アマゾン ウェブ サービス: リスクおよびコンプライアンス

2015 年 4 月

（本書の最新版については、http://aws.amazon.com/compliance/aws-whitepapers/

を参照してください）

本文書は、AWS のお客様が IT 環境をサポートする既存の統制フレームワークに AWS を統合する際に役立つ情報を提供するものです。AWS 統制の評価に関する基本的なアプローチについて説明し、統制環境の統合の際に役立つ情報を提供します。また、クラウドコンピューティングのコンプライアンスに関する一般的な質問について、AWS 固有の情報を掲載しています。

目次

リスクとコンプライアンスの概要

AWS とそのお客様は IT 環境の統制を分担しており、IT 環境を管理する責任は両者にあります。AWS 側の責任分担には、安全性の高い、統制されたプラットフォームでサービスを提供し、幅広いセキュリティ機能をユーザーに提供することが含まれます。お客様側の責任分担には、用途に合わせて安全で統制された方法で IT 環境を設定することが含まれます。お客様から使用方法と設定を AWS にお伝えいただかないとしても、AWS からはお客様に関わるセキュリティと統制環境についてお伝えします。そのために、AWS は次のことを行います。

- 業界の認定と独立したサードパーティによる証明を取得します（本文書で説明します）。
- AWS のセキュリティと統制に関する情報をホワイトペーパーおよびウェブサイトコンテンツで公表します。
- （必要に応じて）NDA に従い AWS のお客様に証明書、レポートなどの文書を直接提供します。

AWS のセキュリティの詳細については、AWS セキュリティセンターを参照してください。AWS セキュリティプロセスの概要ホワイトペーパーでは、AWS の全般的なセキュリティ統制とサービス固有のセキュリティについて説明しています。

責任分担環境

IT インフラストラクチャを AWS に移行すると、お客様と AWS の責任分担モデルを構成します。この共有モデルは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、様々なコンポーネントを AWS が運用、管理、およびコントロールするというものです。このため、お客様の運用上の負担を軽減する助けとなることができます。お客様の責任としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理が想定されます。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用可能な法律および規制に応じて異なります。したがって、お客様は選択するサービスを注意深く検討する必要があります。お客様は、ホストベースのファイアウォール、ホストベースの侵入検知/防御、暗号化とキー管理などのテクノロジーを利用してセキュリティを拡張し、さらに厳格なコンプライアンス要件を満たすことができます。この責任分担モデルという特徴によって、業界固有の認証要件に適合するソリューションの配備を可能にする、柔軟性と顧客コントロールも提供されます。

このお客様と AWS の責任分担モデルは IT 統制にも拡張されます。IT 環境を運用する責任を AWS とお客様の間で分担するのと同様に、IT 統制の管理、運用、および検証も分担となります。AWS 環境にデプロイした物理インフラストラクチャに関連した統制をそれまでお客様が管理していた場合は、AWS が管理することで、お客様にかかる統制の負荷を軽減できます。お客様によって AWS のデプロイ方法は異なります。特定の IT 統制の管理を AWS に移行し、（新しい）分散コントロール環境を構築する作業は、お客様の判断で行うことができます。移行後は、AWS の統制とコンプライアンスの文書（本文書の「AWS の認定とサードパーティによる証明」セクションで説明します）を使用し、必要に応じて統制の評価と検証の手順を実行できます。

次のセクションでは、AWS のお客様が分担統制環境を効果的に評価および検証するためのアプローチについて説明します。

強力なコンプライアンス管理

IT のデプロイ方法にかかわらず、AWS のお客様はこれまでどおり、IT 統制環境全体に対する適切な管理を維持することが求められます。主な作業内容として、（関連資料を基にした）必要なコンプライアンスの目標と要

件の把握、その目標と要件を満たす統制環境の構築、組織のリスク許容度に基づく必要な妥当性の把握、統制環境の運用効率の検証などがあります。AWS クラウドへのデプロイにより、企業が各種の統制や検証方法を適用するにあたって選択の幅が生まれます。

お客様のコンプライアンスと管理が強力な場合は、次の基本的なアプローチが考えられます。

1. AWS から入手できる情報と他の情報をレビューして IT 環境全体について可能な限り理解し、すべてのコンプライアンス要件を文書化します。
2. 企業のコンプライアンス要件を満たす統制目標を設計し、実施します。
3. 社外関係者が行う統制を特定し、文書化します。
4. すべての統制目標が満たされ、すべての主な統制が設計され、効率的に運営されていることを検証します。

この方法でコンプライアンス管理にアプローチすることで、社内の統制環境をより理解することができます。また、実行すべき検証活動を明確にすることができます。

AWS 統制の評価と統合

AWS は、ホワイトペーパー、レポート、認定、その他サードパーティによる証明を通じて、当社の IT 統制環境に関する幅広い情報をお客様にご提供しています。本文書は、お客様が使用する AWS サービスに関連した統制、およびそれらの統制がどのように検証されているかをお客様にご理解いただくことをお手伝いするためのものです。この情報はまた、お客様の拡張された IT 環境内の統制が効果的に機能しているかどうかを明らかにし、検証するのにも有用です。

従来、統制目標と統制の設計と運用効率の検証は、社内外の監査人がプロセスを実地検証し、証拠を評価することによって行われています。お客様またはお客様の社外監査人による直接の監視または検証は、一般的に、統制の妥当性を確認するために行われます。AWS などのサービスプロバイダを使用する場合、企業はサードパーティによる証明および認定を要求し、評価することで、統制目標と統制の設計と運用効率の合理的な保証を獲得します。その結果、お客様の主な統制を AWS が管理している場合でも、統制環境を統一されたフレームワークのまま維持し、効率的に運用しながらすべての統制を把握し、検証することができます。サードパーティによる証明と AWS の認定によって、統制環境を高いレベルで検証できるだけでなく、AWS クラウドの自社の IT 環境に対して特定の検証作業を自社で実行する要求を持つお客様にも役立ちます。

AWS の IT 統制情報

AWS は、次の 2 つの方法で IT 統制情報をお客様に提供します。

1. **固有の統制定義。**AWS のお客様は、AWS が管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1 (SOC 1) Type II レポートで幅広く詳細な IT 統制を公開しています。SOC 1 レポートの旧称は Statement on Auditing Standards (SAS) No. 70、Service Organizations レポートです。一般的に Statement on Standards for Attestation Engagements No. 16 (SSAE 16) レポートと呼ばれ、米国公認会計士協会（AICPA）が作成し、幅広く認められている監査基準です。SOC 1 監査は、AWS で定義している統制目標および統制活動（AWS が管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます）の

設計と運用効率の両方に関する詳細な監査です。「Type II」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWS の外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWS の統制環境に高い信頼を置けることを示します。AWS の統制は、Sarbanes-Oxley (SOX) セクション 404 の財務諸表監査など、多くのコンプライアンス目的に合わせて検討され、設計され、効率的に運用することができます。SOC 1 Type II レポートの利用は、一般的に他の外部認定機関からも許可されています（例えば、ISO 27001 の監査人は顧客の評価を完成するために SOC 1 Type II レポートを要求する場合があります）。

他の固有の統制活動は、AWS の Payment Card Industry (PCI) および連邦情報セキュリティマネジメント法（FISMA）のコンプライアンスに関連します。後述のように、AWS は FISMA Moderate 基準と PCI Data Security 基準に準拠しています。これらの PCI 基準と FISMA 基準は非常に規範的であり、AWS が公開基準に従っていることの独立した検証が求められます。

2. **一般的な統制基準への準拠。**包括的な統制基準が必要な場合には、AWS を業界基準の面から評価することも可能です。AWS は幅広く包括的なセキュリティ基準に準拠し、安全な環境を維持するためのベストプラクティスに従っており、ISO 27001 認定を取得しています。AWS はクレジットカード情報を処理する会社にとって重要な統制に準拠しており、PCI Data Security Standard (PCI DSS) の認定を取得しています。AWS は米国政府機関から要求される幅広く詳細な統制に準拠しており、FISMA 基準に準拠しています。このような一般的な基準に準拠しているので、お客様は所定の統制およびセキュリティプロセスの包括的な特性について詳細な情報を得ることができます。また、コンプライアンスを管理するときに、それらの基準の準拠について考慮できます。

AWS の報告、認定、およびサードパーティによる証明の詳細については、本文書で後述します。

AWS のグローバルなリージョン展開

世界各地に設置されているデータセンターは、所在地によりリージョンに分けられています。本文書の執筆時点では、リージョンは 9 つあります。米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）（オレゴン）、欧州（アイルランド）、アジアパシフィック（シンガポール）、アジアパシフィック（東京）、アジアパシフィック（シドニー）、南米（サンパウロ）です。

AWS リスクおよびコンプライアンスプログラム

AWS では、お客様の管理フレームワークに AWS 統制を組み込むことができるように、リスクおよびコンプライアンスプログラムに関する情報を提供しています。この情報をもとに、AWS に関する統制と管理フレームワーク全体を文書化し、フレームワークの重要な部分としてご利用いただけます。

リスク管理

AWS マネジメントは、リスクを緩和または管理するためのリスク特定やコントロールの実装など、戦略的事業計画を開発してきました。また、少なくとも半年に一度、戦略的事業計画を再評価します。このプロセスでは、マネジメントがその責任領域内のリスクを特定し、これらのリスクを解決するために設計された適切な対策を実施することが求められます。

さらに、AWS 統制環境は、さまざまな内部的および外部的リスクアセスメントによって規定されています。AWS のコンプライアンスおよびセキュリティチームは、情報および関連技術のための統制目標（COBIT）フレームワークに基づいて、情報セキュリティフレームワークとポリシーを規定しました。また、ISO 27002 規格、米国公認会計士協会（AICPA）の信頼提供の原則（Trust Services Principles）、PCI DSS v3.0、および米国国立標準技術研究所（NIST）出版物 800-53 Rev 3（連邦政府情報システムにおける推奨セキュリティ統制）に基づいて、ISO 27001 認証対応フレームワークを実質的に統合しました。AWS は、セキュリティポリシーを維持し、従業員に対するセキュリティトレーニングを提供して、アプリケーションに関するセキュリティレビューを実行します。これらのレビューは、情報セキュリティポリシーに対する適合性と同様に、データの機密性、完全性、可用性を査定するものです。

AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。これらのスキャンは、基礎となる AWS インフラストラクチャの健全性と可視性を確認するためのものであり、顧客固有のコンプライアンス要件に適合する必要のある、顧客自身の脆弱性スキャンに置き換わることを意味するものではありません。お客様は事前に承認を得た上で、お使いのクラウドインフラストラクチャにスキャンを実施することができますが、対象はお客様のインスタンスに限り、かつ AWS 利用規約に違反しない範囲とします。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性/侵入テストリクエストフォームを使用してリクエストを送信してください。

統制環境

AWS は、Amazon 全体の統制環境の様々な面を利用するポリシー、プロセス、および統制活動を含む、包括的な統制環境を管理しています。この統制環境は、AWS のサービスを安全に提供するために用意されています。この集合的統制環境は、AWS の統制フレームワークの効率的な運用を支える環境を構築し維持するために必要な人員、プロセス、テクノロジを網羅しています。クラウドコンピューティング業界の主要機関が特定したクラウド固有の統制について、AWS は、該当する項目を AWS の統制フレームワークに統合しました。AWS は、統制環境の管理についてお客様を支援するため、先進的な実践が実施されるアイデアを求めて、このような業界団体を継続的にチェックします。

Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を確立する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。

AWS の組織構造が、事業運営の計画、実行、統制のフレームワークを支えています。この組織構造によって役割と責任が割り当てられ、適切な人員調達、操業の効率性、そして職務の分離が提供されます。またマネジメントは、重要な人員に関する権限と適切な報告体系を構築しました。当社では従業員に対し、その職務と AWS 施設へのアクセスレベルに応じて、法律および規制が認める範囲での学歴、雇用歴、場合によっては経歴の確認を、採用手続きの一環として実施しています。新たに採用した従業員には体系的な入社時研修を行い、Amazon のツール、プロセス、システム、ポリシー、手順について熟知させます。

情報セキュリティ

AWS では、お客様のシステムおよびデータの機密性、完全性、および可用性を保護するために設計された、公式の情報セキュリティプログラムを実施しました。また、公開ウェブサイトでは、お客様がデータを保護するために役立つ方法を説明したセキュリティホワイトペーパーを公開します。

AWS の報告、認定、およびサードパーティによる証明

AWS は外部の認定機関および独立監査人と協力し、AWS が制定・運用するポリシー、プロセス、および統制に関する重要な情報をお客様に提供しています。

FedRAMP[SM]

AWS は、Federal Risk and Authorization Management Program (FedRAMP[sm]) に準拠したクラウドサービスプロバイダです。AWS は認定された第三者評価組織（3PAO）である FedRAMP[sm] によって実施されるテストを完了し、FedRAMP[sm] 要件に Moderate 影響レベルで準拠することを示して、米国保健福祉省（HHS）により 2 つの Agency Authority to Operate (ATO) を取得しました。すべての米国政府機関は、FedRAMP[sm] レポジトリに格納されている AWS Agency ATO パッケージを利用して、アプリケーションやワークロードに対する AWS の評価、AWS の使用許可の付与、および AWS 環境へのワークロードの移行を行うことができます。2 つの FedRAMP[sm] Agency ATO はすべての米国リージョン（AWS GovCloud（米国）リージョンおよび AWS 米国東部/西部リージョン）に対応しています。

次のサービスは、上記のリージョンの認定範囲内に含まれます。

- Amazon Redshift。Amazon Redshift は、高速で完全マネージド型のペタバイト規模を誇るデータウェアハウスサービスです。シンプルで費用対効果の高さが特長であり、お客様はすべてのデータを既存のビジネスインテリジェンスツールで効率的に分析できます。
- Amazon Elastic Compute Cloud (Amazon EC2)。Amazon EC2 は、クラウド内で自在に規模を変更できるコンピューティング容量を提供します。ウェブスケールのコンピューティングを開発者が簡単に利用できるように設計されています。
- Amazon Simple Storage Service (S3)。Amazon S3 にはシンプルなウェブサービスインターフェイスが用意されており、いつでもウェブ上のどこからでも容量に関係なくデータを保存、取得できます。
- Amazon Virtual Private Cloud (VPC)。Amazon VPC は、AWS の論理的に隔離されたセクションを使用可能にする機能を提供します。そこでは、ユーザーが定義した仮想ネットワーク内で AWS リソースを起動することができます。
- Amazon Elastic Block Store (EBS)。Amazon EBS のストレージボリュームは、予測可能で、可用性と信頼性に優れており、稼働中の Amazon EC2 インスタンスにアタッチしてそのインスタンス内で 1 つのデバイスとして提供されます。
- AWS Identity and Access Management (IAM)。IAM を利用すると、AWS のサービスおよびリソースに対するお客様のユーザーのアクセスを安全にコントロールすることができます。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できます。

AWS の FedRAMP[sm] への準拠の詳細については、AWS の FedRAMP[sm] に関するよくある質問を参照してください。

FIPS 140-2

連邦情報処理規格（Federal Information Processing Standard/FIPS）出版物 140-2 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定する米国政府のセキュリティ基準です。FIPS 140-2 への準拠を必要とするお客様をサポートするために、AWS GovCloud（米国）内の SSL 終端は、FIPS 140-2 検証済みハードウェアを使用して運用されています。AWS は AWS GovCloud（米国）のお客様と連携して、AWS GovCloud（米国）環境の使用時にコンプライアンスの管理に必要となる情報を提供します。

FISMA と DIACAP

AWS は、米国政府機関のシステムを連邦情報セキュリティマネジメント法（Federal Information Security Management Act/FISMA）に準拠した状態で運用することができます。AWS インフラストラクチャは、システム所有者の承認プロセスの一環として、多様な政府機関システムの独立査定人によって評価されています。多数の米国政府機関の勤務者と国防省（DoD）が、NIST 800-37 および DoD Information Assurance Certification and Accreditation Process (DIACAP) に定義されているリスクマネジメントフレームワーク（RMF）プロセスに従い、AWS クラウドでホストされているシステムのセキュリティ認可を達成しています。

HIPAA

米国医療保険の携行性と責任に関する法律（HIPAA）の対象となる事業体とその取引先は、保護すべき医療情報を安全に処理、管理、保存できる環境として AWS 環境を利用しています。AWS はこのようなお客様と事業提携契約を結んでゆきたいと考えています。AWS では、医療情報の処理や保存に AWS の活用をお考えのお客様向けに、HIPAA 関連のホワイトペーパーもご用意しています。Creating HIPAA-Compliant Medical Data Applications with AWS ホワイトペーパーは、AWS を利用して HIPAA と経済的および臨床的健全性のための医療 IT に関する法律（HITECH）コンプライアンスを促進するシステムを運用する方法の企業向け概要説明となっています。

お客様は、アカウントで HIPAA アカウントと指定された任意の AWS サービスを使用できますが、BAA で定義された HIPAA の対象サービスでのみ、PHI を処理、保存、転送できます。現在、HIPAA の対象サービスは、Amazon EC2、Amazon EBS、Amazon S3、Amazon Redshift、Amazon Glacier、および Amazon Elastic Load Balancer の 6 つです。

AWS は標準ベースのリスク管理プログラムに従って、HIPAA の対象サービスが、HIPAA で要求されるセキュリティ、統制、および管理の各プロセスを確実にサポートするようにしています。これらのサービスを使用して PHI を保存、処理することで、お客様と AWS はユーティリティベースの運用モデルに該当する HIPAA 要件に対応することができます。AWS は、お客様の要求に応じて新しい対象サービスに優先順位を付けて追加しています。

ISO 9001

AWS は ISO 9001 認証を達成しており、AWS の ISO 9001 認証は AWS クラウドで品質管理された IT システムを開発、移行、運用するお客様を直接サポートします。お客様は、独自の ISO 9001 プログラムや業界別の品質プログラム（ライフサイエンスでの GxP、医療機器での ISO 13485、航空宇宙産業での AS9100、自動車産業での ISO/TS 16949 など）の取得に、AWS の準拠レポートを証拠として活用できます。品質システムの要件がないお客様にも、ISO 9001 認証により AWS の保証や透明性が向上するというメリットがあります。ISO 9001 認証は、

AWS サービスと運用リージョン（下記）および次のサービスの指定された範囲の品質管理システムを対象としています。

- AWS Cloud Formation
- AWS クラウドハードウェアセキュリティモデル（HSM）
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- AWS Storage Gateway
- Amazon Simple Workflow Service (SWF)
- Amazon Virtual Private Cloud (VPC)
- 基礎となる物理インフラストラクチャと AWS 管理環境

AWS の ISO 9001 認定が対象となる AWS リージョンには、米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）、南米（サンパウロ）、欧州（アイルランド）、アジアパシフィック（シンガポール）、アジアパシフィック（シドニー）、およびアジアパシフィック（東京）が含まれます。

ISO 9001:2008 は製品とサービスの品質を管理するための世界規格です。9001 規格では、国際標準化機構（ISO）の品質マネジメント及び品質保証技術委員会が定義した 8 つの原則に基づいて、品質マネジメントシステムを概説しています。この 8 つの原則は以下のとおりです。

- 顧客重視
- リーダーシップ
- 人々の参画
- プロセスアプローチ
- マネジメントへのシステムアプローチ
- 継続的改善
- 意思決定への事実に基づくアプローチ
- 供給者との互恵関係

ISO 27001

AWS は、次のものを含む AWS インフラストラクチャ、データセンター、およびサービスを対象とした Information Security Management System (ISMS) の ISO 27001 認証を達成しています。これには次が含まれます。

- AWS CloudFormation
- AWS Cloudtrail
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Cloud Compute (EC2)
- AWS Direct Connect
- Amazon EC2 VM Import/Export
- AWS クラウドハードウェアセキュリティモデル（HSM）
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- AWS Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- 基礎となる物理インフラストラクチャ（GovCloud を含む）と AWS 管理環境

ISO 27001/27002 は世界で広く採用されているセキュリティ基準で、会社とカスタマー情報の管理の体系的なアプローチの要件とベストプラクティスを定めるものです。これは、刻々と変化する脅威のシナリオに適する定期的リスク査定に基づいています。認証を取得するためには、会社とカスタマー情報の機密性、完全性、および可用性に影響を与える情報セキュリティリスクを管理する体系的かつ継続的なアプローチが会社にあることを示す必要があります。この認定は、セキュリティ管理や作業に関する重要情報を提供するという Amazon の取り組みを補強するものです。AWS の ISO 27001 認定には、AWS の全リージョンのデータセンターが含まれており、AWS はこの認証を維持するための正式なプログラムを確立済みです。AWS は、ISO 27001 認定に関する追加情報と FAQ をウェブサイトで提供します。

ITAR

AWS GovCloud（米国）リージョンは、武器規制国際交渉規則（**ITAR**）コンプライアンスをサポートしています。包括的な ITAR コンプライアンスプログラム管理の一環として、ITAR 輸出規制の対象となる企業は、保護されたデータへのアクセスを米国人に制限し、およびそのデータの物理的なロケーションを米国の土地に制限することによって、意図しない輸出を制御する必要があります。AWS GovCloud（米国）は、物理的に米国に位置し、そこでは AWS のスタッフによるアクセスを米国人に制限しているという環境を提供しているため、適格企業は、ITAR の規制対象となる、保護された文書およびデータを送信、処理、格納することができます。

AWS GovCloud（米国）環境は、この要件において、顧客の輸出コンプライアンスプログラムをサポートする適切な統制がなされているかどうかを検証するために、独立したサードパーティによる監査を受けています。

PCI DSS レベル 1

AWS は、Payment Card Industry (PCI) データセキュリティ基準（Data Security Standard/DSS）にレベル 1 に準拠しています。お客様は、クラウドでクレジットカード情報を保管、処理、送信する私たちの PCI 準拠のテクノロジーインフラストラクチャで、アプリケーションを実行することができます。2013 年 2 月、PCI Security Standards Council では、PCI DSS Cloud Computing Guidelines をリリースしています。このガイドラインでは、カード保有者のデータ環境を管理しているお客様向けに、クラウドでの PCI DSS 管理作業の留意事項を記載しています。AWS では、お客様向けに PCI DSS Cloud Computing Guidelines を AWS PCI Compliance Package に組み込んでいます。AWS PCI Compliance Package には、AWS PCI Attestation of Compliance (AoC) と AWS PCI Responsibility Summary が含まれています。前者では、AWS が PCI DSS Version 3.0 においてレベル 1 サービス プロバイダに適用される標準を満たしていることが検証されています。後者では、AWS とお客様の間でコンプライアンスに関する責任をどのように分担するかが説明されています。

PCI DSS レベル 1 を対象とするサービスは次のとおりです。

- AWS Auto Scaling
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB (DDB)
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB (SDB)
- Amazon Simple Storage Service (S3)
- Amazon SQS
- Amazon SWF
- Amazon Virtual Private Cloud (VPC)

AWS PCI DSS レベル 1 認証のサービスの最新の範囲は、「PCI DSS レベル 1 に関するよくある質問」に記載されています。

SOC 1/SSAE 16/ISAE 3402

アマゾン ウェブ サービスは現在、Service Organization Controls 1 (SOC 1)、Type II レポートを発行しています。このレポートの監査は、証明業務基準書第 16 号（SSAE 16）および国際保証業務基準書第 3402 号（ISAE 3402）プロ基準に従って実施されます。この 2 つの基準レポートは、米国および国際的な会計監査機関の監査における幅広い要件を満たすために作られています。SOC 1 レポートの監査は、AWS の統制目標が適切に設計されて

いること、およびカスタマーデータを保護するために定義された個々の統制が効果的に機能していることを証明するものです。このレポートは、監査基準書第 70 号（SAS 70）Type II 監査レポートに代わるものです。

レポートには AWS SOC 1 の統制目標が記載されており、このレポート自体に、各統制目標と独立監査人による各統制のテスト手順の結果をサポートする統制活動が特定されています。

目標範囲	目標内容
セキュリティ組織	統制は、情報セキュリティポリシーが組織全体で実施され、伝達されていることについて、合理的な保証を提供するものです。
Amazon ユーザーアクセス	統制は、Amazon ユーザーアカウントが適時に追加、変更、および削除され、定期的にレビューされるように手順が構築されていることについて、合理的な確証を提供するものです。
論理的セキュリティ	統制は、データに対する許可のない内部的および外部的アクセスが適切に制限され、顧客データへのアクセスが他の顧客から適切に隔離されることについて、合理的な確証を提供するものです。
安全なデータ処理	統制は、AWS ストレージの場所と顧客開始点の間のデータ処理がセキュリティで保護され、適切にマッピングされることについて、合理的な保証を提供するものです。
物理的なセキュリティと環境の予防手段	Amazon が操業している建物やデータセンターに対する物理的なアクセスを権限のある人物にのみ制限し、故障や物理的な災害がコンピュータやデータセンター施設に与える影響を最小限に抑える手続きが存在するように、統制によって適切な保証を実現します。
変更管理	統制は、既存の IT リソースに対する変更（緊急／特殊な設定）が記録され、認証され、試験され、承認されて文書化されることについて、合理的な保証を提供するものです。
データの完全性、可用性および冗長性	統制は、伝送、保管、処理など、すべての段階を通じてデータの完全性が維持されることについて、合理的な保証を提供するものです。
インシデント処理	統制は、システム障害が記録、分析、および解決されることについて、合理的な保証を提供するものです。

SOC 1 レポートは、ユーザー組織の財務諸表の監査に関連する可能性が高い、サービス組織の統制を中心に設計されています。AWS の顧客基盤は広大で、AWS サービスの使用も同様に広大なので、お客様の財務諸表に対する統制の適用可能性は、お客様ごとに異なります。そのため、AWS SOC 1 レポートは、会計監査時に必要になる可能性が高い、特定の主要な統制と、多様な使用方法と監査シナリオに合う幅広い IT の一般的な統制を対象に設計されています。そのため、お客様は AWS インフラストラクチャを利用して、会計のレポートプロセスに欠かせないデータなど、重要なデータを保存および処理できます。AWS は、これらの統制の選択内容を定期的に再評価し、この重要な監査レポートのお客様のフィードバックと使用方法について考慮します。

SOC 1 レポートに関する AWS の取り組みは継続中で、定期監査のプロセスを継続していく予定です。SOC1 レポートの対象は次のとおりです。

- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- AWS Direct Connect
- Amazon DynamoDB
- Amazon EC2 VM Import/Export

- Amazon Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Load Balancing (ELB)
- Amazon Elastic MapReduce (EMR)
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon SimpleDB
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow (SWF)
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)

SOC 2

AWS では SOC 1 レポートに加え、Service Organization Controls 2 (SOC 2)、Type II レポートも発行しています。管理の評価における SOC 1 と同様、SOC 2 レポートは、その管理の評価を、米国公認会計士協会（AICPA）の信用提供の原則（Trust Services Principles）で定められている基準に拡張する証明レポートです。これらの原則では、AWS などのサービス組織に適用されるセキュリティ、可用性、処理の完全性、機密性、およびプライバシーに関連する主要業務管理が定義されています。AWS SOC 2 レポートは、統制に関する運用の有効性と設計が、米国公認会計士協会（AICPA）の信用提供の原則（Trust Services Principles）で示されているセキュリティ原則の基準を満たすことを評価したものとなっています。このレポートは、リーディングプラクティスの事前定義された業界標準に基づいて AWS のセキュリティに一層の透明性を与え、AWS の顧客データ保護に対する取り組みを詳細に示すものです。SOC 2 レポートの範囲には、SOC 1 レポートの対象と同じサービスが含まれます。対象となるサービスの詳細については上記の SOC 1 の説明を参照してください。

SOC 3

AWS は Service Organization Controls 3 (SOC 3) レポートを発行しています。SOC 3 レポートは、AWS SOC 2 レポートの要約を公開したもので、AICPA SysTrust セキュリティシールを表示します。レポートには、（SOC 2 レポートに含まれる AICPA の Security Trust Principles に基づく）管理の操作の外部監査人の意見、制御の有効性に関する AWS マネジメントからの表明、AWS インフラストラクチャおよびサービスの概要が含まれます。AWS SOC 3 レポートには、対象サービスをサポートする目標のサービスをサポートする世界中の AWS データセンターすべてを含みます。これは SOC 2 レポートを請求する手続きを踏まなくとも、AWS が外部監査人の保証を得ていることを確認できる便利な資料です。SOC 3 レポートの範囲には、SOC 1 レポートの対象と同じサービスが含まれます。対象となるサービスの詳細については上記の SOC 1 の説明を参照してください。AWS SOC 3 レポートはこちらからご覧ください。

コンプライアンスに関するその他のベストプラクティス

柔軟性を特徴とし、お客様によるコントロールが可能な AWS プラットフォームでは、業界特有のコンプライアンス要件に合わせたソリューションのデプロイが可能です。

- ***CSA***:AWS はクラウドセキュリティアライアンス（CSA）の「Consensus Assessments Initiative Questionnaire (CAIQ)」に回答済みです。CSA が発行するこの調査票は、どのようなセキュリティ統制が AWS の IaaS (Infrastructure as a Service) サービス内に存在するかを文書化する手段の 1 つとなっています。調査票（CAIQ）には、クラウド使用者およびクラウド監査人がクラウドプロバイダに尋ねる可能性がある 140 以上の質問が記載されています。AWS が回答した「CSA Consensus Assessments Initiative Questionnaire」については、この文書の付録 A を参照してください。
- ***MPAA***:アメリカ映画協会（MPAA）は、保護されたメディアとコンテンツを安全に保存、処理、配給するための一連のベストプラクティスをまとめました（http://www.fightfilmtheft.org/facility-security-program.html）。メディア企業ではこのベストプラクティスを、コンテンツとインフラストラクチャのリスクとセキュリティを評価する手段として使用しています。AWS は MPAA のベストプラクティスに準拠していることが実証されており、AWS のインフラストラクチャはすべての適用可能な MPAA インフラストラクチャコントロールに準拠しています。MPAA は「証明書」を提供していませんが、メディア業界のお客様は AWS の MPAA 型コンテンツのリスク査定および評価を補足する AWS MPAA 文書を使用することができます。米国映画協会（MPAA）コンテンツセキュリティモデルに対する AWS の準拠状況については、この文書の付録 B を参照してください。

コンプライアンスに関するよくある質問と AWS

ここでは、クラウドコンピューティングのコンプライアンスに関してよくある質問と、それに対する AWS の回答を掲載します。一般的なコンプライアンスの問題の中には、クラウドコンピューティング環境で評価および運用するとき関係するものや、AWS のお客様の統制管理の取り組みに役立つものがあります。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
1	統制の所有権。クラウドにデプロイしたインフラストラクチャを統制する所有権は誰にありますか?	AWS にデプロイされている部分については、AWS がそのテクノロジの物理コンポーネントを統制します。その他の部分は、接続ポイントや送信の統制を含め、お客様がすべてを所有し、統制します。AWS で定めている統制の内容と、効率的に運用する方法について理解できるように、AWS では SOC 1 Type II レポートを発行し、EC2、S3、VPC を中心とした定義済みの統制、ならびに詳細な物理セキュリティおよび環境統制を公表しています。これらの統制の定義は、ほとんどのお客様のニーズを満たします。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。
2	IT の監査。クラウドプロバイダの監査はどのように実施すればよいですか?	ほとんどのレイヤーと、物理統制よりも上の統制の監査は、お客様の担当です。AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート（SSAE 16）に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。
3	Sarbanes-Oxley への準拠。対象のシステムがクラウドプロバイダ環境にデプロイされている場合、SOX への準拠はどのように達成されますか?	お客様が AWS クラウドで会計情報を処理する場合、AWS システムの一部を Sarbanes-Oxley (SOX) の要件の範囲に組み込むことについては、お客様の監査人が判断してください。お客様の監査人は、SOX の適用可能性について独自に判断する必要があります。ほとんどの論理アクセス統制はお客様が管理するため、関連する基準に統制活動が適合しているかどうかは、お客様が判断されるのが最適です。 SOX 監査人が AWS の物理的統制に関する詳細情報を必要とする場合は、AWS の SOC 1 Type II レポートを参照できます。AWS が提供する統制が詳細に記載されています。
4	HIPAA への準拠。クラウドプロバイダ環境にデプロイしている場合でも、HIPAA のコンプライアンス要件を満たすことができますか?	HIPAA 要件は AWS のお客様に適用され、AWS のお客様が統制します。AWS プラットフォームでは、HIPAA などの業界固有の認定要件を満たすソリューションのデプロイが可能です。お客様は AWS のサービスを利用することで、電子健康記録を保護するために必要な要件以上のセキュリティレベルを維持できます。HIPAA のセキュリティおよびプライバシーに関する規則に準拠したヘルスケアアプリケーションが、お客様によって AWS で構築されています。AWS のウェブサイトには、このトピックに関するホワイトペーパーなど、HIPAA への準拠に関する追加情報が掲載されています。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
5	GLBA への準拠。クラウドプロバイダ環境にデプロイしている場合でも、GLBA の認定要件を満たすことができますか?	ほとんどの GLBA 要件は、AWS のお客様が統制します。AWS は、データの保護、アクセス許可の管理、および AWS インフラストラクチャでの GLBA 準拠アプリケーションの構築をお客様が行うための手段を提供しています。物理セキュリティ統制が効率的に運用されている具体的な保証が必要な場合は、必要に応じて AWS SOC 1 Type II レポートを参照できます。
6	米国連邦規制への準拠。米国政府機関がクラウドプロバイダ環境にデプロイしている場合に、セキュリティおよびプライバシーの規制に準拠することはできますか?	米国連邦機関は、2002 年施行の連邦情報セキュリティマネジメント法（FISMA）、Federal Risk and Authorization Management Program (FedRAMP[sm])、Federal Information Processing Standard (FIPS) 出版物 140-2、武器規制国際交渉規則（ITAR）など、数多くのコンプライアンス基準に準拠することができます。また、該当する法律に規定されている要件に応じて、他の法律や状況への準拠も達成できる場合があります。
7	データの場所。ユーザーデータはどこにありますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。S3 データオブジェクトのデータレプリケーションは、データが保存されているリージョンのクラスタ内で実行され、他のリージョンの他のデータセンタークラスタにはレプリケートされません。データとサーバを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法令遵守または政府機関の要請によりやむをえない場合を除き、お客様のコンテンツを指定されたリージョンからお客様への通告なしに移動することはありません。本文書の執筆時点では、リージョンは 9 つあります。米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）（オレゴン）、欧州（アイルランド）、アジアパシフィック（シンガポール）、アジアパシフィック（東京）、アジアパシフィック（シドニー）、南米（サンパウロ）です。
8	E-Discovery。クラウドプロバイダは、電子的な検出手順および要件を満たすというユーザーのニーズを満たしていますか?	AWS はインフラストラクチャを提供し、その他の部分はお客様が管理します。例えば、オペレーティングシステム、ネットワーク構成、インストールされているアプリケーションなどです。お客様は、AWS を使用して保存または処理する電子文書の特定、収集、処理、分析、および作成に関連する法的手続きに、適切に対応する責任を持ちます。法的手続きに AWS の協力を必要とするお客様には、AWS は要請に応じて連携をとります。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
9	データセンター訪問。クラウドプロバイダでは、ユーザーによるデータセンター訪問を許可していますか?	いいえ。AWS のデータセンターは複数のお客様をホストしており、幅広いお客様が第三者による物理的なアクセスの対象となるため、お客様によるデータセンター訪問は許可していません。このようなお客様のニーズを満たすために、SOC 1 Type II レポート（SSAE 16）の一環として、独立し、資格を持つ監査人が統制の有無と運用を検証しています。この広く受け入れられているサードパーティによる検証によって、お客様は実行されている統制の効果について独立した観点を得ることができます。AWS と機密保持契約を結んでいる AWS のお客様は、SOC 1 Type II レポートのコピーを要求できます。データセンターの物理的なセキュリティの個別の確認も、ISO 27001 監査、PCI 評価、ITAR 監査、FedRAMP[sm] テストプログラムの一部となっています。
10	サードパーティのアクセス。サードパーティは、クラウドプロバイダデータセンターにアクセスできますか?	AWS は、AWS 従業員であっても、データセンターへのアクセスを厳密に統制しています。第三者による AWS データセンターへのアクセスは、AWS アクセスポリシーに従って適切な AWS データセンターマネージャーによって明示的に許可されない限り、実施されません。物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type II レポートを参照してください。
11	特権的アクション。特権的アクションは監視および統制されていますか?	所定の統制によってシステムおよびデータのアクセスを制限し、システムまたはデータに対するアクセスを制限および監視できるようにしています。さらに、お客様のデータおよびサーバーインスタンスは、デフォルトで他のお客様とは論理的に隔離されています。特権のあるユーザーアクセス制御は、AWS SOC 1、ISO 27001、PCI、ITAR、および FedRAMP[sm] の監査中に独立監査人によって確認されます。
12	内部者によるアクセス。クラウドプロバイダは、ユーザーのデータとアプリケーションに対する内部者による不適切なアクセスの脅威に対処していますか?	AWS は、内部者による不適切なアクセスの脅威に対処するための SOC 1 統制を提供しています。また、本文書で説明している公開認定およびコンプライアンスの取り組みにより、内部者によるアクセスに対処しています。すべての認定とサードパーティによる証明で、論理アクセスの予防統制と検出統制が評価されています。さらに、定期的なリスク評価時に、内部者によるアクセスの統制および監視方法を評価しています。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
13	マルチテナント。ユーザーの分離は安全に実施されていますか?	AWS 環境は仮想化されたマルチテナント環境です。AWS は、お客様間を他のお客様から隔離するように設計されたセキュリティ管理プロセス、PCI 統制などのセキュリティ統制を実施しました。AWS システムは、仮想化ソフトウェアによるフィルタ処理によって、お客様に割り当てられていない物理ホストや物理インスタンスにアクセスできないように設計されています。このアーキテクチャは独立 PCI 認定審査機関（QSA） によって検証済みで、2013 年 11 月に発行された PCI DSS 3.0 版のすべての要件に準拠することが確認されています。 また、AWS にはシングルテナントのオプションもあります。専用インスタンスは、単一のお客様専用のハードウェアを実行する Amazon Virtual Private Cloud (Amazon VPC) で起動される Amazon EC2 インスタンスです。専用インスタンスを使用することで、Amazon VPC および AWS クラウドの利点をフルに活用しながら、Amazon EC2 インスタンスをハードウェアレベルで隔離できます。
14	ハイパーバイザの脆弱性。クラウドプロバイダは、ハイパーバイザの既知の脆弱性に対処していますか?	現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザを利用しています。ハイパーバイザは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。Xen ハイパーバイザおよびインスタンスの隔離の詳細については、AWS セキュリティホワイトペーパーをご覧ください。
15	脆弱性の管理。システムには適切にパッチが適用されていますか?	AWS は、ハイパーバイザおよびネットワーキングサービスなど、お客様へのサービス提供をサポートするシステムにパッチを適用する責任を持ちます。この処理は、AWS ポリシーに従い、また ISO 27001、NIST、および PCI の要件に準拠して、必要に応じて実行します。お客様が使用しているゲストオペレーティングシステム、ソフトウェア、およびアプリケーションの統制については、お客様が行い、お客様がそれらのシステムにパッチを適用する責任を持ちます。
16	暗号化。提供されているサービスは暗号化をサポートしていますか?	はい。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティの暗号化テクノロジを使用することもできます。詳細については、AWS セキュリティホワイトペーパーを参照してください。
17	データの所有権。クラウドプロバイダのユーザーデータに対する権利はどのようなものですか?	AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
18	データの隔離。クラウドプロバイダはユーザーデータを適切に隔離していますか?	AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。Amazon S3 は高度なデータアクセス統制を提供しています。具体的なデータサービスのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
19	複合サービス。クラウドプロバイダのサービスは、他のプロバイダのクラウドサービスをベースに利用していますか?	AWS はお客様に AWS サービスを提供するにあたり、サードパーティのクラウドプロバイダは一切使用していません。
20	物理統制と環境統制。これらの統制は、指定したクラウドプロバイダによって運営されていますか?	はい。これらの統制は、SOC 1 Type II レポートに具体的に記載されています。さらに、ISO 27001 や FedRAMP[sm] など、AWS がサポートするその他の認証では、ベストプラクティスの物理統制や環境統制が必要です。
21	クライアント側の保護。クラウドプロバイダでは、PC や携帯機器などのクライアントからのアクセスをユーザーが保護および管理できますか?	はい。AWS では、お客様の要件に合わせて、お客様がクライアントおよびモバイルアプリケーションを管理できます。
22	サーバーのセキュリティ。クラウドプロバイダでは、仮想サーバーをユーザーが保護できますか?	はい。AWS では、お客様独自のセキュリティアーキテクチャを実装できます。サーバーおよびネットワークのセキュリティの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
23	Identity and Access Management。サービスに IAM 機能は含まれますか?	AWS には Identity and Access Management (IAM) サービスシリーズがあるので、お客様は、ユーザー ID の管理、セキュリティ認証情報の割り当て、ユーザーのグループ化による整理、およびユーザーのアクセス許可の管理を一元的に行うことができます。詳細については、AWS ウェブサイトをご覧ください。
24	保守による停止の予定。プロバイダは、保守のためにシステムを停止する予定を指定していますか?	AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要がありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。インスタンスの保守自体は、お客様が統制します。
25	拡張機能。ユーザーが元々の契約を超えて拡張することを許可していますか?	AWS クラウドは分散され、セキュリティと復元力が高いので、潜在的に大きな拡張性があります。お客様は、使用内容に対する料金のみを支払って、拡張または縮小できます。
26	サービスの可用性。高レベルの可用性を確約していますか?	AWS は、サービスレベルアグリーメント（SLA）で高レベルの可用性を確約しています。例えば、Amazon EC2 は、1 年のサービス期間で 99.95% 以上の稼働時間を確約しています。Amazon S3 は毎月 99.9% 以上の稼働時間を確約しています。こうした可用性の評価指標が基準に満たない場合は、サービスクレジットが提供されます。

参照番号	クラウドコンピューティングに関する質問	AWS の情報
27	分散型サービス妨害（DDoS）攻撃。DDoS 攻撃に対してサービスをどのように保護していますか?	AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。DDoS 攻撃の説明などの詳細については、AWS セキュリティホワイトペーパーをご覧ください。
28	データの可搬性。サービスプロバイダに保存されているデータは、ユーザーが依頼すればエクスポートできますか?	AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。
29	サービスプロバイダのビジネス継続性。ビジネス継続性プログラムがありますか?	AWS では、ビジネス継続性プログラムを運用しています。詳細な情報については、AWS セキュリティホワイトペーパーをご覧ください。
30	ユーザーのビジネス継続性。ユーザーがビジネス継続性計画を実装することはできますか?	AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。例えば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。
31	データの耐久性。サービスでは、データの耐久性を規定していますか?	Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトの 99.999999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。
32	バックアップ。サービスで、テープへのバックアップサービスを提供していますか?	AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。
33	値上げ。突然値上げを行うことがありますか?	AWS には、サービス提供のコストが徐々に下がるにつれて、料金を頻繁に下げてきた歴史があります。ここ数年間でも、継続的に値下げを行っています。
34	持続可能性。サービスプロバイダ会社には、長期間の持続可能性がありますか?	AWS はトップクラスのクラウドプロバイダであり、Amazon.com の長期ビジネス戦略です。AWS には、非常に長期間の持続可能性があります。

AWS へのお問い合わせ

AWS の独立監査人が発行したレポートや証明書の取り寄せ、または AWS のコンプライアンスの詳細についてのご質問は、AWS 営業・事業開発部にお問い合わせください。お問い合わせ内容に応じて適切なチームに取り次ぎいたします。AWS のコンプライアンスの詳細については、AWS コンプライアンスサイトを参照するか、awscompliance@amazon.com まで直接ご質問をお送りください。

付録 A:CSA Consensus Assessments Initiative Questionnaire v1.1

クラウドセキュリティアライアンス（Cloud Security Alliance/CSA）は、「クラウドコンピューティング内の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して、あらゆる形式のコンピューティングの保護を支援する目的を持つ非営利組織」です。[参照先: https://cloudsecurityalliance.org/about/] この目標を達成するために、幅広い業界のセキュリティの専門家、会社、および団体がこの組織に参加しています。

CSA Consensus Assessments Initiative Questionnaire には、クラウド使用者およびクラウド監査人がクラウドプロバイダに要求すると CSA が想定している質問が記載されています。また、セキュリティ、統制、およびプロセスに関する一連の質問も記載されています。この質問は、クラウドプロバイダの選択やセキュリティの評価など、幅広い用途に使用できます。AWS はこの調査票に回答済みです。内容は以下のとおりです。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
コンプライアンス	監査の計画	CO-01.1	構造化された、業界で受け入れられている形式（CloudAudit/A6 URI Ontology、CloudTrust、SCAP/CYBEX、GRC XML、ISACA の Cloud Computing Management Audit/Assurance Program など）を使用して、監査要点を作成していますか?	AWS は、いくつかの業界の認定と独立したサードパーティによる証明を取得し、いくつかの認定、レポートなどの関連する文書を、NDA に従って AWS のお客様に直接提供しています。
コンプライアンス	独立監査	CO-02.1	テナントに対して、自社の SAS70 Type II/SSAE 16 SOC2/ISAE3402 または同様のサードパーティ監査レポートを見ることを許可していますか?	AWS は、サードパーティによる証明、認定、 Service Organization Controls 1 (SOC 1) Type II レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。 さらに、AWS 統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。
コンプライアンス		CO-02.2	業界のベストプラクティスおよび指針に従い、クラウドサービスインフラストラクチャのネットワーク侵入テストを定期的に実行していますか?	
コンプライアンス		CO-02.3	業界のベストプラクティスおよび指針に従い、クラウドインフラストラクチャのアプリケーション侵入テストを定期的に実行していますか?	
コンプライアンス		CO-02.4	業界のベストプラクティスおよび指針に従い、内部監査を定期的に実行していますか?	
コンプライアンス		CO-02.5	業界のベストプラクティスおよび指針に従い、外部監査を定期的に実行していますか?	
コンプライアンス		CO-02.6	ネットワーク侵入テストの結果は、必要に応じてテナントが利用できるようにしていますか?	
コンプライアンス		CO-02.7	内部監査および外部参加の結果は、必要に応じてテナントが利用できるようにしていますか?	
コンプライアンス	サードパーティ監査	CO-03.1	テナントに対して、独立した脆弱性評価の実行を許可していますか?	対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様は

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
コンプライアンス		CO-03.2	自社のアプリケーションとネットワークに対して、脆弱性スキャンと定期的な侵入テストを実行する外部のサードパーティはありますか?	ご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性／侵入テストリクエストフォームを使用してリクエストを送信してください。 AWS Security は、外部の脆弱性脅威評価を実行するために、独立したセキュリティ会社と定期的に契約しています。AWS が実施している具体的な統制活動に関する詳細については、AWS SOC 1 Type II レポートに記載されています。
コンプライアンス	各機関との関係と接点の維持	CO-04.1	規定と該当する規制に従って、地元機関との連絡窓口と接点を維持していますか?	AWS は、ISO 27001 基準の要件に従い、業界団体、リスクおよびコンプライアンス組織、地元機関、および規制団体との接点を維持しています。
コンプライアンス	情報システムの規制マッピング	CO-05.1	顧客データを論理的にセグメント化または暗号化することで、別のテナントのデータに不注意でアクセスすることなく単一のテナントに対してのみデータを作成することができますか?	AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているので、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、 AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。
		CO-05.2	データを論理的にセグメント化し、障害またはデータ損失が発生した場合に特定の顧客のデータを回復することができますか?	
コンプライアンス	知的財産	CO-06.1	テナントの知的財産を保護するために実施している統制内容が記載されているポリシーまたは手続きがありますか?	AWS のコンプライアンスおよびセキュリティチームが、情報および関連技術のための統制目標（COBIT）フレームワークに基づく情報セキュリティフレームワークとポリシーを制定しています。AWS セキュリティフレームワークは、ISO 27002 ベストプラクティスおよび PCI データセキュリティ基準を統合しています。 詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。
コンプライアンス	知的財産	CO-07.1	クラウドプロバイダの利益のために、クラウドで提供しているテナントサービスの利用状況のデータマイニングを行う場合、テナントの IP 権利は維持されますか?	リソースの利用状況は、サービスの可用性を効率的に管理するために、必要に応じて AWS によって監視されています。AWS は、リソース利用状況監視の一環として、お客様の知的財産を収集することはありません。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
コンプライアンス	知的財産	CO-08.1	クラウドプロバイダの利益のために、クラウドで提供しているテナントサービスの利用状況のデータマイニングを行う場合、テナントに対して拒否する選択肢を与えていますか?	クラウドで提供しているユーザーサービスの利用状況について、データマイニングは実行していません。
データ管理	所有権および財産管理	DG-01.1	構造化データラベリング基準（ISO 15489、Oasis XML Catalog Specification、CSA データタイプガイダンスなど）に従っていますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様の要件に合う構造化データラベリング基準を実装することができます。
データ管理	分類	DG-02.1	ポリシータグやメタデータを介して仮想マシンを識別する機能を提供していますか（例えば、タグを使用して、ゲストオペレーティングシステムが不適切な国で起動、データのインスタンス化、データの転送を実行しないように制限することなどができますか）?	仮想マシンは、EC2 サービスの一部としてお客様に割り当てられています。お客様は、使用されるリソースとリソースの場所に関する統制を有しています。詳細については、AWS のウェブサイト（http://aws.amazon.com）を参照してください。
データ管理		DG-02.2	ポリシータグ、メタデータ、ハードウェアタグを介してハードウェアを識別する機能を提供していますか（例えば、TXT/TPM、VN-Tag など）?	AWS は、EC2 リソースにタグを設定する機能を提供しています。メタデータの 1 形式である EC2 タグは、ユーザーが親しみやすい名前の作成、検索性の強化、および複数ユーザー間の協調の改善に使用できます。また、AWS マネジメントコンソールは、タギングもサポートしています。
データ管理		DG-02.3	1 つの認証要素としてシステムの地理的位置を使用する機能はありますか?	AWS は、IP アドレスに基づく条件付きユーザーアクセスの機能を提供しています。お客様は条件を追加して、時刻、その発信元の IP アドレス、SSL を使用するかどうかなど、ユーザーがどのように AWS を使用するかをコントロールできます。
データ管理		DG-02.4	依頼に応じて、テナントのデータが格納されている場所の物理的な位置または地理を提供していますか?	AWS は、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 9 つありま す。米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）（オレゴン）、欧州（アイルランド）、アジアパシフィック（シンガポール）、アジアパシフィック（東京）、アジアパシフィック（シドニー）、南米（サンパウロ）です。
データ管理		DG-02.5	テナントに対して、データルーティングまたはリソースインスタンス化の許容可能な地理的位置を定義することを許可していますか?	
データ管理	処理、ラベリング、セキュリティポリシー	DG-03.1	データおよびデータを含むオブジェクトのラベリング、処理、およびセキュリティに関するポリシーおよび手続きが規定されていますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様は、お客様の要件に合うラベリングおよび処理に関するポリシーおよび手続きを実装できます。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
データ管理		DG-03.2	データの集約コンテナとして機能するオブジェクトのために、ラベル継承のメカニズムは実装されていますか?	
データ管理	保持ポリシー	DG-04.1	テナントデータの保持ポリシーを実施するための技術的な統制機能はありますか?	AWS は、お客様に対して、お客様のデータを削除する機能を提供しています。ただし、AWS のお客様は、お客様のデータの統制と所有権を有していますので、お客様の要件に応じてデータの保持を管理するのはお客様の責任です。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。 AWS はお客様のプライバシー保護を慎重に考慮し、AWS が準拠する必要がある法的処置の要求についても注意深く判断しています。AWS は、法的処置による命令に確実な根拠がないと判断した場合は、その命令にためらわずに異議を申し立てます。
データ管理		DG-04.2	政府またはサードパーティからテナントデータに関する依頼を受けた場合の対応手順は文書化されていますか?	
データ管理	安全な廃棄	DG-05.1	テナントの決定による、アーカイブされているデータの安全な削除（消磁や暗号ワイプ処理など）をサポートしていますか?	AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
データ管理		DG-05.2	サービス手配の終了に関する手順を公開できますか?例えば、顧客が環境の利用を終了した場合やリソースを無効にした場合に、テナントデータのコンピューティングリソースすべてを消去する保証などです。	
データ管理	非運用データ	DG-06.1	運用データが非運用環境にレプリケートされたり、使用されたりすることを禁止する手順がありますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。AWS は、お客様が運用環境および非運用環境を保守および開発できるようにしています。運用データが非運用環境にレプリケートされないようにするのは、お客様の責任です。
データ管理	情報漏洩	DG-07.1	マルチテナント環境で、テナント間のデータ漏洩、意図的または予想外の情報漏洩を回避するための統制は用意されていますか?	AWS 環境は仮想化されたマルチテナント環境です。AWS は、お客様間を他のお客様から隔離するように設計されたセキュリティ管理プロセス、PCI 統制などのセキュリティ統制を実施しました。AWS システムは、仮想化ソフトウェアによるフィルタ処理によっ

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
データ管理		DG-07.2	自社のクラウドサービス提供とインターフェースを持つすべてのシステムについて、データ損失防止（Data Loss Prevention/DLP）または漏洩防止ソリューションが用意されていますか?	て、お客様に割り当てられていない物理ホストや物理インスタンスにアクセスできないように設計されています。このアーキテクチャは独立 PCI 認定審査機関（QSA）によって検証済みで、2013 年 11 月に発行された PCI DSS 3.0 版のすべての要件に準拠することが確認されています。 詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
データ管理	リスク評価	DG-08.1	テナントが業界標準の連続モニタリングを実装できるように、セキュリティ統制ヘルスデータを提供していますか（連続モニタリングによって、物理的および論理的統制ステータスの連続的なテナントの検証が可能になりますか）?	AWS は、独立監査人のレポートと認定を発行して、AWS が規定し、運用しているポリシー、プロセス、および統制に関する大量の情報をお客様に提供しています。関連する認定とレポートを AWS のお客様に提供できます。 論理的統制の連続モニタリングは、お客様がお客様のシステムで実行できます。
施設のセキュリティ	ポリシー	FS-01.1	オフィス、部屋、施設、および保護エリアに、安全でセキュアな作業環境を維持するためのポリシーと手続きが規定されている証拠を提示できますか?	AWS は、外部の認定機関および独立監査人と連携し、コンプライアンスフレームワークへの準拠を確認および検証しています。AWS SOC 1 Type II レポートには、AWS が実行している具体的な物理的セキュリティ統制活動に関する詳細情報が記載されています。詳細については、ISO 27001 規格の附属書 A、ドメイン 9.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
施設のセキュリティ	ユーザーアクセス	FS-02.1	経歴検証の対象となるすべての従業員候補、請負業者、およびサードパーティは、現地の法律、規制、倫理、および契約の制限に準拠していますか?	AWS は、適用法令の許容範囲で、従業員の雇用前審査の一環として、その従業員の役職や AWS 施設へのアクセスレベルに応じた犯罪歴の確認を行っています。
施設のセキュリティ	統制されたアクセスポイント	FS-03.1	物理的なセキュリティ境界（フェンス、壁、障壁、守衛、ゲート、電子監視、物理的認証メカニズム、受付、および保安巡回）は実装されていますか?	物理的セキュリティ統制には、フェンス、壁、保安スタッフ、監視カメラ、侵入検知システム、その他の電子的手段などの境界統制が含まれますが、それに限定されるものではありません。AWS が実施している具体的な統制活動に関する詳細については、AWS SOC 1 Type II レポートに記載されています。詳細については、ISO 27001 規格の附属書 A、ドメイン 9.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
施設のセキュリティ	保護エリアの承認	FS-04.1	テナントに対して、（データが保存されている場所とアクセスされる場所に基づく法的管轄に対応するために）データを移動できる地理的位置を指定することを許可していますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。本文書の執筆時点では、リージョンは 9 つあります。米国東部（バージニア北部）、米国西部（オレゴン）、米国西部（北カリフォルニア）、AWS GovCloud（米国）（オレゴン）、欧州（アイルランド）、アジアパシフィック（シンガポール）、アジアパシフィック（東京）、アジアパシフィック（シドニー）、南米（サンパウロ）です。詳細については、AWS のウェブサイト（http://aws.amazon.com for additional details）を参照してください。
施設のセキュリティ	権限のない個人の入場	FS-05.1	権限のない個人が監視対象の建物に入ることができるサービスエリアのようなポイントの入口および出口は、統制され、データの保存およびプロセスから隔離されていますか?	ビデオ監視カメラ、最新鋭の侵入検出システム、その他エレクトロニクスを使った手段を用いて、専門のセキュリティスタッフが、建物の入口とその周辺両方において、物理的アクセスを厳密に管理しています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。また、AWS SOC 1 Type II レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。
施設のセキュリティ	オフサイトの承認	FS-06.1	データの物理的位置を移動できる場合のシナリオを説明する文書を、テナントに提供していますか?（例:オフサイトバックアップ、ビジネス継続性のフェイルオーバー、レプリケーション）	AWS のお客様は、データを保存する物理的リージョンを指定できます。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。 詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
施設のセキュリティ	オフサイトの設備	FS-07.1	資産管理と設備の用途変更について規定するポリシーと手続きを説明する文書を、テナントに提供していますか?	ISO 27001 基準に合わせて、AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。 詳細については、ISO 27001 規格の附属書 A、ドメイン 9.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
施設のセキュリティ	資産管理	FS-08.1	資産の所有権を含めて、すべての重要資産の一覧表を保守していますか?	ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 詳細については、ISO 27001 規格の附属書 A、ドメイン 7.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
施設のセキュリティ		FS-08.2	重要なサプライヤとの関係のすべてについて、一覧表を保守していますか?	
人事のセキュリティ	経歴の審査	HR-01.1	経歴検証の対象となるすべての従業員候補、請負業者、およびサードパーティは、現地の法律、規制、倫理、および契約の制限に準拠していますか?	AWS は従業員に対し、その従業員の役職や AWS 施設へのアクセスレベルに応じて、適用法令が認める範囲で、雇用前審査の一環として犯罪歴の確認を行います。 詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
人事のセキュリティ	雇用契約	HR-02.1	情報セキュリティ統制を提供するときの従業員の役割とテナントの役割に関して、従業員を特別にトレーニングしていますか?	すべての従業員は、AWS の業務行動と倫理行動に関する規範を提供され、修了時に承認を必要とする情報セキュリティトレーニングを定期的に受けています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的に実施しています。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
		HR-02.2	従業員が修了したトレーニングの承認を文書にしていますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
人事のセキュリティ	雇用終了	HR-03.1	雇用終了または雇用手続きの変更に伴う役職と責任の割り当て、文書化、および相談は行われていますか?	AWS の人事チームは、従業員およびベンダーの終了および役職の変更のために従う必要がある内部管理責任を定義しています。従業員や契約社員のアクセス権付与/解除の責任は、人事（HR）、企業運用サービス事業主によって分担されます。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ	管理プログラム	IS-01.1	自社の情報セキュリティ管理プログラム（Information Security Management Program/ISMP）について説明する文書を、テナントに提供していますか?	AWS は、AWS ISMS プログラムとやり取りするお客様に、ISO 27001 認定文書を提供しています。
情報セキュリティ	管理のサポートおよびかかわり	IS-02.1	役員およびライン管理が、割り当て実行の際にわかりやすい文書の指示、責任、明確な割り当てと検証によって、情報セキュリティに対応する正規の行動を確実に実行するためのポリシーは用意されていますか?	AWS Information Security ワークによって、ISO 27001 基準に合わせてポリシーと手続きが規定されています。Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。
情報セキュリティ	ポリシー	IS-03.1	情報セキュリティおよびプライバシーポリシーは、特定の業界基準（ISO-27001、ISO-22307、CoBIT など）に準拠していますか?	AWS Information Security は、COBIT フレームワーク、ISO 27001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。さらに、AWS は SOC 1 Type II レポートを発行しています。詳細については、SOC 1 レポートを参照してください。詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
		IS-03.2	プロバイダが情報セキュリティおよびプライバシーポリシーに準拠するための契約は行っていますか?	
		IS-03.3	自社の統制、アーキテクチャ、およびプロセスと、規制および基準を適切に配慮して対応付けていることを示す証拠を提供できますか?	
情報セキュリティ	基礎の要件	IS-04.1	インフラストラクチャのすべてのコンポーネント（ハイパーバイザ、オペレーティングシステム、ルーター、DNS サーバーなど）について、情報セキュリティの基礎を文書化していますか?	AWS は、ISO 27001 基準に合わせて重要なコンポーネントのシステムの基礎を保守しています。詳細については、ISO 27001 規格の附属書 A、ドメイン 12.1 および 15.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 お客様は、お客様の仮想マシンイメージを提供できます。VM Import を使うと、既存の環境から Amazon EC2 インスタンスに仮想マシンのイメージを簡単にインポートできます。
情報セキュリティ		IS-04.2	情報セキュリティの基礎に対するインフラストラクチャの準拠について、継続的に監視およびレポートすることはできますか?	
情報セキュリティ		IS-04.3	顧客が、顧客の内部基準に準拠するために、顧客の信頼できる仮想マシンイメージを提供することを許可していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ	ポリシーのレビュー	IS-05.1	情報セキュリティまたはプライバシーポリシーに重要な変更を加える場合、テナントに通知していますか?	http://aws.amazon.com/security で入手できる「AWS Overview of Security Processes Whitepaper」および「Risk and Compliance Whitepaper」は、AWS ポリシーの更新を反映して定期的に更新されています。
情報セキュリティ	ポリシーの実施	IS-06.1	セキュリティポリシーおよび手続きに違反した従業員に対して、正規の懲戒または制裁ポリシーは規定されていますか?	AWS は、従業員にセキュリティポリシーを提供し、セキュリティトレーニングを提供することで、情報セキュリティに関する役割と責任について教育しています。Amazon の基準またはプロトコルに違反した従業員は調査され、適切な懲戒（警告、業績計画、停職、解雇など）が実施されます。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 8.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-06.2	ポリシーや手続きに違反した場合にとられる対応について従業員に意識させ、その対応内容をポリシーや手続きに記載していますか?	
情報セキュリティ	ユーザーアクセスポリシー	IS-07.1	ビジネスの目的に必要なくなったシステムアクセス権を適時に削除する統制は用意されていますか?	従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。そうでない場合、アクセス権は自動的に取り消されます。AWS SOC 1 Type II レポートには、ユーザーアクセスの失効の詳細情報が記載されています。また、詳細については、「AWS Security Whitepaper」の「Employee Lifecycle」を参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-07.2	ビジネスの目的で不要になったシステムアクセス権を削除できる速度を追跡するメトリックスを用意していますか?	
情報セキュリティ	ユーザーアクセスの制限および承認	IS-08.1	テナントデータに対するアクセス権を付与および承認する方法を文書化していますか?	AWS のお客様は、お客様のデータの統制と所有権を保持します。お客様のコンテンツの開発、コンテンツ、運用、維持、および使用

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ		IS-08.2	アクセス制御目的のためのプロバイダとテナントのデータ分類手法を調整する方法を持っていますか?	については、お客様が責任を負うものとします。
情報セキュリティ	ユーザーアクセスの失効	IS-09.1	営業員、請負業者、顧客、ビジネスパートナー、またはサードパーティの状況の変化に応じて、組織のシステム、情報資産、およびデータに対するユーザーアクセス権の解除、失効、または変更が適時に行われていますか?	従業員の記録が Amazon のヒューマンリソースシステムから削除されると、アクセス権は自動的に取り消されます。従業員の役職に変化が生じる場合、リソースに対するアクセスの継続が明示的に承認される必要があります。そうでない場合、アクセス権は自動的に取り消されます。AWS SOC 1 Type II レポートには、ユーザーアクセスの失効の詳細情報が記載されています。また、詳細については、「AWS Security Whitepaper」の「Employee Lifecycle」を参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 11 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-09.2	状況の変化には、雇用、協定、または契約の終了、雇用の変更、または組織内の異動が含まれていますか?	
情報セキュリティ	ユーザーアクセスのレビュー	IS-10.1	すべてのシステムユーザーおよび管理者（テナントが保守しているユーザーを除く）の資格認定を少なくとも 1 年に 1 度必須としていますか?	ISO 27001 基準に合わせて、すべてのアクセス権付与は 90 日ごとに確認されており、明示的な再承認を必須としています。承認しないと、リソースへのアクセスは自動的に失効されます。ユーザーアクセス権の確認に固有の統制については、SOC 1 Type II レポートに概要が記載されています。ユーザー資格の統制の例外については、SOC 1 Type II レポートに記載されています。 詳細については、ISO 27001 規格の附属書 A、ドメイン 11.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-10.2	ユーザーの資格が不適切であると判明した場合、すべての修正および認定行動は記録されますか?	
情報セキュリティ		IS-10.3	テナントデータに対して不適切なアクセスが許可されていた場合、ユーザー資格の修正および認定レポートをテナントと共有しますか?	
情報セキュリティ	トレーニングおよび意識	IS-11.1	テナントデータに対するアクセス権を持つすべての個人に対して、クラウド関連のアクセスおよびデータ管理の問題（マルチテナント、国籍、クラウドデリバリーモデルの役割分担、利害衝突など）に関する正規のセキュリティ意識トレーニングプログラムを提供するか、利用できるようにしていますか?	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。作成したポリシーを従業員が理解し、従っていることを検証するために、コンプライアンス監査が定期的に実施されます。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ		IS-11.2	管理者およびデータ管財人は、セキュリティおよびデータ完全性に関する自身の法的責任について、適切な教育をうけていますか?	
情報セキュリティ	業界の情報およびベンチマーク	IS-12.1	情報セキュリティに関連する業界グループおよび専門職団体に参加していますか?	AWS のコンプライアンスおよびセキュリティチームは、セキュリティに関連する業界グループおよび専門職サービスとの関係を維持しています。AWS は、COBIT フレームワークに基づいて情報セキュリティフレームワークおよびポリシーを規定し、ISO 27002 統制および PCI DSS に基づいて ISO 27001 に認定可能なフレームワークを統合しています。詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
		IS-12.2	自社のセキュリティ統制について、業界基準に合わせたベンチマーク検査を実行していますか?	
情報セキュリティ	ロールおよび責任	IS-13.1	自社の管理者の責任とテナントの責任をわかりやすく説明した役割の定義文書をテナントに提供していますか?	AWS の役割と責任、およびお客様の役割と責任の詳細については、「AWS Overview of Security Processes Whitepaper」および「AWS Risk and Compliance Whitepaper」を参照してください。これらのホワイトペーパーは http://aws.amazon.com/security で入手できます。
情報セキュリティ	管理の監視	IS-14.1	管理者は、自分の責任範囲に関連するセキュリティポリシー、手続き、および基準の意識および準拠を維持する責任を負っていますか?	Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。各従業員には当社の業務行動倫理規定が配布され、定期的なトレーニングを受けます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ	役割分担	IS-15.1	クラウドサービス内で役割分担を維持する方法に関する文書を、テナントに提供していますか?	お客様は、AWS リソースの役割分担を管理することができます。 AWS 社内では ISO 27001 規格に準拠した役割分担を行っています。詳細については、ISO 27001 基準の付録 A、ドメイン 10.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ	ユーザーの責任	IS-16.1	公開されているセキュリティポリシー、手続き、基準、適用可能な規制の要件に対する意識と準拠を維持するために、ユーザーに自身の責任について意識させていますか?	AWS は、様々な方法でグローバルレベルの内部コミュニケーションを実施することで、従業員が各自の役割と責任を理解することを手助けし、重要なイベントについて適時伝達しています。この方法には、新規に雇用した従業員に対するオリエンテーションおよびト

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ		IS-16.2	安全でセキュアな作業環境を維持する責任について、ユーザーに意識させていますか?	レーニングプログラムや、Amazon イントラネットを介した情報の電子メールメッセージおよび投稿が含まれます。ISO 27001 基準の付録 A、ドメイン 8.2 および 11.3 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。さらに、詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-16.3	設備を無人のままにする場合にセキュアな方法で行う責任について、ユーザーに意識させていますか?	
情報セキュリティ	ワークスペース	IS-17.1	データ管理ポリシーと手続きでは、関係者のテナントおよびサービスレベルの競合に対応していますか?	AWS データ管理ポリシーは、ISO 27001 基準に合わせて作成しています。ISO 27001 基準の付録 A、ドメイン 8.2 および 11.3 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。AWS SOC 1 Type II レポートには、AWS リソースに対する不正アクセスを防ぐために AWS が実行する特定の統制行動について、その他の詳細情報が記載されています。
情報セキュリティ		IS-17.2	データ管理ポリシーと手続きに、テナントデータに対する不正アクセスの不正監査またはソフトウェアの完全性機能が含まれていますか?	
情報セキュリティ		IS-17.3	仮想マシンの管理インフラストラクチャには、仮想マシンの構築および設定に対する変更を検出するための不正監査またはソフトウェアの完全性機能が含まれていますか?	
情報セキュリティ	暗号化	IS-18.1	テナントごとに一意の暗号化キーを作成できる機能はありますか?	AWS のお客様は、AWS のサーバー側暗号化サービスを利用しない場合、お客様独自の暗号化を管理しています。この場合、AWS はテナントごとに一意の暗号化キーを作成しています。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-18.2	テナントが生成した暗号化キーをサポートするか、テナントが公開キー証明書にアクセスすることなくデータを ID に暗号化することを許可していますか?（例えば、ID ベースの暗号化）?	
情報セキュリティ	暗号化キーの管理	IS-19.1	環境内の（ディスクまたはストレージに）保存されているテナントデータを暗号化していますか?	AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティの暗号化テクノロジを使用することもできます。AWS キー管理手続きは、ISO 27001 基準に合わせて作成しています。詳細については、ISO 27001 基準の付録 A、ドメイン 15.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-19.2	ネットワークおよびハイパーバイザインスタンス間のトランスポート時に、暗号化を利用してデータと仮想マシンイメージを保護していますか?	
情報セキュリティ		IS-19.3	テナントの代理で暗号化キーを管理することはできますか?	
情報セキュリティ		IS-19.4	キー管理手続きを維持していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ	脆弱性およびパッチ管理	IS-20.1	業界のベストプラクティスに従って、ネットワーク層の脆弱性スキャンを定期的に実行していますか?	お客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーションの統制を有しており、脆弱性スキャンを実行し、お客様のシステムにパッチを適用するのは、お客様の責任です。対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様はご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。AWS セキュリティは、すべてのインターネット向きサービスエンドポイントの IP アドレスの脆弱性を定期的にスキャンしています。判明した脆弱性があれば、修正するために適切な関係者に通知します。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 12.5 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-20.2	業界のベストプラクティスに従って、アプリケーション層の脆弱性スキャンを定期的に実行していますか?	
情報セキュリティ		IS-20.3	業界のベストプラクティスに従って、ローカルオペレーティングシステム層の脆弱性スキャンを定期的に実行していますか?	
情報セキュリティ		IS-20.4	脆弱性スキャンの結果を、依頼に応じてテナントに公開していますか?	
情報セキュリティ		IS-20.5	すべてのコンピューティングデバイス、アプリケーション、およびシステムに脆弱性のパッチを迅速に適用できますか?	
情報セキュリティ		IS-20.6	依頼に応じて、リスクに基づくシステムのパッチ適用期間をテナントに提供しますか?	
情報セキュリティ	ウイルス対策および悪意のあるソフトウェア対策	IS-21.1	クラウドサービス提供をサポートするすべてのシステムに、マルウェア対策プログラムがインストールされていますか?	ウイルス対策および悪意のあるソフトウェア対策に関する AWS のプログラム、プロセス、および手続きは、ISO 27001 基準に合わせています。詳細については、AWS SOC 1 Type II レポートを参照してください。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 10.4 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-21.2	署名、リスト、または動作パターンを使用するセキュリティ上の脅威検出システムは、業界で受け入れられている期間内にすべてのインフラストラクチャコンポーネントで更新されていますか?	
情報セキュリティ	障害管理	IS-22.1	文書化したセキュリティ事故対応計画がありますか?	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 規格に準拠して作成されています。AWS SOC 1 Type II レポートには、AWS が実施している具体的な統制活動の詳細が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-22.2	カスタマイズしたテナントの要件をセキュリティ事故対応計画に統合していますか?	
情報セキュリティ		IS-22.3	セキュリティ事故時の自社とテナントの責任内容を示した役割と責任の文書を発行していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ	障害のレポート	IS-23.1	より細かい分析と警告のために、セキュリティ情報およびイベント管理（security information and event management/SIEM）システムは、データソース（アプリケーションログ、ファイアウォールログ、IDS ログ、物理アクセスログなど）を結合していますか?	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 規格に準拠して作成されています。AWS SOC 1 Type II レポートには、AWS が実施している具体的な統制活動の詳細が記載されています。AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。 詳細については、「AWS Overview of Security Processes Whitepaper」および「AWS Risk & Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-23.2	ロギングおよびモニタリングフレームワークでは、特定のテナントに対する事故を分離できますか?	
情報セキュリティ	事故対応の法的準備	IS-24.1	事故対応計画は、法的に許容可能な保管の継続性の管理プロセスおよび統制の業界標準に準拠していますか?	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 規格に準拠して作成されています。AWS SOC 1 Type II レポートには、AWS が実施している具体的な統制活動の詳細が記載されています。AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。 詳細については、「AWS Overview of Security Processes Whitepaper」および「AWS Risk & Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-24.2	事故対応機能には、法的に許容可能な法医学データ収集技術および分析技術の使用が含まれますか?	
情報セキュリティ		IS-24.3	他のテナントデータを停止することなく、特定のテナントについて訴訟のための停止（特定の時点以降のデータの停止）をサポートできますか?	
情報セキュリティ		IS-24.4	召喚令状に対応するためのテナントデータの分離を実施および保証していますか?	
情報セキュリティ	事故対応のメトリックス	IS-25.1	すべての情報セキュリティ事故の種類、規模、および影響を監視および数値化していますか?	AWS セキュリティメトリックスは、ISO 27001 基準に従って監視および分析されています。 詳細については、ISO 27001 基準の付録 A、ドメイン 13.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-25.2	依頼に応じて、統計的な情報セキュリティ事故データをテナントと共有しますか?	
情報セキュリティ	利用規定	IS-26.1	テナントデータまたはメタデータの利用方法またはアクセス方法について文書を提供していますか?	AWS のお客様は、お客様のデータの統制と所有権を保持します。
情報セキュリティ		IS-26.2	調査テクノロジ（検索エンジンなど）を使用して、テナントデータの使用に関するメタデータを収集または作成していますか?	
情報セキュリティ		IS-26.3	調査テクノロジのアクセス対象からデータおよびメタデータを外すことを、テナントに許可していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ	資産の返却	IS-27.1	プライバシー違反を監視し、プライバシーイベントがテナントのデータに影響を与えた場合、テナントに迅速に通知するシステムは用意されていますか?	AWS のお客様は、プライバシー違反についてお客様の環境を監視する責任を有します。 AWS SOC 1 Type II レポートには、AWS の管理対象環境を監視するために実施している統制の概要が記載されています。
情報セキュリティ		IS-27.2	プライバシーポリシーは、業界基準に合わせていますか?	
情報セキュリティ	e コマーストランザクション	IS-28.1	オープンな暗号化手法（3.4ES、AES など）をテナントに提供して、テナントのデータがパブリックネットワークをトラバースする必要がある場合に、テナントがそのデータを保護できるようにしていますか?（例: インターネット）	すべての AWS API は、サーバー認証を提供する、SSL で保護されたエンドポイント経由で利用可能です。AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティの暗号化テクノロジを使用することもできます。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-28.2	インフラストラクチャコンポーネントが、パブリックネットワークで相互に通信する必要がある場合（インターネットベースの環境間のデータレプリケーションなど）、常にオープンな暗号化手法を利用していますか?	
情報セキュリティ	監査ツールのアクセス	IS-29.1	情報セキュリティ管理システムへのアクセスの制限、ログへの記録、および監視を行っていますか?（例:ハイパーバイザ、ファイアウォール、脆弱性スキャナ、ネットワークスニファ、API など）	AWS では、ISO 27001 規格に基づき、AWS リソースに論理的アクセスを認める基準を規定するポリシー文書および手順書を作成済みです。AWS SOC 1 Type II レポートには、AWS リソースに対するアクセスのプロビジョニング管理のために実施している統制の概要が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ	診断および設定ポートのアクセス	IS-30.1	専用のセキュアネットワークを利用して、クラウドサービスインフラストラクチャに対する管理アクセスを提供していますか?	管理プレーンにアクセスする必要のある作業を担当する管理者は、多要素認証を使用して専用の管理ホストにアクセスする必要があります。これらの管理ホストは、特別に設計、構築、設定されており、クラウドの管理プレーン保護機能を強化したシステムです。これらのアクセスは全て記録され、監査されます。管理プレーンにアクセスする必要のある作業を従業員が完了すると、これらのホストと関連するシステムへの特権とアクセス権は取り消されます。
情報セキュリティ	ネットワークおよびインフラストラクチャサービス	IS-31.1	クラウドサービス提供の関連するすべてのコンポーネントについて、容量および使用状況データを収集していますか?	AWS は、ISO 27001 基準に合わせて容量および使用状況データを管理しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
情報セキュリティ		IS-31.2	容量計画および使用状況レポートをテナントに提供していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
情報セキュリティ	携帯デバイスおよびモバイルデバイス	IS-32.1	ノートパソコン、携帯電話、PDA (Personal Digital Assistant) など、携帯型デバイスおよびモバイルデータからの機密データへのアクセスを厳密に制限するためのポリシーおよび手続きが規定さ れ、測定基準が実装されていますか?このようなデバイスは、非携帯型デバイス（プロバイダ組織の施設にあるデスクトップコンピュータなど）よりも一般的に高リスクです。	AWS では、ISO 27001 規格に基づき、AWS リソースに論理的アクセスを認める基準を規定するポリシー文書および手順書を作成済みです。AWS SOC 1 Type II レポートには、AWS リソースに対するアクセスのプロビジョニング管理のために実施している統制の概要が記載されています。 詳細については、「AWS Overview of Security Processes」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ	ソースコードのアクセス制限	IS-33.1	アプリケーション、プログラム、またはオブジェクトソースコードに対する不正アクセスを防ぐための統制を用意し、権限を持つ担当者にのみアクセスを制限していますか?	AWS では、ISO 27001 規格に基づき、AWS リソースに論理的アクセスを認める基準を規定するポリシー文書および手順書を作成済みです。AWS SOC 1 Type II レポートには、AWS リソースに対するアクセスのプロビジョニング管理のために実施している統制の概要が記載されています。 詳細については、「AWS Overview of Security Processes」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-33.2	テナントのアプリケーション、プログラム、またはオブジェクトソースコードに対する不正アクセスを防ぐための統制を用意し、権限を持つ担当者にのみアクセスを制限していますか?	
情報セキュリティ	ユーティリティプログラムのアクセス	IS-34.1	仮想化パーティションの重要な機能（シャットダウン、クローンなど）を管理できるユーティリティは、適切に制限および監視されていますか?	ISO 27001 基準に合わせて、システムユーティリティは適切に制限および監視されています。AWS SOC 1 Type II レポートには、システムアクセスを制限するために実施している統制の詳細情報が記載されています。 詳細については、「AWS Overview of Security Processes」（http://aws.amazon.com/security）を参照してください。
情報セキュリティ		IS-34.2	仮想インフラストラクチャを直接対象とする攻撃（シミング、ブルーピル、ハイパージャンピングなど）を検出できますか?	
情報セキュリティ		IS-34.3	仮想インフラストラクチャを対象とする攻撃は、技術的統制によって回避されていますか?	
法務関連	機密保持契約	LG-01.1	守秘義務契約または機密保持契約の要件は、データの保護に関する組織のニーズを反映し、計画した間隔で運用の詳細の特定、文書化、および確認が行われていますか?	Amazon リーガルカウンセルは Amazon NDA を管理し、AWS のビジネスニーズを反映するために定期的に改訂しています。
法務	サードパーティ契約	LG-02.1	データの処理、保存、および送信が行われる国の法律に従って、外注先プロバイダを選択および監視していますか?	お客様に AWS サービスを提供するために、サードパーティのクラウドプロバイダは一切利用していません。 サードパーティ契約は、必要に応じて Amazon リーガルカウンセルが確認しています。
法務関連		LG-02.2	データの送信元である国の法律に従って、外注先プロバイダを選択および監視していますか?	
法務関連		LG-02.3	弁護士がすべてのサードパーティ契約を確認していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
業務管理	ポリシー	OP-01.1	サービス運用の役割を適切にサポートするためのポリシーおよび手続きが規定され、すべての担当者が利用できるようにしていますか?	AWS 情報セキュリティフレームワークは、COBIT フレームワーク、ISO 27001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。
業務管理	ドキュメント	OP-02.1	情報システムの設定、インストール、および運用を行うための情報システムの文書（管理者およびユーザーガイド、アーキテクチャ図など）は、権限のある担当者が利用できるようにしていますか?	情報システムの文書は、Amazon のイントラネットサイトを使用して AWS 社内の担当者が使用できるようにしています。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
業務管理	容量およびリソース計画	OP-03.1	保守するシステム（ネットワーク、ストレージ、メモリ、I/O など）の過剰サブスクリプションのレベル、および状況またはシナリオに関して文書を提供していますか?	AWS は、容量管理の実施内容を公開していません。AWS は、パフォーマンスレベルの取り組みを伝えるために、サービスに関するサービスレベルアグリーメント（SLA）を発行しています。
業務管理		OP-03.2	ハイパーバイザにあるメモリの過剰サブスクリプション機能の使用を制限していますか?	
業務管理	設備の保守	OP-04.1	仮想インフラストラクチャを使用している場合、クラウドソリューションには、ハードウェアに依存しない復元機能と修復機能が含まれますか?	お客様は EBS Snapshot 機能を使用して、いつでも仮想マシンイメージをキャプチャし、復元できます。お客様は、AMI をエクスポートして、施設内または別のプロバイダで使用できます（ただし、ソフトウェアのライセンス制限に従います）。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
業務管理		OP-04.2	仮想インフラストラクチャを使用している場合、仮想マシンを適時に以前の状態に復元する機能をテナントに提供していますか?	
業務管理		OP-04.3	仮想インフラストラクチャを使用している場合、仮想マシンイメージをダウンロードし、新しいクラウドプロバイダに移植することを許可していますか?	
業務管理		OP-04.4	仮想インフラストラクチャを使用している場合、マシンイメージを顧客のオフサイトの記憶域にレプリケートできる方法で、マシンイメージを顧客が使用できるようにしていますか?	
業務管理		OP-04.5	クラウドソリューションには、ソフトウェアおよびプロバイダに依存しない復元機能および修復機能が含まれますか?	
リスク管理	プログラム	RI-01.1	損失について、サードパーティと保証契約を結んでいますか?	AWS は、AWS のサービスレベルアグリーメント（SLA）に従い、機能停止によって発生する可能性がある損失について、お客様に賠

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
リスク管理		RI-01.2	組織のサービスレベルアグリーメント（SLA）は、機能停止によって発生する可能性がある損失、またはインフラストラクチャ内で発生した損失について、テナントに賠償を提供していますか?	償を提供しています。
リスク管理	評価	RI-02.1	正規のリスク評価は、エンタープライズ全体のフレームワークに適合し、少なくとも年に 1 回または計画した間隔で実行し、定性的および定量的な方法を使用して、すべての特定されたリスクの可能性と影響を判断していますか?	AWS は、ISO 27001 に合わせて、リスク管理プログラムを開発してリスクを軽減し、管理しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 AWS のリスク管理フレームワークの詳細については、「AWS Risk and Compliance Whitepaper」（aws.amazon.com/security）を参照してください。
リスク管理		RI-02.2	内在する未処理のリスクに関連する可能性と影響は、独立して判断され、すべてのリスクカテゴリが考慮されていますか（例えば、監査結果、脅威と脆弱性の分析、規制への準拠など）?	
リスク管理	移行および受け入れ	RI-03.1	妥当な解決期間に従い、会社が規定した基準に基づいて、リスクは受け入れ可能なレベルまで軽減されていますか?	AWS は、ISO 27001 基準の付録 A、ドメイン 4.2 に合わせて、リスク管理プログラムを開発してリスクを軽減し、管理しています。 AWS は独立監査人により ISO 27001 規格に準拠している旨の審査と認証を受けています。 AWS のリスク管理フレームワークの詳細については、AWS リスクとコンプライアンス ホワイトペーパー（http://aws.amazon.com/security で入手可能）を参照してください。
		RI-03.2	妥当な解決期間に従い、会社が規定した基準に基づいて、改善は受け入れ可能なレベルで行われていますか?	
リスク管理	ビジネスおよびポリシー変更の影響	RI-04.1	リスク評価の結果には、セキュリティポリシー、手続き、基準、および統制の関連性と効果を保つように更新する作業が含まれていますか?	AWS のセキュリティポリシー、手続き、基準、および統制の更新は、ISO 27001 基準に合わせて年に 1 回行われています。 詳細については、ISO 27001 基準の付録 A、ドメイン 5.1 を参照してください。AWS は独立監査人により ISO 27001 規格に準拠している旨の審査と認証を受けています。
リスク管理	サードパーティのアクセス	RI-05.1	複数障害の災害復旧機能を提供していますか?	AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。詳細については AWS SOC 1 Type II レポートに記載されています。ISO 27001 基準の付録 A、ドメイン 11.2 に詳細が記載されています。AWS は独立監査人により ISO 27001 規格に準拠している旨の審査と認証を受けています。
		RI-05.2	プロバイダの障害が発生した場合に、アップストリームのプロバイダを使用してサービスの継続性を監視していますか?	
		RI-05.3	依存しているサービスごとに、複数のプロバイダがありますか?	
		RI-05.4	依存するサービスを含む運用の冗長性および継続性のサマリに対するアクセスを提供していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
		RI-05.5	災害を宣言する機能をテナントに提供していますか?	
		RI-05.6	テナントがトリガーするフェイルオーバーオプションを提供していますか?	
		RI-05.7	ビジネスの継続性および冗長性計画をテナントと共有していますか?	
リリース管理	新規開発および獲得	RM-01.1	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、操作、および施設を開発または獲得する場合の管理の承認について、ポリシーおよび手続きは規定されていますか?	AWS は、ISO 27001 基準に合わせて、リソースの新規開発を管理する手続きを用意しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。また、AWS SOC 1 Type II レポートにも詳細な情報が記載されています。
リリース管理	運用の変更	RM-02.1	運用変更管理手続きとその役割/権限/責任について説明した文書を、テナントに提供していますか?	AWS SOC 1 Type II レポートには、AWS 環境における管理体制を変更する際の統制の概要が記載されています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 12.5 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
リリース管理	品質テスト	RM-03.1	品質保証プロセスについて説明した文書を、テナントに提供していますか?	AWS は、ISO 27001 基準に合わせて作成したシステム開発ライフサイクル（System Development Lifecycle/SDLC）プロセスの一部に、品質基準を組み込んでいます。 詳細については、ISO 27001 基準の付録 A、ドメイン 10.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
リリース管理	外注による開発	RM-04.1	すべてのソフトウェア開発について品質基準を満たしていることを確認する統制は用意されていますか?	通常、AWS はソフトウェアの外注開発は行っていません。AWS は、ISO 27001 基準に合わせて作成したシステム開発ライフサイクル（System Development Lifecycle/SDLC）プロセスの一部に、品質基準を組み込んでいます。 詳細については、ISO 27001 基準の付録 A、ドメイン 10.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
リリース管理		RM-04.2	外注されたソフトウェア開発作業について、ソースコードのセキュリティ上の欠点を検出する統制は用意されていますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
リリース管理	権限のないユーザーによるソフトウェアのインストール	RM-05.1	不正なソフトウェアがシステムにインストールされることを制限および監視する統制は用意されていますか?	悪意のあるソフトウェアに対する AWS のプログラム、プロセス、および手続きは、ISO 27001 基準に合わせています。詳細については、AWS SOC 1 Type II レポートを参照してください。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 10.4 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
回復性	管理プログラム	RS-01.1	認識されたリスクイベントの影響を最小限に抑え、適切にテナントへ伝えるために、ビジネス継続性および災害復旧を定義したポリシー、プロセス、および手続きが用意されていますか?	AWS のビジネス継続性ポリシーおよび計画は、ISO 27001 基準に合わせて開発され、テストされています。 AWS とビジネス継続性の詳細については、ISO 27001 基準の付録 A、ドメイン 14.1 および AWS SOC 1 レポートを参照してください。
回復性	影響の分析	RS-02.1	運用サービスレベルアグリーメント（SLA）のパフォーマンスについて、リアルタイムの可視性とレポートをテナントに提供していますか?	Amazon CloudWatch は、AWS クラウドリソースと AWS でお客様が実行するアプリケーションのモニタリングを提供します。詳細については、aws.amazon.com/cloudwatch を参照してください。また、AWS は、Service Health Dashboard にサービスの可用性に関する最新情報を公開しています。status.aws.amazon.com を参照してください。
回復性		RS-02.2	基準に基づく情報セキュリティメトリックス（CSA、CAMM など）をテナントが利用できるようにしていますか?	
回復性		RS-02.3	SLA のパフォーマンスについて、リアルタイムの可視性とレポートを顧客に提供していますか?	
回復性	ビジネス継続性の計画	RS-03.1	地理的に復元力のあるホスティングオプションをテナントに提供していますか?	データセンターは、世界各地にクラスターの状態で構築されています。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
回復性		RS-03.2	インフラストラクチャサービスを他のプロバイダにフェイルオーバーする機能をテナントに提供していますか?	
回復性	ビジネス継続性のテスト	RS-04.1	ビジネス継続性計画の効果を継続させるために、スケジュールした間隔で、または重大な組織または環境の変更時に、計画はテストされますか?	AWS のビジネス継続性計画は、ISO 27001 基準に合わせて開発され、テストされています。 AWS とビジネス継続性の詳細については、ISO 27001 基準の付録 A、ドメイン 14.1 および AWS SOC 1 レポートを参照してください。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
回復性	環境リスク	RS-05.1	自然の原因および災害および意図的な攻撃による破損に対する物理的な保護が予測および設計され、対策が適用されていますか?	AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、ISO 27002 のベストプラクティスに準拠していると認定されました。 詳細については、ISO 27001 規格の附属書 A、ドメイン 9.1 および AWS SOC 1 Type II レポートを参照してください。
回復性	設備の場所	RS-06.1	AWS のいずれかのデータセンターが、影響の大きい環境リスク（洪水、竜巻、地震、台風など）が頻繁に発生する、または発生する可能性が高い場所にありますか?	AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。AWS のサービスは、複数の地理的リージョン内および複数のアベイラビリティーゾーンにわたってデータを保存する柔軟性をお客様に提供しています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。 詳細については、ISO 27001 規格の附属書 A、ドメイン 9.1 および AWS SOC 1 Type II レポートを参照してください。
回復性	設備の電源障害	RS-07.1	公共サービスの停止（停電、ネットワーク崩壊など）から機器を保護するために、セキュリティメカニズムおよび冗長性は実装されていますか?	AWS の機器は、ISO 27001 基準に合わせて機能停止から保護されています。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 AWS SOC 1 Type II レポートには、故障や物理的災害がコンピュータやデータセンター施設に及ぼす影響を最小限に抑えるために実施している統制の詳細が記載されています。 また、詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
回復性	電力および電気通信	RS-08.1	システム間のデータのトランスポート経路を示す文書を、テナントに提供していますか?	データとサーバーを配置する物理的なリージョンは、AWS のお客様が指定します。AWS は、法律または政府機関の要請を遵守することが要求される場合を除き、お客様に通知することなく、お客様が選択したリージョンからサービス利用者コンテンツを移動しないものとします。詳細については AWS SOC 1 Type II レポートに記載されています。また、お客様は、お客様がトラフィックルーティングを制御する専用のプライベートネットワークなど、AWS 施設へのネットワークパスを選択することもできます。
回復性		RS-08.2	テナントは、データのトランスポート方法および経由する法律上の管轄区域を定義できますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティアーキテクチャ	顧客のアクセス要件	SA-01.1	データ、資産、および情報システムに対するアクセス権を顧客に付与する前に、顧客のアクセスに関するすべての特定されたセキュリティ、契約、および規制の要件には契約によって対応および改善されていますか?	AWS のお客様は、適用可能な法律および規制に準拠する範囲で AWS を使用する責任を有しています。AWS は、業界の認定およびサードパーティによる証明、ホワイトペーパー（http://aws.amazon.com/security）を介してセキュリティおよび統制環境をお客様に伝えています。また、認定、レポート、その他の関連する文書を AWS のお客様に直接提供しています。 詳細については、ISO 27001 基準の付録 A、ドメイン 6.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ	ユーザー ID 認証情報	SA-02.1	顧客ベースのシングルサインオン（Single Sign On/SSO）ソリューションの使用、または既存の SSO ソリューションの自社サービスへの統合をサポートしていますか?	AWS Identity and Access Management (IAM) サービスは、AWS マネジメントコンソールへの ID フェデレーションを提供しています。Multi-Factor Authentication は、お客様が利用できるオプション機能の 1 つです。詳細については、AWS のウェブサイト（http://aws.amazon.com/mfa）を参照してください。
セキュリティアーキテクチャ		SA-02.2	オープンな基準を使用して、認証機能をテナントに委任していますか?	
セキュリティアーキテクチャ		SA-02.3	ユーザーの認証および承認の手段として、ID フェデレーション基準（SAML、SPML、WS-Federation など）をサポートしていますか?	
セキュリティアーキテクチャ		SA-02.4	地域の法律およびポリシーの制限をユーザーアクセスに課すために、ポリシーの実施ポイントの機能（XACML など）がありますか?	
セキュリティアーキテクチャ		SA-02.5	データに対する役割ベースおよびコンテキストベース両方の資格を有効にする（テナントのデータの分類を可能にする）ID 管理システムが用意されていますか?	
セキュリティアーキテクチャ		SA-02.6	ユーザーアクセスについて、強力な（マルチファクターの）認証オプション（デジタル証明書、トークン、生体認証など）をテナントに提供していますか?	
セキュリティアーキテクチャ		SA-02.7	サードパーティの ID 保証サービスを使用することを、テナントに許可していますか?	

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティアーキテクチャ	データのセキュリティと完全性	SA-03.1	データセキュリティアーキテクチャは、業界基準を使用して設計されていますか?（例:CDSA、MULITSAFE、CSA によって信頼済みのクラウドアーキテクチャ基準、FedRAMP[sm] CAESARS）	AWS Data Security Architecture は、業界の主要な慣例を組み込むように設計されています。 詳細については、ISO 27001 基準の付録 A、ドメイン 10.8 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ	アプリケーションのセキュリティ	SA-04.1	業界基準（Build Security in Maturity Model [BSIMM] Benchmarks、Open Group ACS Trusted Technology Provider Framework、NIST など）を利用して、システム/ソフトウェア開発ライフサイクル（Systems/Software Development Lifecycle/SDLC）のセキュリティに組み込んでいますか?	AWS のシステム開発ライフサイクルは、業界のベストプラクティスを組み込んでおり、これには AWS セキュリティによる公式の設計レビュー、脅威のモデリング、リスク評価の完遂などが含まれています。詳細については、「AWS Overview of Security Processes」を参照してください。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 12.5 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ		SA-04.2	運用前にコードのセキュリティの欠点を検出するために、自動ソースコード分析ツールを利用していますか?	
セキュリティアーキテクチャ		SA-04.3	すべてのソフトウェアサプライヤが、システム/ソフトウェア開発ライフサイクル（Systems/Software Development Lifecycle/SDLC）セキュリティの業界基準に従っていますか?	
セキュリティアーキテクチャ	データの完全性	SA-05.1	手動またはシステムのプロセスエラーまたはデータ破損を防ぐために、アプリケーションインターフェースおよびデータベースについてデータの入力と出力の整合性ルーチン（一致チェック、編集チェックなど）が実装されていますか?	AWS のデータ整合性統制は AWS SOC 1 Type II レポートに記載されているように、送信、保存、および処理を含むすべての段階でデータの整合性が維持される妥当な保証を提供しています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 12.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ	運用環境および非運用環境	SA-06.1	SaaS または PaaS の提供について、運用プロセスとテストプロセスで別の環境をテナントに提供していますか?	AWS のお客様は、運用環境とテスト環境を作成および保持する機能と責任を有します。AWS のウェブサイトでは、AWS サービスを利用して環境を作成する場合のガイダンスを提供しています（http://aws.amazon.com/documentation/）。
セキュリティアーキテクチャ		SA-06.2	IaaS の提供について、適切な運用環境およびテスト環境を作成する方法のガイダンスをテナントに提供していますか?	
セキュリティアーキテクチャ	リモートユーザーの Multi-Factor Authentication	SA-07.1	Multi-Factor Authentication は、すべてのリモートユーザーアクセスについて必須ですか?	Multi-Factor Authentication は、お客様が利用できるオプション機能の 1 つです。詳細については、AWS のウェブサイト（http://aws.amazon.com/mfa）を参照してください。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティアーキテクチャ	ネットワークセキュリティ	SA-08.1	IaaS の提供について、仮想化ソリューションを使用して、階層化セキュリティアーキテクチャ相当のものを作成する方法のガイダンスを顧客に提供していますか?	AWS のウェブサイトでは、AWS の公開ウェブサイト（http://aws.amazon.com/documentation/）で入手できる複数のホワイトペーパーで、階層化セキュリティアーキテクチャ作成のガイダンスを提供しています。
セキュリティアーキテクチャ	セグメント化	SA-09.1	ビジネスおよびコンテキストのセキュリティ要件を確保するために、システム環境とネットワーク環境は論理的に分離していますか?	AWS のお客様は、お客様が定義した要件に従って、お客様のネットワークセグメントを管理する責任を有します。 AWS 内部では、AWS のネットワークセグメントは ISO 27001 基準に合わせて作成されています。詳細については、ISO 27001 基準の付録 A、ドメイン 11.4 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ		SA-09.2	法律、規制、および契約の要件に準拠するために、システム環境とネットワーク環境は論理的に分離されていますか?	
セキュリティアーキテクチャ		SA-09.3	運用環境と非運用環境を分離するために、システム環境とネットワーク環境は論理的に分離されていますか?	
セキュリティアーキテクチャ		SA-09.4	機密データの保護と隔離のために、システム環境とネットワーク環境は論理的に分離されていますか?	
セキュリティアーキテクチャ	ワイヤレスのセキュリティ	SA-10.1	ネットワーク環境パラメータを保護するためにポリシーと手続きが規定され、メカニズムが実装され、不正なトラフィックを制限するように設定されていますか?	AWS ネットワーク環境を保護するためのポリシー、手続き、およびメカニズムが用意されています。詳細については AWS SOC 1 Type II レポートに記載されています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 10.6 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ		SA-10.2	ベンダーのデフォルト設定の代わりに、認証および送信について強力な暗号化による適切なセキュリティ設定を可能にするために、ポリシーと手続きが規定され、メカニズムが実装されていますか（暗号化キー、パスワード、SNMP コミュニティ文字列など）?	
セキュリティアーキテクチャ		SA-10.3	ネットワーク環境を保護し、不正なネットワークデバイスの存在を検出してネットワークから適時に接続を解除するために、ポリシーと手続きが規定され、メカニズムが実装されていますか?	
セキュリティアーキテクチャ	共有ネットワーク	SA-11.1	共有ネットワークインフラストラクチャがあるシステムへのアクセスは、セキュリティポリシー、手続き、および基準に従って、権限のある担当者に制限されていますか? 外部組織と共有されているネットワークについて、組織間のネットワークトラフィックを分離するために補う統制について詳細に示した文書の計画がありますか?	アクセスは、サービス、ホスト、ネットワークデバイスなどの重要なリソースに厳密に制限されており、Amazon の専用アクセス許可管理システムでアクセスが明示的に承認される必要があります。AWS が実施している具体的な統制活動に関する詳細については、AWS SOC 1 Type II レポートに記載されています。 また、ISO 27001 基準の付録 A、ドメイン 11.3 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。

ドメイン	統制グループ	CID	コンセンサス評価の質問	AWS の回答
セキュリティアーキテクチャ	時計の同期	SA-12.1	同期タイムサービスプロトコル（NTP など）を利用して、すべてのシステムが共通の時間を参照していますか?	AWS 情報システムは、ISO 27001 基準に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ	設備の識別	SA-13.1	既知の機器の場所に基づいて接続認証の整合性を検証するために、自動的な機器識別が接続認証の方法として使用されていますか?	AWS は、ISO 27001 基準に合わせて機器識別を管理しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
セキュリティアーキテクチャ	監査記録および侵入検知	SA-14.1	適時の検出、根本原因の分析ごとの調査、および事故対応を容易にするために、ファイルの完全性（ホスト）およびネットワークの侵入検出（IDS）ツールは実装されていますか?	AWS 事故対応プログラム（事故の検出、調査、および対応）は、ISO 27001 基準に合わせて開発されています。AWS SOC 1 Type II レポートには、AWS が実施している具体的な統制活動の詳細が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
セキュリティアーキテクチャ		SA-14.2	監査ログに対するユーザーの物理的アクセスおよび論理的アクセスは、権限を持つ担当者に制限されていますか?	
セキュリティアーキテクチャ		SA-14.3	規制および基準を、自社の統制、アーキテクチャ、およびプロセスと適切に配慮して対応付けていることを示す証拠を提供できますか?	
セキュリティアーキテクチャ	モバイルコード	SA-15.1	明確に定義されているセキュリティポリシーに従って承認済みのモバイルコードが実行されるように、モバイルコードはインストールおよび使用前に承認され、コードの設定が確認されていますか?	AWS では、お客様の要件に合わせて、お客様がクライアントおよびモバイルアプリケーションを管理できます。
セキュリティアーキテクチャ		SA-15.2	すべての未承認のモバイルコードは実行を禁止していますか?	

付録 B:アメリカ映画協会（MPAA）のコンテンツセキュリティモデルへの AWS の準拠状況

アメリカ映画協会（MPAA） は、保護されたメディアとコンテンツを安全に保管、処理、配信するための一連のベストプラクティスをまとめました。MPAA のコンテンツセキュリティのベストプラクティスについては、http://www.fightfilmtheft.org/best-practice.html を参照してください。
メディア企業はこれらのベストプラクティスを、コンテンツ管理のリスク評価とセキュリティ監査の手段として利用できます。
次の表は、2013 年 1 月 1 日に公開されたアメリカ映画協会（MPAA）のコンテンツセキュリティモデルのガイドラインに対する AWS の準拠状況を示しています。追加情報として、サードパーティが監査した AWS の認証とレポートへの参照が示されています。
* ISO 27002 および NIST 800-53 との対応付けは、『*MPAA コンテンツセキュリティのベストプラクティス共通ガイドライン 2013 年 1 月 1 日*』の定義に従って行われました。

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-1.0	エグゼクティブによるセキュリティの認識/監督	情報セキュリティプログラムとリスク評価結果の定期的な確認を要求することで、情報セキュリティ機能がエグゼクティブ/所有者によって確実に管理されるようにします。	Amazon の統制環境は、当社の最上層部で開始されます。役員とシニアリーダーは、当社のカラーと中心的な価値を規定する際、重要な役割を担っています。AWS は、情報および関連技術のための統制目標（COBIT）フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会（AICPA）の信頼提供の原則（Trust Services Principles）、PCI DSS 3.0 版、および米国国立標準技術研究所（NIST）出版物 800-53 改訂 3（連邦情報システム向けの推奨セキュリティ管理）に基づいて ISO 27001 認証可能なフレームワークを実質的に統合しています。AWS 従業員の完全で定期的な役割に基づくトレーニングには、AWS セキュリティトレーニングが含まれます。作成したポリシーを従業員が理解し、従うために、コンプライアンス監査が実施されます。	MS-1	SOC1 (1.1) SOC2 (S.2.3)	4.1 6.11	12.4 12.5	PM-1 PM-2
MS.S-1.0	エグゼクティブによるセキュリティの認識/監督	エグゼクティブ/所有者によって承認された情報セキュリティ用の統制フレームワーク（ISO 27001 など）を実装する情報セキュリティ管理システムを確立します。						
MS-1.1	エグゼクティブによるセキュリティの認識/監督	企業が担うコンテンツ保護の責任について経営陣やオーナーを教育し、認識を深めるよう指導します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-2.0	リスク管理	施設に関連したコンテンツの盗難・漏えいリスクを特定・優先順位付けするために、コンテンツのワークフローと機密資産に焦点をあてた正規のセキュリティリスク査定プロセスを作成します。	AWS は少なくとも毎年更新、確認される、文書化された正式なリスク評価ポリシーを導入しています。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。 このポリシーに合わせて、すべての AWS リージョンとビジネスを対象とする年次リスク評価が AWS コンプライアンスチームによって行われ、AWS 上級経営幹部によって確認されます。これは、独立監査人によって行われる認証、証明、および報告に加えて行われます。リスク評価の目的は、AWS の脅威と脆弱性を識別し、脅威と脆弱性にリスク評価を割り当て、評価を正式に文書化し、問題の対応に関するリスク処理計画を作成することです。リスク評価結果は AWS 上級経営幹部によって年次ベースで確認されるとともに、大きな変更により新しいリスク評価が必要になった場合は、年間リスク評価の前にも確認されます。 お客様はデータ（コンテンツ）の所有権を維持し、コンプライアンスの目的を満たすためにデータのワークフローに関連するリスクを評価、管理する責任があります。 AWS のリスク管理フレームワークは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-2	SOC2（S3.31、S4.2、S4.3）	4.1 4.2 7.2	12.1 12.2	CA-1 CA-2 CA-5 RA-1 RA-2 RA-3
MS-2.1	リスク管理	顧客の指示に基づき、セキュリティレベルの高いコンテンツを特定します。						
MS-2.2	リスク管理	内部リスク評価を毎年実施し、ワークフローの主要な変更を基準にして（少なくとも、MPAA ベストプラクティス共通ガイドラインおよび該当する補足ガイドラインに基づいて）、識別されたリスクを文書化し、それに基づく対応を行います。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-3.0	セキュリティ組織	セキュリティの窓口となる連絡先を定め、コンテンツおよび資産の保護に関する役職と責任を正式に規定します。	AWS では、AWS セキュリティチームによって管理され、AWS 最高情報セキュリティ責任者（CISO）が率いる、情報セキュリティ組織が設立されています。AWS は、AWS をサポートするすべての情報システムユーザーに対して、セキュリティ認識トレーニングを維持、提供します。この年間セキュリティ認識トレーニングには、セキュリティおよび認識トレーニングの目的、すべての AWS ポリシーの場所、AWS インシデント応答手順（内部および外部セキュリティインシデントの報告方法の手順を含む）の各トピックが含まれます。 AWS 内のシステムは、主要な運用メトリックスやセキュリティメトリックスをモニタリングするよう広範に実装されます。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。しきい値を超えると、AWS インシデント対応プロセスが開始されます。Amazon インシデント対応チームは、業界標準の診断手順を採用して、ビジネスに影響するイベント中に解決策を実行します。スタッフは 24 時間年中無休でインシデントの検出、影響の管理、および解決にあたっています。 AWS の役割と責任は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-3	SOC1 (1.1) SOC2 (S.2.3)	6.1.3	12.4 12.5	PM-2
MS.S-3.0	セキュリティ組織	情報システムと物理的なセキュリティを逐次モニタリングし、不審なアクティビティを識別して、それに対応するセキュリティチームを確立します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-4.0	ポリシーと手順	資産とコンテンツのセキュリティに関するポリシーと手順を規定します。ポリシーは少なくとも次のトピックをカバーしていなければなりません。 • 人事ポリシー • 容認できる使用（例: ソーシャルネットワーク、インターネット、電話） • 資産の分類 • 資産取り扱いポリシー • デジタル記録デバイス（例: スマートフォン、デジタルカメラ、カムコーダー） • 例外ポリシー（例: ポリシーの逸脱を文書化するプロセス） • パスワードコントロール（例: パスワードの最低文字数、スクリーンセーバー） • 施設からの顧客資産借り出し禁止 • システム変化の管理 • 通報ポリシー • 制裁ポリシー（例: 懲戒ポリシー）	AWS は、情報および関連技術のための統制目標（COBIT）フレームワークに基づいて情報セキュリティフレームワークとポリシーを制定していて、ISO 27002 統制、米国公認会計士協会（AICPA）の信頼提供の原則（Trust Services Principles）、PCI DSS 3.0 版、および米国国立標準技術研究所（NIST）出版物 800-53 改訂 3（連邦情報システム向けの推奨セキュリティ管理）に基づいて ISO 27001 認証可能なフレームワークを実質的に統合しています。 AWS は、AWS をサポートするすべての情報システムユーザーに対して、セキュリティ認識トレーニングを維持、提供します。この年間セキュリティ認識トレーニングには、セキュリティおよび認識トレーニングの目的、すべての AWS ポリシーの場所、AWS インシデント応答手順（内部および外部セキュリティインシデントの報告方法の手順を含む）の各トピックが含まれます。 AWS のポリシー、手順、および該当するトレーニングプログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP^{sm} への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-4	SOC1 (1.2) SOC2 （S1.1、 S1.2、 S1.3、 S2.2、 S2.3、 S2.4、 S3.7、 S3.8、 S3.9、 S4.2、 S4.3）	5.1.1 5.1.2 6.1.1 8.1.3 8.2.2	3.1 8.5 12.1 12.2 12.3 12.6	AT-1 AT-2 AT-3 AT-4 PL-1 PS-7

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS.S-4.0	ポリシーと手順	施設によって処理されるコンテンツに固有の詳細なトレーニングを提供します。						
MS-4.1	ポリシーと手順	少なくとも年に 1 度、セキュリティポリシーおよび手順の確認と更新を行います。						
MS.S-4.1	ポリシーと手順	暗号化されたコンテンツを扱うすべてのユーザー用の暗号化とキー管理に関連するアプリケーションとプロセスのトレーニングを実施します。						
MS-4.2	ポリシーと手順	すべてのポリシー、手順、顧客の要件、更新に関して、すべての従業員（例: 社員、一時雇用者、研修生）およびサードパーティの従業員（例: 契約社員、フリーランサー、派遣会社）に合意の署名を義務付けます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-4.3	ポリシーと手順	セキュリティ認識プログラムを開発し、定期的に更新して会社の従業員やサードパーティの従業員を雇用時にトレーニングします。その後、毎年セキュリティポリシーと手順についてトレーニングし、最低でも次の分野に対応します。 • IT セキュリティポリシーおよび手順 • コンテンツ/資産のセキュリティと取り扱い • セキュリティインシデント報告とエスカレーション • 懲戒処分						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-5.0	インシデントへの対応	セキュリティ問題が検知・報告された際に講じる対応策を規定する正規のインシデント対応プランを作成します。	AWS は、文書化された正式なインシデント対応ポリシーとプログラムを実装しています。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。 AWS は、インシデントの管理に 3 段階の手法を利用しています。 1.アクティブ化および通知段階:AWS のインシデントはイベントの検出で始まります。このソースは、次のように複数あります。 a. メトリックスとアラーム - AWS は例外的な状況認識機能を維持しており、ほとんどの問題は 24 時間年中無休のモニタリングと、リアルタイムのメトリックスおよびサービスダッシュボードのアラームにより迅速に検出されます。インシデントの大部分はこのようにして検出されます。AWS は早期インジケータアラームを利用して、最終的にお客様に影響する可能性のある問題を事前に識別しています。 b. AWS 従業員が入力したトラブルチケット c. 技術サポートホットラインへの 24 時間年中無休の電話による問い合わせ。 イベントがインシデント条件を満たす場合、該当するオンコールサポートエンジニア が AWS Event Management Tool システムを利用してエンゲージメントを開始し、該当するプログラムリゾルバー（セキュリティチームなど）を呼び出します。リゾルバーはインシデントの分析を実行して、追加のリゾルバーが必要かどうか判断するとともに、おおよその根本原因を特定します。	MS-5	SOC 1（8.2） SOC 2（S2.4、S3.5、S3.7、S3.9）	13.1 13.1.1 13.2.2	12.9	IR-1 IR-2 IR-4 IR-5 IR-6 IR-7 IR-8
MS-5.1	インシデントへの対応	セキュリティインシデントの検知、分析、修復を担当するインシデント対応チームを編成します。						
MS-5.2	インシデントへの対応	個人が検知したインシデントをセキュリティインシデント対応チームに報告するための、セキュリティインシデント報告手順を作成します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-5.3	インシデントへの対応	お客様のコンテンツが漏洩、盗難、またはその他の侵害（クライアントアセットがないなど）にあった可能性がある場合、インシデントについてお客様に迅速に連絡し、経営幹部やお客様とともに事後会議を実施します。	2.復旧段階: 該当するリゾルバーが、インシデントに対応する修正策を実行します。トラブルシューティング、修正策、および関連コンポーネントに対応すると、問い合わせリーダーはフォローアップドキュメントとフォローアップアクションの形で次の手順を割り当て、問い合わせエンゲージメントを終了します。 3.再構成段階: 該当する修正アクティビティが完了すると、問い合わせリーダーは復旧段階が完了したことを宣言します。インシデントの事後検証および根本原因の深層分析が該当するチームに割り当てられます。事後分析の結果は該当する上級経営幹部によって確認され、設計変更などの該当するアクションがエラー修正（COE）ドキュメントに記載され、完了まで追跡されます。 上記に示した内部コミュニケーションメカニズムに加えて、AWS ではその顧客ベースとコミュニティをサポートするために、外部コミュニケーションのさまざまな方法を導入しています。カスタマーエクスペリエンスに影響を与える運用上の問題についてカスタマーサポートチームが通知を受けることができるようにするためのメカニズムが配備されています。[Service Health Dashboard] が、顧客サポートチームによって管理運営されており、大きな影響を与える可能性のある問題について顧客に警告を発することができます。 AWS のインシデント管理プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。					

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-6.0	ワークフロー	各プロセスにおけるコンテンツのトラッキングと承認チェックポイントを含むワークフローを文書化します。これには、物理的コンテンツとデジタルコンテンツの両方に関する以下のプロセスが含まれます。 • 配信 • 取り込み • 移動 • 保管 • 資産保有者への返還 • 現場からの除去 • 破壊	AWS のお客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーション、およびデータの所有権と統制を有しているため、コンテンツ（データ）のワークフローの文書化はお客様の責任になります。	MS-6	AWS では該当しません	AWS では該当しません	AWS では該当しません	AWS では該当しません
MS-6.1	ワークフロー	コンテンツのワークフローに関連するリスクを防止、検知、修復するための主要コントロールを特定、実装し、その効果性を査定します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-7.0	役割分担	コンテンツのワークフロー内で義務を分離し、分離が現実的でない場合は補正の統制を導入して文書化します。	AWS のお客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーション、およびデータの所有権と統制を有しているため、コンテンツ（データ）のワークフローの義務の分離はお客様の責任になります。 AWS でデジタル資産とワークフローをホストしているお客様は、適切な場合は AWS Identity and Access Management を利用して、デジタル資産とコンテンツ受け渡しの義務の分離に関連する統制要件を導入できます。お客様は、適切な場合は監査ログの確認と維持のために AWS CloudTrail を利用することができます。	MS-7	AWS では該当しません	AWS では該当しません	AWS では該当しません	AWS では該当しません

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-8.0	経歴確認	すべての従業員やサードパーティの従業員の経歴を確認します。	AWS は従業員に対し、その従業員の役職や AWS 施設へのアクセスレベルに応じて、適用法令が認める範囲で、雇用前審査の一環として犯罪歴の確認を行います。 AWS の犯罪歴の確認プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-8	SOC 2（S3.11）	8.1.2	12.7	PS-3
MS-9.0	守秘契約	従業員およびサードパーティの従業員全員に対し、雇用時とその後年 1 回、守秘契約書（例: 機密保持契約書）への署名を義務付けます。これには、コンテンツの取り扱いと保護に関する要件も盛り込みます。	Amazon Legal Counsel が Amazon 機密保持契約書（NDA）を管理しており、AWS の業務要件を反映するために定期的に改訂を加えています。 AWS による機密保持契約書（NDA）の使用は、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-9		6.1.5 8.2.3 8.3.3		PL-4 PS-4 PS-6 PS-8 SA-9
MS-9.1	守秘契約	従業員とサードパーティの従業員の全員に、雇用または契約の終了の時点で所持している顧客のコンテンツと情報をすべて返却するよう義務付けます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-10.0	サードパーティの利用と審査	コンテンツを取り扱うサードパーティの従業員全員に、契約時点で守秘契約書（例: 非開示契約）への署名を義務付けます。	AWS システムとデバイスをサポートするすべての従業員は、入社時研修の一環として、アクセス権を付与される前に機密保持契約書に署名します。さらに、オリエンテーションの一環として、利用規定および Amazon 業務行動倫理規定（行動規定）ポリシーを読んで同意することが従業員に求められます。 AWS システムとデバイスをサポートするサードパーティプロバイダに対する従業員セキュリティ要件は、AWS の親組織である Amazon.com および各サードパーティプロバイダとの相互機密保持契約で確立されます。Amazon リーガルカウンセルおよび AWS 調達チームが、サードパーティプロバイダとの契約で AWS サードパーティプロバイダの従業員セキュリティ要件を定義します。AWS の情報を扱うすべての従業員は、最低でも雇用前審査に合格し、AWS の情報へのアクセス権を付与される前に、機密保持契約書（NDA） に署名する必要があります。 AWS サードパーティの要件は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-10		6.1.5 6.2 6.2.3 10.2 11.1 11.2	12.8	PL-4 PS-4 PS-6 PS-7 PS-8 SA-9
MS.S-10.0	サードパーティの利用と審査	物理的資産に関するサードパーティストレージプロバイダの使用について、クライアントに通知します。						
MS-10.1	サードパーティの利用と審査	サードパーティとの契約にセキュリティ要件を含めます。						
MS.S-10.1	サードパーティの利用と審査	国際的（米国外との取引を行う）運送会社は、"Customs-Trade Partnership Against Terrorism" (CTPAT) の認証を受ける必要があります。						
MS-10.2	サードパーティの利用と審査	サードパーティの従業員に対し、契約を終了する際に資産の返還を求め、守秘義務とセキュリティ条項の遵守を確認するプロセスを導入します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS.S-10.2	サードパーティの利用と審査	運送梱包ベンダーを毎年再評価します。ベンダーが所在地を変更する、またはサービスを追加したときも評価します。						
MS-10.3	サードパーティの利用と審査	適切な場合（運送サービスなど）には、サードパーティの従業員に、責任保証制度と保険に加入することを義務付けます。						
MS.S-10.3	サードパーティの利用と審査	サードパーティのコンテンツ配信システムとウェブサイトへのアクセス権を毎年確認します。						
MS-10.4	サードパーティの利用と審査	職務の遂行に必要な場合を除き、サードパーティによるコンテンツ/制作エリアへのアクセスを制限します。						
MS.S-10.4	サードパーティの利用と審査	機密性の高いコンテンツを扱うサードパーティの従業員の選定および採用プロセスの一環として、セキュリティ適性アクティビティ（セキュリティ評価、自己評価のアンケートなど）を導入します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
MS-10.5	サードパーティの利用と審査	サードパーティの企業が他のサードパーティにコンテンツの取り扱いを委託する場合は、事前にクライアントへ通知することを義務付けます。						
PS-1.0	出入り口	受付とそれ以外のエリアとの間にアクセスコントロールがない施設の場合、すべての出入り口を常に施錠します。	AWS は、データセンターへのアクセスのための多要素認証メカニズム、および権限のある関係者のみが AWS データセンターに入場するための追加のセキュリティメカニズムを利用しています。権限のある関係者は、施設への入場および許可された部屋への入室には、カードリーダーでバッジを使用し、一意の PIN を入力する必要があります。 データセンターへの物理的なアクセスは、AWS の電子アクセス制御システムに基づいて行われます。このシステムの構成では、建物や部屋の入り口ではカードリーダーと PIN パッドを、出口ではカードリーダーのみを使用します。建物や部屋の出口でカードリーダーを使用することで、パスバック防止機能を提供し、許可のない人が許可のある人の後にぴったりついて、バッジなしで入場できないようにします。 アクセス制御システムに加えて、AWS データセンターのすべての入り口は、メインエントランス、配送ドック、屋根の扉/ハッチを含めて、ドアを無理やり開けたり、開放したままにするとアラームが鳴る侵入検出デバイスで保護されています。 AWS データセンターでは、電子メカニズムに加えて、トレーニングを受けた警備員を建物内および	PS-1	SOC 1（5.5） SOC 2（S3.3、S3.4）	9.1.1 9.1.2	9.1	PE-3 PE-6
PS.S-1.0	出入り口	非常口以外のすべての出入り口に警備員を配置します。						
PS-1.1	出入り口	コンテンツエリアをその他の施設エリア（管理事務所など）から分離して、コンテンツを扱うすべてのエリアへのアクセスを管理します。						
PS.S-1.1	出入り口	配送ドックのすべての扉をロックしてアラームを設置し、使用中は配送ドックの扉を監視します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-1.2	出入り口	トラック運転手が施設の他のエリアに入らないように、運転手の入場を分離します。	周囲に毎日 24 時間常駐させています。 システム境界内のデータセンターへのアクセスは必要範囲内でのみ許可され、すべての物理的なアクセス要請は適切なエリアアクセスマネージャー（AAM） によって確認および承認されます。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。					
PS.S-1.3	出入り口	ランダム化されたスケジュールで毎日のセキュリティ巡回プロセスを導入し、巡回結果をログに記録します。						
PS.S-1.4	出入り口	警備員の勤務時間中に検出されたすべてのインシデントを記録、調査、解決します。						
PS-2.0	訪問者の出入り	次の項目を記載した訪問者（外来者）の記録を残します。 • 氏名 • 会社名 • 来社時刻/退去時刻 • 社内担当者/部署 • 訪問者の署名 • 割り当てたバッジ番号	AWS のデータセンターは、外部からはそれとはわからないようになっていて、一般には解放されていません。周囲および建物の入り口の両方で、物理的なアクセスは厳しく管理されています。AWS は、データセンターへのアクセスや情報を、緊急の修理など、それを業務上本当に必要とするベンダー、業者、訪問者にのみ提供しています。データセンターのすべての訪問者は、該当するエリアアクセスマネージャー（AAM） によって事前に承認され、AWS チケット管理システムに記録される必要があります。訪問者は、データセンターに到着したら ID を提示し、登録した後で訪問者バッジが発行されます。また、データセンターにいる間は、承認されたスタッフによって継続的に付き添われます。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-2	SOC 1（5.1） SOC 2（S3.3、S3.4）	9.1.2	9.2 9.4	PE-3 PE-7
PS-2.1	訪問者の出入り	すべての訪問者に ID バッジまたはステッカーを貸与し、常時目に見える位置に着用することを義務付け、退出の際に回収します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-2.2	訪問者の出入り	訪問者にはコンテンツ/制作エリアへの電子アクセスを許可してはなりません。						
PS-2.3	訪問者の出入り	訪問者の滞在中は権限を持つ従業員が必ず同伴するものとします。最低でもコンテンツ/制作エリアへの立ち入りには同伴を必須とします。						
PS-3.0	身分証明書	従業員および長期雇用のサードパーティの従業員（例: 清掃業者）には写真付きの身分証を発行し、常時目に見える位置に着用することを義務付けます。	AWS は、データセンターへの長期にわたるアクセスを認められた従業員に対し、写真付きの身分証を兼ねた電子アクセスカードを発行します。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-3	SOC 1（5.1） SOC 2（S3.3、S3.4）	9.1.2	9.2 9.4	PE-3

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-4.0	周辺のセキュリティ	組織のリスク査定により、施設がリスクにさらされている可能性が判明した場合には、その対策となる周辺のセキュリティ統制を実施します。	データセンターへの物理的なアクセスは、AWS の電子アクセス制御システムに基づいて行われます。このシステムの構成では、建物や部屋の入り口ではカードリーダーと PIN パッドを、出口ではカードリーダーのみを使用します。建物や部屋の出口でカードリーダーを使用することで、パスバック防止機能を提供し、許可のない人が許可のある人の後にぴったりついて、バッジなしで入場できないようにします。 アクセス制御システムに加えて、AWS データセンターのすべての入り口は、メインエントランス、配送ドック、屋根の扉/ハッチを含めて、ドアを無理やり開けたり、開放したままにするとアラームが鳴る侵入検出デバイスで保護されています。 AWS データセンターでは、電子メカニズムに加えて、トレーニングを受けた警備員を建物内および周囲に毎日 24 時間常駐させています。 システム境界内のデータセンターへのアクセスは必要範囲内でのみ許可され、すべての物理的なアクセス要請は適切なエリアアクセスマネージャー（AAM） によって確認および承認されます。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-4	SOC 1（5.5） SOC 2（S3.3、S3.4）	9.1.1	9.1	PE-3
PS.S-4.0	周辺のセキュリティ	施設への不正アクセスのリスクを減らすため、周囲の追加の制限措置（フェンス、車両バリケードなど）を追加で設置します。						
PS.S-4.1	周辺のセキュリティ	常に周囲のゲートを閉じ、遠隔操作でゲートを開放できる専任のオンサイト従業員を配置します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-4.2	周辺のセキュリティ	周囲の入り口に警備員を常駐させ、施設内に車両の入場を許可するプロセス（電子ゲートアーム、駐車許可証など）を導入します。						
PS-5.0	警報	すべての出入り口（非常口を含む）、搬出入り口、非常階段、および制限エリア（保管庫、サーバー/マシンルームなど）をカバーする、集中管理型の音響警報システムを設置します。	AWS データセンターのすべての入り口は、メインエントランス、配送ドック、屋根の扉/ハッチを含めて、ドアを無理やり開けたり、開放したままにするとアラームが鳴り、AWS 集中物理セキュリティモニタリングでもアラームが作成される侵入検出デバイスで保護されています。 AWS データセンターでは、電子メカニズムに加えて、トレーニングを受けた警備員を建物内および周囲に毎日 24 時間常駐させています。すべてのアラームは警備員によって調査され、すべてのインシデントについて根本原因が記録されます。SLA に記載された時間内に対応が行われない場合、すべてのアラームは自動的にエスカレートするよう設定されています。 システム境界内のデータセンターへのアクセスは必要範囲内でのみ許可され、すべての物理的なアクセス要請は適切なエリアアクセスマネージャー（AAM）によって確認および承認されます。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-5	SOC 1（5.5） SOC 2（S3.3、S3.4）	9.1	9.1	PE-3 PE-6
PS-5.1	警報	警報が発生した場合には保安責任者に直接通知が行くようにするか、集中セキュリティグループまたはサードパーティが警報装置を監視するようにします。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-5.2	警報	警報システムへのアクセスを必要とする各人に個別の設定/解除コードを割り当て、その他の人員によるアクセスを制限します。						
PS-5.3	警報	年に 1 度、警報システムの設定/解除操作を許可されている関係者のリストを確認します。						
PS-5.4	警報	警報システムを 6 か月に 1 度テストします。						
PS-5.5	警報	制限エリア（例: 保管庫、サーバー/マシンルーム）内の効果的な場所に動体検知器を設置し、担当の保安要員やサードパーティに通報が行くように設定します。						
PS-5.6	警報	機密エリアへの出入り口が一定時間（例: 60 秒）を超えて開いたままになった場合は通報されるよう、コンテンツ/制作エリアにドア開放アラームを設置します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-6.0	承認	施設へのアクセスを管理し、アクセス権限に変更があった場合にはそれを記録するための手続きを文書化し、実施します。	データセンターへの物理的なアクセスは、AWS の電子アクセス制御システムに基づいて行われます。このシステムの構成では、建物や部屋の入り口ではカードリーダーと PIN パッドを、出口ではカードリーダーのみを使用します。建物や部屋の出口でカードリーダーを使用することで、パスバック防止機能を提供し、許可のない人が許可のある人の後にぴったりついて、バッジなしで入場できないようにします。 アクセス制御システムに加えて、AWS データセンターのすべての入り口は、メインエントランス、配送ドック、屋根の扉/ハッチを含めて、ドアを無理やり開けたり、開放したままにするとアラームが鳴る侵入検出デバイスで保護されています。 AWS データセンターでは、電子メカニズムに加えて、トレーニングを受けた警備員を建物内および周囲に毎日 24 時間常駐させています。 システム境界内のデータセンターへのアクセスは必要範囲内でのみ許可され、すべての物理的なアクセス要請は適切なエリアアクセスマネージャー（AAM） によって確認および承認されます。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-4	SOC 1（5.3、5.5） SOC 2（S3.3、S3.4、S5.3）	11.2 11.2.4	9.1	PE-1 PE-2 PE-3 PE-4 PE-5
PS.S-6.0	承認	毎月、および会社の従業員またはサードパーティの従業員（またはその両方）の役割や雇用状態が変わったときに、制限されたエリア（ボールト、金庫など）へのアクセスを確認します。						
PS-6.1	承認	本稼働システムへのアクセスを、権限を持つ関係者のみに制限します。						
PS-6.2	承認	四半期に 1 度、また従業員やサードパーティの従業員の役職や雇用状態が変更になった場合には随時、制限エリア（例: 保管庫、サーバー/マシンルーム）へのアクセスを確認します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-7.0	電子アクセス	施設全体に電子アクセスシステムを設置し、あらゆる出入り口、およびコンテンツが保存、転送、処理されるすべてのエリアをカバーします。	データセンターへの物理的なアクセスは、AWS の電子アクセス制御システムに基づいて行われます。このシステムの構成では、建物や部屋の入り口ではカードリーダーと PIN パッドを、出口ではカードリーダーのみを使用します。建物や部屋の出口でカードリーダーを使用することで、パスバック防止機能を提供し、許可のない人が許可のある人の後にぴったりついて、バッジなしで入場できないようにします。バッジを作成、印刷する機能はシステムで実行され、一部の中心的なセキュリティ担当者のみに制限されます。すべてのバッジは一定期間のみ有効になり、有効期限の延長には再承認が必要になります。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	MS-9	SOC 1（5.3、5.5） SOC 2（S3.3、S3.4、S5.3）	9.1.2 9.1.3 11.2	9.1	PE-2 PE-3 PE-7
PS.S-7.0	電子アクセス	レプリケーションとマスタリング用に別の部屋を設置します。						
PS-7.1	電子アクセス	電子アクセスシステムの管理操作は適切な担当者だけが行えるように制限します。						
PS-7.2	電子アクセス	未使用キーカードの在庫は施錠されたキャビネットに保管し、人員に割り当てられる前に有効にされることがないよう計らいます。						
PS-7.3	電子アクセス	キーカードを紛失した場合は、そのキーカードをシステム内で無効にしてから新しいキーカードを発行します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-7.4	電子アクセス	サードパーティにアクセスカードを発行する際は、規定に基づき有効期限付きで（例: 90 日間）発行します。						
PS-8.0	キー	マスターキーの配布対象を権限を持つ関係者（例: オーナー、施設管理者）のみに制限します。	施設のマスターキー管理手順を含む物理的セキュリティプロセスと手順は、AWS の物理保安要員が所有、管理、実施しています。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-8	SOC 1（5.5） SOC 2（S3.3、S3.4、S5.3）	7.1.1 9.1.2 9.1.3	9.1	PE-2 PE-3 CM-8
PS-8.1	キー	マスターキーの配布を追跡監視するチェックイン/チェックアウトプロセスを導入します。						
PS-8.2	キー	屋外への出入り口には、特定の錠前師だけが複製できるキーを使用します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-8.3	キー	四半期に 1 度、マスターキー、および施設出入り口など制限エリアへのキーの目録を作成します。						
PS-9.0	カメラ	施設のあらゆる出入り口と制限エリアを録画する CCTV システムを設置します。	物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員により、厳重に管理されています。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ（CCTV）カメラで録画されています。録画は 90 日間保存されます。ただし、法的または契約義務により 30 日間に制限される場合もあります。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-9	SOC 1（5.4） SOC 2（S3.3）	9.1.2 9.1.3 10.10.6	9.1	PE-2 PE-3 PE-6
PS.S-9.0	カメラ	カメラの位置決め、画像の品質、フレームレート、および保持について毎日確認します。						
PS-9.1	カメラ	監視フッテージのカメラの位置決め、画像の品質、照明条件、フレームレート、および適切な保持について少なくとも毎週確認します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-9.1	カメラ	稼働時間中に監視フッテージをモニタリングする従業員またはそのグループを任命し、セキュリティインシデントが検出された場合は即座に調査します。						
PS-9.2	カメラ	CCTV 制御盤と CCTV 装置（例: DVR）への物理的・論理的アクセスを、当該システムの管理/監視業務の責任者のみに制限します。						
PS-9.3	カメラ	カメラの録画映像に正確な日付時刻のタイムスタンプも記録されるようにします。						
PS-10.0	ロギングとモニタリング	制限エリアへの電子アクセスのログを取り、それを確認して、疑わしいイベントがないか確認します。	物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員により、厳重に管理されています。 AWS データセンターのすべての入り口は、メインエントランス、配送ドック、屋根の扉/ハッチを含めて、ドアを無理やり開けたり、開放したままにするとアラームが鳴り、AWS 集中物理セキュリティモニタリングでもアラームが作成される侵入検出デバイスで保護されています。	PS-10	SOC 1（5.3、5.5） SOC 2（S3.3、S3.4、S5.3）	10.10.2 10.10.3 13.1	9.1	AU-3 AU-6 AU-9 AU-11

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-10.0	ロギングとモニタリング	該当する場合は、次のエリアの電子アクセスログを毎週確認します。 • マスター/スタンプボールト • プレマスタリング • サーバー/マシン室 • スクラップルーム • 高セキュリティケージ	AWS データセンターでは、電子メカニズムに加えて、トレーニングを受けた警備員を建物内および周囲に毎日 24 時間常駐させています。すべてのアラームは警備員によって調査され、すべてのインシデントについて根本原因が記録されます。SLA に記載された時間内に対応が行われない場合、すべてのアラームは自動的にエスカレートするよう設定されています。 サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ（CCTV）カメラで録画されています。録画は 90 日間保存されます。ただし、法的または契約義務により 30 日間に制限される場合もあります。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。					
PS-10.1	ロギングとモニタリング	疑わしい電子アクセス活動が発見された場合にはこれを調査します。						
PS-10.2	ロギングとモニタリング	承認済みの電子アクセスインシデントすべてのログを継続的に取得し、フォローアップ活動を行った場合にはそのドキュメントも含めて保管します。						
PS-10.3	ロギングとモニタリング	CCTV 監視映像と電子アクセスログは、少なくとも 90 日間、または法律が認める最大限の期間、安全な場所に保管します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-11.0	検査	従業員およびサードパーティの従業員に対し、手荷物は無作為検査の対象になることを採用時に通知します。また、施設ポリシーに手荷物検査に関する条項を含めます。	AWS は AWS の物理的なセキュリティポリシーに従って、問題発生時にはバッグや手荷物の検査を行う権利を有します。 AWS の物理的なセキュリティメカニズムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-11		8.1.3		
PS.S-11.0	検査	すべての施設従業員と訪問者に対して、次を含む該当の出口検査プロセスを導入します。 • すべての上着、帽子、ベルトを取り外して検査 • ポケットの中身をすべて取り出す • セキュリティ担当者の監督下での身体検査の実行 • すべてのバッグの徹底した検査 • ノートパソコンの CD/DVD トレイの検査 • 検査対象の人から 3 インチ以内でのハンドヘルド金属探知機を使った検査						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-11.1	検査	デジタル記録デバイス（USB サムドライブ、デジタルカメラ、携帯電話など）を持って施設に出入りすることを禁止し、出口検査手順の一環としてこれらのデバイスの所持について検査します。						
PS.S-11.2	検査	生産エリアに食べ物を持ち込む場合は、透明なプラスチック袋や食品容器の使用を強制します。						
PS.S-11.3	検査	オーバーサイズの衣服（バギーパンツ、オーバーサイズのフード付きスウェットシャツなど）の着用を禁止するドレスコードポリシーを導入します。						
PS.S-11.4	検査	施設に持ち込み/持ち出しできる承認されたデバイスを識別するため、番号を付けた、不正開封の跡がすぐにわかるステッカー/ホログラムを使用します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-11.5	検査	出口検査手順をテストするプロセスを導入します。						
PS.S-11.6	検査	施設の駐車場を出る際に、ランダムに車両検査プロセスを実施します。						
PS.S-11.7	検査	機密性の高いコンテンツを処理するレプリケーションラインでエリアを分離し、分離エリアを出る際に検査を実施します。						
PS.S-11.8	検査	警備員の行動をモニタリングするための追加の管理を導入します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-12.0	在庫トラッキング	物理的資産（例: 顧客の資産や新規作成した資産）の詳細なトラッキング機能を持つコンテンツ資産管理システムを導入します。	コンテンツ資産管理は、AWS のお客様が所有、導入、運用します。物理資産の在庫追跡を導入するのは、お客様の責任です。 AWS データセンター環境では、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、構成要素など、データセンターに配送され、受け取られるすべての新しい情報システムコンポーネントについて、データセンターマネージャーへの通知と事前の承認が必要です。アイテムは各 AWS データセンターの配送ドックに届けられ、梱包の損傷または不正開封について検査された後で、AWS 正社員によって署名されます。アイテムは、配送到着時に AWS 資産管理システムおよびデバイス在庫追跡システムでスキャンされて登録されます。 受領されたアイテムは、データセンター内の機器保管室に配置され、データセンターのフロアに設置されるまで、アクセスにはスワイプバッジと PIN の組み合わせが必要になります。アイテムは、スキャン、追跡、殺菌され、承認を受けてデータセンターから出されます。 AWS 資産管理プロセスと手順は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-12		7.1 7.1.1 10.10.3 10.10.6 15.1.3	9.6 9.7	AU-9 AU-11 CM-8 MP-3
PS.S-12.0	在庫トラッキング	長時間ボールトを出たままの資産については自動通知を使用します。						
PS-12.1	在庫トラッキング	顧客資産と作成したメディア（テープ、ハードドライブなど）には受領時にバーコードを付け、使用しない時は保管庫に保管します。						
PS.S-12.1	在庫トラッキング	配送が時間どおりに行われなかったときに、遅延または返却されるアセットをロックして記録します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-12.2	在庫トラッキング	資産移動トランザクションログは最低 90 日間保持します。						
PS-12.3	在庫トラッキング	コンテンツ資産管理システムから取得したログを確認し、異状があれば調査します。						
PS-12.4	在庫トラッキング	資産トラッキングシステムでは、物理的資産に対し、適用できる場合にはスタジオ AKA（いわゆる別名）を使用します。						
PS-13.0	棚卸し	四半期に 1 度、棚卸しを実施します。各顧客について未公開プロジェクトの資産在庫数を数え、資産管理記録と照合し、不一致がある場合にはただちに顧客に連絡します。	お客様のデータと関連するメディア資産に対する統制と責任はお客様にあります。お客様の物理的資産に在庫トラッキングシステムを導入し監視を行うのはお客様の責任となります。 AWS 資産管理システムとデバイス在庫追跡システムでは、AWS データセンター情報システムコンポーネントの体系的な在庫が維持されます。在庫の	PS-13		7.1.1 10.1.3		AU-6 AC-5 IR-4 IR-5

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-13.0	棚卸し	週に 1 回、棚卸しを実施します。各顧客について未公開プロジェクトの資産在庫数を数え、資産管理記録と照合し、不一致がある場合にはただちに顧客に連絡します。	監査は定期的に行われ、FedRAMP[sm] コンプライアンスプログラムの一環として独立監査人によって確認されます。 AWS 資産管理プロセスと手順は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。					
PS-13.1	棚卸し	棚卸しの実施にあたっては、保管庫スタッフと棚卸し実施責任者たちがそれぞれ役割を分担します。						
PS.S-13.1	棚卸し	ワークフロープロセスを通じてフィルム要素（ネガ、未現像フィルムなど）を常時モニタリングします。						
PS-13.2	棚卸し	日別滞留資産表の作成と確認を行い、保管庫から持ち出されたまま戻されていない機密性の高い資産がないかどうかを確認します。						
PS-14.0	ブランクメディア/生フィルムのトラッキング	ブランクメディア/生フィルムには、受領した時点でタグ付けします（バーコードなど固有の識別子を割り当てます）。	AWS のお客様のデータとメディア資産に関する統制と所有権はお客様にあります。メディアストックのセキュリティの管理は、スタジオ/現像施設の責任です。	PS-14		7.1.1 10.7.1		MP-4 MP-2 PE-2 PE-3
PS.S-14.0	ブランクメディア/生フィルムのトラッキング	毎月、原材料（ポリカーボネートなど）の消費を追跡するプロセスを確立します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-14.1	ブランクメディア/生フィルムのトラッキング	ブランクメディア/生フィルムはセキュリティが確保された場所に保管します。						
PS-15.0	顧客の資産	完成した顧客の資産へのアクセスは、資産のトラッキングおよび管理の責任者のみに制限します。	完成した資産の物理的なコピーを検査/管理し、適切な物理的セキュリティが実装されていることを確認するのは、これらの人々の責任です。 MPAA PS-1～PS-14 に記載されているように、AWS はすべての AWS データセンターを通じて物理セキュリティプログラムおよび資産管理プログラムを運用します。これらは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] コンプライアンスプログラムの一環として、第三者の独立監査人によって定期的に確認および評価されます。	PS-15	SOC 1（5.3、5.5） SOC 2（S3.3、S3.4、S5.3）	7.1.1 9.1.2 10.7.1	9.1 9.6 9.7	MP-2 MP-4 PE-2 PE-3
PS.S-15.0	顧客の資産	稼働時間外に機密性の高いエリア（金庫、高セキュリティケージなど）の施錠を解除するには、別々のアクセスカードを持っている 2 社の従業員が必要です。						
PS-15.1	顧客の資産	顧客の資産はセキュリティが確保された制限エリア（例: 保管庫、金庫）に保管します。						
PS.S-15.1	顧客の資産	ステージングエリア用のアクセス管理されたケージを使用し、監視カメラでエリアをモニタリングします。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-15.2	顧客の資産	施設で一晩中維持されている、未配達荷物を保管する施錠された耐火金庫を使用します。						
PS.S-15.3	顧客の資産	未配達の荷物を保存して選別する、施錠され、アクセスが管理され、監視カメラまたは警備員（またはその両方）によってモニタリングされる専用の安全なエリア（セキュリティケージ、セキュリティで保護された部屋など）を導入します。						
PS-16.0	廃棄	返品された、損傷を受けた、または陳腐化した在庫については、必ず消去、消磁、シュレッド、または物理的破壊を施してから廃棄し（例: DVD ならシュレッド、ハードドライブなら破壊）、資産管理台帳に除却した事実を反映します。	AWS の処理手順には、AWS ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドラ イン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。廃棄されたストレージデバイスはすべて業界標準の方法に従って消磁され、物理的に破壊されます。 AWS ストレージデバイスの破棄プロセスは、継続中の ISO 27001 および FedRAMP[sm] コンプライアンスプログラムの一環として第三者の独立監査人によって定期的に確認および評価されます。	PS-16		9.2.6 10.7.2	9.10	MP-6
PS.S-16.0	廃棄	スクラップが破棄される場合に、スクラッププロセスをモニタリングおよび記録するためのセキュリティ担当者を必要とするプロセスを導入します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-16.1	廃棄	リサイクル/破棄処分予定の資産は、セキュリティの確保された場所/容器に保管し、処分前に複製または再利用されることを防ぎます。						
PS.S-16.1	廃棄	資産の破棄および破壊プロセス（資産を指定のコンテナに入れるなど）について、会社のすべての従業員とサードパーティの従業員に定期的なセキュリティトレーニングを実施します。						
PS-16.2	廃棄	資産の廃棄記録は少なくとも 12 か月間保管します。						
PS.S-16.2	廃棄	スクラップ容器に入れる前にディスクをスクラッチします。						
PS-16.3	廃棄	サードパーティ企業にコンテンツの廃棄を委託する場合は、1 件完了するごとに廃棄証明書の発行を義務付けます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-16.3	廃棄	（機械オペレーターの作業なしで）オートメーションを使用して、レプリケーションマシンから拒否されたディスクを直接スクラップ容器に移します。						
PS.S-16.4	廃棄	DCDM ドライブまたは公開前のコンテンツの破棄にサードパーティの企業を使用することを禁止します。						
PS-17.0	出荷	資産を施設外へ出荷するには有効な作業命令書/出荷命令書を提出して許可を受けるよう施設に義務付けます。	AWS データセンター環境では、サーバー、ラック、ネットワークデバイス、ハードドライブ、システムハードウェアコンポーネント、構成要素など、データセンターに配送され、受け取られるすべての新しい情報システムコンポーネントについて、データセンターマネージャーへの通知と事前の承認が必要です。アイテムは各 AWS データセンターの配送ドックに届けられ、梱包の損傷または不正開封について検査された後で、AWS 正社員によって署名されます。アイテムは、配送到着時に AWS 資産管理システムおよびデバイス在庫追跡システムでスキャンされて登録されます。 AWS 資産管理プロセスと手順は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、	PS-17		9.1.2 10.8.2 10.8.3	9.6 9.7	MP-5 AU-11 PE-16
PS.S-17.0	出荷	トラック運転手の情報用に別のログを記録、維持します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-17.1	出荷	資産の出荷情報をトラッキングし、ログを取ります。最低でも以下の項目については実施します。 • 出荷日時 • 出荷人の氏名と署名 • 受取人の氏名 • 宛先 • 運送会社が発行した追跡番号 • 対応する作業命令書への参照	監査中に外部の独立監査人によって確認されます。					
PS.S-17.1	出荷	出荷ドキュメントの数を確認し、出荷ポイントの署名を取得するために、荷物を取り出す担当者を必要とします。						
PS-17.2	出荷	有効な作業命令書/出荷命令書に基づく、施設からの資産持ち出しを承認します。						
PS.S-17.2	出荷	オンサイトで出荷が発生するときに、トレーラーの荷造りを確認、モニタリングします。						
PS-17.3	出荷	集荷待ちの資産のセキュリティを確保します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-17.3	出荷	施設間の出荷の移動時間、ルート、配送時間を記録、モニタリング、確認する正式なプロセスを導入します。						
PS-17.4	出荷	運送会社や宅配業者が施設のコンテンツ/制作エリアに入ることを禁じます。						
PS.S-17.4	出荷	署名された認証パスがある場合を除いて、フィルム要素が出荷以外の方法で施設から出ないようにします。						
PS.S-17.5	出荷	コマの劇場前上映用の出荷印刷（偶数のリール、奇数のリールなど）						
PS-18.0	入荷	コンテンツが納品されたら、受領時に検品を行い、受け入れ検査を実施し、積荷書類（梱包票やマニフェストなど）と照らし合わせます。	新しい情報システムコンポーネントが AWS データセンターで受領されると、データセンター内の機器保管室に配置され、データセンターのフロアに設置されるまで、アクセスにはスワイプバッジと PIN の組み合わせが必要になります。アイテムは、スキャン、追跡、殺菌され、承認を受けてデータセンターから出されます。 AWS 資産管理プロセスと手順は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-18		7.1 7.2 10.8.2 10.8.3	9.6 9.7	MP-3 MP-4 PE-16
PS-18.1	入荷	納品を受領した時に、担当者が入荷記録をつけるよう義務付けます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS-18.2	入荷	次の対応を速やかに行います。 • 受領した資産にタグ付けする（バーコードなど固有の識別子を割り当てる） • 資産を資産管理システムに入力する • 資産を制限エリア（例: 保管庫、金庫）に移動する						
PS-18.3	入荷	夜間に配達があった場合にセキュリティを確保するための設備（施錠できる宅配ボックスなど）を導入します。						
PS-19.0	ラベル貼り	梱包の表面に AKA（「別名」）などのタイトル情報を記載することは禁止します。	AWS 資産ラベルはお客様に依存せず、AWS 資産管理ツール内でハードウェアの在庫を維持するために利用されます。AWS データセンター内では、ハードウェアはお客様やハードウェアに保存されたデータとは物理的に関連付けられません。ソースを問わず、すべての顧客データは機密であると見なされ、すべてのメディアは重要であるものとして扱われます。 AWS 資産管理プロセスと手順は、PCI DSS、ISO 27001、および FedRAMP[sm] への準拠のため、監査中に外部の独立監査人によって確認されます。	PS-19		7.2	9.6 9.7	MP-3
PS-20.0	梱包	資産はすべて密封容器に入れて出荷し、資産価値によっては施錠できる容器を使用します。	物理的な完成メディア資産の梱包は、該当する配給組織（配給、DVD 制作、撮影後の編集に携わる企業など）の責任です。	PS-20		10.8.3		MP-5

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-20.0	梱包	すべての出荷物にシュリンクラップを施し、最終的な出荷の前に梱包を検査し、梱包が適切であることを確認します。						
PS-20.1	梱包	以下のコントロールから 1 つ以上を導入します。 • 途中で開封されたことが分かるテープ • 途中で開封されたことが分かる梱包 • 途中で開封されたことが分かるホログラム形式の封印 • セキュリティが確保できる容器（例: ダイアル錠付きのペリカンケース）						
PS-21.0	輸送車両	自動車やトラックは常にロックし、荷物は外から見えない場所に置きます。	物理的な完成メディア資産（DVD など）の配送は、該当する配給組織（配給、DVD 制作、撮影後の編集に携わる企業など）の責任です。	PS-21				MP-5
PS.S-21.0	輸送車両	運送車両（トレーラーなど）の次のセキュリティ機能を含みます。 • 車室（キャビン）からの分離 • 荷物室のドアをロック、封印できる機能 • セキュリティの高い配送のための GPS						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
PS.S-21.1	輸送車両	機密性の高いタイトルを出荷する場合に、荷室ドアに数字付きシールを貼り付けます。						
PS.S-21.2	輸送車両	高リスクエリアでの機密性の高いコンテンツの配送には、セキュリティエスコートの使用を要求します。						
DS-1.0	WAN	内部ネットワークへの不正アクセスを防止するために、アクセス制御リスト付きのステートフルインスペクションファイアウォールを用いて WAN をセグメント化します。	ルールセット、アクセスコントロールリスト（ACL）、および設定を使用してネットワークファブリック間で情報を流す境界保護デバイス。 Amazon には複数のネットワークファブリックが存在し、それぞれはファブリック間の情報の流れを制御するデバイスによって分離されています。ファブリック間の情報の流れは、それらのデバイスにあるアクセスコントロールリスト（ACL）として存在する承認された機関によって確立されます。これらのデバイスは、ACL の要求に従ってファブリック間の情報の流れを制御します。ACL は適切な従業員が定義、承認し、AWS ACL 管理ツールを使用して管理、デプロイされます。 Amazon の情報セキュリティチームがこれらの ACL を承認します。ネットワークファブリック間の承認されたファイアウォールルールセットとアクセスコントロールリストが、情報の流れを特定の情報システムサービスに制限します。アクセスコントロールリストとルールセットは確認、承認さ	DS-1	SOC 1（3.2、3.3、3.4、3.7、3.9、3.10、3.14、3.15、3.16） SOC 2（S.3.2、S3.4、S.3.5、S4.1、S.4.2、S4.3、S3.12）	11.1 11.4	1.1 1.2 1.3 1.4 2.2 6.6 8.5 11.2	AC-2 AC-3 CM-7
DS-1.1	WAN	ファイアウォールのアクセス制御リスト（ACL）を確認するプロセスを作成し、6 か月に 1 度、構成設定が適切であり事業の要件を満たすことを確認します。						
DS-1.2	WAN	WAN におけるデフォルト設定を deny all とし、セキュアなプロトコルのみを必要に応じて明示的に許可します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-1.3	WAN	外部からアクセス可能なサーバー（例: セキュア FTP サーバー、ウェブサーバー）を DMZ 内に配置します。	れ、定期的に（少なくとも 24 時間ごとに）境界保護デバイスに自動的にプッシュされて、ルールセットとアクセスコントロールリストが最新であることが確認されます。 AWS ネットワーク管理は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。 AWS は、そのインフラストラクチャコンポーネントを通じて最小権限を実装しています。また、特定のビジネス目的を持っていないすべてのポートとプロトコルを禁止しています。AWS は、デバイスの使用に不可欠な機能のみの最小実装という厳格な手法に従っています。ネットワークスキャンを実行し、不要なポートまたはプロトコルが使用されている場合は修正されます。 AWS 環境内のホストオペレーティングシステム、ウェブアプリケーション、およびデータベースでさまざまなツールを利用した、定期的な内外部の脆弱性のスキャンが実行されます。脆弱性のスキャンと解決手法は、AWS の PCI DSS および FedRAMP[sm] への継続的な準拠の一環として定期的に確認されます。					
DS-1.4	WAN	ネットワークインフラストラクチャデバイス（例: ファイアウォール、ルーター、スイッチなど）にパッチを適用するプロセスを定期的に実施します。						
DS-1.5	WAN	セキュリティ構成規格に基づいてネットワークインフラストラクチャデバイスを強化します。						
DS-1.6	WAN	コンテンツへのアクセスを制御する WAN ネットワークインフラストラクチャデバイス（例: ファイアウォール、ルーター）へのリモートアクセスは許可しません。						
DS-1.7	WAN	ネットワークインフラストラクチャデバイスのバックアップを、内部ネットワーク上のセキュアな集中管理サーバーに確保します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-1.8	WAN	年に 1 度、外部からアクセスが可能なホストに対して脆弱性スキャンを行い、問題を修復します。						
DS-1.9	WAN	通信サービスプロバイダによる接続の確立をリクエストすることは、権限を持つ担当者だけに許可します。						
DS-2.0	インターネット	デジタルコンテンツの処理や保存を行うシステム（デスクトップ/サーバー）へのインターネットアクセスを禁じます。	境界保護デバイスは、以下を拒否する deny-all モードで設定されます。 ルールセット、アクセスコントロールリスト（ACL）、および設定を使用してネットワークファブリック間で情報を流す境界保護デバイス。これらのデバイスは deny-all モードで構成され、接続を許可するには承認されたファイアウォールセットを必要とします。AWS ネットワークファイアウォールの管理の詳細については、DS-2.0 を参照してください。 AWS アセットに固有の E メール機能はなく、ポート 25 は利用されません。お客様（スタジオ、現像施設など）は、システムを利用して E メール機能をホストできますが、その場合、E メールの入出力ポイントで適切なレベルのスパムおよびマルウェア保護を採用し、新しいリリースが利用可能	DS-2	SOC 1（3.2、3.3、3.4、3.7、3.9、3.10、3.14、3.15、3.16） SOC 2（S.3.2、S3.4、S.3.5、S4.1、S.4.2、S4.3、S3.12）	7.1.3 11.2.2	1.1 1.2 1.3 1.4 2.2 5.1 6.6 8.5 11.2	CA-3 PL-4

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-2.1	インターネット	本稼働以外のネットワークから次のものをブロックする E メールフィルタリングソフトウェアまたはアプライアンスを導入します。 • フィッシングの疑いがある E メール • 禁止された添付ファイル（例: Visual Basic スクリプト、実行可能ファイルなど） • サイズが 10 MB の上限を超えるファイル	になったらスパムとマルウェアの定義を更新するのはお客様の責任です。 Amazon の資産（ノートパソコンなど）は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。					
DS-2.2	インターネット	ウェブフィルタリングソフトウェアまたはアプライアンスを導入し、ピアツーピアでのファイル交換、ウイルス、ハッキングなど、悪意あるサイトとして知られるウェブサイトへのアクセスを制限します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-3.0	LAN	コンテンツ/制作ネットワークを、制作作業にかかわらないネットワーク（オフィスネットワークや DMZ など）から隔離します。これには、物理的または論理的ネットワークセグメンテーションを使用します。	AWS はネットワークをセグメント化し、管理する機能をお客様に提供しますが、これらのセグメント化された環境の実装と運用については義務を負いません。	DS-3		11.2 11.4.2 11.4.4 10.6.2 10.10		AC-6 AC-17 CM-7 SI-4
DS-3.1	LAN	コンテンツ/制作システムには権限を持つ人間だけがアクセスできるように制限します。						
DS-3.2	LAN	コンテンツ/制作ネットワークへのリモートアクセスは、職務上の責任を果たすためにアクセスを必要とする担当者にのみに制限します。						
DS-3.3	LAN	コンテンツ/制作ネットワーク上の使用していないスイッチポートをすべて無効化し、不正デバイスによるパケット盗聴を防止します。						
DS-3.4	LAN	コンテンツ/制作ネットワーク上のハブやリピーターなどの非スイッチ型デバイスの使用を制限します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-3.5	LAN	コンテンツ/制作ネットワーク内のコンピュータシステムへのデュアルホームネットワーキング（ネットワークブリッジング）を禁止します。						
DS-3.6	LAN	コンテンツ/制作ネットワークに、ネットワークベースの侵入検知または防止システムを導入します。						
DS-4.0	ワイヤレス	コンテンツ/制作ネットワークでのワイヤレスネットワーク接続およびワイヤレスデバイスの使用を禁じます。	AWS アセットに固有のワイヤレス機能はありません。 Amazon 資産（ノートパソコンなど）のワイヤレス機能は、業界標準の安全なワイヤレス設定基準に従って実装、運用されています。Amazon は問題のデバイスを検出するため、継続的にワイヤレスネットワークをモニタリングしています。	DS-4		10.6.1 12.6	11.1	AC-18 SI-4

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-4.1	ワイヤレス	次のセキュリティ管理で、本稼働以外のワイヤレスネットワーク（管理ネットワークやゲストネットワークなど）を設定します。 • WEP を無効化 • AES 暗号化を有効化 • "ゲスト" ネットワークを会社の他のネットワークから分離	AWS のワイヤレスネットワーク管理は、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。					
DS-4.2	ワイヤレス	不正ワイヤレスアクセスポイントをスキャンするプロセスを年に 1 回実施します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-5.0	I/O デバイスセキュリティ	コンテンツの入出力（I/O）には特定のシステムを使用します。	AWS は、システム出力デバイスへのアクセスを、権限を持つ関係者のみに制限しています。認証を取得するアクセスでは、電子リクエストを提出し、アクセスのビジネスケースを提示して、承認された承認者によるその認証の文書による承認を取得する必要があります。AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への継続的な準拠の一環として、第三者の監査人によって個別に確認されます。 個人の電子デバイスやリムーバブルメディアは、AWS 情報システムに接続することが禁止されています。	DS-5	SOC 1（2.1、5.1） SOC 2（S.3.2、S3.3、S.3.4）	10.7.1 10.10.2	7.1 8.2	MP-2 AC-19 PE-5
DS-5.1	I/O デバイスセキュリティ	入出力（I/O）デバイス（例: USB、FireWire、e-SATA、SCSI など）は、コンテンツ I/O として使用するシステムを除き、コンテンツを取り扱い保存するすべてのシステムから遮断します。						
DS-5.2	I/O デバイスセキュリティ	メディアバーナー（例: DVD、Blu-ray、CD バーナー）など、コンテンツの物理メディアへの出力に使用する I/O 専用システムに出力することのできるデバイス全般の設置や使用を制限します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.0	システムセキュリティ	すべてのワークステーションとサーバーにアンチウイルスソフトウェアをインストールします。	AWS 環境内で、パッケージのデプロイ可能なソフトウェア、パッケージグループ、および環境の管理に使用される設定管理ツール。パッケージは、ソフトウェア、コンテンツなど、緊密に関係している関連ファイルの集まりです。パッケージグループは、よく一緒にデプロイされるパッケージのセットです。環境は、ホストクラスのセット（同じ機能を備えたホストまたはサーバー）にデプロイされるパッケージまたはパッケージグループのセットの組み合わせです。環境は、特定の機能をサーバーが満たすために必要なパッケージの完全なセットを表します。 AWS は、ホストで使用されるベースライン OS ディストリビューションを維持します。不要なすべてのポート、プロトコル、およびサービスはベースビルドで無効になります。サービスチームはビルドツールを使用して、ツールで維持されている設定ベースラインに従ってサーバーが機能するために必要な、承認済みソフトウェアパッケージのみを追加します。 サーバーは定期的にスキャンされ、不要なポートまたはプロトコルが使用されている場合は、不具合修正プロセスを使用して修正されます。デプロイされたソフトウェアは、慎重に選定された業界の専門家によって実行される定期的な侵入テストを受けます。また、侵入テストの修正は、不具合修正プロセスを通じてベースラインに組み込まれます。 Amazon 情報セキュリティチームと AWS セキュリティチームは、Secunia および TELUS セキュリティラボから、アプリケーションベンダーの不具合に関するニュースフィードを購読しています。AWS 情報セキュリティチームは、積極的にベンダーの	DS-4		10.4.1 10.1.3 10.8.2 11.3.2 11.4.3 11.4.4		SI-3 SI-2 RA-5 AC-5 SC-2 PE-3 MA-4 PE-5 SA-7 SA-6
DS-6.1	システムセキュリティ	アンチウイルスソフトウェアの定義ファイルを毎日更新します。						
DS-6.2	システムセキュリティ	ファイルベースのコンテンツにはウイルススキャンを行い、コンテンツ/制作ネットワークへの侵入を未然に防ぎます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.3	システムセキュリティ	次のようにウイルススキャンを実行します。 • すべてのワークステーションにおいて、システム全体に対するウイルススキャンを定期的に実施します。 • 非 SAN システムなど、適用可能なサーバーにはシステム全体に対するウイルススキャンを実施します。	ウェブサイトやその他の関連する販売経路を監視して、新しいパッチの有無を確認しています。パッチは、実装前にセキュリティと運用上の影響について評価され、評価に基づいてタイムリーに適用されます。 Amazon の資産（ノートパソコンなど）は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS 設定管理および不具合修正プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によってすべて確認されます。					
DS-6.4	システムセキュリティ	セキュリティの脆弱性を修正するパッチ/更新プログラムで、定期的にシステム（ファイル転送システム、オペレーティングシステム、データベース、アプリケーション、ネットワークデバイス）を更新するプロセスを実装します。						
DS-6.5	システムセキュリティ	ユーザが自分のワークステーションの管理者になることを禁じます。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.6	システムセキュリティ	コンテンツを取り扱う、持ち運び可能なコンピューティングデバイス（例: ラップトップ、タブレット、タワー型パソコン）を置いたまま席を外す場合はケーブルロックを使用します。						
DS-6.7	システムセキュリティ	コンテンツを取り扱う、持ち運び可能なコンピューティングデバイスにはすべて、遠隔消去ソフトウェアをインストールし、ハードドライブなどのストレージデバイスを遠隔ワイプできるようにします。						
DS-6.8	システムセキュリティ	ソフトウェアのインストール権限を承認されたユーザーに制限します。						
DS-6.9	システムセキュリティ	システムのセットアップを組織内部で行う場合のセキュリティベースラインおよび基準を制定します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-6.10	システムセキュリティ	コンテンツ転送サーバーから不要なサービスやアプリケーションをアンインストールします。						
DS-7.0	アカウント管理	コンテンツを取り扱うすべての情報システムとアプリケーションについて、管理者、ユーザー、サービスアカウントに対するアカウント管理プロセスを作成し、実施します。	AWS には、毎年（またはポリシーに影響するシステムへの大きな変更が発生したときに）確認、更新される正式なアクセスコントロールポリシーがあります。このポリシーでは、目的、範囲、役割、責任、および管理コミットメントについて取り上げています。 AWS は最小権限という概念を導入しており、ユーザーがジョブ機能を実行するために必要最小限のアクセスを許可しています。ユーザーアカウントの作成では、最小アクセス権を持つユーザーアカウントが作成されます。これらの最小権限を超えるアクセスには、適切な認証が必要になります。 AWS システムおよびデバイスの承認されたユーザーは、認証されたユーザーのジョブ機能と役割に固有のグループメンバーシップを通じて、アクセス権限が与えられます。グループメンバーシップの条件は、グループ所有者が作成、確認します。ユーザー、グループ、およびシステムアカウントにはすべて一意の ID があり、再利用されません。ゲスト/匿名および一時アカウントは使用されず、デバイスでは許可されません。 ユーザーアカウントは少なくとも四半期ごとに確	DS-7	SOC 1（2.1、2.2） SOC 2（S.3.2、S.3.4）	10.1.3 10.10.4 11.2 11.2.1 11.2.2 11.2.4	7.1 8.1 8.2	AC-2 AC-5 AC-6 AU-2 AU-12 IA-4 PS-4 PS-5 PE-2

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-7.1	アカウント管理	アカウント管理活動のトレース可能な証拠（例: 承認の E メール、変更リクエストフォーム）を維持します。	認されます。四半期ごとに、すべてのグループ所有者は必要に応じて、グループメンバーシップを必要としなくなったユーザーを確認して削除します。この確認は、AWS アカウント管理ツールによってグループ所有者に送信されたシステム通知によって開始されます。この通知では、グループのベースラインを実行するようグループ所有者に伝えます。ベースラインは、グループ所有者によるアクセス権限の完全な再評価です。ベースラインが期限までに完了しない場合、すべてのグループメンバーが削除されます。ユーザーアカウントは、90 日アクティビティがないとシステムによって自動的に無効になります。 AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。 AWS アクセス管理の手順は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。					
DS-7.2	アカウント管理	必ず必要な関係者にのみ権限を与える原則に基づき、知る必要性を持つ人だけに固有の認証情報を割り当てます。						
DS-7.3	アカウント管理	デフォルト管理者アカウントの名前を変更し、このアカウントの使用は認証情報を必要とする特殊な状況（オペレーティングシステムの更新、パッチのインストール、ソフトウェアの更新など）のみに制限します。						
DS-7.4	アカウント管理	役割を分担して、情報システムへのアクセスを割り当てる責任者自身がそのシステムのエンドユーザにならないようにします（自分自身にアクセスを割り当てられる人員がいてはいけません）。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-7.5	アカウント管理	管理者アカウントおよびサービスアカウントの活動をモニターし、監査します。						
DS-7.6	アカウント管理	コンテンツを取り扱うすべての情報システムについてユーザアクセスを確認するプロセスを実施し、四半期に 1 度、アクセスが不要になったユーザアカウントを削除します。						
DS-7.7	アカウント管理	プロジェクトベースでコンテンツへのユーザーアクセスを確認します。						
DS-7.8	アカウント管理	技術的に可能な場合は、コンテンツを処理するシステムローカルアカウントを無効化または削除します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-8.0	認証	情報システムへのアクセスには一意のユーザ名とパスワードを使用するように徹底します。	AWS 人事管理システムのオンボーディングワークフロープロセスの一環として、一意のユーザー ID が作成されます。デバイスプロビジョニングプロセスは、デバイスの ID を確実に一意にするうえで役立ちます。両方のプロセスとも、ユーザーアカウントまたはデバイスを確立するためのマネージャーの承認が含まれます。最初の認証は、プロビジョニングプロセスの一部としてユーザーに対面で提供されるとともに、デバイスにも提供されます。内部ユーザーは SSH パブリックキーをアカウントに関連付けることができます。システムカウントの認証は、リクエスタの ID を確認した後で、アカウント作成プロセスの一部としてリクエスタに提供されます。AWS により、認証の最小強度が定義されます。これにはパスワードの長さが含まれ、複雑なパスワード、パスワードの有効期限の要件、コンテンツ、および SSH キーの最小ビット長が必要です。 AWS パスワードポリシーと実装は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	DS-8	SOC 1（2.5） SOC 2（S.3.2、S.3.4）	11.2.1 11.2.3 11.4.2 11.5.2	8.4 8.5	IA-2 IA-4 IA-5 AC-7 AC-11 AC-17
DS-8.1	認証	情報システムへのアクセスを得るためのパスワードポリシーを強力なものにします。						
DS-8.2	認証	ネットワークへのリモートアクセス（VPN など）には 2 要素認証（ユーザー名/パスワード、ハードトークンなど）を実装します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-8.3	認証	サーバーとワークステーションには、パスワードで保護されたスクリーンセーバーまたはスクリーンロックソフトウェアを実装します。						
DS-9.0	ロギングとモニタリング	セキュリティイベントの記録と報告を行うリアルタイムロギング・レポーティングシステムを実装し、少なくとも以下の情報を収集します。 • いつ（タイムスタンプ） • どこで（ソース） • 誰が（ユーザ名） • 何を（コンテンツ）	AWS は AWS システム内でシステムとデバイス間で監査可能なイベントカテゴリを識別しています。サービスチームは監査機能を設定して、要件に従って継続的にセキュリティ関連イベントを記録しています。ログストレージシステムは、ログストレージの次のニーズが発生すると自動的に容量を増やす、スケーラブルで高可用性のサービスを提供するように設計されています。監査記録には、必要な分析要件をサポートするために、データ要素のセットが含まれます。さらに AWS セキュリティチームまたはその他の適切なチームは、要求時に検査または分析を実行するため、またはセキュリティ関連のイベントやビジネスに影響するイベントに応じて、監査記録を使用できます。	DS-9	SOC 1 （3.6）	10.1 10.10.2 10.10.5	10.1 10.2 10.3	AU-1 AU-2 AU-3 AU-6 SI-4
DS.S-9.0	ロギングとモニタリング	すべてのシステムで、次の目的で使用されるログメカニズムを実装します。 • キーの生成 • キーの管理 • ベンダー証明書の管理	AWS チームの指定された関係者は、監査処理が失敗した場合に、自動化されたアラートを受け取ります。監査処理の失敗には、ソフトウェア/ハードウェアのエラーなどが含まれます。オンコール担当者は、アラートを受け取るとトラブルチケットを発行し、解決されるまでイベントを追跡します。					

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-9.1	ロギングとモニタリング	インシデントへの能動的な対応を容易にするために、ロギングシステムはセキュリティイベントが検出された場合に自動で通知を送信する構成にします。	AWS のログおよびモニタリングプロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。					
DS-9.2	ロギングとモニタリング	ロギング・レポーティングシステムから報告された異常な活動を調査します。						
DS-9.3	ロギングとモニタリング	ログは週に 1 度確認します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-9.4	ロギングとモニタリング	内部または外部のコンテンツの移動と転送のログを有効にし、最低でも次の情報を含めます。 • ユーザー名 • タイムスタンプ • ファイル名 • 送信元 IP アドレス • 送信先 IP アドレス • イベント（例: ダウンロード、表示）						
DS-9.5	ロギングとモニタリング	ログは少なくとも 6 か月間保持します。						
DS-9.6	ロギングとモニタリング	ログへのアクセスは適切な関係者のみに制限します。						
DS-9.7	ロギングとモニタリング	アウトバウンドのコンテンツ転送を行う時は、制作コーディネータへ自動的に通知を送信します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-10.0	セキュリティテクニック	セキュリティテクニック（例: スポイリング、不可視/可視透かし）が利用可能な場合、指示を受けた時に実行できるようにします。	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用できるようにしています。VPC セッションも暗号化されます。 AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。	DS-10		7.2.2 12.3.1 12.3.2	3.4.1	IA-5 SC-9 SC-12 SC-13
DS.S-10.0	高度なセキュリティ手法	次に対応するキー管理プロセスを実装します。 • 信頼されたデバイスの承認と失効 • コンテンツキーの生成、更新、および失効 • コンテンツキーの内部および外部への配布						
DS-10.1	セキュリティテクニック	次のいずれかの方法により、最低でも AES 128 ビット暗号化を使用してハードドライブのコンテンツを暗号化します。 • ファイルベースの暗号化（コンテンツそのものの暗号化） • ドライブベースの暗号化（ハードドライブの暗号化）						
DS.S-10.1	高度なセキュリティ手法	信頼されたデバイスリスト（TDL）のデバイスが、権限所有者の承認に基づく適切なものであることを確認します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-10.2	セキュリティテクニック	復号キーやパスワードを送信する際に、帯域外通信プロトコルを用います（コンテンツ自体と同じストレージメディア上にない）。						
DS.S-10.2	高度なセキュリティ手法	コンテンツキーの有効期間を確認し、有効期限日がクライアントの指示に従うようにします。						
DS-11.0	転送ツール	コンテンツ転送セッションにアクセス制御および最低でも AES 128 ビット暗号化と強力な認証を使用する転送ツールを導入します。	AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用できるようにしています。VPC セッションも暗号化されます。 AWS 接続では、FIPS 承認のハッシュを使用できます。AWS は、API エンドポイント、VPC IPSEC VPN、IAM、MFA ハードウェアトークン、SSH の各アクセス方法を通じてユーザー認証の暗号化モジュールを利用しています。	DS-11	SOC 1（4.1、4.2、4.3） SOC 2（S.3.6）	12.3.1	3.4.1	IA-5 SC-13
DS-11.1	転送ツール	暗号化転送ツールを使用しない例外プロセスは、必ず顧客から事前に書面による承認を得た上で実施します。						
DS-12.0	転送デバイス方法	コンテンツ転送には専用のシステムを実装・使用します。	AWS はネットワークをセグメント化し、管理する機能をお客様に提供しますが、これらのセグメント化された環境の実装と運用については義務を負いません。	DS-12		10.7.1 10.8 11.4.5		AC-4 AC-20 SC-7
DS-12.1	転送デバイス方法	コンテンツの保存や処理を行うシステムから、また制作に関連しないネットワークから、それぞれファイルを転送するための専用システムをセグメント化します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-12.2	転送デバイス方法	コンテンツ受け渡しシステムは非武装地帯（DMZ）に配置し、コンテンツ/実稼働ネットワークには配置しません。						
DS-12.3	転送デバイス方法	送受信が完了したら、ただちにコンテンツ転送デバイスからコンテンツを削除します。						
DS-13.0	クライアントポータル	コンテンツの転送、コンテンツのストリーミング、キーの配布に使用するウェブポータルへのアクセスは、権限を持つユーザーのみに制限します。	AWS では、お客様がクライアントポータルを作成および管理できるようにします。AWS はお客様に代わってこのポータルを実装または管理しません。	DS-13		11.2.2 11.2.4 11.3.2 11.4.5 11.4.7 12.6.1		AC-2 AC-3 AC-4 AC-6 AC-20 IA-5 RA-3 RA-5 SC-10

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-13.1	クライアントポータル	ポータルのユーザーに個別の認証情報を割り当て、認証情報をクライアントに安全に配信します。						
DS-13.2	クライアントポータル	ユーザーが自身のデジタル資産にだけアクセスできることを確認します（顧客 A が顧客 B のコンテンツにアクセスできることがあってはいけません）。						
DS-13.3	クライアントポータル	DMZ 内の専用サーバーにウェブポータルを置き、アクセスを特定 IP およびプロトコルとのやりとりのみに制限します。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-13.4	クライアントポータル	クライアントで承認されない限り、インターネットウェブサーバーでホストされるサードパーティの実稼働追跡ソフトウェアの使用を禁止します。						
DS-13.5	クライアントポータル	内部用/外部用ウェブポータルに HTTPS を使用し、強力な暗号化方式（SSLv3 や TLS v1）の使用を徹底します。						
DS-13.6	クライアントポータル	永続的なクッキーや、認証情報を平文で格納するクッキーは使用しません。						
DS-13.7	クライアントポータル	内部用/外部用ポータル上のコンテンツへのアクセスは、可能な限り事前に定義した期限で自動的に失効するよう設定します。						
DS-13.8	クライアントポータル	年に 1 度、ウェブアプリケーションの脆弱性をテストします。						

いいえ。	セキュリティトピック	ベストプラクティス	AWS 実装	MPAA	AWS SOC	ISO 27002*	PCI	NIST 800-53*
DS-13.9	クライアントポータル	通信サービスプロバイダによる接続の確立をリクエストすることは、権限を持つ担当者だけに許可します。						
DS-13.10	クライアントポータル	制作にかかわらないネットワークからの E メール（ウェブメールを含む）を使用したコンテンツの転送を禁じ、例外ポリシーを使用して例外を管理します。						
DS-13.11	クライアントポータル	少なくとも四半期に 1 度、クライアントウェブポータルへのアクセスを確認します。						

付録 C:オーストラリア信号局（ASD）のクラウドコンピューティングに関するセキュリティ上の考慮事項への AWS の準拠

クラウドコンピューティングに関するセキュリティ上の考慮事項は、クラウドサービスプロバイダが提供するサービスのリスク評価を機関が行うための支援となるように作成されました。ここでは、2012 年 9 月に発行されたセキュリティ上の考慮事項への AWS の準拠について示します。詳細については、http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf を参照してください。

主要な領域	質問	AWS の回答
高可用性および事業継続性の維持	a. 事業におけるデータまたは機能の重要性。ビジネスクリティカルなデータまたは機能をクラウドに移行するのですか?	AWS のお客様は、お客様のコンテンツの統制と所有権を維持します。お客様のコンテンツの分類と使用については、お客様が責任を負うものとします。
	b. ベンダーの事業継続性および災害復旧の計画。当社のデータおよび当社が使用しているベンダーのサービスの両方について、可用性と復旧に関するベンダーの事業継続性および災害復旧の計画のコピーを詳細に確認することはできますか? 災害後に、当社のデータと使用しているサービスが復旧するまでにどのくらいの時間がかかりますか? 当社より規模が大きく、より高額の料金を支払っている、ベンダーの他の顧客は優先されるのですか?	AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。 AWS SOC 1 Type 2 レポートに詳細情報が記載されています。ISO 27001 基準の付録 A、ドメイン 11.2 に詳細が記載されています。AWS は独立監査人により ISO 27001 規格に準拠している旨の審査と認証を受けています。 お客様は、AWS を利用すると、予備の物理データセンターのインフラストラクチャ費用を発生させることなく、重要な IT システムの迅速な復旧が可能になります。AWS クラウドでは、一般的な災害復旧（DR）アーキテクチャの多くがサポートされています。例えば、「パイロットライト」環境では瞬時にスケールアップが可能であり、「ホットスタンバイ」環境では高速フェイルオーバーが可能です。AWS の災害復旧の詳細については、http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf を参照してください。 AWS は、堅牢な継続性計画を実装する機能をお客様に提供しています。例えば、頻繁なサーバーインスタンスバックアップの利用、データの冗長レプリケーション、マルチリージョン/アベイラビリティーゾーンのデプロイアーキテクチャなどです。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。障害時には、自動プロセスが、顧客データを影響を受けるエリアから移動します。 AWS のデータセンターは、環境リスクに対する物理的な保護を組み込んでいます。環境リスクに対する AWS の物理的な保護は、独立監査人によって検証され、ISO 27002 のベストプラクティスに準拠していると認定されました。詳細については、ISO 27001 規格の附属書 A、ドメイン 9.1 および AWS SOC 1 Type II レポートを参照してください。

主要な領域	質問	AWS の回答
	c. データのバックアップ計画。機関の施設、または最初のベンダーの一般的な障害点を持たない 2 番目のベンダーにデータの最新のバックアップコピーを維持するには、追加の料金がかかりますか?	AWS のお客様は、お客様のコンテンツの統制と所有権を有していますので、データのバックアッププランを管理するのはお客様の責任です。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。Amazon S3 サービスはデータ損失の可能性をほぼ 0% にまで低減する設計になっており、データストレージの冗長化によってデータオブジェクトのマルチサイトコピーに匹敵する永続性を実現しています。データの永続性と冗長性については、AWS のウェブサイトをご覧ください。 AWS は、災害復旧をサポートするためにさまざまなクラウドコンピューティングサービスを提供しています。AWS の災害復旧の詳細については、http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf を参照してください。
	d. 当社の事業継続性および災害復旧の計画。別のデータセンターを使用し、理想的には最初のベンダーの一般的な障害点を持たない 2 番目のベンダーにデータやビジネス機能をレプリケートするには、追加の料金がかかりますか? できれば、このレプリケーションは、自動的に "フェイルオーバー" するよう設定し、1 つのベンダーのサービスを使用できなくなった場合に、もう 1 つのベンダーにコントロールが自動的かつスムーズに移行するようにしたいと考えています。	お客様は、お客様のデータの統制と所有権を保持します。お客様は、AMI をエクスポートして、施設内または別のプロバイダで使用できます（ただし、ソフトウェアのライセンス制限に従います）。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。 AWS データセンターは、世界のさまざまなリージョンにクラスター化されて構築されています。すべてのデータセンターはオンラインでお客様にサービスを提供しており、「コールド」状態のデータセンターは存在しません。障害時には、自動プロセスにより、顧客データが影響を受けるエリアから移動されます。重要なアプリケーションは N+1 原則でデプロイされます。そのためデータセンターの障害時でも、トラフィックが残りのサイトに負荷を分散させるのに十分な能力が存在することになります。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。各アベイラビリティーゾーンは、独立した障害ゾーンとして設計されています。つまり、アベイラビリティゾーンは、一般的な都市地域内で物理的に分離されており、洪水の影響が及ばないような場所にあります（洪水地域の分類はリージョンによって異なります）。個別の無停電電源装置（UPS）やオンサイトのバックアップ生成施設に加え、シングルポイントの障害の可能性を減らすために、別々の電力供給施設から異なる配管網を経由して、個別に電力供給を行っています。これらはすべて、冗長的に、複数の Tier-1 プロバイ

主要な領域	質問	AWS の回答
		ダに接続されています。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。 AWS SOC 1 Type 2 レポートに詳細情報が記載されています。ISO 27001 基準の付録 A、ドメイン 11.2 に詳細が記載されています。AWS は独立監査人により ISO 27001 規格に準拠している旨の審査と認証を受けています。
	e. クラウドへのネットワーク接続。機関のユーザーとベンダーのネットワーク間のネットワーク接続は、可用性、トラフィックのスループット（帯域幅）、遅延（レイテンシー）、およびパケット損失の観点で適切ですか。	お客様は、各 AWS リージョンの複数の VPN エンドポイントを含めて、AWS 施設へのネットワークパスを選択することもできます。さらに、AWS Direct Connect により、施設から AWS への専用ネットワーク接続を簡単に確立することができます。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコストを削減する、帯域幅のスループットを向上させる、インターネットベースの接続よりも一貫性のあるネットワークの体験を提供することができます。 詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
	f. ベンダーの可用性の保証。サービスレベル利用規約（SLA）では、ベンダーが堅牢なシステムアーキテクチャとビジネスプロセスを使用して、適切なシステム可用性とサービス品質を提供することが保証されますか?	AWS は、サービスレベルアグリーメント（SLA） で高レベルの可用性を確約しています。例えば、Amazon EC2 は、1 年のサービス期間で 99.95% 以上の稼働時間を確約しています。Amazon S3 は毎月 99.99% 以上の稼働時間を確約しています。こうした可用性の評価指標が基準に満たない場合は、サービスクレジットが提供されます。 顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。複数のアベイラビリティゾーンにアプリケーションを配信することによって、自然災害やシステム障害など、ほとんどの障害モードに対して、その可用性を保つことができます。 AWS は、自動モニタリングシステムを活用して、ハイレベルなサービスパフォーマンスと可用性を提供します。内部的、外部的両方の使用において、様々なオンラインツールを用いた積極的モニタリングが可能です。AWS 内のシステムには膨大な装置が備わっており、主要なオペレーションメトリックをモニタリングしています。重要計測値が早期警戒しきい値を超える場合に運用管理担当者に自動的に通知されるよう、アラームが設定されています。オンコールスケジュールが採用されているので、担当者が運用上の問題にいつでも対応できます。ポケットベルシステムがサポートされ、アラームが迅速かつ確実に運用担当者に届きます。 AWS ネットワーク管理は、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠の一環として、第三者の独立監査人によって定期的に確認されます。

主要な領域	質問	AWS の回答
	g. 機能停止の影響。SLA で想定される最大ダウンタイムは許容できますか? スケジュールされた機能停止枠は、長さと時間帯の両方について許容できますか? またはスケジュールされた機能停止によって重要なビジネスプロセスに問題が生じますか?	AWS では、定期的な保守やシステムのパッチ適用を実行するために、システムをオフラインにする必要がありません。通常、AWS の保守およびシステムのパッチ適用はお客様に影響がありません。インスタンスの保守自体は、お客様が統制します。
	h. SLA に含まれるスケジュールされた機能停止。SLA で保証された可用性の割合には、スケジュールされた機能停止が含まれますか?	AWS は、お客様が複数のアベイラビリティーゾーンとリージョンを活用する環境を構築できるようにしており、スケジュールされた機能停止が発生する環境は運用していません。
	i. SLA の補償。SLA には、スケジュールされていないダウンタイムやデータ損失など、SLA の違反によって発生した実際の損害に関する適切な条項がありますか?	AWS は、AWS のサービスレベルアグリーメント（SLA）に従い、機能停止によって発生する可能性がある損失について、お客様に賠償を提供しています。

主要な領域	質問	AWS の回答
	j. データの完全性および可用性。ベンダーはどのようにして、 冗長性やオフサイトバックアップといったメカニズムを実装してデータの破損や損失を防ぎ、 データの整合性と可用性の両方を保証していますか?	AWS のデータ整合性統制は AWS SOC 1 Type II レポートに記載されているように、送信、保存、および処理を含むすべての段階でデータの整合性が維持される妥当な保証を提供しています。 また、詳細については、ISO 27001 基準の付録 A、ドメイン 12.2 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。 データセンターは、世界各地にクラスターの状態で構築されています。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。顧客は AWS の使用量を計画しながら、複数のリージョンやアベイラビリティーゾーンを利用する必要があります。 リージョンを指定する（Amazon S3 の場合）か、リージョン内のアベイラビリティーゾーンを指定する（EBS の場合）ことで、データを保管する場所を選択します。Amazon EBS に保存されるデータは、これらのサービスの通常オペレーションの一部として、複数の物理的ロケーションで冗長的に保存されます。追加費用はかかりません。ただし、Amazon EBS レプリケーションは複数のゾーンにまたがるのではなく同じアベイラビリティーゾーンに保存されます。 Amazon S3 は極めて堅牢性の高いストレージインフラストラクチャを提供しています。オブジェクトは冗長化のため、同一の Amazon S3 リージョン内の複数施設に分散した複数のデバイスに保存されます。一旦格納されると、Amazon S3 は冗長性が失われた場合にすばやく検出して修復することによってオブジェクトの堅牢性を維持します。Amazon S3 は、チェックサムを用いて、格納されているデータの完全性を定期的に検証しています。破損が検出されると、冗長データを使用して修復されます。S3 に保存されるデータは、1 年間にオブジェクトの 99.999999999% の堅牢性と 99.9% の可用性を提供するよう設計されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
	k. データの復元。ファイル、E メール、またはその他のデータを誤って削除した場合、 バックアップからデータが部分的または完全に復元されるまでにどのくらいの時間がかかり、 許容される最大時間 は SLA に記載されていますか?	AWS のお客様は、お客様のデータの統制と所有権を保持します。AWS は、各リージョン内の複数のアベイラビリティーゾーンだけでなく、複数の地理的リージョン内で、インスタンスを配置してデータを保管する柔軟性をお客様に提供します。
	l. スケーラビリティ。ベンダーのサービスの使用を短期の通知でスケールできるようにするためにベンダー	AWS クラウドは分散され、セキュリティと復元力が高いので、潜在的に大きな拡張性があります。お客様は、使用内容に対する料金のみを支払って、拡張または縮小できます。

主要な領域	質問	AWS の回答
	が提供する予備のコンピューティングリソースの量は、どれくらいですか?	
	m. ベンダーの変更。データを機関または別のベンダーに移動する場合や、ベンダーが突然破産したりクラウドビジネスを終了した場合に、ベンダーのロックインを回避するためにベンダーに依存しない形式でデータにアクセスするにはどうすればよいですか? ベンダーはどれくらい協力的ですか? ベンダーのストレージメディアからデータが完全に削除されることをどのようにして確認できますか? Platform as a Service では、アプリケーションを別のベンダーまたは機関に簡単に移動するポータビリティと相互運用性を提供するために、ベンダーはどのような標準を使用していますか?	お客様は、お客様のデータの統制と所有権を保持します。お客様は、AMI をエクスポートして、施設内または別のプロバイダで使用できます（ただし、ソフトウェアのライセンス制限に従います）。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。 AWS では、必要に応じてお客様がデータを AWS ストレージから出し入れすることを許可しています。S3 用 AWS Import/Export サービスでは、転送用のポータブル記憶装置を使用して、AWS 内外への大容量データの転送を高速化できます。AWS では、お客様がご自分のテープバックアップサービスプロバイダを使用してテープへのバックアップを実行することを許可しています。ただし、AWS ではテープへのバックアップサービスを提供していません。
第三者による不正アクセスからのデータの保護	a. クラウドデプロイモデルの選択。セキュリティがより低い可能性がある パブリッククラウド、セキュリティがより高い可能性があるハイブリッドクラウド、または最もセキュリティが高い 可能性があるプライベートクラウドのどれを検討したらよいですか?	AWS のコンプライアンスセキュリティチームは、Control Objectives for Information and related Technology (COBIT) フレームワークに基づき、情報セキュリティフレームワークを設定しました。AWS セキュリティフレームワークは、ISO 27002 ベストプラクティスおよび PCI データセキュリティ基準を統合しています。 詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。AWS は、サードパーティによる証明、認定、Service Organization Controls 1 (SOC 1) Type II レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 Amazon Virtual Private Cloud (Amazon VPC) で、アマゾン ウェブ サービス（AWS）クラウドの論理的に分離したセクションをプロビジョニングし、ここで、お客様が定義する仮想ネットワークで AWS リソースを起動することができます。独自の IP アドレス範囲の選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。Amazon VPC のネットワーク設定は容易にカスタマイズすることができます。例えば、インターネットとのアクセスが可能なウェブサーバーのパブリック サブネットを作成し、データベースやアプリケーションサーバーなどのバックエンドシステムをインターネットとのアクセスを許可していないプライベート サブネットに配置できます。セキュリティグループやネットワークアクセスコン

主要な領域	質問	AWS の回答
		トロールリストなどの複数のセキュリティレイヤーを活用し、各サブネットの Amazon EC2 インスタンスへのアクセスをコントロールすることができます。 加えて、既存のデータセンターと自分の VPC 間にハードウェア Virtual Private Network (VPN) 接続を作成することができるので、AWS クラウドを既存のデータセンターを拡張するかのように活用することができます。
	b. データの機密性。クラウドに保存またはクラウドで処理するデータは、分類され、機密であるかプライベートである、または当社のパブリックウェブサイトからの情報など、公開されたデータですか? データの集約により、個別の各データよりも機密性が高まりますか? たとえば、大量のデータを保存したり、危害が加えられた場合にアイデンティティの盗難が容易になるさまざまなデータを保存すると、機密性が高まる可能性があります。データの侵害があった場合に、それへの配慮について上層部や政府役人、一般に示すことはできますか?	AWS のお客様は、お客様のデータの統制と所有権を有しています。また、お客様の要件に合う構造化データ分類プログラムを導入することができます。
	c. 法律上の義務。さまざまな法律に準拠してデータを保護、管理するための義務にはどのようなものがありますか? たとえば、プライバシー法、公文書館法、データの種類に固有のその他の法律などです。契約上、ベンダーはこれらの義務を負うことに同意し、オーストラリア政府が満足いくように義務を果たす手助けをしてくれますか?	AWS のお客様は、適用可能な法律および規制に準拠する範囲で AWS を使用する責任を有しています。AWS は、業界の認定およびサードパーティによる証明、ホワイトペーパー（http://aws.amazon.com/security）を介してセキュリティおよび統制環境をお客様に伝えています。また、認定、レポート、その他の関連する文書を AWS のお客様に直接提供しています。 AWS はプライバシーに関するオーストラリアの考慮事項に関連して AWS の使用についてのホワイトペーパーを発行しており、http://d0.awsstatic.com/whitepapersp/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf から入手できます。

主要な領域	質問	AWS の回答
	d. データにアクセスできる国。データが保存、バックアップ、処理されるのは、どの国ですか? データが経由するのはどの国ですか? フェールオーバーや冗長性を持つデータセンターがあるのは、どの国ですか? これらの質問の答えが変更された場合、ベンダーは通知してくれますか?	AWS のお客様は、コンテンツとサーバーを配置する 1 つ以上の AWS リージョンを選択できます。これにより、具体的な地理的要件を持っているお客様が、選択する場所で環境を構築することができます。オーストラリアの AWS のお客様は、アジアパシフィック（シドニー）リージョンに専用で AWS サービスをデプロイし、コンテンツをオーストラリア大陸内に保存することができます。お客様がこの選択を行った場合、お客様がデータの移動を選択しない限り、コンテンツはオーストラリア内に配置されます。お客様は複数のリージョンにコンテンツをレプリケートしてバックアップできますが、AWS はお客様が選択した 1 つ以上のリージョンの外部にコンテンツを移動またはレプリケートすることはありません。 AWS はお客様のセキュリティに関して油断のない注意を払っており、召喚状や裁判所の命令、または該当する法律によって要求されるなど、法的に有効で拘束力のある命令に従う必要がある場合を除き、オーストラリア、米国、またはその他の政府からの要求に応じてデータを公開または移動することはありません。通常、米国以外の政府または規制団体は、有効で拘束力のある命令を取得するには、米国政府との相互法的援助契約など、認められた国際手順を使用する必要があります。さらに、AWS では法律で禁止される場合を除き、可能な場合はコンテンツを公開する前にお客様に通知し、お客様が公開からの保護手段を探せるようにしています。

主要な領域	質問	AWS の回答
	e. データの暗号化テクノロジー。ハッシュアルゴリズム、暗号化アルゴリズム、およびキー長が、ネットワークを移動中にデータを保護するために使用される DSD ISM によって適切であると見なされ、ベンダーのコンピュータとバックアップメディアの両方に保存されますか? ベンダーのコンピュータによって処理中のデータを暗号化する機能はまだ新しいテクノロジーであり、業界と学会によって現在調査対象の領域となっています。暗号化は、データが重要である期間中はデータを保護するために十分強力であると見なされていますか?	AWS では、S3、EBS、SimpleDB、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC セッションも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。お客様は、サードパーティの暗号化テクノロジを使用することもできます。AWS は、AWS インフラストラクチャ内で採用される必要な暗号化用の暗号キーを内部的に確立、管理しています。AWS は NIST で承認されたキー管理テクノロジーとプロセスを AWS 情報システムで使用して対称暗号キーを作成、管理、配布しています。対称キーの作成、保護、配布には、AWS が開発したセキュアキーおよび認証情報マネージャーが使用され、ホストで必要な AWS 認証情報、RSA パブリック/プライベートキー、および X.509 認証をセキュリティ保護、配布するために使用されます。 AWS 暗号化プロセスは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠のために、第三者の独立監査人によって確認されます。 AWS CloudHSM サービスにより、安全なキー管理に対する米国政府標準規格に適合するように設計/検証された HSM 内で暗号キーを保護することができるようになります。データ暗号化に使用される暗号キーを安全に生成、保存、管理することで、ユーザーだけが暗号キーにアクセスできるようになります。AWS CloudHSM により、アプリケーションのパフォーマンスを低下させることなく、厳密なキー管理要件に準拠することができます。 AWS CloudHSM サービスは Amazon Virtual Private Cloud (VPC)と共に動作します。CloudHSM は指定した IP アドレスで VPC 内にプロビジョニングされます。これにより、Amazon Elastic Compute Cloud (EC2)インスタンスに対して簡単でプライベートなネットワーク接続が可能になります。CloudHSM を EC2 インスタンス近くに配置することで、ネットワークレイテンシーは低減され、アプリケーションのパフォーマンスが向上します。AWS には CloudHSM への専用かつ排他的アクセスが用意されており、他の AWS のユーザーとは分離されています。AWS CloudHSM は複数のリージョンとアベイラビリティーゾーン（AZ） で利用でき、Amazon EC2 アプリケーションに対して安全で耐久性の高いキーストレージを追加することができます。
	f. 媒体のサニタイズ。耐用年数の終わりに、データを保存しているストレージメディアをサニタイズするために、どのようなプロセスが使用されていますか? また、それらのプロセスは DSD ISM によって適切と見なされていますか?	AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。

主要な領域	質問	AWS の回答
	g. ベンダーのリモートモニタリングと管理。ベンダーは、データを保存または処理しているコンピュータを管理していますか? 管理している場合、これは外国からリモートに実行されていますか、それともオーストラリアからですか? ベンダーはパッチコンプライアンスレポートやこの作業の実行に使用されるワークステーションのセキュリティに関するその他の詳細情報を提供していますか? また、ベンダーの従業員が信頼できない個人所有のノートパソコンを使用しないようにするために、どのような統制が導入されていますか?	IT インフラストラクチャを AWS に移行すると、お客様と AWS の責任分担モデルを構成します。この共有モデルは、ホストオペレーティングシステムや仮想レイヤーから、サービスが運用されている施設の物理セキュリティまで、様々なコンポーネントを AWS が運用、管理、およびコントロールするというものです。このため、お客様の運用上の負担を軽減する助けとなることができます。お客様の責任としては、ゲストオペレーティングシステム（更新やセキュリティパッチなど）、その他の関連アプリケーションソフトウェア、ならびに AWS より提供されるセキュリティグループファイアウォールの設定の責任と管理が想定されます。
	h. モニタリングおよび管理。既存のツールを、整合性の確認、コンプライアンスの確認、セキュリティのモニタリング、ネットワーク管理に使用し、これらのシステムがローカルに配置されているかクラウドにあるかを問わず、すべてのシステムの可視性を得ることはできますか? ベンダーが提供する追加のツールの使用方法を学習する必要がありますか? ベンダーは、モニタリングを実行できるこのようなメカニズムを提供していますか?	Amazon CloudWatch は、AWS クラウドリソースと AWS でお客様が実行するアプリケーションのモニタリングを提供します。詳細については、aws.amazon.com/cloudwatch を参照してください。また、AWS は、Service Health Dashboard にサービスの可用性に関する最新情報を公開しています。status.aws.amazon.com を参照してください。 AWS Trusted Advisor では、お客様の AWS 環境を検査し、コスト削減、システムパフォーマンスと信頼性の向上、セキュリティギャップの封鎖につながる推奨事項をお知らせします。
	i. データの所有権。当社がデータの法的な所有権を維持するのですか、または所有権はベンダーに帰属し、ベンダーが破産を申請した場合は清算人によって売却対象資産と見なされるのですか?	AWS のお客様は、お客様のデータの所有権と統制を保持します。AWS は、それぞれのお客様のコンテンツを、お客様が選択した AWS サービスをそのお客様に提供するためにのみ使用し、その他の目的に使用することはありません。AWS はお客様のコンテンツをすべて同じように扱い、お客様が AWS に保存するように選択するコンテンツの種類については把握していません。AWS は、お客様が選択したコンピューティング、ストレージ、データベース、およびネットワーキングサービスを使用できるようにするのみです。サービスを提供するために、お客様のコンテンツにアクセスすることはありません。

主要な領域	質問	AWS の回答
	j. ゲートウェイテクノロジー。安全なゲートウェイ環境を作成するために、ベンダーはどのようなテクノロジーを使用していますか? この例には、ファイアウォール、トラフィックフローフィルター、コンテンツフィルター、および該当する場合はウイルス対策ソフトウェアやデータダイオードがあります。	AWS ネットワークは、既存のネットワークセキュリティの問題に対する強固な保護機能を備えており、お客様はさらに堅牢な保護を実装することができます。詳細については、「AWS Overview of Security whitepaper」(http://aws.amazon.com/security) を参照してください。 Amazon の資産（ノートパソコンなど）は、E メールのフィルタリングとマルウェア検出を含むウイルス対策ソフトウェアで設定されています。 AWS ネットワークファイアウォール管理および Amazon のウイルス対策プログラムは、SOC、PCI DSS、ISO 27001、および FedRAMP[sm] への AWS の継続的な準拠の一環として、第三者の独立監査人によって確認されます。
	k. ゲートウェイの認定。ベンダーのゲートウェイ環境は政府のセキュリティ標準や規制に対して認定されていますか?	AWS は、AWS ゲートウェイ環境を含む、業界の認定と独立したサードパーティによる証明を取得します。
	l. E メールコンテンツのフィルタリング。E メールの Software as a Service では、ベンダーは機関の E メールコンテンツポリシーを適用できる、カスタマイズ可能な E メールコンテンツフィルタリングを提供していますか?	お客様はシステムを利用して E メール機能をホストできますが、その場合、E メールの入出力ポイントで適切なレベルのスパムおよびマルウェア保護を採用し、新しいリリースが利用可能になったらスパムとマルウェアの定義を更新するのはお客様の責任です。

主要な領域	質問	AWS の回答
	m. ベンダーの IT セキュリティ体制をサポートするポリシーとプロセス。ベンダーのコンピュータおよびネットワークセキュリティ体制が、脅威およびリスク評価、継続的な脆弱性の管理、セキュリティを組み込んだ変更管理プロセス、侵入テスト、ログおよび定期的なログ分析、オーストラリア政府が支持するセキュリティ製品の使用、オーストラリア政府のセキュリティ標準や規制への準拠を含むポリシーやプロセスによってどのようにサポートされているかの詳細情報を入手できますか?	AWS Information Security は、COBIT フレームワーク、ISO 27001 基準、および PCI DSS 要件に基づいて、ポリシーと手続きを規定しています。 AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。さらに、AWS は SOC 1 Type II レポートを発行しています。詳細については、SOC 1 レポートを参照してください。詳細については、「AWS Risk and Compliance Whitepaper」（http://aws.amazon.com/security）を参照してください。 AWS のお客様は、AWS が管理する主な統制を指定できます。主な統制はお客様の統制環境にとって不可欠であり、年次の会計監査などのコンプライアンス要件に準拠するには、その主な統制の運用効率について外部組織による証明が必要です。そのために、AWS は Service Organization Controls 1 (SOC 1) Type II レポートで幅広く詳細な IT 統制を公開しています。SOC 1 レポートの旧称は Statement on Auditing Standards (SAS) No. 70、Service Organizations レポートです。一般的に Statement on Standards for Attestation Engagements No. 16 (SSAE 16) レポートと呼ばれ、米国公認会計士協会（AICPA）が作成し、幅広く認められている監査基準です。SOC 1 監査は、AWS で定義している統制目標および統制活動（AWS が管理するインフラストラクチャの一部に対する統制目標と統制活動が含まれます）の設計と運用効率の両方に関する詳細な監査です。「Type II」は、レポートに記載されている各統制が、統制の妥当性に関して評価されるだけでなく、運用効率についても外部監査人によるテスト対象であることを示します。AWS の外部監査人は独立し、適格であるため、レポートに記載されている統制は、AWS の統制環境に高い信頼を置けることを示します。
	n. ベンダーの IT セキュリティ体制をサポートするテクノロジー。ベンダーのコンピュータおよびネットワークセキュリティ体制が、セキュリティパッチのタイムリーな適用、ウイルス対策ソフトウェアの定期的な更新、不明な脆弱性に対する保護のための深層防御メカニズム、可能な限り強力なセキュリティ設定で設定で強化されたオペレーティングシステムとソフトウェアアプリケーション、侵入検出/防止システム、およびデータ損失防止メカニズムを含む直接的な技術統制によってサポートされているかに関する詳細情報を入手できますか?	AWS は、サードパーティによる証明、認定、Service Organization Controls 1 (SOC 1) Type II レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 AWS セキュリティは、サービスエンドポイント IP アドレスに接するすべてのインターネットの脆弱性を定期的にスキャンします（お客様のインスタンスはこのスキャンの対象外です）。判明した脆弱性があれば、修正するために適切な関係者に通知します。さらに、脆弱性に対する外部からの脅威の査定が、独立系のセキュリティ会社によって定期的に実行されます。これらの査定に起因する発見や推奨事項は、分類整理されて AWS 上層部に報告されます。 さらに、AWS 統制環境は、通常の内部的および外部的リスク評価によって規定されています。AWS は、外部の認定機関および独立監査人と連携し、AWS の統制環境全体を確認およびテストしています。

主要な領域	質問	AWS の回答
	o. ベンダーの IT セキュリティ体制の監査。当社に提供された環境のスキャンおよびその他の侵入テストの実行を含む、ベンダーのセキュリティ手法の実装を監査できますか? 監査が可能でないという正当な理由がある場合、信頼できるどのサードパーティが監査やその他の脆弱性評価を実行しましたか? ベンダーが実施する内部監査の種類と、それらの評価に使用されるコンプライアンス標準と組織の推奨の手法（クラウドセキュリティアライアンスなど）は何ですか?最近の結果レポートのコピーを詳細に確認することはできますか?	AWS は、サードパーティによる証明、認定、Service Organization Controls 1 (SOC 1) Type II レポートなどの関連するコンプライアンスレポートを、NDA に従ってお客様に直接提供しています。 対象をお客様のインスタンスに限定し、かつ AWS 利用規約に違反しない限り、お客様はご自身のクラウドインフラストラクチャのスキャンを実施する許可をリクエストできます。このようなスキャンについて事前に承認を受けるには、AWS 脆弱性／侵入テストリクエストフォームを使用してリクエストを送信してください。 AWS Security は、外部の脆弱性脅威評価を実行するために、独立したセキュリティ会社と定期的に契約しています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。
	p. ユーザーの認証。Software as a Service を使用するためのユーザーのログインのためにベンダーがサポートする Identity & Access Management システムは何ですか?	AWS Identity and Access Management (IAM) により、お客様のユーザーの AWS サービスおよびリソースへのアクセスを安全にコントロールすることができます。IAM を使用すると、AWS のユーザーとグループを作成および管理し、アクセス権を使用して AWS リソースへのアクセスを許可および拒否できます。 AWS は、ユーザーの ID を 1 つの場所に維持することで、ユーザーの管理を容易にする ID フェデレーションをサポートしています。AWS IAM には SAML (Security Assertion Markup Language) 2.0 のサポートが含まれます。これは、多くの ID プロバイダにより使用されているオープンスタンダードです。この新機能によりフェデレーティッドシングルサインオン（SSO） が可能になり、Shibboleth や Windows Active Directory フェデレーションサービスなどの SAML 準拠の ID プロバイダと連携して、ユーザーが AWS マネジメントコンソールにログインしたり、AWS API をプログラムで呼び出したりすることができるようになります。
	q. データのコントロールの中央集中化。機関のユーザーが、信頼された運用環境以外で未承認または安全でないコンピューティングデバイスを使用して、Software as a Service で機密のデータを保存または処理できないようにするユーザートレーニング、ポリシー、技術統制は何ですか?	該当なし

主要な領域	質問	AWS の回答
	r. ベンダーの物理的なセキュリティ体制。ベンダーは、オーストラリア政府によって支持される物理的なセキュリティ製品やデバイスを使用していますか? ベンダーの物理データセンターはどのようにしてサーバー、インフラストラクチャ、およびそれらに保存されたデータの改ざんや盗難を防止するように設計されていますか? ベンダーの物理的なデータセンターは権威あるサードパーティによって認定されていますか?	AWS 定義の論理統制と物理統制の定義は、SOC 1 Type II レポート（SSAE 16）に文書化されています。また、このレポートは、この監査チームとコンプライアンスチームのレビューに使用できます。また、AWS ISO 27001 およびその他の認定も、監査人のレビュー用に使用できます。 物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。物理的アクセスは、建物の周辺および入り口において、監視カメラや侵入検知システムなどの電子的手段を用いる専門の保安要員その他の手段により、厳重に管理されています。権限を付与されたスタッフが 2 要素認証を最低 2 回用いて、データセンターのフロアにアクセスします。サーバー設置箇所への物理アクセスポイントは、AWS データセンター物理セキュリティポリシーの規定により、閉回路テレビ（CCTV）カメラで録画されています。録画は 90 日間保存されます。ただし、法的または契約義務により 30 日間に制限される場合もあります。 AWS は、このような特権を必要とする正規の業務を有する承認済みの従業員や契約社員に対して、データセンターへの物理的なアクセス権や情報を提供しています。すべての訪問者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが付き添いを行います。 物理的なアクセス、データセンターへのアクセスの承認、その他の関連統制については、SOC 1 Type II レポートを参照してください。 詳細については、ISO 27001 基準の付録 A、ドメイン 9.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
	s. ソフトウェアとハードウェアの調達。クラウドインフラストラクチャソフトウェアとハードウェアが正当なソースから供給され、配送中に悪意を持って変更されないようにするために、どのような調達プロセスが使用されていますか?	ISO 27001 基準に合わせて、AWS の担当者が AWS 専有インベントリ管理ツールを使用して、AWS ハードウェアの資産に所有者を割り当て、追跡および監視を行っています。AWS の調達およびサプライチェーンチームは、すべての AWS サプライヤとの関係を維持しています。 詳細については、ISO 27001 基準の付録 A、ドメイン 7.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。

主要な領域	質問	AWS の回答
ベンダーの顧客による不正アクセスからのデータの保護	a. 顧客の区分け。複数のテナント間で仮想化と "マルチテナンシー" メカニズムが適切な論理的分離とネットワークの分離を保証し、当社と同じ物理的なコンピュータを使用中の悪意を持った顧客がデータにアクセスできないようにするために、どのような保証が ありますか?	現在、Amazon EC2 は、高度にカスタマイズされたバージョンの Xen ハイパーバイザを利用しています。ハイパーバイザは、社内および社外の侵害対策チームによって新規および既存の脆弱性と攻撃進路を定期的に評価しています。また、ゲスト仮想マシン間の強力な隔離を維持するためにも適しています。AWS Xen ハイパーバイザのセキュリティは、評価および監査の際に独立監査人によって定期的に評価されています。 AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。お客様が自身のデータの統制と所有権を有しているので、データの暗号化を選択するのはお客様の責任です。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC セッションも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。
	b. セキュリティ体制の低下。ベンダーによるクラウドインフラストラクチャの使用は、機関の既存のネットワークセキュリティ体制を低下させますか? ベンダーは当社の明示的な同意なしに顧客の 1 社として当社を宣伝し、それが当社を対象とした攻撃につながることはありますか?	AWS のお客様は機密であると見なされ、AWS が明示的な同意なくお客様の詳細を公表することはありません。Amazon Virtual Private Cloud (Amazon VPC) で、アマゾン ウェブ サービス（AWS）クラウドの論理的に分離したセクションを確保し、ここで、お客様が定義する仮想ネットワークで AWS リソースを起動することができます。独自の IP アドレスレンジの選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイの設定など、仮想ネットワーク環境を完全にコントロールできます。
	c. 専用サーバー。当社の仮想マシンを実行する物理的なコンピュータに対してなんらかの制御を得ることはできますか? 追加の料金を支払って、当社と同じ物理的なコンピュータ（専用サーバーや仮想プライベートクラウドなど）を他の顧客が使用しないようにすることはできますか?	VPC により、お客様はハードウェアレベルで物理的に切り離されている Amazon EC2 インスタンスを起動でき、インスタンスはシングルテナントのハードウェアで実行されます。VPC は、「専用」テナンシーで作成できます。この場合、その VPC に対して起動されたインスタンスすべてがこの機能を利用します。また、「デフォルト」テナンシーで作成することもできますが、VPC に対して起動された特定のインスタンスについては、顧客が「専用」テナンシーを指定します。

主要な領域	質問	AWS の回答
	d. 媒体のサニタイズ。データの一部を削除した場合、別の顧客が使用できるようにする前にストレージメディアをサニタイズするためにどのようなプロセスが使用されますか? また、そのプロセスは DSD ISM によって適切であると見なされていますか?	お客様は、お客様のコンテンツの所有権と統制を維持しており、お客様がデータを削除できるようにしています。 AWS の処理手順には、ストレージデバイスが製品寿命に達した場合に、顧客データが権限のない人々に流出しないようにする廃棄プロセスが含まれています。AWS は DoD 5220.22-M（国家産業セキュリティプログラム運営マニュアル）または NIST 800-88（媒体のサニタイズに関するガイドライン）に詳述された技術を用い、廃棄プロセスの一環としてデータ破壊を行います。これらの手順を用いているハードウェアデバイスが廃棄できない場合、デバイスは業界標準の慣行に従って、消磁するか、物理的に破壊されます。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
悪意を持ったベンダーの従業員による不正アクセスからのデータの保護	a. データ暗号化キーの管理。ベンダーは、当社のデータの復号化に使用されるパスワードまたはキーを知っていますか? それとも、ベンダーのみが暗号化されたデータを持つようにするため、当社が自社のコンピュータでデータの暗号化と復号化を行うのですか?	AWS のお客様は、AWS のサーバー側暗号化サービスを利用しない場合、お客様独自の暗号化を管理しています。この場合、AWS はテナントごとに一意の暗号化キーを作成しています。詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
	b. ベンダーの従業員による詳細な調査。従業員を信頼できること確かめるために、ベンダーはどのような従業員雇用調査と詳細な調査プロセスを実施していますか?	AWS は従業員に対し、その従業員の役職や AWS 施設へのアクセスレベルに応じて、適用法令が認める範囲で、雇用前審査の一環として犯罪歴の確認を行います。
	c. ベンダーの従業員の監査。ベンダーの従業員はどのような堅牢な ID およびアクセス管理システムを使用していますか? ベンダーの従業員が行うアクションを記録および確認するため、どのような監査プロセスが使用されていますか?	AWS は、ISO 27001 基準に合わせて、AWS リソースに対する論理アクセスについて最小限の基準を示す正規のポリシー、手続きを規定しています。AWS SOC 1 Type 2 レポートには、AWS リソースに対するアクセスプロビジョニングを管理するために用意されている統制の概要が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
	d. データセンターへの訪問者。データセンターへの訪問者は常に付き添われますか? また、すべての訪問者の氏名とその他の詳細が確認、記録されますか?	すべての訪問者と契約業者は身分証明書を提示して署名後に入場を許可され、権限を有するスタッフが常に付き添いを行います。 AWS は、そのような権限に対して正規のビジネスニーズがある従業員や業者に対してのみデータセンターへのアクセスや情報を提供しています。従業員がこれらの特権を必要とする作業を完了したら、たとえかれらが引き続き Amazon または Amazon Web Services の従業員であったとしても、そのアクセス権は速やかに取り消されます。AWS 従業員によるデータセンターへのすべての物理的アクセスは記録され、定期的に監査されます。

主要な領域	質問	AWS の回答
	e. ベンダーの従業員による物理的な改ざん。ベンダーの従業員が誤ってケーブルを正しくないコンピュータに接続することを避け、ベンダーの従業員によるケーブルの意図的な改ざんの試みをすぐに明らかにするため、ネットワークケーブルの配線はオーストラリアの基準または国際的に認められた基準に従って行われていますか?	物理的セキュリティ統制には、フェンス、壁、保安要員、監視カメラ、侵入検知システムその他の電子的手段による周辺統制が含まれますが、これに限定されるものではありません。これには、ネットワークケーブルに対する適切な保護が含まれます。 AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、ISO 27001 基準の付録 A、ドメイン 9.1 を参照してください。AWS は、ISO 27001 認定基準への対応を確認する独立監査人から、検証および認定を受けています。
	f. ベンダーの請負業者。これらの質問の答えはベンダーのすべての請負業者に同じように該当しますか?	請負業者やベンダーのアクセスのプロビジョニングは、従業員と請負業者の両方に対して同じように管理され、その責任は、人事（HR）、企業運用サービス事業主によって分担されます。ベンダーは、従業員と同じアクセス要件に従います。
セキュリティインシデント処理	a. タイムリーなベンダーサポート。ベンダーは容易に連絡可能で、サポートのリクエストによく対応してくれますか? 可能な最大応答時間は SLA に記載されていますか? または単純なマーケティング要求でベンダーが最善を尽くすのでしょうか? サポートはローカルに提供されますか? それとも外国、または時間を追った手法で複数の国から提供されますか? ベンダーはどのようなメカニズムを使用して当社によるベンダーのサービスの使用に関するセキュリティ体制をリアルタイムで理解して、ベンダーがサポートを提供できるようにしていますか?	AWS サポートは、1 対 1 の、迅速なレスポンスを特徴とするサポートチャネルです。経験豊富な技術サポートエンジニアが 1 日 24 時間、年中無休で対応します。お客様の組織の規模や技術レベルにかかわらず、Amazon Web Services の製品と機能を活用していただけるようサポートいたします。 AWS サポート のどのレベルでも、AWS インフラストラクチャサービスのお客様が作成できるサポートケースの数は無制限となっています。サポート料金のお支払いは月単位で、長期契約は不要です。4 つのレベルがあるので、開発やビジネスのニーズに応じて最適なサポートレベルを柔軟にお選びいただけます。
	b. ベンダーのインシデント対応計画。ベンダーは、DSD ISM に規定されているインシデント対応手順と同様な方法で、セキュリティインシデントを検出し、応答する方法を指定するセキュリティインシデント応答計画を持っていますか? そのコピーを詳細に確認する	Amazon のインシデント管理チームは、業界標準の診断手順を採用しており、事業に影響を与えるイベント時に解決へと導きます。作業員スタッフが、24 時間 365 日体制でインシデントを検出し、影響と解決方法を管理します。AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。

主要な領域	質問	AWS の回答
	ことはできますか?	
	c. ベンダーの従業員のトレーニング。ベンダーのシステムの安全な使用方法について知り、セキュリティインシデントの可能性を認識するために、ベンダーの従業員が必要とする資格、認証、定期的な情報セキュリティの認識は何ですか?	ISO 27001 基準に合わせて、すべての AWS 従業員は、修了時に承認を必須とする定期的な情報セキュリティトレーニングを修了しています。従業員が制定されたポリシーを理解し遵守していることを確認するために、コンプライアンス監査を定期的に実施しています。詳細については、AWS セキュリティプロセスの概要ホワイトペーパー（http://aws.amazon.com/security）を参照してください。
	d. セキュリティインシデントの通知。同意されたしきい値よりも深刻なセキュリティインシデントについて、ベンダーは安全な通信で通知してくれますか（特に、ベンダーに責任がある可能性が高い場合）? ベンダーは、当社のデータの保存または処理に使用するコンピューティング機器を差し押さえる可能性がある法律執行機関または他の機関に自動的に通知を行いますか?	セキュリティインシデントの通知はケースバイケース、および該当する法律で要求される場合に処理されます。すべての通知は安全な通信で行われます。
	e. ベンダーサポートの範囲。データの不正な公開などのセキュリティ違反、または法的な電子開示や証拠提示を行う必要がある場合に、ベンダーはどの程度調査に協力してくれますか?	AWS はインフラストラクチャを提供し、その他の部分はお客様が管理します。例えば、オペレーティングシステム、ネットワーク構成、インストールされているアプリケーションなどです。お客様は、AWS を使用して保存または処理する電子文書の特定、収集、処理、分析、および作成に関連する法的手続きに、適切に対応する責任を持ちます。法的手続きに AWS の協力を必要とするお客様には、AWS は要請に応じて連携をとります。
	f. ログへのアクセス。フォレンシック調査を実行するために、時間を同期した監査ログやその他のログにアクセスする方法と、裁判所での適切な証拠となるようにログが作成および保存される方法は何ですか?	お客様は、自身のゲストオペレーティングシステム、ソフトウェア、アプリケーションの統制を有しており、これらのシステムの状態の論理的なモニタリングを開発するのは、お客様の責任です。AWS 情報システムは、ISO 27001 基準に合わせて、NTP (Network Time Protocol) を介して同期される内部システムクロックを利用しています。 AWS CloudTrail は、複雑なログシステムを実行する負荷の軽減に役立つ、ログユーザーアクティビティのシンプルなソリューションを提供します。詳細については、aws.amazon.com/cloudtrail を参照してください。 Amazon CloudWatch は、AWS クラウドリソースと AWS でお客様が実行するアプリケーションのモニタリングを提供します。詳細については、aws.amazon.com/cloudwatch を参照してください。また、AWS は、Service Health Dashboard にサービスの可用性に関する最新情報を公開しています。status.aws.amazon.com を参照してください。

主要な領域	質問	AWS の回答
	g. セキュリティインシデントの補償。ベンダーのアクション、問題のあるソフトウェアまたはハードウェアがセキュリティ違反の原因となった場合、ベンダーはどのようにして適正な補償を行いますか?	AWS の事故対応プログラム、計画、および手続きは、ISO 27001 基準に合わせて作成されています。AWS SOC 1 Type 2 レポートには、AWS が実行している具体的な統制活動に関する詳細情報が記載されています。 詳細については、「AWS Overview of Security Processes Whitepaper」（http://aws.amazon.com/security）を参照してください。
	h. データスピル。クラウドに保存するには機密性が高すぎると当社が考えるデータが誤ってクラウドに保存され、データスピルとして参照された場合、フォレンシックなサニタライズ手法を使用して、書き出されたデータをどのように削除できますか? データを削除するたびに、物理ストレージメディアの該当する部分はゼロで埋められますか?そうでない場合、削除されたデータが通常の操作の一部として顧客によって上書きされるのにどのくらい長くかかりますか? 通常、クラウドには未使用のストレージ容量が多く用意されています。書き出されたデータをベンダーのバックアップメディアからフォレンシックに削除することはできますか? 書き出されたデータは他にどこに保存されますか? また、それをフォレンシックに削除することはできますか?	お客様は、お客様のコンテンツの所有権と統制を有しています。AWS がお客様に代わって保存するデータはすべて、強力なテナント隔離セキュリティと統制機能で保護されています。AWS では、S3、EBS、EC2 など、ほぼすべてのサービスについて、お客様が独自の暗号化メカニズムを使用することを許可しています。VPC への IPSec トンネルも暗号化されます。また、Amazon S3 は、お客様向けのオプションとしてサーバー側の暗号化も提供しています。詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。 詳細については、AWS リスクとコンプライアンスホワイトペーパー（http://aws.amazon.com/security）を参照してください。

付録 D:用語集

認証:認証とは、誰か、または何かが、実際に申告された通りのものであるかどうか決定するプロセスのことです。

アベイラビリティーゾーン: Amazon EC2 の場所は、リージョンとアベイラビリティーゾーンから構成されます。アベイラビリティーゾーンは、他のゾーンからの影響を受けないように各々独立しています。利用は安価で、同一リージョン内であれば利用可能ゾーン間でのネットワーク接続待ち時間は少なくなります。

DSS: Payment Card Industry Data Security Standard (DSS) は、Payment Card Industry Security Standards Council によって作成され、管理されている国際的な情報セキュリティ基準です。

EBS: Amazon Elastic Block Store (EBS) は、Amazon EC2 インスタンスで使用するためのブロックレベルのストレージボリュームです。Amazon EBS ボリュームは、EC2 インスタンスのライフサイクルから独立して存続するストレージです。

FedRAMP[sm]: Federal Risk and Authorization Management Program (FedRAMP[sm]) は米国政府全体のプログラムであり、クラウド製品およびサービス向けのセキュリティ評価、認証、継続的なモニタリングに関する標準化された手法を提供します。FedRAMP[sm] は、リスク影響レベルが低程度および中程度の米国連邦政府機関のクラウドデプロイおよびサービスモデルに必須です。

FISMA:2002 年施行の連邦情報セキュリティマネジメント法。この法律では、各連邦機関が、機関の業務や資産をサポートする情報および情報システムに対して情報セキュリティを提供する機関全体のプログラムを作成し、文書化して、実施することを要求しています。対象には、他の機関、請負業者、またはその他の情報源が提供または管理する情報が含まれます。

FIPS 140-2:連邦情報処理規格（Federal Information Processing Standards/FIPS）出版物 140-2 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定する米国政府のセキュリティ基準です。

GLBA:1999 年施行の Gramm–Leach–Bliley Act（GLB または GLBA）。Financial Services Modernization Act とも呼ばれます。この法律は、非公開の顧客情報の公開やセキュリティおよびデータの完全性の脅威からの保護などに関して、金融機関の義務を規定しています。

HIPAA:1996 年施行の Health Insurance Portability and Accountability Act (HIPAA)。この法律は、プロバイダ、医療保険計画、および雇用者に対して、電子的なヘルスケアトランザクションと米国内の ID に関する米国の基準確立を要求しています。また、Administration Simplification の条項も、医療データのセキュリティとプライバシーに対応しています。これは、米国の医療システムで電子データのやり取りが広く利用されるように推奨することで、米国の医療システムの効率性と効果を改善するための基準です。

ハイパーバイザ:仮想マシンモニター（VMM）とも呼ばれるハイパーバイザは、ソフトウェア/ハードウェアプラットフォーム仮想化ソフトウェアであり、1 台のホストコンピュータで、複数のオペレーティングシステムを同時に稼動させることができるようにするものです。

IAM:AWS Identity and Access Management (IAM) は、お客様が複数のユーザーを作成し、AWS アカウント内でそのユーザーごとにアクセス許可を管理できるようにします。

ITAR:武器規制国際交渉規則（International Traffic in Arms Regulations/ITAR）は、米国軍需物資リスト（United States Munitions List/USML）の防衛関連の記事およびサービスのエクスポート/インポートを統制する米国政府規則です。政府機関および請負業者は、ITAR に準拠し、保護対象データへのアクセスを制限する必要があります。

ISAE 3402:国際保証業務基準書（International Standards for Assurance Engagements）第 3402 号（ISAE 3402）は、保証業務に関する国際基準です。国際監査および保証基準審議会（International Auditing and Assurance Standards Board/IAASB）によって制定されました。IAASB は、国際会計士連盟（International Federation of Accountants/IFAC）内にある基準を制定する審議会です。ISAE 3402 は、サービス組織についての保証レポートで、世界的に新しく認められている基準です。

ISO 9001:AWS の ISO 9001 認証は AWS クラウドで品質管理された IT システムを開発、移行、運用するお客様を直接サポートします。お客様は、独自の ISO 9001 プログラムや業界別の品質プログラム（ライフサイエンスでの GxP、医療機器での ISO 13485、航空宇宙産業での AS9100、自動車産業での ISO/TS 16949 など）の取得に、AWS の準拠レポートを証拠として活用できます。品質システムの要件がないお客様にも、ISO 9001 認証により AWS の保証や透明性が向上するというメリットがあります。

ISO 27001:IEC ／ IEC 27001 は 、 International Organization for Standardization (ISO) お よ び International Electrotechnical Commission (IEC) によって発行された Information Security Management System (ISMS) の基準です。ISO 27001 では、明示的な管理統制下に情報セキュリティを取り入れるための管理システムを正式に規定しています。正式の仕様になるということは、特定の要件が必須になることを意味します。そのため、組織が ISO／IEC 27001 を採用したことを主張する場合、この基準への準拠について監査され、認定を受けていることになります。

NIST: National Institute of Standards and Technology。この機関は、業界または政府のプログラムの必要に従って、詳細なセキュリティ基準を制定しています。機関が FISMA に準拠する場合、NIST 基準に従う必要があります。

オブジェクト: Amazon S3 に格納される基本的なエンティティです。オブジェクトは、オブジェクトデータとメタデータで構成されます。データ部分を、Amazon S3 から見ることはできません。メタデータは、オブジェクトを表現する名前と値のペアのセットです。これには最終更新日などのデフォルトメタデータや、Content-Type などの標準 HTTP メタデータが含まれています。開発者が、オブジェクトの格納時にカスタムメタデータを指定することもできます。

PCI: Payment Card Industry Security Standards Council のことを指します。PCI は、American Express、Discover Financial Services、JCB、MasterCard Worldwide、および Visa International が創設した独立機関であり、Payment Card Industry Data Security Standard の継続的な発展の管理を目的としています。

QSA: Payment Card Industry (PCI) Qualified Security Assessor (QSA) の称号は、PCI Security Standards Council によって、特定の資格要件を満たし、PCI コンプライアンス評価を実行する権限を持つ個人に与えられます。

SAS 70: Statement on Auditing Standards No. 70:Service Organizations は 、 Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) が発行する監査書です。SAS 70 は、サービス監査人がサービス組織（AWS など）の内部統制を評価し、サービス監査人のレポートを発行する際の指針を示しています。ま

た、SAS 70 は、1 つまたは複数のサービス組織を使用する組織の財務諸表の監査人に対する指針も示しています。SAS 70 レポートは、Service Organization Controls 1 レポートに変更されました。

サービス:ネットワークを通じて提供されるソフトウェアまたはコンピューティング機能（たとえば EC2、S3、VPC など）。

サービスレベルアグリーメント（SLA）:サービスレベルアグリーメントは、サービス契約の一部であり、サービスのレベルを正式に定義しています。SLA は、契約されている（サービスの）提供時間またはパフォーマンスを参照するために使用されます。

SOC 1: Service Organization Controls 1 (SOC 1) Type II レポートは、以前は Statement on Auditing Standards (SAS) 第 70 号、Service Organizations レポート（一般的には SSAE 16 レポート）と呼ばれ、米国公認会計士協会（American Institute of Certified Public Accountants/AICPA）が制定した幅広く認められている監査基準です。この国際基準は、International Standards for Assurance Engagements 第 3402 号（ISAE 3402）と呼ばれています。

SSAE 16: Statement on Standards for Attestation Engagements 第 16 号（SSAE 16）は、米国公認会計士協会（American Institute of Certified Public Accountants/AICPA）の監査基準審議会（Auditing Standards Board/ASB）が発行している証明基準です。この基準は、サービスをユーザー組織に提供する組織の統制についてレポートするためにサービス監査人が引き受ける業務に対応しています。このようなサービス組織の統制は、ユーザー組織の財務報告に係る内部統制（internal control over financial reporting (ICFR) に関連する可能性が高くなります。サービス監査人が 2011 年 6 月 15 日以降に完了したレポート期間については、SSAE 16 が Statement on Auditing Standards 第 70 号（SAS 70）の代わりに使用されるようになりました。

SOC 2: Service Organization Controls 2 (SOC 2) レポートは、サービス組織におけるセキュリティ、可用性、処理の完全性、機密性、プライバシーに関する内部統制を理解する必要がある様々な利用者に供するものです。このレポートは AICPA Guide:Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy に則って実施され、サービス組織とその内部統制の全体を理解しているステークホルダー（顧客、規制当局、取引先、供給者、取締役など）に利用されることを意図しています。

SOC 3:Service Organization Controls 3 (SOC 3) レポートは、サービス組織におけるセキュリティ、可用性、処理の完全性、機密性、プライバシーに関する統制状況を確認したいが、SOC 2 レポートを効果的に利用する必要性や知見をお持ちでない方向けに作成されるものです。このレポートは AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy に則って作成されます。SOC 3 レポートは一般向けレポートなので、自由に配布したり、ウェブサイトにシールとして掲載したりすることができます。

仮想インスタンス:AMI が起動されると、結果的に生じる実行システムがインスタンスとして参照されます。同一の AMI を基にするすべてのインスタンスは、完全に同じものとして開始しますが、インスタンスが終了または失敗する場合、それらに関する情報は失われます。

バージョン履歴

2015 年 4 月
- FedRAMP[sm]、HIPAA、SOC 1、ISO 27001、ISO 9001 の対象サービスを更新しました

2015 年 2 月
- FIPS 140-2 VPN エンドポイントおよび SSL 終端ロードバランサーを更新しました
- PCI DSS 用語を更新しました

2014 年 12 月
- 「認定とサードパーティによる証明」のサマリを更新しました

2013 年 11 月バージョン
- IPsec トンネル暗号化用語を編集しました

2013 年 6 月バージョン
- 「認定とサードパーティによる証明」のサマリを更新しました
- 付録 C:用語集を更新しました
- 書式設定に微調整を加えました

2013 年 1 月バージョン
- 「認定とサードパーティによる証明」のサマリを編集しました
- MPAA コンテンツセキュリティモデルに対する AWS の準拠状況（付録 B）を追加しました

2012 年 11 月バージョン
- 内容を編集し、認定の範囲を更新しました
- SOC 2 および MPAA へのリファレンスを追加しました

2012 年 7 月バージョン
- 内容を編集し、認定の範囲を更新しました
- CSA Consensus Assessments Initiative Questionnaire（付録 A）を追加しました

2012 年 1 月バージョン
- 更新された認定の範囲に基づいて、一部の内容を編集しました
- 一部の文法を修正しました

2011 年 12 月バージョン
- SOC 1/SSAE 16、FISMA Moderate、International Traffic in Arms Regulations、および FIPS 140-2 を反映して、「認定とサードパーティによる証明」を変更しました
- S3 サーバー側暗号化を追加しました
- クラウドコンピューティングに関する問題のトピックを追加しました

2011 年 5 月バージョン
- 初回リリース

通知

© 2010-2014 Amazon.com, Inc., or its affiliates.本文書は、情報提供の目的のみのために提供されるものです。本文書は、本文書の発行日時点での、AWS の提供商品を紹介するものであり、これらは事前の通知なく変更される場合があります。お客様は本文書の情報および AWS 製品の使用について独自に評価する責任を負うものとします。これらの情報は、明示または黙示を問わずいかなる保証も伴うことなく、「現状のまま」提供されるものです。本文書内のいかなるものも、AWS、その関係者、サプライヤ、またはライセンサーからの保証、表明、契約的なコミットメント、条件や確約を意味するものではありません。お客様に対する AWS の責任は AWS 契約によって規定されています。また、本文書は、AWS とお客様との間の契約に属するものではなく、また、当該契約が本文書によって修正されることもありません。