ArcGIS Online クラウド セキュリティ アライアンス (CSA) クラウド コントロール マトリックス (CCM) 3.0.1

2017 年 1 月

本資料は、**ArcGIS Online のクラウド セキュリティ アライアンス (CSA) クラウド コントロール マトリックス (CCM) 3.0.1 を** Esri 社が自己評価した表です。CSA の質問表を参考に、Esri 社の ArcGIS Online が提供するサービスにどのようなセキュリティ管理が存在するのかを文書化しています。質問表にはクラウド サービスの顧客や監査役がクラウド プロバイダーに尋ねたい 133 の質問があります。

CSA は、国際的に活動を展開している非営利法人です。その使命は、クラウド コンピューティングのセキュリティを実現するために、ベスト プラクティスを広め推奨することにあります。そしてクラウドのユーザーに対しては、クラウドの利用に際してのセキュリティの確保に向けての啓発教育を提供します。様々な業種のセキュリティの専門家、企業、組織がこの使命のために CSA に参加しています。Esri は 2013 年から CSA CCM に回答しており、今後も改訂される新しい CCM に対応し、ArcGIS Online に重点を置いたこのドキュメントを更新し続けます。

前バージョン 1.x CCM から 3.x CCM の主な変更点：

- 下記のクラウド データのアクセス、転送、保証する上での情報セキュリティ リスクに対処する 5 つの新しいコントロール ドメインが追加されました。
  - モバイル セキュリティ、サプライチェーンの管理、透明性、説明責任、相互運用性とポータブル性、暗号化と鍵の管理
- クラウド コンピューティングのためのセキュリティ ガイダンス V3 との調和を高めました。
- コントロール ドメイン全体でコントロールの監査性を向上し、コントロール ID の命名規則を拡張しました。
- CSA によりバージョン 3.0.1 の質問のマイナーな更新と修正が行われました。このドキュメントではバージョン 3.0.1 (2016/10/6) の更新に対応しました。

ArcGIS Online は 2014 年に米国農務省 (USDA) から FISMA Low ATO (米国連邦政府機関による情報セキュリティ マネジメント法に基づいた認定) を取得しています。お客様は、ArcGIS Online を利用して認証と合致した拡張可能なタイル サービスを広く一般公開することや、自分の組織内で認証された基盤から機密情報をフィーチャ サービスとしてホストすることもできます。ArcGIS Online に関するセキュリティ、プライバシー、コンプライアンスの詳細については、http://Trust.ArcGIS.com をご参照ください。

ArcGIS Online は国際的レベルのクラウド基盤である Microsoft Azure と Amazon Web Services を利用しています。どちらも CSA の質問表に回答を提供しており、CSA 登録サイトからダウンロードできます。
https://cloudsecurityalliance.org/star/#_registry

ArcGIS Online の CSA の回答の最新バージョンは下記からダウンロードできます。

http://downloads.esri.com/resources/enterprisegis/AGOL_CSA_CCM.pdf

本文書内の質問（Updated Control Specification 列）の翻訳文は、CCM 日本語版(バージョン3.0.1）をご参照ください。

http://cloudsecurityalliance.jp/WG_PUB/CCM_WG/CSA_CCM_v3.0.1_J1.0_Pub.pdf

回答に出てくる略語一覧

OWASP: Open Web Application Security Project

FISMA: Federal Information Security Modernization Act

NIST: National Institute of Standards and Technology

FedRAMP: Federal Risk and Authorization Management Program

CCTV: Closed-circuit Television

ISMP: Institute for Safe Medication Practices

OVF: Open Virtualization Format

SLA: Service Level Agreement

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 （日本語訳）	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Application & Interface Security Application Security アプリケーションとインタフェース セキュリティ アプリケーション セキュリティ	AIS-01	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.	Building and validating ArcGIS Online code against leading security industry standards such as OWASP is the foundation for building a robust offering. This is enforced within the continuous monitoring requirements of the ArcGIS Online FISMA authorization. ArcGIS Online is scanned at a minimum of every 60 days to ensure services are regularly validated against standards such as OWASP.	OWASP などの主要なセキュリティ業界標準に従って ArcGIS Online のコードを構築、実証することは、信頼性の高いサービスを提供する上での基礎となります。これは、ArcGIS Online FISMA 認証の継続的なモニタリング要件の中で実施されています。 ArcGIS Online は最低 60 日ごとに、サービスが OWASP などの標準に従っているか定期的に検査されています。	●		A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SC-6 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13 NIST SP 800-53 R3 SC-14
Application & Interface Security Customer Access Requirements アプリケーションとインタフェース セキュリティ 顧客アクセスの要件	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.	Before using ArcGIS Online, customers are required to review and agree with the acceptable use of data and ArcGIS Online service, as well as security and privacy requirements, which are defined in the Terms of Service @ http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3 and Privacy policy @ http://www.esri.com/legal/privacy. ArcGIS Online maintains a FISMA Low security authorization through the US Government and utilizes cloud infrastructure providers that are ISO 27001 compliant. It is also Safe Harbor compliant for privacy assurance. Additional information concerning the security and privacy of ArcGIS Online may be found within the Trust.ArcGIS.com website.	ArcGIS Online を使用する前に、顧客はデータと ArcGIS Online サービスの利用規約と、下記のサービス利用規約に定義されているセキュリティとプライバシー要件を確認して同意する必要があります。 ライセンスおよびサービス契約書： http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/mla_e204_e300/japanese プライバシー ポリシー： http://www.esri.com/legal/privacy ArcGIS Online は米国政府から FISMA Low セキュリティ認証を取得しており、ISO 27001 に準拠するクラウド基盤のプロバイダーを利用しています。また、プライバシーを保証する Privacy Sheild にも準拠しています。セキュリティとプライバシーに関する詳細情報は、Trust.ArcGIS.com サイトをご参照ください。	●	●	A9.1.1.	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6
Application & Interface Security Data Integrity アプリケーションとインタフェース セキュリティ 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.	Customers can choose to require HTTPS (TLS) for their ArcGIS Online organization to ensure integrity of data in transit. ArcGIS Online utilizes relational databases to manage the integrity of feature datasets uploaded by customers. The cloud infrastructure providers are compliant with ISO 27001 and ensure data integrity is maintained through all phases including transmission, storage and processing.	顧客は ArcGIS Online 組織サイトのデータ転送の完全性を保証するために HTTPS (TLS) を必須にすることができます。ArcGIS Online は顧客がアップロードしたフィーチャ データセットの完全性を管理するためにリレーショナル データベースを利用しています。 クラウド インフラストラクチャ プロバイダーは ISO 27001 に準拠しており、データ転送、格納、処理のすべての段階でデータの完全性を保証します。	●	●	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-3
Application & Interface Security Data Security / Integrity アプリケーションとインタフェース セキュリティ 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.	Esri's Corporate Security policies are based on NIST 800-53 security controls which map to ISO 27001 controls. ArcGIS Online data security measures are in alignment with FISMA Low requirements (that have NIST 800-53 security controls as it's core). ArcGIS Online procedures include requiring that updates are reviewed for unauthorized changes during the release management process. ArcGIS Online's cloud infrastructure providers data security policies, procedures, and processes align with industry standards such as FedRAMP Moderate and ISO 27001.	Esri のコーポレート セキュリティ ポリシーは、 ISO 27001 コントロール上に位置付ける NIST 800-53 セキュリティ コントロールに基づいています。ArcGIS Online のデータ セキュリティの評価基準は NIST 800-53 セキュリティ コントロールが中核にある FISMA Low 要件に合致しています。 ArcGIS Online の手順には、リリース管理プロセス内で更新の際に必ず不正な変更をチェックすることが含まれています。 ArcGIS Online のクラウド インフラストラクチャ プロバイダーのデータ セキュリティ ポリシー、手順、プロセスは、FedRAMP Moderate や ISO 27001 などの業界標準に従っています。	●		A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-13
Audit Assurance & Compliance Audit Planning 監査保証とコンプライアンス 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.	Esri employs a fulltime information assurance team to ensure audits are appropriately planned and coordinated. ArcGIS Online is audited in accordance with FISMA Low requirements which includes ensuring auditors provide an audit plan and agree to Rules of Engagement terms before executing an audit. ArcGIS Online utilizes cloud infrastructure from Microsoft Azure, and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDA's.	Esri はフルタイムの情報保証チームを雇用して、監査が適切に計画、実施されるようにしています。ArcGIS Online は、監査前に監査人が監査計画を提出し、活動規則の条項に同意することが記載された FISMA Low 要件に従って監査が行われています。 ArcGIS Online は Microsoft Azure と Amazon Web Services のクラウド基盤を利用しています。どちらのクラウド インフラストラクチャ プロバイダーも定期的に運用を監査し、それぞれの NDA の下に実施しています。	●		Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-7
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	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.	Independent audits of security controls in place for ArcGIS Online are conducted on a regular basis in alignment with FISMA Low requirements. Cloud infrastructure providers are subjected to regular internal and external audits (at least annually) in alignment with FedRAMP Moderate and ISO 27001 requirements.	ArcGIS Online に対する、FISMA Low 要件に合致した独立したセキュリティ コントロールの監査が定期的に実施されています。 クラウド インフラストラクチャ プロバイダーに対しては、FedRAMP Moderate と ISO 27001 に合致した定期的な内部監査と最低年に 1 回の外部監査が行われています。	●	●	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 RA-5
Audit Assurance & Compliance Information System Regulatory Mapping 監査保証とコンプライアンス 情報システム規制の対応付け	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.	FISMA authorization is based on the NIST 800-53 control framework helping ensure ArcGIS Online complies with applicable data protection and privacy laws. ArcGIS Online has an established process for identifying and implementing changes to services in response to changes in applicable statutes and regulations. Customers retain ownership of their data and are responsible for compliance with laws and regulations specific to their industry or particular use of ArcGIS Online. ArcGIS Online uses cloud infrastructure providers that monitor and update all relevant and regulatory requirements with processes that align with FedRAMP Moderate and ISO 27001.	FISMA 認証は NIST 800-53 コントロール フレームワークに基づいており、ArcGIS Online が適切なデータ保護とプライバシー法に適合することを保証します。ArcGIS Online には適用する法令や規則が変更された場合に、変更点を特定しサービスに変更を実装する既存プロセスがあります。 顧客はデータの所有権を保持し、顧客の業界特有の法や規制、ArcGIS Online の利用規約を順守する責任があります。 ArcGIS Online は FedRAMP Moderate と ISO 27001 と合致する、すべての関連する規制要件プロセスをモニターして更新するクラウド インフラストラクチャ プロバイダーを利用しています。	●	●	Clauses 4.2(b), 4.4, 5.2(c), 5.3(ab), 6.1.2, 6.1.3, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3 9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1, A.18.1.1, A.18.1.3, A.18.1.4, A.18.1.5	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53
Business Continuity Management & Operational Resilience Business Continuity Planning 事業継続管理と運用の再開 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. 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	ArcGIS Online has a full Continunity Plan designed in alignment with FISMA securiy control requirements. ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	ArcGIS Online は、FISMA セキュリティ コントロール要件に従って、完全な事業継続計画を作成しています。 ArcGIS Online のクラウド インフラストラクチャ プロバイダーは、事業継続計画が ISO 27001 標準に適合することを保証します。	●	●	Clause 5.1(h) A.17.1.2 A.17.1.2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10
Business Continuity Management & Operational Resilience Business Continuity Testing 事業継続管理と運用の再開 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.	ArcGIS Online does contingency plan and incident response plan testing at a minimum of annually in alignment with FISMA Low requirements. ArcGIS Online's cloud infrastructure providers business continuity policies, plans, and processes are developed and tested in alignment with ISO 27001 standards.	ArcGIS Online は、危機管理計画とインシデント対応計画を FISMA Low 要件に従い、最低年に 1 回検証しています。 ArcGIS Online のクラウド インフラストラクチャ プロバイダーの事業継続に関する方針、計画、プロセスは、ISO 27001 標準に従って、作成、検証されています。	●	●	A17.3.1	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions 事業継続管理と運用の再開 データ センターの設備 / 環境条件	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.	ArcGIS Online uses cloud infrastructure providers whose datacenters comply with industry standards (such as ISO 27001) for physical security and availability.	ArcGIS Online は、物理的なセキュリティと可用性に関する業界標準 (ISO 27001 など) に適合したクラウド インフラストラクチャ プロバイダーを利用しています。	●		A11.2.2, A11.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)
Business Continuity Management & Operational Resilience Documentation 事業継続管理と運用の再開 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: ・Configuring, installing, and operating the information system ・Effectively using the system's security features	Information system documentation is made available internal to ArcGIS Online personnel through the use of Esri's Intranet site. For security and operational reasons, Esri does not provide internal operations documentation to customers. For best practice security implementation guidance for customer organizations in ArcGIS Online, see: https://doc.arcgis.com/en/trust/security/arcgisonline-best-practices.htm. There are also detailed user guides available in the online help section for ArcGIS Online: http://doc.arcgis.com/en/arcgis-online/	ArcGIS Online に携わる社員が、情報システムに関する文書を Esri 社のイントラネット サイトで内部利用できるようになっています。セキュリティと運用上の理由のため、Esri は内部の運用ドキュメントを顧客には提供しません。 顧客の ArcGIS Online の組織サイトに実装するベスト プラクティスのセキュリティ ガイダンスは下記にあります： https://doc.arcgis.com/ja/trust/security/arcgis-online-best-practices.htm また、詳細なユーザー ガイドを ArcGIS Online のオンライン ヘルプで参照できます： http://doc.arcgis.com/ja/arcgis-online/	●		Clause 9.2(g) A12.1.1	NIST SP 800-53 R3 CP-9 NIST SP 800-53 R3 CP-10 NIST SP 800-53 R3 SA-5

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Business Continuity Management & Operational Resilience Environmental Risks 事業継続管理と運用の再開 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.	Cloud infrastructure provider environmental controls have been implemented to protect the data center (complying with ISO 27001) including: -Temperature control -Heating, Ventilation and Air Conditioning (HVAC) -Fire detection and suppression systems -Power Management systems	データ センターを保護するため、クラウド インフラストラクチャ プロバイダーは ISO 27001 に適合した下記の環境管理を実践しています： - 温度管理 - 暖房、空調、冷房 - 火災探知と消火システム - 電力管理システム	●		A11.1.4, A11.2.1 A11.2.2	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15
Business Continuity Management & Operational Resilience Equipment Location 事業継続管理と運用の再開 機器の保管場所	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.	Windows Azure services' equipment is place in environments which have been engineered to be protected from theft and environmental risks such as fire, smoke, water, dust, vibration, earthquakes, and electrical interference. AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability Zones. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.	ArcGIS Online は下記のクラウド インフラストラクチャ プロバイダーを利用しています。各プロバイダーにおけるリスク対応は以下の通りです。 Windows Azure サービスの設備は、盗難、火災、煙、水、埃、振動、地震、電気障害などの環境リスクを防ぐ設計がされています。 AWS データ センターは環境リスクに対して物理的な防御を取り入れています。AWS サービスは顧客に複数の地理的に離れたリージョンやアベイラビリティ ゾーンにまたがってデータを格納する柔軟性を提供しています。AWS の複数のリージョンやアベイラビリティ ゾーンを利用するには、顧客がそのように指定する必要があります。	●		A11.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15
Business Continuity Management & Operational Resilience Equipment Maintenance 事業継続管理と運用の再開 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.	Cloud infrastructure providers ensure continuity of operations during equipment maintenance. If an upgrade of ArcGIS Online require an outage window, customers will be notified ahead of time.	クラウド インフラストラクチャ プロバイダーは、機器の保守期間に運用の継続性を保証します。ArcGIS Online の更新時に機能を停止する必要がある場合は、事前に顧客にお知らせします。	●		A11.2.4	NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5
Business Continuity Management & Operational Resilience Equipment Power Failures 事業継続管理と運用の再開 機器の電源障害	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	The cloud infrastructure providers' data centers have 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators. Data centers have made arrangements for emergency fuel delivery.	クラウド インフラストラクチャ プロバイダーのデータ センターは、常時、無停電電源装置 (UPS) と発電機を含む非常電源を保有しています。UPS と発電機は定期的に整備と動作確認が行われています。データ センターは緊急時の燃料供給の方策を立てています。	●		A.11.2.2, A.11.2.3, A.11.2.4	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP80 0-53 R3 PE-14
Business Continuity Management & Operational Resilience Impact Analysis 事業継続管理と運用の再開 影響分析	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: ・ 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	ArcGIS Online cloud infrastructure providers perform business impact analysis (BIA) meeting ISO 27001 standards requirements. Customers may view infrastructure and application status information on the following dashboards: AWS: http://status.aws.amazon.com MS Azure: http://www.windowsazure.com/en-us/support/servicedashboard/ ArcGIS Online: http://status.arcgis.com	ArcGIS Online のクラウド インフラストラクチャ プロバイダーは、 ISO 27001 標準の要件に適合したビジネス インパクト評価 (BIA) を実施しています。顧客は基盤とアプリケーションのステータス情報を下記のダッシュボードで参照できます： AWS: http://status.aws.amazon.com MS Azure: https://azure.microsoft.com/ja-jp/status/ ArcGIS Online: http://status.arcgis.com	●	●	A.17.1.1 A.17.1.2	NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 RA-3
Business Continuity Management & Operational Resilience Policy 事業継続管理と運用の再開 ポリシー	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.	ArcGIS Online's cloud infrastructure providers have developed Business Continuity documentation that align with ISO 27001 and FedRAMP Moderate Requirements.	ArcGIS Online のクラウド インフラストラクチャ プロバイダーは、 ISO 27001 と FedRAMP Moderate 要件に合致する事業継続の文書を作成しています。	●		Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5
Business Continuity Management & Operational Resilience Retention Policy 事業継続管理と運用の再開 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.	Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure. ArcGIS Online provides customers with the ability to delete their data; however it is the customer's responsibility to manage data retention to their own requirements. A KBA describing backing up customer data is available at: http://support.esri.com/en/knowledgebase/techarticles/detail/41166	Esri は ArcGIS Online の基盤データを定期的にバックアップしています。顧客のデータは冗長インフラ ストラクチャにレプリケートされます。ArcGIS Online は顧客に自分のデータを削除する機能を提供していますが、顧客自身の要求に基づいてデータ保持を管理する責任は顧客にあります。顧客データのバックアップに関するサポート技術情報は下記をご参照ください： http://support.esri.com/en/technical-article/000011795	●	●	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1 A.8.2.3	NIST SP 800-53 R3 CP-2 NIST SP 800-53 R3 CP-9
Change Control & Configuration Management New Development / Acquisition 変更制御と構成管理 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.	Esri maintains separate non-production systems for testing and validating new development and systems infrastructure capabilities as outlined in the internal ArcGIS Online Configuration Management Plan, aligning with FISMA Low requirements.	FISMA Low 要件に合致した内部 ArcGIS Online 構成管理計画に概説されているように、Esri は本番運用ではないシステムを、新しい開発やシステム インフラストラクチャ機能のテストと検証を行うために、本番運用システムとは分離して保持しています。	●		A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7 A.18.1.3 A.18.1.4	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SA-3 NIST SP 800-53 R3 SA-4
Change Control & Configuration Management Outsourced Development 変更制御と構成管理 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).	Microsoft applies their Security Development Lifecycle, whereas Amazon typically does not outsource development of their software. Both providers solutions align with the ISO 27001 security standard.	Microsoft は Microsoft セキュリティ開発ライフサイクルに従っています。Amazon は通常はソフトウェアの開発をアウトソースしません。両方のプロバイダーのソリューションは ISO 27001 セキュリティ標準に適合します。	●	●	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2	NIST SP 800-53 R3 SA-4 NIST SP 800-53 R3 SA-5 NIST SP 800-53 R3 SA-9
Change Control & Configuration Management Quality Testing 変更制御と構成管理 品質テスト	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.	ArcGIS Online conducts testing and validation prior to release in alignment with FISMA Low requirements. Cloud infrastructure providers ensure changes are tested in various test environments and signed off prior to deployment into production and ensuring alignment with the ISO 27001 standard.	ArcGIS Online は、FISMA Low 要件に従い、リリース前に検証と実証を行っています。クラウド インフラストラクチャ プロバイダーは、 ISO 27001 標準に従い、変更が様々な環境でテストされ、運用に実装する前にサイン オフすることを保証しています。	●		A.6.1.1 A.12.1.1 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.58.1* partial A.14.2.28.1* partial A.14.2.3	
Change Control & Configuration Management Unauthorized Software Installations 変更制御と構成管理 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.	All changes into production go through the Change Management process described in CCC-05.	運用版のすべての変更に、CCC-05 に記載された変更管理プロセスを実施します。	●		A.6.1.2 A.12.2.1 A.9.4.4 A.9.4.1 A.12.5.1 8.1* (partial) A.14.2.4	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 CM-8 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-3
Change Control & Configuration Management Production Changes 変更制御と構成管理 運用の変更	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: ・ business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations ・ infrastructure network and systems components 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.	Esri maintains separate non-production systems for testing and validating new development and systems infrastructure capabilities as outlined in the internal ArcGIS Online Configuration Management Plan, aligning with FISMA Low requirements.	FISMA Low 要件に合致した内部 ArcGIS Online 構成管理計画に概説されているように、Esri は非本番運用システムを、新しい開発やシステム インフラストラクチャ機能のテストと検証を行うために、本番運用システムと分離して保持しています。	●	●	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3	NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 PL-2 NIST SP 800-53 R3 PL-5 NIST SP 800-53 R3 SI-2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	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.	Esri classifies datasets they own according to the Esri Technology Control Plan and then implements a standard set of Security and Privacy attributes. Esri treats all Customer Data in accordance with the commitment outlined in DSI-02. Datasets uploaded to ArcGIS Online are owned by the customer and they are responsible for classifying their dataset and handling accordingly. It is Customer's sole responsibility to ensure that Customer Content is suitable for use with Online Services. Examples of datasets not recommended for Online Services include: International Traffic in Arms Regulations (ITAR), Unclassified Controlled Technical Information (UCTI), and Protected Health Information (PHI).	Esri は、Esri テクノロジ コントロール プランに従って、保有するデータセットを機密区分し、セキュリティとプライバシー属性の標準セットを実装しています。Esri は顧客の全データを DSI-02 に概説されたコミットメントに従って処理しています。 ArcGIS Online にアップロードされたデータセットは、顧客によって保有され、顧客はデータセットを分類し適切な方法で処理する責任があります。顧客のコンテンツがオンライン サービスでの使用に適切であるかを確認することは、顧客側の責任です。オンライン サービスに推奨されないデータセットの例: International Traffic in Arms Regulations (ITAR)、Unclassified Controlled Technical Information (UCTI)、および Protected Health Information (PHI)。	●	●	A.8.2.1	NIST SP 800-53 R3 RA-2
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	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.	ArcGIS Online is a FISMA Low authorized solution by the United States Department of Agriculture (USDA). This includes the requirement to adhere to robust continuous monitoring requirements and security controls are reviewed at a minimum of every three (3) years.As for cloud providers of Amazon Web Services and Microsoft Azure, they will not move ArcGIS Online data from Esri's chosen physical regions (All reside on U.S. soil).	ArcGIS Online は米国農務省 (USDA) から FISMA Low を取得しています。これには、高い信頼性で継続的にモニタリングする要件とセキュリティ コントロールを最低 3 年ごとにレビューする要件が含まれています。クラウド プロバイダーである Amazon Web Services や Microsoft Azure は、ArcGIS Online のデータを Esri が指定した物理的な領域以外には移動しません（すべてのデータは、米国内にあります）。	●	●	Clause4.2 5.2, 7.5, 8.1	
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	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.	Esri stores no payment instrument number information (e.g. credit card) within their systems for Products & Services. Esri utilizes a third party provider which has been audited by a Payment Card Industry Standard certified auditor to ensure your information remains secure. Payment information is transmitted directly to the provider via HTTPS for secure transmission so that payment data is never transmitted or stored by Esri Products & Services.	Esri は支払方法の数値情報（例： クレジット カード番号）を、Esri の製品とサービス システムに保存しません。Esri は Payment Card Industry Standard が認定した監査人が監査するサード パーティ プロバイダーを利用しており、情報がセキュリティ保護されていることを保証します。支払情報は、セキュリティ保護された HTTPS でプロバイダーに直接送信されるので、支払いデータが Esri の製品とサービスに送信または保存されることは絶対にありません。	●	●	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-22 NIST SP 800-53 R3 AU-1
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 / ラベル付け / 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.	ArcGIS Online customers retain ownership of their data and may implement a labeling and handling policy and procedures to meet their requirements.	ArcGIS Online の顧客は顧客のデータの所有権を保持し、ラベリング、処理取り扱いポリシー及び手順を、顧客の要求に基づいて、確立することができます。	●	●	A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-12
Data Security & Information Lifecycle Management Non-Production Data データ セキュリティと情報ライフサイクル管理 非本番運用データ	DSI-05	Production data shall not be replicated or used in non-production environments.	ArcGIS Online customers retain ownership of their own data. ArcGIS Online provides customers the ability to maintain and develop production and non-production organization environments. It is the responsibility of the customer to ensure that their production data is not replicated to the non-production environments. Movement or copying of Customer Data by Esri out of the production environment into a non-production environment is prohibited except where customer consent is obtained for troubleshooting the service, or at the directive of Esri's legal department.	ArcGIS Online の顧客は顧客自身のデータの所有権を保持します。ArcGIS Online は顧客に本番運用/非本番運用の組織サイトの環境を管理、作成する機能を提供します。 サービスのトラブルシューティングのため顧客が同意した場合または Esri の法務部の指示があった場合を除き、Esri が顧客データを本番運用環境から非本番運用環境へ移動、コピーすることは禁じられています。	●		A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.	
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 所有者/管理責任	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Data stored within ArcGIS Online meets FISMA Low categorized requirements. Customers are responsible for implementing workflows to enforce this categorization level. Customers retain full ownership of their data.	ArcGIS Online に格納されたデータは、FISMA Low で分類された要求を満たします。この分類レベルを実施するためのワークフローを実装する責任は、顧客にあります。顧客は、顧客のデータに対するすべての所有権を保持します。	●		A.6.1.1 A.8.1.2 A.18.1.4	NIST SP 800-53 R3 CA-2 NIST SP 800-53 R3 CA-2 (1) NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 SA-2
Data Security & Information Lifecycle Management Secure Disposal データ セキュリティと情報ライフサイクル管理 安全な廃棄	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	When a storage device has reached the end of its useful ArcGIS Online cloud infrastructure providers procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The Cloud infrastructure providers use the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual ”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.	記憶装置が寿命になった際に、ArcGIS Online のクラウド インフラストラクチャ プロバイダーの手順には、許可されていない個人に顧客データがさらされないようにする廃棄プロセスが含まれています。クラウド インフラストラクチャ プロバイダーは、 DoD 5220.22-M (“National Industrial Security Program Operating Manual ”) または NIST 800-88 (“Guidelines for Media Sanitization”) に詳しく述べられた手法を使用して、廃棄プロセスの一環としてデータを破壊します。ハードウェア デバイスがこれらのプロセスで廃棄できない場合は、デバイスを消磁するか、業界標準の方法で物理的に破壊します。	●		A.11.2.7 A.8.3.2	NIST SP 800-53 R3 MP-6 NIST SP 800-53 R3 PE-1
Datacenter Security Asset Management データ センター セキュリティ 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.	ArcGIS Online cloud infrastructure providers have established policies and procedures for addressing their assets aligning with ISO 27001 standards.	ArcGIS Online クラウド インフラストラクチャ プロバイダーは、ISO 27001 標準に従って資産を明記するポリシー及び手順を確立しています。	●		Annex A.8	
Datacenter Security Controlled Access Points データ センター セキュリティ 制御されたアクセス 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.	ArcGIS Online's cloud infrastructure providers have physical security measures for their data centers that comply with high industry standards for physical security controls. For more information, visit their respective compliance sites below. Microsoft Azure: https://www.microsoft.com/enus/trustcenter/Compliance Amazon Web Services: https://aws.amazon.com/compliance/	ArcGIS Online クラウド インフラストラクチャ プロバイダーは、物理的なセキュリティ コントロールの高度な業界標準に適合した、データ センターの物理的なセキュリティ対策を取っています。詳細は、各プロバイダーのコンプライアンス サイトをご参照ください。 Microsoft Azure: https://www.microsoft.com/ja-jp/trustcenter/compliance Amazon Web Services: https://aws.amazon.com/compliance/	●		A.11.1.1 A.11.1.2	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6 NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-8
Datacenter Security Equipment Identification データ センター セキュリティ 機器の識別	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.	Cloud infrastructure providers maintain a current, documented and audited inventory of equipment and network components for which it is responsible. The cloud infrastructure providers managed automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. Cloud infrastructure providers manage equipment identification in alignment with the ISO 27001 standard.	クラウド インフラストラクチャ プロバイダーは、プロバイダーが責任を負っている設備とネットワーク コンポーネントの最新の状態を文書化し、監査された目録を保有しています。クラウド インフラストラクチャ プロバイダーは、デバイスの構成と定義されたポリシーを比較して不一致を自動的に検知する仕組みを持っています。クラウド インフラストラクチャ プロバイダーは、ISO 27001 標準に従って機器を識別する仕組みを使用しています。	●			NIST SP 800-53 R3 IA-4
Datacenter Security Off-Site Authorization データ センター セキュリティ オフサイト承認	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	All ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Service US Regions (East, West), and Microsoft Azure US Regions (South Central, East, West). ArcGIS Online customers will be notified if Esri proposes storing any of their data outside US soil.	ArcGIS Online の顧客データはすべて米国内の Amazon Web Service の US リージョン(East, West) と Microsoft Azure US リージョン (South Central, East, West) 内に限定して格納されています。もし Esri が米国以外にデータの保存を提案した場合、ArcGIS Online の顧客はその旨を事前に通知されます。	●		A.11.2.6 A.11.2.7	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PE-16
Datacenter Security Off-Site Equipment データセンター セキュリティ 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.	ArcGIS Online cloud infrastructure providers have established policies and procedures for addressing off-site equipment aligning with ISO 27001 standards and NIST 800-88 Guidelines on Media Sanitization, which addresses the principle concern of ensuring that data is not unintentionally released.	ArcGIS Online のクラウド インフラストラクチャ プロバイダーは、ISO 27001 標準と、データを気付かずに放出されることがないように保証するメディア サニタイズに関する NIST 800-88 ガイドラインに従って、組織の構外で使用される装置のためのポリシー及び手順を確立しています。	●	●	A.8.1.1 A.8.1.2	NIST SP 800-53 R3 CM-8
Datacenter Security Policy データ センター セキュリティ 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.	Cloud infrastructure provider policies policy define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information. Access to media storage areas is restricted and audited. Access to all cloud provider buildings is controlled, and access is restricted to those with card reader or biometrics for entry into Data Centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. Staff must wear identity badges at all times, and are required to challenge or report individuals without badges. All guests are required to wear guest badges and be escorted by authorized cloud provider personnel.	クラウド インフラストラクチャ プロバイダーは、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を確立しています。メディアを保存するエリアへの入室は制限、監視されています。クラウド プロバイダーの建物への立ち入りは規制されており、データセンターへの入室はカード読み取り装置や生体認証で制限されています。受付の職員は、フルタイムの雇用者や ID カードを持たない認可された請負業者の身元を確認する必要があります。スタッフは常に ID バッジを付けることが求められ、ID バッジを付けていない人物を身元確認して報告をしなければなりません。ゲストはゲスト バッジを付けて、正規のクラウド プロバイダーの職員が同行する必要があります。	●	●	A.11.1.1 A.11.1.2	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Datacenter Security - Secure Area Authorization データ センター セキュリティ 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.	Public access, delivery, loading area and physical/environmental security is covered under the ISO 27001 standards, specifically addressed in Annex A, domain 9. Datacenter entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.	一般の立ち入り、搬送、荷物の積み降ろしエリアの物理的、環境的なセキュリティは、ISO 27001 標準（Annex A, domain 9 に記載）によって保証されています。データセンターの入り口には警備員が 24 時間 365 日体制で配置され、入退室は警備員、認証バッジ、施錠されたドア、CCTV モニターで管理されている。	●		A.11.1.6	NIST SP 800-53 R3 PE-7 NIST SP 800-53 R3 PE-16
Datacenter Security Unauthorized Persons Entry データ センター セキュリティ 許可されていない個人の入室	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.	Cloud infrastructure provider physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors.	クラウド インフラストラクチャ プロバイダーの物理的なアクセスは、建物の周辺と入口での専門セキュリティ スタッフによるビデオ監視や侵入検知システムなどの電子的な方法で厳しく管理されています。許可されたスタッフがデータセンターのフロアにアクセスするには、最低 2 回の 二段階認証を通過する必要があります。	●		A.11.2.5 8.1* (partial) A.12.1.2	NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MA-2 NIST SP 800-53 R3 PE-16
Datacenter Security User Access データセンター セキュリティ ユーザー アクセス	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	Cloud infrastructure provider access is restricted by job function so that only essential personnel receive authorization to manage cloud infrastructure services. Physical access authorization utilizes multiple authentication and security processes: badge and smartcard, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication for physical access to the data center environment.	クラウド インフラストラクチャ プロバイダーの立ち入りは、職務権限により制限されており、必須の担当者のみクラウド インフラストラクチャ サービスを管理する許可を持っています。物理的な入退室の許可には、複数回の認証とセキュリティ プロセスが使用されています（バッジ、スマートカード、生体認証、警備員の配置、継続的なビデオ監視、データセンター環境への物理的な立ち入りの際の二段階認証）。	●		A.11.1.1	NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3 NIST SP 800-53 R3 PE-6
Encryption & Key Management Entitlement 暗号化と鍵の管理 権限付与	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Key management policies, procedures, and processes for ArcGIS Online align with FISMA Low requirements.	ArcGIS Online の鍵管理ポリシー、手順、プロセスは、FISMA Low 要件に適合します。	●	●	Annex A.10.1 A.10.1.1 A.10.1.2	
Encryption & Key Management Key Generation 暗号化と鍵の管理 鍵の生成	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.	ArcGIS Online operational keys are managed by the ArcGIS Online Operations Leads. Critical keys are rotated periodically during product release time windows. Compromised keys are revoked and reissued within 24 hours of detection.	ArcGIS Online の運用にかかわる鍵は、ArcGIS Online の運用リーダーが管理しています。重要な鍵はプロダクトのリリース期間内で定期的に順番に変更します。危害を受けた鍵は検出から 24 時間以内に取り消され、再発行されます。	●		Clauses 5.2(c) 5.3(a) 5.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.3 9.2(g) A.8.2.3 A.10.1.2 A.18.1.5	NIST SP 800-53 R3 SC-12 NIST SP 800-53 R3 SC-13
Encryption & Key Management Sensitive Data Protection 暗号化と鍵の管理 機密データの保護	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.	ArcGIS Online provides customer's administrator the option of requiring encryption-in-transit via HTTPS (TLS) for customer data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. Customer can encrypt their data either through their application or by leveraging an enterprise cloud encryption gateway solution. Many customers that have data sensitivity concerns choose to implement a hybrid solution where more sensitive data is kept onpremises or in a separate cloud with higher security reassurance, such as Esri Managed Cloud Services Advanced Plus(http://doc.arcgis.com/en/trust/security/esri-managed-cloudservices.htm).	ArcGIS Online は顧客に、管理者ユーザーが ArcGIS Online 組織サイトで顧客データを送受信する際に HTTPS (TLS)での暗号化した転送を必須とするオプションを提供しています。 ArcGIS Online は保存された顧客データを暗号化しません。顧客は、顧客のアプリケーションまたはエンタープライズ クラウド暗号化ゲートウェイ ソリューションを利用して、データを暗号化できます。 データの機密度を重視する多くの顧客は、機微なデータをオンプレミスで保有したり、より高いセキュリティ保証がある Esri Managed Cloud Services Advanced Plus (http://doc.arcgis.com/en/trust/security/esri-managed-cloudservices.htm) といった別のクラウドを利用したりするハイブリッド ソリューションを導入しています。	●		A.13.1.1 A.8.3.3 A.13.2.3 A.14.1.3 A.14.1.2 A.10.1.1 A.18.1.3 A.18.1.4	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 IA-7 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-13
Encryption & Key Management Storage and Access 暗号化と鍵の管理 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.	ArcGIS Online Key Management procedures align with FISMA Low requirements.	ArcGIS Online の鍵管理の手順は、FISMA Low 要件に適合します。	●	●	Annex A.10.1 A.10.1.1 A.10.1.2	
Governance and Risk Management Baseline Requirements ガバナンスとリスク管理 基準となる要求	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.	As part of the overall FISMA accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.	総合的な FISMA 認証の一部として、基準となるセキュリティ要求は Continuous Monitoring Program の一部としてレビュー、改善、実装されています。	●		A.14.1.1 A.18.2.3	NIST SP 800-53 R3 CM-2 NIST SP 800-53 R3 SA-2 NIST SP 800-53 R3 SA-4
Governance and Risk Management Data Focus Risk Assessments ガバナンスとリスク管理 データに関するリスク 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: ・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	ArcGIS Online conducts regular risk assessment as part of alignment with FISMA requirements. ArcGIS Online cloud infrastructure providers publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by them.	ArcGIS Online は、FISMA 要件に沿って通常のリスク アセスメントを実施します。ArcGIS Online のクラウド インフラストラクチャ プロバイダーは、確立、運用しているポリシー、手順、規制に関する情報を顧客に提供するため、独立した監査報告書と証明書を発行しています。	●	●	Clauses 5.2(c) 5.3(a) 5.3(b) 6.1.2 6.1.2(a)(2) 6.1.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.2 8.3 9.2(g) A.18.1.1 A.18.1.3 A.18.1.4 A.8.2.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SI-12
Governance and Risk Management Management Oversight ガバナンスとリスク管理 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.	Managers of ArcGIS Online employees are responsible for ensuring awareness of applicable security policies and procedures for team members.	ArcGIS Online 従業員のマネージャーは、チーム メンバーに適切なセキュリティ ポリシーと手順を認識させる責任があります。	●	●	Clause 7.2(a,b) A.7.2.1 A.7.2.2 A.9.2.5 A.18.2.2	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-5 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7
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	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	ArcGIS Online's ISMP is based upon NIST standards as part of FISMA accreditation. For international customers, a mapping of FISMA security controls to ISO 27001 controls is available in NIST Special Publication 800-53 , Appendix H available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf Cloud infrastructure providers implement ISO 27001 certified ISMP's.	ArcGIS Online の ISMP は、FISMA 認証の一部として、NIST 標準に基づいています。海外の顧客に対しては、ISO 27001 コントロールに対するFISMA セキュリティ コントロールの関連付けは NIST Special Publication 800-53 で確認できます。下記 URL の Appendix H をご参照ください：http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf クラウド インフラストラクチャ プロバイダーはISMP で認証された ISO 27001 を実装しています。	●	●	All in sections 4, 5, 6, 7, 8, 9, 10. A.6.1.1 A.13.2.4 A.6.1.3 A.6.1.4 A.18.2.1	
Governance and Risk Management Management Support/Involvement ガバナンスとリスク管理 管理サポート / 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.	Esri's security policies are signed and reviewed by executive management and disseminated to team members in alignment with the FISMA accreditation. Cloud infrastructure providers ensure policy and procedures are in alignment with ISO 27001 standards.	Esri のセキュリティ ポリシーは FISMA 認証に沿って、経営幹部が署名、レビューを行い、チームメンバーに伝達されます。クラウド インフラストラクチャ プロバイダーはポリシーと手順が ISO 27001 標準に沿っているかを確認しています。	●		All in section 5 plus clauses 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c)	NIST SP 800-53 R3 CM-1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Governance and Risk Management Policy ガバナンスとリスク管理 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.	For more information, see GRM-05 above.	詳細は、上部の GRM-05 をご参照ください。	●	●	Clause 4.3 Clause 5 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c) 7.2(d) 7.3(b) 7.3(c) A5.1.1 A.7.2.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1
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	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.	ArcGIS Online and cloud infrastructure employees who violate company standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed.	企業の基準や規約に違反した ArcGIS Online 及びクラウド インフラストラクチャ プロバイダーの従業員は調査され、適切な懲戒処分（例：注意、業務改善計画、停職、解雇）を行います。	●	●	A7.2.3	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-8
Governance and Risk Management Policy Impact on Risk Assessments ガバナンスとリスク管理 リスク アセスメントに基づいたポリシーへの反映	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Decisions to update policies and procedures are based on the risk assessment reports. Risk Assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.	ポリシー及び手順を更新する決定は、リスク アセスメント レポートに基づいています。リスク アセスメントは周期性および、リスク展望図に現れた変更を基に定期的にレビューを行っています。	●	●	Clause 4.2.1 a. 4.2(b) 4.3 c. 4.3(a&b) 4.4 5.1(c) 5.1(d) 5.1(e) 5.1(f) 5.1(g) 5.1(h) 5.2 5.2 e. 5.2(f) 5.3 6.1.1(e)(2). 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 6.2 e. 6.12 (a) (2). 7.1 7.2(a). 7.2(b) 7.2(c) 7.2(d) 7.3(b). 7.3(c) 7.4 7.5.1 (a) 8.1*, partial 8.2 9.1 9.1 e. 9.2. 9.3 9.3(a) 9.3(b&f) 9.3(c). 9.3(c)(1) 9.3(c)(2). 9.3(c)(3) 9.3(d) 9.3(e) 10.1(c) 10.2. A.5.1.2 A.12.1.2 A.15.2.2 A.17.1.1 A.18.2.2 A.18.2.3	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-3 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1
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	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.	ArcGIS Online security policies undergo a formal review and update process at a regularly scheduled interval not to exceed 3 years as part of the FISMA continuous assessment and monitoring process. In the event a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.	ArcGIS Online セキュリティ ポリシーは、FISMA の継続的な評価及び監視プロセスの一部として、3 年未満の間隔の定期スケジュールで、公式のレビュー及び更新プロセスを実施しています。セキュリティ要求で重要な変更が必要な際は、定期スケジュール以外でレビュー及び更新が行われる場合があります。	●	●	Clause 8.1 A.5.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1
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	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).	Risk Assessments are performed on a regular basis and a continuous monitoring plan is in place as specified by FISMA requirements for ArcGIS Online.	ArcGIS Online の FISMA 要求に規定されているように、定期的なリスク アセスメントと継続的な監視計画は実施しています。	●	●	Clause 4.2(b). 6.1.1. 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2). 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1). 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3. 6.1.3(a) 6.1.3(b) 8.1. 9.3(a). 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.17.1.1 A.18.1.1 A.18.2.2. A.18.2.3	NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Governance and Risk Management Risk Management Framework ガバナンスとリスク管理 リスク管理のフレームワーク	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.	The ArcGIS Online FISMA based Risk Assessment Assess phase begins with identifying risks, establishing a risk level by determining the likelihood of occurrence and impact, and finally, identifying controls and safeguards that reduce the impact of the risk to an acceptable level. Accordingly, measures, recommendations and controls are put in place to mitigate the risks to the extent possible.	ArcGIS Online の FISMA に基づいた リスク アセスメントの評価段階では、まずリスクを特定し、発生及び影響の可能性を決定することでリスク レベルを確立します。そして、制御及び予防対策を特定し、リスクの影響を許容できるレベルまで下げます。それに伴い、リスクを可能な限り軽減するように、対策、提案、制御方法を整備します。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.12.6.1 A.17.1.1 A.18.2.2 A.18.2.3	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CA-6 NIST SP 800-53 R3 CA-7 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 RA-2 NIST SP 800-53 R3 RA-3
Human Resources Asset Returns 人事 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.	Employees, contractors and third party users are notified to destroy or return, as applicable, any physical materials that Esri has provided to them during the term of employment or the period of Contractor agreement and any electronic media must be removed from Contractor or third party infrastructure.	従業員、契約者、第三者ユーザーは、Esri から雇用期間あるいは契約期間内に提供された物理的な素材を破棄または返却するように通知されています。電子メディアは契約者あるいは第三者の基盤から削除しなければなりません。	●	●	A.8.1.1 A.8.1.2 A.8.1.4	NIST SP 800-53 R3 PS-4
Human Resources Background Screening 人事 経歴調査	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.	All ArcGIS Online and cloud infrastructure provider employees are required to complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment, and criminal history.	すべての ArcGIS Online とクラウド インフラストラクチャ プロバイダーの従業員は、雇用プロセスの一環として標準的な身元確認を行うことが要求されています。身元確認は、候補者の学歴、雇用履歴、犯罪履歴などに関する情報の確認を含みますが、これらに限定されません。	●	●	A.7.1.1	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-3
Human Resources Employment Agreements 人事 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.	As part of the ArcGIS Online FISMA accreditation employees must sign a Rules of Behavior (RoB) document further enforcing requirements beyond the company employee handbook. Cloud infrastructure providers have their own security training and employee agreements they enforce aligning with ISO 27001 standards.	ArcGIS Online の FISMA 認証の一部として、従業員は会社の従業員ハンドブック以外の要求の順守に関する Rules of Behavior (RoB) に署名しなければなりません。クラウド インフラストラクチャ プロバイダーは独自のセキュリティ トレーニングや ISO 27001 に沿った雇用契約書を提供しています。	●	●	A.13.2.4 A.7.1.2	NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Human Resources Employment Termination 人事 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.	Esri Human Resources Policy drives employee termination processes for ArcGIS Online.	Esri の人事ポリシーは、ArcGIS Online に関わる従業員の退職手続きを適切に行っています。	●	●	A.7.3.1	NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-8
Human Resources Mobile Device Management 人事 モバイル端末管理	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).	Esri has an established mobile device policy. Esri Cloud infrastructure provider personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by cloud infrastructure management.	Esri はモバイル デバイス ポリシーを確立しています。Esri のクラウド インフラストラクチャ プロバイダーの担当者は適切なポリシーを順守することが要求されています。ポリシーでは、クラウド インフラストラクチャ マネージメントによって使用を許可されない限り、モバイル コンピューター デバイスを本番運用環境に持ち込むことを禁止しています。	●	●	A.8.2.1 A.8.3.1 A.8.3.2 A.8.3.3 A.6.2.1 A.6.2.2 A.18.1.4	NIST SP 800-53 R3 AC-17 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 AC-19 NIST SP 800-53 R3 MP-2 NIST SP 800-53 R3 MP-6
Human Resources Non-Disclosure Agreements 人事 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.	Esri Legal Counsel manages and periodically revises the Esri NDA to reflect ArcGIS Online business needs.	Esri Legal Counsel は、ArcGIS Online のビジネス需要を反映して、 Esri NDA (秘密保持契約) の管理と定期的な修正を行っています。	●	●	A.13.2.4	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-9
Human Resources Roles / Responsibilities 人事 役割 / 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.	ArcGIS Online system administrator roles and responsibilities are documented within the ArcGIS Online System Security Plan. User roles and responsibilities are documented within the ArcGIS Online application documentation.	ArcGIS Online システム管理者の役割と責任は、ArcGIS Online System Security Plan 内に文書化されています。利用者の役割と責任は ArcGIS Online の申請書に文書化されています。	●	●	Clause 5.3 A.6.1.1 A.6.1.1	NIST SP 800-53 R3 PL-4 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 PS-2 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Human Resources Technology Acceptable Use 人事 デバイス利用における技術的な対策	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.	Prior to granting access to ArcGIS Online services, customers are required to review and agree to the terms of use. The ArcGIS Online terms of use are available at: http://www.esri.com/legal/pdfs/mla_e204_e300/english.html Customers are responsible for ensuring users are aware of their own organization's acceptable use agreement. Organizations can choose to display a banner within their ArcGIS Online organization to communicate messages such as this. The Esri Employee Handbook specifies acceptable terms of use for all employees. For employees that work with ArcGIS Online, a separate Rules of Behavior (ROB) document is signed.	ArcGIS Online サービスへのアクセスの許諾前に、顧客は利用規約を見直し、承諾することが要求されています。ArcGIS Online の利用規約については、下記の URL をご参照ください。 http://www.esri.com/legal/pdfs/mla_e204_e300/english.html 顧客は、自身の組織の容認できる利用規定であることを確認する責任があります。組織はこのようなメッセージを伝えるために、ArcGIS Online の組織内でバナー表示を選択することができます。Esri Emplyee Handbook はすべての従業員に適切な利用規約を明記しています。ArcGIS Online に関わる従業員は、別の Rules of Behavior (ROB) 文書に署名しています。	●	●	A.8.1.3	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-8 NIST SP 800-53 R3 AC-20 NIST SP 800-53 R3 PL-4
Human Resources Training / Awareness 人事 訓練 / 意識向上	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.	Annual security training is provided for ArcGIS Online employees.	ArcGIS Online の従業員に対して、年に 1 回のセキュリティ トレーニングが提供されます。	●	●	Clause 7.2(a), 7.2(b) A.7.2.2	NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4
Human Resources User Responsibility 人事 利用者の責任	HRS-10	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	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities.	ArcGIS Online の従業員は利用者の責任の概要を説明した Rules of Behavior (ROB) ポリシーを順守しています。	●	●	Clause 7.2(a), 7.2(b) A.7.2.2 A.9.3.1 A.11.2.8	NIST SP 800-53 R3 AT-2 NIST SP 800-53 R3 AT-3 NIST SP 800-53 R3 AT-4 NIST SP 800-53 R3 PL-4
Human Resources Workspace 人事 作業場所	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.	Technical and procedural controls are part of ArcGIS Online's policies including areas such as defined session time-out requirements.	セッションのタイムアウト要件を定義するなどの技術的及び手順制御は、ArcGIS Online のポリシーに含まれます。	●	●	Clause 7.2(a), 7.2(b) A.7.2.2 A.11.1.5 A.9.3.1 A.11.2.8 A.11.2.9	NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 MP-2
Identity & Access Management Audit Tools Access ID とアクセスの管理 監査ツールへのアクセス	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.	Access to information systems audit tools are restricted to authorized personnel within ArcGIS Online.	情報システム監査ツールへのアクセスは、ArcGIS Online 内の権限を与えられた担当者にのみ制限されています。	●	●		NIST SP 800-53 R3 AU-9

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Identity & Access Management Credential Lifecycle / Provision Management ID とアクセスの管理 認証情報のライフサイクル / 規定の管理	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: ・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	ArcGIS Online employees adhere to a rules of behavior policy outlining user access. Operations personnel revoke physical and logical access privileges as a component of the termination process.	ArcGIS Online の従業員は、利用者アクセスの概要を説明した Rules of Behavior (ROB) を順守しています。運営担当者は、退職プロセスの一環として物理的及び論理的なアクセス権を無効にします。	●		A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-7 NIST SP 800-53 R3 AC-14 NIST SP 800-53 R3 IA-1
Identity & Access Management Diagnostic / Configuration Ports Access ID とアクセスの管理 診断 / 構成ポートへのアクセス	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Access to information system diagnostic and configuration ports is restricted to authorized personnel within ArcGIS Online.	情報システムの診断および構成ポートへのアクセスは、ArcGIS Online 内の権限を与えられた担当者に制限されています。	●	●	A.13.1.1 A.9.1.1 A.9.4.4	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 MA-4 NIST SP 800-53 R3 MA-5
Identity & Access Management Policies and Procedures ID とアクセスの管理 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.	Customers have the responsibility of managing access and privilege levels to their ArcGIS Online organization. The use of Enterprise Logins (using SAML 2.0) to identity federation and the use of custom roles in ArcGIS Online to granularly define privileges are recommended best practices. Less than 10 ArcGIS Online Administrators are responsible for managing ArcGIS instances and connect using X.509 certificates. Cloud infrastructure providers have controls in place for limiting access that align with ISO 27001 and FedRAMP Moderate requirements.	顧客は、ArcGIS Online 組織へのアクセスや権限レベルを管理する責任があります。権限を細かく定義した ArcGIS Online のカスタム ロールの使用とフェデレーションを特定するために、SAML 2.0 を使用したエンタープライズ ログインの使用をベスト プラクティスとして推奨しています。 ArcGIS Online の管理者は 9 人以下で、ArcGIS インスタンスを管理する責任があり、 X.509 証明書を使用して接続しています。 クラウド インフラストラクチャ プロバイダーは、ISO27001 と FedRAMP Moderate 要求に沿ったアクセスの制限を適切に制限しています。	●		Annex A.9.2 A.9.2.1 A.9.2.2 A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6	
Identity & Access Management Segregation of Duties ID とアクセスの管理 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.	Cloud infrastructure providers utilize segregation of duties for critical functional to minimize the risk of unintentional or unauthorized access or change to production systems. Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher, and User. For additional information, see: http://doc.arcgis.com/en/arcgisonline/reference/roles.htm	クラウド インフラストラクチャ プロバイダーは、意図していないあるいは認証されていないアクセスを最小限にしたり、本番運用システムに変更するために、重要な機能に職務分離方針を採用しています。顧客は、ArcGIS Online 組織のリソースの職務分離方針を管理する能力を保持しています。ArcGIS Online 内のカスタム ロールの使用は、特定のユーザー グループの許可を、デフォルトのロール (管理者、公開者、ユーザー) よりもさらに細かく適用させることができます。詳細は、下記の URL をご参照ください： http://doc.arcgis.com/ja/arcgis-online/reference/roles.htm	●		A.6.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-6
Identity & Access Management Source Code Access Restriction ID とアクセスの管理 ソース コードのアクセス制限	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.	ArcGIS Online source code libraries are limited to authorized personnel. Source code libraries enforce control over changes to source code by requiring a review from designated reviewers prior to submission. An audit log detailing modifications to the source code library is maintained.	ArcGIS Online のソースコード ライブラリは、権限のある担当者に制限されています。ソースコード ライブラリは送信前に、指名された校正者からのレビューを要求し、ソースコードの変更の制限を実施しています。ソースコード ライブラリの変更を詳細に記述した監査ログはメンテナンスされています。	●		Clause 5.2(c) 5.3(a), 5.3(b), 7.5.3(b) 7.5.3(d) 8.1, 8.3 9.2(g) A.9.4.5 A.18.1.3	
Identity & Access Management Third Party Access ID とアクセスの管理 第三者のアクセス	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.	Third party cloud infrastructure provider access to ArcGIS Online customer data is heavily restricted. Cloud infrastructure provider access is only available on a need-to-know basis and managed by their ISO 27001 security controls.	第三者クラウド インフラストラクチャ プロバイダーの ArcGIS Online 顧客データへのアクセスは、厳しく制限されています。クラウド インフラストラクチャ プロバイダー アクセスは、ISO 27001 セキュリティ コントロールによって管理され Need to know の原則で利用されています。	●	●	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AT-1 NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 CA-1 NIST SP 800-53 R3 CM-1 NIST SP 800-53 R3 CP-1 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 MA-1 NIST SP 800-53 R3 MP-1 NIST SP 800-53 R3 PE-1 NIST SP 800-53 R3 PL-1 NIST SP 800-53 R3 PS-1 NIST SP 800-53 R3 RA-1 NIST SP 800-53 R3 SA-1 NIST SP 800-53 R3 SC-1 NIST SP 800-53 R3 SI-1
Identity & Access Management Trusted Sources ID とアクセスの管理 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.	Customers have the responsibility of managing access and privilege levels to their ArcGIS Online organization. The use of Enterprise Logins (using SAML 2.0) for identity federation to authenticate and the use of custom roles in ArcGIS Online to granularly define privileges are recommended best practices. Less than 10 Esri employees, that are specialized ArcGIS Online administrators, utilizing X.509 certificates for authentication, have access to customer data.	顧客は、ArcGIS Online 組織に対するアクセスや権限のレベルを管理する責任があります。権限を細かく定義した ArcGIS Online のカスタム ロールの使用とフェデレーションを特定するために、SAML 2.0 を使用したエンタープライズ ログインの使用をベスト プラクティスとして推奨しています。 ArcGIS Online の管理に特化した 9 人以下の Esri の従業員は、 認証に、X.509 証明書を使用し、顧客データにアクセスします。	●	●	Annex A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5	
Identity & Access Management User Access Authorization ID とアクセスの管理 ユーザーへのアクセス権限	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.	Less than 10 Esri employees, that are specialized ArcGIS Online administrators, utilizing X.509 certificates for authentication, have access to customer data.	ArcGIS Online 管理に特化した 9 人以下の Esri 従業員は、認証に X.509 証明書を利用し、顧客データにアクセスします。	●	●	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1	NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-4 NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-8 NIST SP 800-53 R3 MA-5 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 SA-7

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Identity & Access Management User Access Reviews ID とアクセスの管理 ユーザー アクセスのレビュー	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.	Customers are responsible for reviewing their user access to their ArcGIS Online organization at defined intervals. The use of Enterprise Logins (using SAML 2.0) is a best practice recommendations to ensure built-in accounts are minimally used. In alignment with FISMA requirements, ArcGIS Online system user access, at all levels, is reviewed at least once per quarter. Customers control access by their own users and are responsible for ensuring appropriate review of such access.	顧客は、決められた間隔で、ArcGIS Online 組織サイトへのアクセスをレビューする責任があります。SAML 2.0 を使用したエンタープライズ ログインの使用は、ビルトイン アカウントを最低限に使用するベスト プラクティスを推奨しています。FISMA 要件に沿って、ArcGIS Online のすべてのレベルでのシステム ユーザー アクセスを少なくとも四半期ごとに見直しています。顧客は、自身が管理するユーザーによるアクセスを制御し、そのようなアクセスの適切なレビューを行う責任があります。	●	●	A.9.2.5	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 PS-6 NIST SP 800-53 R3 PS-7
Identity & Access Management User Access Revocation ID とアクセスの管理 ユーザー アクセスの取り消し	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.	Customers are responsible for managing access to the applications and services customers host on ArcGIS Online. The use of Enterprise Logins (using SAML 2.0) minimizes the requirements for built-in ArcGIS Online accounts and would ensure that removal of a customer user from their Active Directory (or LDAP) would ensure access to ArcGIS Online was also no longer possible.	顧客は、ArcGIS Online にホストしたアプリとサービスへのアクセスを管理する責任があります。SAML 2.0 を使用したエンタープライズ ログインの使用は、ビルトインの ArcGIS Online アカウントの要件を最小限にします。また、Active Directory（または LDAP）から顧客のユーザーを削除すると、ArcGIS Online へのアクセスも不可になることを保証します。	●		Annex A A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.3	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 PS-4 NIST SP 800-53 R3 PS-5
Identity & Access Management User ID Credentials ID とアクセスの管理 ユーザー 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: ・ 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)	Organizations should utilize ArcGIS Online Enterprise Logins to meet all of their organizations username and password management requirements and for adherence to FISMA and ISO 27001 security requirements. Further information concerning ArcGIS Online Enterprise Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterpriselogins.htm If an Identity Provider (IdP) is not available. ArcGIS Online enabled Administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgisonline/administer/configure-security.htm	組織は、ArcGIS Online エンタープライズ ログインを利用し、組織のすべてのユーザー名とパスワード管理の要件に合致させ、 FISMA 及び ISO 27001 セキュリティ要件に順守させることができます。ArcGIS Online エンタープライズ ログインに関する詳細は、下記の URL をご参照ください： http://doc.arcgis.com/ja/arcgis-online/administer/enterprise-logins.htm ID プロバイダーを利用できない場合、ArcGIS Online 組織サイトで管理者がカスタム パスワード ポリシーを実装することも可能です。設定が固定されたユーザー ID ロックアウトを除き、パスワード ポリシーで組織の要件や顧客のポリシーに記述された要件に合致するようにカスタマイズすることができます。カスタム パスワード ポリシーの設定についての詳細は、下記の URL をご参照下さい： http://doc.arcgis.com/ja/arcgis-online/administer/configure-security.htm	●	●	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.4 A.9.2.5 A.9.4.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-2 NIST SP 800-53 R3 AC-3 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IA-1 NIST SP 800-53 R3 IA-2 NIST SP 800-53 R3 IA-2 (1) NIST SP 800-53 R3 IA-5 NIST SP 800-53 R3 IA-5 (1) NIST SP 800-53 R3 IA-6 NIST SP 800-53 R3 IA-8
Identity & Access Management Utility Programs Access ID とアクセスの管理 ユーティリティ プログラムのアクセス	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Customer can choose to use the built-in ArcGIS Online user store or use Enterprise Logins which allows customers to leverage their enterprise AD/LDAP by using an SAML 2.0 compliant Identity Provider (IdP). This would ensure that once a user account is disabled in an organization enterprise user store (AD/LDAP), that user would no longer be able to access ArcGIS Online.	顧客は、ビルトインの ArcGIS Online ユーザー ストアや SAML 2.0 対応した ID プロバイダーを使用して、顧客がエンタープライズ AD/LDAP の活用を許可するエンタープライズ ログインを使用することを選択できます。組織のエンタープライズ ユーザー ストア (AD/LDAP) でユーザー アカウントを無効化すると、そのユーザーは、ArcGIS Online にアクセスできなくなります。	●	●	A.9.1.2 Deleted A.9.4.4	NIST SP 800-53 R3 CM-7
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	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.	Access to logs is restricted as defined by policy, and logs are reviewed on a regular basis in alignment with FISMA Low requirements.	ログへのアクセスは、ポリシーによって定義されたように制限され、ログは FISMA Low 要件に沿って定期的にレビューされています。	●		A.12.4.1 A.12.4.1 A.12.4.2, A.12.4.3 A.12.4.3 A.12.4.1 A.9.2.3 A.9.4.4 A.9.4.1 A.16.1.2 A.16.1.7 A.18.2.3 A.18.1.3	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-2 NIST SP 800-53 R3 AU-3 NIST SP 800-53 R3 AU-4 NIST SP 800-53 R3 AU-5 NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 AU-12 NIST SP 800-53 R3 PE-2 NIST SP 800-53 R3 PE-3
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	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).	Base virtual machine images are provided by the cloud infrastructure provider and refreshed as part of new releases. Console interfaces provide status information for each virtual machine.	クラウド インフラストラクチャ プロバイダーによって仮想マシン イメージが提供され、新しいリリースの一部として更新されます。コンソール インターフェイスは、各仮想マシンのステータス情報を提供します。	●		Annex A.12.1.2 A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	
Infrastructure & Virtualization Security Clock Synchronization インフラと仮想化のセキュリティ 時間の同期	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.	In order to both increase the security of ArcGIS Online, and to provide accurate reporting detail in event logging and monitoring processes and records, all services use consistent clock setting standards (e.g. PST, GMT, UTC etc.). When possible, server clocks are synchronized through the Network Time Protocol which hosts a central time source for standardization and reference, in order to maintain accurate time throughout the ArcGIS Online systems.	ArcGIS Online のセキュリティの向上と、プロセスとレコードを監視しログを取得する場合、正確な報告詳細を提供するために、すべてのサービスは PST, GMT, UTC などの一貫した時刻設定標準を使用しています。可能な場合、サーバーの時間は、標準化と参照のために、中央時間の情報源をホストしている Network Time Protocol を通じて、ArcGIS Online システム全体の正確な時間を維持するように同期しています。	●		A.12.4.1 A.12.4.4	NIST SP 800-53 R3 AU-1 NIST SP 800-53 R3 AU-8
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	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.	ArcGIS Online utilizes the capacity of two major cloud infrastructure providers to meet customer demands. Each cloud provider offers SLAs for their infrastructure – Esri provides an SLA for ArcGIS Online available at: http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-ArcGIS Online-service-level.pdf.	ArcGIS Online は、主要な 2 つのクラウド インフラストラクチャ プロバイダーを利用し、顧客のアクセス需要に応えています。各クラウド インフラストラクチャ プロバイダーは、使用しているインフラストラクチャの SLA を提供しています。Esri の ArcGIS Online の SLA は下記の URL をご参照ください： http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-agol-service-level.pdf	●	●	A.12.1.3	NIST SP 800-53 R3 SA-4
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	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments.	クラウド インフラストラクチャ プロバイダーの仮想化技術は、内部および独立した評価者によって定期的に評価されます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)	
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	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.	The cloud infrastructure providers utilize multiple separate network segments. This infrastructure provider segmentation helps to provide separation of critical, back-end servers and storage devices from the public-facing interfaces.	クラウド インフラストラクチャ プロバイダーは、複数の分けられたネットワーク セグメントを利用しています。クラウド インフラストラクチャ プロバイダー セグメンテーションは、一般に公開されているインターフェイスから重大なバックエンド サーバーとストレージ デバイスの分割した提供を促進しています。	●	●	A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4	NIST SP 800-53 R3 CM-7 NIST SP 800-53 R3 SC-7 NIST SP 800-53 R3 SC-20 (1)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	AroGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	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.	ArcGIS Online uses a standard image for all instances and this includes the deployment of anti-virus on customer-facing instances. Logging within ArcGIS Online aligns with FISMA Low requirements.	ArcGIS Online は、全てのインスタンスで標準イメージを使用しており、これは顧客に公開されたインスタンスで、ウイルス対策の配置を含んでいます。ArcGIS Online 内へのログインは、FISMA Low 要件に沿っています。	●	●	Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	
Infrastructure & Virtualization Security Production / Non-Production Environments インフラと仮想化のセキュリティ 本番運用/ 非本番運用環境	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.	ArcGIS Online utilizes separate production and non-production environments.	ArcGIS Online は区別された本番運用環境と非本番運用環境を使用しています。	●		A.12.1.4 A.14.2.9 A.9.1.1 8.1,partial, A.14.2.2 8.1,partial, A.14.2.3 8.1,partial, A.14.2.4	
Infrastructure & Virtualization Security Segmentation インフラと仮想化のセキュリティ 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: ・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	Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls and host based firewalls are utilized to separate various ArcGIS Online components.	クラウド インフラストラクチャ プロバイダーのネットワークの区分は、ISO27001 の標準に基づいて行われています。クラウド インフラストラクチャ プロバイダーのファイアウォールとホスト ベースのファイアウォールは、さまざまな ArcGIS Online のコンポーネントを区別するために使われています。	●	●	A.13.1.3 A.9.4.1 A.18.1.4	NIST SP 800-53 R3 SC-7
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	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.	Customers can migrate data to ArcGIS Online via HTTPS for encrypted communitcation. Customers can also deploy a separate non-production ArcGIS Online organization for initial data migrating /testing efforts.	顧客は、ArcGIS Onlineに HTTPS 経由で暗号化されたデータを送ることができます。顧客は、初期データの移行や検証の際に、区別された非本番運用環境の ArcGIS Online 組織サイトを配置できます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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 - ハイパーバイザー堅牢性	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).	ArcGIS Online's cloud infrastructure providers use a concept of least privilege for assigning access to all functions. These technical and procedural controls align with ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online のクラウド インフラストラクチャ プロバイダーが全機能へのアクセスを付与する際には最小権限の原則を利用しています。これらの技術上、手続き上の管理は ISO27001 と FedRAMP Moderate の必要事項に基づいて行われます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d), 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	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	Protection of wireless devices and ensuring encryption are part of regular network management security practices within Esri which includes monitoring.Access from a wireless network on a customer premise to the ArcGIS Online environment must be secured by the customer.	無線機器の保護、暗号化の徹底は Esri 社の監視を含む、標準のネットワーク管理のセキュリティ対策の一部です。顧客の敷地内の無線ネットワークからの ArcGIS Online 環境へのアクセスは、顧客自身で保全されなければなりません。	●	●	A.8.1.1 A.8.1.2 A.8.1.3 A.11.2.1 A.11.2.4 A.13.1.1 A.13.1.2 A.13.2.1 A.8.3.3 A.12.4.1 A.9.2.1, A.9.2.2 A.13.1.3 A.10.1.1 A.10.1.2	NIST SP 800-53 R3 AC-1 NIST SP 800-53 R3 AC-18 NIST SP 800-53 R3 CM-6 NIST SP 800-53 R3 SC-7
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	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.	ArcGIS Online's cloud infrastructure providers are subjected to regular internal and external testing. In addition their security controls are reviewed regularly by independent auditors and align with ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online のクラウド インフラストラクチャー プロバイダーは、定期的に内部・外部監査を受けます。また、そのセキュリティー管理は独立した監査者によって定期的に見直され、ISO27001 と FedRAMP Moderate の必要事項に基づいています。	●	●		

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Interoperability & Portability APIs 相互運用性とポータブル性 API	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	The ArcGIS Online API is publically available. For more information see: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm	ArcGIS Online の API は、誰にでも利用可能です。詳細は下記ページをご参照ください: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Interoperability & Portability Data Request 相互運用性とポータブル性 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)	Customers retain ownership of their data at all times and can export their data from ArcGIS Online in standard formats at any time.	顧客は、所有するデータの所有権を常に保有しており、いつでも標準の形式でデータを ArcGIS Online からエクスポートできます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Interoperability & Portability Policy & Legal 相互運用性とポータブル性 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.	The ArcGIS Online REST API is publically available. For more information see: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm . Legal aspects are addressed as part of the Terms of Service at: http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3	ArcGIS Online の REST API は誰でも利用可能です。詳細は下記ページをご参照ください: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm 法律的な事項はサービス規約 (http://www.esri.com/legal/pdfs/mla_e204_e300/english#Addendum_3)の一部で取り組まれています 。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Interoperability & Portability Standardized Network Protocols 相互運用性とポータブル性 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.	Customer's retain ownership of their data at all times and are responsible for the import and export of that data into their ArcGIS Organization. Customer can require HTTPS for their ArcGIS Online organization to ensure data is sent over encrypted means and they must be authenticated to ArcGIS Online to perform this function.	顧客は、所有するデータの所有権を常に保有しており、そのデータの ArcGIS Online 組織アカウントへのインポートとエクスポートに責任を持ちます。顧客は HTTPS を利用して、ArcGIS Online 組織サイトのデータを暗号化して送信することが可能ですが、この機能を利用するためには ArcGIS Online で認証を行う必要があります。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Interoperability & Portability Virtualization 相互運用性とポータブル性 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.	ArcGIS Online's cloud infrastructure providers have virtualization platforms that are reviewed regularly by independent audits and align with ISO 27001 and FedRAMP Moderate requirements. The virtual machine images are not exposed/provided to customers so the utilization of OVF is not appliable.	ArcGIS Online のクラウド インフラストラクチャー プロバイダーは、独立した監査者に定期的に監査され、また ISO 27001 とFedRAMP Moderate の必要事項に基づいた、仮想化プラットフォームを保有しています。仮想マシンのイメージは顧客に公開も提供もされず、OVF の利用も出来ません。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Anti-Malware モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Awareness and Training モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Compatibility モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Mobile Security Device Eligibility モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Device Inventory モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Device Management モバイル セキュリティ デバイス管理	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Encryption モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答（日本語訳）	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	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).	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Legal モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Lockout Screen モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービスプロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Mobile Security Passwords モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Policy モバイル セキュリティ 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).	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Mobile Security Remote Wipe モバイル セキュリティ 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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	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.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
Mobile Security Users モバイル セキュリティ ユーザー	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Wireless/mobile access to cloud infrastructure provider networks is not permitted within the datacenters. Customers are responsible for the control, security, and management of their mobile devices that are used to connect to ArcGIS Online content.	データセンター内でのクラウド インフラストラクチャ プロバイダーのネットワークへの無線・モバイル アクセスは禁止されています。顧客は、ArcGIS Online のコンテンツへ接続して使用するモバイル端末の監視や、セキュリティ、管理に責任を持ちます。	●	●	Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
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	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.	Esri maintains contact with external parties such as regulatory bodies, service providers, and industry forums to ensure appropriate action can be quickly taken and advice obtained when necessary.	Esri は、規制機関、サービス プロバイダー、業界フォーラムなど、必要な時に適切な措置を講じたり助言することを保証する外部の組織と連携しています。	●	●	A.6.1.3 A.6.1.4	NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 SI-5
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	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.	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FISMA requirements.	インシデント管理は、FISMA の要件に整合している ArcGIS Online のインシデント レスポンス プランの文書に記述されています。	●	●	Clause 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex A.16.1.1 A.16.1.2	NIST SP 800-53 R3 IR-1 NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7
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	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.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FISMA requirements. Customers can inform the security team directly of any suspected information security event through the 'Report a Security Concern' page on the Trust.ArcGIS.com site at: http://doc.arcgis.com/en/trust/security-concern/	ArcGIS Online のインシデント レスポンス プログラム、プランやその手順は、FISMA の要件に準拠して開発されています。顧客は、疑わしい情報セキュリティの動きについて、「Report a Security Concern」(Trust.ArcGIS.com site at: http://doc.arcgis.com/en/trust/security-concern/) ページで、セキュリティ チームに直接報告することができます。	●	●	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.6.1.1 A.7.2.1, A.7.2.2, A.16.1.2, A.16.1.3, A.16.1.1	NIST SP 800-53 R3 IR-2 NIST SP 800-53 R3 IR-6 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 SI-5
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	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.	ArcGIS Online's incident response program, plans and procedures have been developed in alignment with FISMA requirements.	ArcGIS Online のインシデント レスポンス プログラム、プランやその手順は、FISMA の要件に準拠して開発されています。	●	●	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g) Annex A.7.2.2, A.7.2.3, A.16.1.7, A.18.1.3	NIST SP 800-53 R3 AU-6 NIST SP 800-53 R3 AU-9 NIST SP 800-53 R3 AU-11 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-7 NIST SP 800-53 R3 IR-8
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	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Information security incidents are classified into severity levels and processed according to the severity level.	情報セキュリティ インシデントは、重要レベルで分類され、そのレベルに応じて処理が行われます。	●	●	A.16.1.6	NIST SP 800-53 R3 IR-4 NIST SP 800-53 R3 IR-5 NIST SP 800-53 R3 IR-8
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	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.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online は、ISO27001 および FedRAMP Moderate の要件に沿ってリスク マネージメントが行われているクラウド インフラストラクチャを利用しています。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).	General site information for ArcGIS Online is available via the Status page of the Trust.ArcGIS.com website. Informaiton about customer specific incidents can be viewed via the MyEsri Support portal.	一般的な ArcGIS Online のサイトの情報は、Trust.ArcGIS.com のステータス ページで確認することができます。顧客の特定の問題の情報については、My Esri Support のポータル サイトで参照が可能です。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)	
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	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.	Amazon Web Services and Microsoft Azure public service level agreements are available for review through the respective service providers. Azure's main underlying network infrastructure is currently managed by Microsoft's Global Foundation Services (GFS). SLAs to service providers or equipment manufacturers are qualified by GFS's ISO 27001 certification. Microsoft Azure SLA information is available at: http://www.windowsazure.com/en-us/support/legal/sla/ . Amazon Web Services EC2 SLA information is available at: http://aws.amazon.com/ec2-sla/ other AWS component SLA's are also available at this site.	Amazon Web Service と Microsoft Azure の SLA は、それぞれのサービス プロバイダーで確認が可能です。Azure の基本的なネットワーク インフラストラクチャは、現状 Microsoft の Global Foundation Services (GFS) に管理されています。サービス プロバイダーや製品製造への SLA は、GFS の ISO27001の認証に適合しています。Microsoft Azure のSLA の情報は下記をご参照ください。 http://www.windowsazure.com/en-us/support/legal/sla/ Amazon Web Service の SLA の情報は下記のサイトをご参照ください。 http://aws.amazon.com/ec2-sla/ なお、その他の AWS のコンポーネントの SLA についても、上記と同じサイトで確認が可能です。	●	●	A.15.1.2 A.13.1.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9
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 プロバイダーの内部評価	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	As part of FISMA Low compliance, ArcGIS Online implements a robust continuous monitoring program to monitor risk which includes regular internal assessments.	FISMA Low コンプライアンスに基づき、ArcGIS Online は一定の間隔で行われる内部監査で脅威を監視する堅牢で継続的なプログラムを実装しています。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f) A.14.2.3 A.12.6.1 A.18.1.1 A.18.2.2 A.18.2.3	
Supply Chain Management, Transparency and Accountability Supply Chain 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	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	Third party agreements are reviewed by Esri Contracts and/or Legal Counsel as appropriate.	Esri Contracts や Legal Counsel が必要に応じて第三者との契約条件を審査します。	●	●	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 PS-7 NIST SP 800-53 R3 SA-6 NIST SP 800-53 R3 SA-7 NIST SP 800-53 R3 SA-9
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 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.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online は、ISO27001 および FedRAMP Moderate の要件に沿ってリスクマネージメントが行われているクラウドインフラストラクチャを利用しています。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)	

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ArcGIS Online Response	ArcGIS Online の回答 (日本語訳)	サプライヤーとの関係		適用範囲	
					サービス プロバイダー	テナント/顧客	ISO/IEC 27001:2013	FISMA —LOW IMPACT—
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	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.	See STA-03 for more information.	STA-03 をご参照ください。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)	
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	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.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online は、ISO27001 および FedRAMP Moderate の要件に沿ってリスク マネージメントが行われているクラウド インフラストラクチャを利用しています。	●		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d) 6.1.2(d)(1) 6.1.2(d)(2) 6.1.2(d)(3) 6.1.2(e) 6.1.2(e)(1) 6.1.2(e)(2) 6.1.3, 6.1.3(a) 6.1.3(b) 8.1 8.3 9.3(a), 9.3(b) 9.3(b)(f) 9.3(c) 9.3(c)(1) 9.3(c)(2) 9.3(c)(3) 9.3(d) 9.3(e) 9.3(f)	
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	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.	ArcGIS Online uses cloud infrastructure providers whose risk management practices align with stringent ISO 27001 and FedRAMP Moderate requirements.	ArcGIS Online は、ISO27001 および FedRAMP Moderate 要件に沿ってリスクマネージメントが行われているクラウド インフラストラクチャを利用しています。	●		A.15.1.2 8.1* partial, 8.1* partial, A.15.2.1 A.13.1.2	NIST SP 800-53 R3 CA-3 NIST SP 800-53 R3 SA-9 NIST SP 800-53 R3 SC-7
Threat and Vulnerability Management Anti-Virus / Malicious Software 脅威と脆弱性の管理 アンチウイルス / 悪質なソフトウェア	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.	A number of key security parameters are monitored to identify potentially malicious activity on the systems which includes the use anti-malware software on systems accepting customer datasets/information. Cloud infrastructure provider anti-virus controls align with ISO 27001 requirements.	顧客のデータセットや情報を保持するシステム上で、悪意のある動きを潜在的に特定するために、アンチ-マルウェア ソフトを使用してたくさんのキー セキュリティ パラメーターを監視しています。クラウド インフラストラクチャ プロバイダーのアンチ ウィルス制御は ISO27001 の要件に沿っています。	●	●	A.12.2.1	NIST SP 800-53 R3 SC-5 NIST SP 800-53 R3 SI-3 NIST SP 800-53 R3 SI-5
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	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.	ArcGIS Online releases which include patches and bug fixes are performed quarterly. If security vulnerabilities are found or reported, they are assessed by security staff. Any vulnerabilities that have an assessed risk of high or critical are patched immediately outside of normal patching routines.	ArcGIS Online のパッチや不具合の修正が含まれたリリースは年 4 回行われます。セキュリティの脆弱性が見つかったり報告されたりした場合は、セキュリティ スタッフがそれらを評価します。危険性が高い、重大と判断された脆弱性については、いかなる場合も通常の周期でのパッチ適用ではなく直ちにパッチが適用されます。	●		8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1	NIST SP 800-53 R3 CM-4 NIST SP 800-53 R3 RA-5 NIST SP 800-53 R3 SI-1 NIST SP 800-53 R3 SI-2 NIST SP 800-53 R3 SI-5
Threat and Vulnerbility Management Mobile Code 脅威と脆弱性の管理 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.	ArcGIS Online does not require installable mobile code such as MS ActiveX, Adobe Flash, and MS Silverlight.	ArcGIS Online は、Microsoft ActiveX や Adobe Flash、Silverlight のインストール可能なモバイル コードを必要としません。	●	●	A.12.2.1	