data Request* *相互運用性と移植容易性* *データ要求*	IPY-02	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	すべての構造化及び非構造化データを顧客が利用できるように、要求に応じて業界標準の形式（.doc、.xls、.pdf、ログ、フラットファイル）で提供しなければならない。	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	顧客の非構造化データは、業界標準の形式（たとえば、.doc, .xls, .pdfの）で利用できますか？
Interoperability & Portability *Policy & Legal* *相互運用性と移植容易性* *ポリシーと法律*	IPY-03	IPY-03.1	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage and integrity persistence.	ポリシー、手順、相互に合意した条項/条件を確立し、サービス間連携アプリケーション（API）、情報処理の相互運用性、及びアプリケーション開発と情報の交換・使用・完全性保持における移植容易性に対する顧客（テナント）の要求事項を満たさなければならない。	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?	貴社のサービスとサードパーティのアプリケーションの間の相互運用性を実現するAPIの使用について、規定するポリシーや手順（サービスレベル契約）を定めていますか？
		IPY-03.2			Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	貴社のサービスとの間のアプリケーションデータの移動（双方向）について規定するポリシーや手順（サービスレベル契約）を定めていますか？
Interoperability & Portability *Standardized Network Protocols* *相互運用性と移植容易性* *標準ネットワークプロトコル*	IPY-04	IPY-04.1	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	プロバイダは、データのインポート及びエクスポートならびにサービス管理のために、安全な（例：暗号化、認証付き）、標準化されたネットワークプロトコルを使用し、そこに含まれる関連する相互運用性や移植容易性の標準を詳しく記述した文書を顧客（テナント）に提供しなければならない。	Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	データのインポート及びエクスポート並びにサービス管理は、安全（たとえば、非クリアテキストかつ認証済み）で、一般に受け入れられている標準プロトコルを通じて行うことができますか？
		IPY-04.2			Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?	相互運用性や移植容易性に関連するネットワークプロトコル標準の利用可能なものを記述した文書を顧客（テナント）に提供していますか？
Interoperability & Portability *Virtualization* *相互運用性と移植容易性* *仮想化*	IPY-05	IPY-05.1	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks, available for customer review.	プロバイダは、相互運用性の確保を支援するために、業界で広く認知された仮想化プラットフォーム及び標準仮想ファイル形式（OVFなど）を使用しなければならない。また、使用されているハイパーバイザーへの独自の変更やすべての（アドオン）ソリューション固有の仮想フック（ハイパーバイザー機能への介入）を文書化し、顧客がレビューできるようにしなければならない。	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	相互運用性を確保するために、業界で広く認知された仮想化プラットフォーム及び標準仮想化フォーマット（OVFなど）を使用していますか？
		IPY-05.2			Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?	使用するハイパーバイザーへの独自の変更や、ソリューション固有の仮想フックを文書化し、顧客がレビューできるようにしていますか？

Mobile Security *Anti-Malware* *モバイルセキュリティ* *アンチマルウエア*	MOS-01	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	プロバイダの情報セキュリティ意識向上訓練に、モバイルデバイス固有のマルウェア対策意識向上訓練を取り入れなければならない。	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?	情報セキュリティ意識向上訓練の一部として、モバイルデバイス固有のマルウェア対策意識向上訓練を実施していますか？
Mobile Security *Application Stores* *モバイルセキュリティ* *アプリケーションストア*	MOS-02	MOS-02	A documented list of approved application stores has been communicated as acceptable for mobile devices accessing or storing provider managed data.	プロバイダが管理するデータにアクセスし、あるいはそのデータを保存しているモバイルデバイスが利用するアプリケーションストアとして、承認されたものをリスト化し文書化する。	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?	企業データの保存や企業システムへのアクセスを行うモバイルデバイスに対して承認されている、アプリケーションストアのリストを文書化し利用できるようにしていますか？
Mobile Security *Approved Applications* *モバイルセキュリティ* *承認されたアプリケーション*	MOS-03	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	企業は、承認されていないアプリケーション、または予め確認済みのアプリケーションストア経由で入手していない承認済みアプリケーションのインストールを禁止するポリシーを文書化しておかなければならない。	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?	許可されたアプリケーション及び承認されているアプリケーションストアからのアプリケーションのみがモバイルデバイスにロードできることを保証するためのポリシー（強制）実行機能（たとえば、XACML）を持っていますか？
Mobile Security *Approved Software for BYOD* *モバイルセキュリティ* *BYOD として承認されたソフトウエア*	MOS-04	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	BYODに関するポリシー及びこれを補強する意識向上訓練において、BYODで使用可能な承認済みアプリケーション、アプリケーションストア、及びアプリケーション拡張とプラグインを明示する。	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?	BYODポリシーとトレーニングは、どのアプリケーションあるいはアプリケーションストアがBYODデバイスに許可されているかを明確に示していますか？
Mobile Security *Awareness and Training* *モバイルセキュリティ* *認知とトレーニング*	MOS-05	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	プロバイダは、モバイルデバイスの定義、及びすべてのモバイルデバイスで許容される使用法及び要求事項を記載したモバイルデバイスのポリシーを文書化しておかなければならない。プロバイダは、プロバイダのセキュリティ意識向上訓練プログラムを通じて、ポリシー及び要求事項を公表し伝達しなければならない。	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?	モバイルデバイス（の種類）及びモバイルデバイスで許容される使用法及び要求事項を明確に定義したモバイルデバイスのポリシーを従業員トレーニングの中に文書化していますか？
Mobile Security *Cloud Based Services* *モバイルセキュリティ* *クラウドベースサービス*	MOS-06	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	企業のモバイルデバイスまたはBYODで使用されるすべてのクラウドベースのサービスは、その使用法と企業の業務データの格納について、事前承認を受けなければならない。	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?	モバイルデバイスを通して企業のビジネスデータを利用、保存するために利用することが許されている、承認済みのクラウドベースのサービスの文書化されたリストがありますか？
Mobile Security *Compatibility* *モバイルセキュリティ* *互換性*	MOS-07	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	企業は、モバイルデバイス、オペレーティングシステム、アプリケーションの互換性の問題に対して検査を行うアプリケーション検証プロセスを文書化しておかなければならない。	Do you have a documented application validation process for testing device, operating system and application compatibility issues?	デバイス、オペレーティングシステム、アプリケーションの互換性の問題をテストするための文書化されたアプリケーション評価手順はありますか？
Mobile Security *Device Eligibility* *モバイルセキュリティ* *デバイスの適格性*	MOS-08	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	BYODポリシーでは、BYODの使用を許可するためにデバイス及び適格性要件を定義しなければならない。	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?	BYOD利用のために許可されるデバイス（の種類）とそのための要件を定義したBYODポリシーがありますか？
Mobile Security *Device Inventory* *モバイルセキュリティ* *デバイスの一覧表*	MOS-09	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices, (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD), will be included for each device in the inventory.	企業データを格納しこれにアクセスするのに使用されるすべてのモバイルデバイスの一覧表を保持し、更新しなければならない。一覧表の各デバイスの項目には、デバイスの状態に関するすべての変更（オペレーティングシステム及びパッチレベル、紛失または使用終了のステータス、デバイスを割当てられた人または（BYOD）デバイスの使用を承認された人など）を記載しなければならない。	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?	企業データを保存及びアクセスするすべてのモバイルデバイスの、デバイスのステータス（OSとパッチレベル、紛失あるいは廃棄、デバイス所有者）を含むインベントリリストを作成・更新していますか？
Mobile Security *Device Management* *モバイルセキュリティ* *データ管理*	MOS-10	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	顧客データを格納、送信、処理することを許可されたすべてのモバイルデバイスに対して、一元的なモバイルデバイス管理策を導入しなければならない。	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?	企業データを保存、移送、処理することが認められているすべてのモバイルデバイスに実装されている、集中管理型モバイルデバイス管理ソリューションがありますか？
Mobile Security *Encryption* *モバイルセキュリティ* *暗号化*	MOS-11	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	モバイルデバイスポリシーは、すべてのモバイルデバイスに対して、デバイス全体か、機微であると特定されたデータの暗号化を義務付け、技術的管理策によって実施しなければならない。	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?	すべてのモバイルデバイスに対して、技術的制御手段により強制適用可能な、デバイス全体あるいは機微なデータに対する暗号の使用を義務付けるモバイルデバイスポリシーがありますか？
Mobile Security *Jailbreaking and Rooting* *モバイルセキュリティ* *ジェイルブレイクとルート化*	MOS-12	MOS-12.1	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and isenforced through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	モバイルデバイスポリシーでは、モバイルデバイスに組込まれたセキュリティ対策の回避を禁止しなければならない（ジェイルブレイク、ルート化など）。この禁止は、デバイス上の検出手段及び予防的手段により、または一元的なデバイス管理システム（モバイルデバイス管理など）により、実施しなければならない。	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?	モバイルデバイスポリシーは、モバイルデバイスに組み込まれたセキュリティ対策の回避を禁止していますか（ジェイルブレイク、ルート化など）？
		MOS-12.2			Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	組み込まれたセキュリティ対策の回避を検出し予防する制御を、デバイスに実装しまたは一元的なデバイス管理システムを通じて、実施していますか？
Mobile Security *Legal* *モバイルセキュリティ* *法律*	MOS-13	MOS-13.1	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations over the loss of non-company data in the case a wipe of the device is required.	BYODポリシーでは、プライバシーの必要保護レベル、訴訟の要件、電子的証拠開示、訴訟ホールド（訴訟等に関連して関係資料・情報を保存すること）等について明確に記述しなければならない。BYODポリシーは、デバイスの全データ消去が必要になった場合の企業データ以外のデータの損失の可能性について明記する。	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery and legal holds?	BYODポリシーは、プライバシーの必要保護レベル、訴訟の要件、電子的証拠開示、訴訟ホールドについて明確に定義していますか？
		MOS-13.2			Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?	組み込まれたセキュリティ対策の回避を検出し予防する制御を、デバイスに実装しまたは一元的なデバイス管理システムを通じて、実施していますか？
Mobile Security *Lockout Screen* *モバイルセキュリティ* *ロックアウト画面*	MOS-14	MOS-14	BYOD and/or company owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	BYODや企業が所有するデバイスには、自動ロック画面を設定する。この要求事項は、技術的管理策を通じて実施されなければならない。	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?	BYODや企業が所有するデバイスに対して、自動ロック式スクリーンを義務付け、技術的強制手段により実施していますか？
Mobile Security *Operating Systems* *モバイルセキュリティ* *オペレーティングシステム*	MOS-15	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	企業の変更管理プロセスを通じて、モバイルデバイスのオペレーティングシステム、パッチレベル、アプリケーションに対する変更を管理しなければならない。	Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?	企業の変更管理プロセスを通じて、モバイルデバイスのオペレーティングシステムに対するすべての変更、パッチレベル、アプリケーションを管理していますか？

Mobile Security *Passwords* *モバイル セキュリティ* *パスワード*	MOS-16	MOS-16.1	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	企業のすべてのデバイスまたはBYODでの使用が認められたデバイスに対するパスワードポリシーは、文書化し、技術的管理策を通じて実施されなければならない。このポリシーは、パスワードや暗証番号（PIN）の長さの変更、認証の要件の変更を禁じなければならない。	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?	企業のすべてのモバイルデバイス又はBYODモバイルデバイスに、パスワードポリシーがありますか？
		MOS-16.2			Are your password policies enforced through technical controls (i.e. MDM)?	パスワードポリシーは、技術的管理策を通じて強制適用されていますか（すなわち、MDM）？
		MOS-16.3			Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?	パスワードポリシーは、モバイルデバイスを通した認証要求の変更（すなわち、パスワード/PINの長さ）を禁止していますか？
Mobile Security *Policy* *モバイル セキュリティ* *ポリシー*	MOS-17	MOS-17.1	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	モバイルデバイスのポリシーでは、BYODのユーザに、データのバックアップの実行を要求し、未承認のアプリケーションストアの使用を禁じ、マルウェア対策ソフトウェアの使用（サポートされている場合）を要求しなければならない。	Do you have a policy that requires BYOD users to perform backups of specified corporate data?	BYODユーザに、指定された企業データのバックアップを行うことを要求するポリシーがありますか？
		MOS-17.2			Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?	BYODユーザに、承認されていないアプリケーションストアの利用の禁止を義務付けるポリシーがありますか？
		MOS-17.3			Do you have a policy that requires BYOD users to use anti-malware software (where supported)?	BYODユーザに、ウイルス防御ソフトウエア（サポートされている場合）の使用を義務付けるポリシーがありますか？
Mobile Security *Remote Wipe* *モバイル セキュリティ* *リモート消去*	MOS-18	MOS-18.1	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	企業のBYODプログラムを通じて使用が許可されたすべてのモバイルデバイス、または企業が支給したモバイルデバイスでは、企業のIT統括部門によるリモート消去が許可されるか、または企業が提供するすべてのデータが企業のIT統括部門によって消去されなければならない。	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?	企業が承認したすべてのモバイル（BYOD）デバイスに対して、IT部門によるリモート消去あるいは企業データの消去を適用していますか？
		MOS-18.2			Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?	企業が支給するすべてのモバイル（BYOD）デバイスに対して、IT部門によるリモート消去あるいは企業データの消去を適用していますか？
Mobile Security *Security Patches* *モバイル セキュリティ* *セキュリティパッチ*	MOS-19	MOS-19.1	Mobile devices connecting to corporate networks or storing and accessing company information shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	企業のネットワークに接続し、企業の情報の格納保存やアクセスを行うモバイルデバイスでは、リモートでソフトウエアバージョン/パッチを確認できるようにしなければならない。デバイスメーカーまたは通信業者の一般向けリリースに応じて、すべてのモバイルデバイスに最新のセキュリティ関連パッチをインストールしなければならない。また、認証されたIT担当者はこのようなアップデートをリモートで行うことができるようにしなければならない。	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?	モバイルデバイスは、製造元あるいはキャリアの一般向けリリースがされる都度、適用可能な最新のセキュリティ関連パッチをインストールしていますか？
		MOS-19.2			Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?	モバイルデバイスは、企業のIT担当者がリモートから確認して最新のセキュリティパッチをダウンロードできるようにしていますか？
Mobile Security *Users* *モバイル セキュリティ* *ユーザ*	MOS-20	MOS-20.1	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	BYODポリシーでは、BYODとして認可されたデバイスが使用またはアクセス可能なシステム及びサーバを明記しなければならない。	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?	BYODポリシーは、BYODとして許可されたデバイスが使用又はアクセス可能なシステム及びサーバを明記していますか？
		MOS-20.2			Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?	BYODポリシーは、BYODとして許可されたデバイスを通したアクセスが認められるユーザのロールを特定していますか？
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance* *セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス* *契約 / 機関の維持*	SEF-01	SEF-01.1	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	コンプライアンスに関する司法当局との直接的な連携及び迅速な実施を必要とするフォレンジック調査の準備を整えておくために、該当する規制当局、国家及び地方の司法当局、その他の法管轄当局との連絡窓口を維持し、定期的に更新（影響を受ける適用範囲の変更、遵守義務の変更など）しなければならない。	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	契約及び関連する規制に関わりある地元の（監督）当局との、リエゾン（連絡係）と連絡窓口を維持していますか？
Security Incident Management, E-Discovery & Cloud Forensics *Incident Management* *セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス* *インシデント管理*	SEF-02	SEF-02.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	定められたITサービスマネジメントのポリシー及び手順に従って、セキュリティ関連の事象を優先順位付けし、適時かつ一貫したインシデント管理を確実に行うために、ポリシー及び手順を確立し、これらを補強するためのビジネスプロセス及び技術的対策を実装しなければならない。	Do you have a documented security incident response plan?	セキュリティインシデント対応計画は文書化されていますか？
		SEF-02.2			Do you integrate customized tenant requirements into your security incident response plans?	テナント固有の要求を、セキュリティインシデント対応計画に含めていますか？
		SEF-02.3			Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?	セキュリティインシデント発生時のあなたとあなたのテナントの間の役割と責任について明記した文書を公開していますか？
		SEF-02.4			Have you tested your security incident response plans in the last year?	前年度、セキュリティインシデント対応計画のテストを行っていますか？
Security Incident Management, E-Discovery & Cloud Forensics *Incident Reporting* *セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス* *インシデントレポーティング*	SEF-03	SEF-03.1	Workforce personnel and external business relationships shall be informed of their responsibility and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	従業員及び外部の取引関係者に自身が負うべき責任を周知しなければならない。また、要求があった場合、従業員及び外部の取引関係者は、速やかにすべての情報セキュリティ事象を報告することに同意し、または契約により合意しなければならない。情報セキュリティ事象は、適用される法令上または規制上の遵守義務に従って、速やかに事前に設定された伝達経路を通じて報告されなければならない。	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	粒度の高い解析やアラートの発信のために、セキュリティ情報イベント管理（SIEM）システムに、データソース（アプリケーションログ、IDSログ、物理的アクセスログなど）を接続していますか？
		SEF-03.2			Does your logging and monitoring framework allow isolation of an incident to specific tenants?	ロギング及びモニタリングの構成は、インシデントをテナントごとに分離するようになっていますか？
Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Legal Preparation* *セキュリティインシデント管理、E ディスカバリ、クラウドフォレンジックス* *インシデントレスポンスの法的準備*	SEF-04	SEF-04.1	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	情報セキュリティインシデントの発生後、関連する司法管轄において行われる可能性のある今後の法的措置を支援する証拠を提出するために、証拠能力の一環連続性確保（chain of custody）を含む適切なフォレンジック手続が必要である。通知に基づいて、セキュリティ違反の影響を受ける顧客や他の外部取引関係者には、法的に認められる範囲で、フォレンジック調査に参加する機会が与えられなければならない。	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	インシデント対応計画は、法的に認められた管理の連鎖プロセス及びコントロール（Chain-of-custody management processes & controls）に基づく業界標準に準拠していますか？
		SEF-04.2			Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	インシデント対応体制には、法的に認められたフォレンジックデータの収集と分析技術を含んでいますか？
		SEF-04.3			Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	他のテナントのデータを凍結せずに、特定のテナントに対する訴訟ホールド（ある時点からのデータを凍結する）を行うことができますか？
		SEF-04.4			Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	法的な召喚状に対してデータを作成する時、テナントのデータの分離を行い、また、それが正しいことを証明できますか？

Security Incident Management, E-Discovery & Cloud Forensics *Incident Response Metrics* *セキュリティインシデント管理、ｅディスカバリ、クラウドフォレンジックス* *インシデントレスポンスマトリックス*	SEF-05	SEF-05.1	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	情報セキュリティインシデントを監視し、その種類や規模、コストを定量化するような機能を導入しなければならない。	Do you monitor and quantify the types, volumes and impacts on all information security incidents?	全ての情報セキュリティインシデントのタイプ、量、インパクトをモニターし数値化していますか？
		SEF-05.2			Will you share statistical information for security incident data with your tenants upon request?	情報セキュリティインシデントの統計データを、要求に応じてテナントに提供できますか？
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity* *サプライチェーンの管理、透明性、説明責任* *データ品質と完全性*	STA-01	STA-01.1	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	プロバイダは、データ品質の欠陥と関連するリスクを収集するために、検査を行い、詳細を明らかにし、クラウドサプライチェーンパートナーとともに作業を行わなければならない。 プロバイダは、サプライチェーン内のすべての人員に対する適切な職務の分割、ロールベースのアクセス、最小権限のアクセスを通じて、データセキュリティリスクを軽減し抑制するための管理策を策定し実装しなければならない。	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?	データ品質の欠陥と関連するリスクの検査を行い、内容を開示し、クラウドサプライチェーンのパートナーとともにそれらを是正するための取組を行っていますか？
		STA-01.2			Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	サプライチェーン内のすべての人員に対する適切な職務の分割、ロールベースのアクセス、最小権限のアクセスを通じて、データセキュリティリスクを軽減し抑制するための管理策を策定し実装していますか？
Supply Chain Management, Transparency and Accountability *Incident Reporting* *サプライチェーンの管理、透明性、説明責任* *インシデントレポーティング*	STA-02	STA-02.1	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	プロバイダは、電子的手段（ポータルなど）を通じて定期的に、影響を受けるすべての顧客とプロバイダがセキュリティインシデント情報を利用できるようにしなければならない。	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals)?	電子的手段（ポータルなど）を通じて定期的に、影響を受けるすべての顧客とプロバイダがセキュリティインシデント情報を利用できるようにしていますか？
Supply Chain Management, Transparency and Accountability *Network / Infrastructure Services* *サプライチェーンの管理、透明性、説明責任* *ネットワーク / インフラストラクチャサービス*	STA-03	STA-03.1	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	相互に合意したサービス、容量の予測、ITガバナンス、サービス管理ポリシー及び手順に従って、業務上不可欠なまたは顧客（テナント）に影響する実/仮想アプリケーション及びシステム間のインタフェース（API）の設計及び設定、インフラストラクチャー基盤のネットワーク及びシステムコンポーネントを設計し、開発し、展開しなければならない。	Do you collect capacity and use data for all relevant components of your cloud service offering?	提供しているクラウドサービスのすべての関連するコンポーネントにおいて、容量及び使用状況のデータを集めていますか？
		STA-03.2			Do you provide tenants with capacity planning and use reports?	テナントに対して、容量計画及び使用状況レポートを提供していますか？
Supply Chain Management, Transparency and Accountability *Provider Internal Assessments* *サプライチェーンの管理、透明性、説明責任* *プロバイダの内部評価*	STA-04	STA-04.1	The provider shall perform annual internal assessments of conformance and effectiveness of its policies, procedures, and supporting measures and metrics.	プロバイダは、ポリシー、手順、これらをサポートする対策や基準の適合性及び有効性の内部評価を年1回実施しなければならない。	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	ポリシー、手順、及びそれをサポートする手段と計測方法について、適合性及び有効性の内部評価を年1回実施していますか？
Supply Chain Management, Transparency and Accountability *Third Party Agreements* *サプライチェーンの管理、透明性、説明責任* *サプライチェーンの合意*	STA-05	STA-05.1	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	プロバイダと顧客（テナント）とのサプライチェーンについての契約書（SLAなど）には、少なくとも、以下のような相互に合意した条項/条件を取り入れなければならない。 ・取引関係及び提供されるサービスの範囲（顧客（テナント）のデータの取得・交換・利用方法、構成テンプレート及び機能、サービス提供及びサポートに必要な人員・基盤ネットワーク・システムコンポーネント、プロバイダ及び顧客（テナント）の役割及び責任、下請け及び外部委託の取引関係、ホストされるサービスの物理的地理的位置、ならびに既知の規制上の法令遵守に関する考慮事項など） ・情報セキュリティの要求事項、プロバイダ及び顧客（テナント）の取引関係の継続期間中の主たる連絡窓口、影響を受けるすべての取引関係によるガバナンス、リスクマネジメント、保証、ならびに、法律上及び規制上の遵守義務を効果的に実行するために導入される詳細な補助的関連ビジネスプロセス及び技術的対策への言及 ・顧客（テナント）への影響力を持つプロバイダの管理下における変更の通知や事前承認 ・影響を受けるすべての顧客（テナント）その他の取引関係者（影響を受けるアップストリーム及びダウンストリームのサプライチェーン）に、セキュリティインシデント（あるいは、確認された漏えい）を適宜通知すること ・評価対象の組織に許容できないビジネスリスクが及ぶことなく、契約条項を遵守しているかどうかを評価し独立して検証すること（業界が認める認証、証明用監査報告書、その他の証明形式など） ・取引関係の終了及び影響を受ける顧客（テナント）データの処理 ・アプリケーション開発、情報の交換、使用、完全性維持を目的とする、顧客（テナント）のサービス間のアプリケーション（API）とデータの相互運用性及び可搬性の要求事項	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?	データを処理、保管、移動する国の法律に則って、委託しているプロバイダの選定及びモニタを行っていますか？
		STA-05.2			Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?	データを作成する国の法律に則って、委託先のプロバイダの選定及びモニタを行っていますか？
		STA-05.3			Does legal counsel review all third-party agreements?	すべての第三者との契約は、弁護士がレビューしていますか？
		STA-05.4			Do third-party agreements include provision for the security and protection of information and assets?	第三者との契約には、情報及び資産のセキュリティと保護に関する条項が含まれていますか？
		STA-05.5			Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	クライアントに対して、すべてのサブプロセス契約のリストとコピーを提供し、それを継続して更新していますか？
Supply Chain Management, Transparency and Accountability *Supply Chain Governance Reviews* *サプライチェーンの管理、透明性、説明責任*	STA-06	STA-06.1	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	プロバイダは、実施内容の整合性を保持し、パートナーのクラウドサプライチェーンの他のメンバーから引き継いだリスクの主な原因を明らかにするための調整を確実に行うために、パートナーのリスクマネジメント及びガバナンスプロセスをレビューしなければならない。	Do you review the risk management and governanced processes of partners to account for risks inherited from other members of that partner's supply chain?	パートナーのサプライチェーンの他のメンバーに起因するリスクに対応するため、パートナーのリスク管理及びガバナンスプロセスをレビューしていますか？
Supply Chain Management, Transparency and Accountability *Supply Chain Metrics* *サプライチェーンの管理、透明性、説明責任* *サプライチェーンマトリックス*	STA-07	STA-07.1	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	関連するサプライチェーン（上流／下流）でプロバイダと顧客（テナント）間のサービス契約（たとえば、SLA）の一貫したレビューを保証するポリシーと手順を実装しなければならない。 レビューは、少なくとも年1回行い、確立された合意事項に準拠しないことを発見しなければならない。レビューは、その結果、整合していない供給者間関係から生じるサービスレベルの不一致や不整合を発見できるように実施すべきである。	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?	プロバイダと顧客(テナント)の間の完全で正確で関連する合意内容（たとえばSLA)を維持するために、ポリシーと手順を確立し、サポートするビジネスプロセスと技術的手段を実装していますか?
		STA-07.2			Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?	サプライチェーン全体（上流／下流）にわたって、提供内容及び条件に対する不適合を計測し検知する能力がありますか？
		STA-07.3			Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?	異業種の供給者関係から生じるサービスレベルの不一致や不整合を管理できますか？

		STA-07.4			Do you review all agreements, policies and processes at least annually?	少なくとも年1回、すべての契約、ポリシー、プロセスをレビューしていますか？
Supply Chain Management, Transparency and Accountability *Third Party Assessment* *サプライチェーンの管理、透明性、説明責任* *第三者の評価*	STA-08	STA-08.1	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party providers upon which their information supply chain depends on.	プロバイダは、年次レビューを実施して、情報サプライチェーン全体で妥当な情報セキュリティが維持されることを保証しなければならない。レビューには、情報サプライチェーンに関与するすべてのパートナー/第三者プロバイダを含めなければならない。	Do you assure reasonable information security across your information supply chain by performing an annual review?	年次レビューを実施して、情報サプライチェーン全体で妥当な情報セキュリティが維持されることを保証していますか？
		STA-8.2			Does your annual review include all partners/third-party providers upon which your information supply chain depends?	年次レビューは、情報サプライチェーンに関与するすべてのパートナー/第三者プロバイダを含んでいますか？
Supply Chain Management, Transparency and Accountability *Third Party Audits* *サプライチェーンの管理、透明性、説明責任* *第三者の監査*	STA-09	STA-09.1	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	第三者のサービスプロバイダは、第三者契約に含まれる情報セキュリティ及び情報の機密性、アクセスコントロール、サービス定義、供給サービスレベル契約書を遵守していることを実証しなければならない。サービス提供の契約書への遵守状況を監督し維持するために、第三者の報告書、記録、サービスの監査及びレビューを事前に定められた間隔で実施しなければならない。	Do you permit tenants to perform independent vulnerability assessments?	テナントに対してテナント独自の脆弱性評価を許可していますか？
		STA-09.2			Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	アプリケーションとネットワークに対して、脆弱性スキャン及び定期的なペネトレーションテストを行う外部の第三者サービスがありますか？
Threat and Vulnerability Management *Antivirus / Malicious Software* *脅威と脆弱性の管理* *アンチウイルス / 悪質なソフトウエア*	TVM-01	TVM-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	組織が所有または管理するユーザのエンドポイントデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）やIT基盤のネットワーク及びシステムコンポーネントにおけるマルウェアの実行を防止するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your systems?	提供されているクラウドサービスをサポートしまたは接続しているマルウェア対策プログラムを、貴社のすべてのシステムにインストールしていますか？
		TVM-01.2			Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?	シグニチャ、リスト、振舞いパターンを使用している脅威検出システムは、すべてのインフラストラクチャコンポーネントにおいて、その分野で許容される頻度で更新されていることを保証しますか？
Threat and Vulnerability Management *Vulnerability / Patch Management* *脅威と脆弱性の管理* *脆弱性 / パッチ管理*	TVM-02	TVM-02.1	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	実装されたセキュリティコントロールの有効性を確実にするために、組織が所有 または管理するアプリケーション、IT基盤のネットワーク及びシステムコンポーネント（たとえば、ネットワーク脆弱性評価、ペネトレーションテスト）内の脆弱性を遅滞なく検出できるように、ポリシー及び手順を確立し、これらを補強するためのプロセス及び技術的対策を実装しなければならない。特定された脆弱性の改善措置を優先順位付けするためのリスクベースのモデルを使用しなければならない。変更は、すべてのベンダー提供パッチ、構成変更、あるいは組織内で開発されたソフトウエアのための変更管理プロセスを通して管理されなければならない。プロバイダは、要求に応じて、顧客（テナント）データがサービスの一部として利用されたり、顧客（テナント）が管理の実施に対する責任の一部を共有したりしている場合は、顧客（テナント）にポリシー及び手順を通知しなければならない。	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	業界における最適な方法を用いて、ネットワークレイヤの脆弱性スキャンを定期的に行っていますか？
		TVM-02.2			Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	業界における最適な方法を用いて、アプリケーションレイヤの脆弱性スキャンを定期的に行っていますか？
		TVM-02.3			Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	業界における最適な方法を用いて、ローカルなオペレーティングシステムレイヤの脆弱性スキャンを定期的に行っていますか？
		TVM-02.4			Will you make the results of vulnerability scans available to tenants at their request?	脆弱性スキャンの結果は、要求に応じてテナントが利用できるようになっていますか？
		TVM-02.5			Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?	すべてのコンピューティングデバイス、アプリケーション、システムに対して、速やかに脆弱性対策パッチを適用できる体制を整えていますか？
		TVM-02.6			Will you provide your risk-based systems patching time frames to your tenants upon request?	テナントの要求に応じて、リスクに応じたシステムのパッチの実施計画を提供していますか？
Threat and Vulnerability Management *Mobile Code* *脅威と脆弱性の管理* *モバイルコード*	TVM-03	TVM-03.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	組織が所有または管理するユーザのエンドポイントのデバイス（支給されたワークステーション、ラップトップ、モバイルデバイスなど）、IT基盤のネットワーク及びシステムコンポーネント上で、承認されていないモバイルコードが実行されるのを防止するために、ポリシー及び手順を確立し、これらを補強するための業務プロセス及び技術的対策を実装しなければならない。ここで、承認されていないモバイルコードとは、信頼できるネットワークまたは信頼できないネットワークのシステム間で転送され、受信者が明示的にインストールや実行をすることなくローカルシステム上で実行されるソフトウエアのことである。	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	モバイルコードは、インストールされ使用される前に承認されていますか？また、承認されたモバイルコードが明確に定義されたセキュリティポリシーに従って確実に運用されるように、モバイルコードの構成をチェックしていますか？
		TVM-03.2			Is all unauthorized mobile code prevented from executing?	承認されていないすべてのモバイルコードは、実行されないようになっていますか？

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ) V3.0.1 GUIDING DOCUMENT PRINCIPLES

INTENT OF THIS TAB: To assist reviewers/users of document to understand both the intent and structure of CAIQ.

GUIDING PRINCIPLES:

- Questionnaire is organized using CSA 16 governing & operating domains divided into "control areas" within CSA's Controls Matrix structure

- Questions are to assist both cloud providers in general principles of cloud security and clients in vetting cloud providers on the security of their offering and company security profile

- CAIQ is not intended to duplicate or replace existing industry security assessments but to contain questions unique or critical to the cloud computing model in each control area

- Each question should be able to be answered yes or no

- If a question can't be answered yes or no then it was separated into two or more questions to allow yes or no answers.

- Questions are intended to foster further detailed questions to provider by client specific to client's cloud security needs. This was done to limit number of questions to make the assessment feasible and since each client may have unique follow-on questions or may not be concerned with all follow-on questions.