
# 日本語公開版の提供について

本書は、Cloud Security Allianceより提供されている「Cloud Control Matrix3.0.1」の
日本語版で、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 |
|---|---|---|
| 2014年11月16日 | 日本語バージョン1.0 | |

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より参照してください。
http://cloudsecurityalliance.jp

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

| Control Domain | CCM V3.0 Control ID | Updated Control Specification | 日本語訳 |
|---|---|---|---|
| Application & Interface Security<br>Application Security<br>アプリケーションとインターフェースセキュリティ<br>アプリケーションセキュリティ | AIS-01 | 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。 |
| Application & Interface Security<br>Customer Access Requirements<br>アプリケーションとインターフェースセキュリティ<br>顧客アクセス要求 | AIS-02 | Prior to granting customers access to data, assets, and information systems, 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。 |
| Application & Interface Security<br>Data Integrity<br>アプリケーションとインターフェースセキュリティ<br>データの完全性 | AIS-03 | 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。 |
| Application & Interface Security<br>Data Security / Integrity<br>アプリケーションとインターフェースセキュリティ<br>データセキュリティ/完全性 | AIS-04 | 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, alteration, 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るポリシー及び手順を確立し維持しなければならない。 |
| Audit Assurance & Compliance<br>Audit Planning<br>監査保証とコンプライアンス<br>監査計画 | AAC-01 | 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、ビジネスプロセスの中断を把握するため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のレビューにフォーカスしなければならない。すべての監査活動は、監査を実施する前に同意を得なければならない。 |
| Audit Assurance & Compliance<br>Independent Audits<br>監査保証とコンプライアンス<br>独立した監査 | AAC-02 | 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。 |

| | | | |
|---|---|---|---|
| Audit Assurance & Compliance<br>Information System Regulatory Mapping<br>監査保証とコンプライアンス<br>情報システムに関する規制の把握 | AAC-03 | 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。 |
| Business Continuity Management & Operational Resilience<br>Business Continuity Planning<br>事業継続管理と運用レジリエンス<br>事業継続計画 | BCR-01 | 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.<br>Requirements for business continuity plans include the following:<br>• Defined purpose and scope, aligned with relevant dependencies<br>• Accessible to and understood by those who will use them<br>• Owned by a named person(s) who is responsible for their review, update, and approval<br>• Defined lines of communication, roles, and responsibilities<br>• Detailed recovery procedures, manual work-around, and reference information<br>• 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。<br>・関連する依存関係に従った目的及び範囲の定義<br>・計画の利用者が理解し利用できるようにすること<br>・(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<br>・伝達経路、役割及び責任の定義<br>・詳細な復旧の手順、手動による回避策及び参考情報<br>・計画発動の手順 |
| Business Continuity Management & Operational Resilience<br>Business Continuity Testing<br>事業継続管理と運用レジリエンス<br>事業継続テスト | BCR-02 | 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。 |
| Business Continuity Management & Operational Resilience<br>Datacenter Utilities / Environmental Conditions<br>事業継続管理と運用レジリエンス<br>データセンタのユーティリティ / 環境状態 | BCR-03 | 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。 |
| Business Continuity Management & Operational Resilience<br>Documentation<br>事業継続管理と運用レジリエンス<br>文書 | BCR-04 | Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:<br>• Configuring, installing, and operating the information system<br>• 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:<br>・情報システムの設定、インストール及び運用<br>・システムのセキュリティ機能の有効利用 |
| Business Continuity Management & Operational Resilience<br>Environmental Risks<br>事業継続管理と運用レジリエンス<br>環境リスク | BCR-05 | 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。 |
| Business Continuity Management & Operational Resilience<br>Equipment Location<br>事業継続管理と運用レジリエンス<br>機器の位置 | BCR-06 | 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。 |

| | | | |
|---|---|---|---|
| Business Continuity Management & Operational Resilience Equipment Maintenance<br>事業継続管理と運用レジリエンス<br>機器のメンテナンス | BCR-07 | 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。 |
| Business Continuity Management & Operational Resilience Equipment Power Failures<br>事業継続管理と運用レジリエンス<br>機器の停電 | BCR-08 | 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。 |
| Business Continuity Management & Operational Resilience Impact Analysis<br>事業継続管理と運用レジリエンス<br>影響解析 | BCR-09 | 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:<br>• Identify critical products and services<br>• Identify all dependencies, including processes, applications, business partners, and third party service providers<br>• Understand threats to critical products and services<br>• Determine impacts resulting from planned or unplanned disruptions and how these vary over time<br>• Establish the maximum tolerable period for disruption<br>• Establish priorities for recovery<br>• Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption<br>• 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。<br>• 重要な製品及びサービスの特定<br>•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<br>•重要な製品及びサービスへの脅威の把握<br>•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<br>• 最大許容停止時間の設定<br>• 復旧の優先順位の設定<br>•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<br>• 再開に必要な資源の見積もり |
| Business Continuity Management & Operational Resilience Policy<br>事業継続管理と運用レジリエンス<br>管理プログラム | BCR-10 | 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。 |
| Business Continuity Management & Operational Resilience Retention Policy<br>事業継続管理と運用レジリエンス<br>保持ポリシー | BCR-11 | 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。 |
| Change Control & Configuration Management New Development / Acquisition<br>変更管理と構成管理<br>新規開発及び調達 | CCC-01 | 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。 |

| | | | |
|---|---|---|---|
| Change Control & Configuration Management Outsourced Development<br>変更管理と構成管理<br>開発の外部委託 | CCC-02 | External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes). | 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。 |
| Change Control & Configuration Management Quality Testing<br>変更管理と構成管理<br>品質検査 | CCC-03 | Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that 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。 |
| Change Control & Configuration Management Unauthorized Software Installations<br>変更管理と構成管理<br>未承認のソフトウェアのインストール | CCC-04 | 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。 |
| Change Control & Configuration Management Production Changes<br>変更管理と構成管理<br>業務の変更 | CCC-05 | Policies and procedures shall be established for managing the risks associated with applying changes to:<br>• business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations<br>• infrastructure network and systems components<br>Technical measures shall be implemented to provide assurance that 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) prior to deployment. | 以下の変更を適用する際のリスクを管理するために、ポリシー及び手順を確立しなければならない：<br>・業務上重要な、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インタフェース（API）の設計及び設定。<br>・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。技術的対策を施すことによって、導入前に、すべての変更が、登録された変更要求、業務上重要なまたは契約（SLA）に基づく顧客（テナント）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。 |

| | | | |
|---|---|---|---|
| Data Security & Information Lifecycle Management Classification<br>データセキュリティと情報ライフサイクル管理<br>分類 | DSI-01 | 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。 |
| Data Security & Information Lifecycle Management Data Inventory / Flows<br>データセキュリティと情報ライフサイクル管理<br>データ保存/フロー | DSI-02 | 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。 |
| Data Security & Information Lifecycle Management eCommerce Transactions<br>データセキュリティと情報ライフサイクル管理<br>eコマーストランザクション | DSI-03 | 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。 |
| Data Security & Information Lifecycle Management Handling / Labeling / Security Policy<br>データセキュリティと情報ライフサイクル管理<br>処理 / ラベル付 / セキュリティポリシー | DSI-04 | Policies and procedures shall be established for the labeling, handling, and 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。 |
| Data Security & Information Lifecycle Management Non-Production Data<br>データセキュリティと情報ライフサイクル管理<br>非実稼働データ | DSI-05 | 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。 |
| Data Security & Information Lifecycle Management Ownership / Stewardship<br>データセキュリティと情報ライフサイクル管理<br>所有者/管理責任 | DSI-06 | 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。 |
| Data Security & Information Lifecycle Management Secure Disposal<br>データセンタセキュリティ<br>安全な廃棄 | DSI-07 | 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。 |
| Datacenter Security Asset Management<br>データセンタセキュリティ<br>資産管理 | DCS-01 | 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 by 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。 |
| Datacenter Security Controlled Access Points<br>データセンタセキュリティ<br>コントロールされたアクセスポイント | DCS-02 | 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。 |
| Datacenter Security Equipment Identification<br>データセンタセキュリティ<br>アイデンティフィケーション | DCS-03 | 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。 |

| | | | |
|---|---|---|---|
| Datacenter Security<br>Off-Site Authorization<br>データセンタセキュリティ<br>オフサイト認証 | DCS-04 | 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。 |
| Datacenter Security<br>Off-Site Equipment<br>データセンタセキュリティ<br>オフサイト機器 | DCS-05 | Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite 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。 |
| Datacenter Security<br>Policy<br>データセンタセキュリティ<br>ポリシー | DCS-06 | 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 storing sensitive information. | 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。 |
| Datacenter Security -<br>Secure Area<br>Authorization<br>データセンタセキュリティ<br>セキュアエリア認証 | DCS-07 | 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。 |
| Datacenter Security<br>Unauthorized Persons<br>Entry<br>データセンタセキュリティ | DCS-08 | 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。 |
| Datacenter Security<br>User Access<br>データセンタセキュリティ<br>ユーザアクセス | DCS-09 | 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。 |
| Encryption & Key<br>Management<br>Entitlement<br>暗号化と鍵管理<br>権限付与 | EKM-01 | 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。 |
| Encryption & Key<br>Management<br>Key Generation<br>暗号化と鍵管理<br>鍵作成 | EKM-02 | 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。 |
| Encryption & Key<br>Management<br>Sensitive Data<br>Protection<br>暗号化と鍵管理<br>機微データの保護 | EKM-03 | 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), data in use (memory), 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。 |
| Encryption & Key<br>Management<br>Storage and Access<br>暗号化と鍵管理<br>保管とアクセス | EKM-04 | 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。 |
| Governance and Risk<br>Management<br>Baseline<br>Requirements<br>ガバナンスとリスク管理<br>ベースライン要求 | GRM-01 | 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 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。 |

| | | | |
|---|---|---|---|
| Governance and Risk Management<br>Data Focus Risk Assessments<br>ガバナンスとリスク管理<br>データフォーカスリスクアセスメント | GRM-02 | Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:<br>• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure<br>• Compliance with defined retention periods and end-of-life disposal requirements<br>• 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。<br>•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<br>•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<br>•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 |
| Governance and Risk Management<br>Management Oversight<br>ガバナンスとリスク管理<br>管理の監視 | GRM-03 | 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。 |
| Governance and Risk Management<br>Management Program<br>ガバナンスとリスク管理<br>管理プログラム | GRM-04 | 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:<br>• Risk management<br>• Security policy<br>• Organization of information security<br>• Asset management<br>• Human resources security<br>• Physical and environmental security<br>• Communications and operations management<br>• Access control<br>• 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。<br>・リスク管理<br>・セキュリティポリシー<br>・情報セキュリティの組織<br>・資産管理<br>・人的セキュリティ<br>・物理的及び環境的セキュリティ<br>・通信及び運用管理<br>・アクセス制御<br>・情報システムの取得、開発及び保守 |
| Governance and Risk Management<br>Management Support/Involvement<br>ガバナンスとリスク管理<br>補強 / 関与 | GRM-05 | 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。 |
| Governance and Risk Management<br>Policy<br>ガバナンスとリスク管理<br>ポリシー | GRM-06 | 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。 |
| Governance and Risk Management<br>Policy Enforcement<br>ガバナンスとリスク管理<br>ポリシー強化 | GRM-07 | 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。 |
| Governance and Risk Management<br>Policy Impact on Risk Assessments<br>ガバナンスとリスク管理<br>リスクアセスメントにおけるポリシーインパクト | GRM-08 | 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。 |

| | | | |
|---|---|---|---|
| Governance and Risk Management<br>Policy Reviews<br>ガバナンスとリスク管理<br>ポリシーレビュー | GRM-09 | 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。 |
| Governance and Risk Management<br>Risk Assessments<br>ガバナンスとリスク管理<br>リスクアセスメント | GRM-10 | 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 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). | 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。 |
| Governance and Risk Management<br>Risk Management Framework<br>ガバナンスとリスク管理<br>リスク管理フレームワーク | GRM-11 | Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval. | 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。 |
| Human Resources<br>Asset Returns<br>人事<br>資産返却 | HRS-01 | 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。 |
| Human Resources<br>Background Screening<br>人事<br>経歴スクリーニング | HRS-02 | 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。 |
| Human Resources<br>Employment Agreements<br>人事<br>雇用契約 | HRS-03 | 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。 |
| Human Resources<br>Employment Termination<br>人事<br>雇用の終了 | HRS-04 | 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。 |
| Human Resources<br>Mobile Device Management<br>人事<br>モバイルデバイス管理 | HRS-05 | 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。 |

| | | | |
|---|---|---|---|
| Human Resources<br>Non-Disclosure Agreements<br>人事<br>守秘義務契約 | HRS-06 | 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。 |
| Human Resources<br>Roles / Responsibilities<br>人事<br>ロール / 責任 | HRS-07 | 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。 |
| Human Resources<br>Technology Acceptable Use<br>人事<br>技術的に受け入れられる使用 | HRS-08 | 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。 |
| Human Resources<br>Training / Awareness<br>人事<br>訓練 / 認識向上 | HRS-09 | 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。 |
| Human Resources<br>User Responsibility<br>人事<br>ユーザ責任 | HRS-10 | All personnel shall be made aware of their roles and responsibilities for:<br>• Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.<br>• 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。<br>•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<br>•安全でセキュアな作業環境を維持すること |
| Human Resources<br>Workspace<br>人事<br>ワークスペース | HRS-11 | 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 are 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。 |
| Identity & Access Management<br>Audit Tools Access<br>アイデンティティとアクセス管理 | IAM-01 | 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。 |
| Identity & Access Management<br>Credential Lifecycle / Provision Management<br>アイデンティティとアクセス管理<br>資格証明のライフサイクル / プロビジョニング管理 | IAM-02 | 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:<br>• 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)<br>• 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)<br>• Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))<br>• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)<br>• Account credential lifecycle management from instantiation through revocation<br>• Account credential and/or identity store minimization or re-use when feasible<br>• Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)<br>• Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions<br>• 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。<br>・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<br>・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）<br>・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<br>・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<br>•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<br>・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<br>・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）<br>・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 |
| Identity & Access Management<br>Diagnostic / Configuration Ports Access<br>アイデンティティとアクセス管理<br>診断 / 設定ポートアクセス | IAM-03 | 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。 |
| Identity & Access Management<br>Policies and Procedures<br>アイデンティティとアクセス管理<br>ポリシーと手順 | IAM-04 | 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。 |

| | | | |
|---|---|---|---|
| Identity & Access Management<br>Segregation of Duties<br>アイデンティティとアクセス管理<br>職務の分離 | IAM-05 | 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。 |
| Identity & Access Management<br>Source Code Access Restriction<br>アイデンティティとアクセス管理<br>ソースコードアクセス制限 | IAM-06 | 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。 |
| Identity & Access Management<br>Third Party Access<br>アイデンティティとアクセス管理<br>第三者アクセス | IAM-07 | 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。<br>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。 |
| Identity & Access Management<br>Trusted Sources<br>アイデンティティとアクセス管理<br>信頼された発行元 | IAM-08 | 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原則と複製制限に基づき管理されなければならない。 |
| Identity & Access Management<br>User Access Authorization<br>アイデンティティとアクセス管理<br>ユーザアクセス権限 | IAM-09 | 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 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。<br>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。 |

| | | | |
|---|---|---|---|
| Identity & Access Management<br>User Access Reviews<br>アイデンティティとアクセス管理<br>ユーザアクセスレビュー | IAM-10 | 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 established user access policies and procedures. | 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。 |
| Identity & Access Management<br>User Access Revocation<br>アイデンティティとアクセス管理<br>ユーザアクセス取り消し | IAM-11 | 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。 |
| Identity & Access Management<br>User ID Credentials<br>アイデンティティとアクセス管理<br>ユーザID認証 | IAM-12 | 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:<br>• Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)<br>• Account credential lifecycle management from instantiation through revocation<br>• Account credential and/or identity store minimization or re-use when feasible<br>• 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。<br>•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）<br>• 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<br>• 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）<br>•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） |
| Identity & Access Management<br>Utility Programs Access<br>アイデンティティとアクセス管理<br>ユーティリティプログラムアクセス | IAM-13 | 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。 |
| Infrastructure & Virtualization Security<br>Audit Logging / Intrusion Detection<br>インフラと仮想化のセキュリティ<br>監査ログ / 侵入検知 | IVS-01 | Higher levels of assurance are required for protection, retention, and lifecycle 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。 |
| Infrastructure & Virtualization Security<br>Change Detection<br>インフラと仮想化のセキュリティ<br>変更検知 | IVS-02 | 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。 |
| Infrastructure & Virtualization Security<br>Clock Synchronization<br>インフラと仮想化のセキュリティ<br>時間同期 | IVS-03 | 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。 |
| Infrastructure & Virtualization Security<br>Information System Documentation<br>インフラと仮想化のセキュリティ<br>情報システム文書 | IVS-04 | 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。 |

| | | | |
|---|---|---|---|
| Infrastructure & Virtualization Security Management - Vulnerability Management<br>インフラと仮想化のセキュリティ<br>管理 - 脆弱性管理 | IVS-05 | 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) |
| Infrastructure & Virtualization Security Network Security<br>インフラと仮想化のセキュリティ<br>ネットワークセキュリティ | IVS-06 | 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 by 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、補完するコントロールによってサポートされなければならない。 |
| Infrastructure & Virtualization Security OS Hardening and Base Conrols<br>インフラと仮想化のセキュリティ<br>OS堅牢性と基本管理 | IVS-07 | 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。 |
| Infrastructure & Virtualization Security Production / Non-Production Environments<br>インフラと仮想化のセキュリティ<br>本番 / テスト環境 | IVS-08 | 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責務の分離。 |
| Infrastructure & Virtualization Security Segmentation<br>インフラと仮想化のセキュリティ<br>区分 | IVS-09 | 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:<br>• Established policies and procedures<br>• Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance<br>• 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。<br>・定められたポリシー及び手順<br>・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<br>・法的及び規制上の遵守義務への準拠 |
| Infrastructure & Virtualization Security VM Security - vMotion Data Protection<br>インフラと仮想化のセキュリティ<br>VMセキュリティ - Vmotionデータ保護 | IVS-10 | 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。 |
| Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening<br>インフラと仮想化のセキュリティ<br>VMMセキュリティ - ハイパバイザ堅牢性 | IVS-11 | 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。 |
| Infrastructure & Virtualization Security Wireless Security<br>インフラと仮想化のセキュリティ<br>ワイヤレスセキュリティ | IVS-12 | Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:<br>• Perimeter firewalls implemented and configured to restrict unauthorized traffic<br>• Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)<br>• User access to wireless network devices restricted to authorized personnel<br>• 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。<br>・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<br>・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)<br>・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<br>・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 |

| | | | |
|---|---|---|---|
| Infrastructure & Virtualization Security<br>Network Architecture<br>インフラと仮想化のセキュリティ<br>ネットワークアーキテクチャ | IVS-13 | 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。 |
| Interoperability & Portability<br>APIs<br>相互運用性と移植容易性 | 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。 |
| Interoperability & Portability<br>Data Request<br>相互運用性と移植容易性<br>データ要求 | 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し、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。 |
| Interoperability & Portability<br>Policy & Legal<br>相互運用性と移植容易性<br>ポリシーと法律 | IPY-03 | 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。 |
| Interoperability & Portability<br>Standardized Network Protocols<br>相互運用性と移植容易性<br>標準ネットワークプロトコル | IPY-04 | 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。 |
| Interoperability & Portability<br>Virtualization<br>相互運用性と移植容易性<br>仮想化 | IPY-05 | 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。 |
| Mobile Security<br>Anti-Malware<br>モバイルセキュリティ<br>アンチマルウェア | 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。 |
| Mobile Security<br>Application Stores<br>モバイルセキュリティ<br>アプリケーションストア | MOS-02 | A documented list of approved application stores has been defined 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。 |
| Mobile Security<br>Approved Applications<br>モバイルセキュリティ<br>承認されたアプリケーション | 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。 |
| Mobile Security<br>Approved Software for BYOD<br>モバイルセキュリティ<br>BYODとして承認されたソフトウエア | 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。 |
| Mobile Security<br>Awareness and Training<br>モバイルセキュリティ<br>認知と訓練 | 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。 |
| Mobile Security<br>Cloud Based Services<br>モバイルセキュリティ<br>クラウドベースサービス | 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。 |
| Mobile Security<br>Compatibility<br>モバイルセキュリティ<br>互換性 | 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。 |
| Mobile Security<br>Device Eligibility<br>モバイルセキュリティ<br>デバイスの適格性 | 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。 |
| Mobile Security<br>Device Inventory<br>モバイルセキュリティ<br>デバイスの一覧表 | 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。 |
| Mobile Security<br>Device Management<br>モバイルセキュリティ<br>データ管理 | 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。 |

| | | | |
|---|---|---|---|
| Mobile Security<br>Encryption<br>モバイルセキュリティ<br>暗号化 | 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。 |
| Mobile Security<br>Jailbreaking and Rooting<br>モバイルセキュリティ<br>ジェイルブレイクとルート化 | MOS-12 | The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition 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、またはー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。 |
| Mobile Security<br>Legal<br>モバイルセキュリティ<br>法律 | MOS-13 | 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 regarding 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する。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喪失の可能性について明記しなければならない。 |
| Mobile Security<br>Lockout Screen<br>モバイルセキュリティ<br>ロックアウト画面 | 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。 |
| Mobile Security<br>Operating Systems<br>モバイルセキュリティ<br>オペレーティングシステム | 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。 |
| Mobile Security<br>Passwords<br>モバイルセキュリティ<br>パスワード | MOS-16 | 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。 |
| Mobile Security<br>Policy<br>モバイルセキュリティ<br>ポリシー | MOS-17 | 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。 |
| Mobile Security<br>Remote Wipe<br>モバイルセキュリティ<br>リモート消去 | MOS-18 | 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。 |
| Mobile Security<br>Security Patches<br>モバイルセキュリティ<br>セキュリティパッチ | MOS-19 | 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。 |
| Mobile Security<br>Users<br>モバイルセキュリティ<br>ユーザ | MOS-20 | 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。 |
| Security Incident Management, E-Discovery & Cloud Forensics<br>Contact / Authority Maintenance<br>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<br>契約 / 機関の維持 | SEF-01 | 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。 |
| Security Incident Management, E-Discovery & Cloud Forensics<br>Incident Management<br>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<br>インシデント管理 | SEF-02 | 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。 |
| Security Incident Management, E-Discovery & Cloud Forensics<br>Incident Reporting<br>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<br>インシデントレポーティング | SEF-03 | Workforce personnel and external business relationships shall be informed of their responsibilities 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。 |

| | | | |
|---|---|---|---|
| Security Incident Management, E-Discovery & Cloud Forensics<br>Incident Response Legal Preparation<br>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<br>インシデントレスポンスの法的準備 | SEF-04 | 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。 |
| Security Incident Management, E-Discovery & Cloud Forensics<br>Incident Response Metrics<br>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<br>インシデントレスポンスマトリックス | SEF-05 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Data Quality and Integrity<br>サプライチェーンの管理、透明性、説明責任<br>データ品質と完全性 | STA-01 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Incident Reporting<br>サプライチェーンの管理、透明性、説明責任<br>インシデントレポーティング | STA-02 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Network / Infrastructure Services<br>サプライチェーンの管理、透明性、説明責任<br>ネットワーク / インフラストラクチャサービス | STA-03 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Provider Internal Assessments<br>サプライチェーンの管理、透明性、説明責任<br>プロバイダの内部評価 | STA-04 | The provider shall perform annual internal assessments of conformance to, 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。 |

| | | | |
|---|---|---|---|
| Supply Chain Management, Transparency and Accountability<br>Supply Chain Agreements<br>サプライチェーンの管理、透明性、説明責任<br>サプライチェーンの合意 | STA-05 | Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:<br>• 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)<br>• 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<br>• Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts<br>• 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)<br>• 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<br>• Expiration of the business relationship and treatment of customer (tenant) data impacted<br>• 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。<br>・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）<br>・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<br>・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<br>・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<br>・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）<br>・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<br>・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 |
| Supply Chain Management, Transparency and Accountability<br>Supply Chain Governance Reviews<br>サプライチェーンの管理、透明性、説明責任<br>ガバナンスのレビュー | STA-06 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Supply Chain Metrics<br>サプライチェーンの管理、透明性、説明責任<br>サプライチェーンマトリックス | STA-07 | 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).<br><br>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。<br><br>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。 |
| Supply Chain Management, Transparency and Accountability<br>Third Party Assessment<br>サプライチェーンの管理、透明性、説明責任<br>第三者の評価 | STA-08 | 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。 |
| Supply Chain Management, Transparency and Accountability<br>Third Party Audits<br>サプライチェーンの管理、透明性、説明責任<br>第三者の監査 | STA-09 | 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。 |
| Threat and Vulnerability Management<br>Anti-Virus / Malicious Software<br>脅威と脆弱性の管理<br>アンチウイルス / 悪質なソフトウエア | TVM-01 | 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。 |

| | | | |
|---|---|---|---|
| Threat and Vulnerability Management<br>Vulnerability / Patch Management<br>脅威と脆弱性の管理<br>脆弱性 / パッチ管理 | TVM-02 | 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 identfied 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。 |
| Threat and Vulnerbility Management<br>Mobile Code<br>脅威と脆弱性の管理<br>モバイルコード | TVM-03 | 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。 |