ArcGIS Online

クラウド・セキュリティ・アライアンス（CSA）コンセンサス評価イニシアティブ調査票（CAIQ）4.0.2 - 2023年6月

本資料は、ArcGIS Online の CSA (Cloud Security Alliance) CAIQ (Consensus Assessment Initiative Questionnaire) の質問に対し、Esri 社の自己評価による回答文（英文）とその日本語訳を記載した表です。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お客様や監査役がクラウド プロバイダーに尋ねたい 261 の質問があります。

CSA は、「クラウドコンピューティングにおけるセキュリティ保証を提供するためのベストプラクティスの使用を促進し、クラウドコンピューティングの使用に関する教育を提供することで、他のあらゆる形態のコンピューティングのセキュリティを確保することを目的とした非営利組織」です (https://cloudsecurityalliance.org/about/)。この組織には、幅広い業界のセキュリティ実務者、企業、および団体が参加し、そのミッションを達成しています。Esri は 2013 年から ArcGIS Online CSA の回答を行っており、最新の更新は、最新の CAIQ 4.0.2 調査票に対応したものです。

ArcGIS Online は、米国内務省から FedRAMP ATO (米国連邦政府機関によるリスクおよび承認管理プログラムに基づいた認定) を取得しており、整合性を確保するために、毎年第三者機関の評価者による監査を受けています。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。
https://downloads.esri.com/resources/enterprisegis/AGOL_CSA_CAIQ.pdf

お客様からのよくある質問には、以下のようなものがあります。

- データはどこでホストされていますか？
  - デフォルトでは、US 本土にある AWS および MS Azure のデータセンター内にデータを保管していますが、新しい組織では、データを EU や AP リージョンなどの US リージョン外に保管することを選択できます。
- データは、保管時と転送時に暗号化されていますか？
  - はい。組織は、転送時には HTTPS w/TLS 1.2 を使用し、保管時には AES-256 を使用します。

- データはバックアップされていますか？
  - データセットのバックアップはお客様の責任で行ってください。
- ArcGIS Online に対してセキュリティ テストを行うことはできますか？
  - はい。ただし、まずセキュリティ評価契約（SAA）を完了する必要があります。
- ファイルはアンチウイルスでスキャンされますか？
  - はい。悪意のあるコードを含むファイルは、アップロードが拒否されます。
- プライバシーはどのように保証されていますか？
  - ArcGIS Online は、GDPR および CCPA の両方に準拠しています。

回答に出てくる略語一覧

OWASP: Open Web Application Security Project

NIST: National Institute of Standards and Technology

FedRAMP: Federal Risk and Authorization Management Program

SLA: Service Level Agreement

ご質問/ご意見/ご感想は、Esri の Software Security & Privacy Team にご連絡ください: SoftwareSecurity@Esri.com

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.	Esri は、BSIMM (Building Security In Maturity Model) をバックボーンとして利用して、製品の開発ライフサイクル全体にセキュリティを最も効果的な方法で浸透させるための取り組みを測定しています。 ArcGIS Online は FedRAMP の認定を受けているため、NIST 標準にも準拠しています。詳細については、ArcGIS Trust Center https://trust.arcgis.com のドキュメントに掲載されている「Secure Development Lifecycle Overview」をご参照ください。	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Audit and assurance polices, procedure and standards are established, documented and approved annually.	監査および保証の方針、手順、基準は毎年策定、文書化され、承認されます。		
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by an independent 3rd party assessor as per FedRAMP requirements which utilizes NIST standards.	ArcGIS Online ソリューションは、NIST 標準に準拠する FedRAMP 要件に従って、独立した第三者評価機関によって毎年評価/監査されています。	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP requirements which is based on a risk management framework.	ArcGIS Online ソリューションは、リスク管理のフレームワークに基づく FedRAMP 要件に従って、第三者評価機関によって毎年評価/監査されています。	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	CSP-owned	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. Along with OWASP Top 10 and SANS 25 ArcGIS Online is FedRAMP authorized and therefore aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.	Esri は、BSIMM (Building Security In Maturity Model) をバックボーンとして利用して、製品の開発ライフサイクル全体にセキュリティを最も効果的な方法で浸透させるための取り組みを測定しています。 ArcGIS Online は、OWASP Top 10 および SANS 25 とともに FedRAMP の認定を受けており、NIST 標準に準拠しています。 詳細については、ArcGIS Trust Center https://trust.arcgis.com のドキュメントに掲載されている「Secure Development Lifecycle Overview」をご参照ください。	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	ArcGIS Online solution is annually assessed/audited by a 3rd party assessor as per FedRAMP requirements.	ArcGIS Online ソリューションは、FedRAMP 要件に従って、第三者評価機関によって毎年評価/監査されています。	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online has a Risk Assessment Process in place as part of the Continuous Monitoring Plan, with includes the generation of a Plan of Actions and Milestones (POAM) for resolution.	ArcGIS Online には、継続的モニタリング計画の一環としてリスク評価プロセスが設けられており、解決のための POAM (Plan of Actions and Milestones) の作成が含まれます。	Remediation	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Esri will notify customers about inappropriate access to their data after a confirmation has been made that their data was inappropriately accessed. Web, system and database scans as part of FedRAMP requirements are reviewed and reported. Static, 3rd party analysis is removed and reported https://trust.arcgis.com/en/ for Security Announcements are published to serve as notification of security information	Esri は、お客様のデータが不適切にアクセスされたことが確認された後、お客様に通知します。FedRAMP 要件の一環として、Web、システム、データベースのスキャンがレビューされ、報告されます。静的なサードパーティの分析は削除され、https://trust.arcgis.com/ で報告されます。セキュリティ情報の通知として、セキュリティに関するお知らせが掲載されます。	Remediation	Audit & Assurance
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information	Esri は、BSIMM (Building Security In Maturity Model) をバックボーンとして利用して、製品の開発ライフサイクル全体にセキュリティを最も効果的な方法で浸透させるための取り組みを測定しています。 ArcGIS Online は FedRAMP の認定を受けているため、NIST 標準にも準拠しています。 詳細については、ArcGIS Trust Center https://trust.arcgis.com のドキュメントに掲載されている「Secure Development Lifecycle Overview」をご参照ください。	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	As part of the implemented FedRAMP program Security polices and procedures along with security related areas associated with FedRAMP NIST 800-53 controls are reviewed and updated at least annually.	実装された FedRAMP プログラムの一環として、FedRAMP NIST 800-53 管理に関連するセキュリティ関連分野とともに、セキュリティ ポリシーと手順が少なくとも年 1 回見直され、更新されます。		
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	ArcGIS Online systems are based off the same baseline with CIS Level 1 benchmarks implemented. The Cloud Infrastructure providers who are ISO 270001 certified manage the backend routers, DNS servers and hypervisors	ArcGIS Online のシステムは、CIS レベル 1 ベンチマークが実装された同じベースラインをベースにしています。ISO 270001 認証を取得したクラウド インフラストラクチャ プロバイダーは、バックエンドのルーター、DNS サーバー、ハイパーバイザーを管理しています。	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	As part of FedRAMP compliance, ArcGIS Online implements a robust continuous monitoring program to monitor risk which includes monthly metric review and internal assessments at least annually. Dashboards are also used for performance review and analysis.	FedRAMP Tailored Low コンプライアンスの一環として、ArcGIS Online では、少なくとも年 1 回の内部評価を含むリスク監視のための堅牢な継続的モニタリング プログラムを実施しています。ダッシュボードはパフォーマンスのレビューと分析にも使用されます。	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. ArcGIS Online is FedRAMP authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.	Esri は、BSIMM (Building Security In Maturity Model) をバックボーンとして利用して、製品の開発ライフサイクル全体にセキュリティを最も効果的な方法で浸透させるための取り組みを測定しています。 ArcGIS Online は FedRAMP の認定を受けているため、NIST 標準にも準拠しています。詳細については、ArcGIS Trust Center https://trust.arcgis.com のドキュメントに掲載されている「Secure Development Lifecycle Overview」をご参照ください。	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	ArcGIS Online performs a significant impact assessment for new information systems, upgrades and maintenance. The changes are assessed by the Development and Security Teams to understand operational and security impact. Results are presented to the Configuration Management Board for final decision determination.	ArcGIS Online では、新しい情報システム、アップグレード、保守に関して、重大な影響評価を実施しています。変更は開発チームとセキュリティ チームによって評価され、運用とセキュリティへの影響を把握しています。結果は構成管理委員会に提示され、最終的な決定が下されます。	Automated Application Security Testing	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Development Teams perform automated unit tests and end to end testing. Security performs dynamic scans that must be remediated before moving to production	開発チームは、自動ユニット テストとエンドツーエンドテストを実施します。セキュリティは、本番環境に移行する前に修正する必要がある動的スキャンを実行します。	Automated Application Security Testing	Application & Interface Security
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Nearly all code is covered in automated testing through our secure development lifecycle prior to release	リリース前のセキュアな開発ライフサイクルを通じて、ほぼすべてのコードが自動テストでカバーされています。	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Deployments when triggered are automated to ensure that baselines are pulled from code repos and to ensure that modifications are not made directly to the production area	ベースラインがコード リポジトリから引き出され、本番環境に直接変更が加えられないように、デプロイが自動化されています。		
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	Security vulnerabilities are prioritized based on risk assessment. Teams are expected to remediate or provide mitigation based on risk level	セキュリティの脆弱性は、リスク評価に基づいて優先順位付けされます。各チームは、リスク レベルに基づき、脆弱性の修正または軽減策を提供します。	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	ArcGIS Online has a vulnerability Risk Assessment Process in place as part of the Continuous Monitoring Plan. This process is used to triage each reported security vulnerability or bug before it is submitted to the respective development team in form of a Change Request (CR). Each CR submitted for ArcGIS Online must include a change description, implementation plan, assessed level of risk, impact analysis, back out plan, assigned resources and a test plan prior to being improved. All changes are tested and validated in a test environment prior to being pushed to production. External organizations can report security issues via our Trust Center, report a security concern area, which is managed by our Product Security Incident Response Team (PSIRT).	ArcGIS Online では、継続的監視計画の一環として、脆弱性リスク評価プロセスが実施されています。このプロセスは、報告されたセキュリティの脆弱性または不具合が変更要求 (Change Request: CR) の形で各開発チームに提出される前に、各セキュリティの脆弱性または不具合をトリアージするために使用されます。ArcGIS Online に提出される各 CR には、変更の説明、実装計画、評価されたリスク レベル、影響分析、バックアウト計画、割り当てられたリソース、および改善前のテスト計画が含まれている必要があります。すべての変更は、本番環境に投入される前に、テスト環境でテストおよび検証されます。外部組織は、当社の Trust Center を通じてセキュリティ問題を報告し、当社の PSIRT (Product Security Incident Response Team) が管理するセキュリティ懸念領域を報告することができます。		
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP requirements. The plan has been tested.	ArcGIS Online には、FedRAMP 要件に沿って設計された完全な継続計画があります。この計画はテスト済みです。	Business Continuity Management Policy and Procedures	Business Continuity Management and Operational Resilience
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP requirements. The plan has been tested. This is assessed by a 3rd party to ensure compliance.	ArcGIS Online には、FedRAMP 要件に沿って設計された完全な継続計画があります。この計画はテスト済みです。これは、コンプライアンスを確保するために第三者によって評価されます。		
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	Shared CSP and 3rd-party	ArcGIS Online operation with two Cloud Service Providers AWS & Microsoft Azure and the CSPs operation in multiple Availability Zones as well as regions for redundancy. Some services are only available from one of the providers.	ArcGIS Online は、AWS と Microsoft Azure の 2 つのクラウド サービス プロバイダー (CSP) で運用されており、CSP は複数のアベイラビリティ ゾーンとリージョンで運用され、冗長性を確保しています。一部のサービスは、いずれかのプロバイダーからしか利用できません。	Risk Assessment and Impact Analysis	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	ArcGIS Online systems run active-active across datacenters in a common region, and if those multiple datacenters experience a disaster, the system can be recovered in remote datacenter locations.	ArcGIS Online システムは、共通の地域にある複数のデータセンター間でアクティブ/アクティブ構成で動作し、それらの複数のデータセンターで災害が発生した場合には、リモートのデータ センターの場所でシステムを復旧することができます。	Business Continuity Strategy	Business Continuity Management and Operational Resilience
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	ArcGIS Online maintains a contingency plan and incident response plan that is in alignment with FedRAMP requirements. Documents are reviewed by external auditors as part of FedRAMP requirements.	ArcGIS Online は、FedRAMP 要件に沿った緊急時対応計画およびインシデント対応計画を維持しています。ドキュメントは、FedRAMP 要件の一環として外部監査機関によってレビューされます。	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP-requirements.	ArcGIS Online には、FedRAMP 要件に沿って設計された完全な継続計画があります。	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	ArcGIS Online Business Continuity plan is not shared publicly however, all relevant internal stakeholders have access to the plan.	ArcGIS Online の事業継続計画は一般には公開されていませんが、社内のすべての関係者は計画にアクセスできます。		
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	Esri's Business continuity plan is reviewed periodically.	Esri の事業継続計画は定期的に見直されます。		
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	Esri's business continuity plan is not tested at planned intervals. Esri maintains a detailed Contingency Plan for ArcGIS Online that involves the following: roles and responsibilities of key personnel, notification and escalation procedures, recovery plans, recovery time objective (RTO) and recovery point objective (RPO) and a clearly defined communication process. The ArcGIS Online Contingency Plan is tested at least annually	Esri の事業継続計画は、計画された間隔でテストされていません。Esri は、ArcGIS Online の詳細な緊急時対応計画を維持しており、これには、主要担当者の役割と責任、通知およびエスカレーション手順、復旧計画、復旧時間目標 (Recovery Time Objective: RTO) および復旧ポイント目標 (Recovery Point Objective: RPO)、および明確に定義されたコミュニケーション プロセスが含まれています。ArcGIS Online の緊急時対応計画は、少なくとも年 1 回テストされます。	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	Every personnel who is read into the ArcGIS Online FedRAMP program has access to risk management plan document.	ArcGIS Online FedRAMP プログラムに読み込まれたすべての担当者は、リスク管理計画文書にアクセスできます。	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and CSC	Customers have full responsibility to backup and restore their datasets. Esri is responsible for backup of the infrastructure.	データセットのバックアップと復元は、お客様の全責任において行われます。インフラストラクチャのバックアップは、Esri の責任において行われます。	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and CSC	Esri does backup infrastructure data and customer is responsible for backup of their data at whatever frequency they desire. Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP requirements	Esri はインフラストラクチャ データのバックアップを行い、お客様は希望する頻度でデータのバックアップを行う責任を負います。データは、FIPS 140-2 準拠の暗号化アルゴリズムである AES-256 で保存時に暗号化されます。これは、FedRAMP 要件と一致しています。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	CSP-owned	ArcGIS Online Cloud infrastructure providers align with ISO 27001 and FedRAMP moderate requirements. Customers can extract datasets in a variety of standard formats that they can restore wherever they desire	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 および FedRAMP Moderate の要件に準拠しています。お客様は、さまざまな標準フォーマットでデータセットを抽出し、必要な場所に復元することができます。	Backup	Business Continuity Management and Operational Resilience
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man- made disasters?	Yes	CSP-owned	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP security control requirements. ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.	ArcGIS Online には、FedRAMP セキュリティ コントロール要件に沿った完全な事業継続計画があります。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 標準に準拠していることを保証します。	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	The plan is reviewed and tested annually together as part of our continuity plan.	計画は、継続計画の一部として毎年見直され、テストされます。		
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Esri's business continuity plan is not tested at planned intervals. Esri maintains a detailed Contingency Plan for ArcGIS Online that involves the following: roles and responsibilities of key personnel, notification and escalation procedures, recovery plans, recovery time objective (RTO) and recovery point objective (RPO) and a clearly defined communication process. The ArcGIS Online Contingency Plan is tested at least annually.	Esri の事業継続計画は、計画された間隔でテストされていません。Esri は、ArcGIS Online の詳細な緊急時対応計画を維持しており、これには、主要担当者の役割と責任、通知およびエスカレーション手順、復旧計画、復旧時間目標 (Recovery Time Objective: RTO) および復旧ポイント目標 (Recovery Point Objective: RPO)、および明確に定義されたコミュニケーション プロセスが含まれています。ArcGIS Online の緊急時対応計画は、少なくとも年 1 回テストされます。	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	No	CSP-owned	Local emergency authorities are not included in annual testing.	地域の緊急対策機関は年次テストに参加していません。		
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	Shared CSP and 3rd-party	ArcGIS Online operation with two Cloud Service Providers AWS & Microsoft Azure and the CSPs operation in multiple Availability Zones as well as regions for redundancy. Some services are only available from one of the providers	ArcGIS Online は、AWS と Microsoft Azure の 2 つのクラウド サービス プロバイダー (CSP) で運用されており、CSP は複数のアベイラビリティ ゾーンとリージョンで運用され、冗長性を確保しています。一部のサービスは、いずれかのプロバイダーからしか利用できません。	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	Teams perform impact assessments based on functionality, security and privacy. This would cover both application and infrastructure changes to ArcGIS Online.	各チームは、機能性、セキュリティ、プライバシーに基づく影響評価を実施します。これは、ArcGIS Online に対するアプリケーションとインフラストラクチャの両方の変更が対象です。	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	The configuration management plan and associated procedures are reviewed and updated at least annually. Our configuration management plan highlights security impact assessments to understand risk when handing both application and infrastructure. Changes are flow though Dev, QA then to PROD. During this time Teams are testing and evaluating risk impact.	構成管理計画と関連手順は、少なくとも年 1 回レビューされ、更新されます。構成管理計画では、アプリケーションとインフラストラクチャの両方を取り扱う際のリスクを理解するために、セキュリティの影響評価を重視しています。変更は、開発、QA、PROD の順に流れます。この間、チームはテストを行い、リスクへの影響を評価します。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	ArcGIS Online procedures established for management or acquisition of new application, systems, databases, infrastructure and services is in alignment with FedRAMP requirements.	新しいアプリケーション、システム、データベース、インフラストラクチャ、サービスの管理または取得のために確立された ArcGIS Online の手順は、FedRAMP 要件と一致しています。	Quality Testing	Change Control and Configuration Management
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Changes to our baselines are CM managed regardless of whether asset management occurs internally or externally.	ベースラインの変更は、資産管理が内部で行われるか外部で行われるかにかかわらず、CM で管理されます。	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	Shared CSP and 3rd-party	Development and DevOPs Teams have access to update application code/ configuration and infrastructure configuration through CM procedures. Only authorized Team members have direct access to AWS and Azure. This is reviewed at least quarterly.	開発チームと DevOPs チームは、CM 手順を通じてアプリケーションのコード/構成とインフラストラクチャ構成の更新にアクセスできます。権限を与えられたチーム メンバーだけが、AWS と Azure に直接アクセスできます。これは少なくとも四半期ごとにレビューされます。	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	N/A	CSP-owned	Hardware is transparent to customer of SaaS offering. No customer equipment resides in the SaaS offering	ハードウェアは、SaaS 提供のお客様は意識する必要がありません。SaaS 提供にはお客様の機器は含まれません。	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	All changes to the ArcGIS Online infrastructure are tracked and recorded through the Change Management documented processes and Procedures, scheduled maintenance windows are published to the ArcGIS Online Status dashboard where any customer can subscribe to for updates at https://status.arcgis.com.	ArcGIS Online インフラストラクチャへのすべての変更は、文書化された変更管理プロセスおよび手順を介して追跡および記録され、定期的なメンテナンス ウィンドウは ArcGIS Online ステータス ダッシュボードに公開され、お客様は誰でも https://status.arcgis.com でアップデートを購読することができます。	Change Management Baseline	
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	All changes to the ArcGIS Online infrastructure are tracked and recorded through the Change Management documented processes and Procedures, scheduled maintenance windows are published to the ArcGIS Online Status dashboard where any customer can subscribe to for updates at https://status.arcgis.com.	ArcGIS Online インフラストラクチャへのすべての変更は、文書化された変更管理プロセスおよび手順を介して追跡および記録され、定期的なメンテナンス ウィンドウは ArcGIS Online ステータス ダッシュボードに公開され、お客様は誰でも https://status.arcgis.com でアップデートを購読することができます。	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	This is part of the Configuration Management plan	これは構成管理計画の一部です。	Exception Management	
CCC-08.2	Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	This is part of the Configuration Management plan and in alignment with FedRAMP requirements	これは構成管理計画の一部であり、FedRAMP 要件に沿ったものです。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	The CM process includes reverting baselines to known stable state if there is a deployment issue.	CM プロセスには、デプロイに問題がある場合、ベースラインを既知の安定状態に戻すことも含まれます。	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	ArcGIS Online の鍵管理ポリシー、手順、プロセスは、FedRAMP 要件に準拠しています。	Encryption and Key Management Policy and Procedures	Cryptography, Encryption & Key Management
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Key management policies and procedures are reviewed and updated annually.	鍵管理ポリシーと手順は、毎年見直され、更新されます。		
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	CSP-owned	ArcGIS Online operational keys are managed by the ArcGIS Online Operations Leads. Critical keys are rotated periodically	ArcGIS Online の運用キーは、ArcGIS Online 運用責任者が管理します。重要なキーは定期的にローテーションされます。	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	ArcGIS Online utilizes encryption in transit and at-rest by default. The customer's administrator can currently disable requiring encryption-in-transit via HTTPS (TLS) for customer data transmitted to and from their ArcGIS Online organization.	ArcGIS Online では、デフォルトでは、通信および停止時の暗号化が使用されます。現在、お客様の管理者は、ArcGIS Online 組織との間で送受信されるお客様のデータに対して、HTTPS (TLS) を介した通信内の暗号化を要求することを無効にすることができます。	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	ArcGIS Online provides encryption at REST with AES-256, and encryption in transit with HTTPS via TLS 1.2.	ArcGIS Online では、REST で AES-256 による暗号化、および TLS 1.2 を介した HTTPS による通信での暗号化を提供しています。	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	CSP-owned	See CEK-01.1	CEK-01.1 をご参照ください。	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements. Endpoints are validated against SSL Labs and evolving standards regularly reviewed.	ArcGIS Online の鍵管理ポリシー、手順、プロセスは、FedRAMP 要件に準拠しています。エンドポイントは SSL ラボで検証され、進化する標準は定期的に見直されます。	Encryption Change Cost Benefit Analysis	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	ArcGIS Online has established an information security management program with designated roles and responsibilities that are appropriately aligned within the organization. Esri management reviews and evaluates the risks identified in the risk management program at least annually. Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	ArcGIS Online は、組織内で適切に連携された指定された役割と責任を持つ情報セキュリティ管理プログラムを確立しています。Esri 社の経営陣は、リスク管理プログラムで特定されたリスクを少なくとも年 1 回見直し、評価します。ArcGIS Online の鍵管理ポリシー、手順、プロセスは、FedRAMP 要件に準拠しています。	Encryption Risk Management	Cryptography, Encryption & Key Management
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	Shared CSP and CSC	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team but stored in Cloud Service Provider Key Management Service which is FIPS 140-2 compliant and also in alignment with FedRAMP requirements. Customers can implement a CASB to encrypt any fields they wan to manage the encryption keys for.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。お客様は、暗号化キーを管理するフィールドを暗号化するために CASB を実装できます。	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	This documentation is assessed annually as part of the ArcGIS Online FedRAMP authorization	この文書は、ArcGIS Online FedRAMP 認証の一環として毎年評価されます。	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS are reviewed annually.	ArcGIS の鍵管理ポリシー、手順、プロセスは毎年見直されます。		
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	CSP-owned	Critical keys are rotated periodically	重要なキーは定期的にローテーションされます。	Key Rotation	
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	CSP-owned	Critical keys are rotated in alignment with FedRAMP Moderate requirements. Cryptographic keys are invalidated when compromised or at the end of their defined lifecycle period.	重要なキーは、FedRAMP Moderate 要件に沿ってローテーションされます。暗号鍵が漏洩した場合、または定められたライフサイクル期間が終了した場合は無効化されます。	Key Revocation	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。	Key Destruction	Cryptography, Encryption & Key Management
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	No	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	キーは KMS および Azure valut で管理されます。自動ローテーションが実施されています。	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	キーは KMS および Azure valut で管理されます。自動ローテーションが実施されています。	Key Suspension	
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	キーは KMS および Azure valut で管理されます。自動ローテーションが実施されています。	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Keys are managed through KMS and Azure vault. Automatic rotation is in place	キーは KMS および Azure valut で管理されます。自動ローテーションが実施されています。	Key Archival	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements. Customer datasets are always encrypted at rest and in-transit.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。お客様のデータセットは保管時および転送時に常に暗号化されています。	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。	Key Recovery	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and 3rd-party	ArcGIS Online encryption keys are maintained by the ArcGIS Online operations team and stored in Cloud Service Provider Key Management Services which are NIST approved and FIPS 140-2 compliant which is in alignment with FedRAMP requirements.	ArcGIS Online の暗号化キーは、ArcGIS Online の運用チームによって管理され、クラウド サービス プロバイダーの鍵管理サービスに保管されます。サービスは、NIST の承認を受け、FedRAMP 要件に沿った FIPS 140-2 に準拠しています。	Key Inventory Management	
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	Sanitization is in alignment with NIST standards	サニタイズは NIST の標準に準拠します。	Off-Site Equipment Disposal Policy and Procedures	Datacenter Security
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	Shared CSP and 3rd-party	When a storage device has reached the end of its useful life, AWS and MS Azure procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Both providers use the techniques detailed in NIST 800- 88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.	ストレージ・デバイスが耐用年数に達した場合の AWS と MS Azure の手順には、お客様のデータが権限のない個人に漏洩しないように設計された廃棄プロセスが含まれています。両プロバイダーは、廃棄プロセスの一環として、NIST 800- 88 (「メディアのサニタイゼーションのためのガイドライン」) に詳述されている技術を使用しています。		
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	Shared CSP and 3rd-party	AWS and Azure Policies are reviewed approved by the cloud service provider's leadership at least annually or as needed basis.	AWS と Azure のポリシーは、少なくとも年 1 回または必要に応じて、クラウド サービス プロバイダーのリーダーシップによって承認されます。		
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	NA	CSP-owned	Hardware is transparent to customer of SaaS offering. No customer equipment resides in the SaaS offering	ハードウェアは、SaaS 提供のお客様は意識する必要がありません。SaaS 提供にはお客様の機器は含まれません。	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	NA	CSP-owned	Not applicable for a SaaS offering	SaaS 提供には該当しません。		
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	NA	CSP-owned	Not applicable for a SaaS offering	SaaS 提供には該当しません。		
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	CSP-owned	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.	クラウド インフラストラクチャ プロバイダーのポリシーは、オフィス、部屋、施設、機密情報が保管されている安全なエリアでの、安全でセキュアな作業環境の維持のために方針を定義し、制御を確立します。	Secure Area Policy and Procedures	
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	CSP-owned	Cloud infrastructure provider policies define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	クラウド インフラストラクチャ プロバイダーのポリシーは、オフィス、部屋、施設、および機密情報が保管されている安全なエリアでの、安全でセキュアな作業環境の維持のために方針を定義し、制御を確立します。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	N/A	CSP-owned	Not Applicable for SaaS offering	SaaS オファリングには適用されません。	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	N/A	CSP-owned	Not Applicable for SaaS offering	SaaS オファリングには適用されません。	Secure Media Transportation Policy and Procedures	
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	Shared CSP and 3rd-party	ArcGIS Online is operated with FedRAMP Moderate controls based on customer organizational business risk requirements requested of Esri. MS Azure and AWS provide the physical assets for ArcGIS Online and obtain at least the same level of assuarance or higher for thier operations.	ArcGIS Online は、お客様組織のビジネス リスク要件の Esri への要望に基づき、FedRAMP Moderate の管理下で運用されます。 MS Azure と AWS は、ArcGIS Online の物理的アセットを提供し、少なくとも同レベルかそれ以上の運用保証を得ています。	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	CSP-owned	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、機器とネットワーク コンポーネントの最新の文書化された、また監査された最新の一覧表を責任を持って保守しています。クラウド インフラストラクチャ プロバイダーは、定義されたポリシーと比較することで、デバイス構成の不一致を検出する自動化されたメカニズムを管理しています。クラウド インフラストラクチャ プロバイダーは、ISO 27001 標準に沿って機器の識別を管理しています。	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	CSP-owned	Cloud infrastructure provider policies define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	クラウド インフラストラクチャ プロバイダーのポリシーは、オフィス、部屋、施設、および機密情報が保管されている安全なエリアでの、安全でセキュアな作業環境の維持のために方針を定義し、制御を確立します。	Controlled Access Points	Datacenter Security
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	CSP-owned	Cloud infrastructure provider policies define and establish controls for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	クラウド インフラストラクチャ プロバイダーのポリシーは、オフィス、部屋、施設、および機密情報が保管されている安全なエリアでの、安全でセキュアな作業環境の維持のために方針を定義し、制御を確立します。		
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	CSP-owned	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、機器とネットワーク コンポーネントの最新の文書化された、また監査された最新の一覧表を責任を持って保守しています。クラウド インフラストラクチャ プロバイダーは、定義されたポリシーと比較することで、デバイス構成の不一致を検出する自動化されたメカニズムを管理しています。クラウド インフラストラクチャ プロバイダーは、ISO 27001 規格に沿って機器の識別を管理しています。	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	CSP-owned	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. No subcontractor access beyond cloud providers	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、ビデオ監視、侵入検知システム、その他の電子的な手段を利用した専門のセキュリティ スタッフによって、敷地と建物への出入口の両方で厳格に管理されています。権限を与えら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 2 要素認証を通過する必要があります。また、クラウド プロバイダー以外の下請け業者のアクセスは禁止されています。	Secure Area Authorization	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	CSP-owned	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. No subcontractor access beyond cloud providers	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、ビデオ監視、侵入検知システム、その他の電子的な手段を利用した専門のセキュリティ スタッフによって、敷地と建物への出入口の両方で厳格に管理されています。権限を与えら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 2 要素認証を通過する必要があります。また、クラウド プロバイダー以外の下請け業者のアクセスは禁止されています。	Secure Area Authorization	Datacenter Security
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	Shared CSP and 3rd-party	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 のクラウド 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管理に関する高い業界標準に準拠した、データ センターの物理的なセキュリティ対策を講じています。詳細については、以下のコンプライアンス サイトをそれぞれご参照ください。 Microsoft Azure: https://www.microsoft.com/enus/trustcenter/Compliance Amazon Web Services: https://aws.amazon.com/compliance	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	Shared CSP and 3rd-party	See MS Azure and Amazon Web Services security documentation for details	詳細については、MS Azure と Amazon Web Services のセキュリティ ドキュメントをご参照ください。	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	CSP-owned	ArcGIS Online Business Impact Assessment and updated annually in alignment with FedRAMP standards.. 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.	ArcGIS Online のビジネス影響評価は、FedRAMP 標準に沿って毎年更新しています。クラウド インフラストラクチャ プロバイダーのデータ センターには、24 時間 365 日の無停電電源装置 (UPS) と非常用電源のサポートがあり、発電機を含む場合もあります。UPS と発電機の両方について、定期的なメンテナンスとテストを実施しています。データ センターでは、緊急時の燃料配送の手配を行っています。	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	CSP-owned	ArcGIS Online is FedRAMP authorized and therefore also aligns with NIST standards.	ArcGIS Online は FedRAMP の認定を受けているため、NIST 標準にも準拠しています。	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	CSP-owned	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.	クラウド インフラストラクチャ プロバイダーのポリシーは、オフィス、部屋、施設、機密情報が保管されている安全なエリアでの、安全でセキュアな作業環境の維持のために方針を定義し、制御を確立します。	Secure Utilities	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	Shared CSP and 3rd-party	ArcGIS Online uses geographically redundant datacenter locations across MS Azure and AWS cloud service providers. The AWS Security Operations Center performs quarterly threat and vulnerability reviews of datacenters and colocation sites. These AWS reviews are in addition to an initial environmental and geographic assessment of a site performed prior to building or leasing. The AWS quarterly reviews are validated by third parties during their SOC, PCI, and ISO assessments. Microsoft data center site selection is performed using a number of criteria, including mitigation of environmental risks. For Azure, in areas where the exists a higher probability of earthquakes, seismic bracing of the facility is employed. Data centers are built as redundant, highly-available components of the Azure platform.	ArcGIS Online は、MS Azure および AWS のクラウド サービス プロバイダー間で地理的に冗長化されたデータ センターを使用しています。AWS セキュリティ オペレーション センターは、四半期ごとにデータ センターとコロケーション サイトの脅威と脆弱性のレビューを実施しています。これらの AWS レビューは、建設または賃貸の前に行われる用地の初期の環境および地理的評価に追加されます。AWS の四半期レビューは、SOC、PCI、ISO の評価において第三者によって検証されます。Microsoft のデータ センター用地の選定は、環境リスクの軽減を含む多くの基準を用いて行われます。Azure では、地震の発生確率が高い地域の場合、施設の耐震補強が採用されます。データ センターは、Azure プラットフォームの冗長で可用性の高いコンポーネントとして構築されています。	Equipment Location	Datacenter Security
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Details to data handling and protection policies and procedures can be found on our Trust Center: https://trust.arcgis.com/en/	データの処理および保護方針と手順の詳細については、Trust Center をご参照ください: https://trust.arcgis.com/en/	Security and Privacy Policy and Procedures	Data Security and Privacy Lifecycle Management
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Data and privacy policies and procedures reviewed annually.	データとプライバシーに関するポリシーと手順は、毎年見直されます。		
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	CSP-owned	Sanitization procedures are in alignment with NIST standards.	サニタイズ手順は NIST 標準に準拠しています。	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	CSP-owned	Customers determine and manage the types of sensitive and personal data they process based on how they use ArcGIS Online. Because the customer would be the data controller, they are required to create and maintain inventories of the sensitive and personal data they process using ArcGIS Online (this is required by contract).	お客様は ArcGIS Online の使用方法に基づいて、処理する機密データと個人データの種類を決定し、管理します。お客様はデータ管理者であるため、ArcGIS Online を使用して処理する機密データおよび個人データのインベントリを作成および維持する必要があります（これは契約により義務付けられています）。	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	Data Classification is a customer responsibility. However, ArcGIS Online has a FedRAMP ATO. This can be used by the customers as a baseline for classifying what type of data they should be hosting in the solution.	データの分類はお客様の責任です。ただし、ArcGIS Online は FedRAMP ATO を取得しています。これは、お客様がソリューションでホスティングすべきデータの種類を分類するための基準として使用することができます。	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Generalized ArcGIS Online data flow documentation for customers is located in the ArcGIS Trust Center documents found here: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf . More detailed operational data flow diagrams are included in the ArcGIS Online System Security Plan and updated at least annually.	お客様向けの一般的な ArcGIS Online データ フロー ドキュメントは、ArcGIS Trust Center のドキュメントにあります: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf より詳細な運用データフロー図は、ArcGIS Online のシステム セキュリティ計画に含まれ、少なくとも年 1 回更新されます。	Data Flow	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Generalized ArcGIS Online data flow documentation for customers is located in the ArcGIS Trust Center documents found here: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf . More detailed operational data flow diagrams are included in the ArcGIS Online System Security Plan and updated at least annually.	お客様向けの一般的な ArcGIS Online データ フロー ドキュメントは、ArcGIS Trust Center のドキュメントにあります: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf より詳細な運用データフロー図は、ArcGIS Online のシステム セキュリティ計画に含まれ、少なくとも年 1 回更新されます。	Documentation	Data Security and Privacy Lifecycle Management
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	CSP-owned	Customers retain full ownership of their data at all times.	お客様は、常にデータの完全な所有権を保持します。	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	No	CSC-owned	Customers retain full ownership of their data at all times.	お客様は、常にデータの完全な所有権を保持します。		
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	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 FedRAMP requirements (that have NIST 800-53 security controls as its 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 の管理に対応する NIST 800-53 セキュリティ管理に基づいています。ArcGIS Online のデータ セキュリティ対策は、FedRAMP 要件 (NIST 800-53 セキュリティ管理を中核とする) に沿っています。ArcGIS Online の手順には、リリース管理プロセスの間に、更新が不正な変更を受けていないかどうかを確認することを要求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 などの業界標準に準拠しています。	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Esri's aligns its privacy practices with industry-recognized privacy principles to implement appropriate administrative, technical and physical controls. Esri aligns privacy engineering decisions with the organization's overall privacy strategy and industry-recognized leading practices of privacy by design and by default.	Esri は、業界で認知されたプライバシー原則に基づき、適切な管理、技術、物理的管理を実施しています。 Esri のプライバシー エンジニアリングに関する決定は、組織の全体的なプライバシー戦略と、業界で認知されているプライバシー バイ デザインやプライバシー バイ デフォルトの主要な実践に沿っています。	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	CSP-owned	Esri's security and privacy policies and procedures are in alignment with FedRAMP authorization, GDPR as well as CCPA regulations. Appropriate flow downs are provided to external providers.	Esri のセキュリティおよびプライバシー ポリシーと手順は、FedRAMP 認定、GDPR および CCPA 規定に準拠しています。適切なフロー ダウンが外部プロバイダーに提供されています。		
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	N/A	CSC-owned	The customer is responsible for conducting a DPIA as GDPR requires controllers to carry out a DPIA where a processing activity is using new technologies and is likely to result in a "high risk to the rights and freedoms" of individuals (Article 35.1 GDPR). Esri is a processor under the articles of GDPR. Customers are expected to analyze the data set that they upload. Esri minimizes data collected by our product.	GDPR では、処理活動が新技術を使用しており、個人の「権利と自由に対する高いリスク」をもたらす可能性が高い場合に DPIA を実施するよう管理者に要求しているため、お客様は DPIA を実施する責任を負います (GDPR 第 35.1 条)。Esri は GDPR の条項に基づき処理します。お客様はアップロードしたデータセットを分析することが求められます。Esri は、弊社製品によって収集されるデータを最小限に抑えています。	Data Protection Impact Assessment	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data- processing-addendums/data-process-addend.pdf	プロセス、手順、技術的な対策は、ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Sensitive Data Transfer	Data Security and Privacy Lifecycle Management
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	CSP-owned	Upon request Esri will provide you with information about whether we hold any of your personal information. Esri will permit you to access, correct, or delete your information in our database by contacting Esri or by logging in to your account and making the appropriate changes. We will respond to all requests for access within a reasonable timeframe.	ご要望に応じて、Esri はお客様の個人情報を保有しているかどうかの情報を提供します。Esri は、Esri に連絡するか、アカウントにログインして適切な変更を行うことで、データベース内の情報にアクセス、修正、削除することを許可します。当社は、合理的な期間内にすべてのアクセス要求に対応します。	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data- processing-addendums/data-process-addend.pdf	プロセス、手順、技術的な対策は、ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data- processing-addendums/data-process-addend.pdf	プロセス、手順、技術的な対策は、ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data- processing-addendums/data-process-addend.pdf	プロセス、手順、技術的な対策は、ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Disclosure of Data Sub- processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSP-owned	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. We recommend customers utilize a separate staging organization from the production one for testing purposes. 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 as needed to provide the services, or as required by law or regulation or by order of a court or other government body in alignment with our privacy supplement statement.	ArcGIS Online のお客様は、自己のデータの所有権を保持します。ArcGIS Online では、本番環境と非本番環境の組織環境を維持および開発する機能をお客様に提供しています。本番環境のデータが非本番環境に複製されないようにするのはお客様の責任です。テストを目的として、本番環境とは別のステージング組織を利用することを推奨します。本番環境から非本番環境への Esri によるお客様データの移動またはコピーは、サービスのトラブルシューティングのためにお客様の同意を得た場合、または Esri の法務部門の指示による場合を除き、禁止されています。	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	CSP-owned	Esri has a set ArcGIS Online Data Retention and Disposal Policy that outline Esri's approach to managing the retention and secure disposal of information in line with our business requirements and legal obligations.	Esri は、業務要件および法的義務に沿った情報の保持および安全な廃棄を管理するための Esri のアプローチを概説する、一連の ArcGIS Online データ保持および廃棄ポリシーを定めています。	Data Retention and Deletion	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Processes, procedures, and technical measures can be found in our Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data- processing-addendums/data-process-addend.pdf	プロセス、手順、技術的な対策は、ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Sensitive Data Protection	Data Security and Privacy Lifecycle Management
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	Esri will promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to reserve the confidentiality of a law enforcement investigation. Further details can be found in Esri's Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Esri は、法執行当局による個人データの開示の法的拘束力のある要求があった場合、法執行当局の捜査の秘密を保持するための刑法上の禁止事項など、別段の禁止事項がない限り、データ エクスポーターに 速やかに通知します。詳細は ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Esri will promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to reserve the confidentiality of a law enforcement investigation. Further details can be found in Esri's Data Processing Addendum: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf	Esri は、法執行当局による個人データの開示の法的拘束力のある要求があった場合、法執行当局の捜査の秘密を保持するための刑法上の禁止事項など、別段の禁止事項がない限り、データ エクスポーターに 速やかに通知します。詳細は ArcGIS Online のデータ処理に関する追加契約に記載されています: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf		
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	CSP-owned	By default, all ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Services US Regions (East, West), and Microsoft Azure US Regions (South Central, East, West). When purchasing a new organization, customers can specify a different region for their data storage. The two alternative regional data hosting locations are the European Union (EU1) and Asia Pacific (AP1) regional offerings. EU1 customer data is stored in Amazon Web Services region EU-West-1 (Ireland) with failover to EU-Central-1 (Germany), and Microsoft Azure region North Europe (Ireland) with failover to West Europe (Netherlands). AP1 customer data is stored in Amazon Web Services region AP-SouthEast-2 (Sydney) with failover to AP-SouthEast-1 (Singapore), and Microsoft Azure region Australia East with failover to Australia SouthEast. Customers are responsible for the backup of their datasets.	デフォルトでは、すべての ArcGIS Online のお客様データは、Amazon Web Service US リージョン (East、West) および Microsoft Azure US リージョン (South Central、East、West) の範囲内の米国内に存在します。新しい組織を購入する際、お客様はデータ ストレージに別のリージョンを指定することができます。2 つの代替リージョナル データ ホスティング ロケーション、欧州連合 (EU1) およびアジア太平洋 (AP1) を指定することができます。EU1 のお客様データは、Amazon Web Services のリージョン EU-West-1 (アイルランド) と EU-Central-1 (ドイツ) へのフェイルオーバー、および Microsoft Azure のリージョン North Europe (アイルランド) と West Europe (オランダ) へのフェイルオーバーに保存します。AP1 のお客様データは、Amazon Web Services のリージョン AP-SouthEast-2 (シドニー) と AP-SouthEast-1 (シンガポール) へのフェイルオーバー、および Microsoft Azure のリージョン Australia East と Australia SouthEast へのフェイルオーバーに保存します。データセットのバックアップは、お客様の責任です。	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Esri's security policies are signed and reviewed by executive management and disseminated to team members in alignment with the FedRAMP accreditation.	Esri のセキュリティ ポリシーは、FedRAMP 認証に沿って、経営陣の署名とレビューが行われ、チーム メンバーに配布されています。	Governance Program Policy and Procedures	Governance, Risk and Compliance
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Esri's security polices and procedures are reviewed and updated annually	Esri のセキュリティ ポリシーと手順は毎年見直され、更新されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	This is part of our FedRAMP program based off NIST 800-53 controls and is audited annually. Esri's security policies and procedures are in alignment with FedRAMP authorization, GDPR as well as CCPA regulations.	これは、NIST 800-53 管理に基づく FedRAMP プログラムの一部であり、毎年監査を受けています。Esri のセキュリティ ポリシーと手順は、FedRAMP 認定、GDPR および CCPA 規定に準拠しています。	Risk Management Program	Governance, Risk and Compliance
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	As part of the overall FedRAMP accreditation, baseline security requirements are constantly being reviewed, improved and implemented as part of a Continuous Monitoring Program.	FedRAMP 全体の認定の一環で、ベースラインのセキュリ ティ要件が常に見直され、改善され、継続的監視プログラムの一環として実施されています。	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	This is part of the Configuration Management plan and followed whenever a deviation from policy occurs.	これは構成管理計画の一部であり、ポリシーからの逸脱が発生するたびに従います。	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	ArcGIS Online is FedRAMP authorized and the program is based off NIST 800-53 controls	ArcGIS Online は FedRAMP 認定であり、プログラムは NIST 800-53 管理に基づいています。	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	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 システム セキュリティ計画内に文書化されています。ユーザーの役割と責任は、ArcGIS Online アプリケーション ドキュメントに記載されています。	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	This documentation is assessed annually as part of the ArcGIS Online FedRAMP authorization	この文書は、ArcGIS Online FedRAMP 認証の一環として毎年評価されます。	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	CSP-owned	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、および業界フォーラムなどの外部関係者との連絡を維持し、必要に応じて適切な措置を迅速に講じ、助言を得ることができるようにしています。	Special Interest Groups	
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	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.	ArcGIS Online およびクラウド インフラストラクチャ プロバイダーのすべての従業員は、採用プロセスの一環として、標準的な身元調査を完了する必要があります。身元調査には、候補者の学歴、職歴、および犯罪歴に関する情報の確認が含まれますが、これに限定されません。	Background Screening Policy and Procedures	Human Resources

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	CSP-owned	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.	ArcGIS Online およびクラウド インフラストラクチャ プロバイダーのすべての従業員は、採用プロセスの一環として、標準的な身元調査を完了する必要があります。身元調査には、候補者の学歴、職歴、および犯罪歴に関する情報の確認が含まれますが、これに限定されません。	Background Screening Policy and Procedures	Human Resources
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Esri corporate policies and procedures are reviewed and updated at least annually.	Esri のコーポレート ポリシーおよび手順は、少なくとも年 1 回見直され、更新されます。		
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。		
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online	ArcGIS Online の従業員は、ユーザーの責任を概説する行動規則ポリシーを遵守します。これには、ArcGIS Online の管理に使用するリソースの保護に関するガイダンスが含まれます。	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online employees adhere to a rules of behavior policy outlining user responsibilities and review their responsibilities annually.	ArcGIS Online の従業員は、ユーザーの責任を概説する行動規則ポリシーを遵守し、毎年その責任を見直します。		
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	N/A	CSP-owned	Esri does not store or process information within remote sites and locations.	Esri は、リモート サイトおよびリモート ロケーション内で情報を保存または処理しません。	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	N/A	CSP-owned	Esri does not store or process information within remote sites and locations.	Esri は、リモート サイトおよびリモート ロケーション内で情報を保存または処理しません。		
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Esri Human Resources Policy drives employee termination processes for ArcGIS Online. These policies are available to all Esri employees	Esri 人事ポリシーは、ArcGIS Online の従業員の解雇プロセスを推進します。これらのポリシーは、Esri の全従業員が利用可能です。	Asset returns	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Esri Human Resources Policy drives employee termination processes for ArcGIS Online. These policies are available to all Esri employees	Esri 人事ポリシーは、ArcGIS Online の従業員の解雇プロセスを推進します。これらのポリシーは、Esri の全従業員が利用可能です。	Employment Termination	Human Resources
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	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 ニーズを反映するために Esri NDA を管理し、定期的に改訂します。	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	ArcGIS Online employees complete security training at least annually	ArcGIS Online の従業員は、少なくとも年 1 回、セキュリティ トレーニングを受講します	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Annual role based & security awareness training is provided for ArcGIS Online employees.	ArcGIS Online の従業員を対象に、年 1 回、役割に応じたセキュリティ意識向上トレーニングを実施しています。		
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Annual role based & security awareness training is provided for ArcGIS Online employees.	ArcGIS Online の従業員を対象に、年 1 回、役割に応じたセキュリティ意識向上トレーニングを実施しています。	Personal and Sensitive Data Awareness and Training	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Personal and Sensitive Data Awareness and Training	Human Resources
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	ArcGIS Online has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) with supporting security training materials. Esri employees accessing ArcGIS Online must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	ArcGIS Online には、システム セキュリティ計画 (System Security Plan: SSP) の一部として詳細な役割と責任のマトリックスがあり、それをサポートするセキュリ ティ トレーニング資料も用意されています。ArcGIS Online にアクセスする Esri の従業員は、アクセスおよび使用に関する従業員の技術的責任および組織的責任を概説した行動規則 (Rules of Behavior: RoB) に署名する必要があります。	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	Identity and access management policies and procedures are part of ArcGIS Online FedRAMP authorization.	ID およびアクセス管理のポリシーおよび手順は、ArcGIS Online FedRAMP 認定の一部です。	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Identity and access management policies and procedures are part of ArcGIS Online FedRAMP authorization and are reviewed and updated at least annually or if a significant change occurs.	ID およびアクセス管理のポリシーおよび手順は、ArcGIS Online FedRAMP 認定の一環として、少なくとも年 1 回または重要な変更が発生した場合に見直され、更新されます。		
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	CSP-owned	This is a Customer Responsibility to enforce the minimum password requirements that meet their agency's security policies. Organizations should utilize ArcGIS Online Organization Specific Logins to meet all of their organizations username and password management requirements and for adherence to FedRAMP accreditation. Further information concerning ArcGIS Online Organization Specific Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.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/arcgis-online/administer/configure-security.htm	各組織のセキュリティ ポリシーに合致する最小限のパスワード要件を適用するのはお客様の責任です。組織は、ArcGIS Online 組織固有のログインを利用して、組織のユーザー名およびパスワード管理のすべての要件を満たし、FedRAMP 認定を遵守する必要があります。ArcGIS Online 組織固有のログインに関する詳細情報は、以下をご参照ください: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm ID プロバイダー (IdP) が利用できない場合、ArcGIS Online では管理者が ArcGIS Online 組織のカスタム パスワード ポリシーを設定できます。固定設定であるユーザー ID のロックアウトを除き、パスワード ポリシーは、これらの要件またはお客様のポリシーに沿った特定の要件に合わせてカスタマイズできます。カスタム パスワード ポリシーの設定の詳細については、以下をご参照ください: https://doc.arcgis.com/en/arcgis- online/administer/configure-security.htm	Strong Password Policy and Procedures	Identity & Access Management
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	This is a Customer Responsibility to enforce the minimum password requirements that meet their agency's security policies. ArcGIS requires passwords be changed at least annually.	各組織のセキュリティ ポリシーに合致する最小限のパスワード要件を適用するのはお客様の責任です。ArcGIS では、パスワードは少なくとも年 1 回変更する必要があります。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	CSP-owned	User access is reviewed quarterly	ユーザーのアクセスは四半期ごとに見直されます。	Identity Inventory	Identity & Access Management
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	CSP-owned	ArcGIS Online roles with corresponding information system access authorizations are defined within the ArcGIS Online Separation of Duties Matrix which as assessed annually as part of it's FedRAMP authorization	ArcGIS Online のロールは、対応する情報システムへのアクセス権限とともに、FedRAMP 認定の一環として毎年評価される職務分掌マトリックス内で定義されています。	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	CSP-owned	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/arcgis-online/reference/roles.htm	クラウド インフラストラクチャ プロバイダーは、重要な機能の職務分掌を実施しており、本番システムへの意図しない不正アクセスや変更のリスクを最小限に抑えています。 お客様は、ArcGIS Online 組織リソースの職務分掌を管理する機能を保持します。ArcGIS Online 内でカスタム ロールを使用して、特定のユーザー グループのアクセス許可を、管理者、公開者、ユーザーのデフォルト ロールよりもさらに細かく適用できます。詳細については、以下をご参照ください: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	CSP-owned	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel must complete the read-in process to the FedRAMP program before they are granted access to any ArcGIS Online resources. No access to customer data is granted.	ArcGIS Online 組織にアクセスを許可する責任はお客様が持ちます。すべての ArcGIS Online 管理担当者は、ArcGIS Online リソースへのアクセスが許可される前に、FedRAMP プログラムへのリードイン プロセスを完了する必要があります。お客様データへのアクセスは許可されません。	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	CSP-owned	ArcGIS Online relies on the Role Based Access Control (RBAC) model. All users in solution need to have a role for which they are granted access to. The customer manages access provisioning and deprovisioning	ArcGIS Online は、ロール ベース アクセス制御 (RBAC) モデルに依存します。ソリューション内のすべてのユーザーは、アクセス許可されたロールを持つ必要があります。お客様は、アクセスのプロビジョニングとデプロビジョニングを管理します。	User Access Changes and Revocation	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org	お客様が ArcGIS Online 組織へのアクセスを管理します。	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org	お客様が ArcGIS Online 組織へのアクセスを管理します。	Segregation of Privileged Access Roles	
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	CSP-owned	ArcGIS Online operations team maintains records of access control grants to all personnel. Periodic access control audits are conducted as per the FedRAMP requirements. Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel must complete the read-in process to the FedRAMP program before they are granted access to any ArcGIS Online resources. No access to customer data is granted.	ArcGIS Online の運用チームは、すべての担当者に対しアクセス制御の記録を管理します。FedRAMP 要件に沿って、アクセス制御に関する定期的な監査が実施されます。ArcGIS Online 組織へのアクセスを許可する責任はお客様が持ちます。すべての ArcGIS Online 管理担当者は、ArcGIS Online リソースへのアクセスが許可される前に、FedRAMP プログラムへのリードイン プロセスを完了する必要があります。お客様データへのアクセスは許可されません。	Management of Privileged Access Roles	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	N/A	CSP-owned	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/arcgis-online/reference/roles.htm	クラウド インフラストラクチャ プロバイダーは、重要な機能の職務分掌を実施しており、本番システムへの意図しない不正アクセスや変更のリスクを最小限に抑えています。 お客様は、ArcGIS Online 組織リソースの職務分掌を管理する機能を保持します。ArcGIS Online 内でカスタム ロールを使用して、特定のユーザー グループのアクセス許可を、管理者、公開者、ユーザーのデフォルト ロールよりもさらに細かく適用できます。詳細については、以下をご参照ください: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm	Management of Privileged Access Roles	Identity & Access Management
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	CSP-owned	Customers manage access to their ArcGIS Online org entirely.	お客様が ArcGIS Online 組織へのアクセスを完全に管理します。	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	ArcGIS Online Infrastructure read-only logs are maintained by the Software Security and Privacy team.	ArcGIS Online インフラストラクチャの読み取り専用ログは、Software Security and Privacy チームによって保守されます。	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	ArcGIS Online Infrastructure read-only logs are maintained by the Software Security and Privacy team.	ArcGIS Online インフラストラクチャの読み取り専用ログは、Software Security and Privacy チームによって保守されます。		
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel are required to have a unique user ID and password to access the system as shared accounts are not leveraged. In order to use administration credentials multifactor authentication is utilized to uniquely identify credentials.	ArcGIS Online 組織へのアクセスを許可する責任はお客様が持ちます。共有アカウントの利用は不可であることから、ArcGIS Online の管理担当者はすべて、システムにアクセスするための固有のユーザー ID とパスワードを持つ必要があります。管理者認証を使用するために、認証を一意に識別する多要素認証が利用されます。	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	CSP-owned	ArcGIS Online has the option to enable Multifactor Authentication(MFA). For details please review the resource below: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	ArcGIS Online では、多要素認証 (MFA) を有効にするオプションがあります。詳細については、以下のリソースをご参照ください: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	ArcGIS Online has the option to enable Multifactor Authentication(MFA). For details please review the resource below: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm	ArcGIS Online では、多要素認証 (MFA) を有効にするオプションがあります。詳細については、以下のリソースをご参照ください: https://doc.arcgis.com/en/arcgis-online/administer/configure-security.htm		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Organizations should utilize ArcGIS Online Organization Specific Logins to meet all of their organizations username and password management requirements and for adherence to FedRAMP accreditation. Further information concerning ArcGIS Online Organization Specific Logins may be found at: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.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/arcgis-online/administer/configure-security.htm	組織は、ArcGIS Online 組織固有のログインを利用して、組織のユーザー名およびパスワード管理のすべての要件を満たし、FedRAMP 認定を遵守する必要があります。ArcGIS Online 組織固有のログインに関する詳細情報は、以下ををご参照ください: http://doc.arcgis.com/en/arcgis-online/administer/enterprise-logins.htm ID プロバイダー (IdP) が利用できない場合、ArcGIS Online では管理者が ArcGIS Online 組織のカスタム パスワード ポリシーを設定できます。固定設定であるユーザー ID のロックアウトを除き、パスワード ポリシーは、これらの要件またはお客様のポリシーに沿った特定の要件に合わせてカスタマイズできます。カスタム パスワード ポリシーの設定の詳細については、以下をご参照ください: https://doc.arcgis.com/en/arcgis- online/administer/configure-security.htm	Passwords Management	Identity & Access Management
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	CSP-owned	Customers have the responsibility to grant access to their ArcGIS Online organization. All ArcGIS Online administration personnel must complete the read-in process to the FedRAMP program before they are granted access to any ArcGIS Online resources. No access to customer data is granted.	ArcGIS Online 組織にアクセスを許可する責任はお客様が持ちます。すべての ArcGIS Online 管理担当者は、ArcGIS Online リソースへのアクセスが許可される前に、FedRAMP プログラムへのリードイン プロセスを完了する必要があります。お客様データへのアクセスは許可されません。	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	CSP-owned	The ArcGIS Online REST API is publicly available and documented on the website at: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm . Significant changes are assessed as part of a Significant Impact Assessment process to ensure appropriate evaluation, approvals and communication.	ArcGIS Online REST API はパブリックに公開されており、Web サイトで文書化されています: https://doc.arcgis.com/en/arcgis-online/reference/develop-with-agol.htm 重要な変更は、適切な評価、承認、コミュニケーションを確実に実施し、Significant Impact Assessment プロセスの一環として評価されます。	Interoperability	Interoperabili ty & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	CSP-owned	See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis- online/manage-data/data-in-online.htm	ArcGIS のサービスの情報処理相互運用性に関する詳細については、ArcGIS Trust Center および ArcGIS Online のドキュメントをご参照ください - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm		
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	ArcGIS Online development code is designed to be portable in other CSP environments.	ArcGIS Online の開発コードは、他の CSP (Cloud Service Providers) 環境でも使用できるように設計されています。	and Portability Policy and Procedures	
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	CSP-owned	See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis- online/manage-data/data-in-online.htm	ArcGIS のサービスの情報処理相互運用性に関する詳細については、ArcGIS Trust Center および ArcGIS Online のドキュメントをご参照ください - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm		
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and procedures are reviewed and updated annually or if there are any significant changes.	方針と手続きは毎年または重要な変更がある場合に見直され、更新されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	CSC-owned	ArcGIS Online has extensive API capabilities allowing customers to programmatically retrieve their data. See the ArcGIS Trust Center and ArcGIS Online documentation for details concerning information processing interoperability of our services - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm	ArcGIS Online には拡張性のある API 機能があり、お客様はプログラムによってデータを取得することができます。ArcGIS のサービスの情報処理相互運用性に関する詳細については、ArcGIS Trust Center および ArcGIS Online のドキュメントをご参照ください - https://doc.arcgis.com/en/arcgis-online/manage-data/data-in-online.htm	Application Interface Availability	Interoperabili ty & Portability
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	ArcGIS Online implements FIPS 140-2 compliant cryptographic algorithms	ArcGIS Online は、FIPS 140-2 に準拠した暗号化アルゴリズムを実装しています。	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	CSP-owned	Customers have complete ownership of their data at all times. Customer datasets are deleted within 60 days of contract termination unless otherwise specified by the customer.	お客様は、常にデータの完全な所有権を持ちます。 お客様のデータセットは、お客様の指定がない限り、契約終了後 60 日以内に削除されます。	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments annually.	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、社内で定期的に評価され、毎年独立した評価が行われています。	Infrastructure and Virtualization Security Policy and Procedures	Infrastructure & Virtualization Security
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Cloud infrastructure providers virtualization technologies are regularly evaluated internally and by independent assessments annually.	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、社内で定期的に評価され、毎年独立した評価が行われています。		
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	ArcGIS Online utilizes the capacity of two major cloud infrastructure providers to meet customer demands and Service Level Agreements (SLA) for availability, quality and capacity. Each cloud provider offers SLAs for their infrastructure	ArcGIS Onlineは、2 つの主要なクラウド インフラストラクチャ プロバイダーの容量を利用して、可用性、品質、容量に関するお客様の要求とサービス レベル契約 (SLA) を満たします。各クラウド プロバイダーは、それぞれのインフラストラクチャの SLA を提供しています。	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	All access to the infrastructure is monitored, tracked and recorded	インフラストラクチャへのアクセスはすべて監視、追跡、記録されます。	Network Security	
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP requirements	データは、FIPS 140-2 準拠の暗号化アルゴリズムである AES-256 で保存時に暗号化されます。これは、FedRAMP 要件と一致しています。		
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	ArcGIS Online data in transit is over HTTPS via TLS 1.2 Only.	転送中の ArcGIS Online のデータは、TLS 1.2 のみを介して HTTPS で転送されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	All ArcGIS Online architectural diagrams (Networks and systems combined) are reviewed in accordance to the FedRAMP requirements. Updates to the diagrams are done as needed usually upon approval for architectural changes	ArcGIS Online のすべての構成図 (ネットワークとシステムを組み合わせたもの) は、FedRAMP 要件に従って見直されます。 構成図の更新は、通常、構成変更の承認時に必要に応じて行われます。	Network Security	Infrastructure & Virtualization Security
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	This is part of the ArcGIS System Security Plan. Access to the details in the ArcGIS Online SSP can be provided upon signing an NDA	ArcGIS システム セキュリティ計画の一部です。ArcGIS Online SSP の詳細へのアクセスは、NDA に署名することで提供されます。		
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	N/A	CSP-owned	ArcGIS Online is a SaaS offering	ArcGIS Online は SaaS で提供されています。	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	ArcGIS Online utilizes separate production and non-production environments. Customers can purchase a separate non-production organization for testing/staging purposes.	ArcGIS Online では、本番環境と非本番環境を分けて運用しています。お客様は、テスト/ステージングを目的とした非運用組織を別途購入することができます。	Production and Non- Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	ArcGIS Online security infrastructure exists on an isolated private network subnet. All logs from every instance are stored in a common repository. Implementation ensures only ArcGIS Online Administrators can read logs. Collected logs are not modified or deleted by anyone.	ArcGIS Online のセキュリティ インフラストラクチャは、隔離されたプライベート ネットワーク サブネット上に存在します。すべてのインスタンスからのすべてのログは、共通のリポジトリに保存されます。ArcGIS Online の管理者のみがログを読むことができるように実装されています。収集されたログは誰にも変更または削除されません。	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to- date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	ArcGIS Online enforces using only TLS 1.2 for encrypted communication with customer systems. Endpoints are regularly validated against SSL Labs and dynamic scanners to ensure the encryption is in alignment with current industry recommendations.	ArcGIS Online では、お客様のシステムとの暗号化通信に TLS 1.2 のみの使用を必須とします。エンドポイントは SSL ラボおよびダイナミック スキャナーに対して定期的に検証され、暗号化が現在の業界の推奨事項に一致していることを確認します。	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	See ArcGIS Online security presentation materials within the ArcGIS Trust Center documents.	ArcGIS Trust Center ドキュメント内の ArcGIS Online セキュリティ プレゼンテーション資料をご参照ください。	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	Shared CSP and 3rd-party	ArcGIS Online utilizes AWS & Microsoft Azure native FedRAMP authorized security features to route users to ArcGIS Online resources, these Cloud Service Provider features provide protection against attacks such as common DDoS attack	ArcGIS Onlineは、AWS と Microsoft Azure のネイティブ FedRAMP 認定セキュリティ機能を利用して、ユーザーを ArcGIS Online リソースに誘導します。これらのクラウド サービス プロバイダーの機能は、一般的な DDoS 攻撃などの攻撃から保護します。	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Logging and monitoring policies are part of the FedRAMP program and reviewed annually. All policies are maintained in a centralized location that is accessible by employees.	ログとモニタリングの方針は FedRAMP プログラムの一環として毎年見直されます。すべての方針は、従業員がアクセスできる一元化された場所で保管されます。	Logging and Monitoring Policy and Procedures	Logging and Monitoring
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Polices and procedures are reviewed annually as part of our FedRAMP authorization	方針と手順は、FedRAMP 認定の一環として毎年見直されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	Audit logs are retained as defined by ArcGIS online retention policy which is in alignment with FedRAMP requirements.	監査ログは、FedRAMP 要件に沿った ArcGIS Online の保持ポリシーに従って保持されます。	Audit Logs Protection	Logging and Monitoring
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team	監査ログは、セキュリティ チームによって ArcGIS Online ソリューション内で毎週レビューされます。	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	Esri security team reviews infrastructure logs weekly. Customers are responsible for monitoring their own activity logs which include user logs and activities.	Esri セキュリティ チームは、インフラストラクチャ ログを毎週レビューします。ユーザー ログおよびアクティビティを含むアクティビティ ログの監視はお客様の責任です。		
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Esri security team and each customer has access to their own organizational audit logs.	Esri セキュリティ チームおよびお客様は、各組織の監査ログにアクセスできます。	Audit Logs Access and Accountability	
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team. Customers re responsible for reviewing their organizational audit logs.	監査ログは、セキュリティ チームによって ArcGIS Online ソリューション内で毎週レビューされます。組織の監査ログのレビューはお客様の責任です。	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	Audit logs are reviewed weekly within the ArcGIS Online solution by the Security team. Customers re responsible for reviewing their organizational audit logs.	監査ログは、セキュリティ チームによって ArcGIS Online ソリューション内で毎週レビューされます。組織の監査ログのレビューはお客様の責任です。		
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	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 のセキュリティを向上させ、イベント ログや監視プロセス、記録の正確なレポートの詳細を提供するため、すべてのサービスは一貫した時刻設定標準 (PST、GMT、UTC など) を使用します。可能な限り、ArcGIS Online システム全体で正確な時刻を維持するために、標準化および参照のための中部時刻のソースをホストする Network Time Protocol を通じてサーバー クロックが同期されます。	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Data logging in alignment with NIST standards	データ ロギングは NIST 規格に準拠しています。	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	Esri has a formal company security policy which addresses the audit and accountability requirements which includes logging. Associated procedures are updated at least annually. AGO weekly log reviews are conducted as part of the continuous monitoring activities which also includes an annual review or when there is a change in the environment.	Esri には、ログを含む監査および説明責任の要件に対応する、正式な企業セキュリティ ポリシーがあります。 関連する手順は少なくとも年 1 回更新されます。AGO のログの毎週のレビューは、継続的な監視活動の一環として実施されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	ArcGIS Online audit records are generated in alignment with FedRAMP Moderate requirements which include ensuring they contain: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes.	ArcGIS Online の監査記録は、FedRAMP Moderate 要件に沿って生成されます。FedRAMP Moderate 要件には、アカウント ログオンの成功と失敗のイベント、アカウント管理イベント、オブジェクト アクセス、ポリシー変更、権限機能、プロセス追跡、システム イベントが含まれます。Web アプリケーションの場合: すべての管理者活動、認証チェック、権限チェック、データ削除、データ アクセス、データ変更、権限変更が含まれます。	Log Records	Logging and Monitoring
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Only accessible by the ArcGIS Online infrastructure administrators	ArcGIS Online インフラストラクチャ管理者のみがアクセス可能です。	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	Key management policies, procedures, and processes for ArcGIS Online align with FedRAMP requirements.	ArcGIS Online の鍵管理ポリシー、手順、プロセスは、FedRAMP 要件に準拠しています。	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Logging is enabled for auditing and reporting cryptographic key usage via the cloud native key management systems.	クラウド ネイティブの鍵管理システムを介して、暗号鍵の使用状況を監査および報告するためのログが有効になっています。	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	Shared CSP and 3rd-party	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 のクラウド 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管理に関する高い業界標準に準拠した物理的なセキュリティ対策をデータ センターに導入しています。詳細については、以下の各社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/enus/trustcenter/Compliance Amazon Web Services: https://aws.amazon.com/compliance/	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	ArcGIS Online has developed a system configuration baseline in alignment with industry best practices such as CIS benchmarks and DISA STIGS.	ArcGIS Online は、CIS ベンチマークや DISA STIGS などの業界のベスト プラクティスに沿ったシステム構成ベースラインを開発しています。	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	No	CSP-owned	Impacted customers are notified within 72 hours	影響を受けるお客様には 72 時間以内に通知します。		
SEF-01.1	Are policies and procedures for security incident management, e- discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FedRAMP requirements.	インシデント管理は、FedRAMP 要件に沿った ArcGIS Online のインシデント対応計画文書に規定されています。	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Incident response plan is tested and reviewed annually	インシデント対応計画は毎年テストされ、見直されます。		

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with the FedRAMP requirements.	ArcGIS Online のインシデント対応計画は、FedRAMP 要件に沿っています。	Service Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with the FedRAMP requirements and reviewed annually.	ArcGIS Online のインシデント対応計画は、FedRAMP 要件に沿ったものであり、毎年見直されます。		
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	ArcGIS Online Incident Response plan is in alignment with FedRAMP requirements.	ArcGIS Online のインシデント対応計画は、FedRAMP 要件に沿っています。	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	ArcGIS Online tests the Contingency and Incident Response Plans annually (at a minimum) in alignment with FedRAMP requirements.	ArcGIS Online は、FedRAMP 要件に沿って、緊急時対応計画およびインシデント対応計画を（最低でも）毎年テストします。	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	The ArcGIS Online Incident Response plan is in alignment with FedRAMP requirements and its effectiveness is measured using metrics that are tracked and monitored and regularly reviewed.	ArcGIS Online のインシデント対応計画は、FedRAMP 要件に沿ったものであり、その有効性は、追跡、監視され、定期的に見直されるメトリクスを使用して測定されます。	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Esri maintains a Product Security Incident Response Team (PSIRT) to manage security incidents using the FIRST PSIRT services framework to guide processes related to the intake, validation, and prioritization of security related events.	Esri はセキュリティ インシデントを管理するために　PSIRT (Product Security Incident Response Teams) を運営し、FIRST PSIRT サービス フレームワークを使用して、セキュリティ関連イベントの取り込み、検証、優先順位付けに関連するプロセスをガイドしています。	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	Impacted customers are notified within 72 of confirmed breach	影響を受けるお客様には、侵害されたことが確認されてから 72 時間以内に通知します。	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Impacted customers are notified within 72 of confirmed breach.	影響を受けるお客様には、侵害されたことが確認されてから 72 時間以内に通知します。		
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	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の外部関係者との連絡を維持し、必要に応じて適切な措置を迅速に講じ、助言を得ることができるようにしています。	Points of Contact Maintenance	
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Managers of ArcGIS Online employees are responsible for ensuring awareness of applicable security policies and procedures for team members. A customer responsibility matrix is available for customers within the ArcGIS Trust Center to ensure alignment with FedRAMP obligations.	ArcGIS Online の従業員の管理者は、チーム メンバーに適用されるセキュリティ ポリシーおよび手順を確実に認識させる責任があります。FedRAMP の義務と整合性を確保するために、お客様には ArcGIS Trust Center 内で、お客様の責任マトリックスを提供しています。	SSRM Policy and Procedures	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Policies and procedures are reviewed and updated annually or in the event of significant changes.	ポリシーと手順は、毎年または重要な変更があった場合に見直され、更新されます。	SSRM Policy and Procedures	Supply Chain Management, Transparency, and Accountability
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and reviewed and updated annually. Esri is incorporating supplementary Supply Chain security requirements from NIST 800-53 Revision 5.	これは私たちのセキュア開発ライフサイクルの一部であり、毎年レビューと更新がされています。Esri は 800-53 Revision 5 から追加されたサプライチェーンのセキュリティ要件を取り入れています。	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	No	CSP-owned	Esri published the ArcGIS Online Customer Responsbilitiy Matrix (CRM) to the ArcGIS Trust Center documents.	Esri は ArcGIS Trust Center のドキュメントに ArcGIS Online のお客様の責任マトリックス (CRM) を公開しました。	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	CSP-owned	Responsibilities are delineated within the ArcGIS Online Customer Responsibility Matrix (CRM).	責任は ArcGIS Online のお客様の責任マトリックス (CRM) 内に定義されています。	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and reviewed and updated annually	これはセキュア開発ライフサイクルの一部であり、毎年レビューされ、更新されます。	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	ArcGIS Online has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the ArcGIS Online control environment.	ArcGIS Online は、正式な定期監査プログラムを確立しており、これには継続的で独立した内部および外部の評価が含まれ、ArcGIS Online の管理環境の実装および運用の有効性を検証しています。	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	A supplier inventory is maintained to ensure validation adherence with ArcGIS Online security and operational standards. As part of ArcGIS Online operations there are no subcontractors authorized by Esri to view any customer owned content that you upload into ArcGIS Online.	サプライヤーのインベントリは、ArcGIS Online のセキュリティおよび運用標準に準拠していることを確認するために管理されています。 ArcGIS Online の運用の一環として、お客様が ArcGIS Online にアップロードしたお客様所有のコンテンツを Esri が閲覧することを許可した下請業者は存在しません。	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	Risk factors and associated assurance materials are reviewed for suppliers at least annually.	リスク要因と関連する保証資料は、少なくとも年 1 回、サプライヤーに対して見直されます。	Supply Chain Risk Management	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	CSP-owned	ArcGIS Online's Terms of use are available within the ArcGIS Trust Center documents tab: https://www.esri.com/content/dam/esrisites/en-us/media/legal/ma-translations/english.pdf	ArcGIS Online の利用規約は ArcGIS Trust Centerのドキュメントにあります: https://www.esri.com/content/dam/esrisites/en-us/media/legal/ma-translations/english.pdf	Primary Service and Contractual Agreement	Supply Chain Management, Transparency, and Accountability
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	CSP-owned	ArcGIS Online third party agreement processes include periodic review and reporting, and are reviewed by independent auditors.	ArcGIS Online の第三者契約プロセスには、定期的なレビューと報告が含まれており、独立した監査者によってレビューされます。	Supply Chain Agreement Review	
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	ArcGIS Online has established a formal, periodic audit program that includes continual, independent internal and annual external assessments to validate the implementation and operating effectiveness of the ArcGIS Online control environment.	ArcGIS Online は、正式な定期監査プログラムを確立しており、これには継続的で独立した内部評価および年次の外部評価が含まれ、ArcGIS Online の管理環境の実装および運用の有効性を検証しています。	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and agreements are reviewed annually	これはセキュア開発ライフサイクルの一部であり、毎年レビューされ、更新されます。	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	CSP-owned	This is part of our Secure Development Lifecycle and agreements are reviewed annually	これはセキュア開発ライフサイクルの一部であり、毎年レビューされ、更新されます。	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	CSP-owned	An annual assessment is conducted of the entire ArcGIS Online solution including Supply Chain organizations, in alignment with FedRAMP requirements	FedRAMP 要件に沿って、サプライチェーン組織を含む ArcGIS Online ソリューション全体について、毎年評価が実施されます。	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	Priority of addressing vulnerabilities in alignment with FedRAMP requirements.	FedRAMP 要件に沿った脆弱性への対応を優先します。	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently	FedRAMP 要件に沿って、ArcGIS Online のシステムで使用またはインストールされている脅威検出シグネチャと行動分析ツールが頻繁に更新されます。	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	All systems in ArcGIS Online as well as administrator workstations have anti-malware installed. This is in alignment to FedRAMP requirements.	ArcGIS Online のすべてのシステムおよび管理者ワークステーションには、マルウェア対策がインストールされています。これは、FedRAMP の要件に沿ったものです。	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently	FedRAMP 要件に沿って、ArcGIS Online のシステムで使用またはインストールされている脅威検出シグネチャと行動分析ツールが頻繁に更新されます。		
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	This is part of our Continuous Monitoring as part of our FedRAMP authorization. Esri's Software Security & Privacy team notifies and coordinates with the appropriate Operations Teams when conducting security-related activities within the system boundary. Activities include, vulnerability scanning, contingency testing, and incident response exercises. ArcGIS Online performs external vulnerability scans at least monthly and identified issues are investigated and tracked to resolution - This is performed annually by a third party assessor against FedRAMP moderate controls, including the addition of pentesting. ArcGIS Online also addressing Emergency Operational Directives as they are issued.	これは FedRAMP 認定の一環としての継続的モニタリングの一部です。Esri のソフトウェア セキュリティ & プライバシー チームは、システム境界内でセキュリティ関連の活動を実施する際に、適切な運用チームに通知し、調整します。これらの活動には、脆弱性スキャン、緊急時対応テスト、インシデント対応の訓練が含まれています。ArcGIS Online は少なくとも毎月、外部の脆弱性スキャンを実施し、特定された問題は調査され、解決まで追跡されます。これは、FedRAMP Moderate 管理に対して、第三者の評価者によって毎年レビューされ、追加の侵入テストも含まれます。ArcGIS Online は、緊急運用指令が発行された場合にも対応しています。	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	In alignment with FedRAMP requirements threat detection signatures and behavioral analysis tools used or installed on systems in ArcGIS Online are updated frequently	FedRAMP 要件に沿って、ArcGIS Online のシステムで使用またはインストールされている脅威検出シグネチャと行動分析ツールが頻繁に更新されます。	Detection Updates	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.	システム、Web アプリケーション、データベースのスキャンを含む ArcGIS Online に対する脆弱性評価は、継続的モニタリング計画の一環として、少なくとも毎月実施されます。	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	CSP-owned	Penetration testing is done through our SAA process.	侵入テストは SAA プロセスを通じて行われます。	Penetration Testing	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.	システム、Web アプリケーション、データベースのスキャンを含む ArcGIS Online に対する脆弱性評価は、継続的モニタリング計画の一環として、少なくとも毎月実施されます。	Vulnerability Identification	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans. Issues are categorized by adjusted CVSS scores to reflect operational risk and remediated in alignment with FedRAMP Moderate timelines: HIGH risk - within 30 days, MODERATE risk - within 90 days, and LOW risk - within 180 days. Critical risk issues are addressed in less then 7 days.	システム、Web アプリケーション、データベースのスキャンを含む ArcGIS Online に対する脆弱性評価は、継続的モニタリング計画の一環として、少なくとも毎月実施されます。問題は、運用上のリスクを反映するように調整された CVSS スコアによって分類され、FedRAMP Moderate のタイムラインに沿って対処されます: 高リスクの場合 30 日以内、中リスクの場合 90 日以内、低リスクの場合 180 日以内。重大なリスクの問題は 7 日以内に対処されます。	Vulnerability Prioritization	Threat & Vulnerability Management
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	See - TVM-08.1 - The ArcGIS Online Continuous Monitoring Plan (in alignment with FedRAMP Moderate control requirements) ensures appropriate tracking and reporting of vulnerabilities through a Plan of Actions and Milestones (POAM) listing. Issues are discussed with authorized resources as part of monthly ConMon meetings.	TVM-08.1 をご参照ください。ArcGIS Online の継続的モニタリング計画 (FedRAMP Moderate コントロール要件に準拠) は、POAM (Plan of Actions and Milestones) リストを通じて、脆弱性の適切な追跡と報告を保証します。問題は、毎月の ConMon ミーティングの一環として、権限を与えられたリソースと議論されます。	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	This is part of our Continuous Monitoring as part of our FedRAMP authorization. Vulnerability scans occur at least monthly and metrics are summarized and discussed as part of the monthly ConMon meeting,	これは、FedRAMP 認定の一環としての継続的モニタリングの一部です。脆弱性スキャンは少なくとも毎月実施され、メトリクスは毎月の ConMon ミーティングの一部として要約され、議論されます。	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Customers are responsible for establishing, documenting and maintaining policies and procedures for endpoints.	エンドポイントに関するポリシーと手順の確立、文書化、維持は、お客様の責任です。	Endpoint Devices Policy and Procedures	Universal Endpoint Management
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	N/A	CSP-owned	Customers are responsible for updating policies and procedures for universal endpoint.	ユニバーサル エンドポイントに関するポリシーと手順の更新は、お客様の責任です。		
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	N/A	CSC-owned	Customers are responsible for maintaining an internal software solution with the approved list of applications that can be installed on managed endpoints based on OS	OS に基づく管理対象のエンドポイントにインストール可能なアプリケーションの承認リストを含む内部ソフトウェア ソリューションの管理は、お客様の責任です。	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	N/A	CSP-owned	Customers are responsible for validating endpoint device compatibility with OS and Applications.	OS やアプリケーションとエンドポイント デバイスの互換性の検証は、お客様の責任です。	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	N/A	CSC-owned	Customers are responsible for maintaining a centralized inventory system for all managed endpoints which ingests data from various inventory systems to prevent duplicates.	重複を防ぐためにさまざまなイベントリ システムからデータを取り込む、すべての管理対象のエンドポイントの集中イベントリ システムの管理は、お客様の責任です。	Endpoint Inventory	

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSP Implementation Description (Optional/Recommended) (日本語訳)	CCM Control Title	CCM Domain Title
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	Customers are responsible for defining, implementing and evaluating technical measures, that enforce policies and controls for all endpoints access.	すべてのエンドポイント アクセスに対するポリシーと制御を実施する技術的手段の定義、実装、評価は、お客様の責任です。	Endpoint Management	Universal Endpoint Management
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	Shared CSP and CSC	AGO system configuration implements an automatic screen lock after a pre-defined period of time of inactivity. Customers are responsible for ensuring lockscreens are enabled for their workstations.	AGO システム構成は、事前に設定した非アクティブな時間が経過した後、自動スクリーン ロックを実装します。ワークステーションでロックスクリーンが有効化になっているかの確認は、お客様の責任です。	Automatic Lock Screen	
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Customers are responsible maintaining changes to the endpoint OS and/or application.	エンドポイントの OS および/またはアプリケーションの変更の管理は、お客様の責任です。	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	N/A	CSC-owned	Customers are responsible for all their managed endpoints to be encrypted based on their organizational security requirements	組織のセキュリティ要件に基づき、管理対象のエンドポイントを暗号化することは、お客様の責任です。	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	Customers are responsible implementing anti-malware detection and prevention technology services on customer managed endpoints.	お客様が管理するエンドポイントにマルウェア検知および防止技術サービスを実装することは、お客様の責任です。	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Esri assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering, software firewalls, and malware detection.	Esri 資産 (ラップトップなど) は、電子メール フィルタリング、ソフトウェア ファイアウォール、マルウェア検知を含むアンチウイルス ソフトウェアで構成されます。	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	NA	Shared CSP and CSC	ArcGIS Online customers are responsible for the management of the data they place into ArcGIS Online. Esri has no insight as to what type of content the customer chooses to store in ArcGIS Online and the customer retains complete control of how they choose to classify their content, where it is stored, used and protected from disclosure.	ArcGIS Online に保存されたデータの管理は、お客様の責任です。Esri は、お客様がどのような種類のコンテンツを ArcGIS Online に保存するかについて一切関知せず、お客様が、コンテンツの分類方法、保存場所、使用方法、開示からの保護について、完全に管理します。	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	No	CSP-owned	Not utilized	利用無し	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	N/A	CSC-owned	Customers are responsible for policies and procedures for mobile device security which reserves the right to remotely wipe mobile devices.	モバイル デバイスをリモート削除する権利を有するモバイル デバイス セキュリティのポリシーと手順は、お客様の責任です。	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third- party endpoints with access to organizational assets?	N/A	CSP-owned	Customers are responsible implementing processes, procedures and technical measures evaluating security of third-party endpoints.	サードパーティ エンドポイントのセキュリティを評価するプロセス、手順、技術的措置の実装は、お客様の責任です。	Third-Party Endpoint Security Posture	
End of Standard							

ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)		CCM Control Title	CCM Domain Title

Summary of answer fields:

Assessment Question

The description of the question.			

CSP CAIQ Answer

The Cloud Service Provider (CSP) must respond with "Yes"/ "No"/ "NA" next to the corresponding assessment question, and for the portion(s) of the CCM control specification they are responsible and accountable for implementing.

Meaning of possible replies:

• "Yes": The portion(s) of the CCM control requirement corresponding to the assessment question is met.

• "No": The portion(s) of the CCM control requirement corresponding to the assessment question is not met.

• "N/A": The question is not in scope and does not apply to the cloud service under assessment.

NOTES:

A "Yes" answer i

A "No" answer indicates that the portion of the control in question is not implemented, while in scope of the assessment. The CSP has to assign the implementation responsibility of the control to the relevant party under column "SSRM control ownership" A "N/A" answer indicates that the portion of the control in question is out of scope of the assessment. The "SSRM control ownership" column is to be left blank (e.g., greyed out), and optionally the CSP may explain why it is the case

Shared Security Responsibility Model (SSRM) control ownership

The CSP control responses shall identify control applicability and ownership for their specific service.

• CSP-owned: The CSP is entirely responsible and accountable for the CCM control implementation.

• CSC-owned: The Cloud Service Customer (CSC) is entirely responsible and accountable for the CCM control implementation.

• Third-party outsourced: The third-party CSP in the supply chain (e.g., an IaaS provider) is responsible for CCM control implementation, while the CSP is fully accountable.

• Shared CSP and CSC: Both the CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is shared between CSP and the third party, but the CSP remains fully accountable.

Note: The CAIQv4 SSRM schema is tailored to CCMv4's Supply Chain Management, Transparency, and Accountability (STA) domain, controls 1-6, and their corresponding implementation guidelines.

CSP implementation description (optional/recommended)

A description (with references) of how the cloud service provider meets (or does not meet) the portion(s) of the SSRM control they are responsible for. If "NA," explain why.